ISPGAYA
instituto superior politécnico

Mestrado em Cibersegurança e Auditoria de Sistemas Informáticos

Unidade Curricular de Dissertação/Projeto/Estágio

2022/23

Daniel Filipe Ribeiro Gonçalves

Gestão de acesso privilegiado: abordagem com a solução CyberArk

Dissertação no âmbito do mestrado Cibersegurança e Auditoria de Sistemas Informáticos orientado pelo Professor Doutor Fernando Luís Ferreira de Almeida e apresentada à Escola Superior de Ciência e Tecnologia.

setembro 2023

Agradecimentos

Agradeço aos meus pais por estarem sempre presentes ao meu lado, contribuindo para o meu sucesso pessoal, académico e profissional. Agradeço à minha namorada por todo o apoio, companheirismo e por me acompanhar nesta jornada.

Agradeço ao Professor Doutor Fernando Almeida pelo acompanhamento e disponibilidade demonstrada ao longo deste projeto. Agradeço ainda a todos os docentes do curso de Cibersegurança e Auditoria de Sistemas Informáticos pelo conhecimento transmitido.

Por último, agradeço ao Instituto Superior Politécnico Gaya pela contribuição para o meu percurso académico que iniciou na licenciatura e finda agora no mestrado, contribuindo também para a minha carreira profissional.

Resumo

Os ciberataques têm surgido com cada vez mais frequência, pelo que se torna fundamental adotar medidas de segurança. Um dos alvos sistemáticos dos ciberataques são as contas privilegiadas, estas podem permitir o acesso a sistemas virtualizados, base de dados, aplicações, dispositivos, controlos industriais, entre outros.

O acesso indevido a estas tecnologias por parte de atores mal-intencionados pode comprometer gravemente uma organização e afetá-la a nível financeiro e reputacional, pelo que se torna imperativo a adoção de medidas de segurança capazes de salvaguardarem a segurança informática.

No âmbito organizacional, podem ser tomadas várias medidas para proteger o acesso não autorizado à informação crítica, pelo que a presente dissertação aborda a área da gestão de acesso privilegiado, também designada como PAM (*Privileged Access Management*).

A adoção de soluções PAM auxilia na salvaguarda da segurança da informação, protegendo contra ameaças internas e externas, com o objetivo de evitar a divulgação de informação confidencial, roubo de identidade e violações de segurança.

A utilização de PAM permite reforçar a segurança no acesso aos recursos, sendo capaz de controlar, monitorizar e justificar cada sessão iniciada. É possível integrar PAM com várias tecnologias e adotar medidas complementares, por exemplo, autenticação multifator efetivando a legitimidade do uso da conta privilegiada.

Ao longo da dissertação, serão abordadas diversas temáticas que englobam a área de PAM, por exemplo, acessos e contas privilegiadas, gestão de credenciais e monitorização.

O presente trabalho visa assim oferecer, fundamentalmente, uma introdução à gestão de acesso privilegiado, tendo como ponto de partida uma arquitetura baseada na solução PAM da CyberArk, avançando para o desenvolvimento de *plugins* e componentes de conexão que permitem respetivamente gerir credenciais de forma segura e monitorizar sessões privilegiadas, finalizando com a discussão sobre a pertinência do uso deste tipo de soluções.

Palavras-chave: Acesso privilegiado, Gestão de Identidade, Contas privilegiadas, Gestão de credenciais, Gestão de Acesso Privilegiado, PAM, CyberArk

Abstract

Cyberattacks have been occurring with increasing frequency, so it is essential to adopt security measures. One of the systematic targets of cyberattacks are privileged accounts, which can allow access to virtualized systems, databases, applications, devices, industrial controls, among others.

Improper access to these technologies by malicious actors can severely compromise an organization and affect it financially and reputationally, so it becomes imperative to adopt security measures capable of safeguarding IT security.

Within an organization, several measures can be taken to protect unauthorized access to critical information, so this dissertation addresses the area of privileged access management, also known as PAM.

The adoption of PAM solutions helps safeguard information security, protecting against internal and external threats, in order to prevent the disclosure of confidential information, identity theft, and security breaches.

The use of PAM allows for increased security in accessing resources, being able to control, monitor, and justify each session initiated. It is possible to integrate PAM with various technologies and adopt complementary measures, for example, multi-factor authentication enforcing the legitimacy of the use of the privileged account.

Throughout the dissertation several topics that encompass the PAM area will be addressed, for example, privileged access and accounts, credential management and monitoring.

This work aims to offer an introduction to privileged access management, having as a starting point an architecture based on CyberArk's PAM solution, moving on to the development of plugins and connection components that allow managing credentials in a secure way and monitoring privileged sessions, ending with a discussion about the relevance of using this type of solutions.

Keywords: Privileged Access, Identity Management, Privileged accounts, Credential management, Privileged Access Management, PAM, CyberArk

Résumé

Les cyberattaques sont de plus en plus fréquentes et il est donc essentiel d'adopter des mesures de sécurité. L'une des cibles systématiques des cyberattaques sont les comptes à privilèges, qui peuvent permettre d'accéder à des systèmes virtualisés, des bases de données, des applications, des appareils, des contrôles industriels, etc.

Un accès inapproprié à ces technologies par des acteurs malveillants peut gravement compromettre une organisation et l'affecter financièrement et sur le plan de la réputation il est donc impératif d'adopter des mesures de sécurité capables de préserver la sécurité informatique.

Au niveau de l'organisation, plusieurs mesures peuvent être prises pour protéger l'accès non autorisé aux informations critiques. Ce mémoire aborde donc le domaine de la gestion des accès privilégiés, également connue sous le nom de PAM (Privileged Access Management).

L'adoption de solutions PAM permet de préserver la sécurité de l'information, en la protégeant contre les menaces internes et externes, dans le but de prévenir la divulgation d'informations confidentielles, l'usurpation d'identité et les failles de sécurité.

L'utilisation de la PAM permet de renforcer la sécurité de l'accès aux ressources, en étant capable de contrôler, de surveiller et de justifier chaque session initiée. Il est possible d'intégrer la PAM à diverses technologies et d'adopter des mesures complémentaires, par exemple l'authentification multifactorielle, rendant ainsi effective la légitimité de l'utilisation du compte privilégié.

Tout au long de la dissertation, plusieurs sujets qui englobent le domaine de la PAM seront abordés, par exemple, les accès et comptes privilégiés, la gestion et le contrôle des références.

Ce travail vise à fournir une introduction à la gestion des accès privilégiés, en commençant par une architecture basée sur la solution PAM de CyberArk, en passant par le développement de plugins et de composants de connexion permettant la gestion sécurisée des credentials et le contrôle des sessions privilégiées, et en terminant par une discussion sur la pertinence de l'utilisation de ce type de solution.

Mots-clés: Accès Privilégié, Gestion des Identités, Comptes privilégiés, Gestion des justificatifs, Gestion des Accès Privilégiés, PAM, CyberArk

Índice

Lista de figuras

Lista de abreviaturas e siglas

API	Application Programming Interface
APT	Ameaça Persistente Avançada
CID	Confidencialidade, Integridade e Disponibilidade
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CPM	Central Policy Manager
DR	Disaster Recovery
ENISA	Agência da União Europeia para a Cibersegurança
HIPAA	Health Insurance Portability and Accountability Act - Lei da Portabilidade e Responsabilidade dos Seguros de Saúde
IA	Inteligência Artificial
IACS	Automation and Control Systems
ICS	Industrial Control Systems - Sistemas de controlo industrial
ICS-CERT	The Industrial Control Systems Cyber Emergency Response Team
IIS	Internet Information Services
IoT	Internet of Things - Internet das Coisas
ITSM	Information Technology Service Management - Gestão de Serviços de Tecnologia da Informação
NIST	National Institute of Standards and Technology
NCSC	National Cyber Security Centre
PA	PrivateArk Client
PAM	Privileged Access Management - Gestão de Acesso Privilegiado
PCI DSS	Payment Card Industry Data Security Standard - Padrão de Segurança de Dados do Setor dos Cartões de Pagamento
PLC	Programmable Logic Controllers - Controladores Lógicos Programáveis
PSM	Privileged Session Manager

PTA	Privileged Threat Analytics
PVWA	Password Vault Web Access Interface
RBAC	Role-based access control - Controlo de acesso baseado em funções
RDP	Remote Desktop Protocol
RGPD	Regulamento Geral sobre a Proteção de Dados
SCADA	Supervisory control and data acquisition - Sistemas de controlo de supervisão e aquisição de dados
SDK	Software Development Kit
SI	Sistema de Informação
SSH	Secure Shell
TI	Tecnologia da Informação
TIC	Tecnologias de Informação e Comunicação
TPC	Terminal Plugin Controller
TTPs	Táticas, Técnicas e Procedimentos

1. Introdução

A evolução e inovação das tecnologias de informação e serviços de comunicação facilitam e melhoram o dia a dia dos indivíduos e das organizações. As tecnologias tornaram-se num elemento essencial na nossa sociedade e isso reflete-se em áreas como o setor das finanças, telecomunicações, transportes, educação ou saúde, aumentando significativamente o nível dos serviços oferecidos (Alkhazi et al., 2022). No entanto, esta evolução agregado à importância da internet nos dias de hoje, trazem também preocupações relacionadas com a segurança dos utilizadores e das organizações, que pode implicar, entre várias ocorrências, perdas financeiras e perda de confiança (Karabatak & Mustafa, 2018).

As falhas de segurança informática e vulnerabilidades do *software* presente nos sistemas informáticos, estão a ser explorados cada vez mais por atores maliciosos, tendo despertado a atenção de governos, empresas e meio académico (Santos et al., 2017). A utilização de sistemas antigos ou a falta de atualizações regulares estão na origem de vários ciberataques (Tervoort et al., 2020). Os atores maliciosos, seja através de engenharia social, como ataques de *phishing*, disseminação de *malware*, ataques de negação de serviço, entre outras técnicas, tentam obter acesso às redes informáticas corporativas e às aplicações de forma a comprometerem a sua infraestrutura, segurança da informação e outros recursos críticos (Al-Khater et al., 2020; Mallikarajunan et al., 2019; Z. Wang et al., 2020). A literatura refere também várias técnicas utilizadas por cibercriminosos para explorar vulnerabilidades e falhas informáticas e potenciar os ataques, tais como a utilização de *malware* como o *ransomware* ou vírus, falhas de segurança em dispositivos IoT (Internet das coisas) ou engenharia social (Sajal et al., 2019). É extremamente difícil manter um sistema totalmente seguro pelo que a utilização de código malicioso por parte de cibercriminosos é tida como uma das grandes ameaças no setor das tecnologias de informação. Deste modo, a necessidade de fortalecer a segurança informática quer para uso pessoal, quer organizacional é uma realidade (Krishnan & Egambaram, 2020). Os atores maliciosos procuram tipicamente comprometer contas com acessos privilegiados para poderem aceder a sistemas críticos e com informação sensível (Tirtadjaja et al., 2021), trazendo resultados que podem ser devastadores para as organizações (Moses & Rowe, 2015). As contas privilegiadas são contas com capacidade de mudar ou impactar um serviço operacional, podendo ser definidas como contas de administrador com níveis mais altos de permissões para aceder a sistemas e aplicações. Por isso, um utilizador com acesso a contas privilegiadas pode ter acesso a informações confidenciais de uma organização e, eventualmente, comprometer a segurança dos dados, redes sociais, entre outros ativos (Walker, 2019).

Com isso, o presente trabalho permitirá obter uma compreensão ampla sobre a área de gestão de acesso privilegiado e como pode impactar positivamente as organizações, no sentido de reforçarem a sua segurança no ciberespaço e obterem maior controlo e monitorização quando utilizados acessos privilegiados por parte dos utilizadores.

1.1. Enquadramento

A gestão de acesso privilegiado é um tema relevante no contexto atual das organizações. Estas têm sido alvos de atores maliciosos, internos e externos, com o objetivo de comprometerem contas privilegiadas. As contas privilegiadas possuem níveis de acesso elevados aos sistemas e recursos críticos organizacionais, que permitem aceder a informações críticas e realizar ações não autorizadas. O comprometimento destas contas representa um risco considerável ao nível da segurança da informação, pois podem resultar em violações de dados, acesso não autorizado a sistemas e outros recursos, implicando graves prejuízos financeiros e danos reputacionais.

1.2. Objetivos

O presente estudo sobre a gestão de acesso privilegiado teve como objetivo realizar a revisão da literatura de modo abrangente, bem como apresentar a arquitetura base utilizada na componente prática do estudo, nomeadamente, o desenvolvimento de componentes de conexão e CPM *plugins* (Central Policy Manager *plugins*). A revisão da literatura desempenhou um papel essencial na compreensão do tema e faz a ligação entre a segurança da informação, a cibersegurança e a área de gestão de acesso privilegiado e, assim sendo, é explicitada a pertinência sobre o uso de PAM, os conceitos, desafios e benefícios inerentes a esta área. Por fim, na componente prática do estudo, foi apresentada a arquitetura base da solução PAM da CyberArk que alicerçou os desenvolvimentos realizados.

Em suma, a parte inicial do estudo, nomeadamente, a revisão da literatura, pretendeu fornecer uma visão abrangente sobre a área de PAM para, no final, com o desenvolvimento de componentes de conexão e *plugins* integrados na solução da CyberArk, comprovar a pertinência do uso desta tecnologia por parte das organizações e como estas podem efetuar a gestão de credenciais e sessões privilegiadas com maior segurança e controlo.

1.3. Relevância do estudo

A gestão de acesso privilegiado é uma área com foco na gestão de identidades, nomeadamente, contas privilegiadas. As soluções PAM permitem a gestão e controlo de contas privilegiadas, contas essas com privilégios elevados aos sistemas organizacionais. O estudo permitiu compreender os alvos típicos dos cibercriminosos, que incidem sobretudo nas contas privilegiadas e quais as soluções que existem para fazer face a estes atores. Constatou-se que a introdução de PAM nas organizações pode auxiliar na mitigação de riscos de ciberataques, reduzir ameaças internas e externas e melhorar a eficiência operacional da gestão de contas privilegiadas.

Portanto, o paralelismo do estado da arte com os desenvolvimentos práticos efetuados neste estudo auxiliou na compreensão de como a área de PAM pode contribuir para atingir a segurança das organizações e outros objetivos como a gestão eficaz de contas privilegiadas, redução de riscos, atingir a conformidade regulatória, entre outos benefícios.

1.4. Metodologia

A metodologia adotada foi baseada numa abordagem teórica abrangente e prática, com foco na compreensão da arquitetura da solução PAM da CyberArk, e com o desenvolvimento de componentes de conexão e *plugins* e a sua integração com a ferramenta da CyberArk. Inicialmente, foi realizada a revisão teórica para obter uma compreensão aprofundada sobre o tema em estudo, nomeadamente, os conceitos, benefícios, desafios, entre outros. Foram identificados os riscos associados ao acesso remoto privilegiado e à gestão de contas privilegiadas, explicitado através da revisão da literatura e, posteriormente, com os desenvolvimentos efetuados, ou seja, como é que esses riscos podem diminuir tendo como ponto central soluções PAM.

Concluindo, na realização deste estudo foi adotada a metodologia qualitativa, com o objetivo de verificar se os benefícios da utilização de PAM, referidos na literatura, estão estritamente relacionados com os resultados obtidos nos desenvolvimentos práticos efetuados.

1.5. Resultados esperados

Os resultados esperados com o estudo são os seguintes:

- Revisão da literatura existente: Espera-se realizar uma revisão da literatura abrangente sobre a gestão de acesso privilegiado, CyberArk e outros temas relevantes relacionados com a área de PAM. Isso permitirá obter informação atualizada sobre o conhecimento teórico disponível sobre o assunto em estudo.
- Segurança do acesso remoto privilegiado: O estudo realizado tem o objetivo de proporcionar uma compreensão aprofundada dos desafios relacionados com o acesso remoto privilegiado. Espera-se identificar as melhores práticas para mitigar esses desafios, fortalecendo a segurança dos acessos remotos e reduzir os riscos associados.
- Solução CyberArk: Espera-se obter um conhecimento base sobre a arquitetura da solução PAM da CyberArk, como os tipos de servidores necessários e como estes interagem entre si.
- Desenvolvimentos: É expectável que os desenvolvimentos de componentes de conexão e *plugins* contribuam para auxiliar a compreensão sobre como é possível integrar inúmeras tecnologias com PAM. Para além disso, é também fundamental entender as funcionalidades destes componentes e *plugins* que permitem auxiliar na gestão segura de contas e sessões privilegiadas.

Com os resultados esperados enumerados acima, pretende-se que este estudo forneça uma base sólida sobre a área de gestão de acesso privilegiado, como é que soluções PAM permitem a gestão automática, eficaz e segura de contas privilegiadas. Pretendeu-se também abordar a importância do uso destas soluções por parte das organizações para fazer face aos constantes ciberataques que estas enfrentam, e como PAM se pode tornar num ponto chave, ajudando a fortalecer a segurança da informação, mitigando riscos associados a violações de segurança e auxiliar na conformidade regulatória.

Por fim, pretendeu-se fazer a ligação da revisão da literatura com os desenvolvimentos práticos realizados, de modo a comparar as duas vertentes e discutir os resultados obtidos.

1.6. Estrutura da dissertação

O estudo encontra-se estruturado da seguinte forma:

- Capítulo 2 (Revisão da literatura), são apresentados os conhecimentos e conceitos fundamentais para uma visão abrangente sobre a segurança da informação, a cibersegurança, incidentes e violações de segurança e como as ameaças como atores maliciosos internos e externos procuram comprometer contas privilegiadas. Por fim, é efetuada a revisão teórica sobre a gestão de identidades.
- Capítulo 3 (Gestão de Acesso Privilegiado), é fornecida uma visão ampla sobre a área de gestão de acesso privilegiado, nomeadamente, a importância das contas privilegiadas nos sistemas organizacionais e como estas devem ser protegidas para evitar danos catastróficos para as organizações. São também abordados tópicos como acesso remoto, cadeia de ataque na gestão de identidades, fluxo de funcionamento típico de uma solução PAM, assim como benefícios e boas práticas.
- Capítulo 4 (Descrição do estudo), é efetuada uma descrição teórica que auxilia na compreensão do trabalho e o contexto do mesmo.
- No Capítulo 5 (Metodologia de investigação) é apresentada a descrição da metodologia de trabalho adotada.
- No Capítulo 6 (Apresentação, análise e discussão dos resultados) é apresentada a arquitetura que tem como base o estudo realizado. É efetuada a introdução aos servidores e componentes que constituíram a base deste projeto, seguido depois do desenvolvimento prático e discussão dos resultados.
- No Capítulo 7 (Contributos e limitações do estudo) são apresentados os fatores que, de alguma forma, limitaram o estudo.
- Capítulo 8 (Conclusões) refere-se à conclusão do estudo e breve discussão sobre a área de PAM.

2. Revisão da literatura

Neste capítulo é realizada a introdução à segurança da informação e cibersegurança. Na sequência destes tópicos, são também abordados eventos indesejados como incidentes e violações de segurança, bem como as ameaças que estão em constante evolução. Para além disso, é ainda abordado o tópico de gestão de identidade, com foco na gestão de acesso privilegiado devido à necessidade das organizações protegerem os seus sistemas, dados e outros recursos críticos perante as constantes ameaças às identidades.

2.1. Segurança da Informação

As empresas cada vez mais estão interessadas em serviços tecnológicos para acelerar os seus processos de negócio comparativamente com os processos tradicionais, para isso, tornou-se necessário proteger os sistemas contra as ameaças, tornando-os mais eficientes e dando maior enfase à segurança da informação (Alkhudhayr et al., 2019; Kirilchuk et al., 2022; Mirtsch et al., 2021). Os sistemas de informação (SI) estão expostos a vários tipos de ameaças que podem provocar pequenas perdas, como a destruição total do sistema de informação, bem como perdas financeiras significativas (A. Grishaeva & I. Borzov, 2020; Falowo et al., 2022). Os danos causados pelas ameaças podem afetar a confidencialidade ou integridade dos dados, assim como afetar a disponibilidade dos servidores (Karim et al., 2021; Tsochev & Stankov, 2020). Torna-se assim num desafio diário, a constante monitorização das ameaças por parte das organizações, onde tentam compreender quais as ameaças que podem afetar os seus ativos de informação e como podem combate-las (Alsowail & Al-Shehari, 2020; Jayabalan, 2020; Jouini et al., 2014).

As tecnologias de informação aumentaram consideravelmente as oportunidades de negócio (Ayisi Nyarko & Kozári, 2021; Mohammed et al., 2020), contudo, estas oportunidades trouxeram consigo riscos para a segurança da informação (Badsha et al., 2019; Khan et al., 2022; Soomro et al., 2016). Um dos acrónimos mais conhecidos e debatidos na segurança da informação é a "CIA", ou CID em português – o que se traduz em confidencialidade, integridade e disponibilidade, e representa os pilares fundamentais da segurança da informação (Warkentin & Orgeron, 2020). Os termos confidencialidade, integridade e disponibilidade têm sido bastante utilizados em contexto militar desde há milhares de anos, por exemplo, no tempo de Júlio César desde a Guerra das Gálias contra as tribos gaulesas (Baybulatov & Promyslov, 2020). Estes pilares servem para garantir a segurança de qualquer sistema de informação, como redes informáticas, sistemas de *software* ou sistemas *cloud*, assegurando a proteção dos dados ou das informações desses sistemas (Singh et al., 2018).

Relativamente à confidencialidade, o primeiro pilar, este consiste em proteger contra o acesso não autorizado, garantindo a segurança das informações, redes e sistemas. Existem várias tecnologias que permitem reforçar a segurança da informação, salvaguardando, nomeadamente, a confidencialidade, estas devem incluir a encriptação e autenticação robusta e controlos de acesso rigorosos (Panek, 2020). Em suma, a confidencialidade consiste em garantir que os dados são assegurados e que são apenas revelados às partes a que se destinam (Mnjama et al., 2017). A integridade está relacionada com a garantia da autenticidade da informação, pois não deve ser modificada ou destruída por indivíduos que não tenham autoridade para realizar tal atividade. Existem várias medidas para garantir a integridade dos dados como a utilização de antivírus, criação de protocolos de autenticidade e de não repúdio, utilização de *checksum*, entre outros (Asllani et al., 2018). Por fim, a disponibilidade é a capacidade do acesso à informação a partir de um local específico e no formato correto quando necessário. Quando os dados não estão disponíveis sempre que necessário pode levar a perdas consideráveis e irrecuperáveis (Mishra et al., 2018). Falhas típicas que afetam a disponibilidade são os casos de ataques de negação, falhas de energia, incêndios ou catástrofes ambientais, pelo que é fundamental realizar cópias de segurança, dispor de sistemas redundantes, armazenamento de dados fora do local e garantir a proteção física dos sistemas de informação (Asllani et al., 2018). Para além destas características, a norma ISO 27000 refere também a pertinência de outras propriedades importantes para a segurança da informação como a autenticidade, a responsabilidade, o não-repúdio e a fiabilidade (Monev, 2020).

A segurança é uma combinação de pessoas, processos e tecnologia, pelo que a sensibilização das pessoas para a segurança da informação é um elemento fulcral para combater as ciberameaças (Alkhazi et al., 2022). Esta é assim considerada uma parte essencial da gestão das tecnologias de informação devido ao papel fulcral que assume na continuidade de negócio de uma organização (Prabowo et al., 2018).

Em suma, a segurança da informação é definida como a proteção da informação, dos sistemas e do *hardware* que utiliza, armazena e transmite a informação, para garantir a salvaguarda dos dados e a proteção dos procedimentos operacionais (Alkhudhayr et al., 2019). Os autores Reid e Van Niekerk, definem como um processo que envolve a proteção da informação contra ameaças, com o objetivo de garantir a continuidade do negócio, obter conformidade legal, manter vantagens competitivas, minimizar os riscos comerciais e maximizar o retorno dos investimentos e as oportunidades de negócio. As soluções de segurança da informação envolvem a proteção física, processual e lógica da informação e envolvem pessoas, processos e tecnologias (Reid & Van Niekerk, 2014). As organizações têm, portanto, vindo a aumentar o seu orçamento para reforçar a segurança informática, tendo em consideração as ações conscientes e inconscientes que ameaçam os

SI. As ameaças podem ser internas ou externas à organização, pelo que os atores maliciosos focam-se, tipicamente, na apreensão de contas privilegiadas, pois estas têm autorizações mais amplas aos sistemas de informação, ao contrário de outro tipo de contas. De realçar que, as ameaças internas são muitas vezes descuradas pelas equipas de TI das organizações, pois estas tendem a dar maior relevância a fatores externos. Constata-se que os ataques internos têm como base as tecnologias, contudo, o fator humano não deve ser negligenciado. O treino e a consciencialização dos funcionários devem ser postos em prática, assim como abordagens orientadas para a tecnologia, para auxiliar na mitigação de ataques internos (Sindiren & Ciylan, 2018).

2.2. Cibersegurança

A sociedade e as organizações em geral estão cada vez mais centradas na informação, isto significa que os indivíduos estão gradualmente mais expostos a riscos e ameaças relacionadas com as suas transações ou informações. Isto levou à definição de outro tipo de segurança, nomeadamente, a cibersegurança. Especialistas referem que os utilizadores das tecnologias de informação necessitam de níveis básicos de conhecimento e sensibilização no domínio da cibersegurança. Com isso, há efetivamente a necessidade de um esforço conjunto, entre a sociedade, governos e organizações privadas para combater os problemas de segurança. Estas questões afetam indivíduos que utilizam o ciberespaço, seja no contexto privado ou social, tornando pertinente esta área. A cibersegurança remete para a proteção dos interesses de um indivíduo, sociedade ou nação, assim como os respetivos ativos que necessitam de proteção contra os riscos relacionados com a sua interação com o ciberespaço (Reid & Van Niekerk, 2014). Sendo assim, o ciberespaço desempenha um papel importante em todos os processos da sociedade atual, o que engloba a política, a economia, a tecnologia, questões sociais, entre outros (Starodubtsev et al., 2020). O conceito ciberespaço é algo difícil de definir, pelo que a literatura apresenta várias definições sobre o mesmo. Este pode ser definido como uma informação virtual, constituída por uma componente física – computadores, sistemas e infraestruturas, capaz de assegurar a interação dos sistemas. Permite a interação das redes e os seus utilizadores, sendo a informação transmitida, guardada e partilhada. Baseia-se em infraestruturas físicas e recursos humanos georreferenciados, relacionados às categorias de soberania, nacionalidade e propriedade (Rohith & Batth, 2019). Outra definição presente na literatura considera o ciberespaço como um ambiente informático virtual ou meio eletrónico que auxilia a comunicação *online*, por exemplo, a conexão entre indivíduos através das telecomunicações e computadores, permitindo armazenar, modificar ou trocar dados (Koppisetty et al., 2019).

A cibersegurança consiste na prevenção ou mitigação de ações maliciosas que têm o objetivo de comprometer sistemas ou aceder a informações importantes (Bogoda et al., 2019). O termo cibersegurança é bastante popular e relevante para os sistemas digitais modernos, por isso, tal como mencionado, o modelo tríade CIA assume uma elevada preponderância também no contexto da cibersegurança, com o objetivo de proteger a confidencialidade, manter a integridade e garantir a disponibilidade. A cibersegurança é utilizada em dois domínios, na tecnologia da informação e na tecnologia operacional. Ambas estão relacionadas com sistemas de *software* e *hardware* ligados em rede com o objetivo de lidar com informação. As tecnologias de informação referem-se a uma grande diversidade de empresas, por exemplo, companhias de seguro, bancos ou governos, com o propósito de gerirem o seu negócio. Enquanto que, as tecnologias operacionais representam os sistemas informáticos dedicados à monitorização e controlo de dispositivos físicos, por exemplo, bombas, válvulas ou reguladores. As tecnologias operacionais referem-se assim a sistemas de controlo de supervisão e aquisição de dados (SCADA), controladores lógicos programáveis (PLC) ou outros componentes de sistemas de controlo e automação industrial (IACS) (Baybulatov & Promyslov, 2020). A cibersegurança partilha grande parte do espaço da segurança da informação, protegendo a informação e as tecnologias da informação e comunicação, assegurando a proteção do ciberespaço. A segurança da informação relaciona o fator humano com os vários papéis que este assume no processo de segurança, enquanto que, a cibersegurança refere os seres humanos como potenciais alvos de ciberataques ou mesmo participando inconscientemente nesses ataques. Apesar de as pessoas continuarem a ser vistas como uma ameaça e vulnerabilidade, estas são consideradas um ativo importante que deve ser protegido no ciberespaço. Deste modo, a cibersegurança pode ser definida como a proteção de ativos, nomeadamente, pessoas, aparelhos domésticos, infraestruturas de comunicação e informação, recursos dos sistemas de informação de um individuo ou organização, assim como, a sociedade em geral, incluindo infraestruturas críticas nacionais, ou seja, engloba a proteção de qualquer pessoa ou coisa que possa ser atingida no ciberespaço. A cibersegurança promove assim a proteção de ativos, tendo em consideração as vulnerabilidades existentes na utilização das tecnologias de informação e comunicação (TIC) que compõem a base do ciberespaço, assim como aqueles se o utilizam (Von Solms & Van Niekerk, 2013).

