Journal of Technology & Information

Uma abordagem Sobre a Gestão e Tratamento de Eventos e Incidentes Utilizando o Microsoft Sentinel

An Approach to Managing and Handling Events and Incidents Using Microsoft Sentinel

Recebido: 16/04/2024 | Revisado: 28/04/2024 | Aceito: 13/05/2024 | Publicado: 15/05/2024

https://www.doi.org/10.5281/zenodo.11191699

Caique Vinicius Cândido Serpeloni
Fatec Santana de Parnaíba
https://orcid.org/0009-0009-2956-281X
cserpeloni@hotmail.com

Jenifer Oliveira Alencar
Fatec Santana de Parnaíba
https://orcid.org/0009-0005-6704-9401
jenifer2010oliveira@gmail.com

Edison Brener Santos Malta
Fatec Santana de Parnaíba
https://orcid.org/0009-0004-6288-6553
brener.mata@gmail.com

Ricardo Leardini Lobo
Fatec Santana de Parnaíba
https://orcid.org/0009-0004-2051-396X
ricardo.lobo@fatec.sp.gov.br

Journal of Technology & Information

Resumo

O estudo em questão teve como objetivo analisar como o Microsoft Sentinel pode auxiliar empresas na gestão e tratamento automatizado de eventos e incidentes de segurança. Para tal, foi utilizada a metodologia de estudo de caso, acompanhando a utilização pós-implantação de um Sistema de Gerenciamento de Informações e Eventos de Segurança (SIEM) em uma empresa. O principal enfoque da pesquisa é destacar os benefícios que a ferramenta nativa da nuvem, Microsoft Sentinel, pode oferecer para aprimorar a segurança das informações de uma organização. A metodologia utilizada foi o estudo de caso, realizado em uma empresa real de médio porte, e a natureza da pesquisa é qualitativa. Dessa forma, serão analisados os recursos disponíveis no Sentinel, tais como inteligência artificial e aprendizado de máquina, que permitem a detecção e prevenção de ameaças em tempo real, permitindo uma resposta mais rápida a possíveis incidentes de segurança. Ao final da pesquisa, foi possível ter um panorama dos benefícios do Microsoft Sentinel para a segurança da informação empresarial e um entendimento da sua utilização em um ambiente corporativo. A pesquisa demonstra que a implantação e configuração da ferramenta possibilitam a centralização de operações, de maneira que os eventos e incidentes de segurança podem ser gerenciados e respondidos de forma automatizada. Assim, principal contribuição alcançada com este artigo, é demonstrar que existe a possibilidade de atuar com o Microsoft Sentinel em ambiente corporativo e com grande volume de dados de forma a auxiliar demais interessados na implementação de soluções de segurança em organizações.

Palavras-chave: Segurança da informação, Eventos e Incidentes, SIEM, Microsoft Sentinel.

Abstract

The study in question aimed to analyze how Microsoft Sentinel can help companies in the automated management and treatment of security events and incidents. To this end, the case study methodology was used, following the post-implementation use of a Security Information and Event Management System (SIEM) in a company. The main focus of the research is to highlight the benefits that the cloud-native tool, Microsoft Sentinel, can offer to improve an organization's information security. The methodology used was a case study, carried out in a real medium-sized company, and the nature of the research is qualitative. In this way, the resources available in Sentinel will be analyzed, such as artificial intelligence and machine learning, which allow the detection and prevention of threats in real time, allowing a faster response to possible security incidents. At the end of the research, it was possible to have an overview of the benefits of Microsoft Sentinel for corporate information security and an understanding of its use in a corporate environment. The research demonstrates that the implementation and configuration of the tool enables the centralization of operations, so that security events and incidents can be managed and responded to in an automated way. Therefore, the main contribution achieved with this article is to demonstrate that there is the possibility of working with Microsoft Sentinel in a corporate environment and with a large volume of data in order to help others interested in implementing security solutions in organizations.

Keywords: Information security, Events and Incidents, SIEM, Microsoft Sentinel.

1. Introdução

Com os avanços tecnológicos, as empresas estão buscando novas técnicas para se atualizar no mercado. Segundo o índice de Transformação Digital da Dell Technologies 2020 (DT Index 2020), cerca de 80% das empresas aceleraram algum programa de transformação digital em 2020 (DELL, 2020).

Com tanta tecnologia, o tráfego de dados empresariais na rede se tornou massivo, tornando as empresas mais suscetíveis a eventos e incidentes de segurança. Segundo o site Cert.br em 2019 houve 875.327 incidentes reportados, representando um aumento de mais de 20% em relação ao ano de 2018 (CERT.BR, 2020).

Os altos índices de incidentes de segurança em empresas motivaram a busca por ferramentas que possam gerenciar e tratar esses eventos de forma automatizada. Uma das soluções disponíveis para essa finalidade é o *Security Information and Event Management* (SIEM), oferecido pela Microsoft Sentinel.

O SIEM permite uma visão geral da empresa, integrando dados de diferentes fontes e dispositivos para detecção e prevenção de possíveis ameaças em tempo real. Ele é capaz de coletar e correlacionar eventos de segurança em toda a organização, permitindo uma análise mais completa e eficaz da situação (Microsoft, 2022).

Com a utilização do SIEM, é possível identificar e mitigar ataques de forma mais rápida e eficiente, além de garantir a conformidade com as políticas de segurança da empresa. Ele é especialmente útil em empresas com alto volume de dados e diversas fontes de informação, permitindo que a gestão de segurança seja mais integrada e automatizada. A ferramenta Microsoft Sentinel oferece essa solução de forma nativa na nuvem, permitindo maior agilidade e eficiência na gestão de segurança da informação empresarial (Microsoft, 2022).

