MONOGRAFIA DE PROJETO FINAL DE GRADUAÇÃO

ANÁLISE DE ALERTAS E INCIDENTES EM UM CENTRO DE OPERAÇÕES DE SEGURANÇA: MELHORES PRÁTICAS

João Vitor de Queiroz Braga

Curso Superior de Engenharia de Redes de Comunicação

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

MONOGRAFIA DE PROJETO FINAL DE GRADUAÇÃO

ANÁLISE DE ALERTAS E INCIDENTES EM UM CENTRO DE OPERAÇÕES DE SEGURANÇA: MELHORES PRÁTICAS

João Vitor de Queiroz Braga

Monografia de Projeto Final de Graduação submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Bacharel em Engenharia de Redes de Comunicação

Banca Examinadora

Dr. Georges Daniel Amvame Nze, EnE/UnB _____
Orientador

Dr. Fábio Lúcio Lopes de Mendonça, EnE/UnB _____
Examinador Interno

Esp. Raissa Marcon Constante, UNISUL/SC _____
Examinador Externo

FICHA CATALOGRÁFICA

BRAGA, J.V.Q.
ANÁLISE DE ALERTAS E INCIDENTES EM UM CENTRO DE OPERAÇÕES DE SEGURANÇA: MELHORES PRÁTICAS [Distrito Federal] 2023.
xvi, 43 p., 210 x 297 mm (ENE/FT/UnB, Bacharel, Engenharia de Redes de Comunicação, 2023).
Monografia de Projeto Final de Graduação - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Proteção de Endpoints	2. Detecção de Intrusão
3. Proteção de Dados	4. Ataques cibernéticos
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

BRAGA, J.V.Q. (2023). *ANÁLISE DE ALERTAS E INCIDENTES EM UM CENTRO DE OPERAÇÕES DE SEGURANÇA: MELHORES PRÁTICAS*. Monografia de Projeto Final de Graduação, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 43 p.

CESSÃO DE DIREITOS

AUTOR: João Vitor de Queiroz Braga
TÍTULO: ANÁLISE DE ALERTAS E INCIDENTES EM UM CENTRO DE OPERAÇÕES DE SEGURANÇA: MELHORES PRÁTICAS.
GRAU: Bacharel em Engenharia de Redes de Comunicação ANO: 2023

João Vitor de Queiroz Braga
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP: 70919-970 - Brasília-DF - Brasil

Dedico este trabalho aos meus pais Sirlânio e Gislene, por sempre terem me incentivado a estudar e a querer ser uma pessoa melhor a cada dia e a minha noiva Júlia, por ser minha companheira de vida e sempre me apoiar, amo vocês.

AGRADECIMENTOS

O sonho de me formar no ensino superior sempre permeou meus pensamentos desde que eu comecei a ter noção do quão importante isso seria para o meu futuro. O estudo te leva onde você quiser, eu sempre escutei isso, porém, somente na universidade eu realmente entendi o que essa frase significava. O conhecimento é a maior ferramenta que uma pessoa pode ter, só chegamos onde estamos hoje, como sociedade, através de muito estudo, vários profissionais deram suas vidas para que pudéssemos ter uma vida melhor, o avanço da ciência, medicina, engenharia e demais áreas, foram responsáveis por termos chegado onde chegamos hoje, como sociedade, tudo através de muito estudo, e estudar foi o que me trouxe até este momento da minha vida, meu projeto final de graduação.

Quero agradecer primeiramente a Deus, por me fazer ser quem eu sou, por ter me mantido de pé até aqui, por ter me dado inteligência e sabedoria, sem Ele nada disso seria possível. Ele me deu forças em todos os momentos que pensei em desistir, e foram muitos, só Ele e eu sabemos. Não foi uma jornada fácil, foi uma jornada de muito esforço, dedicação, fracassos e por fim, o maior sucesso de todos, a finalização bem sucedida que está chegando.

Agradeço aos meus pais, por todo o apoio e ajuda ao longo desses anos escolares e universitários, agradeço por sempre terem cuidado de mim com tanto amor e carinho, se eu sou quem eu sou hoje, se estou onde estou hoje, vocês tem papel fundamental nisso tudo, eu amo muito vocês e agradeço demais por tudo, meu sucesso, é o sucesso de vocês!

Agradeço a minha noiva, Júlia, por sempre ser minha parceira, por me incentivar a ser melhor a cada dia, por ser paciente em todos os finais de semana que eu tive que estudar e não pude vê-la, por se dar por mim, cuidando de mim e me ajudando sempre, quando eu estava quase desistindo, ela era usada por Deus pra me dizer que eu poderia ir mais longe, que eu tinha que continuar, perseverar, não só por mim, mas por ela também. Eu te amo demais, meu amor!

Agradeço aos meus amigos pela parceria ao longo desses anos na UnB, sem vocês, eu não estaria me formando, sem cada uma das ajudas, cada conselho, cada choro, eu não estaria aqui. Agradeço a todos pela parceria, Júlia Jamile, Geovana de Melo, Bruno Scholles, Daniel Pereira, Lucas Alexandre, Gustavo Barbosa, Samuel Soares, Bruno Brandão, Nelson Roberto, dentre vários outros companheiros de jornada, meu muito obrigado por tudo, só quem viveu sabe.

Agradeço aos professores da UnB por terem me forjado um profissional capacitado e preparado não só para vida acadêmica e mercado de trabalho, mas para as situações da vida cotidiana, foram várias lições aprendidas na UnB levarei todas elas comigo pro resto da minha vida. Meu agradecimento especial ao professor Georges, meu orientador, por todos os conhecimentos na área de redes e por me fazer querer aprender mais e ser melhor sempre, aos professores Lineu Neto, Ricardo Ruviaro, meus professores de Cálculo 1, por terem sido tão atenciosos com aquele calouro em 2016 e ao professor Ricardo Zelenovsky por ter sido tão compassivo quando passei por um situação familiar complicada ao longo da sua disciplina Sistemas Microprocessados.

Agradeço por fim à Teltec Solutions, empresa que trabalho atualmente, por me incentivar a ser melhor, estudar, tirar certificações e me fornecer todo apoio ao longo desse período de projeto final, agradeço em especial aos meus colegas de monitoramento, Taianne e Eduardo, por me ajudarem e me apoiarem quando

precisava resolver algo deste trabalho no meio do expediente, por serem voz de Deus pra me acalmar quando eu estava agitado. E a minha incrível chefe Raissa, que faz parte da banca avaliadora deste trabalho e foi uma grande incentivadora do meu crescimento profissional, me orientando e trabalhando para meu bem estar e desenvolvimento profissional dentro da Teltec.

Foi uma bela e árdua jornada, que está se encerrando, e mesmo me lembrando dela de forma conflitante, foi um jornada absurdamente intensa. Só posso dizer uma coisa, eu te amo, UnB! Seus prédios, seu verde, suas paisagens, suas pessoas, você não é somente uma universidade, você é uma entidade, você é viva, como é difícil entrar, mas muito mais complicado sair, enfim, obrigado por ter sido minha casa por todos esses anos, sentirei saudades.

Não existe sorte, o que existe é esforço e dedicação...

RESUMO

Com o crescimento muito acelerado de ataques cibernéticos, faz-se cada vez mais necessário o uso de um Centro de Operações de Segurança (SOC), em organizações públicas e privadas. É fundamental ter uma equipe bem treinada e procedimentos bem organizados e documentados, a fim de que todo o potencial do SOC seja obtido. Visando isso, neste trabalho, serão propostas melhores práticas a serem seguidas por um SOC a fim de que os alertas e incidentes que vierem a acontecer sejam resolvidos da melhor forma possível, de maneira rápida e eficaz. Para isso, através das melhores práticas documentadas por alguns autores e organizadas para o caso abordado, que é uma organização sem um SOC, que deseja implementar um, será construído um cenário inicial, assim havendo processos modelados que servirão de exemplo para outras empresas, de como agir, quando agir e quem deve agir. Além disso, serão citadas tecnologias que visam otimizar o trabalho do SOC, possibilidades de melhorias futuras e as expectativas para o futuro do SOC.

Palavras-chave: SOC, cibersegurança, ataque, incidente, alerta, SIEM, melhores práticas.

ABSTRACT

With the very rapid growth of cyber attacks, the use of a Security Operations Center (SOC) is increasingly necessary in public and private organizations. It is essential to have a well-trained team and well-organized and documented procedures, so that the full potential of the SOC is obtained. With this in mind, this work will propose best practices to be followed by a SOC, so that alerts and incidents that may occur are resolved in the best possible way, quickly and effectively. To achieve this, through the best practices documented by some authors and organized for the case discussed, which is an organization without a SOC, which wishes to implement one, an initial scenario will be constructed, thus having modeled processes that will serve as an example for other companies, of how to act, when to act and who should act, in addition, technologies that aim to optimize the work of the SOC, possibilities for future improvements and expectations for the future of the SOC will be mentioned.

Keywords: SOC, cybersecurity, attack, incident, alert, SIEM, best practices.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SÍMBOLOS

Siglas

SOC	*Security Operation Center*
GPDR	*General Data Protection Regulation*
LGPD	*Lei de Proteção de Dados Pessoais*
SQL	*Structured Query Language*
XSS	*Cross-Site Scripting*
SIEM	*Security Information and Event Management*
SOAR	*Security Orchestration, Automation, and Response*
XDR	*Extended Detection and Response*
IoT	*Internet of Things*
NIST	*National Institute of Standards and Technology*
FP	*Falso Positivo*
VP	*Verdadeiro Positivo*
UEBA	*User and Entity Behavior Analytics*
EDR	*Endpoint Detection and Response*
NDR	*Network Detection and Response*
APT	*Advanced Persistent Threat*
MSP	*Managed Service Providers*
NOC	*Network Operation Center*
UEBA	*User and Entity Behavior Analytics*

1 INTRODUÇÃO

Um Centro de Operações de Segurança, do inglês, Security Operations Center, mais conhecido pela sigla SOC, é uma parte fundamental da infraestrutura de cibersegurança de uma organização. Trata-se de um ambiente centralizado e altamente especializado, projetado para monitorar, detectar, responder e mitigar ameaças e incidentes de segurança em tempo real [15]. Em um mundo cada vez mais digital e interconectado, na qual as ameaças cibernéticas estão em constante evolução, um SOC desempenha um papel crucial na proteção dos ativos digitais e na manutenção da integridade, confidencialidade e disponibilidade dos sistemas de uma organização.

De maneira resumida, um SOC é composto por profissionais de cibersegurança altamente treinados, que utilizam ferramentas avançadas de monitoramento e análise de segurança para acompanhar atividades de rede, identificar potenciais ameaças e responder de maneira eficaz a incidentes de segurança. Este ambiente é o ponto de encontro de informações de suma importância do ponto de vista de segurança, permitindo uma visão abrangente das operações da organização e a coordenação de ações para proteger seus ativos digitais.

Com a constante evolução das ameaças cibernéticas, as organizações estão expostas a riscos cada vez maiores de ataques cibernéticos. Um dos principais motivos para gastos em segurança é a proteção de dados sensíveis, tanto os da própria organização como os de seus clientes e funcionários. A perda ou comprometimento dessas informações pode resultar em violações de privacidade, penalidades legais e sérios danos à reputação.

Além disso, muitas organizações estão sujeitas a regulamentações rigorosas, como o GDPR na União Europeia ou a LGPD no Brasil. O não cumprimento dessas regulamentações pode resultar em multas substanciais. Investir em segurança é uma forma de estar de acordo com as leis propostas. A confiança do cliente e a reputação da organização também estão em jogo quando se trata de segurança cibernética. Uma violação de segurança pode abalar a confiança dos clientes na organização, e os gastos em cibersegurança demonstram um compromisso em proteger os dados dos clientes, fortalecendo, assim, a confiança e a imagem da organização.

A economia a longo prazo também é uma consideração importante. Embora os gastos com cibersegurança representem um investimento inicial substancial, evitar uma única violação de dados ou ataque cibernético pode resultar em economia a longo prazo, uma vez que se evitam custos de recuperação e perda de negócios. Em resumo, os gastos em cibersegurança são essenciais para a sobrevivência e o sucesso a longo prazo de uma organização, protegendo dados, garantindo conformidade, mantendo a confiança do cliente e prevenindo interrupções nos negócios. Além disso, demonstram um compromisso com a segurança e a responsabilidade, o que é um ativo valioso nos negócios modernos. Portanto, a cibersegurança deve ser considerada uma prioridade estratégica em qualquer organização.

1.1 OBJETIVO GERAL

O objetivo geral deste trabalho é mostrar as melhores práticas a serem utilizadas em um SOC no processo de análise de alertas e incidentes, levando em consideração um cenário inicial mais simples. Isso será feito através uma série de fases, propondo recomendações baseadas nas melhores práticas, a partir de alguns autores, a fim de fazer que o SOC atinja seu potencial total, que é de prevenir, detectar, responder e mitigar incidentes de segurança de forma eficiente e eficaz.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos têm como principal sentido embasar o objetivo geral deste trabalho. Eles são:

1. Mapear processos a fim de serem úteis na análise de alertas e resposta a incidentes.
2. Emular análises em alertas reais a fim de propor um cenário possível.
3. Citar tecnologias que podem ser usadas a fim de melhorar a exatidão das análises do SOC.
4. Traçar possibilidades de futuro para o SOC.

1.3 MOTIVAÇÃO

A motivação por trás deste trabalho se deu por conta do trabalho que eu exerço hoje. Sou Analista de SOC de uma empresa com pouco mais de um ano de operação. Estamos no processo de mapeamento de processos de maneira mais concisa, bastantes coisas documentadas, procedimentos, runbooks, playbooks, mas estamos sempre buscando melhorar e nos aperfeiçoar no serviço que prestamos. Isso me motivou a escrever este trabalho a fim de mapear melhores práticas na análise de alertas e incidentes para um SOC recém criado, que podem ser aplicadas para outras empresas e SOCs já existentes.

2 FUNDAMENTAÇÃO TEÓRICA

Essa seção tem como foco dar base a todas as considerações que serão feitas a diante no trabalho, sendo uma base teórica completa para o entendimento de conceitos mais avançados ao longo da análise. Portanto, visa realizar um revisão gradual de conceitos e fundamentos teóricos que serão necessários para o entendimento do trabalho.

2.1 AMEAÇA

No contexto de cibersegurança, uma ameaça se refere a qualquer evento, ação, objeto ou entidade que tem o potencial de causar um incidente, ou seja, danos aos sistemas de informação, redes, dispositivos e dados de uma organização. Essas ameaças podem variar em natureza e origem e são uma preocupação fundamental na proteção da segurança da informação [15]. Alguns exemplos de ameaças que estão no dia a dia de um SOC são:

- **Malware:** É um software malicioso. São exemplos, vírus, worms, cavalos de troia e ransomwares. São projetados para se infiltrar em sistemas e causar danos, roubar dados ou extorquir dinheiro;
- **Engenharia Social:** Técnicas que exploram falhas humanas, enganando pessoas a fim de obter informações confidenciais. São exemplos, phishing, pretexting e tailgating;
- **Ataque de Negação de Serviço (DoS/DDoS):** Tentativas de sobrecarregar sistemas, redes ou serviços com tráfego malicioso, tornando-os inacessíveis para usuários legítimos;
- **Vulnerabilidade de Software:** São fraquezas presentes em aplicativos, programas, sistemas operacionais ou hardwares que podem ser exploradas por invasores para ganhar acesso não autorizado;
- **Ataque de Força Bruta:** Tentativas repetidas de adivinhar senhas ou chaves de criptografia, geralmente usando automação;
- **Ataques de Injeção:** Exploração de vulnerabilidades em sistemas que permitem que invasores insiram código malicioso, como injeção SQL e XSS;
- **Roubo de Identidade:** O uso não autorizado da identidade de outra pessoa, geralmente para acessar recursos ou cometer atividades ilegais em seu nome;
- **Vazamento de Dados:** Divulgação não autorizada de informações confidenciais, geralmente resultando em perda de privacidade ou riscos à segurança;
- **Ataques de Engenharia Reversa:** Análise de produtos ou sistemas para descobrir como funcionam, muitas vezes para desenvolver um malware ou explorar vulnerabilidades;

- **Ameaças Internas:** Funcionários ou parceiros que agem de maneira maliciosa ou sem orientações e acabam comprometendo a segurança, muitas vezes resultando em vazamento de informações;
- **Escalação de Privilégio:** Quando indivíduos ou entidades não autorizados tentam ou conseguem acessar informações confidenciais ou sistemas;
- **Ataques a Dispositivos IoT:** Invasões a dispositivos IoT a fim de acessar redes ou coletar dados pessoais.

