PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

UM ESTUDO SOBRE SOLUÇÕES DE ATAQUES CIBERNÉTICO COM SIEM COM FOCO NA PLATAFORMA *SPLUNK*

MAILODI VIEIRA SABATH

GOIÂNIA
2024

MAILODI VIEIRA SABATH

UM ESTUDO SOBRE SOLUÇÕES DE ATAQUES CIBERNÉTICO COM SIEM COM FOCO NA PLATAFORMA *SPLUNK*

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade de Goiás, como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação

Orientador (a):

Profª. Dr. Solange da Silva.

Banca examinadora:

Prof. Me. Gildenor De Souza Amorim Cavalcante

Prof. Me. Anibal Santos Jukemura

GOIÂNIA

2024

UM ESTUDO SOBRE SOLUÇÕES DE ATAQUES CIBERNÉTICO COM SIEM COM FOCO NA PLATAFORMA *SPLUNK*

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Ciências da Computação, em: 09/ 12/ 2024.

_____

Orientador (a): Profª. Dr. Solange da Silva.

_____

Prof. Me. Gildenor De Souza Amorim Cavalcante

_____

Prof. Me. Anibal Santos Jukemura

GOIÂNIA

2024

Dedico este trabalho para meus pais por todo apoio e carinho em todos os momentos da minha vida.

AGRADECIMENTOS

Agradeço a Deus por me dar força e saúde para que concluísse os desafios enfrentados durantes os meus estudos.

Gostaria de agradecer a minha família minha mãe Lucimar de França Sabath, meu pai Ademir Vieira de Melo, meu irmão Maike Vieira Sabath, por sempre me apoiarem e incentivar a conquistar meus objetivos.

Um agradecimento especial a minha orientadora Solange da Silva, por todo apoio e paciência para a realização deste trabalho.

E a todos os professores e amigos que contribuíram de alguma forma para este trabalho.

RESUMO

O objetivo geral deste trabalho foi fazer uma revisão bibliográfica e descrever as funcionalidades da ferramenta *Splunk* na detecção, resposta e prevenção de ataques cibernéticos. Quanto aos aspectos metodológicos nos procedimentos técnicos esta pesquisa é bibliográfica e documental. O estudo permitiu observar uma preocupação em torno da segurança cibernética, os danos que esses ataques podem causar às empresas em relação a perda e roubo de dados além de prejuízos financeiros. Existem diversas técnicas de ataques cibernéticos, algumas mais comuns tais como o *phishing*, DDoS e *ransomware*, mostrando que há uma constante adaptação dos atacantes em relação às medidas de segurança. Alguns modelos descrevem as etapas de um ataque cibernético - dois deles são o *MITRE ATT&CK* e o *Cyber Kill Chain,* esses modelos possibilitam as organizações compreenderem melhor as táticas dos invasores. Um SIEM centraliza e correlaciona os eventos de logs de segurança de diversas fontes, com isso é possível analisar de forma mais abrangente, identificando os padrões suspeitos. O SOC é responsável por monitorar toda a infraestrutura tecnologia da organização, é o SOAR busca trazer automação para muitas das tarefas manuais comuns, com o objetivo de aprimorar a eficiência e a consistência nas operações de segurança. Conclui-se que um SIEM centraliza e correlaciona os eventos de logs de segurança de diversas fontes, com isso é possível analisar de forma mais abrangente, identificando os padrões suspeitos. O *Splunk* é um SIEM altamente escalável e eficiente, além de possuir a vantagem na indexação e na pesquisa de arquivos de log, facilitando a análise de grandes volumes de dados. Além disso, a ciência forense cibernética consiste em extrair informações, analisar dados e obter inteligência que possa ser apresentada em um tribunal como provas, garantindo conformidade legal e implementação de políticas de auditoria e, com isso, a integridade das informações são preservadas. Com ela é possível fazer uma conexão das práticas que são capazes de favorecer atividades criminosas. Concluiu-se que as empresas podem aprimorar a segurança cibernética e reduzir riscos utilizando o *Splunk* como SIEM. Essa ferramenta permite centralizar e correlacionar eventos de segurança, possibilitando análise em tempo real, identificação de padrões maliciosos e gerenciamento avançado de logs. Com todas essas ferramentas para a análise de grandes volumes de dados, o *Splunk* acaba sendo muito útil para as

empresas na proteção contra ameaças cibernéticas. Foi possível concluir também que as empresas podem melhorar a segurança cibernética e reduzir riscos usando o *Splunk* como SIEM. Com isso é possível centralizar e correlacionar eventos de segurança, possibilitando a análise em tempo real, a identificação de padrões maliciosos, além de possuir um gerenciamento de logs avançado.

Palavras chaves: Segurança da Informação. Ataques cibernéticos. *Splunk*. SIEM. SOR. Gerenciamento de logs. Ciência forense.

ABSTRACT

The overall objective of this study was to conduct a bibliographic review and describe the functionalities of the Splunk tool in detecting, responding to, and preventing cyberattacks. Regarding methodological aspects, in its technical procedures, this research is bibliographic and documentary. The study highlighted a growing concern about cybersecurity, the damage these attacks can cause to companies in terms of data loss and theft, as well as financial losses. There are various cyberattack techniques, some of the most common being phishing, DDoS, and ransomware, demonstrating the attackers' constant adaptation to security measures. Some models describe the stages of a cyberattack—two of them are the MITRE ATT&CK and the Cyber Kill Chain. These models enable organizations to better understand the attackers' tactics. A SIEM centralizes and correlates security log events from various sources, allowing for more comprehensive analysis and the identification of suspicious patterns. The SOC is responsible for monitoring the organization's entire technological infrastructure, while SOAR seeks to bring automation to many common manual tasks to enhance efficiency and consistency in security operations. It is concluded that a SIEM centralizes and correlates security log events from various sources, allowing for a broader analysis and identification of suspicious patterns. Splunk is a highly scalable and efficient SIEM, with advantages in indexing and searching log files, facilitating the analysis of large volumes of data. Moreover, cyber forensic science involves extracting information, analyzing data, and obtaining intelligence that can be presented in court as evidence, ensuring legal compliance and the implementation of audit policies. This preserves information integrity and enables connections to be made between practices that might facilitate criminal activities. It was concluded that companies can enhance cybersecurity and reduce risks by using Splunk as a SIEM. This tool allows for the centralization and correlation of security events, enabling real-time analysis, identification of malicious patterns, and advanced log management. With all these capabilities for analyzing large volumes of data, Splunk proves to be highly useful for companies in protecting against cyber threats.

Keywords: Information Security. Cyberattacks. Splunk. SIEM. SOAR. Log Management. Forensic Science.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS E ABREVIATURAS

APT	*Advanced Persistent Threat ou* Ameaça Persistente Avançada.
ATT&CK	*Adversarial Tactics, Techniques and Common Knowledge*
DMA	*Direct Memory Access* ou Acesso direto à memória
DNS	*Domain Name System* ou Sistema de nome de domínio
DDoS	*Distributed Denial of Service* ou Ataque distribuído de negação de serviço
DoS	*Denial of Service* ou Ataques de negação de serviço
DSDL	*Splunk App for Data Science and Deep Learning*
ID	Identidade
IDS	*Intrusion Detection Systems ou* Sistema de detecção de intrusos
IoT	*Internet of Things* ou Internet das Coisas
PACS	*Picture Archiving and Communication System* ou Sistemas de armazenamento e comunicação de imagens
NIST	*National Institute of Standards and Technology* ou Instituto Nacional de Padrões e Tecnologia
REST	Representational State Transfer ou Tansferência de estado representacional
RDP	*Remote Desktop Protocol*
RSA	*Rivest Shamir Adleman*
SaaS	*Software as a Service* ou *Software* como Serviço
SANS	*System Administration, Networking and Security* ou Administração de sistemas, redes e segurança
SEM	Gerenciamento de Eventos de Segurança
SIEM	*Security Information and Event Management*
SIM	Gerenciamento de Informações de Segurança
SOAR	*Security Orchestration Automation and Response ou* Orquestração, automação e resposta de segurança
SOC	*Security Operation Centers Explained* ou Centro de operações de segurança
TCC	Trabalho de Conclusão de Curso
TI	Tecnologia da Informação

UI	*User Interface* ou Interface do Usuário
URL	*Uniform Resource Locator* ou Localizador Uniforme de Recursos

SUMÁRIO

1 INTRODUÇÃO

Na segurança da informação, existem três pilares principais: integridade, disponibilidade e confidencialidade. Manter esses pilares íntegros é um dos maiores desafios, já que os atacantes estão constantemente desenvolvendo novas formas de comprometer sistemas, visando danificar a segurança dos dados corporativos (*ServiceIT*, 2021).

Com a evolução das tecnologias digitais, diversos aspectos da vida social migraram para a internet, incluindo atividades industriais, empresariais e interações sociais. Infelizmente, essa migração também se estendeu ao setor criminal (*Hiscox*, 2019).

O cibercrime tornou-se uma realidade permanente devido ao seu alto potencial lucrativo e à impunidade, facilitada pela capacidade dos cibercriminosos de operar globalmente (*Lallie et al*., 2023).

Identificar, investigar e reagir de forma eficiente às ameaças à segurança é uma tarefa bastante desafiadora. Para esses desafios a tecnologia de segurança cibernética *Security Information and Event Management* (SIEM) apresenta uma visão robusta e simplificada dos seus dados, proporcionando *insights* sobre as atividades de segurança e recursos operacionais das organizações, para manter uma vantagem contra as ameaças cibernéticas (*Kidd*, 2023).

Ao decorrer dos últimos 14 anos, o SIEM passou por uma evolução, passando a ter uma abordagem de investigação estática e *post mortem* para um sistema de análise em tempo real. Esta transformação trouxe várias mudanças, com o objetivo de obter um recurso altamente exigentes e uma necessidade constante de serviços cada vez mais robustos (Velásquez, 2023).

O *Splunk* é uma plataforma com várias funções criada com o objetivo de coletar, monitorar e analisar dados. Essas ferramentas podem auxiliar as organizações na coleta, rastreamento e transformação de vários tipos de dados em informações valiosas (*Elmastaş; Eyüpoğlu*, 2023).

O *Splunk* possui a sua capacidade de analisar dados de diversas fontes em tempo real, por exemplo os aplicativos de rede, *hardware*, nuvem e solução *Software as a Service* (SaaS). Com isso o *Splunk* desempenha um papel fundamental auxiliando as

organizações a permanecerem um passo à frente das ameaças cibernéticas, sejam elas internas ou externas (*Kidd*, 2023).

Justifica estudar este tema porque a análise de dados desempenha um papel crucial na prevenção de ataques cibernéticos, permitindo a detecção precoce dos ataques e uma resposta rápida para uma melhoria contínua das estratégias de segurança.

Diante deste contexto, este trabalho visa responder a seguinte questão: **Como as empresas podem otimizar a segurança da informação e mitigar os riscos associados ao crime cibernético, usando tecnologias como o SIEM, com foco na plataforma *Splunk*?**

O objetivo geral é fazer uma revisão bibliográfica para descrever as funcionalidades da ferramenta *Splunk* na detecção, resposta e prevenção de ataques cibernéticos.

Os objetivos específicos são:

- Avaliar o cenário atual de ameaças cibernéticas enfrentadas pelas empresas.
- Identificar as características e funcionalidades do SIEM.
- Analisar as capacidades e recursos específicos da plataforma *Splunk*.
- Buscar estudos de casos que utilizam e mostram a eficácia do *Splunk*.

Espera-se que os resultados deste trabalho possam auxiliar:

- Informando como o do SIEM impacta na prevenção de ataques cibernéticos,
- Apresentando aos usuários e administradores das empresas a ferramenta *Splunk*;

2 REFERENCIAL TEÓRICO

Este capítulo divide-se em duas partes: uma abordando conceitos e definições e outra apresentando alguns trabalhos relacionados.

2.1. Conceitos e definições

Os ataques cibernéticos contra empresas tornaram-se uma preocupação crescente na era digital. Os prejuízos relacionados a esses ataques incluem

destruição de dados, perdas financeiras, roubo de propriedade intelectual, fraudes, entre outros impactos (*Georgiadou; Mouzakitis; Askounis*, 2021).

Há várias técnicas de invasão cibernética destinadas a contornar as medidas de segurança de uma organização. Algumas dessas técnicas incluem *backdoors*, engenharia social, *phishing*, manipulação de URLs, ataques distribuídos de negação de serviço (DDoS), *ransomware*, espionagem (*eavesdropping*), *spoofing*, *botnets*, ataques baseados em identidade, acesso direto à memória (DMA) e injeção de código (Rossi, 2024). A Figura 1 mostra alguns ataques cibernéticos é uma pequena descrição sobre eles.

Figura 1 – Tipos de ataques cibernéticos.

Fonte: Rossi (2024)

A finalidade dos ataques cibernéticos varia conforme os objetivos dos atacantes. Em geral, empresas de grande porte, agências governamentais, instituições financeiras e organizações que lidam com dados sensíveis são os alvos mais frequentes, devido ao seu potencial lucrativo ou à relevância dos danos que um ataque pode causar. Funcionários com acesso a informações valiosas como executivos, profissionais de Tecnologia da Informação (TI) é usuários com dados financeiros importantes, são os alvos mais comuns para vazamentos de dados (Rossi, 2024).

Os invasores estão sempre adaptando suas táticas, explorando vulnerabilidades nas aplicações em vez de depender apenas de força bruta para violar sistemas ou derrubar infraestruturas críticas. Por causa disso, diversas empresas estão procurando parceiros de cibersegurança que ofereçam soluções para proteção contra essa variedade de ameaças que estão em constante evolução (Akamai, 2022).

2.1.1. Phishing

Uma das formas de ataques cibernético em que os criminosos se passam por instituições legítimas com o objetivo de enganar as vítimas para obter suas informações pessoais é o *Phishing*. Os atacantes geralmente utilizam email, telefone ou mensagens de texto para entrar em contato com o usuário (Gonçalves, 2023).