A cibersegurança é assim parte integrante da segurança da informação. A segurança das aplicações, a segurança das redes, a segurança da *cloud* ou infraestruturas críticas estão inseridas na cibersegurança. Os controlos de acesso, os controlos processuais, os controlos de conformidade e os controlos técnicos integram a segurança da informação. Em suma, o conceito cibersegurança tem o objetivo de proteger o ciberespaço contra ciberataques, enquanto que a segurança da informação tem o propósito de proteger a informação contra ameaças digitais ou físicas (Taherdoost, 2022).

2.3. Incidentes e Violações de segurança

Os incidentes de cibersegurança têm assumido cada vez mais protagonismo, atingido organizações em todo o mundo. Estas estão a lutar contra a evolução das ameaças, e tentam acompanhar este cenário que está em constante mudança (Sohime et al., 2020). Os termos incidente e violação são termos bastante utilizados no domínio da segurança da informação. De acordo com a Verizon, incidente refere-se a um evento de segurança que compromete a integridade, confidencialidade ou disponibilidade de um ativo de informação. Relativamente à violação de segurança, esta organização define como um incidente que resulta na divulgação confirmada de dados a uma parte não autorizada. Segundo dados do relatório sobre investigações de violações de dados de 2022, existem quatro caminhos que podem ameaçar as organizações, nomeadamente, credenciais, *phishing*, exploração de vulnerabilidades e *botnets*. Dados deste relatório, demonstram que a disseminação de *ransomware* continua a aumentar e a exponenciar os ganhos dos cibercriminosos, no mesmo sentido a exploração e comprometimento da cadeia de abastecimento continuaram com números elevados, pelo que em 2021 foi responsável por 62% dos incidentes. Enquanto que, erros, como por exemplo, um sistema de armazenamento de *cloud* mal configurado tem também uma representatividade considerável assumindo 13% das violações de segurança em 2021. No ano de 2022, constatou-se que o fator humano continuou a ter grande impacto nos incidentes e violações de segurança, isto engloba situações como credenciais roubadas, esquemas de *phishing*, utilização indevida, entre outros (Verizon, 2022).

O panorama das ciberameaças está assim em constante mutação, cada vez mais complexo e sob várias formas, sendo assim é fundamental compreender os cibercriminosos e como eles operam. A ciberdefesa proativa, orientada por informações e centrada na sensibilização e preparação contra ataques previstos por parte das organizações podem auxiliar a entender o âmbito de um ataque e responder a questões tais como – quem, o quê, onde, quando, porquê e como. A pergunta "quem" refere-se à atribuição do atacante e identifica assim o individuo, grupo, organização ou nação que realizou a operação. "O quê" permite entender o contexto do ataque, ao passo que o "onde" está relacionado com a origem do ataque e o seu alvo. O "quando" remete para a data e hora do ataque e pode ser determinístico ou probabilístico, e o "porquê" ajuda a esclarecer a motivação, as metas e os objetivos do adversário. Por fim, o "como" é composto pelas designadas TTPs, ou seja, as táticas, técnicas e procedimentos necessários para a realização do ataque (Mavroeidis et al., 2021).

2.4. Ameaças

Conforme o relatório da Verizon de 2021, 70% das violações de dados envolveram o abuso de privilégios, isto pode ter sido provocado por contas comprometidas, negligência ou ameaças internas, resultando no acesso e exfiltração de dados sensíveis (Check Point, 2022b). Assim como evidenciado anteriormente, os ciberataques estão a tornar-se um fator de risco mundial (Bhardwaj et al., 2021; M. I. Ali et al., 2020), pelo que a utilização constante de tecnologias como a computação *cloud*, a internet móvel ou a IoT tornaram o ciberespaço numa enorme fonte de ameaças (Tsochev et al., 2020). Ataques conhecidos como *worms*, cavalos de troia, *botnets* ou APT (ameaça persistente avançada), entre outros, materializam essas ameaças colocando em risco a segurança da informação das organizações, podendo comprometer alvos empresariais e obter vantagens económicas (Jin et al., 2018). Dada esta constante evolução das tecnologias de informação e comunicação, e a crescente utilização da internet, tornaram as organizações mais propensas a vários tipos de vulnerabilidades (Jouini et al., 2014). Por isso, devido à exploração dos sistemas de informação e dos dados organizacionais, a preocupação com a cibersegurança e a sua gestão têm aumentado (Battaglioni et al., 2022).

Uma ciberameaça é uma atividade com o objetivo de comprometer a segurança de um sistema de informação, pode afetar a integridade, confidencialidade ou disponibilidade de um sistema ou informação. Os atores que materializam essas ameaças, podem ser indivíduos isolados, hacktivistas, grupos terroristas, estados, entre outros grupos, com intenções maliciosas, que exploram e aproveitam vulnerabilidades para obter acesso a dados, dispositivos, sistemas e redes das vítimas. As motivações podem variar dependendo do grupo de atores, mas pode incidir no domínio geopolítico, ideológico, fatores de descontentamento, ganhos financeiros, entre outros motivos (Northern Ireland Security Centre, 2020). As ameaças de segurança podem ser de origem interna ou externa às organizações. Os ataques de pessoas internas, como funcionários, fornecedores ou outras entidades parceiras representam uma ameaça maior comparativamente com os ataques externos (Macak et al., 2020). Estes podem ser vistos como infiltrados, atuando assim contra os interesses das organizações que representam. Estes atores internos maliciosos representam, efetivamente, uma ameaça devido ao conhecimento interno organizacional que possuem sobre os recursos, sistemas, dados e operações (Rahman et al., 2022). Desta forma, as organizações estão cada vez mais focadas neste tipo de atores (Gheyas & Abdallah, 2016; Le & Zincir-Heywood, 2021), sendo uma fonte de clara preocupação para a sua cibersegurança (Schoenherr & Thomson, 2020).

De acordo com a CISA (Cybersecurity and Infrastructure Security Agency), organização dos Estados Unidos da América com a missão de liderar e assegurar a segurança e resiliência das infraestruturas críticas do país, categoriza as ameaças da seguinte forma: intencionais, não intencionais (por negligência e acidental), ameaças de conluio e ameaças de terceiros. Estes termos estão definidos abaixo (Cybersecurity and Infrastructure Security Agency, 2020):

- **Ameaça não intencional por negligência:** refere-se ao momento em que um funcionário expõe uma organização a uma ameaça por descuido. Exemplos práticos de neglicência são, por exemplo, quando os funcionários optam por ignorar as políticas de segurança colocando em risco as suas organizações, a perda de um dispositivo com informações sensíveis, ou ignorar as atualizações dos sistemas.
- **Ameaça não intencional acidental:** quando um funcionário, por erro, provoca um risco não intencional, como por exemplo, quando através de um erro de digitação são enviados emails para endereços eletrónicos errados ou quando funcionários são enganados por esquemas de *phishing*.
- **Ameaça intencional:** quando os funcionários tomam ações para prejudicar as organizações, seja para benefício pessoal, por falta de reconhecimento, algum tipo de descontentamento ou por motivos de despedimento, sendo designados por atores maliciosos. Exemplo de ameaças intencionais são os casos de fuga de informação sensível, roubo de dados ou propriedade intelectual, entre outros.
- **Ameaça de conluio:** quando os funcionários de uma organização colaboram com atores externos com o objetivo de comprometer uma organização. Casos em que cibercriminosos recrutam funcionários de empresas para cometer algum tipo de fraude, roubo de propriedade intelectual e espionagem são exemplos claros de ameaças de conluio.
- **Ameaça de terceiros:** são tipicamente cometidas por funcionários subcontratados, entidades parceiras e outros membros que não pertencem aos quadros de uma organização, mas que possuem permissões de acesso às instalações, sistemas, redes ou pessoas para poderem executar as suas funções.

As ameaças internas, destacaram-se nos últimos anos, exemplos disso são os casos do Facebook, Tesla ou Google. Em 2018, o Facebook despediu um engenheiro de segurança acusado de explorar informação privilegiada para perseguir mulheres. Também em 2018, um funcionário da Tesla terá sabotado os sistemas da empresa e enviado informações confidenciais a entidades terceiras. Em 2020, um antigo executivo da Google foi condenado a 18 meses de prisão por ter roubado segredos

corporativos relacionados com veículos autónomos e partilhado com o seu mais recente empregador, a Uber (Micro Focus, 2023). Os ataques internos são, de facto, uma clara preocupação para as organizações, originando perdas significativas, que podem levar ao comprometimento de informações confidenciais e propriedade intelectual (Khaliq et al., 2020). Desta forma, a aplicação do modelo de segurança *zero trust*, ou confiança zero em português, teria sido fundamental para mitigar alguns destes casos. Este modelo assume que os atores maliciosos já se encontram dentro do sistema, e que nada nem ninguém é confiável. Com a aplicação do *zero trust* a vigilância teria sido superior, os funcionários teriam sempre que validar quem são, validar os dispositivos, o acesso e os privilégios seriam limitados, sendo que, deste modo, as organizações reduziriam a exposição a ameaças de segurança internas e externas (Kemp, 2018).

A ENISA, Agência da União Europeia para a Cibersegurança, fundada em 2004, é a agência que tem como objetivo ajudar a garantir um elevado nível de cibersegurança na União Europeia, apresenta as ameaças emergentes para 2030, onde várias delas já são bastante relevantes nos dias de hoje. As ameaças a ter em consideração estão relacionadas com (ENISA, 2023):

- Compromisso das dependências de *software* na cadeia de fornecimento.
- Campanhas elevadas de desinformação.
- Aumento do autoritarismo da vigilância digital / perda de privacidade.
- Erro humano e exploração de sistemas antigos nos ecossistemas ciberfísicos.
- Ataques direcionados reforçados por dados de dispositivos inteligentes.
- Falta de análise e controlo das infraestruturas e objetos espaciais.
- Aumento das ameaças híbridas avançadas.
- Escassez de competências.
- Prestadores de serviços transfronteiriços de TIC como ponto único de falha.
- Abuso da Inteligência Artificial (IA).

É impossível uma organização conseguir vigiar constantemente as atividades dos seus funcionários, sendo, por isso, difícil erradicar as ameaças internas dos seus sistemas. Deste modo, as organizações devem adotar uma postura proativa e monitorizar o comportamento dos seus funcionários e prestadores de serviços, para minimizar o impacto destas ameaças. A adoção de práticas de segurança para reforçar as infraestruturas corporativas e proteger os dados são fundamentais caso

existam atividades não esperadas. A formação e a sensibilização dos colaboradores para a segurança, soluções de análise comportamental para monitorizar ações invulgares dos funcionários, como horários de trabalho fora do normal ou picos de dados irregulares, assim como, monitorização de esquemas de *phishing*, fazem parte de um conjunto de medidas proativas que as organizações podem adotar. O facto dos funcionários apenas terem acesso aos ficheiros que necessitam é algo também importante, o que possibilita um maior controlo sobre o acesso autorizado aos sistemas. Também a implementação da autenticação multifator permite garantir que as informações críticas estão salvaguardadas e que apenas os colaboradores que dela necessitam possam aceder (Poremba, 2022). Assim, a consciencialização dos funcionários assume um papel fulcral para a segurança das organizações. Esta pode ser definida pelo seu nível de consciência sobre os riscos inerentes à área de cibersegurança e pode ser desenvolvido através de programas de formação providenciados pelas organizações aos seus trabalhadores. Como forma de avaliar o nível de consciencialização dos funcionários, é possível utilizar, por exemplo, o guia de boas práticas do NIST (National Institute of Standards and Technology), o NIST SP 800-53 - controlos de segurança e privacidade para sistemas de informação e organizações ou utilizar a *framework* da CIS (Center for Internet Security) referente à consciencialização para a segurança e formação de competências (Battaglioni et al., 2022).

2.5. Gestão de Identidade e Acesso Privilegiado

O crescente uso das novas tecnologias não trouxe apenas benefícios para a sociedade, mas também incentivou criminosos a lançarem fraudes e explorarem indevidamente a tecnologia com o intuito de obter vantagens financeiras (M. A. Ali et al., 2019). O alvo típico num ciberataque são as palavras-passe de acesso aos sistemas. Os cibercriminosos para além de tentarem o acesso a contas de utilizador normais, procuram também obter acesso a contas de utilizador privilegiadas, como é o caso das contas de administrador. Estas contas têm, por norma, permissões para efetuar a manutenção, gestão e reparação dos sistemas de informação e são conhecidas como “Chaves do Reino”. O abuso de contas privilegiadas por parte de atores maliciosos pode causar danos significativos às organizações, uma vez que essas contas possuem privilégios elevados nos sistemas (Sindiren & Ciylan, 2018). A utilização gradual de tecnologias pelas organizações tem conduzido a um aumento considerável no uso de diferentes aplicações, consequentemente, a tarefa de gerir todas as identidades presentes nas organizações tem-se revelado cada vez mais desafiador. Deste modo, é introduzido o conceito de gestão de identidade, este consiste na gestão centralizada de identidades e gestão de identidades de acesso. A gestão de identidade pode lidar com palavras-passe, controlo de

conformidade, gestão do acesso aos dados, pedidos de acesso, entre outros. O objetivo das organizações passa por manter a sua competitividade e, para isso, é necessário transformar os seus programas de gestão de identidades para prevenir e responder a ameaças de cibersegurança. As organizações requerem mais segurança, pelo que a implementação de uma abordagem assente na Gestão de Identidade e Acesso (IAM) e Gestão de Acesso Privilegiado, ou seja, PAM, é fundamental para a proteção dos dados organizacionais sensíveis (Alruwies et al., 2021).

As soluções de IAM permitem gerir o acesso a recursos e engloba a verificação do utilizador e a autorização de acordo com os recursos protegidos e a função do utilizador. IAM pode ser definido como um método que fornece um nível de proteção apropriado para recursos e dados organizacionais através de regras e políticas aplicadas aos utilizadores. Esta área é composta pelas componentes de gestão de identidade e gestão de acesso, a primeira componente trata, por exemplo, da criação e revogação de identidades, e a segunda trata da autenticação, autorização e gestão das políticas. A gestão de identidade e acesso tem no seu domínio serviços de autenticação, serviços de gestão de autorizações, gestão de identidades, identidade federada e a gestão de conformidade (Sharma et al., 2015). A utilização de soluções de Gestão de Identidade e Acesso podem ajudar na gestão de utilizadores privilegiados, contudo, deixam lacunas que, se exploradas por cibercriminosos pode resultar no comprometimento de credenciais privilegiadas. O IAM tem no seu domínio todas as contas de utilizador de uma organização, estas podem ser geridas e monitorizadas por soluções IAM, contudo, as contas privilegiadas não humanas, ou seja, contas de acesso aos principais sistemas e recursos organizacionais, que são facilmente esquecidas e negligenciadas, ficam ao encargo de PAM que garante a consistência e a conformidade. Neste sentido, o IAM deve ser utilizado conjuntamente com soluções PAM para eliminar as lacunas no sistema de gestão e supervisão de autenticação, minimizando o risco do acesso indevido a sistemas sensíveis. PAM possui assim várias características, como por exemplo (R. Wang, 2018) :

- Vastos controlos de permissão para contas privilegiadas.
- Bloqueio de credenciais.
- Automatização do protocolo de rotação de autenticação.
- Controlo de acesso com base em funções e responsabilidades.
- Auditoria e monitorização, inclusive das tarefas realizadas pelos administradores de sistemas.
- Relatórios de sessões e registos.
- Capacidade de parar ou intervir numa sessão autenticada específica.

- Descoberta de contas privilegiadas não utilizadas ou esquecidas, permitindo reduzir a superfície de ataque.

Haber, refere que as organizações ao longo do seu percurso entenderão, de maneira mais transparente, que a integração de PAM com IAM fornece um elevado nível de proteção organizacional contra vetores de ataque baseados em identidades e contas (Haber, 2020).

O acesso privilegiado é uma das áreas mais sensíveis das organizações, as contas privilegiadas, como contas de administrador, super utilizador, *root* ou contas de administrador de domínio possuem acesso ilimitado, com privilégios elevados, que dão o controlo total dos sistemas aos utilizadores que os estão a gerir. O comprometimento deste tipo de contas pode resultar em violações de conformidade dando origem a coimas e incidentes de segurança provocando a perda de confiança na marca e a perdas financeiras (Esposito, 2023). A adoção de soluções PAM auxilia na gestão do acesso privilegiado, permite registar todas as atividades efetuadas, seja em formato de vídeo através da gravação das sessões ou relatório através do registo de teclas, documentando todas as sessões caso seja necessário rever o fluxo de utilização. Em conclusão, com o PAM as organizações, através da gestão de sessões e credenciais, acesso seguro, auditoria sobre qualquer sessão privilegiada, alertas e registos, ficam mais seguras para combater a utilização acidental ou deliberada do acesso privilegiado (Purba & Soetomo, 2019).

3. Gestão de Acesso Privilegiado

As soluções de Gestão de Acesso Privilegiado permitem proteger, controlar e monitorizar o acesso dos utilizadores com contas privilegiadas aos recursos das organizações. Estas soluções permitem reforçar a segurança da informação das organizações, reduzindo as ameaças de acesso não autorizado, sendo capazes de garantir a segurança avançada das credenciais, sistemas e dados, assegurar a ofuscação das credenciais e monitorizar a atividade dos utilizadores (Abukari & Bankas, 2020). O NIST, agência governamental americana com foco em tecnologia, define sistema de gestão de acesso privilegiado como um sistema que auxilia e monitoriza o acesso privilegiado a recursos, com foco nos sistemas de gestão de configurações e gestão de vulnerabilidades (Souppaya et al., 2020). Gestão de acesso privilegiado é a junção de ferramentas e tecnologias que permite alocar níveis de permissão elevados a contas com acesso a recursos críticos, controlos administrativos, informações confidenciais, e capacidade de alterar definições, tornando este tipo de contas alvo de ciberataques. A área de PAM tem no seu domínio, por exemplo, a gestão de palavras-passe partilhadas, gestão de sessões privilegiadas, gestão de acessos privilegiados a

fornecedores, assim como a gestão de acessos a aplicações. A implementação de PAM auxilia as organizações a protegerem-se contra ameaças externas, impedindo que pessoas mal-intencionadas tenham acesso a dados confidenciais através de contas internas. PAM permite também combater as ameaças internas como funcionários que, de forma inadvertida ou maliciosa, tentam obter acesso a informação corporativa (Lewis, 2021). PAM foca-se em proteger contra o acesso não autorizado e uso indevido das contas privilegiadas, garantindo que essas contas utilizem mecanismos de autenticação robustos, impedindo o abuso do seu nível elevado de acesso aos sistemas (Check Point, 2022a). A implementação de PAM deve incluir uma estrutura robusta, isto pode incluir governança, gestão de inventário dos canais de acesso privilegiado, gestão de utilizadores privilegiados, controlo e monitorização (Hoesl et al., 2017). Esta área possibilita minimizar a superfície de ataque e prevenir ou mitigar os danos causados, seja por atores internos ou externos à organização (Cybrary, 2021). De acordo com a publicação do National Cyber Security Centre (NCSC), PAM é uma medida de segurança adicional para auxiliar na administração de sistemas informáticos. Esta dificulta as ações dos cibercriminosos, na tentativa de explorar sistemas informáticos e assim ganhar acesso a sistemas críticos. As ferramentas PAM dispõem de um sistema de monitorização que permite a identificação do uso indevido dos sistemas informáticos, funcionando como uma medida dissuasora contra ameaças internas. Auxilia também os administradores de sistemas a protegerem os recursos informáticos, ajudando-os contra alterações não intencionais introduzindo barreiras complementares (National Cyber Security Centre, 2020).

As políticas de autenticação para acesso a infraestruturas representam um papel fulcral na segurança dos ambientes informáticos (Otta et al., 2023; Shacklett & Rosencrance, 2021). Por isso, é relevante que exista segregação de funções, que consiste em que nenhum utilizador terá mais permissões que o necessário para cumprir a sua função, sendo uma estratégia de mitigação bastante importante neste contexto. A separação de funções, juntamente com o "princípio do menor privilégio" e a utilização de *softwares* PAM podem ajudar a limitar a utilização indevida de privilégios, garantindo que os utilizadores tenham exclusivamente acesso aos dados que necessitam para a realização da sua função, garantindo uma gestão cautelosa dos privilégios. Existe a necessidade de efetuar uma supervisão e registo do acesso e controlo dos utilizadores às infraestruturas corporativas, pelo que se justifica a utilização de sistemas PAM. Estes sistemas focam-se em pessoas, processos e tecnologias, ajudando a lidar com as falhas inerentes a estes 3 fatores. As pessoas são um ativo fundamental para as organizações, pelo que podem perder dados inadvertidamente, por exemplo através de ciberataques ou, eventualmente, de forma intencional, ao partilhar dados corporativos com outras entidades pelos mais diversos motivos. Relativamente aos ciberataques e às suas consequências, estes podem levar ao roubo de contas, registos de *logs*

comprometidos, violação e perda de dados, uso indevido de privilégios, elevação de privilégios, entre outros. Por sua vez, os processos são um aspeto central de PAM, pois é através de processos que são estabelecidas as regras de como e quando os privilégios podem ser escalados (Tep et al., 2015).

É pertinente frisar a importância das pessoas ou utilizadores, que irão utilizar os sistemas, sejam eles utilizadores finais, administradores ou outras partes interessadas. É necessária ponderação no momento de alocar privilégios, pois quanto maior for o nível de privilégios, maior poderá ser o impacto de uma violação de segurança. A atribuição de acessos privilegiados a pessoas externas à organização, como por exemplo, a entidades parceiras ou fornecedores, representam um elevado risco para uma organização (Walker, 2019).

Em suma, a gestão de acesso privilegiado permite controlar o acesso a informações sensíveis como propriedade intelectual, informações financeiras e comerciais, dados pessoais, entre outros, sendo fundamental para evitar riscos e mitigar as consequências de um possível ciberataque. PAM é visto pelas organizações como uma estratégia de cibersegurança capaz de reduzir as superfícies de ataque, diminuir os riscos no ciberespaço, enquanto que, permitem a redução de custos operacionais e complexidade, auxiliando a garantir a conformidade, tendo em consideração regulamentações importantes tais como o Regulamento Geral sobre a Proteção de Dados (RGPD) (Senhasegura, 2022).

3.1. Acesso privilegiado

Acesso privilegiado é um nível de acesso informático elevado atribuído a utilizadores específicos, que necessitam deste tipo de acessos para executar tarefas administrativas, aceder a sistemas ou informações (Cannard, 2021). O acesso privilegiado deve ser considerado como uma das prioridades de segurança por parte das organizações devido ao eventual impacto significativo e à elevada probabilidade dos cibercriminosos comprometerem este tipo de acesso. Os atacantes procuram explorar estes acessos, pelo facto de incluir administradores de tecnologias de informação e outros utilizadores que possuem acessos a ativos críticos das organizações. Os cibercriminosos aproveitam-se das vulnerabilidades de acesso privilegiado para disseminarem *ransomware* e roubarem dados corporativos, causando um impacto rápido e negativo no negócio (Microsoft, 2023). Neste sentido, os atores maliciosos internos são uma clara preocupação para as organizações, estes são vistos como uma ameaça de segurança crítica, pois, como funcionários, possuem acessos aos recursos organizacionais, como por exemplo, à rede corporativa, conseguindo facilmente contornar os mecanismos de deteção existentes, sem desencadear alertas (Liu et al., 2019).

O controlo de acessos assume um papel fundamental na proteção das organizações, requer uma análise criteriosa no momento de alocar acessos aos colaboradores, tendo como base as suas tarefas diárias, ou seja, que informações e aplicações podem necessitar para o desempenho das suas funções. Neste contexto, privilégio remete para um tipo de acesso que possui permissões especiais, nomeadamente, contas de administradores, *root* ou super utilizadores, ou seja, privilégios com nível de acesso mais elevado que utilizadores finais, conseguindo, entre várias funções, conceder e revogar acessos, alterar níveis de acesso e repor credenciais. Deste modo, é necessária prudência no momento de atribuição de acessos privilegiados. Este processo deve passar pela identificação de funções e regras de acesso, devido ao risco de comprometimento deste tipo de acesso, pois poderá ter implicância no negócio das organizações e, por conseguinte, acarretar perdas monetárias, afetar a reputação ou diminuir a própria capacidade competitiva. O comprometimento do acesso privilegiado está maioritariamente ligado a ciberataques, que têm como alvo os funcionários de uma dada organização. Estas ações podem ser consideradas intencionais com o objetivo de obter ganhos pessoais ou outras motivações, e ações não intencionais devido a campanhas de *phishing* ou *malware* (Ramaseshan, 2018).

3.2. Contas privilegiadas

As contas privilegiadas permitem a gestão da infraestrutura tecnológica das organizações, assumindo uma função estratégica que, entre vários exemplos, possibilita efetuar alterações nas configurações dos sistemas e *softwares*, executar tarefas administrativas, gerir contas de utilizadores, realização de *backups* e atualizações de segurança, assim como aceder a informações privilegiadas. As pessoas representam, assim, uma possível ameaça para as organizações, tendo em consideração que os colaboradores de uma empresa podem ser vistos como uma ameaça interna emergente, podendo abusar dos privilégios que possuem. Também ameaças externas como cibercriminosos procuram explorar este tipo de contas para ações danosas. A integração de contas privilegiadas em PAM permite, de facto, limitar o acesso dos utilizadores, garantindo que apenas tenham acesso aquilo que efetivamente necessitam (Senhasegura, 2022).

As contas privilegiadas são consideradas alvos de grande valor pelos cibercriminosos, pelo que restringir o acesso apenas aos utilizadores que delas necessitam é fundamental para proteger a infraestrutura corporativa. Por isso, quanto menos contas privilegiadas existirem, menos oportunidades os atores maliciosos têm à disposição para poderem explorar (Australian Cyber Security Centre, 2022).

A CyberArk, empresa de segurança da informação, com foco na gestão de identidade, conta com clientes bastante influentes, cuja cota de mercado é de cerca de 50% no domínio da lista Fortune 500 (lista anual das 500 maiores empresas dos Estados Unidos da América), dá conta dos ciberataques diários avançados e internos na tentativa de explorar contas privilegiadas. Estas contas são consideradas como as "chaves do reino", pois possuem acessos elevados aos sistemas organizacionais de uma rede corporativa. A CyberArk realça assim as recomendações de organizações como o NIST que defendem a importância de proteger, gerir e monitorizar as contas privilegiadas (CyberArk, 2019).

Comparativamente com as contas privilegiadas, as contas padrão representam uma identidade, como por exemplo, as contas de Active Directory, e permitem que os utilizadores tenham acesso a informação organizacional não confidencial. Quanto às contas privilegiadas, estas têm como base níveis de permissões elevados e permitem o acesso a sistemas organizacionais e dados confidenciais, acesso a servidores, base de dados, aplicações, a possibilidade de extrair dados, entre outros (Carson, 2022a). As contas privilegiadas incluem contas de utilizadores humanos e não humanos. As contas de utilizadores humanos são contas de acesso privilegiado com o objetivo de efetuar determinadas funções dentro da organização, como por exemplo, administradores. Exemplos deste tipo de contas são contas administrativas ou *break glass*. As contas não humanas, são contas utilizadas por sistemas, aplicações ou serviços que interagem com outros sistemas e realizam atividades privilegiadas (CyberArk, 2020c).

As contas privilegiadas são, tradicionalmente, utilizadas por pessoas da área das tecnologias da informação, pelo que permitem executar comandos e efetuar alterações em sistemas - no caso do Linux temos o utilizador "*root*" e no Windows o "administrador". Deste modo, são apresentados os seguintes exemplos de contas privilegiadas habitualmente presentes dentro das organizações (BeyondTrust, 2022; Burnis, 2017; Carson, 2021):

- **Contas administrativas locais:** fornecem acesso administrativo a serviços locais.
- **Contas administrativas de domínio:** fornecem acesso administrativo privilegiado a todas as estações de trabalho e servidores no domínio.
- **Contas *break glass*:** contas *break glass* ou também designadas por contas de emergência, são contas com acesso administrativo a sistemas seguros em caso de emergência.
- **Contas de serviço:** contas privilegiadas locais ou de domínio utilizadas por aplicações ou serviços para interagir com o sistema operativo.
- **Contas de serviço de domínio ou active directory:** contas para permitir alterações nas propriedades dos utilizadores, como palavras-passe, entre outros.

- **Contas de aplicações:** contas utilizadas por aplicações para aceder a bases de dados, executar tarefas, *scripts* e aceder a outros sistemas.

Quanto às contas *break glass*, de realçar a importância das mesmas no contexto de PAM, estas contas de emergência são utilizadas para fazer face a incidentes, quando os métodos habituais de acesso falham. Estas contas possuem altos privilégios e são utilizadas para restaurar as operações devido a eventos graves ou interrupções do sistema. As contas *break glass* são utilizadas para aceder, em última instância, a sistemas privilegiados dando, por exemplo, acesso a contas privilegiadas Unix e Linux, a utilizadores de base de dados SYS e SA ou acesso a sistemas Windows através da conta administrador (Haber, 2020).