Diante desse cenário, este estudo possui uma questão de pesquisa: “Como automatizar a gestão e tratamento de eventos e incidentes utilizando um SIEM?” e possui como objetivo: Conhecer quais os mecanismos de visibilidade, análise, gestão, tratamento e automatização de eventos e incidentes coletados na organização pelo Microsoft Sentinel. Além disso, este estudo busca aumentar a gestão e tratamentos de eventos e incidentes em uma empresa, de forma a torná-la mais proativa com as situações adversas a suas políticas de segurança e contribuir com pesquisas que tratem o Microsoft Sentinel nas empresas.

A presente pesquisa se justifica com base nos dados do relatório sobre incidentes de segurança do Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Ensino e Pesquisa (CAIS) juntamente com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br, que mostra que os ataques cibernéticos estão mais comuns e causando grandes impactos financeiros e de reputação para as organizações. O total de notificações recebidas pelo CERT.br em 2019 foi de 875.327. Este número foi 22% maior que o total do ano de 2018 (CERT.br, 2022).

Pensando neste cenário justifica-se a preocupação das empresas em buscar novas tecnologias com o intuito de antecipar e mitigar possíveis incidentes, como o SIEM, que consiste em uma solução que ajuda as organizações a detectar, analisar e responder as ameaças de segurança antes que elas prejudiquem as operações da empresa (Microsoft, 2022).

Para isso, a pesquisa irá tratar de como o Microsoft Sentinel irá ajudar uma empresa a ter uma ferramenta de detecção e tratamento de incidentes. A escolha pelo Sentinel se deu devido ao relatório da empresa de consultoria Gartner, que em 2021 apontava a empresa Microsoft como visionaria. No relatório de 2022 da mesma consultoria, ela sobe para líder, mostrando que possui potencial para se tornar a solução mais utilizada do mercado (GARTNER, 2022).

Em razão disso, este trabalho está fundamentado em abordar uma das tecnologias atuais, tornando se relevante pois será apresentado não apenas conceitos de segurança, mas também será analisado e aplicado a ferramenta em uma empresa, para provar sua eficiência nas detecções e alertas de eventos e incidentes na rede das organizações.

2. Referencial Teórico

Ao longo do presente capítulo, serão apresentadas as principais fontes de pesquisa bibliográfica para o embasamento do estudo de caso proposto. As fontes de dados utilizadas para a pesquisa bibliográfica foram o Google Acadêmico e a base *Springer* Link.

2.1. Segurança da Informação

A internet é um dos principais meios para transmitir informações, com ela é possível mandar mensagens, *e-mails*, fazer ligações, transações bancárias entre muitas outras coisas. E com tantos dados a apenas um clique, é importante pensar na segurança deles (VELASCO, 2019).

Ainda de acordo com Velasco (2019), “Segurança da informação é um conjunto de ações e boas práticas que tem como finalidade proteger um grupo de dados”. Com isso, o papel da segurança da informação é manter os dados sempre protegidos, sendo importante no resguardo de todas as categorias de dados contra roubo e danos (TOTVS, 2021).

De acordo com Telium Networks (2018), a segurança da informação é definida por meio dos pilares: confidencialidade, integridade, disponibilidade, autenticidade e legalidade. De acordo com Almeida (2021), a confidencialidade está relacionada com a privacidade dos dados, onde são tomadas ações para que as informações confidenciais de uma pessoa física ou jurídica não sejam roubadas. Ainda de acordo com Almeida (2021)

a integridade é a preservação dos dados, garantindo que eles circulem e sejam armazenados da mesma maneira que foram criados. Já a disponibilidade diz respeito ao tempo e a acessibilidade das informações, sendo essencial que eles possam ser consultados a qualquer momento (TELIUM NETWORKS, 2018).

A autenticidade se refere à certeza que realmente é o usuário portador da autorização que está acessando as informações, geralmente testadas por meio de um processo de *login* e senha. Já a legalidade, também conhecida como irretratabilidade, garante que a empresa não possa negar a autoria das informações (Almeida, 2021).

2.2. Eventos e Incidentes

De acordo com a Organização Internacional de Normalização (ISO), um evento é uma ocorrência identificada de um sistema, serviço ou estado de rede indicando uma possível violação de segurança da informação, política ou falha de controles, ou uma situação previamente desconhecida que pode ser relevante para a segurança (ISO, 2009).

Segundo Nist (2013), um incidente de segurança pode ser definido como uma ocorrência que compromete ou pode comprometer a confidencialidade, integridade ou disponibilidade de um sistema de informação, bem como a informação que ele processa, armazena ou transmite. Também pode ser considerado um incidente de segurança a violação ou ameaça iminente de violação das políticas de segurança, procedimentos ou políticas de uso aceitável. Essas definições ajudam a entender a gravidade dos incidentes de segurança e a importância de preveni-los ou gerenciá-los de forma adequada para evitar prejuízos para a organização e seus usuários (NIST, 2013).

2.3. SIEM

Segundo a empresa AV-TEST, em março de 2018 foram reportados 771.077.699 malwares e diante desse cenário, foi necessário a criação e/ou implantação de diversas tecnologias para mitigar e manter o ambiente o mais seguro possível, como por exemplo, Sistemas de Detecção de Invasões (IDS), Sistemas de Prevenção de Intrusão (IPS), para a detecção e prevenção de intrusões, *firewalls* com o intuito de efetuar a segurança do perímetro e bloqueio de portas e utilização de antivírus com a finalidade de efetuar a segurança nas *workstations* (Santos, 2019).