A Figura 2.1, cita as principais ameaças na área de cibersegurança no ano em que este trabalho foi feito, 2023.

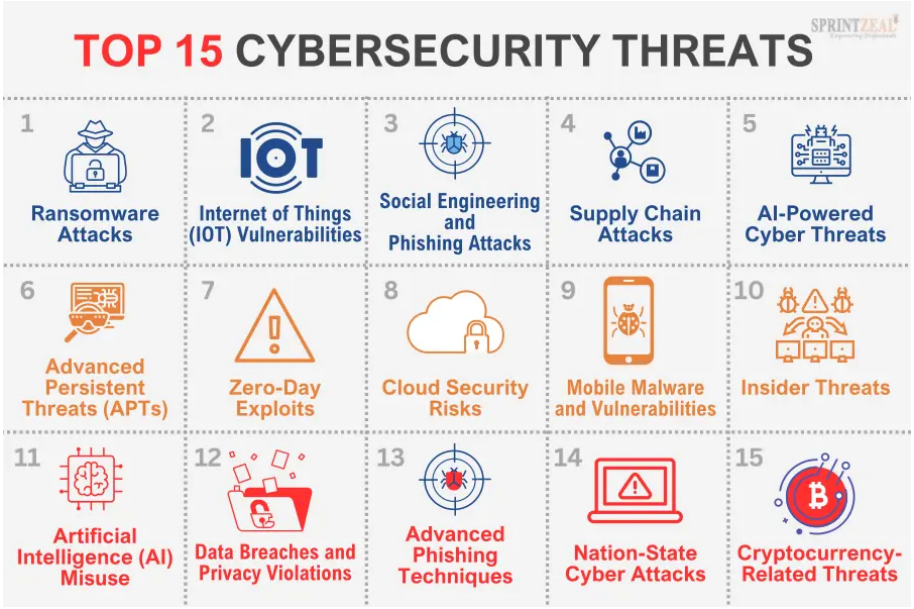

Figura 2.1: Top 15 Cybersecurity Threats in 2023 | Sprintzeal. Fonte: [1]

2.2 VULNERABILIDADE

No contexto de cibersegurança, uma vulnerabilidade se refere a uma fraqueza, falha ou ponto de exposição em um processo, sistema, software ou rede que pode ser explorada por ameaças cibernéticas, como hackers, malwares e outros agentes maliciosos. Essas vulnerabilidades podem permitir que invasores ganhem acesso não autorizado a sistemas, exponham dados confidenciais, interrompam serviços ou causem vários outros danos. [16]

Vulnerabilidades podem ter várias origens, como erros de programação, configurações inadequadas, falta de atualizações de segurança e design inadequado de sistemas. Alguns exemplos comuns de vulnerabilidades são: bugs de software, que são erros de programação que podem permitir que invasores explorem o código para ganhar acesso não autorizado ou causar mau funcionamento do software. Senhas fracas, senhas fáceis de adivinhar ou mal gerenciadas podem ser exploradas por ataques de força bruta ou phishing. Falta de atualizações, sistemas desatualizados muitas vezes têm vulnerabilidades conhecidas que não foram

corrigidas por meio de atualizações de segurança. Configurações de segurança mal feitas, configurações inadequadas em servidores, firewalls e outros dispositivos podem deixar brechas de segurança. Interfaces expostas na internet de maneira inadequada, interfaces de administração e serviços expostos à Internet sem proteção adequada podem ser alvos fáceis para invasores. Falta de controle de acesso, permissões inadequadas podem permitir que usuários não autorizados acessem recursos sensíveis. [17]

A identificação e correção de vulnerabilidades são partes essenciais da gestão de segurança da informação. Isso envolve a realização de testes de segurança, auditorias, monitoramento constante e a constante atualização dos firewalls e atualizações gerais de segurança para mitigar essas vulnerabilidades e reduzir o risco de exploração por ameaças cibernéticas. Além disso, práticas de segurança sólidas, como a implementação de políticas de segurança, conscientização dos funcionários e a aplicação de medidas de controle de acesso, desempenham um papel fundamental na prevenção e proteção contra vulnerabilidades.

Na Figura 2.2, temos o ciclo de gerenciamento de vulnerabilidades. Ele é um processo contínuo, que varia de autor pra autor.

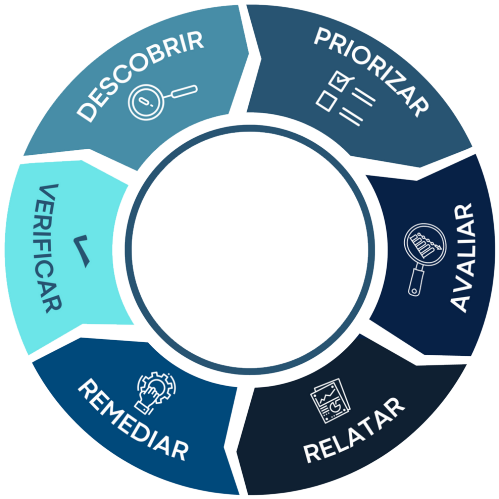

Figura 2.2: Ciclo de gestão de vulnerabilidades. Fonte: [2]

No exemplo citado, existem seis passos. O primeiro é descobrir, que consiste em criar e manter um diretório de ativos. O segundo é priorizar, onde é atribuído um valor a cada grupo de ativos que reflita sua criticidade. O terceiro é avaliar, consiste em criar um perfil de risco para cada um de seus ativos e avaliá-los. Isso permite determinar quais riscos eliminar primeiro com base em vários fatores, como os níveis de ameaça a vulnerabilidade e criticidade, bem como classificação. O quarto é relatar, que consiste em criar um plano para seus ativos conforme os riscos e níveis de importância, determinados nos estágios anteriores. O quinto passo é remediar, sendo o momento no qual ações efetivas são tomadas, é implementado o plano de segurança, são consertadas as vulnerabilidades de acordo com os riscos para o negócio. E o sexto e último passo é verificar, nele são usados auditorias e acompanhamento do processo para garantir a eliminação das vulnerabilidades. Essa parte não consiste em apenas uma ação: organizações devem escanear e avaliar seu ambiente regularmente. [2]

2.3 INCIDENTE

O conceito de incidente é bastante discutido no cenário de cibersegurança atualmente. Ele possui várias interpretações, a depender do cenário e do contexto inserido. A seguir será mostrado o que será considerado neste trabalho.

Um incidente de segurança da informação refere-se a qualquer evento adverso ou ação que compromete a confidencialidade, integridade ou disponibilidade dos dados, sistemas ou rede de uma organização. Incidentes geralmente possuem uma gravidade mais alta, como violações graves de segurança que resultam em perda de dados, interrupções de serviços ou danos financeiros significativos. Os incidentes podem ser ataques cibernéticos, sendo eles ataques de ransomware, ataques de negação de serviço (DDoS) ou intrusões em sistemas de computadores, vazamento de dados, uso inadequado de recursos, falhas de segurança, sejam elas vulnerabilidades de sistemas, aplicativos ou dispositivos que podem ser exploradas por pessoas mal-intencionadas. Desastres naturais e falhas de energia que venham a interromper a disponibilidade de sistemas e dados e erros humanos, que podem ser intencionais ou não intencionais, como exclusão acidental de dados ou divulgação inadvertida de informações confidenciais também são considerados incidentes de segurança da informação. [18]

Quando um incidente de segurança ocorre, as organizações deveriam ter procedimentos em vigor para detectar, responder e mitigar o impacto desses incidentes. Isso pode envolver a notificação das partes afetadas, investigação, restauração de sistemas, correção de vulnerabilidades e implementação de medidas para evitar futuros incidentes semelhantes. Além disso, em muitos casos, é necessário cumprir requisitos regulatórios e legais, como a notificação de violações de dados às autoridades e às partes afetadas. [19]

2.4 SIEM

Um SIEM, em português, Sistema de Gerenciamento de Eventos e Informações de Segurança, é uma solução de software projetada para fornecer uma visão abrangente e centralizada das atividades de segurança em uma rede ou sistema. Ele desempenha um papel crítico na detecção, prevenção e resposta a ameaças cibernéticas. Um SIEM coleta dados de diversos dispositivos e aplicativos, como firewalls, antivírus, IDS/IPS e servidores, e os consolida em um único local. Isso permite que os analistas de segurança monitorem eventos, alertas e incidentes em tempo real, identificando anomalias e potenciais ameaças à segurança. Além disso, o SIEM pode automatizar a análise de registros, geração de relatórios de conformidade e fornecer uma visão valiosa a fim de melhorar a postura de segurança de uma organização. [20]

Após a coleta dos dados, eles são normalizados, o que significa que são convertidos em um formato comum para facilitar a análise. Em seguida, ocorre a correlação, onde o SIEM identifica padrões e relações entre eventos. Isso ajuda a detectar ameaças que podem passar despercebidas quando se analisa apenas eventos individuais. Ele utiliza regras e algoritmos para analisar os eventos e identificar possíveis ameaças à segurança, podendo assim gerar alertas em tempo real quando são encontrados eventos suspeitos ou violações de políticas de segurança predefinidas.

Os dados de log coletados são armazenados em um banco de dados seguro, geralmente por um período específico. Isso permite que as organizações atendam a requisitos regulatórios e também facilitem investigações posteriores. Um SIEM pode criar relatórios detalhados sobre as atividades de segurança, que são úteis para fins de conformidade regulatória e auditorias internas. Isso é particularmente importante em setores sujeitos a regulamentações rígidas, como saúde, financeiro e governo.

Além da detecção, um SIEM também auxilia na resposta a incidentes. Ele fornece informações valiosas para os profissionais de segurança identificarem a gravidade dos incidentes e tomarem medidas apropriadas para contê-los. Muitos SIEMs podem ser integrados a outras soluções de segurança, como SOAR, antivírus e soluções de gerenciamento de identidade, aprimorando a capacidade de resposta a ameaças. Alguns SIEMs também utilizam técnicas de machine learning e inteligência artificial para melhorar a detecção de ameaças, identificando padrões mais complexos e ameaças avançadas. Na Figura 2.3, temos um exemplo de dashboard de um SIEM, neste caso o USM Anywhere da empresa AT&T. Exemplos dessa solução serão usados mais adiante.

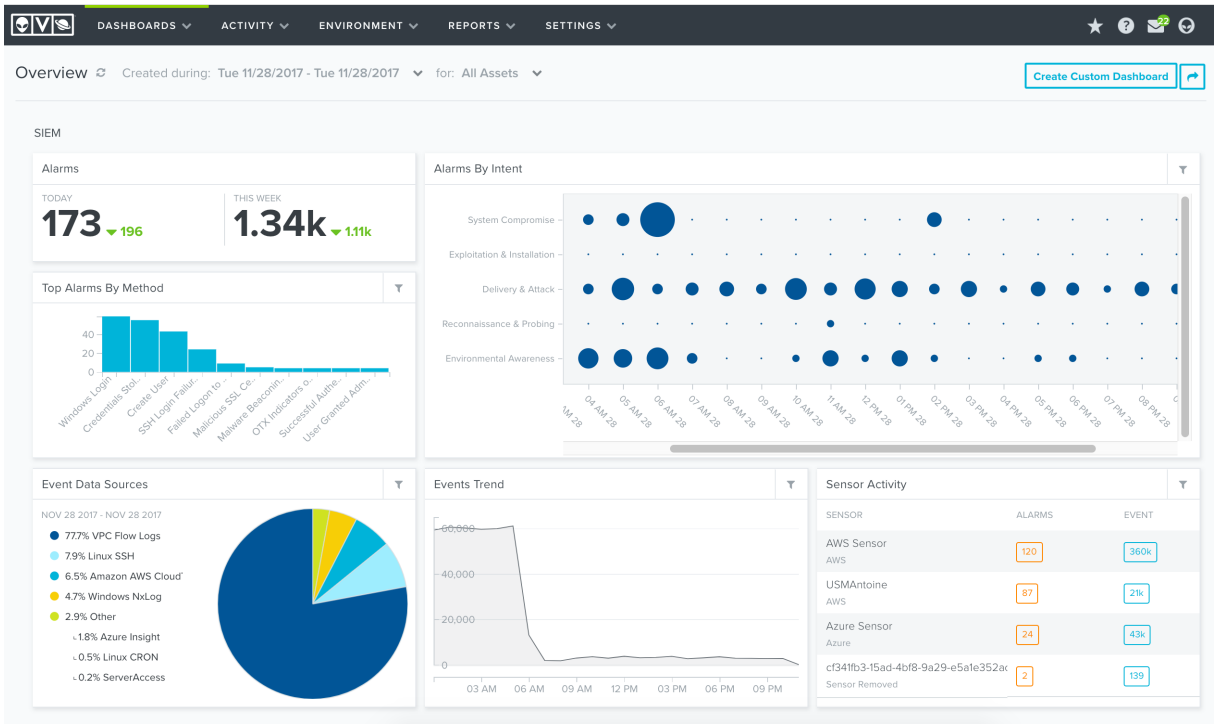

Figura 2.3: Exemplo de dashboard do SIEM USM Anywhere. Fonte: [3]

2.5 SOAR

Um SOAR, em português, Orquestração, Automatização e Resposta de Segurança, é uma plataforma de segurança cibernética projetada para ajudar as organizações a melhorar sua capacidade de resposta a incidentes de segurança.

A orquestração se refere à coordenação de atividades de segurança cibernética. Um sistema SOAR permite que as equipes de segurança automatizem processos complexos de resposta a incidentes, coordenando

ações entre diferentes ferramentas e sistemas de segurança. Isso ajuda a melhorar a eficiência e a consistência das operações de segurança. A automatização envolve a execução de tarefas de segurança de rotina sem intervenção humana. Isso pode incluir a execução de verificações de segurança, a implementação de medidas corretivas e a coleta de informações para análise. A automatização reduz a carga de trabalho manual, acelera a resposta a incidentes e minimiza o risco de erros. Nesse contexto, a resposta a incidentes é a capacidade de uma plataforma SOAR de ajudar as equipes de segurança a tomar medidas efetivas quando ocorrem alertas ou incidentes de segurança. Isso pode incluir a isolamento de sistemas comprometidos, a aplicação de correções e a documentação de incidentes para análise pós-incidente e relatórios. [21]

Algumas empresas acabam usando ambos em conjunto para obter uma estratégia completa de segurança cibernética, na qual o SIEM fornece a detecção de ameaças e o SOAR ajuda a automatizar a resposta a essas ameaças. Na Figura 2.4, temos um exemplo de dashboard de um SOAR, neste caso, o Cortex XSOAR da fabricante Palo Alto.