A definição de contas privilegiadas varia de organização para organização e do tipo de indústria, sendo por isso necessário definir inicialmente as funções de cada utilizador e descrever os privilégios necessários para executar essas mesmas funções. É também importante delinear, em caso de ciberataque, quais os sistemas que devem ser logo recuperados após um incidente, tais como os sistemas de dados confidenciais, permissões de alto nível e a capacidade de configurar e aceder a outros sistemas. Outro fator importante são os acessos disponibilizados a fornecedores e entidades parceiras, esse tipo de acessos deve ser limitado às pessoas que necessitem de tal acesso e deve ser revogado quando concluírem a sua função. Adotando esta postura conscienciosa, é possível minimizar a questão das contas privilegiadas esquecidas ou não geridas dentro dos sistemas PAM. No entanto, algumas das razões para que as contas privilegiadas não sejam devidamente geridas prendem-se com (McCarthy, 2023):

- Demasiado nível de acesso concedido para contornar as restrições de acesso aos sistemas. Por vezes, existem fluxos de trabalho que podem atrasar a realização de algumas tarefas no imediato, por isso os administradores de sistemas concedem permissões elevadas para melhorar a produtividade dos utilizadores, contudo, essas permissões atribuídas podem acabar por se tornar esquecidas ou não monitorizadas, transformando-se numa porta de entrada para os riscos.
- Funcionários quando trocam de cargo dentro da empresa mantêm, por norma, os acessos a sistemas que não necessitam. Por isso, é fundamental uma gestão eficaz dos sistemas, para revogar credenciais sempre que necessário, pois, essas permissões quando exploradas por atores maliciosos sobretudo internos com vasto conhecimento da estrutura corporativa, podem causar imensos danos às organizações.

- Quando funcionários deixam a empresa nem sempre o acesso privilegiado é revogado, dessa forma as contas destes utilizadores acabam por ficar esquecidas.
- Contas de serviço para aceder a aplicações, sistemas e dispositivos vêm tipicamente com credenciais padrão incorporadas, pelo que se torna fácil de explorar, tornando-se assim alvos prioritários para atores maliciosos.
- Credenciais estáticas, onde a rotação e a atualização das mesmas de forma manual podem ser um trabalho árduo e propenso a erros, tais como a falta de robustez das novas palavras-passe, credenciais que não chegaram a ser alteradas ou não possuem data de expiração.
- A partilha de palavras-passe por parte de administradores que gerem contas de serviço ou equipas de TI que partilham palavras-passe para acesso aos sistemas torna difícil o processo de gerir e auditar as contas privilegiadas.
- Em suma, é, de facto, fundamental haver uma supervisão eficiente durante o processo de criação e alocação de privilégios para reduzir a porta de entrada a ciberataques.

3.3. Acesso remoto

As organizações utilizam, tipicamente, os protocolos RDP (Remote Desktop Protocol) e SSH (Secure Shell) como meios de acesso remoto a sistemas e recursos que inclui aplicações críticas e dados sensíveis. O protocolo RDP é assim um protocolo de comunicação desenvolvido pela Microsoft que permite a gestão de ambientes de trabalho virtuais e remotos. Este tipo de protocolo, possui uma interface gráfica e permite que funcionários de uma dada organização possam aceder aos sistemas da empresa a partir de qualquer local. O protocolo RDP é a opção mais utilizada para efetuar a conexão a sistemas Windows, pelo que, por outro lado, temos o protocolo SSH normalmente associado a sistemas Unix e Linux. Relativamente à usabilidade, o protocolo RDP é mais simples de utilizar devido à sua interface gráfica, ao contrário do SSH que utiliza uma interface de linha de comandos. Quanto ao método de autenticação o protocolo RDP utiliza credenciais padrão, ao passo que o SSH utiliza, habitualmente, chaves públicas e privadas (Carson, 2022b). No entanto, estes protocolos de comunicação de rede não são infalíveis e podem ser alvos de ciberataques como ataque de força bruta para tentar obter as credenciais do utilizador. Neste sentido, uma das formas de proteger os protocolos de comunicação e as sessões efetuadas é através de soluções PAM. As soluções de gestão de acesso privilegiado permitem armazenar as credenciais de contas privilegiadas num cofre encriptado. Podem ser ainda aplicadas políticas de segurança para limitar o acesso aos utilizadores e, desta forma, o acesso não autorizado aos sistemas

organizacionais fica reduzido, bem como a capacidade de efetuar alterações ou exfiltração de dados (Carson, 2022b). O acesso remoto pode assim ser integrado com soluções de gestão de acesso privilegiado, permitindo o armazenamento de credenciais e possibilitando que essas mesmas credenciais sejam inseridas no sistema, criando as sessões privilegiadas a servidores remotos. Deste modo, com recurso a PAM é possível realizar a auditoria de sessões, este é um desafio presente nas organizações devido à utilização de *proxies* que encaminham o tráfego de sessões remotas possibilitando a gravação das sessões. O acesso remoto e a monitorização de privilégios são um desafio constante para as organizações, contudo, a integração com soluções PAM possibilita simplificar este processo (Haber, 2020). Em síntese, a utilização de PAM permite assim controlar, monitorizar e registar sessões de acesso privilegiado, nomeadamente sessões RDP e SSH, e pode incluir auditoria e relatórios (McCarthy, 2023).

3.4. Desafios da gestão de acessos

A área de gestão de acessos tem vários desafios tais como i) falta de visibilidade e consciencialização, ii) falta de supervisão de credenciais privilegiadas e auditabilidade, iii) partilha de contas privilegiadas, iv) credenciais *hard-coded*, credenciais padrão, chaves SSH, v) sistemas *cloud*, vi) acessos privilegiados para fornecedores e outras entidades, entre outros (Haber, 2020):

I. As organizações possuem, por vezes, inúmeras contas privilegiadas pelo que nem sempre fazem a melhor gestão, ficando algumas inclusivamente esquecidas. Por isso, torna-se fundamental a utilização dos sistemas PAM para efetuar toda esta gestão.

II. É perentório que atividades realizadas através das contas privilegiadas sejam monitorizadas para garantir a conformidade e a segurança das sessões caso sejam utilizadas indevidamente. Este processo é totalmente automatizado através das soluções PAM, o que em caso de uma atividade maliciosa estar a decorrer em tempo real, estas soluções permitem tomar as devidas providências para mitigar ações não autorizadas ou maliciosas.

III. A partilha de contas privilegiadas por parte de administradores de sistemas, como contas *root* ou administrador, dificulta o processo de rastrear as ações realizadas, o que complica o processo de auditoria e responsabilização.

IV. Muitos dos dispositivos, por exemplo, IoT trazem credenciais padrão totalmente visíveis em guias ou ficheiros, pelo que é importante alterar estas credenciais e utilizar uma solução PAM para poder gerir os dispositivos com segurança. Este tipo de soluções permite também gerir chaves SSH com maior segurança.

V. Relativamente aos ambientes *cloud* e virtualizados as soluções PAM permitem gerir as credenciais de acesso a estes sistemas, bem como fornecer a capacidade de auditabilidade e monitorização das sessões e assim verificar a sua conformidade.

VI. A gestão de acesso privilegiado por parte de fornecedores e outros parceiros é outro dos desafios presentes nesta área. Por isso, a utilização do PAM permite simplificar este processo, dando o acesso aos sistemas a fornecedores e outras entidades, sendo capaz de monitorizar as suas atividades durante as sessões remotas, efetuar a gestão das credenciais segundo as políticas organizacionais pré-estabelecidas, entre outras vantagens, facilitando toda a sua gestão.

3.5. Cadeia de ataque

Os ciberataques têm como alvo principal as contas privilegiadas e o resultado destes tende a originar um grande número violações de dados (Simister, 2022). Desta forma, cibercriminosos, entidades parceiras e funcionários desonestos são os tipos de vetores de ameaças mais comuns (BeyondTrust, 2022). Sistemas, como por exemplo, Sistemas de Infraestrutura Crítica que abrangem áreas como a área fabril, transportes, abastecimento de água, energia, entre outros, são exemplos de sistemas que podem ser expostos a ameaças no ciberespaço. A ICS-CERT (The Industrial Control Systems Cyber Emergency Response Team), incentiva as organizações a adotarem práticas de segurança robustas e inclusive a efetuarem uma gestão de privilégios de forma cautelosa, com o auxílio das tecnologias PAM (Haber & Hibbert, 2018).

Os ciberataques podem, por exemplo, recorrer a engenharia social, *phishing*, exploração de credenciais, exploração de vulnerabilidades, palavras-passe padrão ou *spyware* (Simister, 2022):

I. Engenharia social e *Phishing*: Estas técnicas utilizadas por cibercriminosos, são métodos bastante comuns para a obtenção ilegítima de credenciais. Tipicamente os autores maliciosos disfarçam-se, apresentando-se como uma entidade credível, capaz de induzir as vítimas a partilharem as suas credenciais.

II. Exploração de credenciais: A exploração de credenciais pode incluir ataques de força bruta, tentativa de adivinhar as palavras-passe, ataques de dicionário, ataques de *rainbow tables*, entre outros. Os cibercriminosos podem também tentar adivinhar as perguntas de segurança para obter acesso às contas privilegiadas, bem como tentar comprometer os mecanismos de redefinição de palavras-passe.

III. Vulnerabilidades: Outro fator explorado pelos atacantes são as vulnerabilidades presentes em sistemas operativos, protocolos de comunicação, navegadores *web*, aplicações, sistemas *cloud*, infraestruturas de rede, entre outros.

IV. Palavras-passe padrão: As palavras-passe padrão são também alvo de exploração, pois nem sempre as organizações alteram as credenciais que vêm de fábrica.

V. *Spyware*: O *spyware* é outro tipo de técnica utilizada para comprometer contas privilegiadas. Com isso, através de, por exemplo, *keyloggers*, tudo o que é digitado pela vítima é monitorizado e enviado para os atacantes.

A implementação de PAM vem assim ajudar na mitigação de ciberataques, auxiliando as organizações na segurança dos seus ativos e, desta forma, prevenir o acesso a identidades, roubo de dados e afetar a disponibilidade dos sistemas. Tipicamente, os cibercriminosos seguem várias etapas para o desenvolvimento de ciberataques, estas dão origem à designada cadeia de ataque, que é assim composta pelas seguintes fases (CyberArk, 2021):

I. **Atores maliciosos:** Os atores podem ser internos ou externos à organização, sendo que os externos utilizam uma variedade de técnicas para conseguirem aceder aos sistemas, enquanto, os atores internos utilizam o seu conhecimento sobre a infraestrutura organizacional e os seus acessos para desenvolverem os ataques.

II. **Roubo de credenciais:** Os cibercriminosos utilizam técnicas como engenharia social, registo de atividades do teclado para poderem ver o que foi digitado e *scripts* para detetarem credenciais, chaves SSH, *hashes*, entre outros, em repositórios.

III. **Movimento lateral e vertical:** Os cibercriminosos depois de terem o acesso à infraestrutura do seu alvo, podem movimentar-se lateralmente de estação de trabalho para estação de trabalho, ou então moverem-se verticalmente e acederem a outros tipos de sistemas, como sistemas *cloud*.

IV. **Abuso e elevação de privilégios:** Depois de aceder aos sistemas do alvo, os atores maliciosos avançam para a elevação de privilégios de forma a obterem acessos, por exemplo, de administrador para conseguirem a informação desejada e realizaram outras ações maliciosas.

V. **Ações e objetivos:** Como última fase da cadeia de ataque, os atores maliciosos têm como objetivos o roubo de informação, distribuição de *ransomware*, interrupção dos serviços, danos ao nível da reputação, entre outros.

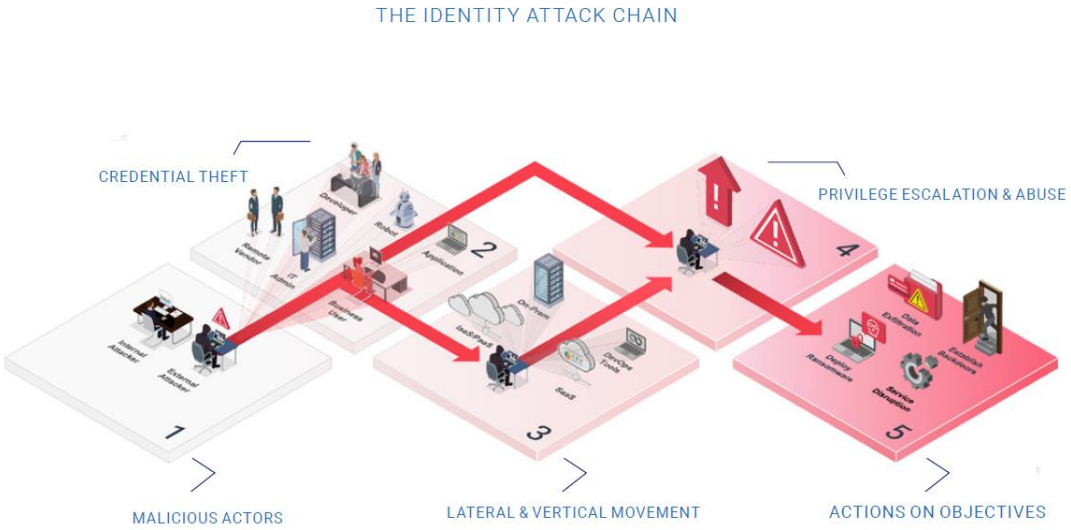


Figura 1 - Cadeia de ataque, adaptado de CyberArk, 2021

Neste sentido, a CyberArk reforça a necessidade de criação de programas de cibersegurança eficazes com o objetivo de reduzir o risco e defender as organizações contra ataques informáticos, muitas vezes centrados em comprometer as identidades. Consequentemente, a CyberArk desenvolveu o CyberArk Blueprint, um guia orientador no domínio da segurança de identidade para ajudar as organizações a avaliar e priorizar as vulnerabilidades de acesso privilegiado que está assente em três princípios orientadores. Estes estão relacionados com a cadeia de ataque utilizada por atores maliciosos, nomeadamente, a prevenção do roubo de credenciais, a interrupção do movimento lateral e vertical e a limitação do aumento e abuso de privilégios. O CyberArk Blueprint permite às organizações compreender a cadeia de ataque às identidades, avaliar a sua postura de segurança, aprender as melhores práticas de segurança de identidades e auxiliar na criação de planos, com recurso a controlos de segurança específicos para mitigar os riscos de ataques às identidades (CyberArk, 2020a). A CyberArk através da CyberArk Blueprint para a segurança de identidades, refere um conjunto de controlos específicos para fazer face aos três princípios orientadores mencionados acima, de forma a reduzir os riscos de ataques e mitigar os mesmos. Deste modo, é de seguida apresentado apenas alguns dos controlos sugeridos pela CyberArk, que permitem reduzir os ricos perante ciberataques (CyberArk, 2022b).

Prevenir o roubo de credenciais

- Cofre de palavras-passe e segredos: Guardar palavras-passe e segredos num cofre, de forma a permitir a encriptação, não repúdio e controlo de acesso sobre os mesmos. Este é um controlo de segurança basilar que possibilita outros controlos como a rotação e isolamento.
- Rotação de palavras-passe e segredos: Este é o processo de alterar as palavras-passe com base nas políticas de segurança definidas pelas organizações, este processo pode ser automático ou manual. Isto possibilita a rotação de segredos ou palavras-passe complexas e a diminuição do tempo de vida das mesmas, o que reforça a segurança dos sistemas.

Interrupção do movimento lateral e vertical

- Controlo de acesso baseado em funções (RBAC): O *Role-based access control* é um mecanismo de controlo de acessos estabelece funções e privilégios, está assente num modelo de privilégio mínimo e determina se as identidades devem ter acesso a um recurso específico. Esta técnica evita movimentos laterais e verticais, restringindo o âmbito de acesso somente aos recursos e permissões necessários para desempenhar essa função.
- Isolamento da sessão: O isolamento de sessão, por exemplo RDP, *Web* ou SSH, permite o isolamento do utilizador final com a estação de trabalho, garantindo também que o utilizador apenas acede ao recurso que necessita, restringindo movimentos laterais e verticais caso existam ações maliciosas.
- Análise de sessão: A análise de sessão possibilita que os registos de auditoria e a atividade de sessão sejam automaticamente analisados com o objetivo de determinar se as ações realizadas pelo utilizador são ações não autorizadas ou maliciosas e emite alertas sempre que detetadas. Estas ações podem incluir fugas de informação, criação não autorizada de novos utilizadores ou tentativas de movimentos laterais ou verticais.

Limitação do aumento e abuso de privilégios

- Privilégio mínimo: A aplicação do princípio do menor privilégio permite reduzir proactivamente o nível de privilégios de uma identidade ao nível mínimo necessário para o desempenho da sua função.

- Controlo de aplicações: Este mecanismo, através das políticas de segurança definidas, possibilita a permissão ou restrição do acesso a aplicações, quais os utilizadores que têm tais permissões, se essas permissões são elevadas, se a aplicação pode ser iniciada a qualquer momento ou se tem um espaço temporal pré-definido, entre outros. Este tipo de controlo visa impedir a execução de *software* malicioso.
- Registo de auditoria: Registo de auditoria ou *logs*, é o meio através do qual são criados os registos para efeitos de auditoria para atividades de utilizadores humanos e não humanos. Estes *logs* registam assim tudo o que foi realizado durante as sessões privilegiadas, pode ser criado um rasto em tempo real que não pode ser repudiado e auxilia na redução do risco de escalação de privilégios e abuso de privilégios.

3.6. Fluxo de funcionamento

Geralmente, as soluções PAM possuem funcionalidades como a existência de um cofre digital de palavras-passe, sendo este considerado um local seguro para armazenar credenciais. Possuí rotação automática de palavras-passe, processo de aprovação para permitir e revogar permissões e também a possibilidade de habilitar a autenticação multifator para as contas privilegiadas. Para além disso, deve incluir a gestão automatizada de contas, isto permite automatizar o processo de criação, modificação e eliminação de contas. Deve ainda incluir a monitorização das contas em tempo real, ou seja, as atividades realizadas em contas privilegiadas devem ser ativamente monitorizadas, classificadas e consultadas sempre que necessário. Por fim, deve incluir a capacidade de gerar relatórios e alertas em tempo real para análise interna ou para ser enviado às autoridades competentes quando aplicável (Simister, 2022).

As ferramentas PAM reúnem assim as credenciais de contas privilegiadas num repositório seguro para isolar a sua utilização e registar as respetivas atividades, isto permite reduzir o risco de roubo ou uso indevido deste tipo de credenciais de acesso. Dependendo das configurações estabelecidas pelos administradores destas soluções, o sistema PAM pode restringir que os utilizadores privilegiados escolham as suas próprias palavras-passe, isto é devido ao gestor de credenciais existente que pode fornecer palavras-passe para serem utilizadas apenas num determinado dia ou então sempre que uma nova sessão é iniciada é também gerada uma nova palavra-passe (Lewis, 2021). Inicialmente, os administradores de uma solução PAM definem os métodos de acesso às contas privilegiadas para os vários recursos, assim como podem definir políticas e condições para a sua utilização. Depois de configurado, o sistema PAM já pode ser utilizado pelos utilizadores. Com isso, um utilizador pode requisitar o acesso a um recurso, tendo para isso que apresentar uma

justificação para que o acesso seja validado e registado. Este pedido e aprovação surgem devido ao facto de um utilizador não administrador, não ter acesso às credenciais de acesso a estes recursos críticos. Por isso, o utilizador deve solicitar o acesso, sem ter qualquer visibilidade da palavra-passe da conta privilegiada. Posteriormente, depois do utilizador fechar a sessão privilegiada, a palavra-passe pode ser automaticamente alterada consoante a política definida pelos administradores PAM. Por fim, os administradores podem monitorizar as atividades e gerir as sessões dos utilizadores em tempo real se necessário, pelo que estas soluções contam ainda com algoritmos de *machine learning* para identificar ameaças e utilização indevida dos recursos (Cybrary, 2021).

O fluxo apresentado na figura 2 representa a estrutura de funcionamento de uma solução PAM. É possível verificar que um utilizador para entrar num servidor ou outro tipo de dispositivo, deve efetuar um pedido de acesso e só depois de aprovado é que consegue executar a sua função. Este fluxo demonstra ainda que as sessões são geridas através de uma sessão *proxy* para providenciar maior segurança, sendo essas sessões monitorizadas e gravadas. Estas podem ser, posteriormente, reproduzidas pelos administradores das soluções PAM, são ainda gerados os *logs* ou registo de atividades para eventual auditoria e criado um arquivo com mesmos esses *logs*.

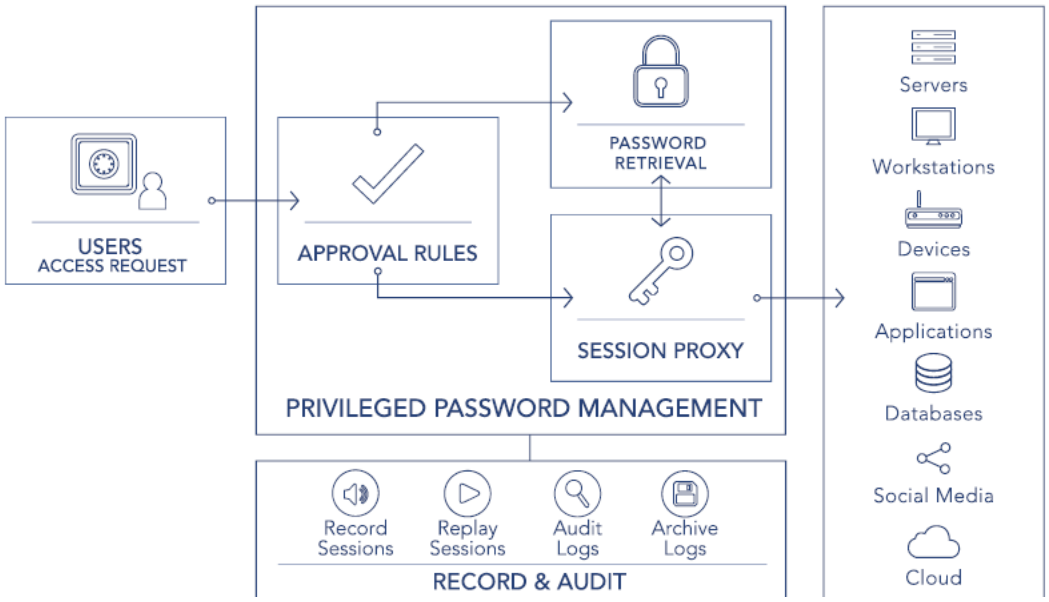


Figura 2 - Gestão de acesso privilegiado - fluxo de utilização e recursos protegidos, Haber, 2020

Em suma, as soluções PAM permitem saber quem acedeu a um dado sistema, que sistema foi acedido, quando foi acedido e qual a justificação do acesso. Desta forma, há transparência sobre quais as sessões que foram iniciadas, o que foi realizado e quem tem acesso, ou seja, as soluções

PAM possibilitam controlar o que está relacionado com esses sistemas ou informações, podendo limitar o acesso se necessário e garantir o seu armazenamento de forma segura.

3.7. Benefícios de PAM

Existem aspetos importantes inerentes à área de PAM como a implementação do principio do menor privilégio, controlos de acesso baseado em funções, automação e monitorização das atividades das contas privilegiadas, entre outros (Simister, 2022). PAM é baseado no principio do menor privilégio, que constata que utilizadores, aplicações e sistemas devem ter apenas acesso às permissões necessárias para executarem a sua função (Check Point, 2022a).

Deste modo, temos também presente a metodologia acesso *just-in-time* que é uma forma de providenciar acesso privilegiado seguro a utilizadores humanos e não humanos em tempo real para executar uma tarefa específica. Esta metodologia providencia o acesso a contas e recursos privilegiados apenas quando necessário, durante um período de tempo definido, minimizando o acesso permanente. Com o limitar de acesso, a metodologia *just-in-time* visa reduzir o abuso de contas privilegiadas. Desta foram, restringe a janela de tempo que um cibercriminoso ou uma ameaça interna dispõe para obter acesso a contas privilegiadas e mover-se lateralmente através dos sistemas organizacionais, evitando obter acesso não autorizado a dados confidenciais. Por fim, esta metodologia garante também que atividades privilegiadas sigam as políticas definidas no IAM, Gestão de Serviços de Tecnologia da Informação (ITSM) e PAM, permitindo também obter um registo das atividades realizadas (CyberArk, 2020b).

A Cybrary e a One Identity enumeram alguns dos benefícios do PAM (Cybrary, 2021; Weihe, 2022b):

- **Monitorização e registo de atividades em ambientes privilegiados:** as soluções PAM dão uma clara visibilidade dos utilizadores com acessos privilegiados, sendo capaz de efetuar a gestão e monitorização das contas privilegiadas, manter *logs* detalhados das sessões e automatizar as políticas de acesso da organização.
- **Garante a conformidade:** restringe o acesso a sistemas confidenciais, exige várias autenticações ou aprovações e restringe as atividades.
- **Superfície de ataque:** limita os privilégios dos utilizadores, processos e aplicações, protegendo contra ameaças internas e externas, limitando a superfície de ataque e diminuindo as possíveis entradas e ataques por parte dos agentes maliciosos.

- **Proteção contra cibercriminosos:** as tecnologias PAM auxiliam na gestão de *passwords*, gerando-as automaticamente e de forma aleatória, colocando-as num cofre digital. Por isso, o conceito de mínimo privilégio entra em vigor, pois o PAM remove privilégios excessivos e auxilia também na mitigação de *malware* e outras ameaças, garantindo a monitorização em tempo real e ajudando a identificar possíveis ataques.
- **Credenciais seguras num cofre digital:** as soluções PAM possuem um cofre digital capaz de guardar e gerir credenciais, como credenciais com permissões de administrador.
- **Custos:** as soluções PAM permitem adotar boas práticas na gestão de acessos privilegiados, reduzindo a possibilidade de consequências nefastas para as organizações, seja a nível financeiro ou reputacional.
- **Integração com IAM:** a possibilidade de integrar IAM e PAM, permite que todas as contas com e sem acesso privilegiado sejam geridas e possuam autenticação multifator, *login* único (*single sign-on*), entre outros benefícios.

Também Haber & Hibbert, 2018, referem vários benefícios que o PAM pode trazer para, por exemplo, Sistemas de Controlo Industrial (ICS, na sigla original), bem como para qualquer outra área de implementação, nomeadamente:

- Descobrir todos os dipositivos geridos e não geridos nas infraestruturas organizacionais.
- Descobrir e inventariar contas privilegiadas utilizadas de forma automática.
- Armazenamento de palavras-passe e chaves SSH numa base de dados segura e centralizada.
- Rotação de palavras-passe automática para reduzir o risco de perda ou roubo de credenciais. Por exemplo, mudar as palavras-passe segundo um período de tempo pré-estabelecido ou alterar após cada sessão remota efetuada.
- Verificar se existem palavras-passe padrão em qualquer sistema ou dispositivo.
- Definir um fluxo de trabalho de acesso aos dispositivos, por exemplo, tendo em consideração um processo de aprovação para permitir o acesso remoto quando necessário.
- Gravar sessões remotas para documentar e rever as ações efetuadas sobre os dispositivos.
- Relatórios completos das contas utilizadas quando ocorrem atividades remotas.

3.8. Sistemas de conformidade e auditoria

Um ciberataque bem-sucedido pode implicar que um *malware* ou uma ciberameaça atinja um determinado nível de acesso ou permissões, exemplo disso é um ataque de *ransomware* (Maalem Lahcen et al., 2020). Este ataque permite cifrar dados organizacionais importantes e sensíveis, onde os cibercriminosos exigem o pagamento de um resgate para devolver o acesso aos respetivos proprietários (Dargahi et al., 2019). Com isso, a gestão de acesso privilegiado pode impactar positivamente as organizações, pois reforça a segurança no ciberespaço e permite maior controlo e monitorização quando utilizadas contas privilegiadas. Para além disso, a implementação de PAM é essencial para cumprir legislações e regulamentações como o Regulamento Geral sobre a Proteção de Dados (RGPD), Padrão de Segurança de Dados do Setor dos Cartões de Pagamento (PCI DSS), Lei da Portabilidade e Responsabilidade dos Seguros de Saúde (HIPAA), entre outras regulamentações semelhantes com o objetivo de impedir o acesso não autorizado a informações sensíveis (Check Point, 2022a). PAM é visto como uma componente fundamental para assegurar a conformidade com as regulamentações da indústria e também governamentais. Estes sistemas podem ser integrados num programa de segurança e gestão de risco, permitindo simplificar os requisitos de auditoria e conformidade, visto que possuem capacidades como gravar e registar todas as atividades relacionadas com as infraestruturas críticas de TI e dados organizacionais confidenciais (Lewis, 2021). Devido a imposições legais, instituições governamentais como instituições bancárias da União Europeia estão obrigadas a revalidar contas privilegiadas a cada 6 meses, o que torna pertinente o uso de gestão de acesso privilegiado (Hoesl et al., 2017). Neste sentido, os bancos devem agir de acordo com o princípio de menor privilégio, ou seja, os utilizadores devem possuir apenas as permissões necessárias para o cumprimento eficaz das suas funções. Com a adição de PAM, o raio de ação de um ator malicioso torna-se limitado pelo que, mesmo em caso de ciberataque, os comandos que estes atores podem executar são também eles limitados. Desta forma, em caso de haver ações maliciosas o processo de investigar e mitigar ataques internos é mais célere, devido ao controlo de acesso, gravação de sessões e auditoria (Morris, 2018).