Segundo Gartner, consultoria renomada, o SIEM tem o intuito de oferecer suporte a detecção de ameaças, conformidade e gerenciamento de segurança por meio da coleta e análise dos eventos de segurança, com o recurso de capturar esses *logs* de diversas fontes, como Linux, Windows, Cisco, Antivírus, dentre outros. Seus principais recursos englobam um amplo escopo de coleta e gerenciamento dos eventos de *log* com a capacidade de analisar diferentes recursos operacionais (GARTNER, 2022).

O termo SIEM é o resultado da junção dos termos *System Information Manager* (SIM), que efetua o monitoramento dos *logs* em tempo real e o *System Event Manager* (SEM), onde é efetuado o armazenamento dos dados a longo prazo, efetua também a análise e cria relatórios (Santos, 2019).

Também permite que sejam organizados os dados recebidos, sejam eles, eventos, *logs* ou notificações, de diversas fontes e dispositivos de forma centralizada (Santos, 2019).

O SIEM oferece diversos benefícios que auxiliam na segurança da informação, dentre eles: Centralizar a visão geral de possíveis ameaças, permitir a análise, identificação e resposta a possíveis ameaças, prover inteligência contra ameaças avançadas, fornecer recursos de auditoria e relatório de conformidade, bem como maior transparência e melhor monitoramento dos eventos de segurança da informação

(GARTNER, 2022).

O Microsoft Sentinel é capaz de integrar e analisar dados de diversas fontes, o que permite uma visão mais completa e automatizada dos eventos de segurança. A escolha entre essas soluções dependerá das necessidades específicas de cada organização, bem como de fatores como custo, facilidade de uso e compatibilidade com outros sistemas (GARTNER, 2022).

2.4. Microsoft Sentinel

O Microsoft Sentinel é uma ferramenta que fornece SIEM e *Security Orchestration, Automation and Response* (SOAR), que respectivamente significam, Gerenciamento de informações e eventos de segurança e Orquestração de segurança, automação e resposta. Ele é uma solução escalonável e nativa de nuvem (Santos, 2019).

Resumidamente, o Sentinel trará uma visão geral da empresa, amenizando os ataques de um modo geral e trabalhando perfeitamente com um volume de dados alto e de diversas fontes. Com isso, ele traz alguns benefícios voltados ao ambiente da organização, sendo eles: Coleta de dados na nuvem, detecção de ameaças que não foram descobertas e investigando ameaças com a inteligência artificial. Dentre esses benefícios, a resposta a incidentes de forma rápida e proativa, com a orquestração interna e automação de tarefas destaca-se como um dos principais (Microsoft, 2022).

Ainda segundo a Microsoft (2022), um outro ponto importantíssimo a ser comentado referente ao Sentinel, é que ele permite relacionar alertas a incidentes utilizando regras de análise. Basicamente, incidentes são grupos de alertas, que juntos, indicam uma possível ameaça para analisar, investigar e mitigar. Ele também permite a utilização de regras de *machine learning*, que basicamente, interligam a evolução do estudo de reconhecimento de padrões e teoria do aprendizado computacional com a inteligência artificial, para mapear o comportamento da rede e assim investigar alguma anormalidade.

Também é possível automatizar tarefas comuns utilizando guias estratégicos de ferramentas existentes, pois o Sentinel oferece uma arquitetura que oferece uma automação escalonável. Ele possui mais de 200 conectores para diversas ferramentas e serviços, são elas: ServiceNow, Jira, ZenDesk, Microsoft Teams, entre outros. E esses conectores permitem aplicar qualquer lógica personalizada para a maior adequação e compatibilidade com o ambiente. Ainda, é possível investigar o escopo e a causa raiz das ameaças com a ferramenta de investigação profunda, auxiliando no entendimento do escopo e encontrando a causa raiz de uma possível ameaça (GARTNER, 2022).

Por fim, vale destacar a possibilidade de estruturar buscas em consultas na estrutura do *MITTRE ATT&CK*, que basicamente, é uma diretriz para classificar e descrever ataques cibernéticos e intrusões, abordando 14 categorias de técnicas e táticas que os invasores utilizam e podem utilizar dentro de um ambiente (Microsoft, 2022).

Tais técnicas e táticas são amplamente utilizadas para a criação de um perfil de detecção personalizado, tendo como base as consultas de busca. E durante essas buscas, pode-se criar indicadores para retornar aos eventos interessantes ao ambiente. Também é possível utilizar esses eventos, correlacionando com outros eventos e assim criar um incidente categórico e convincente para a análise (Santos, 2019).

3. Metodologia

Este tópico é destinado à apresentação da modalidade da pesquisa; aos procedimentos de coleta e análise de dados, a amostra, e busca apresentar os passos realizadas durante o desenvolvimento da pesquisa para a obtenção dos resultados e posterior realização das análises.

A metodologia utilizada foi o estudo de caso único, como abordado por Yin (2017) e a natureza da pesquisa é qualitativa, como demonstrado por Theophilo e Martins (2016), pois o estudo pretende acompanhar, documentar e automatizar os processos de

gerenciamento e tratativa de eventos e incidentes utilizando o Microsoft Sentinel em um ambiente real. A coleta de dados se dará por intermédio de análises técnicas do ambiente organizacional (Gil, 2022). Foram explorados no cenário de segurança da informação, o gerenciamento e tratamentos desses eventos e incidentes antes da implantação do SIEM e o levantamento do cenário pós aplicação.

O estudo de caso se deu em um ambiente real, sendo realizado em uma empresa de médio porte (aproximadamente 100 colaboradores), localizada na região metropolitana de São Paulo, cujos demais dados não tiveram autorização de uso acadêmico.

Como unidade de análise utilizou-se o Microsoft Sentinel. Na Tabela 1 são apresentadas as características utilizadas para a realização do trabalho.