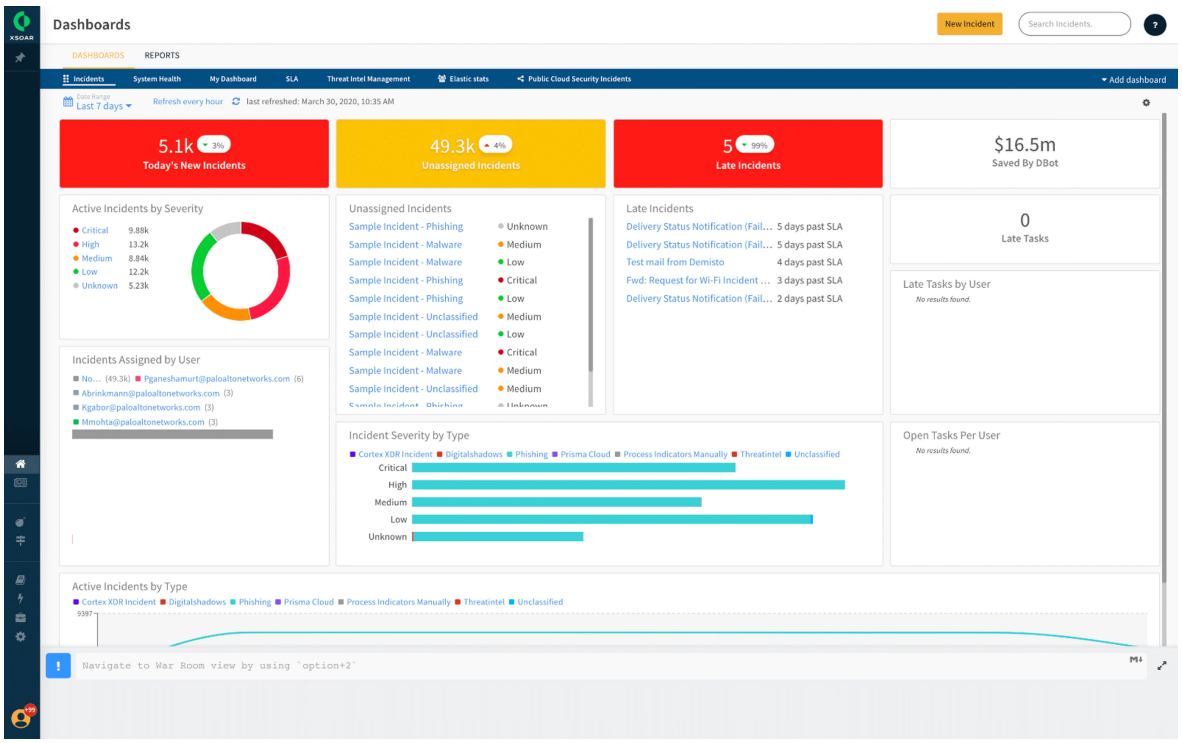

Figura 2.4: Exemplo de dashboard do SOAR Cortex XSOAR. Fonte: [4]

2.6 XDR

Um XDR, em português, Detecção e Resposta Estendidas, é um serviço de segurança cibernética que se concentra na detecção e resposta a ameaças, porém com uma abordagem mais ampla e integrada. Os serviços prestados por um XDR incluem, integração de dados, já que ele reúne dados de várias fontes de segurança, como dispositivos finais, redes, servidores e aplicativos, para criar uma visão mais integrada das ameaças em toda a infraestrutura de uma organização. Isso permite uma detecção mais abrangente e uma resposta mais eficaz a incidentes.

Um XDR utiliza análises avançadas e inteligência artificial para identificar ameaças e comportamentos suspeitos em toda a infraestrutura, incluindo ameaças que podem não ser detectadas por soluções tradicionais de segurança. Um XDR fornece ferramentas para coordenar a resposta a incidentes em toda a organização, permitindo uma ação rápida e eficaz para conter e remediar ameaças. Ele é extremamente escalável e pode ser adaptado para atender às necessidades de organizações de diferentes tamanhos e complexidades.

O XDR é uma resposta às crescentes ameaças cibernéticas e à necessidade de uma abordagem mais integrada à segurança. Ele ajuda as organizações a lidar com ameaças de maneira mais eficaz, reduzindo o tempo de detecção e resposta a incidentes e melhorando a postura geral de segurança. [22]

Na Figura 2.5, temos um exemplo de dashboard de um XDR, neste caso, o Falcon XDR da empresa CrowdStrike.

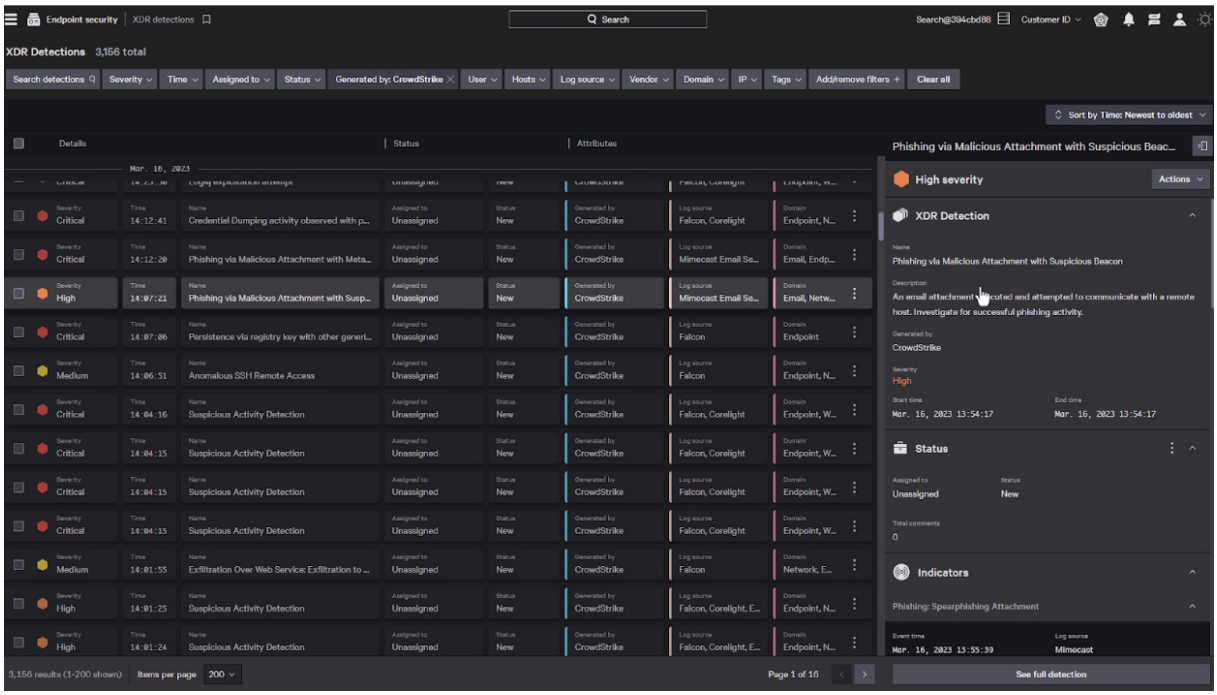

Figura 2.5: Exemplo de dashboard do XDR Falcon XDR. Fonte: [5]

As principais diferenças entre SIEM, SOAR e XDR estão relacionadas às suas funcionalidades, objetivos e focos.

Um SIEM é projetado principalmente para coletar, armazenar e analisar dados de segurança, com ênfase na detecção de eventos e ameaças de segurança. Ele fornece visibilidade em tempo real dos eventos de segurança e atividades de rede.

O XDR, por sua vez, representa uma solução mais abrangente que expande as funcionalidades do SIEM ao incorporar dados de endpoints, redes e nuvem. Essa abordagem proporciona uma visão mais abrangente da segurança da rede, possibilitando uma detecção aprimorada de ameaças. Com recursos de detecção de ameaças avançadas, resposta automatizada a incidentes, correlação de eventos provenientes de diversas fontes de dados e análise de ameaças em tempo real, os profissionais de segurança conseguem identificar e responder a ameaças de maneira mais eficiente, reduzindo assim o tempo de resposta a incidentes. [23]

Já um SOAR se concentra na automação, orquestração e resposta a incidentes de segurança. Ele é projetado para melhorar a eficiência das operações de segurança cibernética, acelerando a resposta a incidentes e ações corretivas. Um SIEM pode gerar alertas e fornecer informações valiosas sobre incidentes, mas a ação corretiva geralmente é realizada manualmente. O SOAR é especializado na automação e coordenação de respostas a incidentes, executando ações corretivas de forma automatizada. [24]

2.7 EVENTOS E ALERTAS

No contexto de um SIEM, um evento se refere a uma ocorrência ou atividade específica que é registrada e monitorada dentro da ferramenta. Esses eventos são geralmente relacionados à segurança cibernética e podem ser de natureza variada, como tentativas de login, tráfego de rede, alterações em configurações de sistemas, detecção de malware, dentre outros, existem uma infinidade de possibilidades de eventos. Cada evento é uma unidade de informação que pode conter detalhes importantes sobre o que aconteceu, quando aconteceu, onde aconteceu e quem estava envolvido.

Esses eventos são coletados de várias fontes, como firewalls, servidores, estações de trabalho, dispositivos de rede e são normalmente processados e analisados pelo SIEM. Dessa forma ele pode, então, correlacionar eventos para identificar potenciais ameaças e gerar alertas para a equipe de segurança.

No contexto de um SIEM, um alerta é uma notificação gerada pelo sistema com base na análise de eventos coletados de várias fontes de dados. Esses alertas são acionados quando o SIEM identifica uma atividade suspeita, um comportamento fora do padrão ou um evento que pode representar uma ameaça à segurança da organização. Existe a possibilidade também da criação de um regra para que determinado tipo de evento gere um alerta, a depender de variáveis previamente estabelecidas.

A geração de alertas é uma parte fundamental da funcionalidade de um SIEM, uma vez que ajuda a equipe de segurança a identificar e responder rapidamente a potenciais incidentes. Além disso, os alertas normalmente são classificados com base em sua prioridade, por exemplo sendo categorizado como baixa, média, alta e crítica, permitindo que os analistas de segurança priorizem as ações apropriadas. Uma vez que um alerta é gerado, a equipe de segurança pode investigar o incidente, tomar medidas corretivas e, se necessário, iniciar procedimentos de resposta a incidentes.

Na Figura 2.6, temos um exemplo de como eventos são mostrados em uma interface de SIEM, neste caso, o SIEM open-souce Sagan.

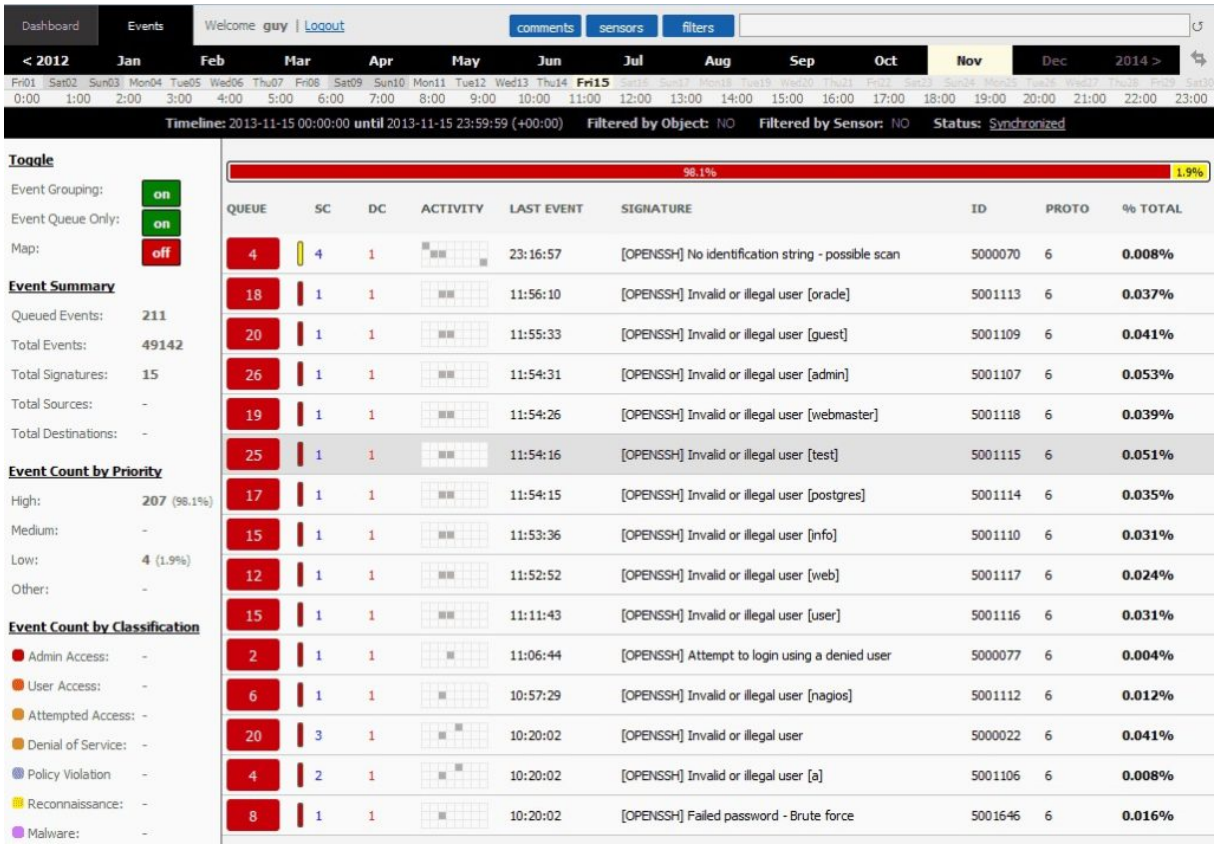

Figura 2.6: Exemplo de eventos mostrados no SIEM Sagan. Fonte: [6]

2.8 PRIORIDADES DOS ALERTAS

Explicando melhor o que caracteriza cada uma das prioridades dos alertas citadas anteriormente, tem-se:

- Crítica: Todos os serviços encontram-se inacessíveis, afetando todos os usuários devido a um incidente;
- Alta: Uma funcionalidade ou serviço significativo está severamente comprometido por um incidente, impactando a maioria dos usuários, embora ainda possam continuar a operar;
- Média: Incidente que resulta apenas em interrupção localizada do serviço ou degradação, afetando apenas um pequeno grupo de usuários;
- Baixa: Incidentes que não impactam serviços em geral, podendo afetar apenas um usuário específico ou não gerar impacto em geral. Isso inclui questões relacionadas a funcionalidades, novas solicitações de execução e configurações comuns que não afetam os usuários em larga escala.

2.9 CHAMADO INTERNO

Um conceito importante de ser entendido no contexto deste trabalho é o de chamado interno. Ele é uma forma de registro de quais passos foram tomados, quais ações foram feitas em relação a um determinado alerta ou incidente. Geralmente esses chamados são abertos em plataformas de gerenciamento de chamados, onde todas as partes interessadas no processo tem acesso ao registro e podem editá-lo. Em um chamado podem estar presentes informações como, nome do usuário envolvido no alerta, máquina, resumo do alerta/incidente, procedimento feitos e demais observações. A Figura 2.7 mostra uma ilustração de interface de chamado.

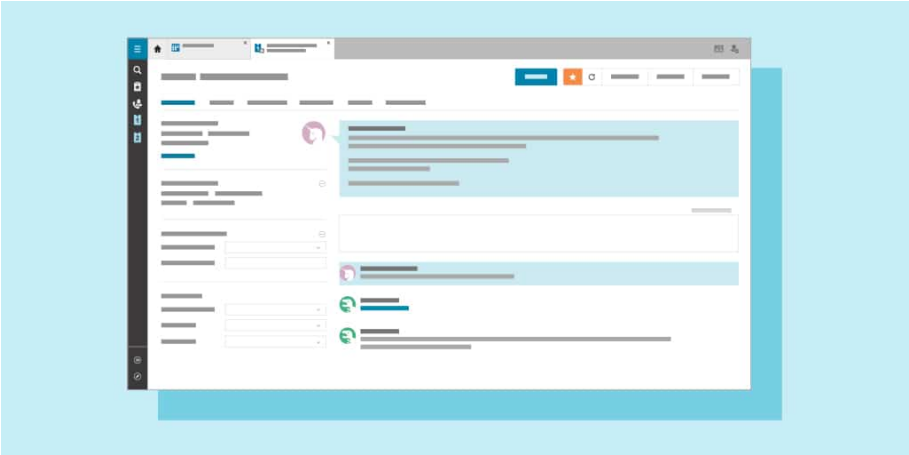

Figura 2.7: Ilustração de como seria um chamado numa plataforma de gerenciamento de chamados. Fonte: [7]

2.10 VERDADEIRO POSITIVO

Na área de cibersegurança, temos um verdadeiro positivo quando um resultado obtido por um sistema de detecção ou uma análise feita identifica corretamente uma ameaça ou ataque real. Em outras palavras, é quando um sistema de segurança ou um analista detecta uma atividade ou evento malicioso e classifica corretamente como uma ameaça legítima. Por exemplo, se um SIEM identifica corretamente um ataque real e emite um alerta, esse alerta é um verdadeiro positivo.