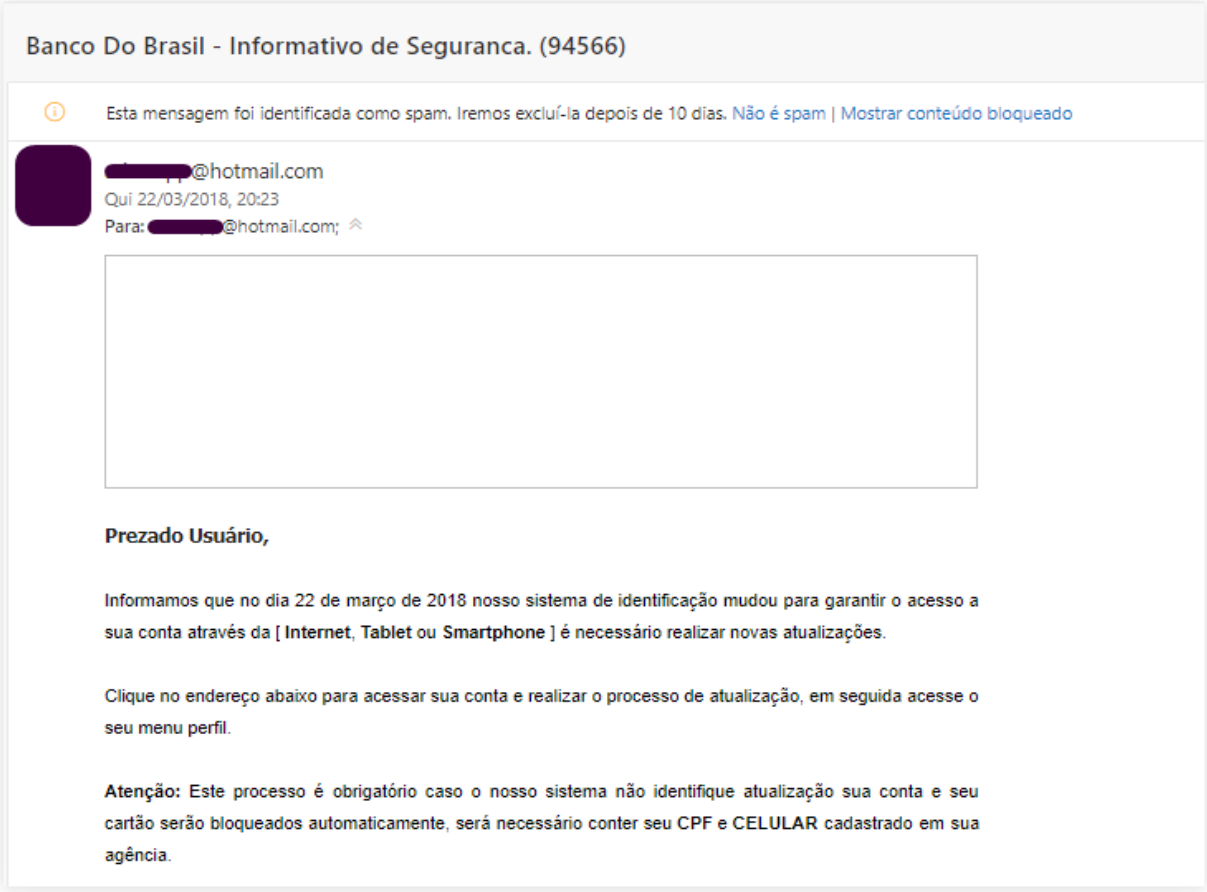
O termo *phishing* vem da “pesca”, na qual reflete a estratégia do invasor de lançar uma isca no intuito de observar quem respondeu. Os ataques de *phishing* geralmente tem como alvo usuários desavisados, assim aproveitando do usuário e da sua falta de conhecimento sobre segurança na Internet (Raza, 2023).

A falta de conhecimento, a desatenção ou o excesso de confiança transformam os funcionários na maior vulnerabilidade de segurança na internet para as empresas. Portanto é tão necessário o investimento em treinamento para os colaboradores e para manter uma política de segurança cibernética dentro da empresa (Zimmer, 2020).

Um exemplo comum de *phishing* é um e-mail falso, na qual o atacante se passa por uma grande rede social, avisando o destinatário para ele redefinir a sua senha por causa de a uma suposta ameaça de segurança, induzindo o usuário a compartilhar sua senha atual. Assim o atacante captura essas informações confidenciais do

usuário. No exemplo de ataque *phishing* é mostrado na Figura 2, em que o atacante se passa por um banco (Sá, 2023).

Figura 2 – Ataque de *Phishing*



Fonte: Gonçalves (2023).

Segundo Gonçalves (2023) o país que sofre com ataques de *phishing* no mundo e o Brasil. Segundo ela os principais tipos de ataques de *phishing* são:

- ***Blind Phishing***: É o mais comum, em que os e-mails são enviados para vários indivíduos sem nenhum critério, contando apenas com a sorte de encontrar usuários desavisados e os enganar.
- ***Spear Phishing***: Os alvos deste ataque possuem destinos específicos, por exemplo um grupo de pessoas, funcionários de uma empresa ou uma pessoa em particular. Sua finalidade é acessar informações privadas ou informações financeiras dessas pessoas.
- ***Clone Phishing***: Os atacantes criam uma cópia dos sites verdadeiros e, com isso, os usuários acabam preenchendo formulários maliciosos e os atacantes capturam informações desses usuários.

- ***Whaling***: Indivíduos do alto escalão da organização e o alvo desse ataque, como os diretores executivos ou figuras públicas relevantes, com o objetivo obter as informações relevantes ou apenas fazer ataques para prejudicar outra empresa, sob ordem da empresa em que eles trabalham.
- ***Vishing***: Nesse ataque os criminosos utilizam ferramentas de voz, como por exemplo uma ligação telefônica ou mensagens de voz. Os criminosos fingem ser uma autoridade legítima, uma empresa de cartão de crédito por exemplo, com isso eles tentam obter as informações confidenciais do usuário.
- ***Pharming***: Tem como objetivo corromper o Sistema de Nome de Domínio (DNS), assim levando os usuários para os sites falsos ao digitar URL legítimas. Neste caso mesmo que o usuário insira o endereço correto, ele pode ser direcionado para um site falso que foi projetado para roubar informações.
- ***Smishing***: É realizado por mensagens de texto, tem o objetivo de induzir o usuário a agir por impulso, constrangendo-o sobre dívidas que estão pendentes ou prometendo prêmios com valores atraentes.

2.1.1. Ransomware

O *ransomware* é um ataque cibernético específico que tem sido bastante mencionado nos noticiários. Este termo refere-se a um tipo de *software* malicioso o *malware* que é uma definição que engloba desde aplicativos espiões, *spywares* que monitoram e roubam dados, a *ransomwares*, que tem a capacidade de se infiltrar nos sistemas, criptografar os arquivos (Garret, 2021).

O *ransomware* é um tipo de *malware* que se infiltra nos sistemas de computador por de diversos meios, como por exemplo o *phishing* e *downloads* maliciosos. Ao entrar dentro do sistema, acontece o bloqueio no acesso dos arquivos ou à tela do computador. Os atacantes exigem um resgate para liberá-los, o pagamento para liberar o acesso e geralmente e feito através de criptomoedas como por exemplo as bitcoins (*Wickramasinghe*, 2023).

Alguns exemplos de *ransomware* que causaram prejuízos nos últimos anos, são descritos por *Wickramasinghe* (2023) abaixo:

- ***CryptoLocker***: Foi descoberto em 2013, ele criptografava os arquivos dos dispositivos *Windows* com chave pública *Rivest Shamir Adleman* (RSA), depois

exigia o resgate em criptomoeda, afetou mais de 250.000 sistemas e rendou aos criminosos pelo menos US$ 3 milhões em nove meses.

- ***WannaCry***: Descoberto em 2017, afetou sistemas *Windows* desatualizados que possuíam a vulnerabilidade *EternalBlue*, causando cerca de US$ 4 bilhões em danos e afetando cerca de 150 países.
- ***Petya***: O *ransomware Petya* foi descoberto em 2016, na qual ele criptografava o discos rígidos por completo e se propagava através de formulários de emprego falsos.
- ***W-2 Scareware***: Em 2017, os ataques de *scareware* foram responsáveis por roubarem formulários W2, esses formulários são documentos fiscais importantes para os Estados Unidos. Os funcionários recebiam vários spams de e-mails, o resultando desse ataque foi perdas de milhares de dólares.
- ***Maze***: Está ativo desde 2019, o *ransomware maze* ameaça vazar os dados que estão criptografados caso não houver o pagamento do resgate.
- ***Cerber***: É um *ransomware* de serviço popular em que ele criptografava silenciosamente os arquivos, além de tentar bloquear os recursos de segurança do *Windows*.
- ***Dharma***: Foi descoberto em 2016, em se espalha por meio de e-mails de spam e de vulnerabilidades no *Remote Desktop Protocol* (RDP).
- ***DarkSide***: Inicialmente atacou máquinas *Windows* e se espalhou para as máquinas *Linux*, atacando as máquinas *VMware* sem *patches* ou roubando as credenciais do *vCenter.*
- ***Bad Rabbit***: Apareceu em 2017, seu foco principal era as agências de mídia russas, mas acabou se espalhando através de sites afetados com atualizações falsas do *Adobe Flash*.

2.1.2. Ataque distribuído de negação de serviço

Uma estratégia maliciosa que tem como objetivo interromper o tráfego normal de um servidor, serviço ou rede é o DDoS. Sua finalidade é sobrecarregar o alvo com uma inundação de tráfego da Internet. Alguns desses ataques são bem-sucedidos devido ao uso de vários sistemas de computadores comprometidos como fontes de tráfego, incluindo dispositivos de Internet das Coisas (IoT). Fazendo uma comparação

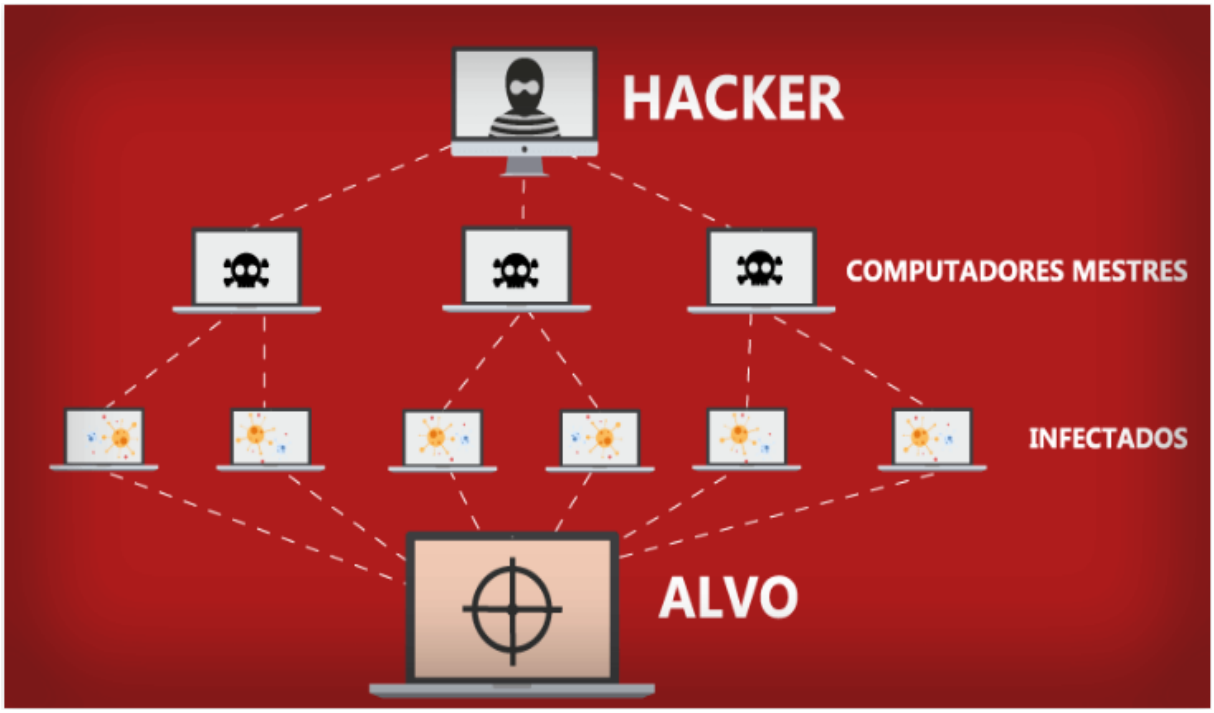
análoga um ataque DDoS seria com um engarrafamento repentino que impede o tráfego normal chegue ao seu destino (Cloudflare, 2024).

O DDoS é uma variação do Ataques de negação de serviço (DoS) um tipo de ataque malicioso que geralmente possuiu apenas um atacante, como por exemplo um único servidor ou computador que está sendo controlado por um hacker. No caso do DDoS, são múltiplos atacantes que se utilizar de computadores ou servidores, distribuindo e coordenando os ataques contra um único alvo, assim sobrecarregando o sistema deixando-o fora do ar (Gonçalves, 2023).

A Figura 3 mostra como é um ataque de DDoS, na qual os atacantes utilizam de várias máquinas infectadas com *malware*, chamadas de *bots*, algumas vezes utilizando milhares delas de diferentes endereços IP. Juntas essas máquinas formam uma *botnet* ou rede zumbi, os invasores as controlam de forma remota (*Wickramasinghe*, 2023).

Quando o ataque está acontecendo o *hacker* direciona a *botnet* para eles enviarem uma grande quantidade de tráfego ou solicitações para a máquina alvo, assim sobrecarregando o alvo e impossibilitando-o de responder. Isso resultará na negação de serviço e pessoas reais serão impedidas de acessar os sites ou sistemas afetados (*Wickramasinghe*, 2023).

Figura 3 – Ataque de DDoS



Fonte: Gonçalves (2023)

2.2. Modelos que descreve as etapas de um ataque cibernético

Cientistas de todo mundo estão dedicando seus esforços na modelagem de padrões e técnicas de ataques à segurança cibernética, analisando ataques feitos por pessoas mal-intencionadas. Em busca de entender e antecipar como os invasores podem agir, na quais estratégias podem ser empregadas e quais ações maliciosas eles podem tentar realizar (*Georgiadou*; *Mouzakitis*; *Askounis*, 2021).

O *Adversarial Tactics, Techniques, and Common Knowledge* (*MITRE ATT&CK*) é uma base de conhecimento que classifica é descreve ataques cibernéticos. Foi criado pela *Mitre Corporation* e lançado em 2013. A estrutura *ATT&CK* foi vagamente baseada na *Lockheed Martin Cyber Kill Chain*, com muito mais detalhes (*Wickramasinghe*, 2023).

Esse modelo apresentam uma abordagem sistemática para analisar e classificar as diferentes etapas de um ataque cibernético, desde a fase inicial de reconhecimento e planejamento até a execução e manutenção do acesso não autorizado ao sistema de destino (*InternationalIt*, 2023). A Figura 4 ilustra cinco funcionalidades do *MITRE ATT&CK*.

A Figura 4 – Aplicações do *MITRE ATT&CK*

Fonte: Traduzido de: *Wickramasinghe* (2023)

O *MITRE ATT&CK* é um *framework* que mantém uma base de dados sobre ameaças persistentes avançadas A*dvanced Persistent Threat* (APT). Ele categoriza as principais táticas, técnicas e procedimentos de diversos tipos de ameaças, oferecendo uma visão abrangente das diferentes fases do ciclo de vida de um ataque (Adriano *et al*.,2023).

Visando ajudar a criar modelos de ameaças distintos o MITRE *ATT&CK* aborda vários setores, incluindo empresas, governo e serviços de segurança cibernética. O *MITRE* utiliza de técnicas de ataque e das táticas dos adversários, para fornecer técnicas, que são utilizadas para detectá-los e eliminá-los (*Wickramasinghe*, 2023).