Tabela 1 - Características do estudo

ITEM	DESCRIÇÃO	AUTORES
QUESTÃO DE PESQUISA	▪ Como automatizar a gestão e tratamento de eventos e incidentes utilizando um SIEM?	
NATUREZA	▪ Qualitativa	Theophilo e Martins (2016).
METODOLOGIA	▪ Estudo de caso único	Yin (2017).
COLETA DE DADOS	▪ Análise documental e Entrevista	Gil (2022).
UNIDADE DE ANÁLISE	▪ Microsoft Sentinel	

Fonte: Os autores.

3.1. Processo Metodológico

Conforme a Figura 1, as etapas desta pesquisa são:

Passo 1: Análise das documentações. Efetuado a análise dos documentos referentes ao gerenciamento e tratamento dos eventos e incidentes relacionados à Segurança da Informação na organização.

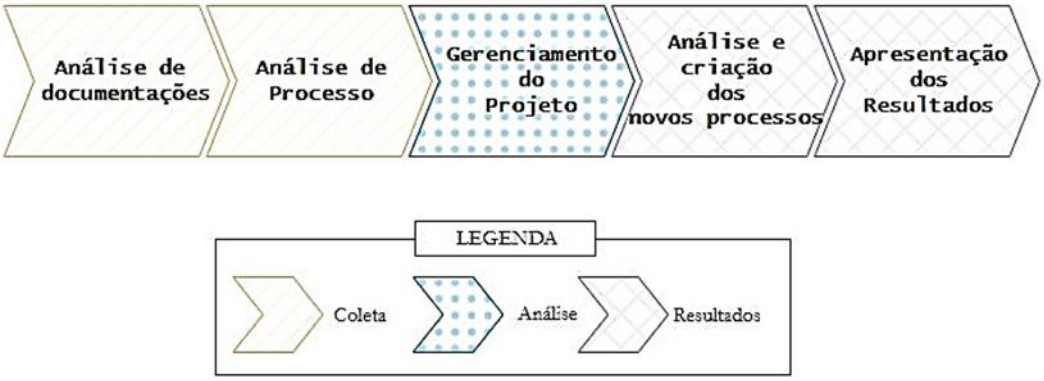
Passo 2: Análise do processo. Após a análise dos documentos, efetuamos a análise do processo desse gerenciamento como um todo, de forma geral.

Passo 3: Gerenciamento do projeto. Efetuado a criação e gerenciamento do projeto de implantação da ferramenta, para melhor planejamento e aplicação como um todo.

Passo 4: Análise e criação de novos processos. Foram efetuadas as criações de novos processos, documentações para o novo procedimento de gerenciamento de eventos e incidentes.

Passo 5: Apresentação dos resultados. Foram apresentados os resultados, referentes a automatização e o aumento de eficiência na área de Segurança da Informação.

Figura 1 – Processo Metodológico

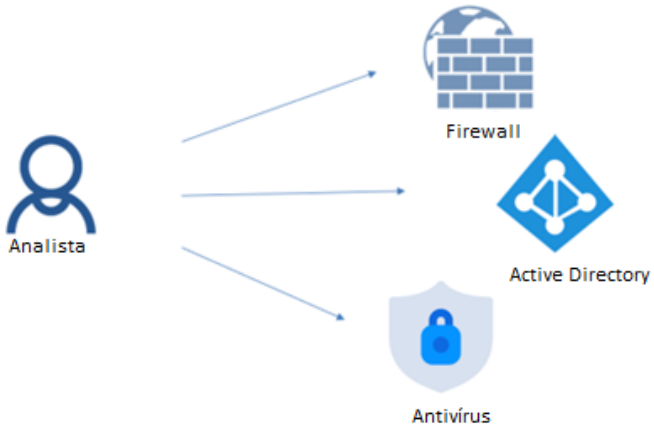


Fonte: Os autores.

4. Análise e Interpretação dos Resultados

A topologia descentralizada é uma das principais abordagens para a criação de infraestruturas de rede em larga escala, em que cada nó da rede é independente e pode se comunicar com qualquer outro nó. Nesse contexto, o gerenciamento descentralizado é o cenário inicial do estudo de caso em questão, que busca avaliar a eficácia de uma solução de segurança baseada em nuvem para a proteção de sistemas distribuídos. Com essa abordagem, é possível avaliar como era o trabalho do analista de segurança antes de implantar a solução, conforme diagrama apresentado na Figura 2.

Figura 2 – Gerenciamento descentralizado

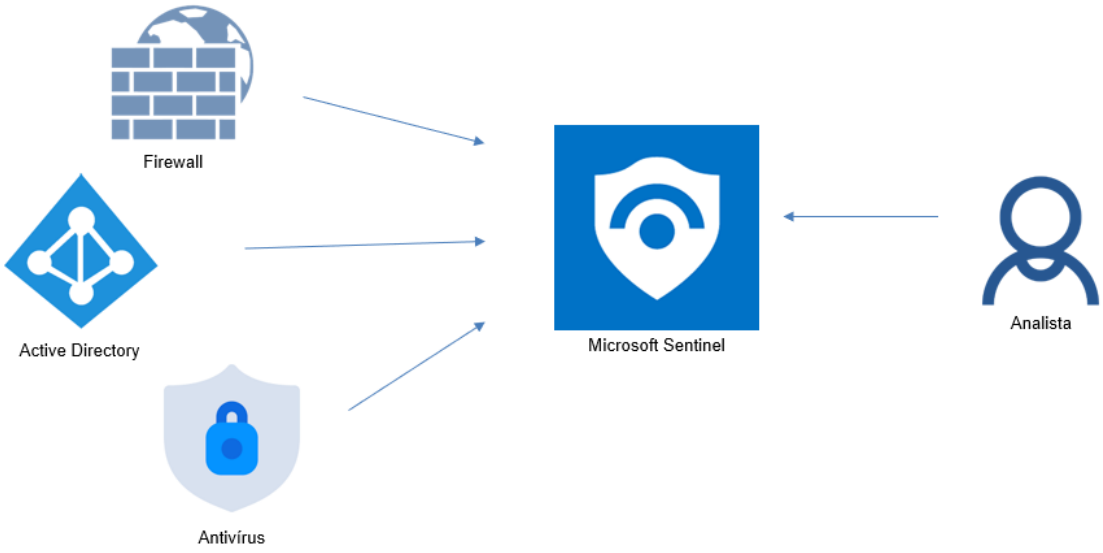


Fonte: Os autores.