2.11 VERDADEIRO NEGATIVO

Temos um verdadeiro negativo quando um resultado obtido por um sistema de detecção ou uma análise feita identifica corretamente que não há uma ameaça ou atividade maliciosa. Em outras palavras, é quando o sistema de segurança ou um analista reconhece corretamente que uma determinada ação ou evento é benigno, e não uma ameaça real. Em resumo, um verdadeiro negativo indica que o sistema de segurança está operando corretamente ao reconhecer que uma atividade não representa uma ameaça à segurança.

2.12 FALSO POSITIVO

Temos um falso positivo quando um sistema de detecção ou análise erroneamente identifica uma atividade como maliciosa quando, na realidade, ela é inofensiva ou legítima. Em outras palavras, é um alerta falso que sugere a presença de uma ameaça que não existe. Por exemplo, se um sistema de antivírus sinaliza erroneamente um arquivo legítimo como malware, isso é um falso positivo. Da mesma forma, um SIEM pode gerar um alerta falso se interpretar incorretamente padrões normais de tráfego como atividade maliciosa.

Os falsos positivos são preocupantes na contexto avaliado porque podem levar a uma sobrecarga de trabalho para a equipe de SOC, resultando em investigações desnecessárias. Portanto, minimizar falsos positivos é um objetivo importante para garantir que os alertas emitidos pelos sistemas de segurança sejam confiáveis e mereçam uma investigação mais aprofundada.

2.13 FALSO NEGATIVO

Temos um falso negativo quando um sistema de detecção ou análise falha em identificar uma ameaça ou atividade maliciosa. Em outras palavras, é quando o sistema não emite um alerta ou não reconhece corretamente uma ameaça legítima. Por exemplo, se um antivírus não detecta um malware que está presente em um sistema, isso é um falso negativo.

Os falsos negativos são preocupantes na cibersegurança porque indicam uma falha na capacidade do sistema de identificar adequadamente ameaças reais. Isso pode resultar em falta de resposta a incidentes de segurança genuínos, permitindo que atividades maliciosas ocorram sem serem detectadas. Portanto, minimizar falsos negativos é crucial para garantir a eficácia dos sistemas de segurança e a proteção adequada contra ameaças cibernéticas.

A Figura 2.8 mostra um resumo das quatro possibilidades de análise citadas até aqui.

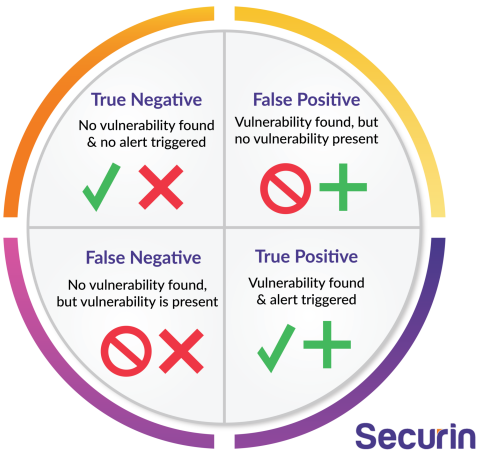

Figura 2.8: Esquemático que resume as quatro possibilidades de análise. Fonte: [8]

2.14 RUNBOOK

No contexto de cibersegurança, um runbook é um documento detalhado que fornece instruções, um passo a passo sobre como lidar com um alerta ou incidente de segurança específico. O termo runbook é derivado da ideia de que o documento fornece um conjunto de instruções que podem ser executadas como um "script" durante uma análise. Eles podem incluir informações sobre como identificar, conter, erradicar e recuperar-se de incidentes de segurança. Eles também podem incluir informações sobre a comunicação com partes interessadas, registros de eventos relevantes, ferramentas a serem utilizadas e outros detalhes importantes para lidar com um alerta ou incidente de segurança de maneira eficiente. Manter os runbooks atualizados e treinar a equipe para segui-los é uma prática importante na gestão do SOC, contribuindo para uma resposta coordenada e eficaz a incidentes.

2.15 PLAYBOOK

No contexto de cibersegurança, um playbook é um conjunto de procedimentos, diretrizes e melhores práticas organizadas de forma sistemática para ajudar as equipes a responderem a incidentes de segurança. Assim como os runbooks, os playbooks são documentos que fornecem orientações, um passo a passo, porém, o termo playbook é geralmente usado de forma mais ampla e pode se referir a estratégias abrangentes para abordar uma variedade de situações e não apenas incidentes de segurança específicos.

Os playbooks podem abranger diversas áreas da cibersegurança, incluindo resposta a incidentes, gestão de crises, conformidade regulatória, testes de segurança, entre outros. Eles são projetados para oferecer orientação consistente e eficiente durante a execução de tarefas específicas.

Em um playbook de resposta a incidentes, por exemplo, você pode encontrar informações sobre como identificar uma violação de segurança, quem contatar em caso de incidente, quais ações tomar para conter e erradicar a ameaça, como recuperar sistemas afetados e como conduzir uma análise pós-incidente. Os playbooks são uma parte essencial da gestão proativa da segurança cibernética, ajudando as organizações a estar preparadas para lidar com uma variedade de cenários de ameaças.

2.16 BLUE TEAM

O Blue Team é uma parte fundamental em um SOC e desempenha um papel crucial na defesa cibernética de uma organização. Eles são a equipe de defesa. Eles são responsáveis por manter a infraestrutura de TI segura, monitorar continuamente a rede em busca de ameaças, realizar análises de segurança, responder a incidentes e, em geral, proteger a organização contra ameaças cibernéticas. Eles monitoram os sistemas de segurança, como firewalls, IDS/IPS, registros de eventos de segurança e outros dispositivos para identificar atividades suspeitas ou indicadores de comprometimento.

Quando uma ameaça ou incidente de segurança é identificado, o Blue Team é encarregado de responder rapidamente para conter e mitigar a ameaça. Isso pode envolver isolar sistemas comprometidos, aplicar

patches de segurança, investigar a causa raiz do incidente e tomar medidas para evitar futuras ocorrências. O Blue Team também realiza análises pós-incidentes para entender como o incidente ocorreu, que danos foram causados e como a segurança pode ser aprimorada. Isso ajuda a organização a aprender com incidentes passados e a fortalecer suas defesas cibernéticas. O Blue Team também é responsável por implementar e fazer cumprir as políticas de segurança da organização, garantindo que todos os sistemas e funcionários estejam em conformidade com as diretrizes de segurança. A Figura 2.9 traz uma representação alegórica do que é o Blue Team.

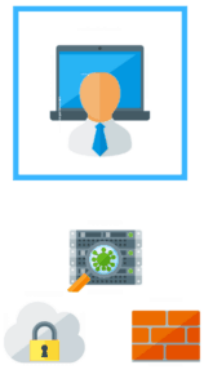

Figura 2.9: Representação alegórica do Blue Team. Fonte: [9]

O Blue Team muitas vezes trabalha em colaboração com o Red Team, que será melhor explicado a seguir, que é uma equipe que simula ataques cibernéticos para testar as defesas da organização. [25]

2.17 RED TEAM

O Red Team de um SOC desempenha um papel complementar ao Blue Team. Ele é fundamental para a avaliação da segurança cibernética de uma organização. O termo refere-se a uma equipe de profissionais de segurança cibernética que simula ataques cibernéticos contra a infraestrutura e sistemas de uma organização com o objetivo de identificar vulnerabilidades e fraquezas em suas defesas.

O Red Team atua como um adversário simulado, realizando ataques cibernéticos controlados contra os sistemas e redes da organização. Esses ataques podem incluir tentativas de invasão, exploração de vulnerabilidades, engenharia social e outras técnicas usadas por invasores reais. Seu objetivo principal é testar a eficácia das defesas cibernéticas da organização. Isso inclui avaliar a capacidade do Blue Team em detectar, responder e se defender contra os ataques simulados.

Durante os ataques simulados, o Red Team procura identificar vulnerabilidades de segurança, fraquezas em políticas de segurança e outros pontos de entrada que possam ser explorados por invasores reais. Eles documentam essas vulnerabilidades e relatam à equipe de segurança. O Red Team desempenha um papel importante na melhoria da postura de segurança da organização. Os relatórios de suas atividades permitem que a organização tome medidas corretivas para fortalecer sua segurança cibernética e reduzir riscos. [25] A Figura 2.10 traz uma representação alegórica do que é o Red Team.

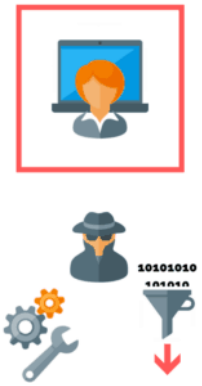

Figura 2.10: Representação alegórica do Red Team. Fonte: [9]

2.18 NIST

O National Institute of Standards and Technology, mais conhecido pela sigla NIST, é uma entidade não governamental americana que estimula a inovação através do progresso científico, estabelecimento de padrões e avanço na tecnologia de medição. O Framework de Cibersegurança do NIST (NIST CSF) é formado por normas, orientações e melhores práticas destinadas a auxiliar organizações no aprimoramento da gestão de riscos relacionados à segurança cibernética.

O NIST CSF foi idealizado com a flexibilidade necessária para integrar-se aos procedimentos de segurança já existentes em organizações de diversos setores. Ele representa um ponto de partida robusto para a implementação de medidas de segurança da informação e gestão de riscos cibernéticos em praticamente qualquer entidade do setor privado no mundo. [26]

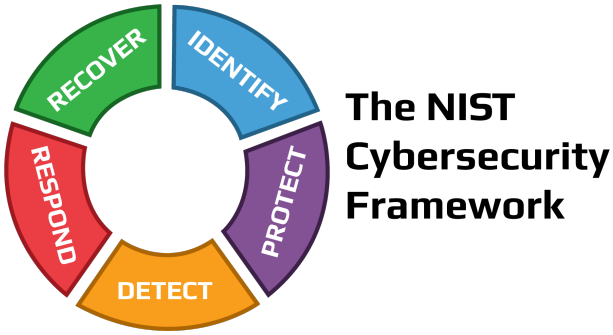

Figura 2.11: Logo do framework NIST CSF. Fonte: [10]

O NIST CSF compreende funções, categorias, subcategorias e referências informativas. As funções proporcionam uma visão geral das práticas ideais de segurança, sendo essenciais para formar uma cultura operacional contínua que aborde o risco dinâmico da segurança cibernética. Elas não devem ser consideradas como passos processuais isolados, mas sim como atividades a serem realizadas de maneira simultânea. Por sua vez, as categorias e subcategorias oferecem planos de ação mais específicos destinados a departamentos ou processos particulares dentro de uma organização [26]. Explicando a logo mostrada acima e exemplificando as funções e categorias do NIST, tem-se:

- Identificar: Para proteger contra ameaças cibernéticas, a equipe de segurança deve compreender completamente os ativos e recursos mais críticos da organização. A função de identificação engloba áreas como gerenciamento de ativos, ambiente de negócios, governança, avaliação de riscos e estratégia de gerenciamento de riscos.
- Proteger: Esta função abrange uma variedade de controles de segurança técnica e física para desenvolver e implementar proteções apropriadas, visando proteger a infraestrutura crítica. Categorias como gerenciamento de identidade e controle de acesso, conscientização e treinamento, segurança de dados, processos e procedimentos de proteção de informações, manutenção e tecnologia de proteção são abordadas.
- Detectar: A função de detecção implementa medidas que alertam a organização sobre possíveis ataques cibernéticos. Categorias de detecção incluem anomalias e eventos, monitoramento contínuo de segurança e processos de detecção.
- Responder: Categorias relacionadas à função de resposta garantem uma reação apropriada a ataques cibernéticos e outros eventos de segurança. Tópicos específicos abordados são planejamento de resposta, comunicações, análise, mitigação e melhorias.
- Recuperar: Atividades de recuperação implementam planos de resiliência cibernética, assegurando a continuidade dos negócios em caso de ataques cibernéticos, violações de segurança ou outros eventos. As funções de recuperação englobam melhorias no planejamento de recuperação e nas comunicações.

O NIST também possui um documento bem conhecido relacionado a resposta a incidentes, o Computer Security Incident Handling Guide. Ele é um documento que fornece diretrizes abrangentes para lidar com incidentes de segurança da informação. O guia visa auxiliar organizações na preparação, resposta e recuperação eficazes diante de eventos de segurança cibernética. Este será o procedimento que usaremos neste trabalho, por ser o mais conhecido e recomendado por especialistas na área. As fases do plano de resposta são mostradas na Figura 2.12. Ela será melhor explicada na Metodologia. [27]

Figura 2.12: Plano de de resposta a incidente do NIST. Fonte: [11]

Os principais tópicos abordados no documento são:

- Preparação: Aborda a importância de estabelecer e manter uma capacidade de resposta a incidentes. Isso envolve a criação de políticas, procedimentos e planos para lidar com incidentes de segurança;
- Detecção e Análise: Oferece orientações sobre como detectar incidentes de segurança, investigar suas causas e avaliar o impacto para entender a extensão do problema;
- Contenção, Erradicação e Recuperação: Descreve estratégias para conter a propagação de incidentes, eliminar ameaças, restaurar sistemas e dados afetados, e retornar às operações normais;
- Comunicação e Cooperação: Destaca a importância da comunicação eficaz durante um incidente, tanto internamente quanto externamente. Inclui orientações sobre como colaborar com outras organizações, compartilhando informações relevantes;
- Documentação: Sugere práticas para documentar detalhes relacionados ao incidente, incluindo a coleta de evidências, a fim de apoiar análises futuras e melhorar a postura de segurança da organização;
- Melhoria Contínua: Enfatiza a necessidade de avaliar o desempenho após um incidente, identificando lições aprendidas e ajustando políticas e procedimentos para melhorar a resiliência e a capacidade de resposta no futuro.

Em resumo, este documento do NIST fornece um conjunto abrangente de diretrizes e boas práticas para ajudar as organizações a se prepararem para, responderem a, e se recuperarem de incidentes de segurança da informação, visando melhorar a postura geral de segurança cibernética.

2.19 SANS

Systems Administration and Network Security, em português, Administração de Sistemas e Segurança de Rede, mais conhecido pela sigla SANS, é líder global em treinamento, certificação e pesquisa em segurança da informação. Fundada em 1989, a SANS dedica-se a ajudar profissionais e organizações a permanecerem à frente do cenário de ameaças em constante evolução.

SANS oferece cursos de treinamento práticos abrangentes e certificações em segurança da informação e segurança cibernética, bem como uma variedade de outros tópicos relacionados à segurança. Através de sua rede global de centros de treinamento, a SANS oferece cursos sobre uma ampla variedade de tópicos, incluindo resposta a incidentes, análise forense, análise de malware e codificação segura.

O SANS Institute também fornece vários recursos para ajudar organizações e profissionais a se manterem atualizados sobre as mais recentes ameaças, tendências e práticas recomendadas de segurança. Esses recursos incluem blogs, boletins informativos, webcasts e conferências.

SANS também é líder em pesquisa de segurança cibernética. O SANS Institute publicou centenas de artigos de pesquisa e white papers sobre tópicos como resposta a incidentes, análise de malware e

codificação segura. O Instituto também fornece uma variedade de ferramentas relacionadas à segurança, como o SANS Internet Storm Center, que fornece análises em tempo real de ameaças cibernéticas.

O SANS Institute está empenhado em ajudar organizações e profissionais a permanecerem à frente do cenário de ameaças em constante evolução. Através de seu treinamento e pesquisa abrangentes, a SANS fornece o conhecimento e as habilidades necessárias para responder de forma rápida e eficaz a incidentes de segurança.