A WALLIX, organização que atua na área da gestão de identidades, reforça a utilidade dos sistemas de controlo em tempo real fornecidas pelas soluções de gestão de acesso privilegiado. Estes sistemas de controlo permitem definir ações proibidas sob os utilizadores privilegiados, pelo que, em caso destes utilizadores tentarem executar tais ações, as contas são automaticamente bloqueadas e as equipas de segurança alertadas (WALLIX, 2016). Isto permite também garantir a conformidade com importantes padrões de cibersegurança como NIST ou ISO 27001 (Senhasegura, 2022).

3.9. Boas práticas

Existem várias organizações que atuam na área de gestão de acesso privilegiado, pelo que a consultora Gartner destaca os líderes, os desafiadores, os concorrentes e os visionários nesta área. Empresas como CyberArk, BeyondTrust e Delinea, são algumas das empresas que surgem nesta lista e que seguem como líderes no segmento de PAM (Gartner, 2022).

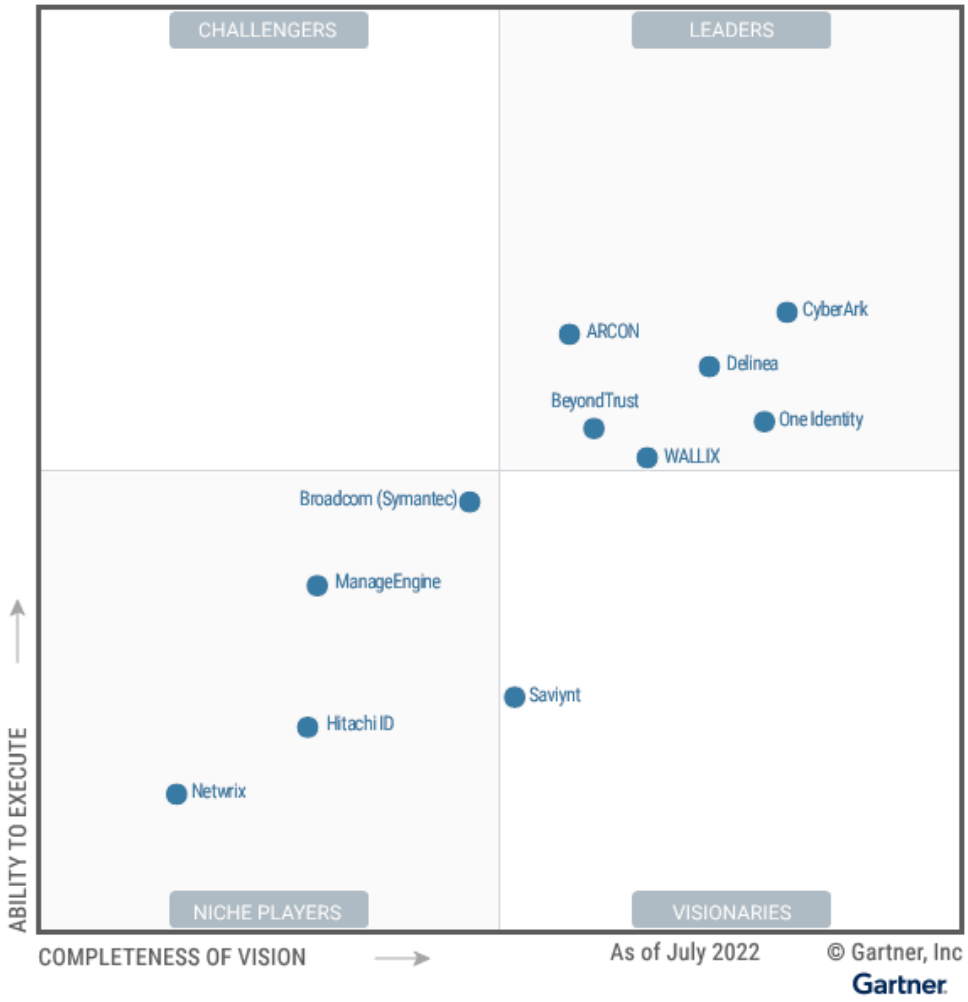


Figura 3 - Quadrante mágico Gartner 2022: Gestão de acesso privilegiado

A One Identity enumera um conjunto de boas práticas na hora de implementar uma solução PAM, pelo que passo a citar algumas (Weihe, 2022a):

i. Manter as contas privilegiadas atualizadas, ou seja, todas as contas privilegiadas de uma organização devem ser listadas e somente utilizadas através de soluções PAM. Contabilizar e monitorizar as contas privilegiadas, pelo que contas privilegiadas de origem desconhecida ou com credenciais fracas, devem ser investigadas.

ii. Deve ser realizada a monitorização das contas privilegiadas, contudo, essa monitorização não tem que ser necessariamente manual, pois cada sessão é gravada e é possível rever todas as atividades, seja em modo vídeo ou através do registo de atividades. Podem ser estabelecidas regras de monitorização que avalia o que é realizado pelo utilizador e emite alertas consoante a política de segurança adotada pelas organizações face a atividades suspeitas.

iii. Utilizar o princípio de menor privilégio, também designado por "*principle of least privilege*", isto significa que o utilizador apenas tem acesso aos recursos que necessita para o desenvolvimento das suas tarefas. As tecnologias PAM permitem conceder acesso aos recursos por um período de tempo pré-estabelecido e posteriormente remover o acesso assim que concluídas as tarefas.

iv. Deve ser incutido o sentido de responsabilidade e estabelecer regras para evitar a partilha de contas privilegiadas por parte dos utilizadores, pois cada membro deve estar ciente do risco deste tipo de partilha. A formação dos utilizadores é um fator importante quando utilizadas as soluções PAM para aceder a recursos críticos das organizações. É importante que estes utilizadores tenham o conhecimento dos processos e benefícios que estas soluções providenciam para evitar eventuais erros e minimizar possíveis ameaças.

v. Elaborar documentação de boas práticas relativa à gestão de acesso é outro dos procedimentos fundamentais para uma boa utilização das soluções PAM e dos recursos críticos organizacionais. Isto facilita também o processo de auditoria, pois será possível visualizar as políticas e diretrizes estabelecidas pelas organizações.

vi. Por fim, deve ser tido em consideração a melhoria contínua da utilização dos serviços PAM e dos processos adotados. Isto permitirá perceber se o PAM está a ter o sucesso desejado, se os processos estão otimizados, se ajustáveis às necessidades dos utilizadores e otimizados ao nível da eficiência e facilidade de utilização.

O NCSC providencia diretrizes para a implementação de soluções PAM por parte das organizações, de forma a reduzir a superfície de ataque quer dos dispositivos, como também do serviço PAM (National Cyber Security Centre, 2020):

- Restringir dispositivos: Apenas permitir dispositivos confiáveis pela organização para aceder ao serviço PAM.

- Apenas utilizadores autorizados: Utilizar autenticação robusta e permitir apenas o acesso a administradores autorizados de forma a solicitarem as credenciais para a administração dos sistemas.
- Justificar a intenção de administrar sistemas: Os administradores quando solicitam as credenciais para aceder aos sistemas, devem justificar a sua intenção como parte do processo de solicitação. Desta forma, o processo de aprovação é simplificado, e agirá como forma de dissuadir o acesso aos sistemas por parte de pessoas mal-intencionadas.
- Aprovação aos sistemas PAM: Devem ser consideradas as regras de solicitação e aprovação que regem o acesso às interfaces de administração do sistema PAM. Deve ser tido em consideração o impacto de o sistema ser, eventualmente, comprometido e utilizar essa situação como suporte para a tomada de decisão.
- Utilizar credenciais robustas: As credenciais dos serviços PAM devem ser criptograficamente fortes e protegidas quando utilizadas, para evitar que um cibercriminoso consiga quebrar essa credencial ou, eventualmente, roubar enquanto está a ser utilizada.
- Definir o período de validade de uma credencial: Ao implementar um período de tempo limitado para o acesso à credencial pode, eventualmente, dificultar o trabalho de um atacante. No entanto, esse tempo tem que ter um equilíbrio tendo em conta que um administrador de sistemas de uma organização vai ter a necessidade de utilizar a credencial para exercer as suas tarefas.
- Privilégios mínimos: Providenciar aos administradores de sistemas apenas os privilégios suficientes para a realização das suas tarefas.
- Proteger os sistemas PAM: Os sistemas PAM são sistemas de grande interesse para os atacantes, pelo que estes devem ser cuidadosamente configurados, regularmente atualizados, de acesso restrito e devem estar integrados nos sistemas de monitorização da organização.
- Disponibilidade do sistema PAM: Deve ser tido em consideração o impacto que pode trazer para a organização se o sistema PAM ficar indisponível. A organização deve adotar medidas como disponibilidade de *backups* se necessário, e outros métodos que assegurem a disponibilidade contínua dos sistemas.

3.10. Recolha de indicadores

O ataque informático à empresa SolarWinds em 2020, permitiu que atores maliciosos comprometessem a infraestrutura dessa organização, mais especificamente o ambiente de desenvolvimento do *software* Orion, *software* esse que permite a monitorização e gestão das redes informáticas. O ataque envolveu a injeção de código malicioso no *software* Orion, e permitiu comprometer não só a própria SolarWinds assim como empresas clientes, como empresas privadas listadas na Fortune 500, agências governamentais, e outras organizações em todo o mundo (Duro, 2021; Sayed et al., 2022). Os atores maliciosos introduziram código malicioso no *software* que era distribuído aos clientes através das atualizações habituais do *software* da SolarWinds. O *backdoor* implementado permitiu que os atores maliciosos tivessem acesso não autorizado aos sistemas das organizações afetadas, conduzindo a operações de espionagem, recolha de dados e roubo de informações confidenciais (Oladimeji & Kerner, 2023). A motivação deste ciberataque sob a SolarWinds estava baseada no facto do *software* Orion estar ligado a componentes importantes das organizações como *switches*, *routers*, *firewalls*, infraestruturas virtualizadas, Active Directory, ferramentas de gestão de armazenamento, entre outras. Desta forma, os cibercriminosos comprometeram a base de dados do Orion, tendo acesso às credenciais lá armazenadas, sendo algumas delas credenciais privilegiadas. Os atores maliciosos para além de terem acesso a este tipo de credenciais, adicionaram uma conta *backdoor* capaz de fornecer acesso contínuo às aplicações e serviços da rede alvo, contornando alguns dos mecanismos de segurança organizacionais implementados pelas vítimas (Lazarovitz, 2021). Este ataque realçou que a gestão da identidade e acesso privilegiado são uma área crítica para as organizações, devido à possibilidade de comprometimento e manipulação (Hensley, 2021). Quando o *malware* infetou as máquinas dos clientes, este já possuía privilégios elevados, contudo, algo que retardou este ciberataque em algumas organizações foi o facto de várias adotarem o princípio de menor privilégio, este baseia-se que os utilizadores apenas têm as permissões necessárias para desempenharem as suas funções diárias. – Por isso, o princípio de menor privilégio, considerado uma boa prática de cibersegurança, deve ser implementado pelas organizações, pois auxilia na proteção do acesso privilegiado a dados e ativos críticos e ajuda as equipas de segurança a impedir o movimento lateral dificultando a tarefa dos atores maliciosos (Lazarovitz, 2021). Este princípio é um elemento fundamental do modelo de *zero trust*, sendo este último um conceito que se baseia na premissa de que as organizações não devem confiar em nenhum individuo, dispositivo, rede, entre outros elementos, verificando constantemente a identidade de quem tenta aceder aos sistemas antes de conceder o acesso (Lazarovitz, 2021).

Assim, de seguida, são apresentadas algumas das conclusões que se podem tirar do ataque à SolarWinds e que podem contribuir para aumentar o conhecimento e melhorar as práticas de segurança das organizações de forma transversal (Lazarovitz, 2021):

- As identidades, sejam humanas ou máquinas, podem ser comprometidas, sendo fundamental identificar, isolar e impedir que as ameaças obtenham acesso privilegiado capazes de se movimentarem lateralmente.
- Devido aos ataques informáticos se focarem cada vez mais no comprometimento de identidade e abuso de credenciais privilegiadas, é necessário obter uma visão completa da identidade, com recurso ao inventário de credenciais privilegiadas. Deste modo, é possível visualizar e gerir palavras-passe, chaves de acesso, chaves API, entre outros.
- É importante que as credenciais privilegiadas estejam armazenadas em cofres e com mecanismos de rotação de palavras-passe, ajudando a reduzir a sua exposição. Para além disso, a gestão contínua de sessões privilegiadas possibilita também que as equipas de segurança detetem, desde cedo, eventuais situações de ameaça, dificultando o trabalho dos atores maliciosos.
- A aplicação do princípio de menor privilégio é um fundamento de extrema importância, pois permite reduzir a exposição de um ciberataque e pode, eventualmente, impedir a disseminação de *malware* e ajuda a evitar que os atores maliciosos utilizem privilégios elevados para ampliar o acesso e se movimentarem lateralmente.
- Como forma de reduzir as falhas de segurança, limitar os movimentos dos atores maliciosos e detetar sinais de ataques, surgem assim as soluções de gestão de acesso privilegiado. É importante definir uma estratégia de gestão de identidade sólida, pelo que as soluções de gestão de acesso privilegiado permitem manter a visibilidade e controlo necessários para que as organizações se possam proteger adequadamente.

Este ataque teve um impacto significativo em muitas organizações e realçou a importância da implementação de medidas de cibersegurança mais rigorosas, uma vez que as ameaças estão cada vez mais sofisticadas, sendo que a proteção das redes e sistemas é uma tarefa contínua e crucial (Hensley, 2021). É fundamental reconhecer a significância da adoção de políticas robustas de segurança de identidade que limitem o acesso privilegiado a sistemas, minimizem a exposição e facilitem a deteção precoce de potenciais ataques (Lazarovitz, 2021).

O PAM representa uma abordagem que visa proteger, controlar, monitorizar e gerir a atividade privilegiada dos recursos, com o objetivo de reduzir o risco. Deste modo, é novamente referido o

conceito de privilégios mínimos, que consiste no fornecimento de acesso privilegiado apenas a utilizadores e recursos que necessitem de tais permissões para a realização de uma tarefa. A implementação de PAM é realizada através de soluções, políticas e procedimentos que se focam na gestão de privilégios, sendo que estas soluções fornecem as ferramentas necessárias para proteger os ativos, como recursos críticos que possuem informações e infraestruturas sensíveis. As soluções PAM providenciam várias funcionalidades e componentes como o armazenamento e gestão de palavras-passe, gestão de sessões, entre outras capacidades conforme se pode verificar na figura 4 (Haber & Rolls, 2020).

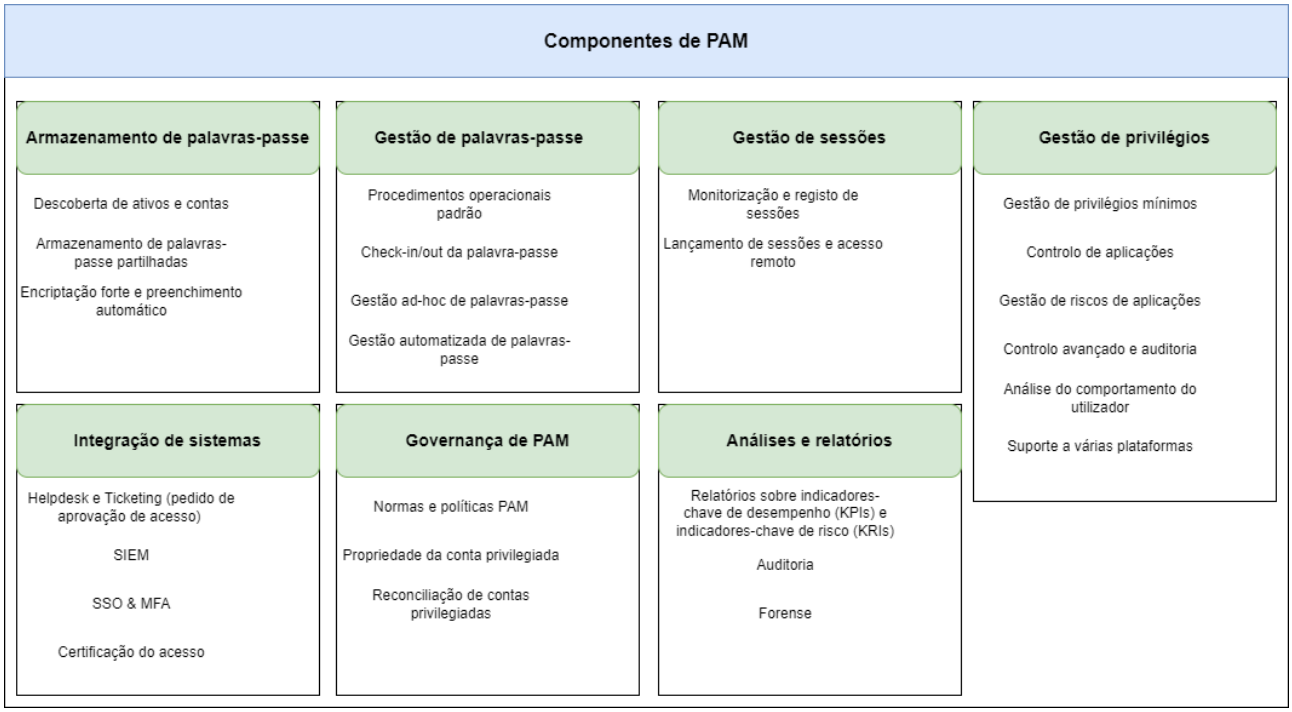


Figura 4 - Componentes de PAM, adaptado de Haber & Rolls, 2020

Após o enquadramento teórico realizado sobre as funcionalidades de PAM e a verificação dos componentes que constituem a base de uma solução PAM, o objetivo prático do presente estudo é verificar a conformidade de alguns dos grupos categorizados acima. Deste modo, e tendo em consideração que o âmbito deste estudo procura demonstrar a pertinência de PAM, sobretudo, na gestão e armazenamento de palavras-passe e na gestão de sessões privilegiadas, através dos desenvolvimentos de CPM *plugins* e componentes de conexão, as categorias alvo deste estudo incidem sobre os primeiros três grandes grupos presentes na figura 4 – Armazenamento de palavras-passe, Gestão de palavras-passe e Gestão de sessões.

É esperado que as ferramentas PAM no domínio do armazenamento e gestão de palavras-passe e gestão de sessões possuam as seguintes capacidades (Haber & Rolls, 2020):

- **Armazenamento de palavras-passe –** As soluções PAM possuem funcionalidades capazes de armazenar credenciais como, por exemplo, guardar as contas num cofre, sendo possível efetuar a recuperação manual ou automática dessas mesmas credenciais. Possui a funcionalidade de descoberta de ativos, esta permite identificar ativos ligados numa rede, assim como as respetivas contas e importar para a solução PAM. Quanto ao armazenamento de *passwords* estas são guardadas em cofres e podem ser partilhadas, através da abordagem de um-para-muitos permitindo que vários utilizadores possam aceder à mesma conta privilegiada. As credenciais armazenadas devem ser encriptadas para evitar ações não autorizadas por atores maliciosos. Para além dessa função, as ferramentas PAM devem ser capazes de injetar automaticamente as *passwords* nos sistemas privilegiados proporcionando uma melhor experiência ao utilizador e proteger as palavras-passe da exposição humana ou *softwares* maliciosos.
- **Gestão de palavras-passe –** As soluções PAM permitem gerir palavras-passe, estas podem englobar contas humanas ou não humanas como contas de serviço, aplicação, *scripts* entre outros. O PAM possibilita gerir a complexidade da palavra-passe ou determinar a frequência da rotação da mesma de acordo com as políticas organizacionais estabelecidas. Para além disso, permite efetuar a gestão automatizada de credenciais, assim como a gestão *ad-hoc* de credenciais. A gestão *ad-hoc* é útil para situações como recuperação de desastres ou outras emergências. As soluções PAM fornecem a funcionalidade de *check in* e *check out* que permite que uma conta privilegiada apenas pode ser acedida por um utilizador em simultâneo.
- **Gestão de sessões –** A gestão de sessões é outro componente fundamental de PAM, este permite registar as interações do utilizador. Inclui a monitorização e registo de sessões, que significa a capacidade de efetuar o registo da atividade das sessões privilegiadas para efeitos de auditoria, em tempo real ou numa data posterior, sendo esta informação disponibilizada em formatos legíveis. Para além desta função, as ferramentas PAM possibilitam a execução de sessões, esta função remete para a capacidade de executar automaticamente uma sessão, que inclui a injeção automática das credenciais no sistema alvo a partir da solução PAM.

Este estudo, tem como objetivo principal destacar a importância do uso de soluções PAM, tendo como enfâse de investigação os componentes de gestão e armazenamento de palavras-passe e

a gestão de sessões privilegiadas. Para além disso, pretende-se ainda analisar as funcionalidades que o *software* da CyberArk possui em comparação com as informações disponíveis na literatura atual, de forma a compreender como estes mecanismos contribuem para a segurança das organizações. Portanto, o objetivo visa compreender como a solução da CyberArk auxilia na monitorização, controlo e isolamento de credenciais e sessões privilegiadas.

4. Descrição do estudo

O estudo abrange a gestão de acesso privilegiado e como soluções deste tipo podem auxiliar as organizações no fortalecimento da segurança das suas contas privilegiadas, acesos remotos e, consequentemente, a segurança dos seus sistemas, aplicações, dispositivos e outros recursos críticos organizacionais. As soluções de Gestão de Acesso Privilegiado permitem proteger, controlar e monitorizar as contas privilegiadas com acesso aos recursos das organizações. Estas soluções visam responder às constantes ameaças de acesso não autorizado e uso indevido das contas privilegiadas, sendo capazes de garantir a segurança avançada das credenciais de forma automática e centralizada.

Em conclusão, este estudo incidiu sobre a revisão teórica da área de gestão de acesso privilegiado e como pode ajudar as organizações a enfrentarem desafios complexos como ciberataques perpetrados por atores maliciosos internos e externos, com o objetivo de comprometer contas privilegiadas. Para além disso, o estudo destacou os benefícios enumerados pela área de gestão de acesso privilegiado e pretendeu comparar com as funcionalidades oferecidas pela solução PAM da CyberArk.

5. Metodologia de investigação

Para a realização deste estudo sobre Gestão de Acesso Privilegiado foi adotada uma metodologia de tipo qualitativa. Numa primeira fase, o estudo baseia-se numa revisão teórica abrangente sobre a área de PAM, seguida do desenvolvimento de componentes de conexão e *plugins* integrados na solução de gestão de acesso privilegiado da CyberArk. Esta abordagem permite uma compreensão aprofundada dos conceitos e práticas relacionadas com PAM, nomeadamente, gestão de contas privilegiadas e acessos remotos.

O trabalho elaborado na presente dissertação é assim um projeto de desenvolvimento no âmbito da solução PAM da CyberArk. O estudo pretende responder à pergunta de até que ponto a solução PAM da CyberArk está em conformidade com a informação apresentada na literatura atual face ao

que é esperado numa solução de PAM, com especial foco no armazenamento e gestão de credenciais e gestão de sessões privilegiadas.

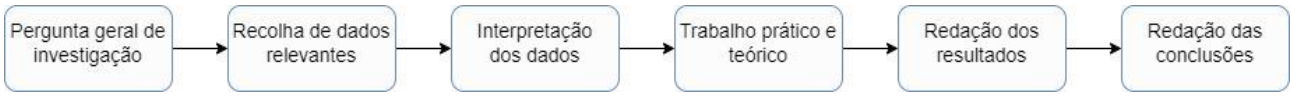


Figura 5 - Principais fases do estudo

O estudo iniciou com a formulação da perguntar geral de investigação, pelos que os artigos e documentos técnicos foram selecionados tendo como base a sua relevância com o tema. A seleção destas informações passou pelas fases de recolha de dados relevantes e interpretação dos dados, com o objetivo de responder à pergunta de investigação em estudo. Em suma, pretendeu-se destacar a importância das soluções PAM, o que envolveu o desenvolvimento prático com recurso à solução da CyberArk. Este trabalho teve como objetivo efetuar a comparação dos componentes recolhidos, nomeadamente, os componentes de gestão e armazenamento de credenciais e a gestão de sessões privilegiadas, com as funcionalidades que a CyberArk possuí, procedendo-se no final à discussão dos resultados e redação das conclusões. Os critérios comparativos são identificados através da revisão da literatura mencionados em estudos anteriores relacionados com PAM, que servirão de indicadores para avaliar e comparar os resultados do desenvolvimento prático efetuado.

O trabalho resultante da literatura é baseado em conhecimentos comprovados no domínio da segurança da informação. Deste modo, procura-se perceber se os indicadores mencionados no terceiro capítulo deste estudo, na secção 3.10. Recolha de indicadores, com recurso à literatura atual da área de gestão de acesso privilegiado, está alinhada com as funcionalidades evidenciadas pela solução da CyberArk referenciadas na secção 6.3. Desenvolvimento e análise.

O objeto de investigação e desenvolvimento, é assim centrado na área de gestão de acesso privilegiado, composta por vários subsistemas, ferramentas e políticas de segurança. Os dados de investigação recolhidos são na sua maioria textuais sob a forma de documentos científicos e documentos técnicos. Os métodos de investigação e interpretação dos dados utilizam a metodologia qualitativa focados no campo da análise e pesquisa de informações científicas e técnicas relacionadas com o tema alvo. Os dados qualitativos recolhidos ao longo da investigação passarão pelo processo de codificação, que significa a seleção de dados empíricos importantes, nomeadamente indicadores, que servirão como termo comparativo perante as características fornecidas pelo *software* da CyberArk. Neste sentido, será feito o relacionamento desses indicadores, obtidos através de várias fontes, com a solução PAM da CyberArk.

A revisão da literatura envolveu a recolha de informação relacionada com a segurança da informação, cibersegurança e gestão de identidades, que constata que atores maliciosos procuram comprometer contas com acessos privilegiados para poderem aceder a sistemas organizacionais críticos, com resultados que podem implicar danos reputacionais ou financeiros (Weihe, 2022b).

Como refere a literatura, os ciberataques têm ocorrido com maior frequência (Battaglioni et al., 2022), sendo as contas privilegiadas um dos alvos principais dos atores maliciosos, estas contas permitem assim acesso a sistemas, bases de dados, aplicações, dispositivos e outros recursos críticos (Australian Cyber Security Centre, 2022). No âmbito organizacional, as empresas podem adotar várias estratégias, aquela que entra neste domínio são as soluções de gestão de acesso privilegiado. PAM fornece funcionalidades que permitem a integração com várias tecnologias e a adoção de medidas complementares. Um dos primeiros aspetos é a integração com sistemas de Gestão de Acesso e Identidade, permitindo uma gestão adequada das contas e acessos em toda a infraestrutura organizacional (Alruwies et al., 2021). PAM fornece visibilidade dos utilizadores com acesso privilegiado, efetua a gestão e monitorização de contas privilegiadas e fornece um registo de atividades completo (Weihe, 2022a). Este tópico abordado na revisão teórica do presente estudo, foi demonstrado de modo prático no sexto capítulo, tendo sido possível evidenciar os seus benefícios através do desenvolvimento de componentes de conexão e *plugins*.

Nesse contexto, a solução oferecida pela CyberArk ganhou destaque como uma opção proeminente na gestão de acessos privilegiados. De acordo com a consultora Gartner, a CyberArk segue como um dos líderes na área de PAM, destacada perante os outros competidores, fornecendo uma abordagem baseada no modelo de *zero trust* e privilégio mínimo (CyberArk, 2022a). Esta esta consultora destaca a CyberArk como a maior marca de PAM, com uma vasta história neste setor, detendo a maior parte da quota do mercado (Gartner, 2022).