Sem o uso do SIEM, o gerenciamento de segurança de informações é um processo fragmentado e trabalhoso, exigindo que os analistas verifiquem manualmente cada aplicação separadamente. Por exemplo, eles precisam acessar o *firewall* para identificar os endereços de rede que estão realizando escaneamento de porta, verificar o antivírus em busca de alertas maliciosos e checar o Active Directory para identificar usuários bloqueados devido a tentativas de *login* sem sucesso.

Em contrapartida, o uso de um SIEM como o Microsoft Sentinel permite que os analistas visualizem todas as aplicações em uma única interface. Todos os sistemas são cadastrados no Sentinel e os logs são analisados automaticamente. Com regras pré-configuradas, o sistema pode disparar alertas de eventos ou incidentes para os administradores, simplificando o processo de gerenciamento e permitindo uma resposta mais rápida a ameaças em potencial, conforme apresentado no diagrama da Figura 3.

Figura 3 – Gerenciamento centralizado



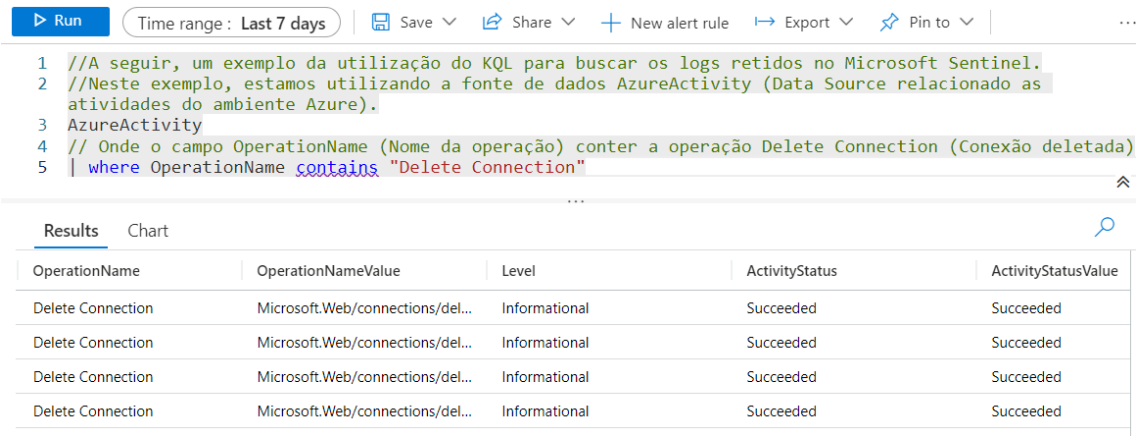
Fonte: Os autores.

A Figura 4 apresenta a funcionalidade de *log* no Microsoft Sentinel. O módulo em questão é a tela de desenvolvimento de *query*, onde se utiliza a Kusto Query Language (KQL) para criar casos de uso e disponibilizar fontes de dados, entre outras funcionalidades. É possível observar o uso de uma fonte de dados de eventos de segurança, especificamente a fonte de dados do Active Directory. Por meio de um filtro, são identificados eventos relacionados aos seguintes IDs: 4728, 4732 e 4756. Esses IDs correspondem a eventos registrados no diretório do Active Directory e, por meio deles, é

possível realizar pesquisas na base de conhecimento da Microsoft para obter informações sobre o significado de cada ID.

Esses IDs estão relacionados a eventos específicos, como escalonamento de privilégios e adição de usuários a grupos com privilégios administrativos, tanto localmente quanto no domínio. O objetivo desse caso de uso é analisar e responder a possíveis ataques de escalonamento de privilégios e atividades de movimentação no ambiente.