Eles também possuem um Plano de Resposta a Incidentes, que é uma estrutura que as organizações usam para responder a incidentes de segurança. Ele foi projetado para ajudar as organizações a responder de forma rápida e eficaz. O plano descreve as etapas que precisam ser tomadas para identificar, conter, erradicar e se recuperar de incidentes de segurança. Inclui também medidas para garantir que sejam retiradas lições do incidente e que sejam tomadas medidas adequadas para prevenir incidentes futuros.

O Plano de Resposta a Incidentes SANS é baseado em 6 componentes: preparação, identificação, contenção, erradicação, recuperação e lições aprendidas.

1. Preparação: O primeiro passo é preparar-se para um incidente de segurança. Isto inclui a criação de um plano para responder a um incidente de segurança, a definição de funções e responsabilidades para responder a um incidente de segurança e a garantia de que as ferramentas e recursos necessários estão disponíveis;

2. Identificação: A segunda etapa é identificar um incidente de segurança. Isto inclui o monitoramento de incidentes de segurança, o reconhecimento de indicadores de comprometimento e a determinação do escopo e do impacto do incidente;

3. Contenção: A terceira etapa é conter o incidente de segurança. Isso inclui isolar os sistemas afetados, desabilitar contas de usuários e evitar maiores danos;

4. Erradicação: O quarto passo é erradicar o incidente de segurança. Isso inclui a remoção de software malicioso, correção de sistemas vulneráveis e restauração de dados afetados;

5. Recuperação: A quinta etapa é recuperar-se do incidente de segurança. Isso inclui restaurar os sistemas para um estado bom conhecido, restaurar dados e validar se o incidente foi completamente resolvido;

6. Lições aprendidas: A sexta e última etapa é aprender com o incidente de segurança. Isto inclui a análise do incidente para identificar as causas profundas, avaliar a eficácia da resposta e implementar medidas para prevenir incidentes semelhantes no futuro.

O Plano de Resposta a Incidentes SANS fornece às organizações uma abordagem estruturada para responder a incidentes de segurança. Seguindo as etapas descritas no plano, as organizações podem responder de forma rápida e eficaz aos incidentes de segurança e minimizar os danos causados pelo incidente. O esquemático mostrado na Figura 2.13 mostra o plano de resposta a incidentes. [12]

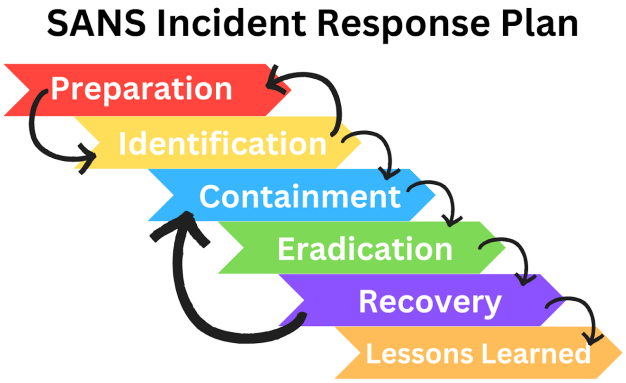

Figura 2.13: Plano de resposta a incidentes da SANS. Fonte: [12]

2.20 MSP E MSSP

Os Provedores de Serviços Gerenciados (MSPs) desempenham a função de monitorar, supervisionar e garantir a execução contínua e remota de processos terceirizados, especialmente aqueles relacionados à tecnologia, a partir de um centro centralizado de gerenciamento. Um exemplo concreto seria uma empresa que mantém um Centro de Operações de Rede (NOC) para monitorar a infraestrutura de vários clientes. Outro exemplo seria uma empresa que utiliza tecnologias para gerenciar operações como backups e atualizações de software para outras empresas. Isso proporciona uma redução de custos ou uma especialização mais acentuada em áreas específicas. A escolha e contratação dessas empresas são feitas conforme a necessidade do cliente.

Para otimizar os custos trabalhistas, os MSPs incorporam softwares de monitoramento e gerenciamento remoto. Isso viabiliza a resolução de problemas à distância e a capacidade de atender simultaneamente a múltiplos clientes. Além das funções mencionadas, essas empresas podem oferecer serviços adicionais, como aplicativos para a gestão de servidores, redes e outras especialidades destinadas aos usuários finais das organizações.

Ao optar pelos serviços de MSPs, as empresas eliminam a necessidade de manter uma equipe de TI em tempo integral. Ao mesmo tempo, têm a vantagem de poder acionar a empresa contratada quando precisarem de assistência técnica especializada. Geralmente o monitoramento se dá de maneira 24x7.

Além da economia de custos, a utilização desses serviços proporciona segurança. Os MSPs podem garantir a realização de backups de segurança dos dados e a atualização de softwares e sistemas operacionais, entre outras medidas. A Figura 2.14 mostra exemplos de serviços que podem ser prestados por um MSP.

As empresas que se especializam em serviços gerenciados de segurança são conhecidas como Managed Security Services Providers (MSSPs) ou provedores de serviços gerenciados de segurança.

As MSSPs costumam prestar serviços no modelo 24×7 também e oferecem serviços como administração de firewall a distância e disponibilização dos dados gerenciais ao cliente a partir de um portal próprio. [28]

Figura 2.14: Exemplo de serviços que podem ser prestados por um MSP. Fonte: [13]

2.21 UEBA

A análise de comportamento de usuários e entidades, mais conhecida pela sigla UEBA, é um tipo de software de segurança que utiliza análise comportamental, algoritmos de aprendizado de máquina e automação para identificar comportamentos anormais e potencialmente perigosos de usuários e dispositivos. A UEBA é particularmente eficaz na identificação de ameaças internas, como insiders maliciosos ou hackers que utilizam credenciais internas comprometidas, os quais podem passar despercebidos por outras ferramentas de segurança, uma vez que imitam o tráfego de rede autorizado.

O termo UEBA, cunhado pela primeira vez pela Gartner em 2015, representa uma evolução da análise de comportamento de usuários (UBA). Enquanto a UBA apenas acompanhava padrões de comportamento de usuários finais, a UEBA também monitora entidades não relacionadas a usuários, como servidores, roteadores e dispositivos IoT, em busca de comportamentos anômalos ou atividades suspeitas que possam indicar ameaças ou ataques de segurança.

A UEBA é utilizada em um SOC em conjunto com outras ferramentas de segurança empresarial, e sua funcionalidade muitas vezes está incluída em soluções de segurança empresarial, como SIEM, EDR e XDR. [29]

2.22 INTELIGÊNCIA DE AMEAÇAS

A Inteligência de Ameaças, do inglês, Threat Intelligence, refere-se à coleta, processamento e análise de dados para compreender o comportamento de ataques de adversários. Esse tipo de inteligência possibilita tomadas de decisão em segurança mais rápidas, informadas e baseadas em dados, permitindo a transição de um estado reativo para um proativo.

Atualmente, o setor de segurança cibernética enfrenta diversos desafios, incluindo a persistência cres-

cente de ataques, o volume diário de dados repletos de informações e alarmes falsos em vários sistemas de segurança, além da escassez de profissionais qualificados.

Algumas organizações tentam incorporar fontes de dados de ameaças em suas redes, mas enfrentam dificuldades em lidar com esses dados brutos, aumentando a carga de trabalho dos analistas. O processo de inteligência de ameaças é composto por seis fases, descritas abaixo e são ilustradas na Figura 2.15. [30]

1. Planejamento e Direção: Formular as perguntas adequadas para impulsionar a criação de inteligência de ameaças. Priorizar objetivos com base nos valores da organização, impacto da decisão e sensibilidade ao tempo;
2. Coleta: Coletar dados brutos que atendam aos requisitos definidos. Utilizar uma variedade de fontes internas e externas, como logs de eventos de rede e registros de incidentes anteriores;
3. Processamento: Classificar e organizar os dados brutos com tags de metadados. Automatizar a coleta e processamento para lidar com a grande quantidade de dados;
4. Análise: Compreender os dados processados em busca de possíveis problemas de segurança. Apresentar a inteligência de ameaças em formatos compreensíveis, como listas ou relatórios revisados;
5. Divulgação: Distribuir a inteligência acabada aos consumidores pretendidos no momento adequado. Rastrear a continuidade entre ciclos de inteligência para preservar o aprendizado;
6. Comentários: Analisar o relatório final de inteligência e determinar se as dúvidas foram respondidas. Impulsionar objetivos e procedimentos para o próximo ciclo de inteligência.

A inteligência de ameaças também é dividas em três tipos:

- Estratégico: Informações amplas para um público não técnico;
- Tático: Detalhes das táticas, técnicas e procedimentos para um público mais técnico;
- Operacional: Conhecimento técnico sobre ataques específicos.

O uso da inteligência de ameaças na prática se dá em casos como, investigação da exposição de informações, URLs e IPs com ferramentas como Shodan, Censys e Google Dorks. Utilização de ferramentas como VirusTotal, URL Haus Abuse e IP Abuse para bloquear IPs e domínios suspeitos. Utilização do Mitre Att&ck para entender e mapear adversários. Utilização de SIEMs para estruturar dados e bases colaborativas como MISP para consultar ameaças potenciais. [30]

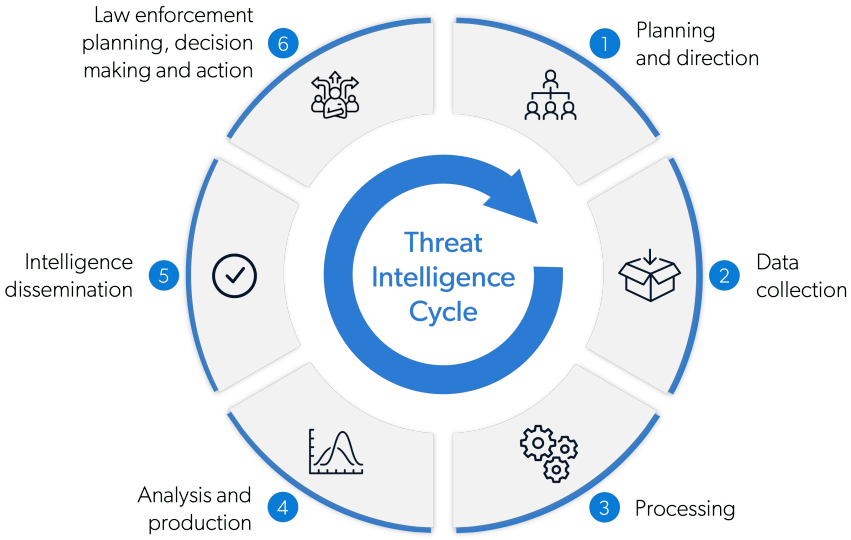

Figura 2.15: Fases da inteligência de ameaças. Fonte: [14]

3 METODOLOGIA

Neste capítulo, será mostrada a metodologia em que todo esse trabalho se baseará, as fases a serem percorridas, qual é o ambiente a ser considerado e quais serão as ferramentas utilizadas para que seja feita a análise e discussão das melhores práticas. É importante ser levado em consideração, que a situação analisada se baseará, em uma possibilidade menor e mais barata de estrutura de SOC, porém serão citadas outras tecnologias e tendências que podem serem aplicadas. [15] [31]

3.1 CENÁRIO INICIAL

O cenário inicialmente proposto refere-se a uma empresa de TI que presta serviços gerenciados a seus clientes, ou seja, ela é um MSP. Vamos chamá-la de empresa ACME. Os serviços prestados por ela são gerenciamento de infraestrutura de rede em clientes externos. Levando este cenário em conta, a ideia deste trabalho é mostrar quais seriam as melhores práticas de análise de alertas e incidentes da maneira mais simples e direta no SOC interno da empresa, ou seja, é um serviço para a própria empresa ACME, o que será monitorado serão os colaboradores que trabalham lá e a sua própria infraestrutura de rede e demais dispositivos. Este é um trabalho inicial, que pode ser complementado de diversas formas, com diversos outros serviços, que serão melhor comentados adiante. A infraestrutura de rede da empresa é composta por roteadores, switches, firewall e dispotivos finais. Os alertas serão recebidos na interface de um SIEM, onde estão inventariados todas as máquinas da rede, sendo conhecidos seus endereços de IP, MAC e demais informações.

Antes de começarmos a proposta do trabalho, é preciso entender a diferença entre um alerta e um incidente de segurança. No contexto de um SOC e deste trabalho, a diferença entre eles está relacionada à gravidade e à validação do ocorrido. As diferenças principais são, um alerta é uma notificação gerada por uma ferramenta de monitoramento de segurança em resposta a um evento que pode indicar uma possível ameaça. Nem todos os alertas se traduzem automaticamente em incidentes. Muitos alertas podem ser benignos ou ter uma explicação não maliciosa. Os alertas podem variar em criticidade, como já citado anteriormente.

Já um incidente de segurança é uma situação confirmada em que ocorreu uma violação da segurança ou ocorreu uma tentativa bem-sucedida de exploração de vulnerabilidades. Nem todos os alertas se transformam em incidentes, no entanto, um incidente na maioria das vezes começa com a detecção de um alerta. A validação de um alerta como um incidente envolve uma análise mais aprofundada para determinar se uma ameaça real está ocorrendo e qual será o impacto potencial. Essa validação será melhor detalhada adiante.

Em resumo, um alerta é uma notificação inicial que pode indicar um potencial problema, enquanto um incidente de segurança é uma confirmação de que ocorreu uma violação de segurança real. A transição de alerta para incidente ocorre após a validação e análise detalhada da ameaça. O SOC desempenha um papel fundamental nesse processo, garantindo uma resposta eficaz a alertas significativos que se transformam em incidentes de segurança.

3.2 PROPOSTA

Esse trabalho seguirá algumas fases, descritas a seguir:

- Fase 1: Estruturação da equipe do SOC;
- Fase 2: Instalação da solução de SIEM escolhida e demais configurações;
- Fase 3: Criação da documentação e do processo de como o SOC funcionará;
- Fase 4: Emulação do ambiente em produção;
- Fase 5: Serviços, tecnologias, métricas, o futuro do SOC e ameaças emergentes.

3.2.1 Fase 1: Estruturação da equipe do SOC

Este trabalho foi todo desenvolvido levando em conta o SOC interno da empresa ACME, como já citado anteriormente. A equipe do SOC e suas respectivas funções, começando do cargo mais baixo para o mais alto, serão mostradas abaixo. [15]

- **Analista de Segurança 1 (Júnior):** É responsável por monitorar continuamente o SIEM a fim de tratar os alertas quando eles chegam, ou seja, quando um evento ocorre e um alerta é gerado no SIEM, ele é o primeiro a atuar. Caso seja a primeira vez que o alerta chegou ao SIEM, ele aciona o Analista de Segurança 2 para ajudá-lo a abrir o chamado interno e fazer a documentação referente àquele alerta.
- **Analista de Segurança 2 (Pleno):** Tem mais expertise que o Analista de Segurança 1, sendo assim, quando o primeiro analista não sabe qual ação tomar para validar o alerta, ou quando se depara com um novo alerta, não documentado, ele aciona o Analista de Segurança 2, que com sua maior experiência propõe uma solução, assim ajudando o Analista de Segurança 1 a montar o chamado ou a encaminhar para o Analista de Infraestrutura, caso necessário.
- **Analista de Segurança 3 (Sênior):** É o mais experiente entre os analistas, o que tem mais conhecimento técnico, tanto do SIEM, quanto de cibersegurança no geral, caso nenhum dos analistas anteriores consigam atender o alerta, e propor uma forma de analisá-lo, ele é acionado. Ele atua diretamente em melhorias constantes no ambiente da empresa junto com o Engenheiro de Cibersegurança. Os analistas de segurança citados até aqui, junto com o Engenheiro de Cibersegurança, fazem parte do que categorizamos anteriormente como Blue Team.
- **Pentester:** Pode ser um agente externo a equipe do SOC em si, porém desempenha um papel crucial ao ajudar a identificar e corrigir vulnerabilidades nos sistemas da organização. Ele trabalha em estreita colaboração com a equipe do Blue Team para fortalecer a postura de segurança da organização. Ele faz parte do que categorizamos anteriormente como Red Team.
- **Analista de Infraestrutura:** Ele não faz parte do SOC em si, mas faz parte do time de TI da empresa, ele atua junto com os analistas de segurança caso necessário em alguma demanda que seja preciso

uma atuação direta em algum dispositivo da rede da empresa, seja ele roteador, switch, máquinas de usuários e etc.