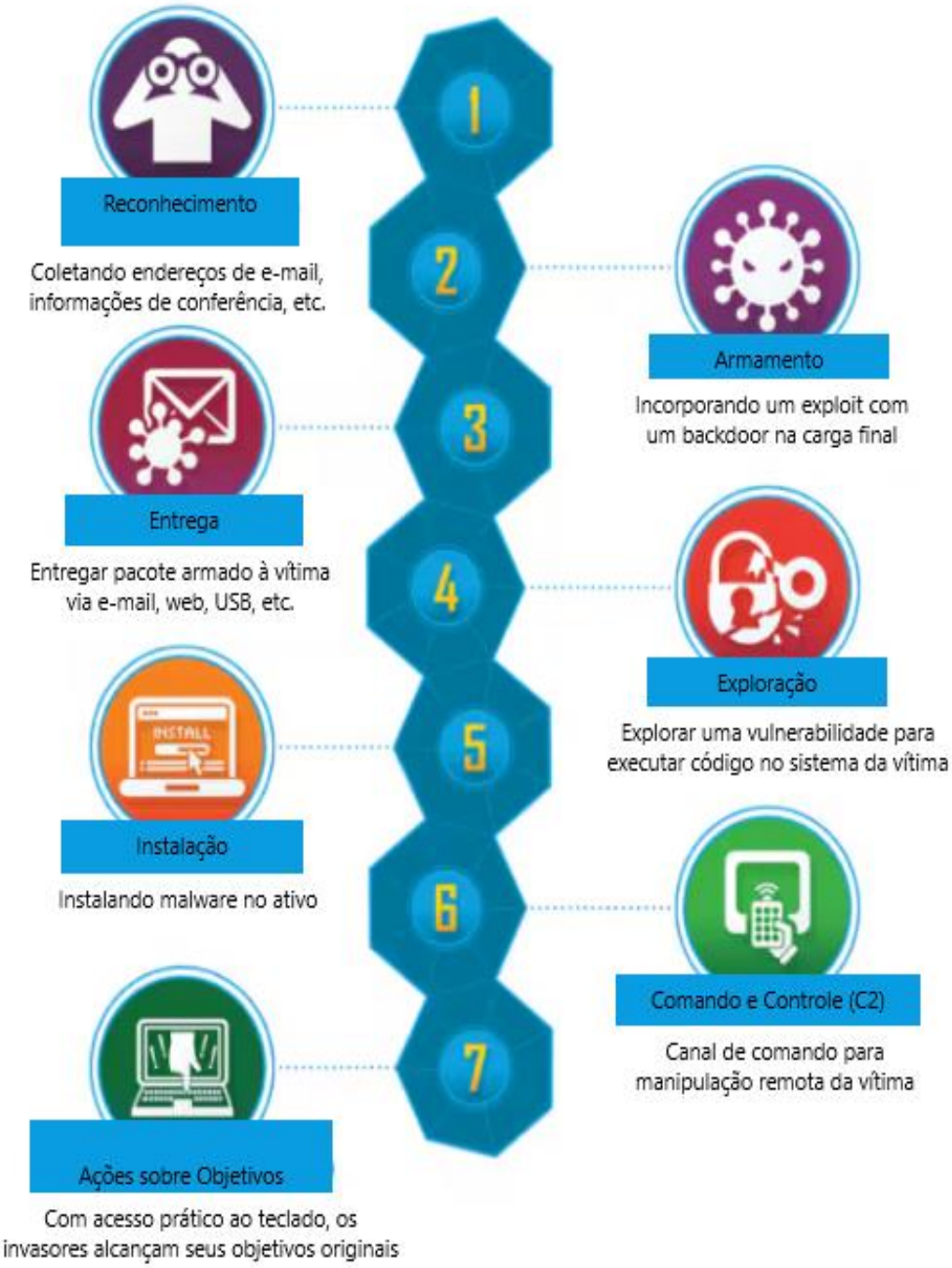
Outro modelo conhecido é o *Cyber Kill Chain,* utilizado para indicar diferentes estágios de um ataque, nos quais esses ataques podem ser aproveitados para desenvolver um plano de ação para impedir um ataque em andamento (*Yamin et al*.,2022).

O *Cyber Kill Chain* é frequentemente comparado à estrutura *MITRE ATT&CK*, no qual o ele também ilustra as fases de um ataque cibernético, sua principal diferença está no fato de que as táticas do *MITRE* não são listadas em nenhuma ordem específica, diferente do *Cyber Kill Chain* que mostra um agrupamento específico dos estágios (*Kidd*, 2022).

A estrutura do *Cyber Kill Chain* é orientada por inteligência, é utilizada para identificar a atividade de intrusão em uma operação cibernética, as etapas dos ataques utilizado por um invasor para atingir seus objetivos são definidos por essa estrutura (*Yamin et al*.,2022).

Segundo *Kidd* (2022) esse é o modelo mais utilizado nas indústrias. O modelo original da *Cyber Kill Chain* da *Lockheed Martin possui* sete estágios conforme apresentado na Figura 5, no qual cada estágio explora a metodologia e a motivação de um cibercriminoso e todo o cronograma do ataque. Isso ajuda as organizações a compreenderem e combater as ameaças.

Figura 5 – Fases do *Cyber Kill Chain*



Fonte: Traduzido de: *Kidd* (2022)

- **Reconhecimento:** Essa fase os invasores sondam os alvos para identifica vulnerabilidades e pontos para possíveis entrada, utilizando de diversas táticas como por exemplo a coleta de endereços de e-mail, ferramentas de espionagem e *scanners* automatizados.

- **Armamento:** As informações coletadas na fase anterior são utilizadas pelo atacante para cria ou modifica *malwares,* com o intuito de explorar os pontos vulneráveis do alvo.
- **Entrega:** Durante essa fase os atacantes tentam entrar na rede ou sistema do alvo, utilizando de técnicas de ataques cibernéticos como por exemplo o *phishing*, engenharia social ou exploram vulnerabilidades para instalar *malware* no sistema. Obtendo as permissões necessárias para ter acesso a dados confidenciais, os invasores tomam controle do sistema e causa danos significativos à organização.
- **Exploração:** Os atacantes tentam acessar outros sistemas viajando lateralmente através da rede da organização, tentando identificar pontos de entrada adicionais ao longo da rede.
- **Instalação:** O invasor tenta instalar *malware* e implantar outras ferramentas cibernéticas na rede alvo, para assim obter controle adicional de mais sistemas, como contas e dados do alvo.
- **Comando e controle:** Essa fase é crucial para o sucesso do ataque, pois permite o invasor monitorar as orientações remotas das atividades maliciosas. Técnicas de ofuscação são utilizadas pelos atacantes, como exclusão de arquivos, preenchimento binário e assinatura de código, com o objetivo de esconder sua presença no sistema, desviando a atenção das equipes de segurança. Os invasores podem também realizar ataques DoS em outros sistemas, com o objetivo de distrair e sobrecarregar o sistema causando a queda ou travamento do sistema.
- **Ação:** Essa fase de *Cyber Kill Chain* e a mais longa pode durar semanas ou meses, tem vários objetivos, tais como o *supply chain attacks*, *data exfiltration* ou criptografar os dados e destruição de dados. O ataque depende do objetivo dos invasores e das informações coletadas nas fases anteriores. Alguns exemplos são ataque a fornecedores de software para bancos, roubo de segredos comerciais de empresas e extorsão de dinheiro através de *ransomware*.

2.3. Gerenciamento de resposta a incidentes

Gerenciar incidentes significa identificar, administrar, registrar e analisar ameaças em eventos de segurança cibernética. Seu objetivo é reduzir o impacto nas operações comerciais é prevenir novas ocorrências. Utilizar essas práticas em qualquer empresa que tenha uma equipe responsável no tratamento de incidentes, facilita a execução um plano de resposta mais eficiente ao detectar qualquer anomalia (*Siddiqui*, 2023).

Para obter uma resposta eficiente a incidentes de segurança é preciso ter diversas funções e responsabilidades específicas, por exemplo o Comandante do Incidente que é responsável por todo o gerenciamento de processos de resposta, o operador de TI que monitora o sistema de TI e o Gerente de Incidentes que é responsável por lidar com os incidentes de grande escala. Existe outra função importante para o gerenciamento de incidentes, os Analistas de Incidentes eles analisam os dados, identificam à causa raiz e recomendam melhorias no processo de gerenciamento de incidentes (*Siddiqui*, 2023).

Um conjunto de ações estratégicas organizadas e realizadas por uma organização depois de um ataque cibernético ou alguma violação de segurança é chamada resposta a incidentes. Essas ações têm como propósito identificar rapidamente o ataque, mitigar seu impacto, conter danos e abordar a causa do ataque, com o objetivo de reduzir o risco de novos incidentes (*Watts*, 2023).

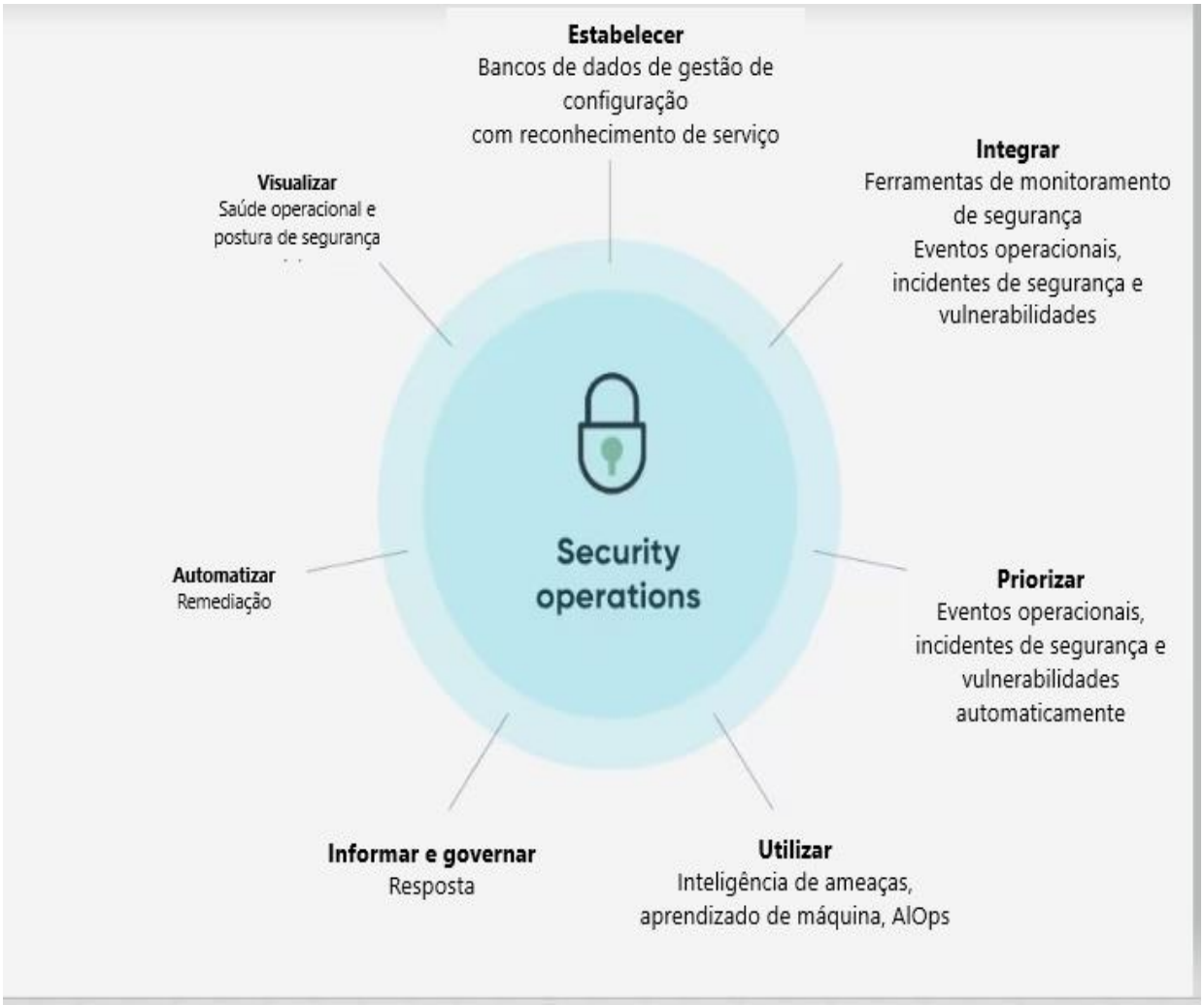
As ameaças cibernéticas podem causar diversos prejuízos, alguns deles são a violações de dados, perdas financeiras e danos à reputação. Uma resposta rápida que ajuda a diminuir os danos e o gerenciamento de resposta a incidentes que garante a conformidade legal, mantem a continuidade operacional e cria confiança com as partes interessadas (*Watts*, 2023).

2.3.1. Centro de operações de segurança

O *Security Operations Center* (SOC) é responsável por monitorar toda a infraestrutura tecnologia da organização, é composto de uma equipe interna ou terceirizada de profissionais de segurança de TI, na qual monitoram a e detectam eventos de segurança cibernética em tempo real, com prontidão e eficácia para

resolvê-los, seja por meio de medidas preventivas ou corretivas, visando garantir a proteção dos ativos digitais da empresa (*Ibm*, 2020). A Figura 6 ilustra sete funcionalidades do SOC.

Figura 6 – Funcionalidades do SOC



Fonte: Traduzido de: *Servicenow* (2024)

Os modelos de SOC disponibilizam programas de *software* como Serviço SaaS. A equipe de especialistas do SOC desenvolve uma estratégia de segurança cibernética, com operação ideal de 24 horas por dia, 7 dias por semana, para monitorar redes e *endpoints* de maneira constante. Se uma ameaça ou vulnerabilidade for identificada, o SOC trabalha com equipes de TI locais para elaborar uma resposta e investigar sua origem (*Servicenow*, 2024).

A equipe SOC tem sua área de atuação na parte de segurança cibernética de uma organização, concentrando seus esforços em prevenir, detectar e responder ameaças. Outras responsabilidades são realiza a monitorização constante de

identidades, dispositivos finais, servidores, bases de dados, aplicações de rede, páginas web e outros sistemas, com o objetivo de identificar possíveis ataques cibernéticos. Sem um SIEM, o SOC enfrentaria grandes dificuldades para desempenhar com eficiência sua missão (*Microsoft*, 2022).

O SIEM desempenha um papel de centralizador das diversas atividades do SOC, são eles o monitoramento, resposta a incidentes, gerenciamento de logs, relatórios de conformidade e aplicação de políticas. Apenas o log de um bom SIEM já se tornaria uma ferramenta necessária para qualquer SOC (*Kidd*, 2023).

2.3.2. SOAR

No SOC, os analistas são responsáveis por monitorar, detectar e responder a ameaças cibernéticas em tempo real, lidando com enormes volumes de dados de diversas fontes, como logs de sistemas operacionais, fluxo de rede, feeds de inteligência de ameaças e alertas de sistemas de antivírus e *Intrusion Detection Systems* (IDS) (*Bridges et al*., 2023).

Geralmente, esses centros utilizam uma plataforma de SIEM para consolidar esses dados, no entanto a triagem manual ainda é a norma, o que torna o processo demorado e propenso a erros. As ferramentas de *Security Orchestration Automation and Response* (SOAR) prometem aliviar essa carga ao integrar diferentes sistemas, automatizar tarefas rotineiras e facilitar a colaboração entre analistas, tornando o trabalho mais ágil e eficiente (*Bridges et al*., 2023).

O SOAR é uma tecnologia relativamente recente que busca trazer automação para muitas das tarefas manuais comuns, com o objetivo de aprimorar a eficiência e a consistência nas operações de segurança. Essa tecnologia fortalecer a postura de segurança das organizações (*Bridges et al*., 2023).

A implementação do SOAR ocorre de forma coordenada com o Centro de Operações de Segurança (SOC) de uma organização. Essas plataformas monitoram *feeds* de inteligência de ameaças e acionam respostas automatizadas para os problemas de segurança, auxiliando as equipes de TI na mitigação rápida e eficiente de ameaças em sistemas complexos (*Hat*, 2022).

2.4. Trabalhos Relacionados

Esta parte apresenta alguns trabalhos relacionados ao tema em estudo.

2.4.1. Análise e Detecção de Phishing com *Splunk*

O Trabalho de Conclusão de Curso (TCC) de Araújo (2019) descreve uma importante ferramenta contra ameaças cibernéticas, que é a análise e detecção de *phishing* com o *Splunk*. Segundo o autor uma das formas de ataques mais comuns é o *phishing,* por causa de sua facilidade de implementação e eficácia. Utilizando o *Splunk* como um SIEM na identificação e resposta contra esses ataques cibernéticos.