Figura 4 – Microsoft Sentinel - *Logs*

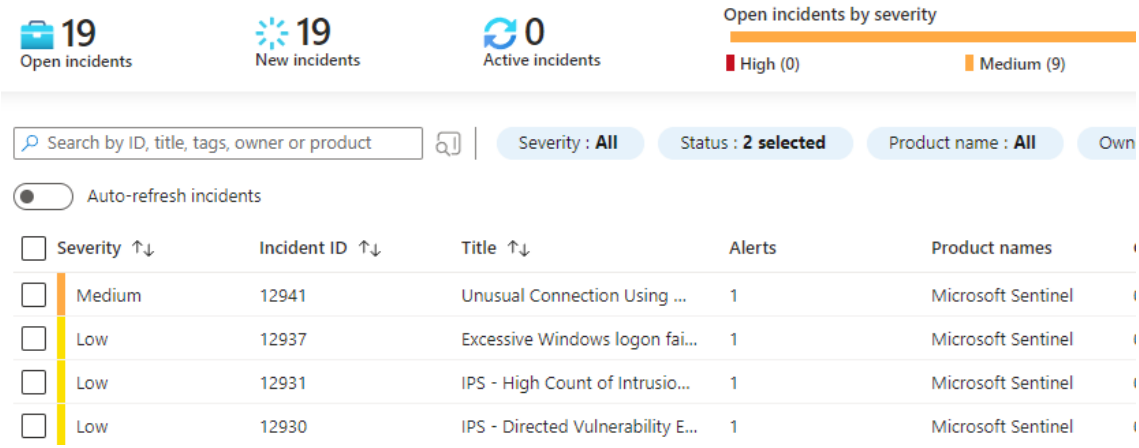


Fonte: Os autores

Na Figura 5 apresentada abaixo, é destacado o módulo de incidentes, cujo propósito é gerenciar todos os incidentes capturados a partir das regras de casos de uso criadas. Na análise desta imagem, é possível observar a existência de 19 incidentes em aberto. Dentre esses incidentes, algumas regras foram responsáveis pela sua geração, de acordo com as condições especificadas nas consultas. Entre essas regras, destaca-se a regra denominada "*Excessive Windows Logon Failures*". Essa regra é configurada para acionar um incidente caso seja identificado que um determinado usuário tenha sofrido três ou mais falhas consecutivas de login. Nesse caso, é gerado um alerta para que seja realizada uma análise do incidente.

Outra regra mencionada é a "*Unusual Connection Using*". Essa regra é aplicada à fonte de dados do *firewall*, sendo capaz de capturar qualquer conexão remota que utilize os protocolos *Secure Socket Shell* (SSH) ou *Remote Desktop Protocol* (RDP). Essa regra também possui uma lista de exceções que contempla alguns usuários autorizados a utilizar o recurso de acesso remoto.

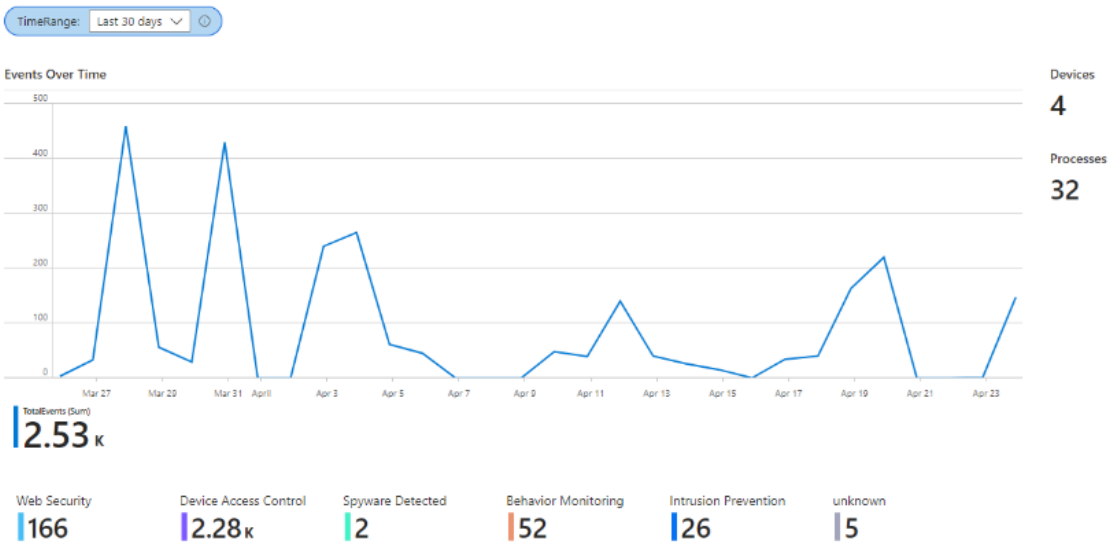
Figura 5 – Microsoft Sentinel - *Incidents*



Fonte: Os autores.

A Figura 6 apresenta o módulo de pasta de trabalho permite aos usuários criar pastas de trabalho personalizadas para facilitar a obtenção rápida de informações a partir dos dados disponíveis. No exemplo apresentado, foi criada uma pasta de trabalho correlacionada com uma fonte de dados de antivírus. Dessa forma, diversos painéis foram incluídos, como o painel "Eventos ao longo do tempo" ilustrado na imagem, o qual permite rastrear eventos maliciosos e suas subcategorias em termos de volume. O desenvolvimento da pasta de trabalho também envolve a utilização de consultas KQL.