- **Líder Técnico:** Ele desempenha um papel fundamental na gestão e liderança da equipe de analistas de segurança. Sua função envolve não apenas habilidades técnicas aprimoradas, mas também a capacidade de coordenar operações, desenvolver estratégias eficazes e garantir a eficiência do SOC como um todo. Ele está abaixo somente do Gestor do SOC e no mesmo nível de articulação do Engenheiro de Cibersegurança.
- **Engenheiro de Cibersegurança:** É responsável por configurar e atualizar as ferramentas de segurança, desde do SIEM, até os firewalls, IDS/IPS e antivírus. Ele também desenvolve as políticas de segurança da empresa e procedimentos a serem tomados em cada tipo de incidente.
- **Gerente do SOC:** O gerente de SOC supervisiona a equipe toda, ele é o cargo mais alto dentro de um SOC, ele estabelece as metas e estratégias de segurança, e relata o desempenho da equipe à alta administração da empresa. Ele é responsável por garantir que o SOC esteja alinhado com as políticas de segurança da empresa.

Os cargos acima citados não estão limitados a uma pessoa por cargo, geralmente em uma empresa grande estes cargos possuem múltiplas pessoas, entretanto, o cargo que normalmente é ocupado somente por uma pessoa é o cargo de gerência do SOC. O fluxograma mostrado na Figura 3.1 ilustra melhor a divisão da equipe.

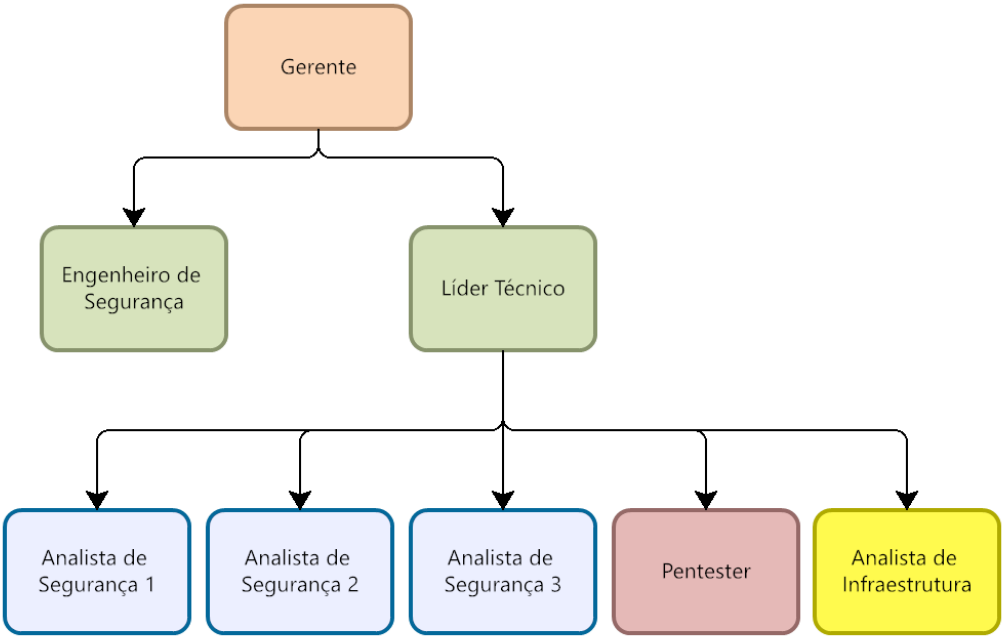

Figura 3.1: Fluxograma da hierarquia do SOC que iremos considerar para esta análise de caso. Fonte: Elaboração própria

A diferenciação de cores se dá pelas áreas de atuação, sendo em laranja a gerência, em verde os cargos

técnicos, em azul o Blue Team, em vermelho o Red Team e em amarelo membros adicionais/externos da equipe.

3.2.2 Fase 2: Instalação da solução de SIEM escolhida e demais configurações

Será abstraído deste trabalho o processo de instalação do SIEM e demais configurações. Este trabalho será focado nas melhores práticas de análise de alertas e incidentes, ou seja, será considerado que o SIEM está configurado e recebendo eventos e alertas das fontes monitoradas.

3.2.3 Fase 3: Criação da documentação e do processo de como o SOC funcionará

Os processos estabelecidos para lidar com alertas e incidentes de segurança são elementos fundamentais para garantir a eficácia de um SOC. Diante de um incidente, é imperativo que a equipe do SOC atue com agilidade e eficiência para limitar os prejuízos e prevenir a ocorrência de novos incidentes. [15]

3.2.3.1 Alertas

Nesta seção iremos considerar todo o processo de análise de um alerta e a resposta a um incidente. Começando pelos alertas, o processo de análise de um alerta é mostrado na Figura 3.2.

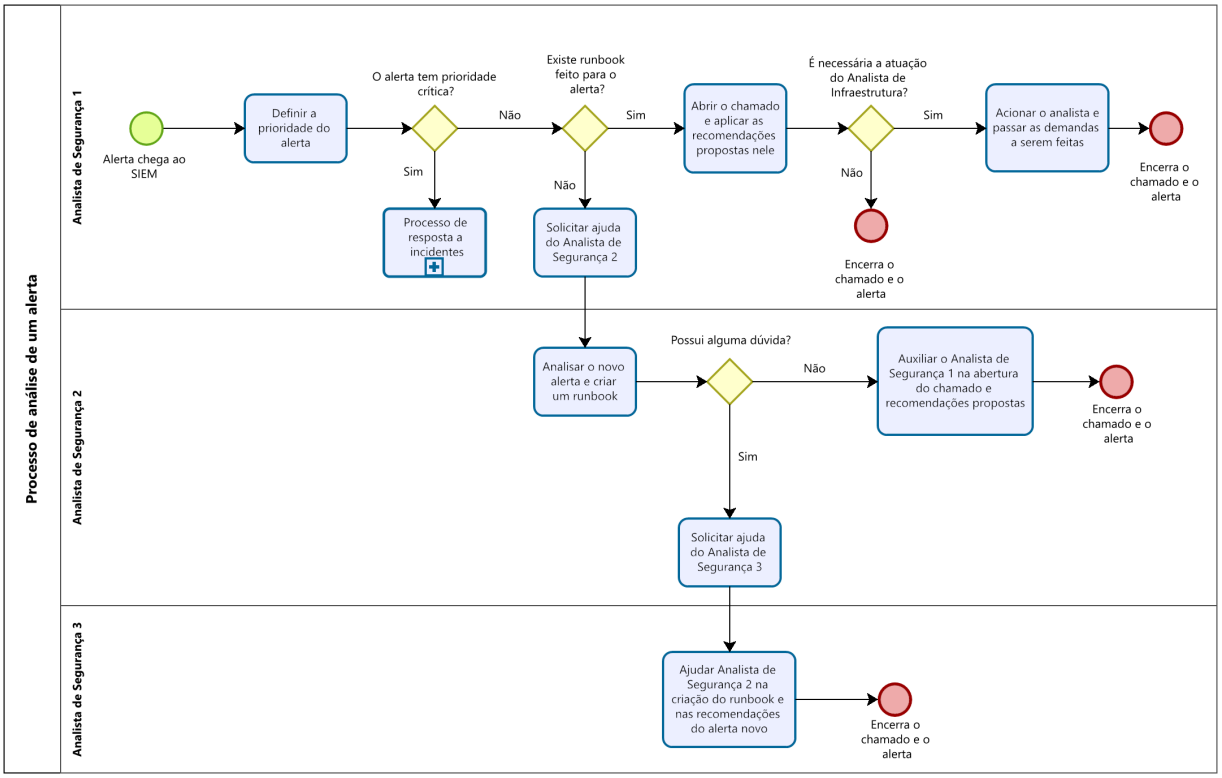

Figura 3.2: Fluxograma do processo de análise de um alerta que chega ao SIEM. Fonte: Elaboração própria

Quando um alerta chega ao SIEM, o primeiro a fazer essa análise inicial é o Analista de Segurança 1.

A primeira ação dele é definir a prioridade do alerta, ele deve levar em consideração a prioridade dada pelo SIEM e definir a prioridade a ser usada nas tratativas internas. Ele fará isso com base no contexto do alerta, ou seja, levando em conta o conhecimento dele sobre a organização e sua infraestrutura. É importante salientar que essa prioridade pode mudar a depender das validações feitas e das recomendações a serem tomadas.

Caso o alerta tenha prioridade baixa, média ou alta, o processo chega a um ponto de decisão. Caso seja de uma das três prioridades, o alerta continuará a ser analisado como um alerta, caso não seja, assim sendo, de prioridade crítica, existe outro processo, já que o alerta se torna um incidente, esse processo será melhor explicado mais adiante. Isso não quer dizer que alertas de prioridade baixa, média e alta não possam ser considerados incidentes, vai depender das validações feitas e das recomendações a serem tomadas. Caso tenha sido constatado após a análise que realmente houve características que categorizam como um incidente, a prioridade e procedimento de resposta do alerta podem ser mudados.

Considerando que o alerta não seja de prioridade crítica, tem-se outro ponto de decisão. Existe um runbook feito para este tipo de alerta? Caso não tenha, o Analisa de Segurança 2 é acionado para ajudar na confecção do documento e na abertura do chamado interno, caso ele tenha alguma dúvida, ele aciona o Analista de Segurança 3 para ajudá-los na análise. Ao longo desse processo, caso tenha alguma validação ou recomendação a ser tratada diretamente na infraestrutura da empresa, o Analista de Infraestrutura pode ser acionado e por fim o chamado interno e o alerta são encerrados.

Caso tenha um runbook feito, o Analista de Segurança 1 continua as tratativas, sendo assim, o chamado interno é aberto e as validações ou ações, caso necessárias, realizadas, com ou sem o apoio do Analista de Infraestrutura e o chamado interno e o alerta são encerrados. Caso após a validação tenha sido constatado que o alerta se tratou de um falso positivo, o alerta é fechado, podendo ou não ter sido chamado aberto, a depender de qual fase da análise foi constatado ser um FP.

Caso seja necessário suprimir o alerta, a supressão é feita nesta fase. Um ponto a ser levado em consideração aqui é, caso um alerta seja considerado um FP para um usuário, não quer dizer que ele será FP para outros usuários da empresa, por conta disso, muitas vezes é necessário que seja feita uma validação caso a caso. Porém existem exemplos de alertas novos que após uma primeira validação, futuros alertas semelhantes serão considerados FP para a empresa, ai é feita a supressão do alerta, sem levar em consideração o usuário presente nele.

O chamado interno se faz importante nesse procedimento a fim de ficar documentado tudo que foi feito para a solução daquele alerta/incidente, para que futuros casos, possam ter além do runbook, um caso real para se basearem e terem parâmetro de análise e comparação.

3.2.3.2 Incidentes

Os alertas que são recebidos no SIEM com prioridade crítica costumam ter procedimentos específicos mapeados em playbooks de incidentes, geralmente alertas críticos são situações que interrompem o funcionado de determinado sistema ou parte dele. São exemplos de alerta de prioridade crítica, que por consequência se tornam incidentes logo que chegam ao SIEM, um ransomware detectado, um ataque DDoS, vazamento de dados confidenciais dentre outros. Na documentação utilizada para tratar o incidente

teremos o seguinte passo a passo a ser analisado e validado:

O processo mostrado na Figura 2.12 é o plano de resposta a incidentes do NIST, onde temos quatro fases que serão melhor explicadas a seguir.

Como já citado anteriormente, é crucial que o SOC possua um plano de resposta a incidentes claramente delineado, especificando os passos a serem tomados para identificar, reagir e se recuperar de incidentes de segurança. Esse plano deve abranger atribuições de tarefas e responsabilidades, diretrizes para escalonamento, protocolos de comunicação e critérios para documentação. Essa fase é conhecida como preparação.

A equipe do SOC necessita de instrumentos de monitoramento em tempo real para identificar incidentes de segurança no momento em que acontecem. Ao identificar um incidente, é responsabilidade da equipe do SOC validar a ocorrência e avaliar o alcance e as consequências do incidente. Essa é a fase de Detecção e Análise.

A equipe de SOC precisa controlar o incidente a fim de prevenir danos mais extensos. Isso inclui ações como isolar os sistemas ou dispositivos impactados, bloquear o tráfego prejudicial e desconectar os sistemas comprometidos da rede. É necessário realizar uma investigação do incidente para identificar a causa e a extensão do ataque. Isso requer a análise de registros e outras fontes de dados, bem como a aplicação de inteligência contra ameaças. A equipe de SOC precisa ter um plano de resposta para corrigir o incidente. Isso pode incluir a aplicação de correções ou atualizações, a recuperação de dados de backups ou a reconstrução de sistemas. Além disso, o SOC deve trabalhar proativamente para prevenir a ocorrência de incidentes semelhantes no futuro. Essa é a fase de Contenção, Erradicação e Recuperação.

Após a conclusão da análise, com o chamado interno encerrado e as referidas tratativas feitas, é necessário que a equipe do SOC conduza uma análise pós-incidente para identificar possíveis melhorias. Isso implica na revisão do processo de resposta a incidentes, na identificação de lacunas ou vulnerabilidades, e no desenvolvimento de um plano para abordá-las.

4 ANÁLISE E DISCUSSÃO

Neste capítulo, será feita a análise e discussão baseada na metodologia descrita anteriormente, abrangendo as Fases 4 e 5 propostas. Será mostrado como seriam feitas as análises propostas em casos reais, ou seja, serão emuladas análises com base em alertas chegaram ao SIEM da empresa ACME, eles tiveram suas informações alteradas para que fosse preservado a privacidade dos dados. Os alertas de exemplo, foram retirados do SIEM USM Anywhere da empresa AT&T. Ele é um SIEM que centraliza o monitoramento de segurança de redes e dispositivos na nuvem, porém, podendo ter agentes instalados nas máquinas locais, detectando ameaças praticamente em qualquer dispositivo que esteja conectado na rede.

4.1 FASE 4: EMULAÇÃO DO AMBIENTE EM PRODUÇÃO

4.1.1 Análise de alertas: Caso 1

O primeiro alerta a ser considerado será um alerta de Logon na VPN fora do Brasil, ele é mostrado na Figura 4.1.

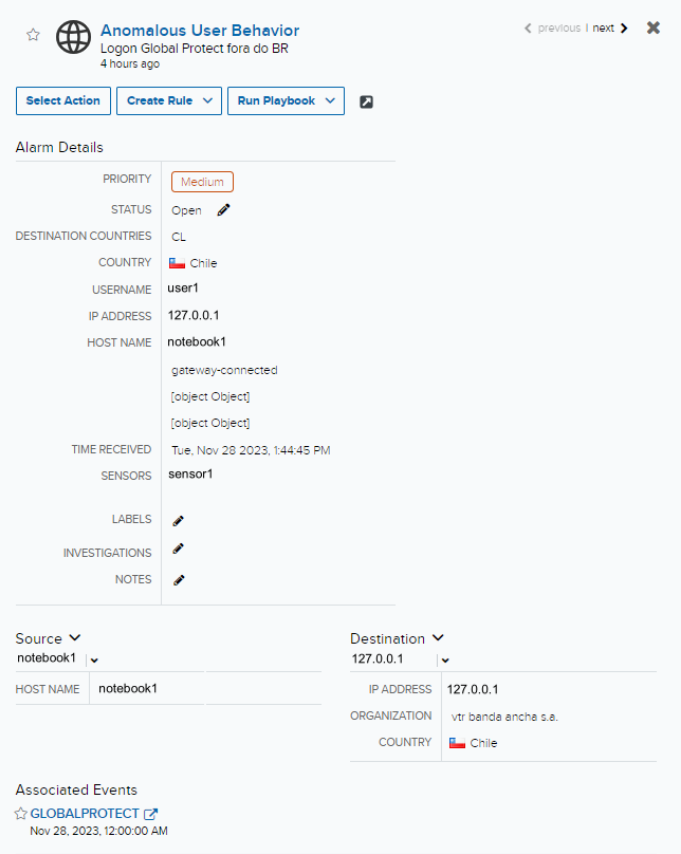

Figura 4.1: Alerta de logon na VPN fora do Brasil. Fonte: USM Anywhere da Empresa ACME

Esse alerta se refere a um logon bem sucedido fora do Brasil na VPN da empresa. Será considerada a solução de VPN da empresa Palo Alto, chamada Global Protect. A empresa ACME que tem colaboradores espalhados por todo o Brasil, eles usam essa VPN para se conectar com a infraestrutura de redes da empresa. Seguindo o fluxograma presente na Figura 3.2, onde tem-se o passo a passo do processo de análise de um alerta, temos que assim que o alerta chega, é definida a prioridade dele (Figura 4.2).