O presente estudo propõe abordar a eficácia e as características inerentes a essa solução, baseando-se na análise de informações científicas e na observação prática. Este estudo visa assegurar a fiabilidade da recolha de informações, através da seleção de fontes de qualidade que formem uma amostra representativa do conhecimento atualmente disponível na área de gestão de acesso privilegiado. A avaliação da fiabilidade é um elemento fulcral no contexto desta dissertação e está divida em dois pontos. Primeiramente, a recolha de literatura presente no segundo capítulo e a investigação sobre a área de gestão de acesso privilegiado presente no terceiro capítulo apresentam resultados introdutórios e textuais sobre o domínio da investigação. O segundo ponto prende-se com a recolha de indicadores, que permitam estabelecer elementos característicos expectáveis das soluções PAM para, deste modo, permitir comparar as características documentadas na literatura com as funcionalidades que a solução da CyberArk providencia. Procura-se entender as

características associadas à solução PAM da CyberArk, a expectativa referente ao seu uso e respetiva análise da aplicação prática. A análise comparativa entre as práticas observadas e a literatura científica existente constituirá uma abordagem integral para avaliar a coerência da solução da CyberArk.

Em suma, será conduzida uma análise à solução PAM da CyberArk, com o intuito de identificar como esta solução se alinha às práticas recomendadas conforme a literatura, com especial foco nas funcionalidades de gestão e armazenamento de credenciais e gestão de sessões.

6. Apresentação, análise e discussão dos resultados

6.1. Descrição

Neste capítulo será apresentado o projeto desenvolvido no domínio da Gestão de acesso Privilegiado. O trabalho está assente na solução de Gestão de Acesso Privilegiado da CyberArk (*CyberArk Privileged Access Manager - Self-Hosted v12.2*). Esta é uma solução considerada líder no seu segmento, de acordo com a Gartner, oferecendo recursos de segurança e gestão de acesso para contas privilegiadas em toda a infraestrutura de uma organização (Gartner, 2022). A arquitetura da solução PAM *Self-Hosted*, baseia-se na tecnologia Vaulting da CyberArk e é uma solução de ciclo de vida completo, capaz de gerir contas privilegiadas e chaves SSH. As palavras-passe podem ser armazenadas, partilhadas ou transferidas de forma segura entre os funcionários autorizados dentro de uma organização. A arquitetura desta solução é projetada com base num modelo de múltiplas camadas de segurança que incorpora elementos como *firewall*, VPN, autenticação, controlo de acesso, encriptação, entre outros, providenciando maior segurança no domínio das palavras-passe. Esta solução PAM pode ser acedida através de um cliente Windows, interface *web* ou através do uso de APIs. A arquitetura é composta por dois elementos principais, nomeadamente, o Cofre (Vault, em inglês) ou Motor de Armazenamento e o segundo é a interface (interfaces Windows, *Web* e SDK) (CyberArk, 2023c).

Posto isto, tal como mencionado anteriormente, foi efetuado o enquadramento teórico de forma a recolher indicadores dividido por categorias para poder efetuar uma análise comparativa, ou seja, recolher indicadores sobre o que é esperado uma solução PAM oferecer e comparar, sobretudo de forma prática, com as funcionalidades oferecidas pelo *software* da CyberArk. Será apresentada a arquitetura em que está assente a solução da CyberArk, e serão identificados os componentes chave que permitiram realizar este projeto. De realçar que, este estudo tem limitações ao nível do uso de alguns componentes devido à arquitetura estar implementada numa infraestrutura organizacional

real. Consequentemente, serão expostos os desenvolvimentos efetuados, nomeadamente, o componente de conexão (*connection component*, em inglês) que serve para criar sessões remotas seguras através de um *proxy*, capaz de isolar a estação de trabalho do utilizador e a máquina remota alvo. Para além do componente de conexão, será exposto o desenvolvimento do *plugin*, estes *plugins*, ou seja, Central Policy Manager *plugins*, também designados por CPM *plugins*, permitem que o utilizador, através da interface *web* da CyberArk, consiga verificar se a palavra-passe da conta privilegiada está correta, permite alterar a palavra-passe, ou por último reconciliar as palavras-passe caso a tecnologia do dispositivo remoto assim o permita.

Desta forma, é pretendido demonstrar a pertinência das soluções PAM e como estas ajudam a proteger, gerir, controlar e monitorizar as atividades associadas a todos os tipos de identidades privilegiadas.

6.2. Arquitetura CyberArk

A arquitetura CyberArk apresentada neste subcapítulo será referenciada e esclarecida com recurso à documentação técnica disponível no site oficial desta organização de segurança e gestão de identidades (CyberArk, 2023c). Esta solução oferece proteção proativa, sistemas de deteção e ações em tempo real. A proteção proativa surge através de credenciais seguras, permissões apenas para utilizadores autorizados, responsabilidade individual de cada utilizador, isolamento de sessões e limitação do âmbito dos privilégios. Os mecanismos de deteção referem-se à monitorização contínua, capaz de identificar comportamentos maliciosos e de alto risco, bem como aos alertas disponíveis. A resposta em tempo real, traduz-se na possibilidade de suspender ou encerrar sessões de utilizadores em tempo real e um registo forense completo.

Os componentes que fazem parte da estrutura basilar utilizada neste projeto são o Digital Vault ou simplesmente Vault, PrivateArk Client (PA), Password Vault Web Access Interface (PVWA), Privileged Session Manager (PSM) e Central Policy Manager (CPM).

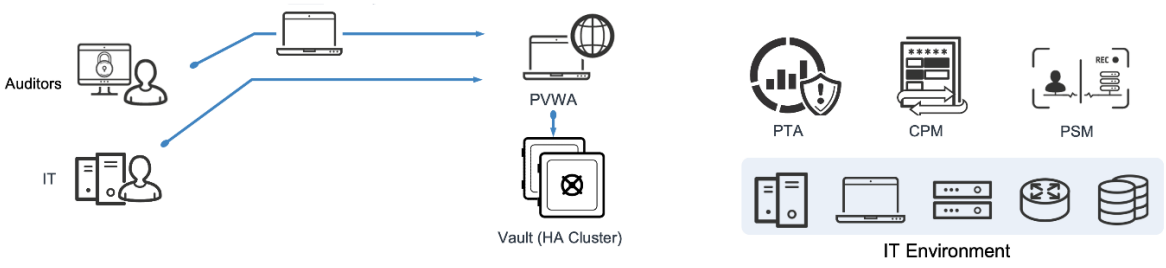


Figura 6 - Arquitetura CyberArk PAM - Self-Hosted, CyberArk, 2023

Vault: O CyberArk Digital Vault está assente numa máquina Windows Server, é considerado um servidor seguro e é utilizado para armazenar informações de contas privilegiadas, dados, e outras configurações do sistema. Dentro do Vault existem assim sub-cofres (*safes*), esses *safes* permitem guardar informações como credenciais de contas privilegiadas e informações do sistema. Este é o elemento central, pois é o Vault que permite que outros componentes tenham acesso às credenciais, pelo que as ações do utilizador são registadas.

PSM: O Privileged Session Manager é implementado em servidores Windows e permite que as organizações protejam, controlem e monitorizem o acesso privilegiado a dispositivos na sua rede. O PSM, através de componentes de conexão, garante o acesso remoto seguro aos sistemas e outros recursos sensíveis, isolando o utilizador final dos dispositivos alvo, sem revelar palavras-passe ou outras chaves, mantendo um alto nível de segurança. Este componente gere o acesso a contas privilegiadas e aplica políticas que determinam quem são os utilizadores autorizados a aceder às contas privilegiadas, quando e com que finalidade. O PSM possibilita a restrição de comandos não autorizados quando executados por um utilizador, permite também gravar todas as atividades realizadas durante as sessões privilegiadas, fornece auditorias e possibilita a reprodução dos vídeos, sendo que estas gravações ficam armazenadas no Vault e podem ser consultadas por utilizadores autorizados, como os auditores. O PSM pode ser integrado com outro componente, nomeadamente o Privileged Threat Analytics (PTA), componente este que não foi considerado para o desenvolvimento deste estudo. A integração do PSM com o PTA, permite às organizações identificarem, em tempo real, sessões privilegiadas com um significativo grau de risco. Consequentemente, a deteção de atividades não expectáveis ou atividades potencialmente maliciosas permite que as organizações se foquem na análise da situação e respondam prontamente. Deste modo, pode constatar-se que o PSM age como um *proxy* permitindo conexões seguras a sistemas críticos, isolando as mesmas e monitorizando a atividade de contas privilegiadas. Por fim, a CyberArk também dispõe do PSM para conexões SSH, este está instalado em máquinas Unix e opera com o mesmo objetivo dos PSMs para máquinas Windows.

CPM: O Central Policy Manager está também instalado em servidores Windows, sendo que a gestão de palavras-passe é efetuada através deste componente. O CPM, através de CPM *plugins*, permite a gestão de palavras-passe, e consequentemente permite efetuar três operações, o *Verify*, *Change* e *Reconcile*. Este componente consegue verificar se as palavras-passe de contas privilegiadas estão em conformidade (*verify*). É capaz de alterar automaticamente as palavras-passe em máquinas remotas e armazenar no Vault de forma segura, sem intervenção humana, conforme as

políticas definidas pelas organizações (*change*). E, por último, dependendo do dispositivo remoto, fornece a possibilidade de reconciliar palavras-passe (*reconcile*). O reconciliar da palavra-passe é o processo de recuperar a palavra-passe de uma conta privilegiada de um dispositivo, com recurso a uma segunda conta privilegiada com permissões mais elevadas (administrador), sendo assim, capaz de redefinir a palavra-passe do utilizador alvo sem saber a *password* anterior. O processo de reconciliação só é possível se a aplicação ou dispositivo remoto permitirem que um administrador defina as palavras-passe dos utilizadores.

PVWA: O Password Vault Web Access Interface é a interface *web* que fornece aos utilizadores o acesso a informações de contas privilegiadas. Este componente está instalado numa máquina Windows Server, e utiliza tipicamente o serviço *web* assente no Internet Information Services (IIS). O PVWA permite solicitar, aceder e gerir palavras-passe privilegiadas, assim como fornece uma visão abrangente sobre todo o sistema PAM, como os componentes instalados (Vault, CPM, PSM, entre outros) e o seu estado de conexão. Para além disso, este componente apresenta estatísticas e é também utilizado por administradores PAM para configurar as políticas de acesso dos utilizadores. O PVWA permite que os utilizadores efetuem conexões remotas privilegiadas através da interface *web* e permite que os auditores possam monitorizar essas mesmas sessões.

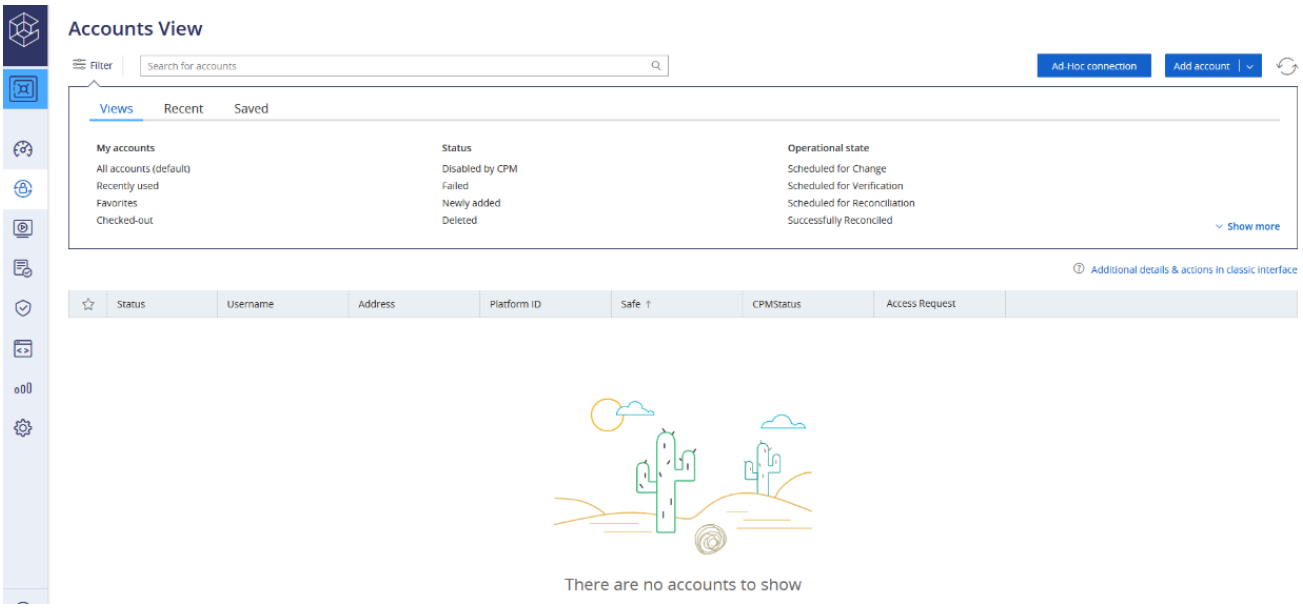


Figura 7 - PVWA

PrivateArk: O PA é uma aplicação Windows responsável pela gestão da solução PAM da CyberArk. Este pode ser instalado no servidor Vault ou em outras estações, como por exemplo, nos servidores CPM ou PSM. O PrivateArk permite aos administradores acederem às informações

armazenadas no Vault. O administrador PAM pode, por exemplo, criar vários *safes* dentro do Vault, bem como criar utilizadores. Os *safes* contêm propriedades que definem, entre outras configurações, quem poderá aceder a determinado *safe*, se um utilizador ou um grupo de utilizadores, por exemplo administradores, auditores, operadores, etc. No PrivateArk é possível definir propriedades dos utilizadores, como palavras-passe e níveis de controlo, bem como monitorizar as atividades referentes às *passwords* dos mesmos, conseguindo saber quem acedeu às informações, quando e de onde. Cada comando efetuado no PrivateArk, como pedidos, transferências de ficheiros ou configurações, é encriptado antes de ser transportado para o Vault. O PrivateArk é assim a interface *legacy* que permite comunicar com o Vault, enquanto que o PVWA é a interface *web*, mais moderna e de fácil uso, contudo, o PrivateArk continua a ser relevante, pois possui algumas características que ainda não estão disponíveis na interface *web*. Na figura 8 é possível visualizar o PrivateArk Client e o Vault disponível nesta arquitetura.

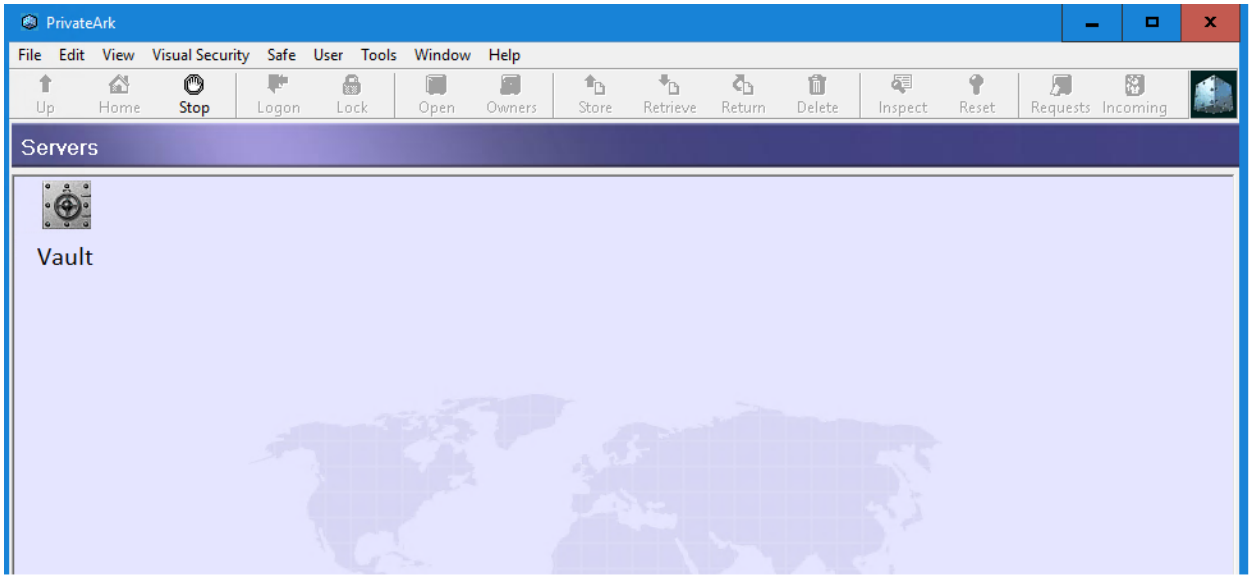


Figura 8 – PrivateArk

Por sua vez, na figura 9 o utilizador já se encontra dentro do Vault e é possível visualizar os *safes* que armazenam, entre outras informações, credenciais e ficheiros de configuração da solução PAM da CyberArk.

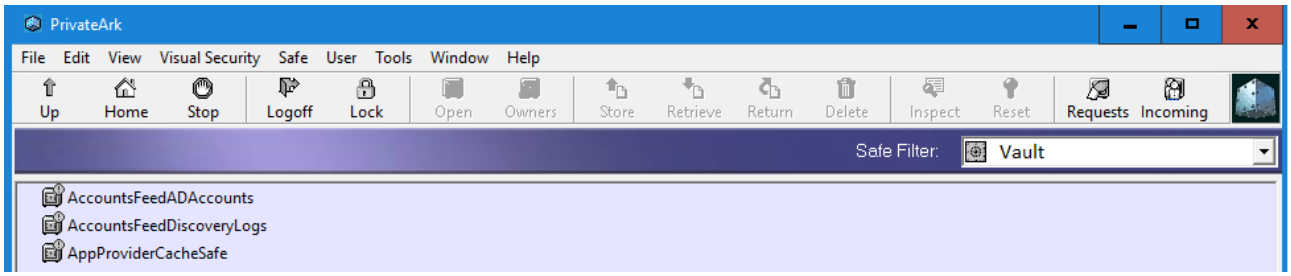


Figura 9 - PrivateArk cofres

6.3. Desenvolvimento e análise

Este subcapítulo abordará os desenvolvimentos efetuados sob a solução PAM da CyberArk com foco nos componentes de conexão e CPM *plugins* e como estes interagem com os diversos componentes presentes na solução *CyberArk Privileged Access Manager - Self-Hosted*. Os componentes de conexão e CPM *plugins* são essenciais para o bom funcionamento do PAM, pois as suas funcionalidades e flexibilidade permitem uma integração abrangente e eficaz de sistemas, dispositivos e aplicações. No final, pretende-se analisar o resultado dos desenvolvimentos efetuados com o enquadramento teórico que abrange o armazenamento e a gestão de palavras-passe, assim como a gestão de sessões privilegiadas. Relativamente ao armazenamento e gestão de *passwords*, estes têm como base garantir que as credenciais estejam seguras, encriptadas e guardadas em cofres, pelo que podem ser partilhadas inclusive numa abordagem de um-para-muitos, permitindo que vários utilizadores possam aceder à mesma conta privilegiada. Pretende-se verificar de que modo é efetuada a gestão de credenciais, como o seu nível de complexidade, a frequência da rotação, a possibilidade de gestão de palavras-passe *ad-hoc*, assim como a gestão automatizada. Por fim, quanto à gestão de sessões será analisada a forma de como são automaticamente estabelecidas as conexões aos dispositivos remotos, a funcionalidade de injetar as credenciais armazenadas no sistema PAM nos dispositivos privilegiados alvo, assim como a monitorização e registo de sessões.

6.3.1. Componente de conexão

Os componentes de conexão desempenham um papel importante na conexão da solução PAM e os sistemas ou aplicações com as quais está integrado, estabelecendo uma comunicação segura. Estes componentes permitem conectar a uma variedade de tecnologias como, sistemas operativos, bases de dados, aplicações, redes sociais, entre outros, garantindo a sua integração com contas privilegiadas em diferentes sistemas. Os componentes de conexão utilizam o servidor PSM para efetuarem as conexões aos sistemas alvo e oferecem autenticação segura, encriptação de dados, gestão e monitorização de sessões e atividades. O componente de conexão é um pedaço de código ou *script* que permite aos utilizadores da solução da CyberArk conectarem-se automaticamente ao sistema alvo, sem a necessidade de saberem a palavra-passe dos sistemas. A CyberArk disponibiliza o próprio *marketplace* com alguns componentes previamente desenvolvidos, contudo, para dispositivos que não estejam disponíveis no seu *marketplace*, a CyberArk dispõe da sua *framework* para desenvolvimento de componentes *web*, assim como dá suporte a linguagens de automação para desenvolvimentos customizados, por exemplo aplicações Windows ou base de dados. O desenvolvimento de componentes de conexão podem ser assim realizados através da *Secure Web Application Connectors Framework* disponibilizado pela CyberArk, esta *framework* permite desenvolver componentes *web*. Para efetuar conexões remotas a outro tipo de sistemas ou aplicações, como por exemplo base de dados Microsoft SQL Server ou Oracle SQL Developer, a CyberArk recomenda a utilização de AutoIT, uma linguagem de automação (*scripting*). Para este estudo foi desenvolvido um componente de conexão customizado com recurso à linguagem de *scripting* AutoIT, este permite efetuar uma ligação entre a máquina do utilizador e a máquina remota, nomeadamente uma base de dados Microsoft SQL Server Management. O uso do componente de conexão permite maior segurança, isolamento da sessão e permite efetuar o registo das atividades realizadas, bem como a sua monitorização.

Na figura 10 é demonstrado o fluxo de funcionamento do PSM através do PVWA. Primeiramente, o utilizador deve autenticar-se no PVWA (1), e de seguida selecionar uma conta privilegiada e o respetivo componente de conexão (2) para iniciar a sessão remota com recurso ao PSM (3). O componente de conexão obtém assim as credenciais guardadas no Vault e conecta-se às máquinas remotas com recurso ao servidor PSM (4) através dos vários protocolos disponíveis (5). Por fim, assim que a sessão remota é iniciada, o processo de gravação de sessão é também iniciado e, no final, essa informação é armazenada no Vault (6).

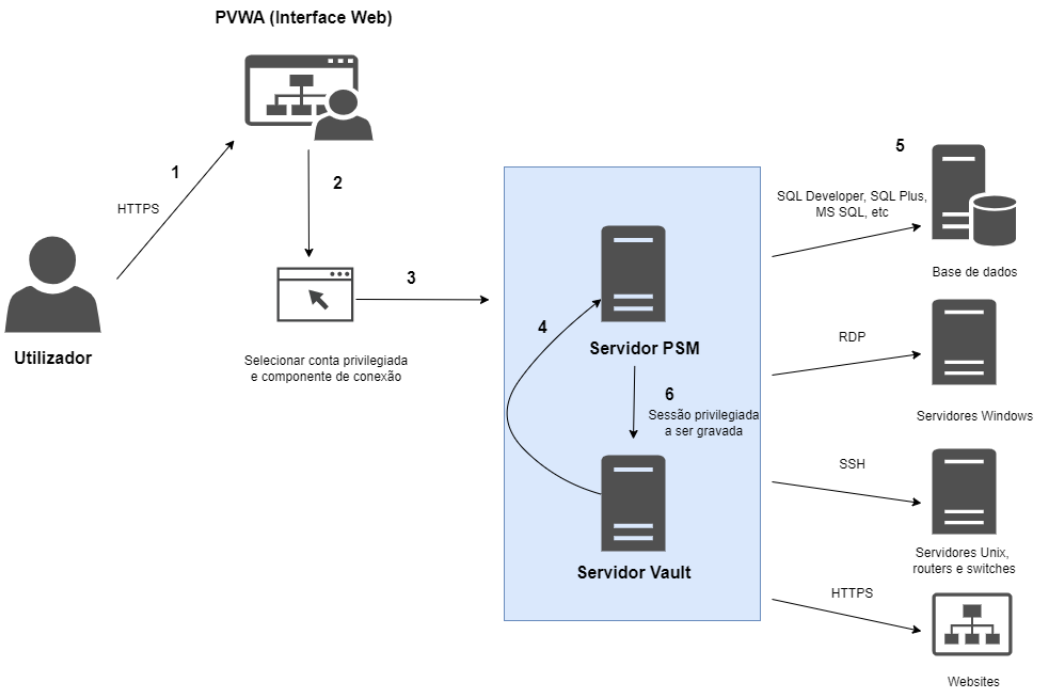


Figura 10 - Fluxo do PSM através do PVWA, adaptado de CyberArk

Fluxo de funcionamento do componente de conexão

O utilizador deve efetuar o *login* no PVWA e pesquisar pela conta privilegiada de acesso ao sistema remoto pretendido. De seguida, o utilizador deve selecionar a conta privilegiada e o componente de conexão pretendido e seguir os procedimentos necessários.

Dependendo das definições que a plataforma que suporta este componente esteja configurada, esta pode conter o mecanismo de Dual Control ativado. O sistema Dual Control é um mecanismo de controlo do Vault, isto significa que estando em modo ativo, sempre que o utilizador tente usar a conta privilegiada vai ser criado um pedido de acesso, que deverá ser autorizado por um administrador. Deste modo, como primeiro passo, o utilizador deverá inserir a justificação da utilização da conta privilegiada para iniciar a conexão remota.

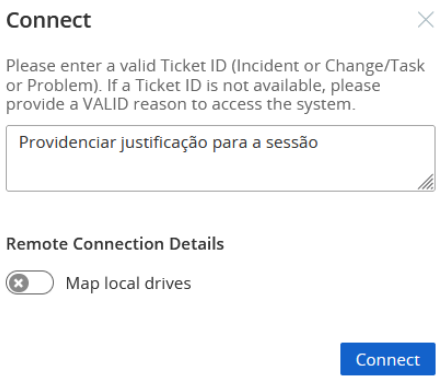


Figura 11 - Inserir justificação para validar a conexão

Após clicar no botão *Connect*, é descarregado um ficheiro RDP que permitirá o acesso remoto sem revelar a palavra-passe ao utilizador final. Após clicar no ficheiro RDP, a sessão é assim iniciada, pelo que é emitida uma mensagem a indicar que a sessão está a ser gravada com recurso às potencialidades do servidor PSM conforme é possível verificar na figura 12.

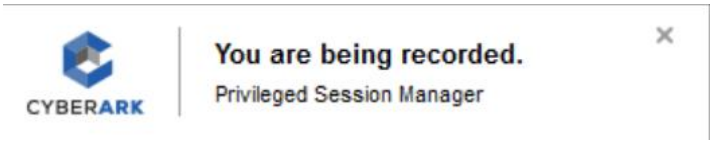


Figura 12 - Gravação da sessão iniciada

A figura 13 demonstra a sessão RDP iniciada através do componente de conexão e também a mensagem referente ao processo de gravação de sessão.

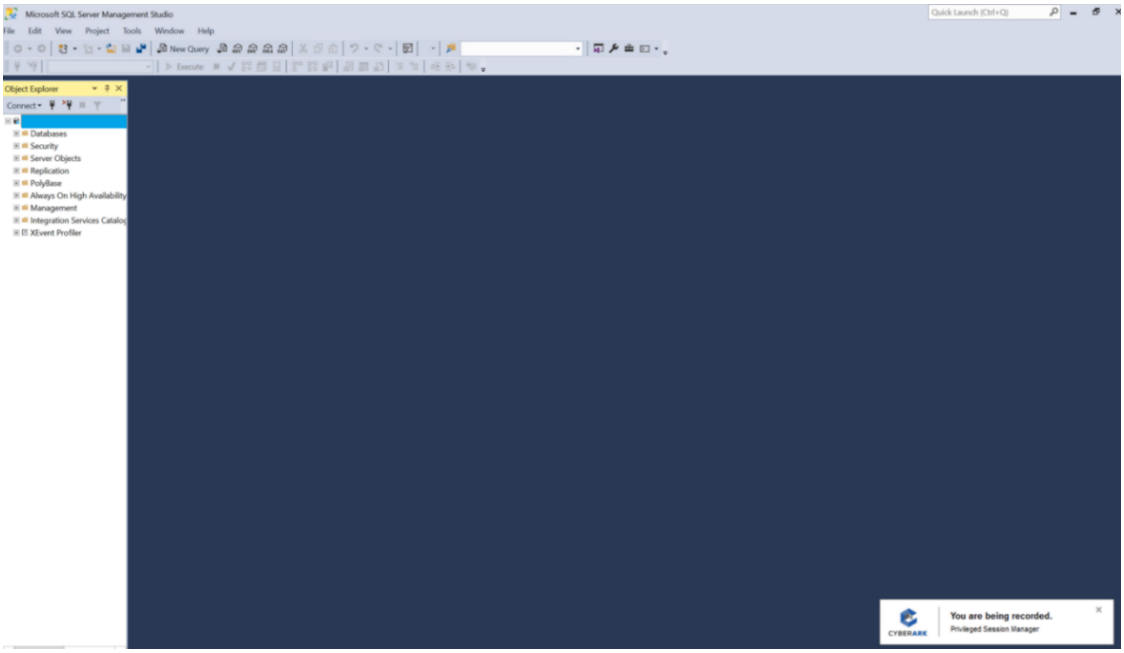


Figura 13 - Microsoft SQL Server Management, sessão iniciada

Após a sessão ser iniciada, o registo de atividades começa a atualizar em tempo real. Na figura 14 é possível observar alguns dados obtidos durante a sessão. Esta imagem indica o nome do componente de conexão (MicrosoftSQLServerComponenteConexao) e o ID (identificador) da sessão que o utilizador está a usar nesta sessão remota. Quanto aos dados referentes ao utilizador que iniciou a sessão, a base de dados, endereço do servidor e a conta privilegiada utilizada foram ocultados por não ser informação pertinente para este estudo.