Os dados gerados por dispositivos em redes domésticas são usados pelo autor para identificar tentativas de fraude é acessos não autorizados. Utilizando a consulta dos logs e a detecção de anomalias, verificação de bloqueios e, caso necessário e feita a identificação de incidentes.

Com base nos estudos o autor conclui que o *Splunk* é uma abordagem eficiente para a proteção contra os ataques cibernéticos, destacando também a importância da conscientização dos usuários sobre a prevenção de ataques cibernéticos como uma medida adicional de segurança.

2.4.2. Detectando Anomalias usando *Machine Learning* no *Splunk*

Rocha (2023) pesquisou sobre como é feita a detecção de anomalias usando *machine learning* no *Splunk*. O autor destaca a importância da detecção de ataques cibernéticos e faz um alerta sobre as limitações das abordagens atuais que são baseadas em assinaturas. Além disso, o autor destaca a eficiência do *machine learning* utilizado na detecção de anomalias, pois é possível modelar o comportamento normal de sistemas para assim identificar as atividades suspeitas.

Foi introduzido o *Splunk App for Data Science and Deep Learning*, no qual são destacados os seus recursos utilizando-os para integrar o *Splunk* com algoritmos de *machine learning.* Os passos para as instalações dos programas são detalhados além

de como configurar o container *Docker* para obter os dados de exemplo para treinamento.

No trabalho o autor mostra como preparar os dados de *firewall* para análise e aborda a criação de um modelo de detecção usando *autoencoders*, uma arquitetura de redes neurais. O processo de implementação do modelo é feito no ambiente *Jupyter Notebo*ok.

O autor conclui que existe uma necessidade de superar as limitações das abordagens tradicionais de detecção de ciberataques e, para isso, à detecção de anomalias é uma solução promissora. Os modelos de detecção usando *autoencoders* e sua implementação no *Jupyter Notebook* fornecem uma base sólida para a aplicação prática dessas técnicas. Além disso a uma integração desse modelo com o *Splunk*.

2.4.3. *Ransomware* e Cibersegurança: A informação ameaçada por ataques a dados

O trabalho de Fornasier, Spinato e Ribeiro (2020) apresenta um contexto entre avanço tecnológico e a sofisticação dos crimes cibernéticos, mostrando que há uma preocupação aos ataques de *ransomware* em relação a proteção de dados igualando os dados a uma moeda real.

Os autores comparam os ataques feitos a empresas e pessoas comuns, fazendo uma pesquisa bibliográfica e mostrando alguns dos prejuízos mais comuns relacionado a ataques de *ransomware.*

Com base nos estudos os autores concluíram que esses ataques de *ransomware* são difíceis de rastrear e que as empresas não hesitam em pagar para ter seus dados roubados de volta, através de criptomoedas, tornando o rastreamento do dinheiro ainda mais difícil e a punição dos criminosos quase inexistente.

2.4.4. Crimes Cibernéticos, Privacidade e Cibersegurança

O estudo de Nolasco e Silva (2022) apresenta uma análise da evolução do Brasil no quesito cibersegurança, destaca os desafios enfrentados e as perspectivas para o futuro. Os autores argumentam sobre a necessidade de uma infraestrutura sólida para

governança cibernética e investimentos em educação e suporte, além disso, destaca a importância do fortalecimento das instituições para o combate aos crimes virtuais e a proteção dos dados e informações.

Para que tenha uma maior segurança jurídica no meio cibernético, o autor afirma que é necessário que as instituições responsáveis pela aplicação da lei sejam fortificadas. Isso inclui o aprimoramento das tecnologias de investigação, a capacitação de agentes e o apoio internacional para combater os crimes cibernéticos.

Os autores concluem que embora o Brasil enfrentar grandes problemas no campo da cibersegurança, ele já deu passos importantes para que tenha uma maior segurança de dados e proteção dos usuários nos meios cibernéticos. Mas ainda existe muito a se fazer, pois é essencial que haja investimento em infraestrutura, educação, suporte e fortalecimento das leis para enfrentar os desafios desse cenário que está sempre evoluindo.

3 MÉTODO

Quanto a natureza, esta pesquisa é um resumo de assunto. Baseia-se em apenas organizar uma área de conhecimento, indicando sua evolução histórica e estado de arte (*Wazlawick*, 2014).

Em relação aos objetivos, esta pesquisa é exploratória, caracterizando-se pela ausência de uma hipótese ou objetivo estritamente predefinido. Frequentemente, é considerada o estágio inicial de um processo de investigação mais abrangente (*Wazlawick*, 2014).

Nos procedimentos técnicos, esta pesquisa adota abordagens bibliográficas e documentais. A pesquisa bibliográfica baseou-se na análise de materiais publicados, incluindo livros, teses, recursos online e revistas científicas. Esse método permite oferecer uma visão ampla de diversos fenômenos, superando, em certos aspectos, as limitações de pesquisas diretas (Gil, 2022).

De acordo com Gil (2022), para realizar uma pesquisa bibliográfica é necessário seguir as seguintes etapas:

a) Escolha do tema: Estudo sobre soluções de ataques cibernéticos utilizando SIEM, com foco na plataforma *Splunk*.

b) Revisão preliminar da literatura: foi realizado o levantamento bibliográfico preliminar de periódicos e artigos relacionados ao assunto de pesquisa, para o pesquisador se habituar com a área de estudo escolhida. Foi utilizado as. bases de dados da CAPES, repositório de TCC da Pontifícia Universidade Católica de Goiás e Google Acadêmico.

c) Formulação da pergunta de pesquisa: **Como as empresas podem otimizar a segurança da informação e mitigar os riscos associados ao crime cibernético, usando tecnologias como o SIEM, com foco na plataforma *Splunk*?**

d) Identificação das fontes: Esta etapa envolveu a consulta a diversos recursos, como dissertações, periódicos científicos e obras de referência, entre outros.

e) Análise do conteúdo: foi examinado minuciosamente as informações coletadas, estabelecendo conexões diretas com a pergunta de pesquisa e foi avaliado a consistência dos argumentos apresentados em relação ao problema proposto.

f) Fichamento: O fichamento priorizou trabalhos altamente relevantes para a pesquisa. No entanto, documentos com contribuições de relevância média ou baixa também foram considerados, buscando enriquecer as reflexões do autor.

g) Escrita do Trabalho de Conclusão de Curso.

A pesquisa documental compartilha semelhanças metodológicas com a pesquisa bibliográfica, porém se diferencia principalmente pelas fontes utilizadas. Enquanto a pesquisa bibliográfica se fundamenta nas reflexões e contribuições de diversos autores sobre um tema específico, a pesquisa documental tem foco em materiais que já foram examinados anteriormente, mas que podem ser reinterpretados conforme os objetivos do estudo (Gil, 2022).

De acordo com Gil (2022), a pesquisa documental também é composta por etapas, porém este estudo se concentrará especificamente em uma delas, que é:

a) Análise e interpretação dos dados: foram analisados os documentos do site da *SPLUNK* e periódicos para descrever de forma objetiva, detalhada e com qualidade o conteúdo completo desta ferramenta.

4 SIEM Conceitos e Definições

O SIEM é uma estratégia de gerenciamento de segurança que integra as funcionalidades de Gerenciamento de Informações de Segurança (SIM) e

Gerenciamento de Eventos de Segurança (SEM), formando um sistema unificado para gerenciar eventos de segurança (*Rosencrance*; *Gillis*, 2023).

O SIEM desempenha a função de detectar ameaças e anomalias. A estratégia permite a análise de grandes volumes de dados em segundos para identificar e alertar sobre atividades incomuns. Essa capacidade de análise rápida torna o SIEM essencial, uma vez que realizar essa tarefa manualmente seria praticamente inviável (*Kidd*,2023).

O SIEM é um centralizador e correlacionado de eventos de logs de segurança, desempenha funções de análise, fornecer *insights* e diagnósticos de incidentes com base nos *logs* de eventos de várias *appliances*, como servidores (Medeiros, 2023). A Figura 7 ilustra o SIEM como um centralizador de todos os eventos.

Figura 7 –Centralizador de eventos SIEM

Fonte: Medeiros (2023)

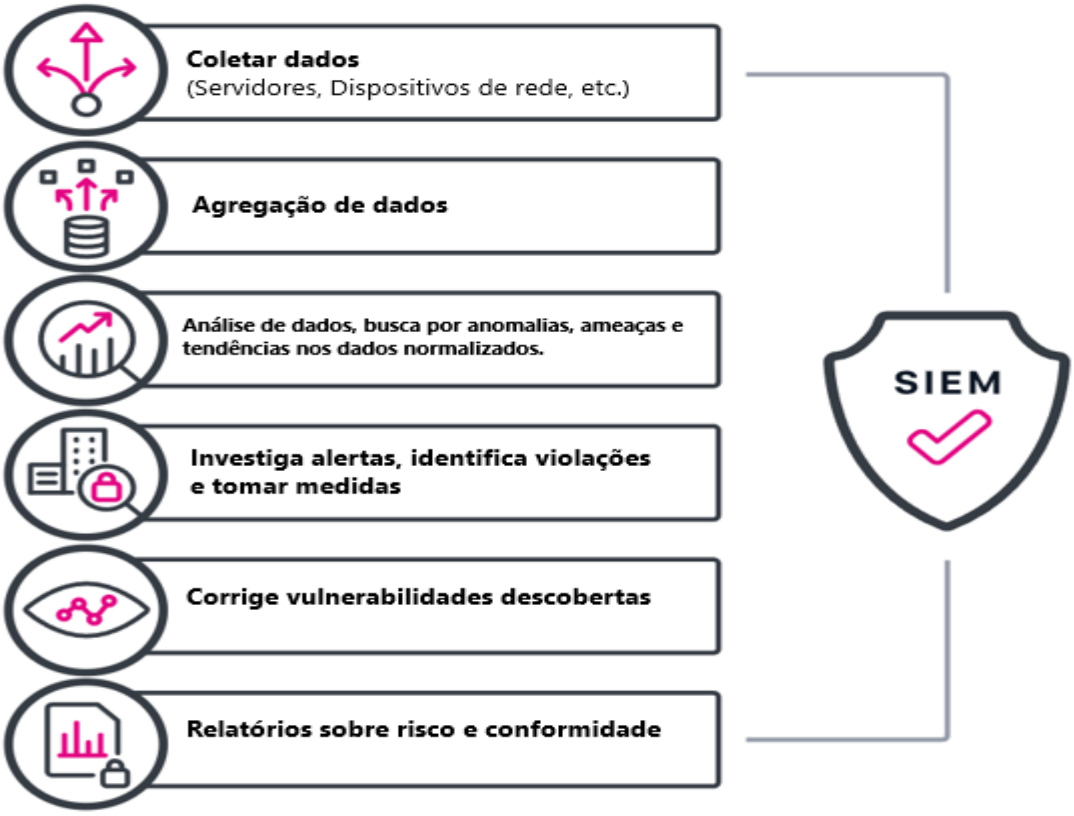
De acordo com Simas (2022), um SIEM deve oferecer as seguintes funcionalidades:

- Gerenciamento de log: Coleta e agregação de dados de diferentes dispositivos conectados à rede.

- Normalização: Organização e padronização dos dados coletados, facilitando a análise.
- Correlação de eventos: Comparação e análise de dados provenientes de diversas fontes para identificar padrões.
- Resposta a incidentes: Mapeamento e execução de ações necessárias com base em protocolos predefinidos para tratar ameaças reais ou identificar falsos positivos.

A Figura 8 ilustra a aplicação SIEM que reúne dados de fontes distintas dentro da sua infraestrutura de rede.

Figura 8 – Aplicações do SIEM



Fonte: Traduzido de *Kidd* (2023)

Várias empresas desenvolveram soluções de software SIEM para detectar ataques de rede e anomalias em infraestruturas de TI. Entre as grandes corporações que oferecem essas soluções estão HP, IBM, Intel e McAfee. Ferramentas inovadoras como o *Splunk* também surgiram nesse contexto, destacando-se pela eficiência e funcionalidades avançadas (Granadillo; Zarzosa; Diaz, 2021).

5 *SPLUNK*

O *Splunk* é uma solução tecnológica que se destaca por sua alta escalabilidade e eficiência, sendo especializada na indexação e pesquisa de arquivos de log de sistemas. Entre suas principais funcionalidades, está a análise de dados gerados por máquinas, o que oferece inteligência operacional valiosa. O *Splunk* possui independência de banco de dados para o armazenamento de informações, já que utiliza seus próprios índices para armazenar os dados (*Intellipaat*,2024).

O *Splunk* é classificado como um SIEM, uma ferramenta que não apenas armazena e pesquisa e analisa logs, mas também é capaz de indexar e identificar automaticamente padrões de dados. É utilizado na segurança de TI na proteção da rede de uma organização, sendo possível fazer o monitoramento contínuo do sistema, detectando de forma eficiente os eventos de segurança (Araújo, 2019).

Para um administrador de sistemas tentar diagnosticar um problema em seu sistema e se deparando com logs complexos e não estruturados, tais como o da Figura 9, seria extremamente trabalhoso identificar a ocorrência na falha sem gastar muitas horas decifrando cada palavra (*Vardhan*, 2024).

Figura 9 – Logs não estruturados

Fonte*: Vardhan* (2024)

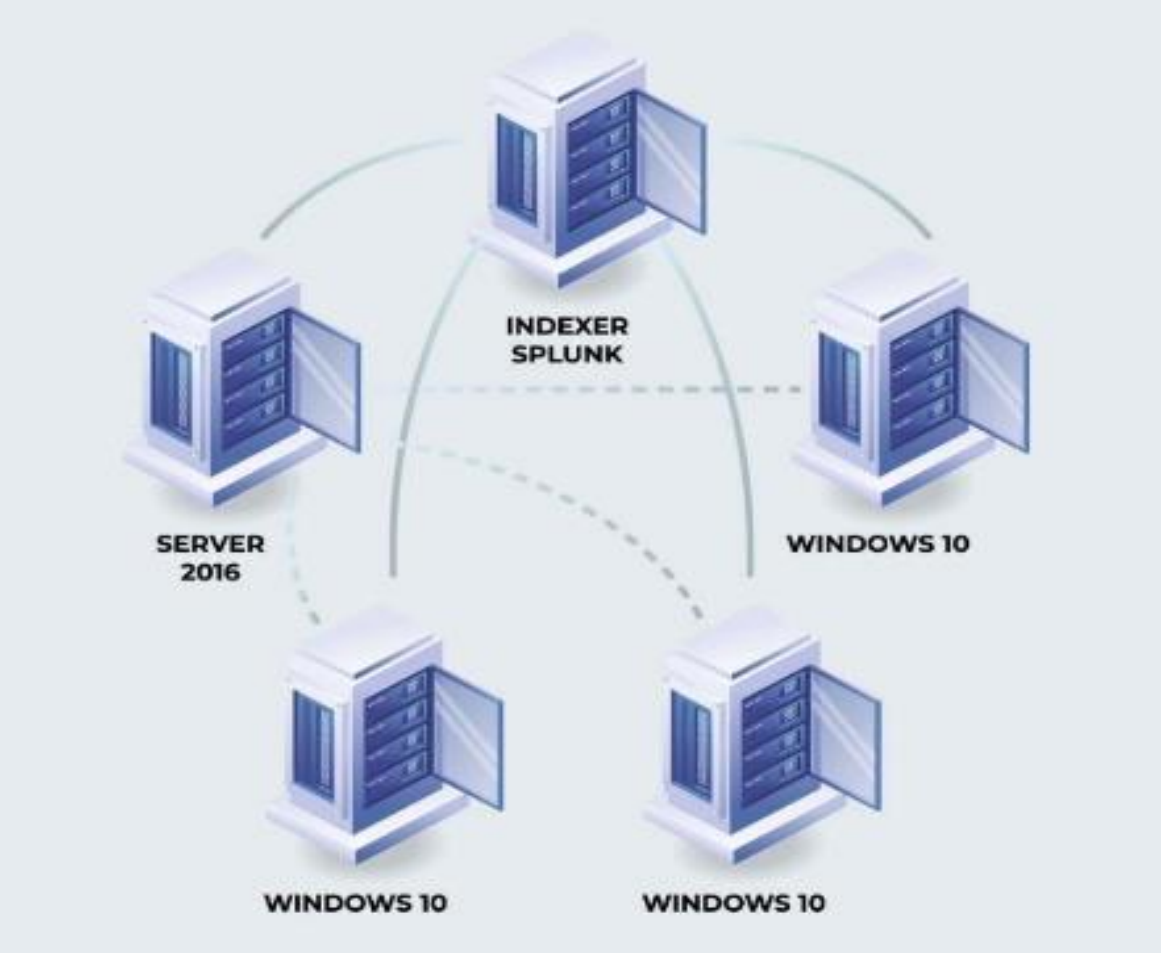
O *Splunk* facilita a extração de dados relevantes, simplificando a identificação e a compreensão de problemas. Inicialmente, era utilizado apenas para lidar com grandes volumes de dados, mas rapidamente tornou-se uma ferramenta indispensável no

mundo do *Big Data*, possibilitando análises avançadas e visualizações detalhadas (*Vardhan*, 2024).