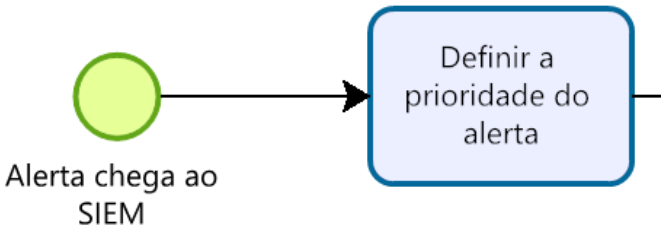

Figura 4.2: Fase do fluxograma onde é definida a prioridade do alerta. Fonte: Elaboração própria

Neste primeiro caso, o SIEM trouxe o alerta com prioridade média, essas prioridades são determinadas pelo SIEM com base nas regras criadas para geração de alertas e na detecção do comportamento suspeito feita pelo SIEM, ou seja, os parâmetros configurados inicialmente no SIEM fazem com que cada alerta tenha sua prioridade determinada. Neste caso cabe ao analista decidir qual será a prioridade final a ser considerada, levando em conta o contexto do alerta, mesmo que o alerta tenha chegado ao SIEM com prioridade média, caso o analista veja que aquele comportamento é algo divergente após uma validação rápida, o alerta pode mudar de prioridade dentro da escala proposta, caso ela seja considerado crítico, existe o procedimento de resposta a incidente. Para fim de continuidade da explicação, a prioridade do chamado será mantida, a fim de que seja analisado melhor, ao longo do processo, essa tomada de decisão é mostrada na Figura 4.3, onde é mostrada a referida fase no fluxograma da Figura 3.2.

Figura 4.3: Fase do fluxograma onde é validado se o alerta tem prioridade crítica ou não. Fonte: Elaboração própria

É validado se existe ou não runbook para o alerta. Esse ponto de decisão é mostrado na Figura 4.4.

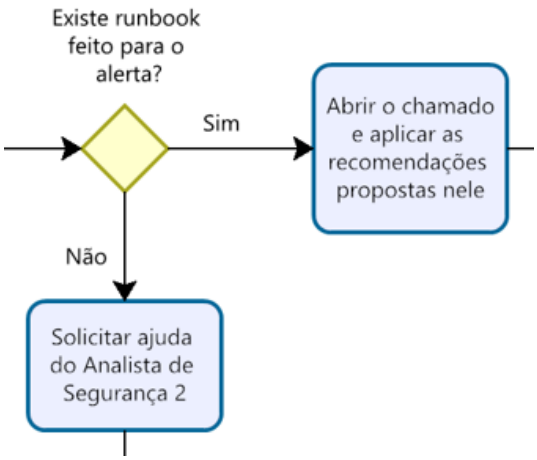

Figura 4.4: Fase do fluxograma onde é validado se existe runbook para o alerta. Fonte: Elaboração própria

Caso não haja runbook feito, o Analista de Segurança 2 é acionado e o processo continua seguindo o fluxograma mostrado na Figura 4.5 com outros pontos de decisão, que podem envolver ou não o Analista de Segurança 3 e o Analista de Infraestrutura.

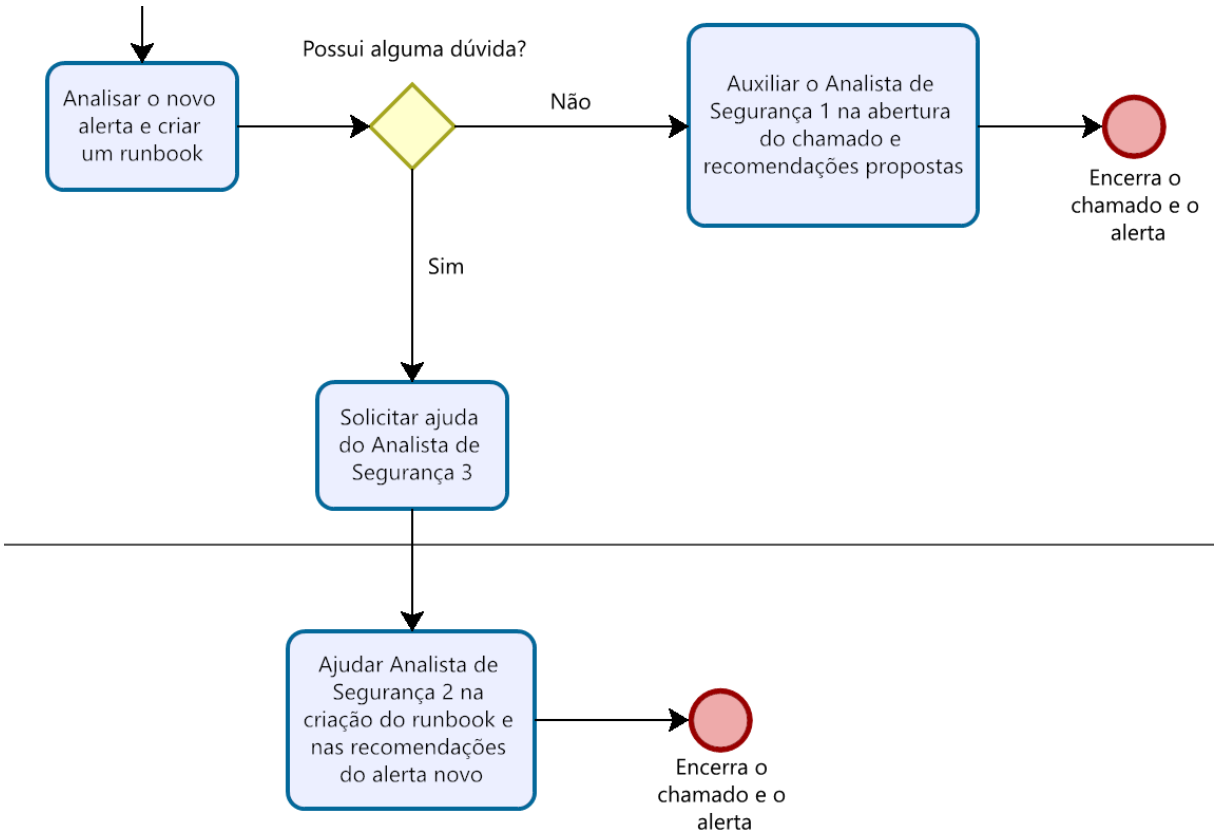

Figura 4.5: Restante do processo caso não haja runbook feito para o alerta. Fonte: Elaboração própria

Dando prosseguimento a análise, será considerado a existência de um runbook para aquele alerta, essa documentação já foi feita anteriormente e que as recomendações presentes no runbook, são:

- Validar com o usuário se ele realizou o logon fora do Brasil, mais precisamente no país presente no alerta, no dia e horário presentes no alerta.

Neste caso, é tomada a ação presente no runbook e a validação documentada no chamado seria, "Validar com o usuário user1, se ele realizou logon na VPN fora do Brasil, mais precisamente no Chile, no dia 28/11/2023 às 13:44."Essa validação é feita pelo próprio Analista de Segurança 1, diretamente com o usuário a fim de entender o ocorrido, pois se trata de um comportamento anormal.

Aqui é onde se chega numa parte da análise em que o cenário pode mudar completamente, existem duas possibilidades. Caso o usuário valide a ação, o alerta é considerado um FP, e é fechado, a resposta do usuário é documentada no chamado interno e ele também é encerrado. Porém, caso o usuário não valide a ação, o alerta se torna um VP, o que faz ele se tornar um incidente de segurança da informação, nesse caso, deverão ser tomadas medidas a fim de tratar o incidente. Um exemplo de recomendação ao usuário seria de troca de senha e a finalização de todas as sessões de VPN. Essas ações são tomadas de imediato pois a não validação da ação pelo usuário indica que suas credenciais foram comprometidas. O incidente deve passar por todas as fases já citadas a fim de entender melhor o ocorrido. Essa validação com o usuário se torna fundamental quando o alerta trata diretamente da ação do usuário, pois a resposta do usuário é o limiar que determina se é um FP ou um VP. Caso o alerta apresente uma máquina e não um usuário, é feita uma validação diretamente no dispositivo, é o caso que será analisado a seguir, o Caso 2.

4.1.2 Caso 2

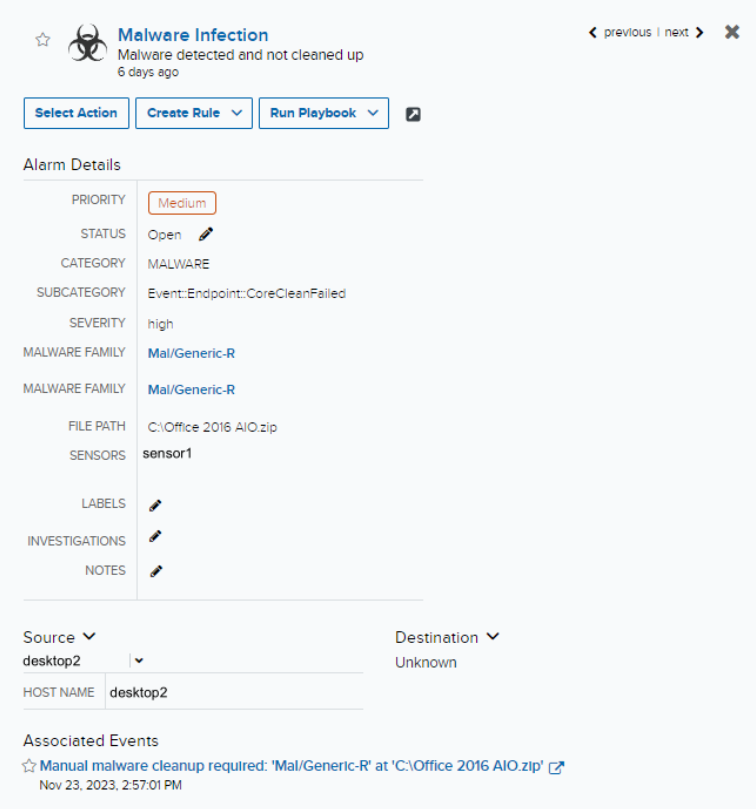

Figura 4.6: Alerta de malware detectado e não limpo. Fonte: USM Anywhere da Empresa ACME

O alerta mostrado na Figura 4.6 se refere a um malware detectado em uma máquina onde o antivírus não conseguiu fazer a limpeza automática do arquivo malicioso, sendo assim, a limpeza deve ser feita de maneira manual. Este alerta vem da fonte de dados do antivírus Sophos, como citado anteriormente não será explicado como funciona a captação dos logs, vamos considerar que ele são recebidos pelo SIEM.

Seguindo o fluxograma presente na Figura 3.2, seguindo o passo a passo do processo de análise de um alerta, tem-se que assim que o alerta chega, é definida a prioridade dele (Figura 4.2), o SIEM trouxe como prioridade média, neste caso a prioridade do chamado será alterada pelo analista para alta, por se tratar de um malware detectado e não limpo, ou seja, um caso que requer atenção imediata (Figura 4.3).

É validado se existe ou não runbook para o alerta (Figura 4.4), neste caso, vamos considerar que não existe um runbook, o Analista de Segurança 1, deverá acionar o Analista de Segurança 2 a fim de criar a documentação para o caso, eles abrem juntos o chamado interno, decidem quais serão as ações a serem tomadas e após o tratamento do alerta a documentação é feita, a prioridade sempre será o tratamento do alerta (Figura 4.5). As validações a serem feitas, serão:

- Validar se o arquivo é efetivamente malicioso e apagar manualmente o arquivo presente no caminho presente no alerta.

Neste caso, ação é feita e a validação é documentada no chamado interno, a recomendação documentada seria, "Apagar manualmente o arquivo malicioso presente no caminho "C:/Office 2016 AIO.zip". Essa ação é feita pelo próprio Analista de Segurança 1, na máquina presente no alerta, caso seja um servidor, ele faz o acesso remoto direto, caso seja uma máquina de usuário, o acesso é combinado de antemão com o usuário e o analista faz o acesso a fim de remover o arquivo. Existe a possibilidade dessas ações serem automatizadas no SIEM, esse tópico será abordado melhor adiante.

4.1.3 Análise de um incidente: Caso 3

Diferente das análises dos alertas anteriores, no exemplo de análise de incidentes não será usado um caso real, mas serão levantados questionamentos a serem validados diante da situação proposta. Será abordado um incidente específico dentre os vários que podem ocorrer.

Suponhamos que chegou ao SIEM, um alerta que indica que está ocorrendo um ataque DDoS, ou seja, seria um alerta de prioridade crítica, sendo assim, ele será considerado diretamente um incidente e deverá passar pelo procedimento de resposta a incidentes, que é mostrado na Figura 2.12, mais precisamente, o procedimento de resposta a um ataque DDoS, que deve estar previamente documentado pela empresa. Por isso a importância da primeira fase, indicada na Figura 2.12, a preparação. Se faz necessário que a empresa tenha documentado planos de resposta a incidentes dos ataques mais frequentes. [32]

A fase seguinte é a fase de detecção e análise (Figura 2.12), nesta fase o time de SOC deve confirmar se o tráfego anormal identificado é realmente um ataque DDoS, isso pode ser feito através de ferramentas de detecção e análise, como IDS/IPS, XDR, dentre outros. Deve ser realizada uma análise detalhada do tráfego para entender os padrões do ataque e seus vetores e por fim, classificar o ataque DDoS com base em sua natureza, podendo ser volumétrico, por aplicativo, dentre outras opções.

Na fase de contenção, erradicação e recuperação (Figura 2.12), é onde será feita a implementação de medidas para isolar o tráfego malicioso, como atualização de configurações de firewall ou redirecionamento de tráfego. Caso haja, nesta fase deve ser ativado os serviços de mitigação de DDoS. Esses passos compõem a contenção.

A erradicação é onde serão feitas as tentativas de identificação da origem do ataque DDoS, analisando logs e registros de tráfego. Serão aplicadas as atualizações de segurança necessárias para corrigir vulnerabilidades exploradas durante o ataque.

Já na fase de recuperação, será feita a gradual restauração dos serviços afetados, monitorando continuamente para garantir a estabilidade durante a sua volta. É também onde será feita a avaliação do impacto do ataque nos sistemas, dados e operações. É aqui onde serão feitas as documentações para futuras análises.

Finalizando o processo, se tem a fase de atividade pós-incidente (Figura 2.12), onde será conduzida uma revisão pós-incidente para avaliar a eficácia das medidas tomadas e identificar áreas de melhoria. A documentação é atualizada com base nas lições aprendidas e nas mudanças no cenário de ameaças.

4.2 FASE 5: SERVIÇOS, TECNOLOGIAS, MÉTRICAS, O FUTURO DO SOC E AMEAÇAS EMERGENTES

4.2.1 Serviços e tecnologias

Até o presente momento foram citados processos relacionados principalmente a equipe de SOC e ao SIEM, este sendo utilizado como principal fonte de alertas, isso ocorreu pois, a ideia foi trazer as melhores práticas para o cenário mais simples e acessível possível, porém existe uma gama variada de serviços e tecnologias que um SOC pode utilizar a fim de aumentar a segurança da organização e ajudar na análise de alertas e incidentes de maneira mais eficaz.

4.2.1.1 Serviços

Começando pelos serviços, um SOC pode oferecer resposta a incidentes e gerenciamento de eventos e informações de segurança, que é feito pelo SIEM, ambos os serviços já foram citados e explicados anteriormente.