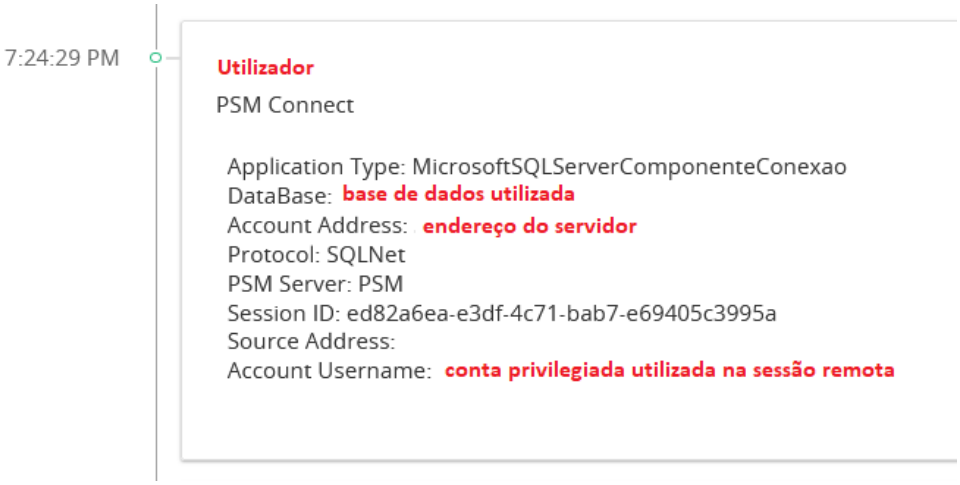


Figura 14 - Registo de atividades 1

Na figura 15 é possível observar outro aspeto importante providenciado pela CyberArk, nomeadamente, o *keystroke logging* ou registo de teclado. Este tipo de *log* regista todos os comandos efetuados pelos utilizadores, o que permite monitorizar a sessão e obter um registo detalhado caso exista algum incidente futuro.

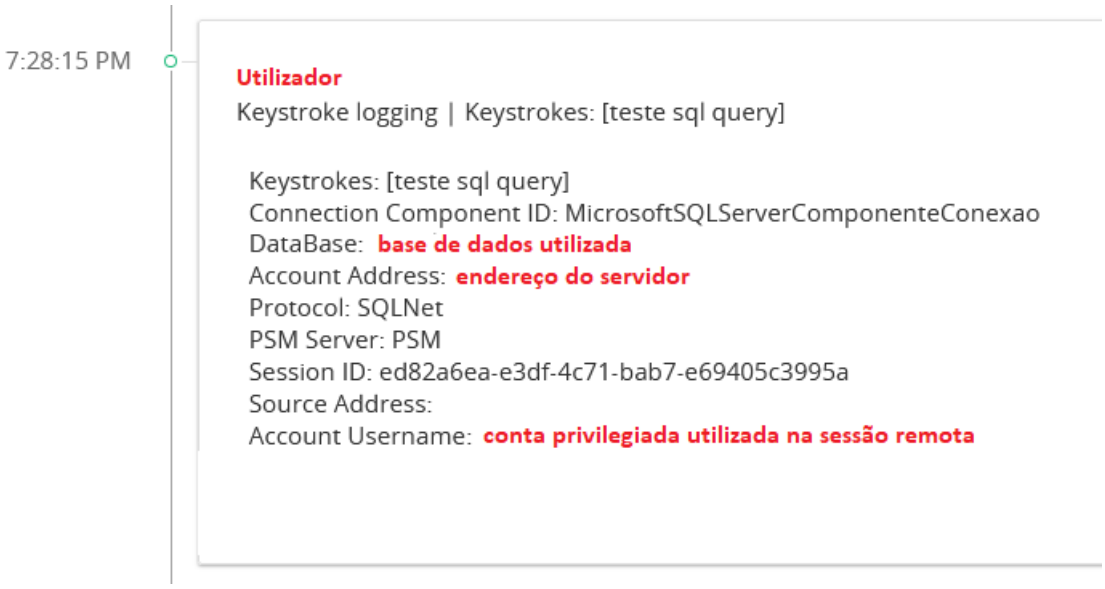


Figura 15 - Registo de atividades 2

Na figura 16 é possível observar o registo de término da sessão privilegiada por parte do utilizador que teve uma duração de 21:25 minutos.

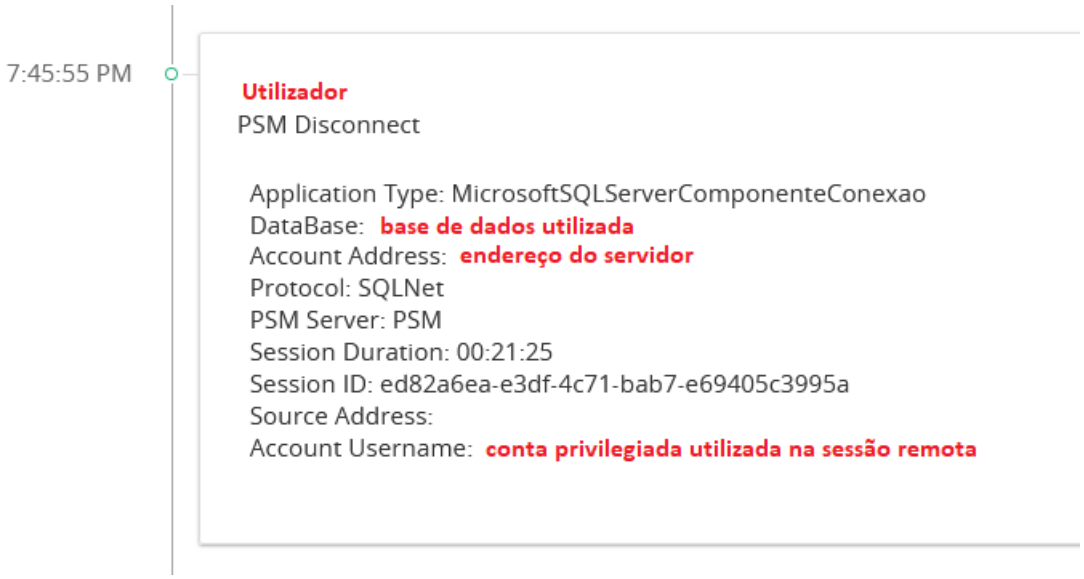


Figura 16 - Sessão privilegiada encerrada

Por fim, outro aspeto importante é o facto das sessões privilegiadas poderem ser alvo de gravação e serem revisitadas durante o período temporal estabelecido na política da organização.

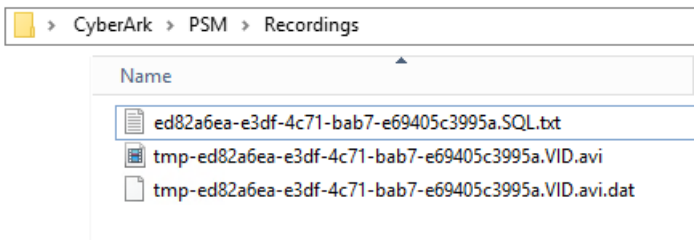


Figura 17 - Localização da gravação das sessões privilegiadas no servidor PSM

6.3.2. CPM *Plugin*

Os CPM *plugins* são utilizados para efetuar a conexão do sistema PAM às máquinas alvo de forma a gerir as credenciais de acesso. Tal como mencionado anteriormente, estes *plugins* fornecem três tipos de funcionalidades, a verificação das palavras-passe nas máquinas de destino (*verify*), alteração das palavras-passe (*change*) e a reconciliação (*reconcile*). Para além destas operações, há também a possibilidade de atualizar novas palavras-passe manualmente no Vault.

O modo de alterar as palavras-passe é diferente de sistema para sistema, como por exemplo, servidores Windows ou Unix, como de aplicação para aplicação, como base de dados Microsoft SQL Server e Oracle SQL Developer. Os CPM *plugins* estão associados a plataformas e estas definem as políticas estabelecidas pelas organizações, por exemplo, ao nível das credenciais estas podem definir o tamanho da palavra-passe ou a proibição de alguns caracteres. A proibição de caracteres, por vezes, é limitada à tecnologia do dispositivo remoto, ou seja, há tecnologias que não permitem o uso de alguns caracteres especiais, pelo que essa definição deve refletir-se na plataforma que suporta o CPM *plugin* correspondente.

A CyberArk possui a sua própria *framework* para o desenvolvimento de CPM *plugins web*, nomeadamente, a *Web Application CPM plugin Framework*, esta *framework* permite que a solução PAM efetue a conexão remota aos servidores de destino de modo a executar as operações de verificação, alteração ou reconciliação automática de palavras-passe e guardá-las no Vault. Tal como os componentes de conexão customizados, a CyberArk suporta também diferentes tecnologias para o desenvolvimento customizado de CPM *plugins*. A CyberArk disponibiliza a solução de gestão de credenciais .NET SDK, esta foi concebida para interagir com a solução PAM *Self-Hosted*. Com o .NET SDK os programadores podem desenvolver CPM *plugins* tendo como base a linguagem de programação C#, esta permite desenvolver *plugins* para sistemas Shell como SSH e sistemas *web* ou integrar com APIs. O .NET SDK é bastante abrangente sendo possível utilizar vários pacotes disponibilizados pelo NuGet, como é o caso do Selenium para integração com dispositivos *web*. Para além destes métodos de desenvolvimento, a CyberArk possibilita o desenvolvimento em C++ e dispõe ainda do Terminal Plugin Controller (TPC), uma plataforma para criar *plugins* de máquinas de estado e um interpretador para executar esses mesmos *plugins*. O TPC auxilia no desenvolvimento de novos CPM p*lugins*, podendo ser integrado com linguagens de terminal e *script*, como por exemplo Python, Powershell, cScript, entre outras.

Por fim, tal como para os componentes de conexão, a CyberArk possui também o *marketplace* de CPM *plugins* para algumas tecnologias. Deste modo, é apresentado nas figuras 18 e 19 o fluxo de um CPM *plugin* para as operações de verificação e alteração de palavras-chave ou chaves SSH respetivamente. De realçar que o processo de reconciliação é semelhante ao processo de alteração.

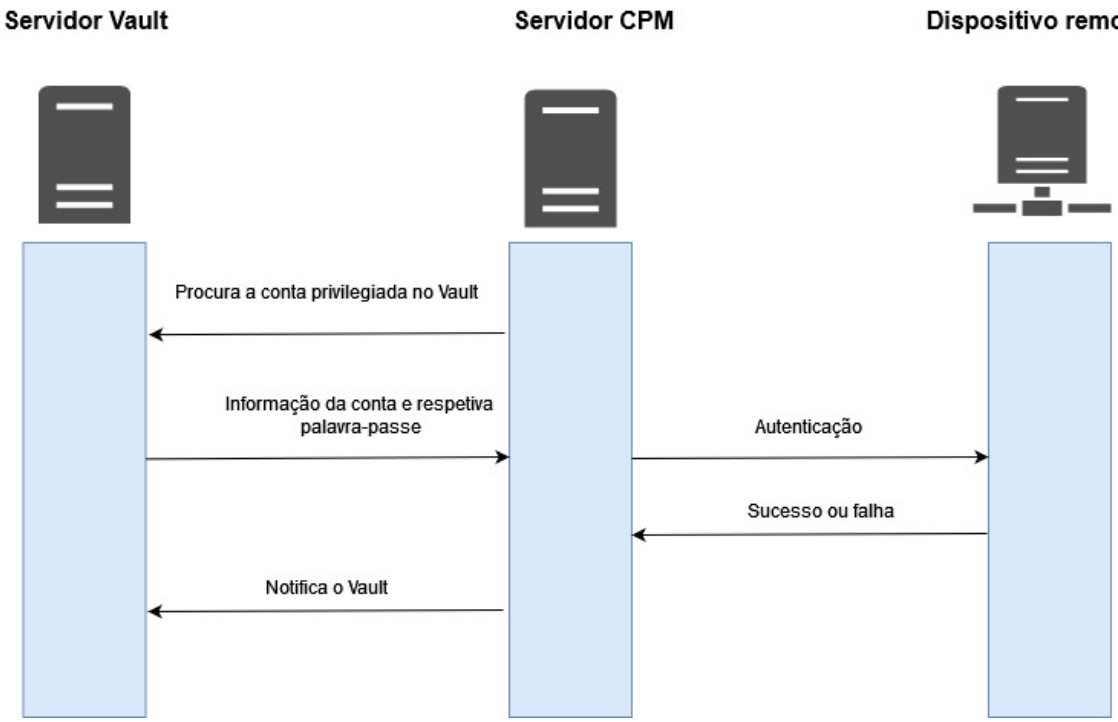


Figura 18 - CPM plugin fluxo da operação de verificação, adaptado de CyberArk

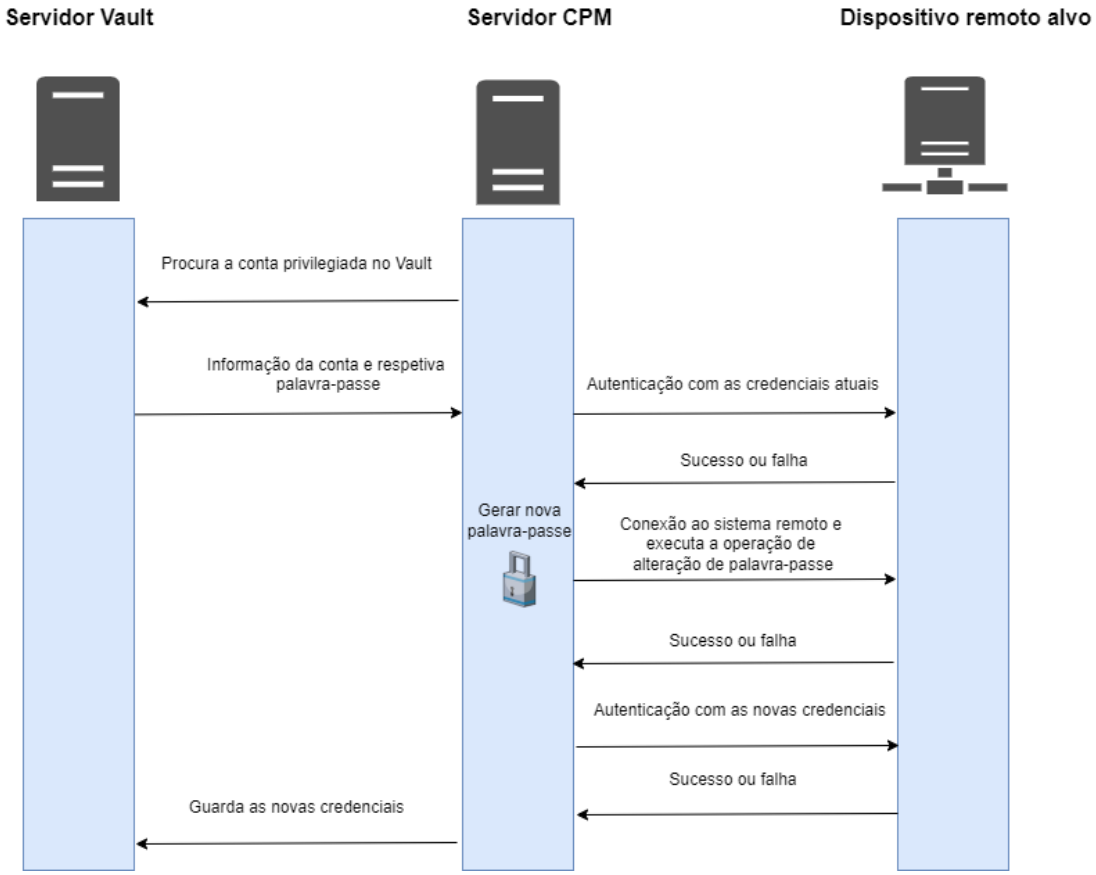


Figura 19 - CPM plugin fluxo da operação de alteração, adaptado de CyberArk

Fluxo de funcionamento do CPM *Plugin*

Os CPM *plugins* fornecem recursos avançados de segurança, gestão e controlo de contas privilegiadas, sendo capazes de atender às necessidades das diferentes tecnologias integradas.

Estes componentes permitem que a solução PAM da CyberArk se conecte a uma grande variedade de sistemas e aplicações, como sistemas operativos, bases de dados, dispositivos de rede, entre outros, de modo a gerir contas privilegiadas e efetuar as operações de verificação, alteração ou reconciliação de palavras-passe. Ao contrário do componente de conexão em que o objetivo é o utilizador final efetuar a conexão remota, por exemplo RDP ou SSH, com recurso às funcionalidades do servidor PSM (servidor *proxy*) aos dispositivos alvo para executar as suas tarefas habituais em função do seu cargo na organização, os *plugins* apenas executam as três operações mencionadas anteriormente, sem que o próprio utilizador tenha visibilidade do que está a acontecer. Isto significa que, o utilizador final com recursos à interface *web* da CyberArk, o PVWA, vai realizar as ações que necessita e ficará a aguardar o resultado, assim que o ciclo de ações do servidor CPM termine. No final do processo, o utilizador terá visibilidade sobre o estado das ações que acionou, nomeadamente, se a operação foi efetuada com sucesso, ou porventura, se a ação falhou e qual o motivo da falha. Em suma, os *plugins* permitem a configuração de políticas de acesso, rotação automática de palavra-passe, possui registo de atividades, desempenhando um papel fundamental para as organizações devido à gestão centralizada e eficiente de contas privilegiadas.

O CPM *plugin* abordado neste estudo foi desenvolvido com recurso à solução .NET SDK disponibilizada pela CyberArk, onde é possível, entre várias possibilidades, desenvolver *plugins* para terminais SSH ou *web*. Como o dispositivo remoto era um dispositivo de rede, capaz de gerir políticas de segurança em dispositivos de rede, como *firewalls*, *routers* ou *switches*, foi utilizado o .NET SDK com C# integrado com Selenium de modo a interagir com os elementos *web* do dispositivo. Isto significa que, com a utilização do Selenium, o *plugin* desenvolvido é capaz de clicar automaticamente em elementos de uma página com o objetivo de reproduzir as ações de um humano, automatizando o processo de rotação de credenciais. Este processo de rotação é totalmente isolado do utilizador final, as ações decorrem dentro do servidor CPM, sem visibilidade para os utilizadores, onde estes apenas conseguem ter acesso ao registo de atividades que foram ativadas.

Inicialmente o utilizador com recurso ao CyberArk, deve efetuar o processo de autenticação no PVWA e procurar pela conta privilegiada para poder gerir as credenciais do dispositivo alvo.

Este dispositivo de rede suporta as três operações típicas de um CPM *plugin*, nomeadamente as operações de verificação, alteração e reconciliação de palavras-passe, como é possível visualizar na

figura 20, canto superior esquerdo (*Change*, *Reconcile* e *Verify*). Para fazer a reconciliação da palavra-passe, o dispositivo remoto possui uma conta com privilégios mais elevados (administrador) para poder alterar a palavra-passe da conta com privilégios mais limitados.

Na figura 20 é assim possível visualizar a interface *web* da CyberArk (PVWA), o lado esquerdo da imagem apresenta um conjunto de definições referentes à conta privilegiada e no lado direito é possível visualizar a conta de reconciliação associada.

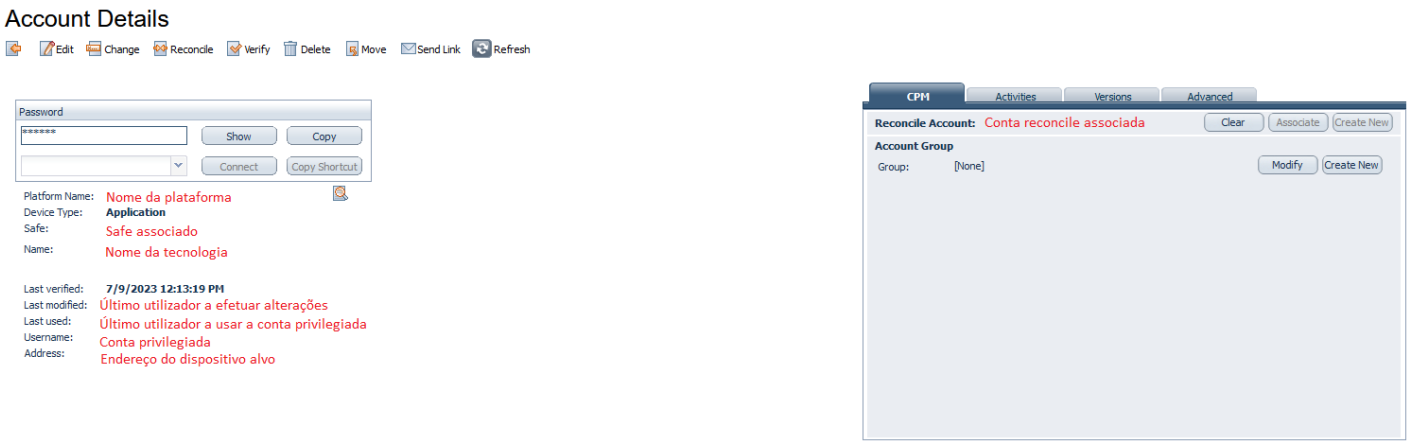


Figura 20 - PVWA dados sobre a conta privilegiada

Na figura 21 podemos observar o registo de atividades originadas através da ação acionada pelo utilizador final. Neste primeiro caso, o utilizador selecionou a operação de verificação da credencial. Esta operação vai permitir internamente ao servidor CPM efetuar o *login* automático no *website* do dispositivo de rede. De realçar que este processo é totalmente isolado do utilizador final, pelo que o mesmo não tem qualquer visibilidade das operações que estão a ser realizadas em tempo real no servidor CPM. O utilizador apenas obtém o registo de cada operação efetuada, pelo que o resultado é exposto nas atividades da conta privilegiada, tal como se pode verificar nas próximas figuras.

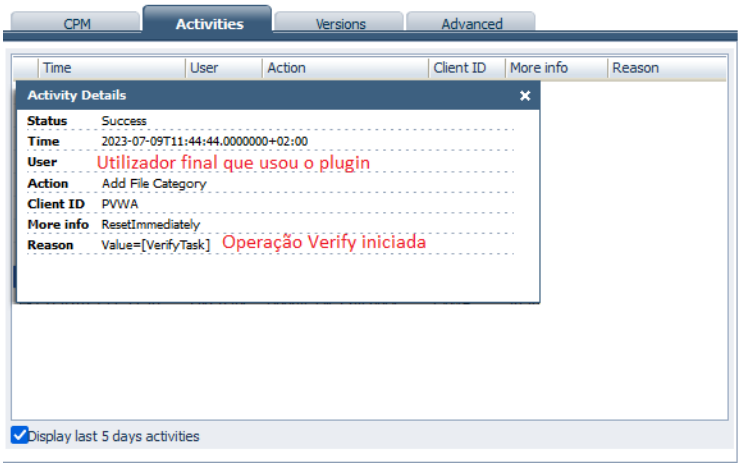


Figura 21 - Operação verify iniciada

Na figura 22 observamos que o estado da operação (*Status*) indica que a ação foi realizada com sucesso, o que confirma que as credenciais que estão no Vault encontram-se efetivamente corretas.

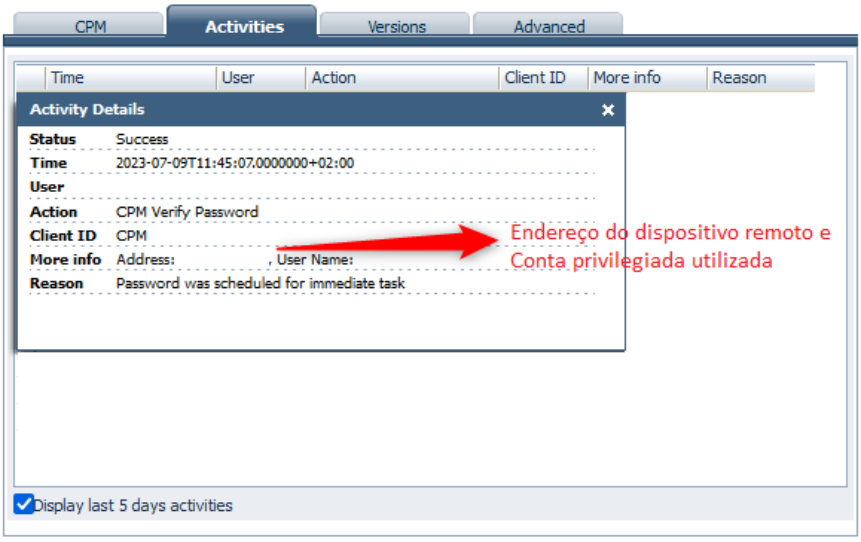


Figura 22 - Verify efetuado com sucesso

A operação de alteração da palavra-passe é idêntica ao de verificação, ou seja, a conta privilegiada vai efetuar o *login* automático no dispositivo remoto através do servidor CPM, contudo, para além de efetuar a autenticação, vai navegar automaticamente pelos menus do dispositivo e efetuar a alteração da palavra-passe. A figura 23 demonstra o processo de alteração a ser iniciado.

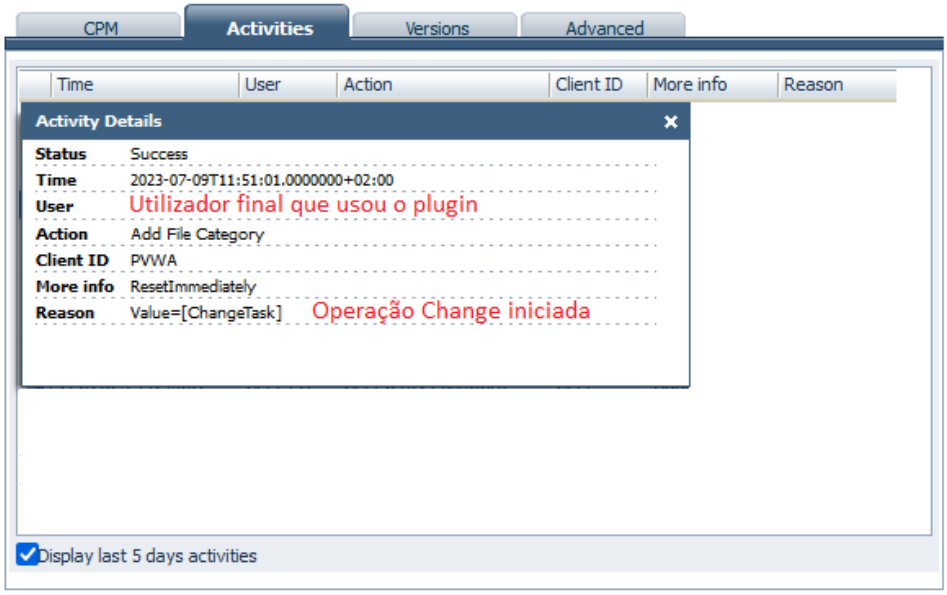


Figura 23 - Operação change iniciada

Na figura 24 obtemos um painel idêntico ao visualizado na operação *verify* e podemos observar que a operação de alteração teve sucesso, assim como também é possível observar o endereço remoto de destino e o nome da conta privilegiada utilizada.

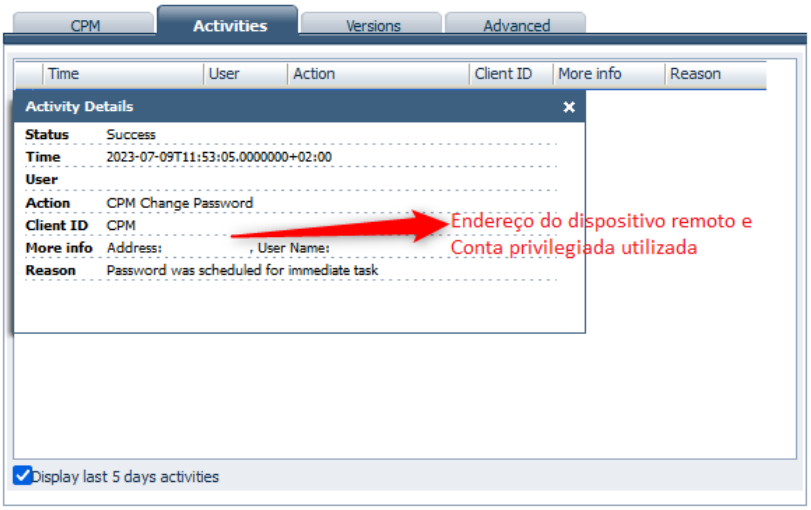


Figura 24 - Change efetuado com sucesso

Por fim, na última operação realizada, a operação de reconciliação da palavra-passe é um processo também idêntico ao processo de alteração, contudo, em vez de ser utilizada a mesma conta privilegiada das ações *verify* e *change*, é utilizada uma segunda conta, com privilégios elevados, tipicamente conta administrador, para efetuar o *reconcile*. Esta segunda conta vai, de modo automático, efetuar a autenticação no dispositivo de rede através do servidor CPM e definir a palavra-passe da conta privilegiada com menores privilégios de acordo com as políticas organizacionais estabelecidas.