Gerenciar grandes volumes de dados manualmente se torna inviável, devido a grande quantidade de linhas e colunas envolvidas. Para esse contexto é necessária uma ferramenta que seja capaz de administrar o fluxo contínuo de informações é lidar com possíveis interrupções (*Intellipaat*,2024).

O *Splunk* desempenha um papel importante nesse cenário, enfrentando os problemas de *overflows* massivos que ocorrem nos servidores web, ajudando o usuário fornecendo documentação de suporte (*Intellipaat*,2024). A Figura 10 mostra o *Splunk* em uma rede.

Figura 10 – Estrutura geral do *Splunk* em uma rede.

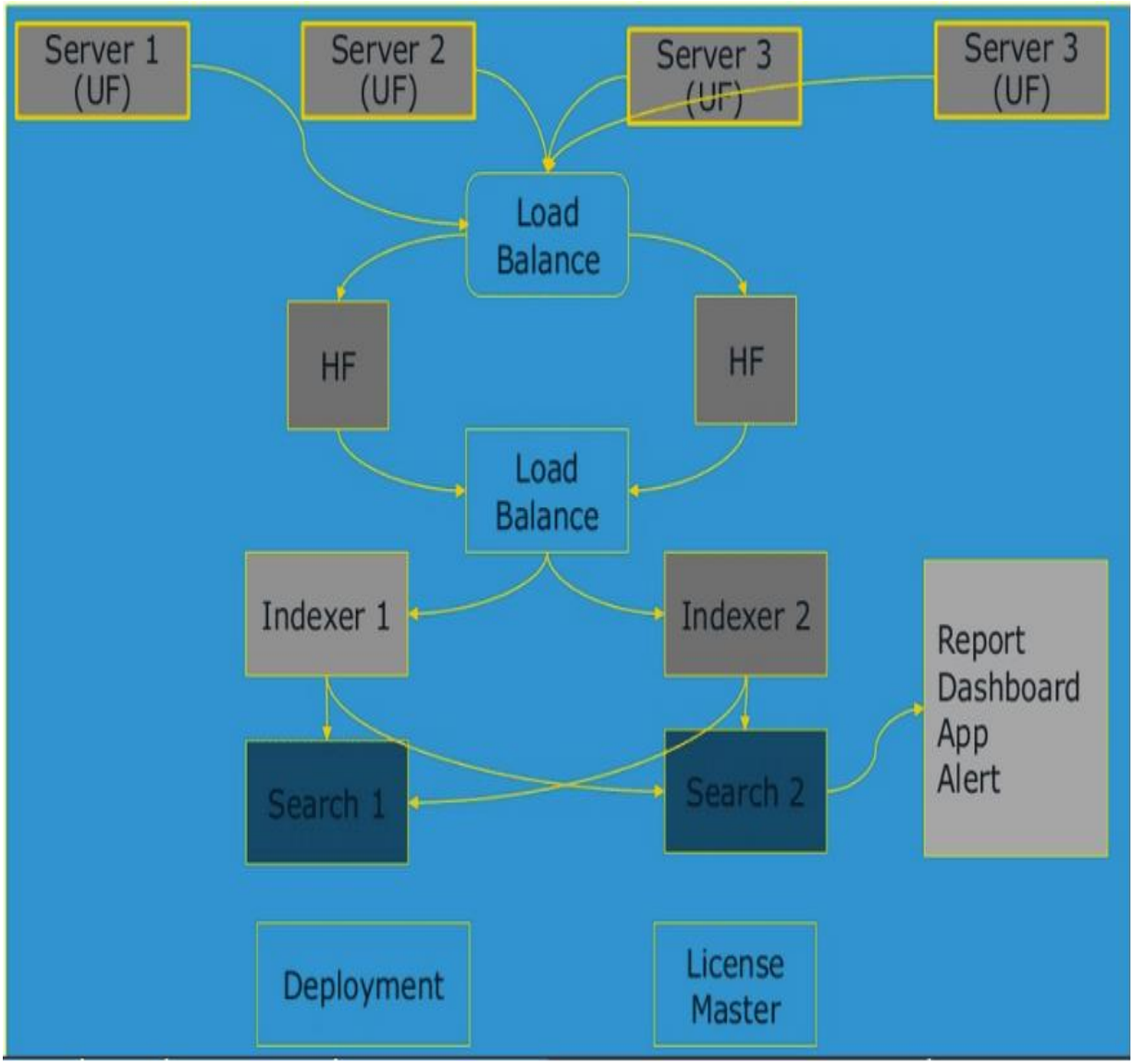


Fonte: *Elmastaş* e *Eyüpoğlu* (2023)

O *Splunk* funciona como um encaminhador, em que os dados de máquinas remotas são coletados e enviados para um índice. Em seguida um indexador processa esses dados em tempo real, depois armazena e indexando-os no disco. Por meio do

cabeçalho de pesquisa, os usuários finais acessam o *Splunk*, permitindo assim busca, análise e visualização os dados, como mostra a Figura 11 (*Fortinet*, 2024).

Figura 11 – *Splunk* como um encaminhador



Fonte: Fortinet (2024)

5.1. Arquivos de Log

Arquivos de log são registros gerados por softwares, contendo dados sobre atividades, operações e padrões de uso de aplicações, servidores ou sistemas de TI. Esses arquivos possuem um registro de histórico de todos os processos de eventos e mensagens, com informações detalhadas adicionais, por exemplo os carimbos de data/hora, esses carimbos mostram o que aconteceu internamente no sistema e quando aconteceu. Isso significa que, em caso de falha nos sistemas, há um registro

detalhado sobre todas as ações que ocorreram antes do incidente, permitindo uma análise detalhada do problema (Aws, 2023).

5.2. Gerenciamento de *logs* com *Splunk*

O gerenciamento de log é uma prática para tratar com grandes volumes de dados e mensagens de registro geradas por computadores, servidores, bancos de dados, sites, dispositivos de rede e *endpoints* entre outros sistemas é aplicações que geram registros. Os *logs* são informações sobre os eventos realizados nos sistemas, essas informações podem ser utilizadas para monitorar o desempenho do sistema e caso apareça alguma inconsistência os *logs* são uteis na solução de problemas que foram detectados (*Chia*, 2023).

As informações sobre eventos registrados nos sistemas podem ser utilizadas em diversas situações de negócios, como a identificação de violações de segurança, a resolução de problemas técnicos e o monitoramento do desempenho do sistema. Diversos órgãos reguladores exigem que as empresas tenham os seus dados de registro por um determinado tempo, com o objetivo de facilitar a regulamentações de conformidade, utilizando o gerenciamento de logs é possível cumprir esses requisitos de forma mais simplificada (*Chia*, 2023).

5.3. Correlação de eventos relacionados em logs com *Splunk*

Segundo *York* (2023) diversas técnicas são utilizadas para fazer a correlação de eventos é necessário identificar e associar os dados dos eventos, com o intuito para descobrir as causas dos problemas. A utilização de processos manuais é ineficiente, pois existem os *softwares* de correlação de eventos que usa algoritmos de aprendizado em uma máquina para identificar padrões em grandes conjuntos de dados. As técnicas mais comuns são:

- Baseado no tempo: Uma análise dos eventos é feita rapidamente antes ou durante um evento, com o objetivo de identificar as relações temporais. Permitindo aos usuários que eles estabeleçam um intervalo de tempo ou defina uma condição de latência para correlação.

- Baseado em regras: Os eventos são comparados com variáveis específicas, como por exemplo data e hora, tipo de transação ou localização do usuário. Uma nova regra é escrita para cada variável, muitas organizações não adotam esse tipo de abordagem pois acaba sendo inviável.
- Baseado em padrões: Utiliza-se de técnicas de tempo e regras para encontrar ligações entre os eventos, respeitando os padrões definidos.
- Baseado em topologia: É feito um mapeamento dos eventos para uma topologia dos dispositivos ou aplicativos de rede afetados, facilitando a visualização dos incidentes dentro do ambiente de TI.
- Baseado em domínio: Utiliza dos dados de monitoramento das áreas específicas das operações de TI, com esses dados é feita a correlação de eventos. No qual pode ser feita a coleta dos dados de todos os domínios é correlacioná-los entre si.
- Baseado em história: Uma comparação entre os eventos passados com os eventos atuais é feita, para uma melhor compreensão é ver se eles se coincidem. Semelhante a correlação baseada em padrões, sua diferença e que é feito apenas uma comparação de eventos idênticos.

O processo para a correlação de *log* é examinar um conjunto de eventos relacionados, baseada em regras definidas para interpretar os dados desses eventos. Ao ativar a correlação de log, é possível empregar uma identidade (ID) de correlação para identificar a origem de registros, seja uma solicitação de uma *User Interface* (UI), ou uma chamada *Representational State Transfer* (REST) na qual produziu a entrada de *log* (IBM, 2024).

No contexto de detecção de ataque a correlação de logs pode ser usada esses eventos, diversas atividades podem ocorrer simultaneamente. Analisando todos esses eventos em juntos, é possível compreender melhor o momento e a natureza do ataque. Durante um ataque, é possível identificar um usuário efetuando login em um servidor e instalando *software* em um sistema de arquivos sem autorização. Com a correlação de logs, é viável determinar o momento exato do ataque e os sistemas comprometidos (*Elmastaş; Eyüpoğlu*, 2023).

Equipes de TI são responsáveis por correlacionam logs de *softwares antivírus*, *firewalls,* entre outras ferramentas de segurança. Com o objetivo de obter informações sobre possíveis ameaças, com isso auxilia a detecção de violações de segurança é a

identificação de ameaças em tempo real. É possível utilizar essa prática por meio da integração do software de correlação de eventos de TI com o SIEM. Com essa integração e possível que os *logs* recebidos sejam correlacionados e normalizados, com isso simplifica a identificação de novos problemas de segurança (*York* ,2023).

5.4. Desvantagem do *Splunk*

O alto custo do *Splunk* para grandes volumes de dados já que ele utiliza um modelo de precificação baseado no volume de dados indexados e nos usuários ativos. Os custos são aumentados exponencialmente à medida que os volumes de dados crescem, o que torna inviável para algumas empresas (*Intellipaat*,2024).

A complexidade na otimização de pesquisas e a criação de consultas eficientes no *Splunk* pode ser um desafio, já que as abordagens para otimizar as pesquisas não segue um modelo claro ou padronizada. E necessário profissionais com experiência significativa no uso da plataforma ou então ir na tentativa e erro, o que pode impactar a produtividade (*Intellipaat*,2024).

A concorrência com soluções de código aberto e outra desvantagem pois o setor de TI tem buscado alternativas de código aberto que oferecem maior flexibilidade e menor custo. Essa concorrência representa um desafio constante para a adoção e retenção do *Splunk* no mercado (*Intellipaat*,2024).

6 INCIDENTE FORENSE

Com o uso cada vez mais comum de tecnologias nos ambientes corporativos, empresas e indivíduos tornam-se reféns dessas ferramentas. Consequentemente, os crimes cibernéticos estão se tornando cada vez mais frequentes e provar a ocorrência desses crimes não é uma tarefa simples (Raza, 2024).

A maior parte das evidências desses crimes encontra-se em computadores e dispositivos móveis. A ciência forense cibernética, um campo da segurança digital, busca coletar provas que possam levar cibercriminosos à justiça. Esse campo abrange desde a identificação e preservação até a análise e apresentação de evidências digitais em tribunais (Raza, 2024).

7 CIÊNCIA FORENSE CIBERNÉTICA

A sociedade está cada vez mais dependente de ferramentas tecnológicas digitais. Embora essa dependência traga inúmeros benefícios, também apresenta desafios significativos. Entre eles estão os crimes cibernéticos, que causam prejuízos tanto a indivíduos quanto a organizações e governos (Andrade, 2024).

Um setor essencial para combater esses crimes é a forense digital, que engloba todo o processo de investigação e solução de crimes cibernéticos, extraindo informações, analisando dados contribuindo para identificar e responsabilizar os autores de crimes digitais (Andrade, 2024).

A ciência forense cibernética teve início oficial na década de 1980, período em que os primeiros computadores pessoais começaram a se popularizar. A perícia cibernética evoluiu nesse contexto para lidar com novos tipos de evidências digitais, que surgiram à medida que os crimes migraram para o ambiente digital (Raza, 2024).

A análise forense cibernética garante conformidade legal e implementação de políticas de auditoria e, com isso, a integridade das informações são preservadas. Com ela é possível fazer uma conexão das práticas que são capazes de favorecer atividades criminosas (Raza, 2024).

De acordo com Raza (2024), as etapas de um procedimento forense cibernético incluem:

- Identificação: Determinação das evidências necessárias.
- Preservação: Etapa que visa garantir a integridade e a segurança das evidências.
- Análise: Busca entender os *insights* oferecidos pelas informações.
- Documentação: Consiste na criação e recuperação de dados, com isso é possível descrever a sequência de ações.
- Apresentação: Oferece uma visão estruturada dos insights extraídos, levando a uma conclusão.

Durante todas as etapas, os investigadores devem seguir procedimentos que assegurem a abrangência, objetividade, autenticidade e integridade das informações (Raza, 2024).

No Brasil, análise forense digital vem ganhando destaque com a Polícia Federal e as Polícias Civis. Os Estados estão implementando unidades especializadas em

forense digital com o objetivo de enfrentar o aumento no número crescente de crimes virtuais no país (Andrade, 2024).

A área de análise forense digital enfrenta dilemas éticos e técnicos, já que a tecnologia está sempre em evolução. Com os surgimentos da inteligência artificial e a IoT por exemplo, são inovações que por um lado proporcionam avanços, por outro elevam os riscos de ciberataques (Andrade, 2024).

A forense digital na segurança não se limita a crimes já cometidos. Essa área possui um papel fundamental na prevenção e na mitigação de riscos, fornecendo às organizações e indivíduos ferramentas e conhecimentos necessários para a proteção de um ambiente digita, que está, cada vez mais, perigoso (Andrade, 2024).