Figura 6 – Microsoft Sentinel - *Workbooks*



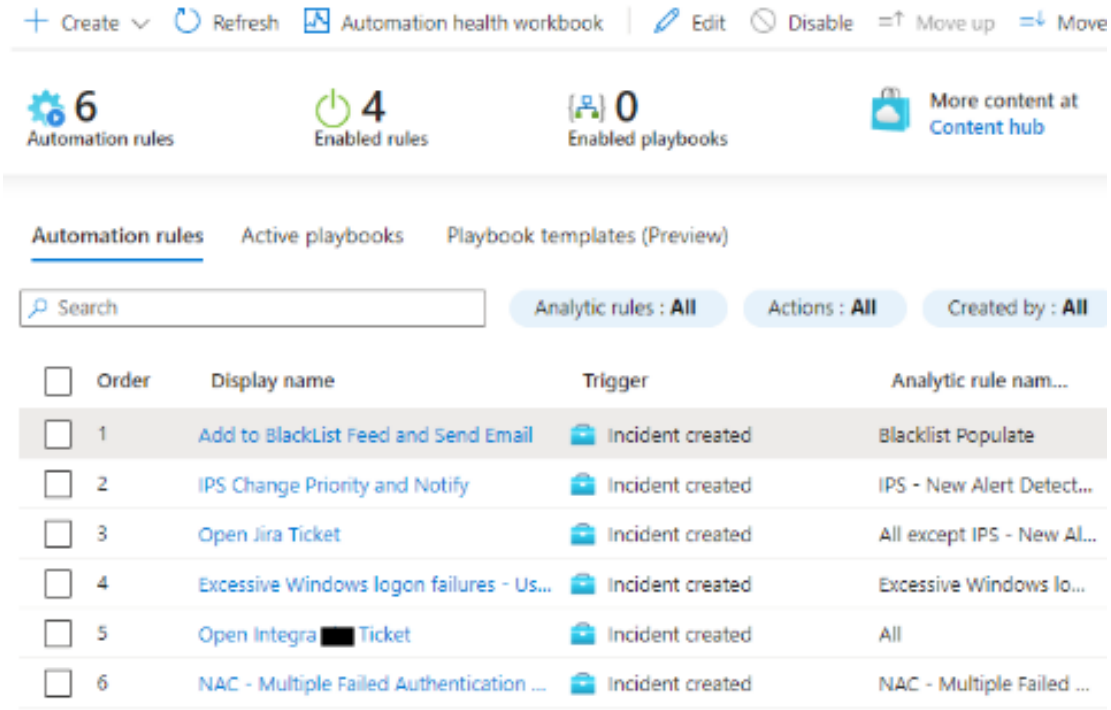
Fonte: Os autores.

Todas as regras e casos de uso criados possuem conectividade com o *Mittre Attack Framework*, permitindo assim o gerenciamento e correlação de todas as regras com suas respectivas instruções que classificam um ataque cibernético. Essa abordagem tem possibilitado a análise dos pontos fortes e fracos dos casos de uso no ambiente, bem como uma melhoria contínua desses casos, contribuindo para o aprimoramento da segurança em geral.

O módulo Análise tem a responsabilidade de manter, gerenciar e manipular todas as regras criadas para o ambiente em questão. Um exemplo de regra utilizada é a *Black List Populate.* Essa regra tem como função receber os *logs* do CiscoIPS e identificar possíveis ataques, como varredura de portas, força bruta e outras atividades suspeitas. Quando um evento desse tipo é detectado, a regra captura o endereço IP responsável e o adiciona automaticamente a uma lista negra, que é armazenada em um arquivo de texto no serviço AWS S3.

Esse arquivo, contendo os endereços IP capturados pela regra, é configurado diretamente no serviço de *firewall*, resultando no bloqueio em tempo real dos endereços IP registrados. Todo esse processo é realizado de forma automatizada, dispensando a necessidade de um analista realizar a análise do caso. E, por fim, é apresentado o módulo de automação. Nesse contexto, existem dois casos de automação implementados.

Figura 7 – Microsoft Sentinel – Notificação



Fonte: Os autores.

O primeiro caso de automação diz respeito à integração dos incidentes abertos com a plataforma JIRA, conforme demonstrado na Figura 7. Por meio do gerenciador de *tickets*, JIRA, é possível automatizar o processo de recebimento de alertas e a geração de *tickets* para a atuação da equipe *Security Operations Center* (SOC). Nesse processo automatizado, são utilizadas duas formas de notificação. A primeira consiste no

recebimento dos alertas por meio de um grupo de *e-mail* designado, enquanto os casos considerados críticos são recebidos por meio de um grupo específico no aplicativo Telegram. Essas notificações permitem uma resposta ágil e efetiva por parte da equipe responsável.

O segundo caso, está relacionado ao exemplo mencionado no módulo Análise, no qual foram estabelecidas condições para que a regra possa capturar os endereços IP dos atacantes e adicioná-los a uma lista de bloqueio, que está diretamente conectada ao *firewall*. Essa automação visa agir prontamente contra possíveis ameaças.

4.1. Discussão

Conforme discutido em Desenvolvimento de Pesquisa, a gestão de análises pode ser realizada de maneira descentralizada, na qual analistas ou responsáveis por tratar incidentes em uma organização realizam a análise de incidentes de segurança de forma manual, sem o auxílio de tarefas automatizadas.

A implantação e configuração da ferramenta possibilitam a centralização, de maneira que os eventos e incidentes podem ser gerenciados e respondidos de forma automatizada. Quando ocorrer um incidente em um *firewall*, agora é possível bloquear automaticamente um invasor que tenta mapear as portas *Transmission Control Protocol* (TCP) e *User Datagram Protocol* (UDP), utilizando regras e automações incorporadas ao SIEM. Esse procedimento contribui para um tempo de resposta mais ágil aos eventos. Com a descentralização, o tempo médio de captura, análise e resposta do analista foi de 10 minutos, o que resultou na redução do congestionamento em tempo real, quando utilizado o centralizado.

No contexto de servidores *Active Directory*, a centralização, detecção e análise de todos os eventos relacionados a ele são viabilizados por meio da criação de regras. Qualquer escalonamento suspeito de privilégios de administrador pode ser identificado,

conforme evidenciado na análise dos resultados. Com a obtenção dessa identificação, um *ticket* é criado para a resposta no JIRA.

Com a ferramenta de antivírus, é possível centralizar todas as ocorrências e incidentes encontrados no ambiente interno, automatizando e padronizando o gerenciamento de ordens de serviço. As notificações por *e-mail* e outras plataformas ajudam a reduzir o tempo de resposta a incidentes.

5. Conclusões

O Microsoft Sentinel se destaca como uma solução poderosa e abrangente para os desafios modernos de segurança cibernética. Ao alavancar recursos avançados de IA e aprendizado de máquina, o Sentinel capacita as organizações a detectar e responder proativamente a ameaças em tempo real, fornecendo uma camada crucial de defesa contra ameaças cibernéticas em evolução.