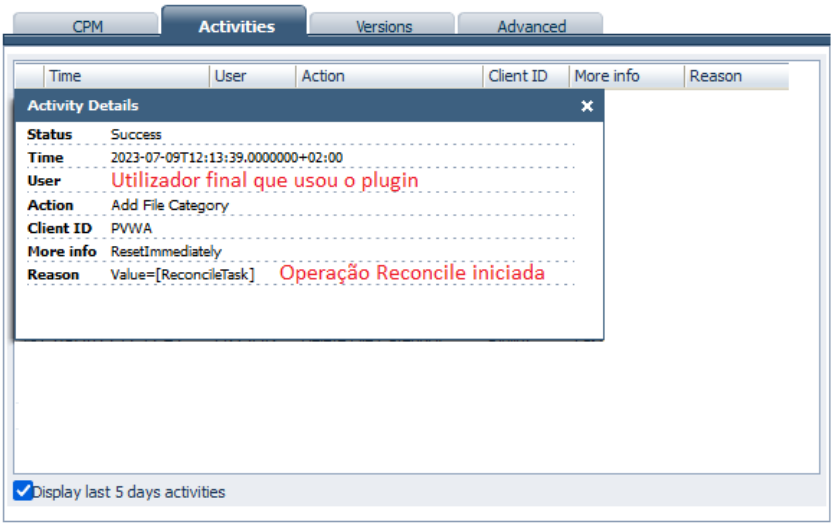


Figura 25 - Operação reconcile iniciada

Esta última figura demonstra que a operação de reconciliação foi bem-sucedida, e permite também visualizar o endereço da máquina remota alvo e a conta privilegiada utilizada onde ocorreu a alteração da palavra-passe.

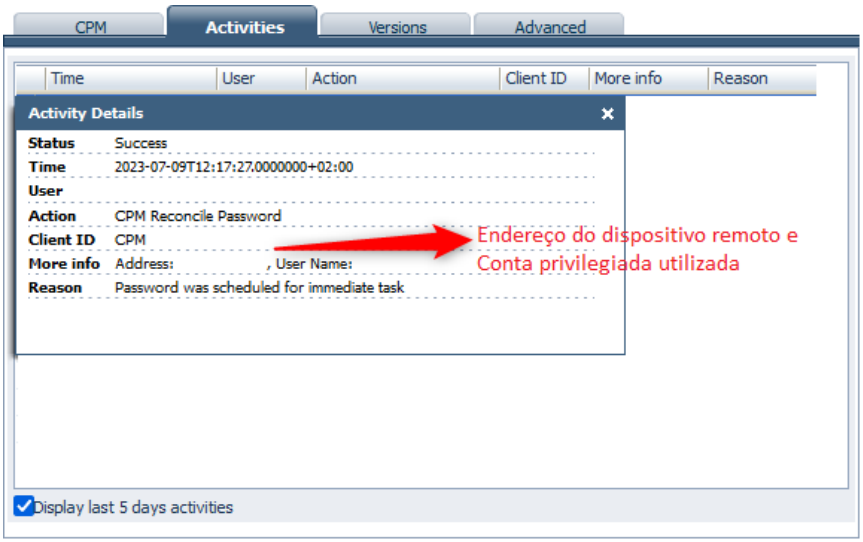


Figura 26 - Reconcile efetuado com sucesso

6.4. Discussão

O presente estudo pretendeu contribuir para a área de gestão de acesso privilegiado oferecendo uma ampla visão teórica e relacionando com os desenvolvimentos efetuados neste capítulo. Assim, pretende-se comparar os resultados obtidos na secção 6.4. Desenvolvimento e análise com os indicadores recolhidos na secção 3.10. Recolha de indicadores, com ênfase no armazenamento e gestão de credenciais e gestão de sessões. Os pontos em análise são referentes ao armazenamento de credenciais num cofre, encriptação de credenciais, gestão automática e manual de credenciais, injeção automática de credenciais nos dispositivos remotos alvo, complexidade das palavras-passe e, por fim, a gestão, a monitorização e o registo de sessões.

Os desenvolvimentos efetuados estão assentes na arquitetura da CyberArk, sendo o Vault a peça central da estrutura. Este é um servidor capaz de armazenar dados de contas privilegiadas e outras configurações do sistema de forma segura. Este servidor fornece assim informações a outros servidores, como é o caso do PSM e CPM, para que possam utilizar as credenciais armazenadas dentro do próprio Vault. Um dos pontos levantados por Haber & Rolls, 2020, a encriptação dos dados, o Vault utiliza a encriptação AES-256 compatível com o Federal Information Processing Standard (FIPS 140-2) (CyberArk, 2023a), este padrão é emitido pelo NIST e é reconhecido como um padrão confiável para a avaliação de produtos de segurança criptográfica (National Institute of Standards and Technology, 2002). As palavras-passe e ficheiros armazenados no Vault são assim encriptados, sendo atribuída uma chave de encriptação simétrica única a cada versão de cada

palavra-passe ou ficheiro armazenado. Estas chaves de encriptação são disponibilizadas de forma segura exclusivamente a utilizadores autenticados que detêm as devidas autorizações de controlo de acesso (CyberArk, 2023f).

A gestão de palavras-passe pode ser realizada de forma manual ou automática, pelo que a *Master Policy*, política que define as linhas orientadoras base para a gestão de contas numa organização com recurso à solução da CyberArk, determina a frequência com que as *passwords* são geridas (CyberArk, 2023j)**.** Neste sentido, tendo em consideração o CPM *plugin* desenvolvido constata-se a possibilidade da gestão de *passwords*, garantindo que o processo decorre com segurança, salvaguardando a proteção das credenciais e dispositivos remotos. Esta gestão, é de fácil uso e através da interface gráfica da CyberArk, o PVWA, fornece a visibilidade referente ao registo das atividades realizadas, nomeadamente, quem acionou as ações de verificação, alteração ou reconciliação das credenciais, assim como o momento em que ocorreu.

A solução PAM - Self-Hosted permite, de facto, a gestão de palavras-passe com recurso do Central Policy Manager, (CyberArk, 2023c), assim como permite definir as políticas de *passwords* conforme demonstrado na figura 29 deste estudo**.** A complexidade das *passwords* pode variar consoante a política organizacional definida. Existem várias definições possíveis de se configurar como, por exemplo, definir o tamanho exato da palavra-passe, definir a quantidade mínima de caracteres especiais ou numéricos e definir o número mínimo de letras maiúsculas ou minúsculas. Para além destas configurações, a solução da CyberArk permite também definir os caracteres proibidos, isto torna-se útil, pois, existem sistemas que não aceitam determinados caracteres no momento de alteração da *password*, permitindo assim uma configuração personalizada.

A gestão de credenciais pode ser efetuada, inclusive de forma automática, de acordo com as políticas empresariais, permitindo verificar, alterar ou reconciliar as *passwords* em máquinas remotas e guardá-las em segurança no Vault sem intervenção humana**.** Assim sendo, as credenciais são guardadas e acedidas através de um ponto central, o Vault, tendo como base as políticas de segurança estabelecidas pelas organizações, podendo eliminar tarefas administrativas manuais, que são por vezes demoradas, com o objetivo de melhorar a segurança das credenciais privilegiadas. A solução PAM - Self-Hosted permite também uma gestão *ad-hoc* de credenciais, isto significa que se a palavra-passe for alterada fora do contexto de PAM, é possível modificá-la de forma manual no Vault com o objetivo de sincronizar o sistema PAM com os dispositivos remotos em causa (CyberArk, 2023e). A solução da CyberArk possui a funcionalidade de *check in* / *check out* de contas, esta função permite que as contas privilegiadas possam ser utilizadas apenas por um utilizador em simultâneo, ficando a conta bloqueada pelo utilizador que a está a usar. O processo

para desbloquear a conta pode ser definido na *Master Policy* da solução PAM, pelo que pode ser um processo manual ou automático conforme as políticas definidas (CyberArk, 2023b).

A gestão de sessões é outra das características em análise neste estudo. O componente Privileged Session Manager permite às organizações proteger, controlar e monitorizar o acesso privilegiado (CyberArk, 2023h). O PSM permite iniciar sessões de forma automática injetando as credenciais nas máquinas alvo, sendo capaz de monitorizar e registar sessões privilegiadas. Este componente permite assim gravar as sessões em formato de vídeo e armazena-las no Vault (CyberArk, 2023i). Para além do formato de vídeo, o PSM regista também em formato de texto, capturando, por exemplo, comandos executados em bases de dados, fornece um registo completo de todas as teclas digitais durante uma conexão SSH, sendo estas informações úteis para eventuais auditorias. A CyberArk providencia também a monitorização de sessões em tempo real, permitindo que utilizadores autorizados supervisionem as sessões, sendo capazes de interagir com a sessão e executar tarefas como, por exemplo, encerrar a sessão alvo (CyberArk, 2023g). O Vault armazena assim cada pedido de credenciais efetuado, assim como as gravações de sessões privilegiadas. No caso das sessões privilegiadas, o sistema guarda a informação do utilizador que acedeu à conta, a duração da sessão, o ID do servidor PSM utilizado, o ID da sessão, o endereço do dispositivo alvo e o protocolo utilizado para estabelecer a conexão (CyberArk, 2023d).

Deste modo, fazendo o paralelismo da componente teórica com a prática, constata-se que os componentes de conexão permitem que o utilizador final aceda automaticamente ao recurso privilegiado sem saber a respetiva palavra-passe. O componente de conexão faz uso do servidor PSM que serve como *proxy* e é capaz de isolar, monitorizar e controlar as sessões remotas durante o acesso privilegiado. O isolamento de sessão significa que a estação de trabalho do utilizador final é isolada da máquina remota, isto garante que as ações realizadas durante a sessão remota não afetem a máquina alvo, minimizando o risco de comprometimento do sistema e protegendo contra movimentos laterais e verticais, abuso e elevação de privilégios, tal como abordado na cadeia de ataque da CyberArk. A monitorização de sessões permite registar os detalhes das sessões privilegiadas como o registo de atividades, comandos executados e outros eventos relevantes. Este ponto insere-se na garantia de conformidade, tópico também abordado na revisão da literatura, pois fornece informações detalhadas dos eventos ocorridos. No desenvolvimento prático do estudo, o componente de conexão desenvolvido deu uma visão ampla sobre as funcionalidades da monitorização, nomeadamente, a gravação da sessão em formato de vídeo, entre outras funcionalidades citadas anteriormente. O controlo de sessões permite que os administradores de soluções PAM monitorizem e controlem as sessões privilegiadas em tempo real, com a possibilidade de poderem encerrar ou bloquear sessões com atividades suspeitas, definir tempo

limite de sessões, ativar o modo de pedido de acesso de sessões, entre outros benefícios. Deste modo, fica demonstrada a pertinência deste tipo de soluções para as organizações que lidam com identidades privilegiadas, ficando estes mesmos registos disponíveis para consulta futura caso necessário, seja por motivos de auditoria ou análise forense.

De acordo com a revisão da literatura, as contas privilegiadas são contas com capacidade de mudar ou impactar um serviço operacional, pelo que com o crescimento das organizações e a adoção de mais tecnologias dificulta a gestão de credenciais e a proteção dos seus ativos. Neste sentido, os CPM *plugins*, inclusive o *plugin* desenvolvido para este estudo, visam auxiliar as organizações na complexidade de gerir credenciais privilegiadas. Os CPM *plugins* suportam uma variedade de sistemas e aplicações e são projetados para gerir este tipo de contas. Os *plugins* têm como funcionalidades realizar as operações de verificação, alteração e reconciliação das palavras-passe. Tal como verificado, a solução PAM da CyberArk possui um cofre digital capaz de gerir e armazenar as credenciais integradas nesta solução, como palavras-passe e chaves SSH, de forma centralizada, automática e segura, permitindo obter um inventário completo das contas geridas.

A CyberArk possui também o sistema de Dual Control, isto significa que o utilizador final deverá solicitar um pedido de aprovação para realizar o acesso remoto elevando, desta forma, a segurança dos acessos. Assim como demonstrado em figuras anteriores, o PrivateArk, assim como o PVWA, fornece visibilidade sobre as atividades que decorreram ou estão a decorrer sob os sistemas PAM, indicando qual foi o *safe* acedido, quem acedeu, em que momento acedeu e quais as operações que realizou. Para além disso, regista também as operações que falharam como, por exemplo, as sessões onde não foi possível estabelecer a conexão com o PSM ou alertas sobre a falha de alterações de credenciais. A figura 27 demonstra as capacidades de monitorização do *software* da CyberArk, permitindo analisar várias atividades, como por exemplo, a sessão privilegiada iniciada e a respetiva justificação ou razão (“Teste de sessão”).

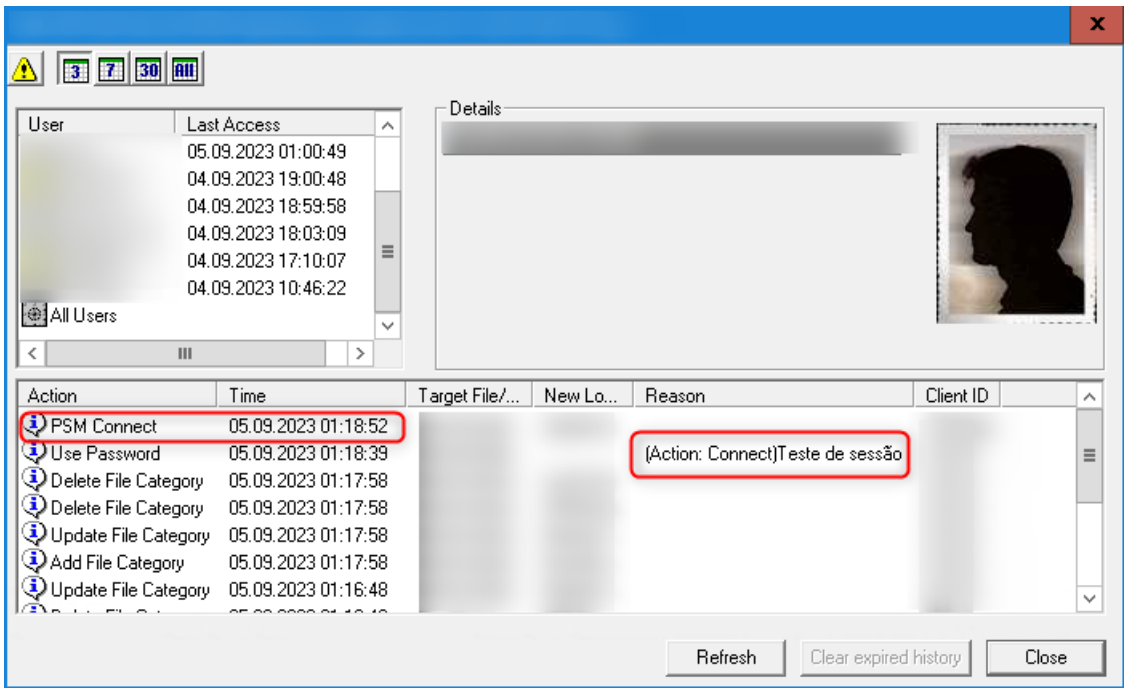


Figura 27 - PrivateArk registo de atividades

Em suma, a solução PAM da CyberArk através dos CPM *plugins* fornece às organizações o fortalecimento da segurança das contas privilegiadas, consequência da gestão centralizada e automática de credenciais e das políticas de palavras-passe que podem ser definidas pelas organizações, assim como auxilia nos processos de auditoria e conformidade que as mesmas pretendem alcançar. Por sua vez, as funcionalidades dos componentes de conexão podem também desempenhar um papel crucial para as organizações, pois cumprem a missão de isolar, monitorizar e controlar sessões remotas privilegiadas em tempo real, protegendo contra atores maliciosos internos e externos, auxiliando a mitigar possíveis riscos.

Assim, conclui-se que a revisão da literatura está estritamente ligada com os resultados obtidos no desenvolvimento prático do estudo, demonstrando a pertinência do uso de soluções PAM, como a da CyberArk, por parte das organizações, pois permitem efetuar a gestão centralizada de contas privilegiadas, isolamento e controlo de sessões, justificação da sessão, monitorização e registos em tempo real, ente outros benefícios.

7. Contributos e limitações do estudo

O presente estudo contribuiu para uma compreensão aprofundada da área de Gestão de Acesso Privilegiado, apresentando o estado da arte, fluxo de funcionamento de uma solução PAM, benefícios e desafios, bem como aspetos a considerar referentes ao acesso remoto. Posterior a esta

informação, foi apresentada a arquitetura da solução PAM da CyberArk e respetivos componentes. Foi possível demonstrar os desenvolvimentos efetuados, como os componentes de conexão e os CPM *plugins* e como estes garantem que as sessões remotas e a gestão de credenciais se tornem mais seguras respetivamente.

Este estudo teve como limitação o facto de apenas estar disponível licenças comerciais para a solução PAM da CyberArk, às quais não foi possível obter o acesso para uso pessoal e académico. Esta limitação refletiu-se na arquitetura do projeto, pois a arquitetura utilizada está assente numa infraestrutura organizacional real, pelo que o acesso a alguns componentes foi limitado ou impossível de realizar. O componente Privileged Threat Analytics foi um dos componentes que não foi possível testar, este tem o objetivo de monitorizar continuamente a utilização das contas privilegiadas e fornece uma camada de segurança adicional. O PTA é capaz de detetar e conter atividades não autorizadas realizadas através de contas privilegiadas, contendo ciberataques em curso. Este componente, através de algoritmos estatísticos, gera perfis de atividades e permite estabelecer comportamentos padrão por parte do utilizador que usa contas privilegiadas, conseguindo, em tempo real, diferenciar atividades regularmente realizadas de atividades não regulares, o que pode significar desvios ao nível do comportamento o que indica que a conta terá sido comprometida, sendo classificados como incidentes de segurança, emitindo alertas. O PTA permite analisar em tempo real o tráfego da rede, os eventos do Vault, eventos de máquinas Windows e Linux, recebe dados do Active Directory, e encaminha esses dados para sistemas de Gestão de Eventos e Informações de Segurança ou envia notificações por e-mail.

8. Conclusões

O presente estudo teve como objetivo apresentar uma visão abrangente sobre os principais contributos da área de Gestão de Acesso Privilegiado, dando enfase à solução PAM da CyberArk, com destaque para os principais componentes que constituem a arquitetura desta solução. Foi explorado como é que os principais componentes da CyberArk interagem entre si, fornecendo uma solução robusta para a gestão de sessões e credenciais privilegiadas.

Inicialmente, foi abordado o estado da arte da segurança da informação e cibersegurança com ênfase na gestão de identidades. O estudo demonstrou a pertinência da implementação de PAM por parte das organizações e como esta área assume cada vez mais destaque na proteção e gestão de contas privilegiadas, sendo esta uma prioridade para as organizações. A literatura refere que as contas privilegiadas são alvo constante dos atores maliciosos internos e externos com o objetivo de comprometer os sistemas organizacionais. Através de várias técnicas como, por exemplo,

engenharia social, estes atores maliciosos procuram roubar credenciais privilegiadas e movimentarem-se lateralmente e verticalmente dentro das infraestruturas organizacionais para conseguirem escalar privilégios, obterem acesso a sistemas e informações críticas, distribuição de *malware*, interrupção dos sistemas, assim como danos financeiros e reputacionais. A revisão teórica refere a necessidade de implementar soluções PAM nas organizações, pois garantem a proteção das contas privilegiadas e mitigação dos riscos associados. Foi também apresentado o fluxo de funcionamento de soluções PAM e como estas efetuam a gestão centralizada de contas privilegiadas, através de políticas de acesso, autenticação e autorização. O acesso remoto foi outro dos tópicos abordados, com foco em sessões RDP e SSH, pelo que a solução da CyberArk fornece recursos que garantem a autenticação segura e a gestão de acesso privilegiado em diferentes cenários. Constatou-se que a introdução de PAM, permite um maior controlo sob o acesso remoto devido ao registo detalhado de atividades e isolamento de sessões, capaz de proteger contas privilegiadas em sessões remotas. Foram abordados os benefícios das soluções PAM e como estas permitem proteger sistemas críticos e dados sensíveis, reduzir riscos de violações de segurança, assim como mitigar ameaças internas e externas. A literatura refere a capacidade deste tipo de soluções de monitorizar e verificar o registo de atividades em ambientes privilegiados. Refere que o PAM limita a superfície de ataque através da limitação dos privilégios dos utilizadores, processos e aplicações protegendo contra ameaças internas e externas. Estas soluções auxiliam as organizações a atingir a conformidade regulatória, proteção de credenciais num cofre digital, capaz de as guardar e gerir de forma segura, definir fluxos de trabalho de acessos aos dispositivos tendo em consideração o processo de aprovação para permitir o acesso remoto quando necessário. Para além disto, e entre outros benefícios enumerados na revisão da literatura, estas soluções de gestão de acesso privilegiado permitem gravar as sessões remotas e rever as ações efetuadas nas aplicações, dispositivos ou sistemas. Assim sendo, a monitorização e a auditoria foram pontos realçados ao longo do estudo, pois ajudam a garantir a conformidade de acordo com legislações, regulamentações e importantes padrões de cibersegurança, bem como na deteção de potenciais ameaças.

Quanto aos desenvolvimentos efetuados, nomeadamente, os componentes de conexão e os CPM *plugins*, seguido da respetiva integração com a solução da CyberArk, foi discutida a sua importância e como é que estes componentes permitem a integração com diferentes sistemas, aplicações e dispositivos. O desenvolvimento do componente de conexão demonstra a função fundamental que este representa para uma solução PAM. O componente de conexão utiliza o servidor PSM, este age como um *proxy*, e permite que a solução da CyberArk interaja com uma variedade de sistemas estabelecendo uma comunicação segura, isolada, com encriptação dos dados,

e monitorização e registo de atividades em tempo real. O CPM *plugin* desenvolvido, permite a rotação de credenciais privilegiadas para o dispositivo remoto alvo, com a possibilidade de efetuar as operações de verificação, alteração e reconciliação da palavra-passe. Os CPM *plugins* integrados na solução da CyberArk, com recurso do servidor CPM, auxiliam as organizações na gestão automática de credenciais de acordo com as políticas estabelecidas pelas organizações. Contudo, e apesar dos vastos benefícios enumerados sobre PAM para as organizações, este estudo expôs os desafios associados a esta área, como por exemplo, a consciencialização e formação dos funcionários, tema bastante pertinente na área de TI e fulcral quando se lida com contas, sistemas e dados críticos e sensíveis.

Por fim, conclui-se que a revisão teórica está diretamente relacionada com os resultados alcançados durante o desenvolvimento prático, destacando a importância da adoção de soluções PAM, como a da CyberArk, pelas organizações. Estas soluções auxiliam assim na implementação de políticas de segurança, políticas de complexidade de palavras-passe, gestão de contas privilegiadas, acesso controlado de acordo com as funções dos utilizadores, armazenamento de informações centralizado e seguro, auditoria e monitorização das atividades.

Referências bibliográficas

A. Grishaeva, S., & I. Borzov, V. (2020). Information security risk management. *International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*. https://doi.org/10.1109/ITQMIS51053.2020.9322901

Abukari, A. M., & Bankas, E. K. (2020). Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond. *International Journal of Scientific & Engineering Research*, *11*(4). https://www.researchgate.net/publication/341098664_Some_Cyber_Security_Hygienic_Protocols_For_Teleworkers_In_Covid-19_Pandemic_Period_And_Beyond

Ali, M. A., Azad, M. A., Parreno Centeno, M., Hao, F., & van Moorsel, A. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems*, *100*, 408–427. https://doi.org/10.1016/j.future.2019.03.041

Ali, M. I., Kaur, S., Khamparia, A., Gupta, D., Kumar, S., Khanna, A., & Al-Turjman, F. (2020). Security Challenges and Cyber Forensic Ecosystem in IoT Driven BYOD Environment. *IEEE Access*, *8*, 172770–172782. https://doi.org/10.1109/ACCESS.2020.3024784

Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. *IEEE Access*, *10*, 132132–132143. https://doi.org/10.1109/ACCESS.2022.3230286

Alkhudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019). Information Security:A Review of Information Security Issues and Techniques. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 1–6. https://doi.org/10.1109/CAIS.2019.8769504

Alruwies, M., Mishra, S., & Abdul, M. (2021). Identity Governance Framework for Privileged Users. *Computer Systems Science and Engineering*, *40*(3), Artigo 3. https://doi.org/10.32604/csse.2022.019355

Alsowail, R. A., & Al-Shehari, T. (2020). Empirical Detection Techniques of Insider Threat Incidents. *IEEE Access*, *8*, 78385–78402. https://doi.org/10.1109/ACCESS.2020.2989739

Asllani, A., Lari, A., & Lari, N. (2018). Strengthening information technology security through the failure modes and effects analysis approach. *International Journal of Quality Innovation*, *4*(1), 5. https://doi.org/10.1186/s40887-018-0025-1

Australian Cyber Security Centre. (2022). *Technical example: Restrict administrative privileges*. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/small-business-cyber-security/small-business-cloud-security-guide/technical-example-restrict-administrative-privileges

Ayisi Nyarko, D., & Kozári, J. (2021). Information and communication technologies (ICTs) usage among agricultural extension officers and its impact on extension delivery in Ghana. *Journal of the Saudi Society of Agricultural Sciences*, *20*(3), 164–172. https://doi.org/10.1016/j.jssas.2021.01.002

Badsha, S., Vakilinia, I., & Sengupta, S. (2019). Privacy Preserving Cyber Threat Information Sharing and Learning for Cyber Defense. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 0708–0714. https://doi.org/10.1109/CCWC.2019.8666477

Battaglioni, M., Rafaiani, G., Chiaraluce, F., & Baldi, M. (2022). MAGIC: A Method for Assessing Cyber Incidents Occurrence. *IEEE Access*, *10*, 73458–73473. https://doi.org/10.1109/ACCESS.2022.3189777

Baybulatov, A. A., & Promyslov, V. G. (2020). Cybersecurity Assessment Using Delay from Backlog Bound Calculation. *2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT)*, 1–6. https://doi.org/10.1109/AICT50176.2020.9368731

BeyondTrust. (2022). *What is Privileged Access Management (PAM)?* https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam

Bhardwaj, G., Gupta, R., Pratap Srivastava, A., & Vikram Singh, S. (2021). Cyber Threat Landscape of G4 Nations: Analysis of Threat Incidents & Response Strategies. *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, 75–79. https://doi.org/10.1109/ICIEM51511.2021.9445307

Bogoda, L., Mo, J., & Bil, C. (2019). A Systems Engineering Approach To Appraise Cybersecurity Risks Of CNS/ATM and Avionics Systems. *2019 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, 1–15. https://doi.org/10.1109/ICNSURV.2019.8735376

Burnis, A. (2017). *7 Types of Privileged Accounts: Service Accounts and More*. https://www.cyberark.com/resources/blog/7-types-of-privileged-accounts-service-accounts-and-more

Cannard, M. (2021). *What Is Privileged Access Management (PAM)?* https://blog.netwrix.com/2021/07/02/privileged-access-management/

Carson, J. (2021). *The 7 Deadly Privileged Accounts You MUST Discover, Manage, and Secure*. Delinea. https://delinea.com/blog/top-7-types-of-privileged-accounts-to-protect

Carson, J. (2022a). *Privileged Access Management (PAM)*. https://delinea.com/what-is/privileged-access-management-pam

Carson, J. (2022b). *RDP Security: How to secure Remote Desktop Protocol*. Delinea. https://delinea.com/blog/rdp-security

Check Point. (2022a). *What is Privileged Access Management (PAM)?* Check Point Software. https://www.checkpoint.com/cyber-hub/what-is-privileged-access-management-pam/

Check Point. (2022b). *What is the Principle of Least Privilege (POLP)?* https://www.checkpoint.com/cyber-hub/network-security/what-is-the-principle-of-least-privilege-polp/

CyberArk. (2019). *The Three Phases of Securing Privileged Accounts: A Best Practices Guide*. https://www.cyberark.com/resources/white-papers/the-three-phases-of-securing-privileged-accounts-a-best-practices-guide

CyberArk. (2020a). CyberArk Delivers Blueprint for Privileged Access Management Success. *CyberArk*. https://www.cyberark.com/press/cyberark-delivers-blueprint-for-privileged-access-management-success/

CyberArk. (2020b). *Just-In-Time Access*. https://www.cyberark.com/what-is/just-in-time-access/

CyberArk. (2020c). *Privileged Access Management (PAM)*. https://www.cyberark.com/what-is/privileged-access-management/

CyberArk. (2021). *CyberArk Blueprint for Identity Security Success Whitepaper*. https://www.cyberark.com/resources/white-papers/cyberark-blueprint-for-identity-security-success-whitepaper

CyberArk. (2022a). *2022 Gartner® Magic Quadrant™ for Privileged Access Management*. https://www.cyberark.com/resources/analyst-reports/2022-gartner-magic-quadrant-for-privileged-access-management