8 DESAFIOS NA CIÊNCIA FORENSE CIBERNÉTICA

Os especialistas enfrentam dificuldades na recuperação de dados criptografados, principalmente devido à falta de acesso a informações em sistemas de nuvem e à necessidade de lidar com grandes volumes de dados de logs de rede. Além disso, restrições legais e tecnologias ultrapassadas podem limitar a capacidade investigativa (Raza, 2024).

Apesar dos desafios, existem vários recursos disponíveis que conseguem auxiliar na segurança cibernética e análise forense, como os Institutos System *Administration, Networking and Security* (SANS) e o *National Institute of Standards and Technology* (NIST), entre outros institutos de tecnologia (Raza, 2024).

Com a efetivação de novas leis e padrões de conformidade, a análise forense cibernética torna-se cada vez mais necessária, impulsionando o crescimento desse campo tecnológico. Empresas que buscam processar cibercriminosos precisarão realizar esse tipo de análise para construir casos sólidos (Raza, 2024).

9 ANÁLISE COMPORTAMENTAL EM CIBERSEGURANÇA

A análise comportamental em segurança cibernética utiliza inteligência artificial e aprendizado de máquina para examinar grandes volumes de dados e identificar padrões incomuns que possam indicar atividades maliciosas. Essas análises são

utilizadas para detectar ameaças como roubo de dados, ataques DDoS, além de identificar comportamentos suspeitos de ameaças internas (*Wickramasinghe*, 2023).

Com a identificação dessas anomalias, as organizações utilizam da análise comportamental para detectar ameaças à segurança com antecedência, e com isso, consigam implementar melhores mecanismos de proteção. A análise comportamental pode ser utilizada em vários componentes conectados de uma organização, como usuários, dispositivos, redes e ambientes de nuvem (*Wickramasinghe*, 2023).

As ferramentas modernas de análise comportamental fornecem monitoramento em tempo real, *dashboards* interativos para visualização de dados, relatórios para auditorias de segurança e sistemas de alerta. Essas ferramentas não apenas detectam ameaças, mas também fornecem recomendações para melhorar da segurança geral (*Wickramasinghe*, 2023).

O processo da análise comportamental tem início com a coleta e transformação de dados, seguida pela análise usando algoritmos de *machine learning* para detectar anomalias e termina com alertas para as equipes de segurança. O sistema continua aprendendo e melhorando suas capacidades de detecção ao longo do tempo, tornando-se cada vez mais eficaz contra novas ameaças (*Wickramasinghe*, 2023).

Dois tipos de análise comportamental são a análise de comportamento de usuários e entidades, além da análise do comportamento da rede. Essas abordagens ajudam a identificar atividades suspeitas, como tentativas de login incomuns, uso não autorizado de recursos ou padrões de tráfego anômalos (*Wickramasinghe*, 2023).

A utilização de análise comportamental, focada no comportamento de usuários, tem se mostrado eficaz aumentando a segurança cibernética das organizações, deixando a identificação de ameaças mais avançadas, respostas rápidas a incidentes, e resolução de questões de conformidade. Utilizando essas práticas, as organizações estão mais bem equipadas para enfrentar os desafios de segurança atuais e evitar grandes perdas financeiras decorrentes de ataques cibernéticos (*Wickramasinghe*, 2023).

10 *SPLUNK DASHBOARD*

Os *dashboards* oferecem diversos tipos de visualizações, compostos por painéis. Esses painéis podem incluir módulos como caixas de busca, campos,

gráficos, tabelas e listas. Os painéis dos *dashboards* na maioria das vezes estão ligados a relatórios. Depois de criar uma visualização de busca ou salvar um relatório é possível adicionar essas informações a um novo *dashboard* ou apenas inserir em um já existente (Sinha, *Mukhopadhyay*, 2021).

Os *dashboards* do Splunk são amplamente acessados devido à sua fácil compreensão, permitindo contar histórias e facilitando o trabalho em equipe. Porém criar *dashboards* continuamente nem sempre agrega valor, é apenas uma maneira de transformar dados em ação de forma rápida (Li, 2022).

Os *dashboard*s possuem mecanismos de segurança, nos quais é possível mascarar ou criptografar os dados confidenciais dos usuários que estão visualizando o *dashboard*. No setor bancário as informações pessoais dos usuários devem ser mascaradas ou criptografadas antes de serem exibidas no *dashboard*, como dados bancários e informações de cartões por exemplo (Sinha, *Mukhopadhyay*, 2021).

A melhor prática para mascarar dados ocorre durante a gravação nos logs da aplicação. Caso isso não seja possível, recomenda-se mascarar os dados antes de transferi-los para o servidor *Splunk*. Esses dados sensíveis podem ser mascarados utilizando uma expressão regular simples (Sinha; *Mukhopadhyay*, 2021).

Os *dashboards* são feitos para contar uma história significativa, fornecer *insights* úteis as pessoas que estão visualizando, para que não precise ser recriado ou ajustado tornando-se obsoleto em pouco tempo. Os *dashboards* podem ser atualizados, reutilizados e ampliados, com isso, maximizando seis benefícios e obtendo *insights* de forma mais eficiente (Li, 2022).

10.1. Princípios e Melhores Práticas para *Dashboards*

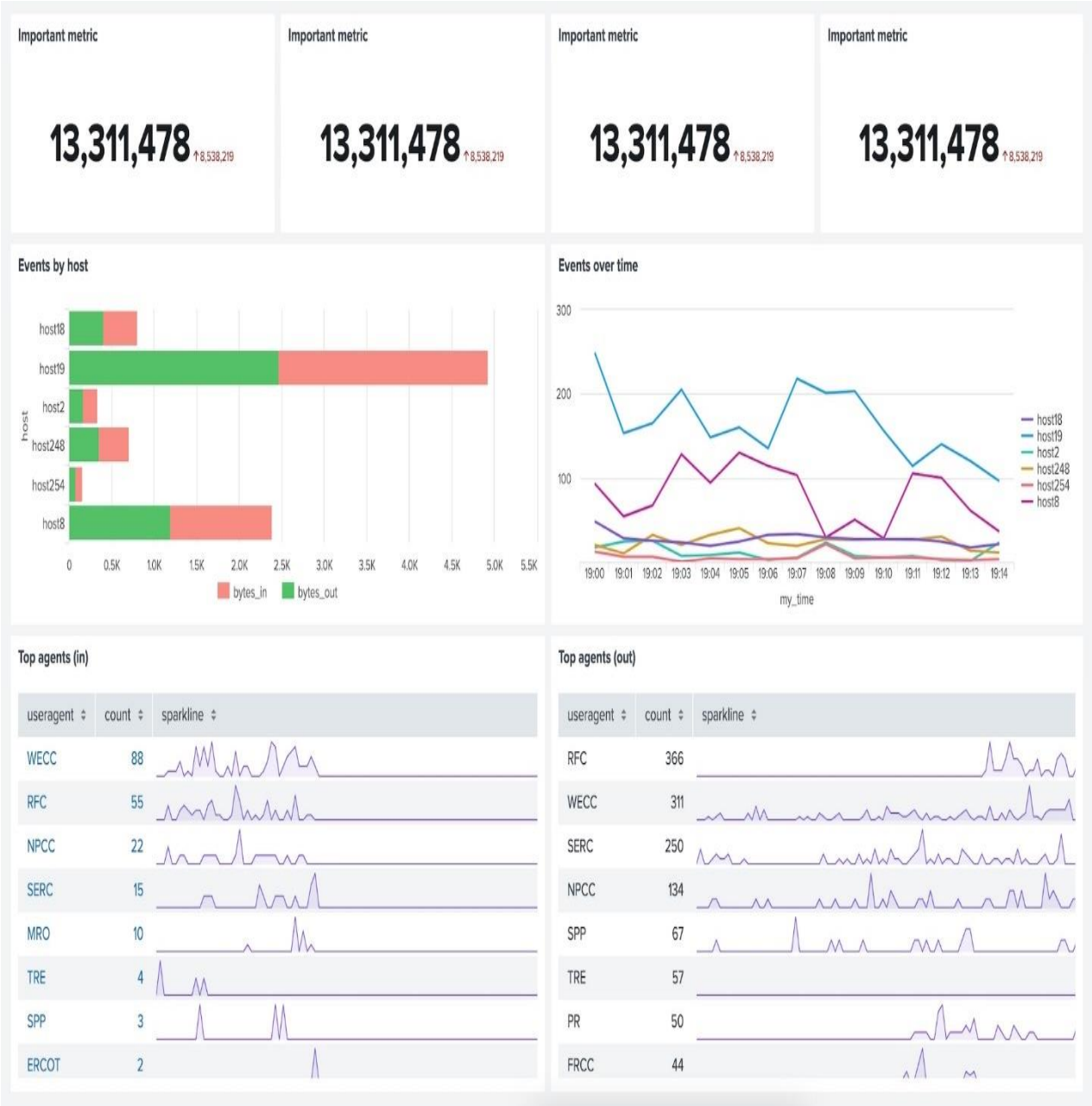
Segundo Li (2022) para começar um Design de *Dashboards* é necessário entender a história que será contada, além dos objetivos, ações e o público-alvo, esses resultados irão influenciar nas seguintes questões:

- Se é necessário a criação de um novo *dashboard* ou caso exista é feita apenas uma atualização nesse *dashboard.*
- Qual modelo usar.
- Quais partes do modelo devem ser atualizadas.
- Os dados que precisam ser coletados e exibidos.

10.2. Modelos e Exemplos de *Dashboard* no *Splunk*

O primeiro conjunto de exemplos fornece modelos para monitoramento. A Figura 12 mostra o monitoramento da postura de segurança. Este exemplo foi realizado utilizando o *Splunk Enterprise Security*. As métricas que estão no topo do *dashboard* são itens discretos listados lado a lado. Se itens estiverem conectados ou exista uma ocorrência em que os itens possam ser exibidos melhor, pode-se utilizar de outros modelos (Li, 2022).

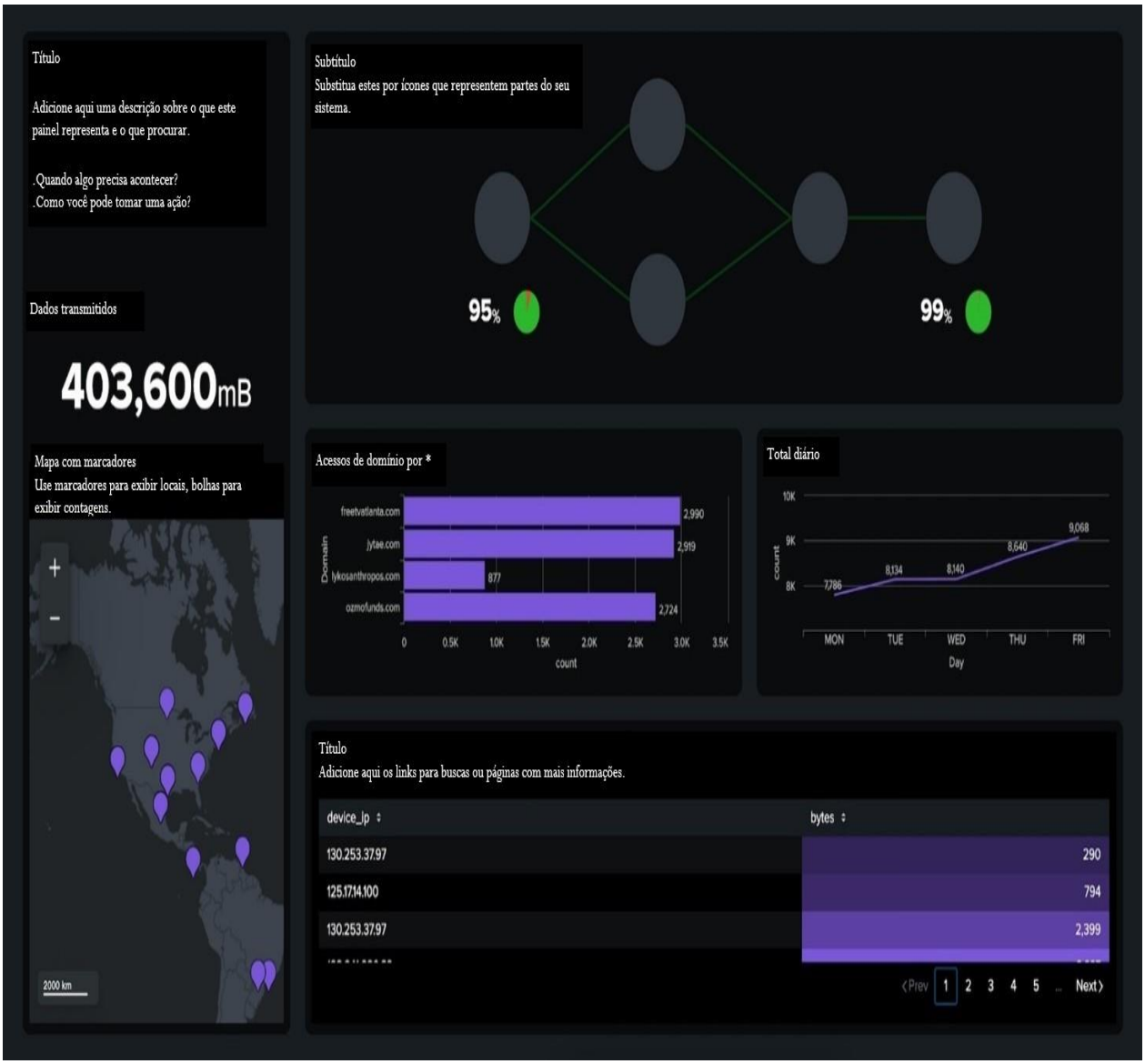
Figura 12 - *Dashboard* de monitoramento.



Fonte: Li (2022).

A Figura 13 utiliza de *layouts* em grade e absoluto. O *layout* em grade organiza de maneira natural os componentes e o *layout* absoluto exigem um cuidado extra com espaçamento e alinhamento adicionais, podendo também incluir formas de fundo. Essas formas devem ser utilizadas de forma discreta em termo de contraste, com um espaçamento adequado para não distrair os visualizadores das informações principais (Li, 2022).

Figura 13 - *Dashboard* com *layouts* em grade e absoluto.



Fonte: Traduzido de: Li (2022).

Segundo Li (2022) um *dashboard* de monitoramento deve fornecer contexto rápido, apresentar informações-chave e indicação de ações necessárias, além de informações de como executá-las. Reduzir o número de cliques e simplificar tarefas repetitivas para aumentar a eficiência é o que se espera desses *dashboards*. Dentro de uma única tela são incluídos alguns exemplos:

- Descrições e métricas no topo para assim oferecer contexto rápido de determinada tarefa, permitindo a compreensão de qualquer visualizador entender o que é mostrado;
- *Insights* sobre métricas ao longo do tempo ou por categoria para a compreensão do estado atual;
- Dados detalhados ao final para uma explicação mais profunda, com orientações sobre como agir quando for necessário.
- Mostrar apenas os componentes essenciais;
- A utilização de filtros que possibilita a adaptação das visualizações para diferentes situações;
- Utilizam cores para comunicar status;
- Fontes inteligentes como completo para o contexto da visualização.

11 ESTUDOS DE CASO COM *SPLUNK*

11.1. Fortalecimento da Cibersegurança em um Hospital com SIEM e *Splunk*

Em Portugal, um hospital de grande porte enfrentava problemas de segurança cibernética, principalmente devido à presença de sistemas críticos de informação médica, como o *Picture Archiving and Communication System* (PACS). Esses sistemas estavam interligados a vários dispositivos médicos e redes internas. Por causa disso o hospital se sentia vulnerável a ataques cibernéticos capazes de comprometer os dados sensíveis dos pacientes é parar o funcionamento dos serviços médicos (Coutinho *et al*., 2023).