A aplicação do Microsoft Sentinel se estende por vários setores e indústrias. De instituições financeiras que protegem dados confidenciais de clientes a organizações de assistência médica que protegem registros de pacientes, o Sentinel oferece uma plataforma robusta que pode ser adaptada para atender a necessidades específicas de segurança. Sua escalabilidade e flexibilidade permitem uma integração perfeita com a infraestrutura de segurança existente, capacitando as equipes de segurança a obter ideias mais profundas, automatizar a resposta a incidentes e aprimorar a inteligência geral contra ameaças.

Além disso, a integração do Microsoft Sentinel com os serviços do Azure e sua extensa biblioteca de conectores permitem que as organizações coletem, analisem e correlacionem dados de segurança de uma ampla variedade de fontes. Essa abordagem holística permite detecção e resposta abrangentes a ameaças, ajudando as equipes de

segurança a identificar padrões, tendências e possíveis vulnerabilidades em toda a infraestrutura.

À medida que as ameaças cibernéticas continuam a evoluir e se tornar mais sofisticadas, as organizações devem adotar soluções inovadoras como o Microsoft Sentinel para fortalecer sua postura de segurança. Ao alavancar tecnologias de ponta, como inteligência artificial e aprendizado de máquina, o Sentinel fornece uma abordagem proativa e inteligente para segurança cibernética, permitindo que as organizações fiquem um passo à frente dos agentes mal-intencionados.

Em um mundo onde violações de dados e ataques cibernéticos se tornaram comuns, o Microsoft Sentinel oferece um mecanismo de defesa robusto e eficaz, capacitando as organizações a proteger seus ativos valiosos e manter a confiança de seus clientes, definindo um novo padrão para operações de segurança de próxima geração, tornando-o uma ferramenta indispensável na luta contra ameaças cibernéticas.

Durante o desenvolvimento desta pesquisa, contudo, algumas limitações foram encontradas, sendo possível listar as seguintes: por se tratar de um *software* ainda recente no mercado, a quantidade de documentação, exemplos práticos de aplicação e fóruns de discussão disponíveis sobre o mesmo é limitada, sendo a própria documentação oficial a única fonte confiável de dados, dificultando a pesquisa e estudo de casos reais de implantação da ferramenta. Também há de se destacar a limitação do estudo em si: a ferramenta foi testada em uma organização de médio porte, contudo, não há como garantir que a mesma forma de implementação terá sucesso em organizações de grande porte.

Com o estudo da implantação dessa aplicação, foi possível realizar a automatização de bloqueios relacionados as tentativas de invasões e uma melhor gestão e centralização dos eventos e incidentes relacionados à segurança da informação. Assim, esta pesquisa pretende contribuir com informações de implementação prática e características teóricas substanciais a respeito do *software* Microsoft Sentinel como um auxílio para organizações aumentarem seu nível de segurança da informação.

Por fim, como contribuições e trabalho futuro, pretende-se realizar a implementação do software Microsoft Sentinel, nos moldes apresentados neste estudo, em organizações de maior porte, para avaliação do comportamento do *software* com um volume maior de dados.

Referencial Bibliográfico

ALMEIDA, Abraão. (2021). *Conheça os 5 pilares da segurança da informação das empresas*. https://blog.hosts.green/pilares-daseguranca-da-informacao/

CERT.BR. (2020). *Estatísticas dos Incidentes Reportados ao CERT.br*. https://www.cert.br/stats/incidentes/

DELL TECHNOLOGIES. (2020). A*valiação do andamento da transformação digital ao redor do mundo.* 2020. https://www.dell.com/ptbr/dt/perspectives/digital-transformation-index.htm#scroll=off

GARTNER. (2022). *Security Information and Event Management (SIEM).* 2022. https://www.gartner.com/en/informationtechnology/glossary/security-information-and-event-management-siem

GIL, Antonio. (2022). *Como elaborar projetos de pesquisa*. Em GEN - Atlas. 7ª Ed. Atlas.

ISO. ISO/IEC27000:2009. (2009). *Information technology — Security Techniques — Information security management systems.* https://revista.fatectq.edu.br/interfacetecnologica/article/view/40/37

Microsoft. *Microsoft Sentinel.* (2022). https://azure.Microsoft.com/pt-pt/products/Microsoftsentinel/https://azure.Microsoft.com/pt-pt/products/Microsoft-sentinel/

NIST. (2013). *Guia de tratamento de incidentes de segurança do computador: recomendações do Instituto Nacional de Padrões e Tecnologia*. https://nist.ent.sirsi.net/client/en_US/default/search/detailnonmodal/ent:$002f$002fSD_ILS$002f0$002fSD_ILS:104535/one?qu=NIST.SP.800-61r2&te=ILS&lm=NISTPUBS

Santos, L. SIEM. (2019). *Open-Source Solutions: A Comparative Study*.

https://www.researchgate.net/publication/338052058_SIEM_Open_Source_Solutions_A_Comparative_Study

TOTVS. (2021). *Segurança da informação: o que é e boas práticas*. https://www.totvs.com/blog/negocios/seguranca-dainformacao

TELIUM NETWORKS. (2018). *Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação,* https://www.telium.com.br/blog/confidencialidade-integridadee-disponibilidade-os-tres-pilares-da-seguranca-da-informacao

THEOFILO, Carlos; MARTINS, Gilberto. (2016). *Metodologia Da Investigação Cientifica*. Ed. Atlas.

VELASCO, Ariane. (2019). *O que é Segurança da Informação* https://canaltech.com.br/seguranca/seguranca-da-informacaoo-que-e-158375/

YIN, Robert. (2017). *Case Study Research and Applications: Design and Methods*. Sage Publications, Inc.