CyberArk. (2022b). *Understanding the Identity Attack Chain with the CyberArk Blueprint*. https://cyberark-customers.force.com/s/article/Understanding-the-Identity-Attack-Chain-with-the-CyberArk-Blueprint

CyberArk. (2023a). *Digital Vault Security Requirements*. https://docs.cyberark.com/PAS/12.2/en/Content/Security/CyberArk-DV-Server-Security-Standards-Requirements.htm

CyberArk. (2023b). *Privileged Access Manager—Self-Hosted Account check-out and check-in*. https://docs.cyberark.com/PAS/12.2/en/Content/PASIMP/Accounts-Check-out-and-Check-in.htm

CyberArk. (2023c). *Privileged Access Manager—Self-Hosted Architecture*. https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.2/en/Content/PASIMP/Privileged-Account-Security-Solution-Architecture.htm

CyberArk. (2023d). *Privileged Access Manager—Self-Hosted Audits*. https://docs.cyberark.com/PAS/Latest/en/Content/PASIMP/Auditing-in-PSM.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7C_____8

CyberArk. (2023e). *Privileged Access Manager—Self-Hosted Change Password*. https://docs.cyberark.com/PAS/12.2/en/Content/NewUI/NewUI-Change-credentials.htm

CyberArk. (2023f). *Privileged Access Manager—Self-Hosted Introduction*. https://docs.cyberark.com/PAS/12.2/en/Content/PASIMP/Introducing-the-Privileged-Account-Security-Solution-Intro.htm

CyberArk. (2023g). *Privileged Access Manager—Self-Hosted Monitor Privileged Sessions*. https://docs.cyberark.com/PAS/12.2/en/Content/PASIMP/Monitoring-Privileged-Sessions.htm

CyberArk. (2023h). *Privileged Access Manager—Self-Hosted Privileged Session Manager*. https://docs.cyberark.com/PAS/12.2/en/Content/PASIMP/Privileged-Session%20Manager-Introduction.htm

CyberArk. (2023i). *Privileged Access Manager—Self-Hosted Privileged Session Manager*. https://docs.cyberark.com/PAS/12.2/en/Content/PAS%20SysReq/System%20Requirements%20-%20PSM.htm

CyberArk. (2023j). *Privileged Access Manager—Self-Hosted Version 10 Interface*. https://docs.cyberark.com/PAS/12.2/en/Content/Landing%20Pages/LPVersion10Interface.htm?TocPath=End%20User|Privileged%20Accounts|Version%2010%20Interface|_____0

Cybersecurity and Infrastructure Security Agency. (2020). *Insider Threat Mitigation Guide*. https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide

Cybrary. (2021). *What Is Privilege Access Management?* https://www.cybrary.it/blog/what-is-privilege-access-management/

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques*, *15*(4), 277–305. https://doi.org/10.1007/s11416-019-00338-7

Duro, R. (2021). *Ataques em cadeia: O que sabemos sobre o ataque à SolarWinds e o porquê da sua importância*. IT Insight. https://www.itinsight.pt/news/opiniao/ataques-em-cadeia-o-que-sabemos-sobre-o-ataque-a-solarwinds-e-o-porque-da-sua-importancia

ENISA. (2023). *ENISA Foresight Cybersecurity Threats for 2030*. https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

Esposito, B. (2023). *Staying ahead of Privileged Access Management security risks: Success strategies*. https://www.oneidentity.com/community/blogs/b/privileged-access-management/posts/staying-ahead-of-privileged-access-management-security-risks-success-strategies

Falowo, O. I., Popoola, S., Riep, J., Adewopo, V. A., & Koch, J. (2022). Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents. *IEEE Access*, *10*, 134038–134051. https://doi.org/10.1109/ACCESS.2022.3231847

Gartner. (2022). *Magic Quadrant for Privileged Access Management*. https://www.gartner.com/doc/reprints?id=1-2AMZ88JO&ct=220721&st=sb

Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. *Big Data Analytics*, *1*(1), 6. https://doi.org/10.1186/s41044-016-0006-0

Haber, M. J. (2020). *Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations*. Apress. https://doi.org/10.1007/978-1-4842-5914-6

Haber, M. J., & Hibbert, B. (2018). Industrial Control Systems (ICS). Em M. J. Haber & B. Hibbert (Eds.), *Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations* (pp. 131–137). Apress. https://doi.org/10.1007/978-1-4842-3048-0_13

Haber, M. J., & Rolls, D. (2020). Privileged Access Management. Em M. J. Haber & D. Rolls (Eds.), *Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution* (pp. 137–150). Apress. https://doi.org/10.1007/978-1-4842-5165-2_13

Hensley, B. (2021). Identity is the new perimeter in the fight against supply chain attacks. *Network Security*, *2021*(7), 7–9. https://doi.org/10.1016/S1353-4858(21)00074-X

Hoesl, R., Metz, M., Dold, J., & Hartung, S. (2017). *Capability Framework for Privileged Access Management*. https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/capability-framework-for-privileged-access-management

Jayabalan, M. (2020). Towards an Approach of Risk Analysis in Access Control. *2020 13th International Conference on Developments in eSystems Engineering (DeSE)*, 287–292. https://doi.org/10.1109/DeSE51703.2020.9450772

Jin, X., Cui, B., Yang, J., & Cheng, Z. (2018). An Adaptive Analysis Framework for Correlating Cyber-Security-Related Data. *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, 915–919. https://doi.org/10.1109/AINA.2018.00134

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of Security Threats in Information Systems. *Procedia Computer Science*, *32*, 489–496. https://doi.org/10.1016/j.procs.2014.05.452

Karabatak, M., & Mustafa, T. (2018). Performance comparison of classifiers on reduced phishing website dataset. *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, 1–5. https://doi.org/10.1109/ISDFS.2018.8355357

Karim, N. A., Kaur, J., & Khalib, M. N. (2021). Benefit vs Cost:Examining Factors of Intention to Comply Information Security Policy. *2021 IEEE International Conference on Computing (ICOCO)*, 291–296. https://doi.org/10.1109/ICOCO53166.2021.9673542

Kemp, T. (2018). *What Tesla's Spygate Teaches Us About Insider Threats*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2018/07/19/what-teslas-spygate-teaches-us-about-insider-threats/

Khaliq, S., Abideen Tariq, Z. U., & Masood, A. (2020). Role of User and Entity Behavior Analytics in Detecting Insider Attacks. *2020 International Conference on Cyber Warfare and Security (ICCWS)*, 1–6. https://doi.org/10.1109/ICCWS48432.2020.9292394

Khan, A. W., Zaib, S., Khan, F., Tarimer, I., Seo, J. T., & Shin, J. (2022). Analyzing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach. *IEEE Access*, *10*, 65044–65054. https://doi.org/10.1109/ACCESS.2022.3179822

Kirilchuk, S., Reutov, V., Nalivaychenko, E., Shevchenko, E., & Yaroshenko, A. (2022). Ensuring the security of an automated information system in a regional innovation cluster. *Transportation Research Procedia*, *63*, 607–617. https://doi.org/10.1016/j.trpro.2022.06.054

Koppisetty, H., Potdar, K., & Jain, S. (2019). Cyber-crime, Forensics and use of Data Mining in Cyber Space: A Survey. *2019 International Conference on Smart Systems and Inventive (ICSSIT)*, 722–727. https://doi.org/10.1109/ICSSIT46314.2019.8987921

Krishnan, M., & Egambaram, L. (2020). PAM: Process authentication mechanism for protecting system services against malicious code attacks. *Sādhanā*, *45*(1), 141. https://doi.org/10.1007/s12046-020-01381-7

Lazarovitz, L. (2021). Deconstructing the SolarWinds breach. *Computer Fraud & Security*, *2021*(6), 17–19. https://doi.org/10.1016/S1361-3723(21)00065-8

Le, D. C., & Zincir-Heywood, N. (2021). Anomaly Detection for Insider Threats Using Unsupervised Ensembles. *IEEE Transactions on Network and Service Management*, *18*(2), 1152–1164. https://doi.org/10.1109/TNSM.2021.3071928

Lewis, S. (2021). *Privileged access management (PAM)*. https://www.techtarget.com/searchsecurity/definition/privileged-access-management-PAM

Liu, L., Chen, C., Zhang, J., De Vel, O., & Xiang, Y. (2019). Insider Threat Identification Using the Simultaneous Neural Learning of Multi-Source Logs. *IEEE Access*, *7*, 183162–183176. https://doi.org/10.1109/ACCESS.2019.2957055

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*(1), 10. https://doi.org/10.1186/s42400-020-00050-w

Macak, M., Vanát, I., Merjavý, M., Jevočin, T., & Buhnova, B. (2020). Towards Process Mining Utilization in Insider Threat Detection from Audit Logs. *2020 Seventh International Conference on Social Networks Analysis, Management and Security (SNAMS)*, 1–6. https://doi.org/10.1109/SNAMS52053.2020.9336573

Mallikarajunan, K. M. E. N., Preethi, S. R., Selvalakshmi, S., & Nithish, N. (2019). Detection of Spyware in Software Using Virtual Environment. *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, 1138–1142. https://doi.org/10.1109/ICOEI.2019.8862547

Mavroeidis, V., Hohimer, R., Casey, T., & Jesang, A. (2021). Threat Actor Type Inference and Characterization within Cyber Threat Intelligence. *2021 13th International Conference on Cyber Conflict (CyCon)*, 327–352. https://doi.org/10.23919/CyCon51939.2021.9468305

McCarthy, M. (2023). *What is PAM Security? Privileged Access Management Explained*. https://www.strongdm.com/privileged-access-management

Micro Focus. (2023). *What is an Insider Threat?* https://www.microfocus.com/en-us/what-is/insider-threat

Microsoft. (2023). *Securing privileged access*. https://learn.microsoft.com/en-us/security/privileged-access-workstations/overview

Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers & Security*, *109*, 102383. https://doi.org/10.1016/j.cose.2021.102383

Mishra, A. A., Surve, K., Patidar, U., & Rambola, R. K. (2018). Effectiveness of Confidentiality, Integrity and Availability in the Security of Cloud Computing: A Review. *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, 1–5. https://doi.org/10.1109/CCAA.2018.8777537

Mnjama, J., Foster, G., & Irwin, B. (2017). A privacy and security threat assessment framework for consumer health wearables. *2017 Information Security for South Africa (ISSA)*, 66–73. https://doi.org/10.1109/ISSA.2017.8251776

Mohammed, A.-M., Idris, B., Saridakis, G., & Benson, V. (2020). Chapter 8 - Information and communication technologies: A curse or blessing for SMEs? Em V. Benson & J. Mcalaney (Eds.), *Emerging Cyber Threats and Cognitive Vulnerabilities* (pp. 163–174). Academic Press. https://doi.org/10.1016/B978-0-12-816203-3.00008-3

Monev, V. (2020). Defining and Applying Information Security Goals for Blockchain Technology. *2020 International Conference on Information Technologies (InfoTech)*, 1–4. https://doi.org/10.1109/InfoTech49733.2020.9211073

Morris, C. (2018). *Why Banks Need Privileged Access Management to Secure Their Systems*. https://biztechmagazine.com/article/2018/01/why-banks-need-privileged-access-management-secure-their-systems

Moses, S., & Rowe, D. C. (2015). The SNAP principle for mitigating privileged account breaches: How secondary non-admin privileged accounts can reduce breach impact. *2015 World Congress on Internet Security (WorldCIS)*, 32–38. https://doi.org/10.1109/WorldCIS.2015.7359408

National Cyber Security Centre. (2020). *Use privileged access management*. https://www.ncsc.gov.uk/collection/secure-system-administration/use-privileged-access-management

National Institute of Standards and Technology. (2002). *Security Requirements for Cryptographic Modules* (Federal Information Processing Standard (FIPS) 140-2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.140-2

Northern Ireland Security Centre. (2020). *Cyber Threats*. NI Cyber Security Centre. https://www.nicybersecuritycentre.gov.uk/cyber-threats

Oladimeji, S., & Kerner, S. (2023). *SolarWinds hack explained: Everything you need to know*. TechTarget. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Otta, S. P., Panda, S., Gupta, M., & Hota, C. (2023). A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure. *Future Internet*, *15*(4), Artigo 4. https://doi.org/10.3390/fi15040146

Panek, C. (2020). Understanding security layers. Em *Security Fundamentals* (pp. 1–31). Wiley. https://doi.org/10.1002/9781119650737.ch1

Poremba, S. (2022). *What are insider threats? Definition, types, and how to mitigate them*. https://enterprise.verizon.com/resources/articles/s/the-risk-of-insider-threat-actors/

Prabowo, H., Shihab, M. R., & Aji, R. F. (2018). Practical Implementation Of Information Security Management In The Energy Sector Insights From An Oil And Gas Organization In Indonesia. *2018 International Workshop on Big Data and Information Security (IWBIS)*, 159–163. https://doi.org/10.1109/IWBIS.2018.8471716

Purba, A., & Soetomo, M. (2019). Assessing Privileged Access Management (PAM) using ISO 27001:2013 Control. *ACMIT Proceedings*, *5*(1), 65–76. https://doi.org/10.33555/acmit.v5i1.76

Rahman, M. M. H., Naeem, M. A. A., & Abubakar, A. (2022). Threats From Unintentional Insiders: An Assessment of an Organization's Readiness Using Machine Learning. *IEEE Access*, *10*, 110294–110308. https://doi.org/10.1109/ACCESS.2022.3214819

Ramaseshan, S. (2018). *Effective Interactive Privileged Access Review*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2018/volume-5/effective-interactive-privileged-access-review

Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures. *2014 Information Security for South Africa*, 1–7. https://doi.org/10.1109/ISSA.2014.6950492

Rohith, C., & Batth, R. S. (2019). Cyber Warfare: Nations Cyber Conflicts, Cyber Cold War Between Nations and its Repercussion. *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, 640–645. https://doi.org/10.1109/ICCIKE47802.2019.9004236

Sajal, S. Z., Jahan, I., & Nygard, K. E. (2019). A Survey on Cyber Security Threats and Challenges in Modern Society. *2019 IEEE International Conference on Electro Information Technology (EIT)*, 525–528. https://doi.org/10.1109/EIT.2019.8833829

Santos, H., Pereira, T., & Mendes, I. (2017). Challenges and reflections in designing Cyber security curriculum. *2017 IEEE World Engineering Education Conference (EDUNINE)*, 47–51. https://doi.org/10.1109/EDUNINE.2017.7918179

Sayed, M. A., Atallah, R., Assi, C., & Debbabi, M. (2022). Electric vehicle attack impact on power grid operation. *International Journal of Electrical Power & Energy Systems*, *137*, 107784. https://doi.org/10.1016/j.ijepes.2021.107784

Schoenherr, J. R., & Thomson, R. (2020). Insider Threat Detection: A Solution in Search of a Problem. *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1–7. https://doi.org/10.1109/CyberSecurity49315.2020.9138862

Senhasegura. (2022). *Privileged Access Management (Pam): A Complete Guide*. https://senhasegura.com/privileged-access-management-pam-a-complete-guide/

Shacklett, M., & Rosencrance, L. (2021). *Authentication*. https://www.techtarget.com/searchsecurity/definition/authentication

Sharma, A., Sharma, S., & Dave, M. (2015). Identity and access management- a comprehensive study. *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 1481–1485. https://doi.org/10.1109/ICGCIoT.2015.7380701

Simister, A. (2022). *What is Privileged Access Management?* https://www.lepide.com/blog/what-is-privileged-access-management/

Sindiren, E., & Ciylan, B. (2018). *Privileged Account Management Approach for Preventing Insider Attacks*.

Singh, K. P., Rishiwal, V., & Kumar, P. (2018). Classification of Data to Enhance Data Security in Cloud Computing. *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 1–5. https://doi.org/10.1109/IoT-SIU.2018.8519934

Sohime, F. H., Ramli, R., Rahim, F. A., & Bakar, A. A. (2020). Exploration Study of Skillsets Needed in Cyber Security Field. *2020 8th International Conference on Information Technology and Multimedia (ICIMU)*, 68–72. https://doi.org/10.1109/ICIMU49871.2020.9243448

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Souppaya, M., Stine, K., Simos, M., Sweeney, S., & Scarfone, K. (2020). *Critical Cybersecurity Hygiene: Patching the Enterprise* (pp. 15–15). National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/white-paper/2020/03/30/critical-cybersecurity-hygiene-patching-the-enterprise/final

Starodubtsev, Yu. I., Balenko, E. G., Vershennik, E. V., & Fedorov, V. H. (2020). Cyberspace: Terminology, Properties, Problems of Operation. *2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, 1–3. https://doi.org/10.1109/FarEastCon50210.2020.9271282

Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia Computer Science*, *215*, 483–487. https://doi.org/10.1016/j.procs.2022.12.050

Tep, K. S., Martini, B., Hunt, R., & Choo, K.-K. R. (2015). A Taxonomy of Cloud Attack Consequences and Mitigation Strategies: The Role of Access Control and Privileged Access Management. *2015 IEEE Trustcom/BigDataSE/ISPA*, *1*, 1073–1080. https://doi.org/10.1109/Trustcom.2015.485

Tervoort, T., De Oliveira, M. T., Pieters, W., Van Gelder, P., Olabarriaga, S. D., & Marquering, H. (2020). Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review. *IEEE Access*, *8*, 84352–84361. https://doi.org/10.1109/ACCESS.2020.2984376

Tirtadjaja, W., Rana, M. E., & Shanmugam, K. (2021). Managing High Privileged Accounts in IT Enterprise: Enhanced Security Infrastructure. *2021 International Conference on Data Analytics for Business and Industry (ICDABI)*, 655–660. https://doi.org/10.1109/ICDABI53623.2021.9655847

Tsochev, G., & Stankov, I. (2020). A Study On Information Security Management. *2020 XXIX International Scientific Conference Electronics (ET)*, 1–4. https://doi.org/10.1109/ET50336.2020.9238331

Tsochev, G., Trifonov, R., Nakov, O., Manolov, S., & Pavlova, G. (2020). Cyber security: Threats and Challenges. *2020 International Conference Automatics and Informatics (ICAI)*, 1–6. https://doi.org/10.1109/ICAI50593.2020.9311369

Verizon. (2022). *DBIR - Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/2022-data-breach-investigations-report-dbir.pdf

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Walker, P. (2019). Why do PAM projects fail? *Network Security*, *2019*(9), 15–18. https://doi.org/10.1016/S1353-4858(19)30109-6

WALLIX. (2016). *What is Privileged Session Management?* https://www.wallix.com/blog/privileged-session-management/

Wang, R. (2018). *Privileged Account Management and Identity Access Management: Same Family, Different Strengths*. https://delinea.com/blog/privileged-account-management-and-identity-access-management-same-family-different-strengths

Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access*, *8*, 85094–85115. https://doi.org/10.1109/ACCESS.2020.2992807

Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management*, *52*, 102090. https://doi.org/10.1016/j.ijinfomgt.2020.102090

Weihe, H. (2022a). *8 Benefits of Privileged Access Management*. https://www.oneidentity.com/community/blogs/b/one-identity/posts/8-benefits-of-privileged-access-management

Weihe, H. (2022b). *Why is Privileged Access Management important?* https://www.oneidentity.com/community/blogs/b/one-identity/posts/why-is-privileged-access-management-important

Apêndices e/ou anexos

```
#AutoIt3Wrapper_UseX64=n
Opt("MustDeclareVars", 1)
AutoItSetOption("WinTitleMatchMode", 3) ; EXACT_MATCH!

;============================================================
;             PSM AutoIt Dispatcher Skeleton
;             ------------------------------
;
; Use this skeleton to create your own
; connection components integrated with the PSM.
; Areas you may want to modify are marked
; with the string "CHANGE_ME".
;
; Created : April 2013
; Cyber-Ark Software Ltd.
;============================================================
#include "PSMGenericClientWrapper.au3"

;====================================
; Consts & Globals
;====================================
Global Const $DISPATCHER_NAME                       = "Microsoft SQL Server" ; CHANGE_ME
Global Const $CLIENT_EXECUTABLE                     = "C:\Program Files (x86)\Microsoft SQL Server Management Studio 18\Common7\IDE\ssms.exe" ; CHANGE_ME
Global Const $ERROR_MESSAGE_TITLE                   = "PSM " & $DISPATCHER_NAME & " Dispatcher error message"
Global Const $LOG_MESSAGE_PREFIX                    = $DISPATCHER_NAME & " Dispatcher - "

Global $TargetUsername
Global $TargetPassword
Global $TargetAddress
Global $ConnectionClientPID = 0

;====================================
; Code
;====================================
Exit Main()

;====================================
; Main
;====================================
Func Main()

    ; Init PSM Dispatcher utils wrapper
    ToolTip ("Initializing...")
    if (PSMGenericClient_Init() <> $PSM_ERROR_SUCCESS) Then
        Error(PSMGenericClient_PSMGetLastErrorString())
    EndIf

    LogWrite("successfully initialized Dispatcher Utils Wrapper")

    ; Get the dispatcher parameters
    FetchSessionProperties()

    LogWrite("mapping local drives")
    if (PSMGenericClient_MapTSDrives() <> $PSM_ERROR_SUCCESS) Then
        Error(PSMGenericClient_PSMGetLastErrorString())
    EndIf

    LogWrite("starting client application")
    ToolTip ("Starting " & $DISPATCHER_NAME & "...")
```

Figura 28 - Componente de conexão: estrutura base em AutoIT

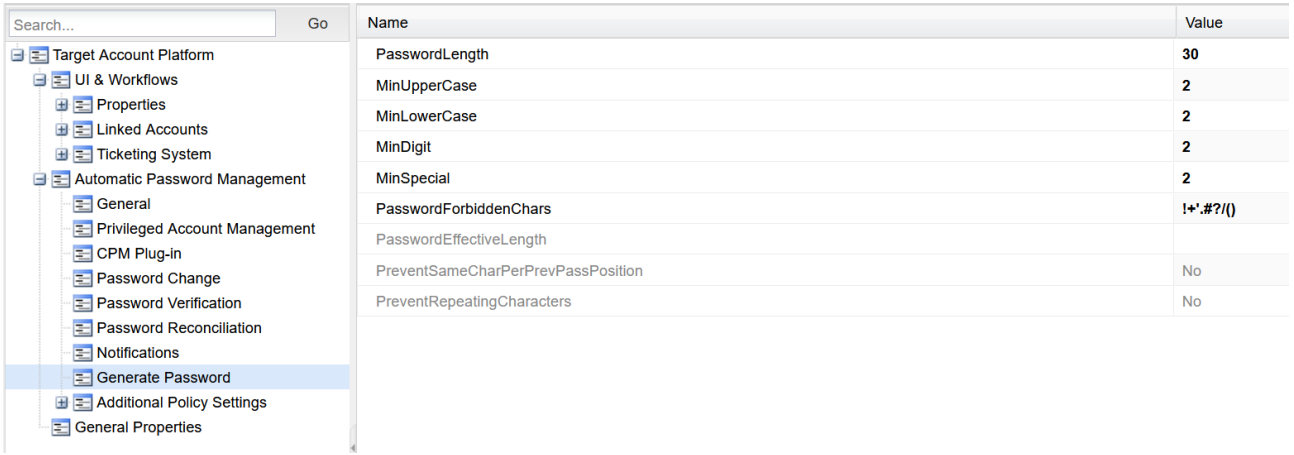
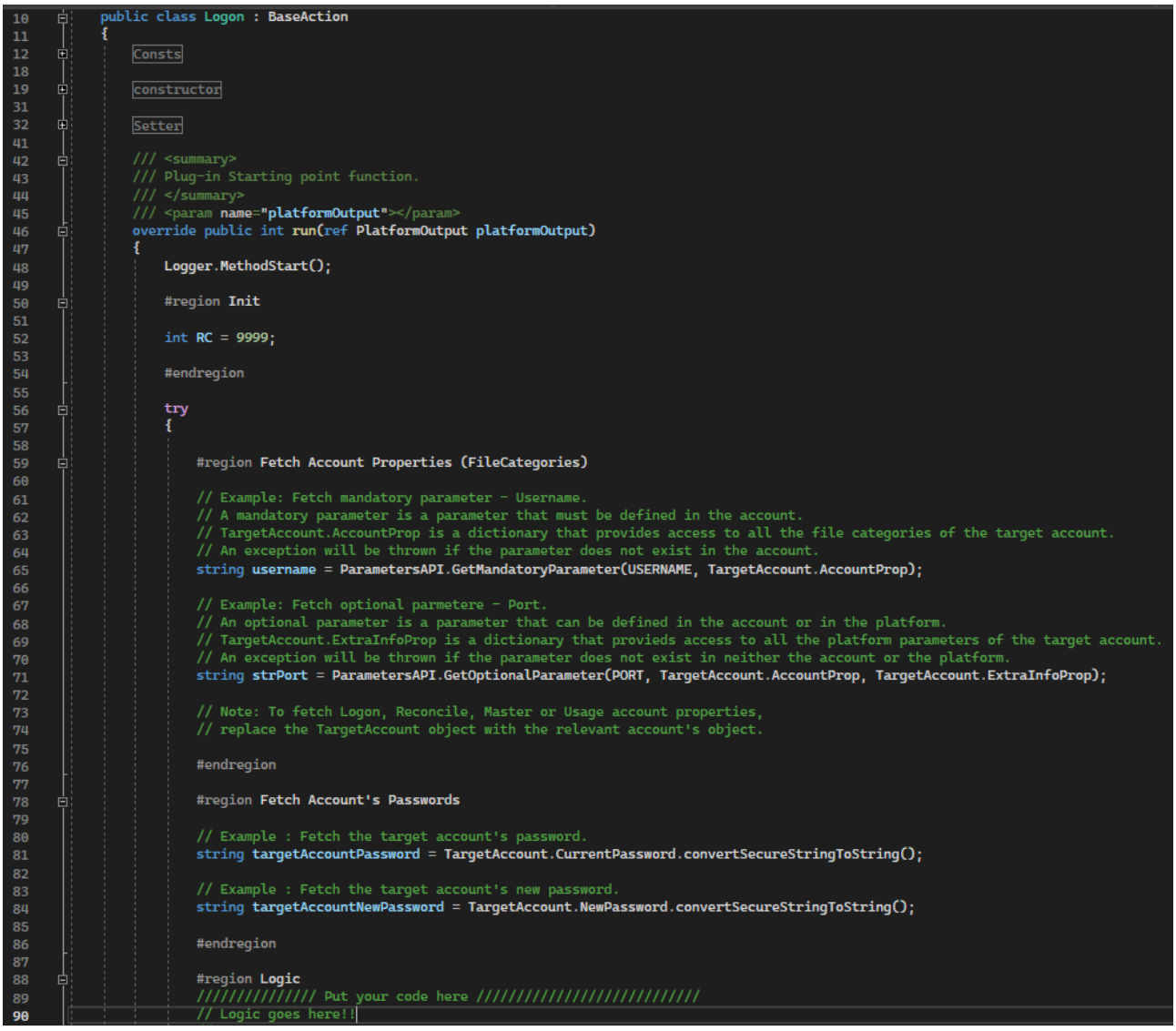


Figura 29 - CyberArk PVWA: CPM plugin, exemplo de política de definição de palavra-passe



```
public class Logon : BaseAction
{
    Consts

    constructor

    Setter

    /// <summary>
    /// Plug-in Starting point function.
    /// </summary>
    /// <param name="platformOutput"></param>
    override public int run(ref PlatformOutput platformOutput)
    {
        Logger.MethodStart();

        #region Init

        int RC = 9999;

        #endregion

        try
        {

            #region Fetch Account Properties (FileCategories)

            // Example: Fetch mandatory parameter - Username.
            // A mandatory parameter is a parameter that must be defined in the account.
            // TargetAccount.AccountProp is a dictionary that provides access to all the file categories of the target account.
            // An exception will be thrown if the parameter does not exist in the account.
            string username = ParametersAPI.GetMandatoryParameter(USERNAME, TargetAccount.AccountProp);

            // Example: Fetch optional parmetere - Port.
            // An optional parameter is a parameter that can be defined in the account or in the platform.
            // TargetAccount.ExtraInfoProp is a dictionary that provieds access to all the platform parameters of the target account.
            // An exception will be thrown if the parameter does not exist in neither the account or the platform.
            string strPort = ParametersAPI.GetOptionalParameter(PORT, TargetAccount.AccountProp, TargetAccount.ExtraInfoProp);

            // Note: To fetch Logon, Reconcile, Master or Usage account properties,
            // replace the TargetAccount object with the relevant account's object.

            #endregion

            #region Fetch Account's Passwords

            // Example : Fetch the target account's password.
            string targetAccountPassword = TargetAccount.CurrentPassword.convertSecureStringToString();

            // Example : Fetch the target account's new password.
            string targetAccountNewPassword = TargetAccount.NewPassword.convertSecureStringToString();

            #endregion

            #region Logic
            /////////////// Put your code here ////////////////////////
            // Logic goes here!!
```

Figura 30 - CPM plugin: estrutura base em .NET SDK