A etapa inicial da implementação constituiu em integrar os sistemas críticos do hospital ao SIEM. Isso incluía o PACS, que é responsável pelo armazenamento de imagens médicas, servidores que gerenciam os dados hospitalares e os

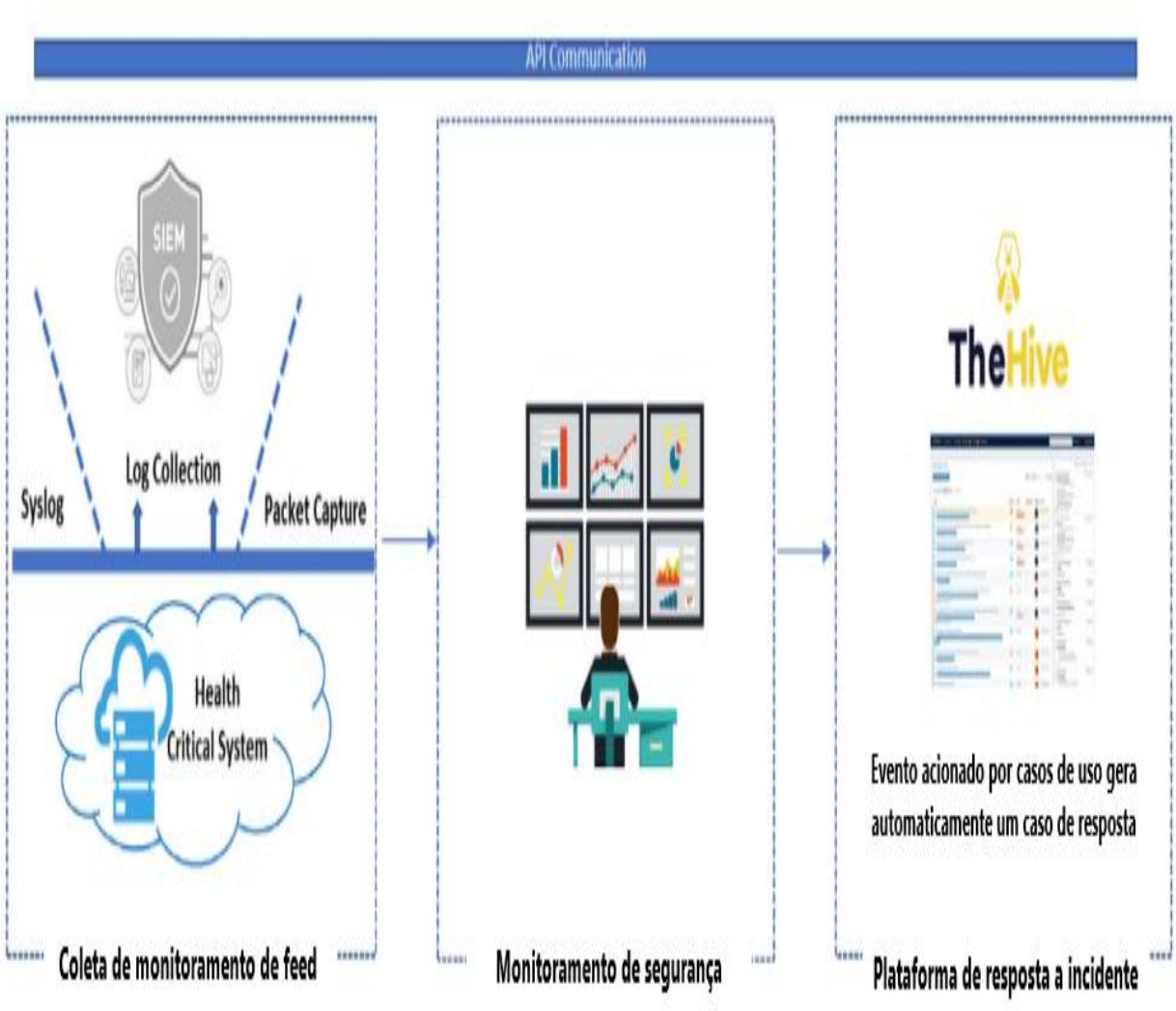
equipamentos médicos, como tomógrafos e aparelhos de ressonância magnética. As redes de comunicação interna foram incluídas na solução, já que nelas circulam dados sensíveis (Coutinho *et al*., 2023).

Para a visualização e análise desses dados, o *Splunk* foi escolhido como a ferramenta principal. Ele foi configurado para coletar logs de diferentes fontes, processar essas informações e fornecer alertas em tempo real sobre acessos não autorizados, comportamentos suspeitos e anomalias no tráfego de rede (Coutinho *et al*., 2023).

Com o SIEM e o *Splunk* configurados, a equipe de TI iniciou o monitoramento da infraestrutura do hospital, buscando indícios de possíveis ataques cibernéticos. Os pontos de seguranças que mais chamaram mais atenção durante o monitoramento foram as tentativas de login fora do horário de expediente ou após várias falhas de autenticação, indicando possíveis ataques de força bruta (Coutinho *et al*., 2023).

Respostas automáticas foram configuradas no sistema SIEM com o suporte do *Splunk*, com isso ao identificar um incidente, como por exemplo uma tentativa de login não autorizada ou um pico de tráfego inesperado, alertas eram gerados automaticamente e um registro do incidente era feito em uma plataforma de gerenciamento de incidentes, como o *TheHive*. A equipe de segurança do hospital era notificada imediatamente e procedimentos automáticos podiam ser iniciados, a Figura 14 mostra esse processo (Coutinho *et al*., 2023).

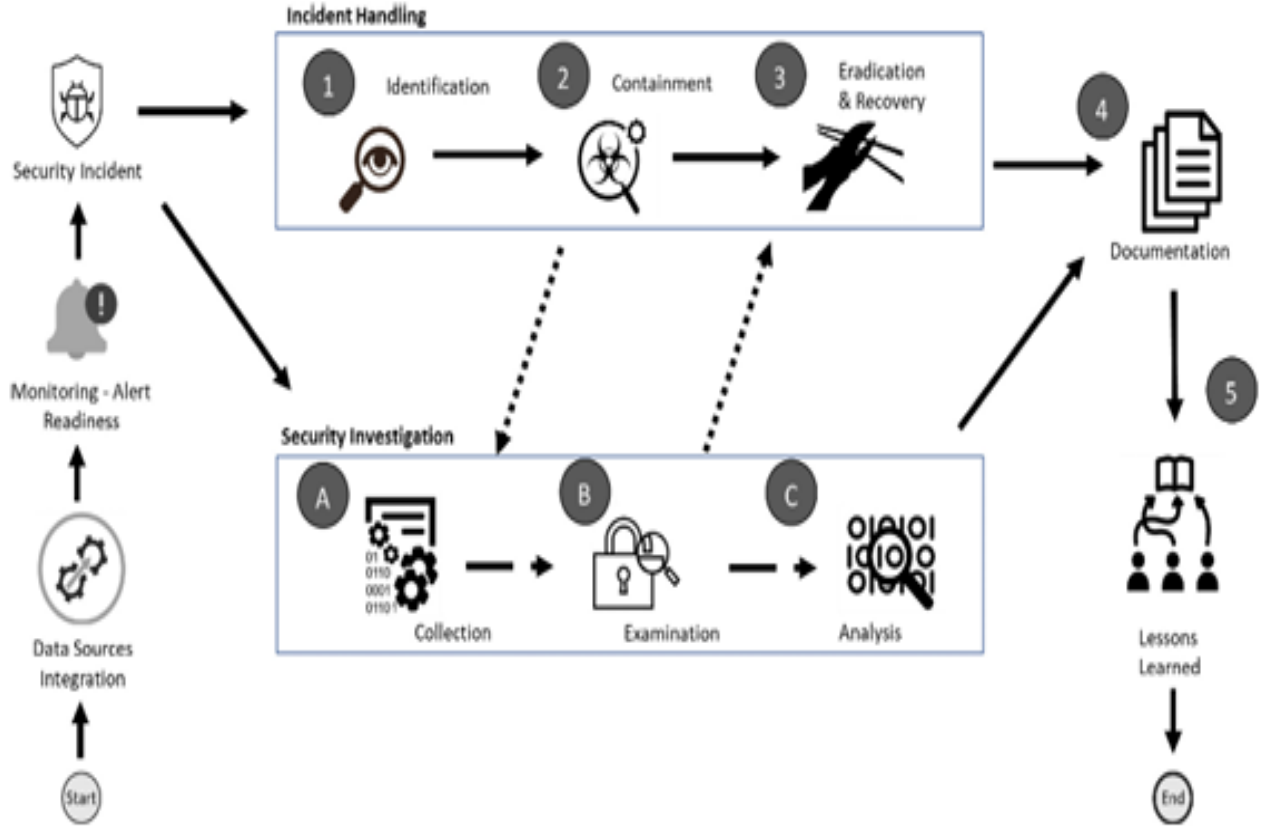
Figura 14 - Gerenciamento de incidentes e resolução de incidentes.



Fonte: Traduzido de: Coutinho *et al.* (2023).

Além da possibilidade de fazer monitoramento em tempo real, o *Splunk* possibilitou uma análise detalhada de logs, ajudando a equipe de TI na elaboração de relatórios periódicos sobre os incidentes de segurança, a Figura 15 mostra como é feita essa análise. Para a análise pós-incidente esses relatórios foram essenciais, pois lições valiosas foram retiradas deles. Levando a ajustes contínuos nas regras de segurança para que a detecção e a resposta a ameaças futuras sejam melhoradas (Coutinho *et al*., 2023).

Figura 15 - Procedimento completo de resposta a incidentes.



Fonte: Coutinho *et al*. (2023).

Como resultado, o hospital teve uma melhora significativa em sua segurança cibernética. Com a detecção antecipada das ameaças a equipe de TI conseguiu identificar e mitigar comportamentos suspeitos, como tentativas de acesso não autorizados e indícios de *ransomware*, antes que o sistema fosse afetado (Coutinho *et al*., 2023).

O tempo de resposta a incidentes foi significativamente reduzido, com isso os impactos de possíveis ataques foram reduzidos. O *Splunk* desempenhou um papel importante, permitindo à equipe de segurança identificar anomalias e reagir com agilidade devido a visibilidade que ele fornece sobre as atividades de rede e os dispositivos médicos (Coutinho *et al*., 2023).

11.2. Estudos De Caso na Empresa Puma

A PUMA, uma das principais marcas globais de esportes e vestuário, na qual enfrentava problemas na sua plataforma de e-commerce, resultando em perdas significativas de vendas e danos à reputação da marca. A falta de visibilidade sobre os problemas de pedidos dos clientes fazia com que a empresa perdesse milhares de dólares em vendas por hora (*Splunk*, 2024).

Ao adotar o *Splunk* Cloud Platform em parceria com a AIOPSGROUP, a PUMA conseguiu monitorar em tempo real os eventos em seus 45 sites de *e-commerce*, reduzir o tempo de detecção de problemas de horas para minutos, e resolver rapidamente questões críticas que poderiam impedir os clientes de concluir suas compras (*Splunk*, 2024).

11.3. Estudos De Caso no Instituto De Tecnologia De *Nova Jersey*

Outro exemplo de instituição que prioriza a integração de dados é o Instituto de Tecnologia de Nova *Jersey* (ITNJ). Com a plataforma *Splunk*, o ITNJ conseguiu combinar diversos fluxos de dados acadêmicos, de eventos e de infraestrutura, fortalecendo a segurança física e digital do campus (*Prevost*, 2024).

O ITNJ usa o *Splunk* para coletar dados não óbvios de várias áreas da experiência estudantil e do campus. Isso permite que as equipes de TI monitorem o progresso da universidade em relação a objetivos críticos, como aumentar a presença no campus. Essa estratégia contribuiu para um aumento impressionante de 28% na matrícula nos últimos anos (*Prevost*, 2024).

A equipe de TI do ITNJ utiliza o *Splunk Observability* Cloud e o *Splunk Synthetic Monitoring* para observar atividades em toda a infraestrutura do campus, prevenindo e respondendo melhor a interrupções. Com uma visão completa do ambiente em nuvem, o ITNJ consegue identificar problemas e atualizar aplicativos antes de momentos críticos, como inscrições e exames, evitando interrupções para os estudantes (*Prevost*, 2024).

O INTJ também se destaca por seu SOC movido por estudantes, em parceria com a *Splunk*. O uso da *Splunk* pelo ITNJ para integrar dados em sua infraestrutura mostra como a visibilidade abrangente dos dados pode impactar positivamente a

experiência estudantil, servindo como um exemplo para outras universidades (*Prevost*, 2024).

12 CONCLUSÃO

Este projeto teve o intuito de responder a seguinte questão de pesquisa: Como as empresas podem otimizar a segurança da informação e mitigar os riscos associados ao crime cibernético, usando tecnologias como o SIEM, com foco na plataforma *Splunk*?

O estudo destacou a crescente preocupação com a segurança cibernética e os danos que ataques podem causar às empresas, incluindo perda e roubo de dados, além de prejuízos financeiros. Existem diversas técnicas de ataques cibernéticos, algumas mais comuns tais como o *phishing*, DDoS e *ransomware*, mostrando que há uma constante adaptação dos atacantes em relação às medidas de segurança. Alguns modelos descrevem as etapas de um ataque cibernético - dois deles são o *MITRE ATT&CK* e o *Cyber Kill Chain. E*sses modelos possibilitam as organizações compreenderem melhor as táticas dos invasores, permitindo o desenvolvimento de estratégias mais eficazes contra-ataques cibernéticos.

O SOC é responsável por monitorar toda a infraestrutura tecnologia da organização, e composto de uma equipe interna ou terceirizada de profissionais de segurança de TI, na qual monitoram a e detectam eventos de segurança cibernética em tempo real, a equipe SOC tem sua área de atuação na parte de segurança cibernética de uma organização, concentrando seus esforços em prevenir, detectar e responder ameaças.

Além disso, o SOAR busca trazer automação para muitas das tarefas manuais comuns, com o objetivo de aprimorar a eficiência e a consistência nas operações de segurança. A implementação do SOAR ocorre de forma coordenada com o SOC de uma organização. Essas plataformas monitoram *feeds* de inteligência de ameaças e acionam respostas automatizadas para os problemas de segurança.

Conclui-se que um SIEM centraliza e correlaciona os eventos de logs de segurança de diversas fontes, com isso é possível analisar de forma mais abrangente, identificando os padrões suspeitos. O *Splunk* é um SIEM altamente escalável e

eficiente, além de possuir a vantagem na indexação e na pesquisa de arquivos de log, facilitando a análise de grandes volumes de dados.

Além disso, a ciência forense cibernética consiste em extrair informações, analisar dados e obter inteligência que possa ser apresentada em um tribunal como provas, garantindo conformidade legal e implementação de políticas de auditoria e, com isso, a integridade das informações são preservadas. Com ela é possível fazer uma conexão das práticas que são capazes de favorecer atividades criminosas.

Concluiu-se que as empresas podem aprimorar a segurança cibernética e reduzir riscos utilizando o *Splunk* como SIEM. Essa ferramenta permite centralizar e correlacionar eventos de segurança, possibilitando análise em tempo real, identificação de padrões maliciosos e gerenciamento avançado de logs. Com todas essas ferramentas para a análise de grandes volumes de dados, o *Splunk* acaba sendo muito útil para as empresas na proteção contra ameaças cibernéticas.

Para continuidade deste trabalho sugere-se:

- Utilizar a Inteligência Artificial integrada com *Splunk* para prevenir ou identificar ataques.
- Investigar soluções de monitoramento e resposta a incidentes para proteger dispositivos IoT.

13 REFERÊNCIAS

ADRIANO T.P., ROCHA A., OLIVEIRA C.E.B.O., ALMEIDA F. **USO DE UMA FERRAMENTA DE GESTÃO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO PARA DETECÇÃO DE ATAQUES CIBERNÉTICOS.** Revista Foco, 2023**.** Disponível em: <10.54751/revistafoco.v16n10-063>. Acesso em: 10 março 2024.

ANDRADE, Ingrid Lima. **Forense digital aplicada ao combate de crimes cibernéticos: uma revisão**. DOI: <10.54751/revistafoco.v17n7-152>. Revista Foco, 2024. Acesso em: 14 out. 2024.

*AKAMAI***. O que é um ataque cibernético ou ciberataque?** *AKAMAI***,** 2024 Disponível em:< https://www.akamai.com/pt/glossary/what-is-a-cyber-attack>. Acesso: 8 abril 2024.

ARAÚJO, Allan de Lima. **Análise e Detecção de Phishing com *Splunk*.** 2019. Trabalho de Graduação (Graduação em Ciência da Computação) - Centro de Informática, Universidade Federal de Pernambuco, Recife, 2019.

AWS**. O que são arquivos de log?** AWS, 2023. Disponível em: <https://aws.amazon.com/pt/what-is/log-files/>. Acesso em: 30 de março de 2024.

CHIA A***. Log Management: Introduction & Best Practices***. *Splunk*, 2023 Disponível em: <https://www.splunk.com/en_us/blog/lear n/logmanagement.html#:~:text=One%20popular%20log%20management%20option, monitoring%20and%20analysis%20of%20logs>. Acesso em: 30 de março de 2024.

*CLOUDFLARE***. O que é ataque de DDoS?** *CLOUDFLARE*, 2024. Disponível em: <https://w ww.cloudflare.com/pt-br/learning/ddos/what-is-a-ddos-attack/>. Acesso em: 4 de maio 2024.

COUTINHO B.; FERREIRA J.; YEVSEYEVA I.; FERNANDES V.B. ***Integrated cybersecurity methodology and supporting tools for healthcare operational information systems*****.** *Computers & Security*, 2023. Acesso em: 14 out. 2024.

ELMASTAŞ, M. S.; *EYÜPOĞLU*, C. ***Detection of Current Attacks in Active Directory Environment with Log Correlation Methods: Aktif Dizin Ortamındaki Güncel Saldırıların Log Korelasyon Yöntemleri ile Tespiti*****.** *Journal of Aeronautics and Space Technologies*. Disponível em: <https://jast.hho.msu.edu.tr/index.ph p/JAST/article/view/540>. Acesso em: 3 março 2024.

FORNASIER, M. O.; SPINATO, T. P.; RIBEIRO, F. L. **Ransomware e cibersegurança: a informação ameaçada por ataques a dados**. Revista *Thesis Juris*, 2020. DOI: <10.5585/rtj.v9i1.16739>. Disponível em: <https://periodicos.unin ove.br/thesisjuris/article/view/16739>. Acesso em: 20 abril 2024.

FORTINET**. O que é *Splunk*?** *FORTINET*, 2024 Disponível em: <https://www.fortinet.co m/resources/cyberglossary/what-is-splunk>. Acesso em: 28 de abril 2024.

GEORGIADOU A.; MOUZAKITIS S.; ASKOUNIS D. ***Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework****.* Sensors, 2021. Disponível em: <https://doi.org/10.3390/s21093267>. Acesso em: 11 março 2024.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa. 7. ed.** São Paulo: Editora Atlas Ltda., 2022.

GONÇALVES A. **DDoS: O que é, Como funciona e Como se Proteger de Ataques Maliciosos na Internet.** *Hostinger*, 2023. Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-ddos-e-como-se-proteger-de-ataques>. Acesso: 2 maio 2024. **O que é phishing e como se proteger de golpes na internet.** *Hostinger*. 2021. Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-phishing-e-como-se-proteger-de-golpes-na-internet#Como-se-proteger-de-ataquesphishing>. Acesso em: 2 maio 2024.

GRANADILLO, G.G; *ZARZOSA*, G.Z.; *DIAZ*, R. ***Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures****.*

Sensores ,2021. Disponível em: <https://doi.org/10.3390/s21144759>. Acesso em: 1 de março 2024.

*HISCOX**. The Hiscox Cyber Readiness Report 2023***. *HISCOX**,*** 2023 Disponível em: <https://www.hiscox.co.uk/cyberreadiness>. Acesso em: 3 março 2024.

IBM***. Security Operations Center (SOC).*** IBM, 2020. Disponível em: <https://www.ibm.com/br-pt/topics/security-operations-center>. Acesso em: 11 março 2024. **Correlação de eventos relacionados em logs**. IBM, 2024. Disponível em: <https://www.ibm.com/docs/pt-br/mas-cd/maximo-manage/continuous-delivery?topic=filter-correlation-related-events-in-logs>. Acesso em: 27 de março 2024.

*INTELLIPAAT***. O que é *Splunk*? Um guia para iniciantes.** *INTELLIPAAT*, 2024. Disponível em: **<**https://intellipaat.com/blog/what-is-splunk/>. Acesso em: 27 de março 2024.

*INTERNATIONALIT***. O que é MITRE ATT&CK e como usar esse framework?** *INTERNATIONALIT*, 2023. Disponível em: **<**https://www.internationalit.com/post/o-que-é-mitre-att-ck-e-como-usar-esse-framework>. 1 de set. de 2023. Acesso em: 12 março 2024.

*KIDD, Chrissy**. Cyber Kill Chains Explained: Phases, Pros/Cons & Security Tactics.*** *Splunk*, 2022. Disponível em: <https://www.splunk.com/en_us/blog/learn/cyber-kill-chains.html>. Acesso em: 10 março 2024. KIDD C. **SIEM: Security Information & Event Management Explained.** *Splunk*, 2023. <https://www.splunk.com/enus /blog/learn/siem-security-information-event-managem ent.html>. Acesso em: 1 de março 2024.

*KIDD, Chrissy. **SIEM: Security Information & Event Management Explained***. *Splunk*, 2023. Disponível em: <https://www.splunk.com/en_us/blog/learn/siem-security-information-event-managem ent.html>. Acesso em: 11 março 2024. *KIDD C. **SOCs: Security Operation Centers Explained**. Splunk*, 2023. Disponível em: <https://www.splunk.com/en_us/blog/learn/soc-security-operation-center.html>. Acesso em: 11 março 2024.

LALLIE H.S.; *LYNSAY* A.S.; *JASON* R.C.N.; *EROLAD* A.; *EPIPHANIOUA* G.; *MAPLE* C.; *BELLEKENS* X. ***Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic***. Elservier, 2021. <https://doi.org/10.1016/j.cose.2021.102248>. Acesso em: 3 de março 2024.

LI, Lizzy. ***Dashboard Design: Getting Started With Best Practices*** **(Part 1).** *Splunk*, 01 set. 2022. Disponível em: <https://www.splunk.com/blog/dashboard-design-best-practices-part-1.html>. Acesso em: 10 set. 2024.

MEDEIROS, Rafael. **Gestão de Logs com SIEM.** Medium, 2023. Disponível em: <https://medium.com/@rafael.mmedeiros/gestão-de-logs-com-siem-cac5a748c82d>. Acesso em: 10 março 2024.

MICROSOFT**. O que é um SOC (centro de operações de segurança)?** MICROSOFT, 2022. Disponível em: <https://www.microsoft.com/pt-br/security/business/security-101/what-is-a-security-operations-center-soc>. Acesso em: 11 março 2024.

NOLASCO, L. G.; SILVA, B. D. M. **Crimes cibernéticos, privacidade e cibersegurança**. Revista *Quaestio Iuris*, 2022. DOI: 10.12957/rqi.2022.67976. Disponível em: <https://www.e-publicacoes.uerj.br/quaestioiuris/article/view/67976>. Acesso em: 20 abril 2024.

PONTES R.A.B.; RICE A.E.; OESCHA S.; NICHOLS J.A.; WATSONA C.; SPAKES K.; NOREMA S.; HUETTEL M.; JEWELL B.; WEBER B.; GANNONA C.; BIZOVI O.; HOLLIFIELDA S.C.; ERWINB S. ***Testing SOAR tools in use*****.** Disponível em: <https://doi.org/10.1016/j.cose.2023.103201>. Elsevier, 2023. Acesso em: 12 março 2024.

PREVOST, Mary Lou. **Data Integration for Higher Education: An NJIT and *Splunk* Case Study.** *Splunk*, 2024 Disponível em: <https://www.splunk.com/en_us/blog/conf-splunklive/data-integration-for-higher-education-an-njit-and-splunk-case-study.html>. Acesso em: 01 set. 2024.

RAZA, Muhammad . ***Phishing Scams & Attacks: A Complete Guide.*** *Splunk*, 2023. Disponível em: https://www.splunk.com/en_us/blog/learn/phishing-scams-attacks.html**.** Acesso: 2 maio 2024. ***What Is Cyber Forensics?*** *Splunk*, 2024. Disponível em: <https://www.splunk.com/en_us/blog/learn/cyber-forensics.html>. Acesso em: 24 de agosto 2024.

REDHAT***. SOAR | Security Orchestration Automation and Response.*** REDHAT, 2024. Disponível em: <https://www.redhat.com/pt-br/topics/security/what-is-soar>. Acesso em: 12 março 2024.

ROSENCRANCE L.; GILLIS A.S.G. **SIEM ou gerenciamento de eventos e informações de segurança**. Disponível em: <https://www.computerweekly.com/br/definicoe/SIEM-ou-gerenciamento-de-eventos-e-informacoes-de-seguranca>. *TechTarget*, 2023. Acesso em: 09 março 2024.

ROSSI L.C. **Ataque cibernético: O que é e como você pode proteger a sua empresa desse mal.** Euax, 2024. Disponível em: <https://www.euax.com.br/2024/03/ataque-cibernetico/>. Acesso em: 08 abril 2024.

*SERVICEIT***. Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação**. *Serviceit*, 2021. Disponível em: <https://service.com.br/confidencial idade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao/>. Acesso em: 09 março 2024.

*SERVICENOW**. What is a security operations center (SOC)?*** *SERVICENOW,* 2024. Disponível em: <https://www.servicenow.com/products/security-operations/what-is-soc.html#:~:text=Definition%20of%20a%20security%20operations,to%20data%20breaches%20and%20cyberattacks>. Acesso: 8 abril 2024.

SIDDIQUI L. ***Incident Management: The Complete Guide****. Splunk*, 2023. Disponível em: <https://www.splunk.com/en_us/blog/learn/incident-management.html>. Acesso: 8 abril 2024.

SÁ, M. A. S. **Vulnerabilidade em redes de computadores corporativas: estudos de caso sobre ataques de *ransomware***. Trabalho de Graduação (Graduação em Engenharia de Computação) - Escola Politécnica e de Artes, Pontifícia Universidade Católica de Goiás. Goiânia, 2023.

SIMAS, Márcio. **Detecção Monitoramento e Correlação de Eventos como estratégia e planejamento de resposta a incidentes num SOC através de SIEM e SOAR.** Disponível em: <https://www.tempest.com.br/wp-content/uploads/2022/12/11_30_ Marcio-Simas_Tempest_-Deteccao-Monitoramento-e-Correlacao-de-Eventos-como-estrategia-e-planejamento-de-resposta-a-incidentes-num-SOC-atraves-de-SIEM-e-SOAR.pdf>.*Tempest*, 2022. Acesso em: 09 março 2024.

SINHA S; *MUKHOPADHYAY* D. ***Splunk*** **Dashboard: An Application Activities Presenter and Statistical Analyzer**. International Journal of Computer Applications, 2021. Acesso em: 11 set. 2024.

*Splunk****. Improves Its E-Commerce Experience to Boost Revenue by $10,000 Per Hour****. Splunk*, 2024. Disponível em: <https://www.splunk.com/en_us/customers/success-stories/puma.html>. Acesso em: 01 set. 2024.

VARDHAN. ***What Is Splunk? A Beginners Guide To Understanding Splunk****.* Disponível em: <https://www.edureka.co/blog/what-is-splunk/>. Acesso em: 28 de abril 2024.

VELÁSQUEZ L.M.J.; *MONTERRUBIO*, S.M.M.; *CRESPO* S.E.L.; ROSADO D.G. ***Systematic review of SIEM technology: SIEM-SC birth***. *International Journal of Information Security*, 2023. Disponível em: <https://doi.org/10.1007/s10207-022-00657-9>. Acesso em: 1 de março 2024.

WATTS, Stephen. ***Incident Response: A Brief Introduction****. Splunk*, 2023. Disponível em: <https://www.splunk.com/en_us/blog/learn/incident-response.html>. Acesso: 8 abril 2024.

WICKRAMASINGHE, Shanika. ***MITRE ATT&CK: Your Complete Guide To The ATT&CK Framework.*** *Splunk*, 2023. Disponível em: <https://www.splunk.com/en_us/blog/learn/mitre-attack.html>. Acesso em: 10 março 2024. *WICKRAMASINGHE, S.* ***DDoS Attacks in 2024: Distributed DoS Explained.*** Disponível em: <https://www.splunk.com/en_us/blog/learn/ddos-attacks.html>. Acesso em: 4 de maio 2024.

WICKRAMASINGHE, Shanika. **Behavioral Analytics in Cybersecurity.** *Splunk*, 2023. Disponível em: <https://www.splunk.com/en_us/blog/learn/behavioral-analytics.html#:~:text=*Splunk*%20User%20Behavior%20Analytics%20(UBA,intervention%20is%20required%20for%20analysis>. Acesso em: 24 de agosto 2024.

YAMIN M.M., ULLAH M., ULLAH H., KATT B., HIJJI M., KHAN M. ***Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security***. *Mathematics*, 2022. Disponível em: <https://doi.org/10.3390 /math10122054>. Acesso em: 10 março 2024.

YORK, *Tyler*. ***IT Event Correlation: Software, Techniques and Benefits*****.** *Splunk*, 2023. Disponível em: <https://www.splunk.com/e n_us/blog/learn/it-event-correlation.html>. Acesso em: 27 de março 2024.

ZIMMER, Kelvin. **Hacker x empresas: quais os ataques cibernéticos mais comuns?** *Lumiun Blog*. 2020. Disponível em: <https://www.lumiun.com/blog/ha ckers-empresas-quais-os-ataques-ciberneticos-mais-comuns/>. Acesso em: 2 maio 2024.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR

Av. Universitária, 1069 • Setor Universitário
Caixa Postal 86 • CEP 74605-010
Goiânia • Goiás • Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br • reitoria@pucgoias.edu.br

RESOLUÇÃO n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O(A) estudante Mailodi Vieira Sabath do Curso de Ciencia da Computação, matrícula 20191002800836, telefone: 62 996187036 e-mail vieirasabath@hotmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do Autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado UM ESTUDO SOBRE SOLUÇÕES DE ATAQUES CIBERNÉTICO COM SIEM COM FOCO NA PLATAFORMA SPLUNK, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto(PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 12 de setembro de 2024.

gov.br Documento assinado digitalmente
MAILODI VIEIRA SABATH
Data: 12/09/2024 09:46:10-0300
Verifique em https://validar.iti.gov.br

Assinatura do autor: _____

Nome completo do autor: Mailodi Vieira Sabath_____

Assinatura do professor–orientador: _____ gov.br Documento assinado digitalmente
SOLANGE DA SILVA
Data: 13/12/2024 19:45:50-0300
Verifique em https://validar.iti.gov.br

Nome completo do professor-orientador: _____