O serviço de inteligência de ameaças engloba a coleta e análise de dados relacionados a ameaças para identificar possíveis ameaças e vulnerabilidades emergentes. Isso inclui o rastreamento de agentes de ameaças, análise de malwares e avaliação de riscos potenciais.

O gerenciamento de vulnerabilidades consiste na identificação de pontos fracos nos sistemas e aplicativos da organização, seguida pela aplicação de correções e atualizações para mitigar o risco de exploração.

Os testes de penetração e os serviços de red teaming envolvem a avaliação das defesas da organização por meio da simulação de ataques e tentativas de explorar vulnerabilidades. Essas atividades auxiliam a equipe SOC na identificação de fragilidades na postura de segurança da organização, permitindo a imple-

mentação de medidas para aprimorá-la.

E por fim, a análise de comportamento de usuários e entidades (UEBA). Esse serviço envolve a análise do comportamento de usuários e entidades nos sistemas e redes da organização para detectar potenciais ameaças e anomalias. Essa abordagem auxilia a equipe do SOC na identificação e resposta a ameaças antes que causem danos significativos. [15]

4.2.1.2 Tecnologias

As tecnologias que podem ser usadas para a realização desses serviços são, SIEM, SOAR e XDR, que já foram explicadas na fundamentação teórica e outras mais que serão explicadas a seguir.

Os EDRs são soluções que monitoram e protegem dispositivos finais, como notebooks, desktops e servidores, contra potenciais ameaças à segurança. Já os NDR são soluções que monitoram e protegem o tráfego de rede para identificar possíveis ameaças à segurança, respondendo a elas em tempo real.

No quesito segurança em nuvem, são empregadas soluções para gerenciar e proteger ambientes em nuvem, defendendo-os contra possíveis ameaças à segurança. Existem também SIEMs e SOARs que são hospedados na nuvem, ou seja, tem sua infraestrutura toda em nuvem e fazem todo seu processamento lá. O USM, SIEM citado anteriormente, se enquadra nessa categoria.

Em termos gerais, a tecnologia implementada em um SOC deve ser cuidadosamente escolhida e integrada para atender às necessidades de segurança da organização, alinhando-se de maneira eficaz aos fluxos de trabalho e processos do SOC. Além disso, é crucial manter a tecnologia atualizada regularmente para assegurar sua eficácia contínua contra ameaças emergentes à segurança. [15]

4.2.2 Métricas e desempenho

A avaliação do desempenho de um SOC é fundamental para compreender a eficácia de suas operações e identificar oportunidades de aprimoramento. Abaixo estão algumas métricas importantes para mensurar o desempenho de um SOC: [33] [15]

- Tempo Médio de Detecção (MTTD): O MTTD mede o intervalo de tempo médio que a equipe do SOC leva para identificar um incidente de segurança. Um MTTD menor indica maior eficiência da equipe na detecção de incidentes.
- Tempo Médio de Resposta (MTTR): O MTTR mede o intervalo de tempo médio que a equipe do SOC leva para responder um alerta ou incidente de segurança por completo. Um MTTR mais baixo sugere maior eficiência no processo de resposta.
- Tempo Médio de Atendimento (MTTA): O MTTA mede o tempo médio que a equipe de SOC leva para começar a responder e analisar um incidente. Portanto, essa métrica ajuda a avaliar a eficiência dos processos de resposta a incidentes. Um MTTA mais baixo sugere maior eficiência no processo de resposta e análise de incidentes.
- Taxa de Falsos Positivos: Esta taxa quantifica quantos alertas gerados pelo SIEM não representam

incidentes reais de segurança. Uma taxa de falsos positivos elevada indica possível desperdício de recursos em alarmes falsos, podendo estar negligenciando ameaças reais.

4.2.3 O futuro do SOC

A inteligência artificial estará cada vez mais presente no SOC, o que já foi um dia considerado um futuro distante, hoje já é realidade e estará cada vez mais presente, tendo um impacto direto na análise de incidente e alertas. Várias atividades que são repetitivas poderão ser automatizadas, cabe aos profissionais saberem configurar as plataformas da forma correta, acompanhar seu desempenho inicial para que a elas funcionem de maneira satisfatória para o cenário real, assim fazendo que o trabalho seja mais ágil e preciso.

A automação de processo teria um impacto bem grande no procedimento mostrado neste trabalho, caso houvesse automação de alguns alertas, máquinas poderiam ser isoladas da rede automaticamente em casos de alerta de ransomware. No exemplo citado, o Caso 3, durante um ataque DDoS, políticas de contenção poderiam ser enviadas automaticamente para o firewall caso houvesse um conector entre o SIEM e o firewall. É uma infinidade de análises que podem gerar diversos outros trabalhos.

À medida que um número crescente de empresas faz a transição para a computação em nuvem, é indispensável que o SOC tenha a capacidade de se ajustar a essas transformações, garantindo uma gestão eficiente e uma proteção eficaz dos ambientes em nuvem.

A colaboração entre empresas se faz fundamental para as boas práticas e posturas de segurança bem-sucedidas sejam aplicadas no mercado como um todo. As requisitos de conformidade e normas serão cada vez mais severas e cabe ao SOC se adequar a elas, tanto na forma de gerir os dados e principalmente de como protegê-los dos ataques. [15]

4.2.4 Ameaças emergentes

No contexto de ameaças emergentes, algumas que ganharam notoriedade atualmente foram, APTs, que são ataques elaborados e persistentes criados com o objetivo específico de evitar a detecção e obter acesso não autorizado aos sistemas de uma organização e ataques de ransomwares, que estão cada vez mais frequentes. [32]

Com o aumento da conectividade de dispositivos à Internet, há uma crescente ameaça de ataques direcionados à IoT. Esses ataques podem visar dispositivos residenciais inteligentes, dispositivos de saúde e sistemas de controle industrial. [15]

São exemplos de APTs:

- Roubo de Dados Sensíveis: O ataque APT da APT28 (também conhecida como Fancy Bear), associada ao governo russo, visou organizações governamentais e empresas ao redor do mundo para roubo de dados sensíveis e informações estratégicas;
- Espionagem Corporativa e Governamental: O ataque APT1, atribuído ao governo chinês, teve como alvo várias organizações globais, principalmente nos EUA, com o objetivo de espionagem industrial

e coleta de informações sensíveis;

- Comprometimento de Infraestrutura Crítica: O Stuxnet, um malware altamente sofisticado, foi projetado para atacar sistemas SCADA e comprometeu o programa nuclear iraniano.

São características e exemplos de ataques de ransomware:

- Criptografia de Dados: O ataque do ransomware WannaCry atingiu organizações em todo o mundo, criptografando dados e exigindo resgates para a chave de descriptografia. Afetou organizações como o NHS (Serviço Nacional de Saúde) no Reino Unido;
- Interrupção de Operações: O ataque do ransomware NotPetya começou como um ataque a sistemas financeiros na Ucrânia e rapidamente se espalhou, afetando empresas globais. Causou interrupções significativas nas operações e causou prejuízos financeiros substanciais;
- Extorsão Financeira: O grupo de ransomware REvil (ou Sodinokibi) é conhecido por ataques de ransomware direcionados a empresas, exigindo grandes quantias em dinheiro para a recuperação dos dados;
- Danos à Reputação: Além dos custos financeiros, os ataques de ransomware podem causar danos significativos à reputação da organização, especialmente se dados sensíveis ou informações confidenciais dos clientes forem comprometidos;
- Impacto na Continuidade do Negócio: Ransomwares como o Ryuk têm como alvo organizações e buscam impactar a continuidade do negócio, forçando paralisações operacionais até que o resgate seja pago ou a infraestrutura seja restaurada.

Ambos os tipos de ataques têm o potencial de causar danos financeiros, operacionais e de reputação significativos. A prevenção, detecção precoce e resposta eficaz são cruciais para minimizar esses impactos. A educação contínua e a implementação de práticas sólidas de segurança cibernética são essenciais para proteger as organizações contra essas ameaças cada vez mais sofisticadas.

São exemplos de ataques conta dispositivos IoT:

- Mirai Botnet (2016): Um dos ataques mais notórios contra dispositivos IoT foi o ataque Mirai em 2016. O malware Mirai visava dispositivos IoT, como câmeras de segurança, roteadores e gravadores de vídeo. Ele os infectava e os transformava em "zumbis"controlados remotamente, formando uma botnet poderosa que foi usada para realizar ataques de negação de serviço distribuído (DDoS). Grandes sites e serviços, incluindo Twitter, Reddit e Netflix, foram afetados;
- BlueBorne (2017): O ataque BlueBorne explorava vulnerabilidades nas conexões Bluetooth de dispositivos IoT. Ele permitia que invasores se conectassem remotamente a dispositivos, como smartphones, smartwatches e alto-falantes inteligentes, sem a necessidade de autenticação. Uma vez conectados, os invasores podiam executar código malicioso nos dispositivos comprometidos;

- TrickBot e Ryuk (2019): Embora inicialmente associado a ataques contra sistemas bancários, o TrickBot evoluiu para incluir funcionalidades de ataque contra dispositivos IoT. Em conjunto com o ransomware Ryuk, TrickBot foi utilizado para atacar sistemas Windows e dispositivos IoT em ambientes corporativos.

Esses exemplos destacam a diversidade de ameaças enfrentadas pelos dispositivos IoT e a importância de implementar práticas de segurança robustas, como atualizações regulares de firmware, senhas fortes, monitoramento de tráfego e segmentação de rede, para mitigar riscos de segurança associados à IoT.

5 CONCLUSÃO

Em síntese, este trabalho teve como objetivo mostrar através de fases, focando na análise de casos e de mapeamento de processos, as melhores práticas a serem utilizadas em um SOC, com o foco na análise de alertas e incidentes.

As melhores práticas não são estáticas, elas se atualizam constantemente e podem ser adaptadas para cada empresa. São infinitos cenários onde elas podem ser aplicadas e adaptadas com base no contexto vigente, quantidade de membros do SOC, capital de investimento em soluções, tamanho de infraestrutura dentre outras características que podem variar.

O que se entende de fundamental em todos os possíveis casos é o estabelecimento de uma documentação bem feita e atualizada e o alinhamento da função de cada um dentro do SOC. Todos os membros precisam saber o que fazer caso aconteça um incidente. Qual procedimento deve ser feito, quem deve ser acionado, isso é a base para a aplicação das melhores práticas em cada situação. A ponderação sobre o futuro não tão distante do SOC foi feita de maneira rasa neste trabalho já que esse tema por si só já geraria outro trabalho.

Analisando o contexto de organizações públicas e privadas, é crucial para as organizações que buscam se manter à frente das ameaças e das novas tecnologias no campo da cibersegurança se manterem atualizadas. À medida que as ameaças cibernéticas continuam a se desenvolver e se tornar mais complexas, o SOC precisa acompanhar essa evolução para assegurar sua eficácia na defesa contra possíveis ameaças.

Resumindo, o futuro do SOC será influenciado por diversas tendências e prognósticos. A automação irá desempenhar um papel ainda mais relevante no SOC, resultando em tempos de resposta a incidentes mais rápidos e maior precisão. Tecnologias como inteligência artificial e aprendizado de máquina serão empregadas ainda mais para automatizar tarefas rotineiras, permitindo que os analistas do SOC foquem em ameaças mais complexas. O SOC deverá integrar cada vez mais outras tecnologias de segurança. Essa integração proporcionará uma visão mais abrangente da postura de segurança da organização e permitirá respostas mais eficazes a incidentes.

E por fim, com a crescente migração para ambientes em nuvem, espera-se que o SOC também adote uma abordagem baseada na nuvem. Isso facilitará o gerenciamento e a proteção de ambientes em nuvem, exigindo abordagens e ferramentas específicas para lidar com os novos desafios associados.

5.1 TRABALHOS FUTUROS

Como já dito anteriormente, este trabalho é uma base, o início de uma análise, podem surgir vários trabalhos a partir daqui, alguns temas que poder ser explorados são:

- O funcionamento de um SOC em uma SDN;

- Automação em um SOC usando SOAR;
- O poder da IA dentro de um SOC;

Dentre diversos outros temas que são relacionados ao tópicos citados na seção futuro do SOC.

REFERÊNCIAS BIBLIOGRÁFICAS

1 THEMEZHUB. *Top 15 Cybersecurity Threats in 2023 | Sprintzeal*. Disponível em: <https://www.sprintzeal.com/blog/top-cybersecurity-threats>.

2 MERIZIO, L. *As fases do ciclo de vida da gestão de vulnerabilidades*. nov. 2022. Disponível em: <https://blog.next4sec.com/mercado-e-gestao/ciclo-de-vida-da-gestao-de-vulnerabilidade/>.

3 CYBERINSIDERS. *PRODUCT REVIEW: AlienVault USM Anywhere*. dez. 2017. Disponível em: <https://www.cybersecurity-insiders.com/product-review-alienvault-usm-anywhere/>.

4 AUTOMAçãO de segurança (SOAR) para todos. Disponível em: <https://www.paloaltonetworks.com.br/cortex/cortex-xsoar>.

5 CrowdStrike Falcon® Insight XDR | Products. Disponível em: <https://www.crowdstrike.com/products/endpoint-security/falcon-insight-xdr/>.

6 CONTRIBUTOR, S. *10 Best Free and Open-Source SIEM Tools - DNSstuff*. nov. 2019. Disponível em: <https://www.dnsstuff.com/free-siem-tools>.

7 GESTãO de Chamados | Melhor suporte, clientes mais satisfeitos | TOPdesk. Disponível em: <https://www.topdesk.com/pt/recursos/gestao-de-chamados/>.

8 VULNERABILITY Validation & False Positive Elimination | Securin. Disponível em: <https://www.securin.io/vulnerability-validation-false-positive-elimination/>.

9 MBA, J. F. *What Is A Red Team VS A Blue Team In Cyber Security?* set. 2020. Disponível em: <https://purplesec.us/red-team-vs-blue-team-cyber-security/>.

10 COHEN, J. *3 Reasons to Align With the NIST Cybersecurity Framework*. abr. 2019. Disponível em: <https://kybersecure.com/3-reasons-to-align-with-nist-cybersecurity-framework/>.

11 FreeBSD Brasil. Disponível em: <https://www.freebsdbrasil.com.br/produtos/apoio-contra-incidentes.html>.

12 MONTAG, G. *SANS Incident Response Framework*. jan. 2023. Disponível em: <https://wirexsystems.com/resource/sans-incident-response-framework/>.

13 MANAGED Service Providers Should Provide Cloud Services - Open Source Listing. Disponível em: <https://www.opensourcelisting.com/managed-service-providers/>.

14 THREAT Intelligence Lifecycle - Silobreaker. Disponível em: <https://www.silobreaker.com/glossary/threat-intelligence-lifecycle/>.

15 MUGHAL, A. A. Building and Securing the Modern Security Operations Center (SOC). *International Journal of Business Intelligence and Big Data Analytics*, v. 5, n. 1, p. 1–15, jan. 2022. Disponível em: <https://research.tensorgate.org/index.php/IJBIBDA/article/view/21>.

16 WHAT is a Vulnerability? Definition + Examples | UpGuard. Disponível em: <https://www.upguard.com/blog/vulnerability>.

17 VULNERABILITY in Security: A Complete Overview | Simplilearn. fev. 2022. Disponível em: <https://www.simplilearn.com/vulnerability-in-security-article>.

18 WHAT is a Cybersecurity Incident? | Cybersecurity Awareness. Disponível em: <https://computing.fnal.gov/securityawareness/what-is-a-computer-security-incident/>.

19 WHAT is incident response? | IBM. Disponível em: <https://www.ibm.com/topics/incident-response>.

20 DIEGO. *O que é SIEM e quais suas principais funcionalidades?* jun. 2021. Disponível em: <https://www.gcsec.com.br/o-que-e-siem-e-quais-suas-principais-funcionalidades/>.

21 O que é SOAR? | Security Orchestration Automation and Response. Disponível em: <https://www.redhat.com/pt-br/topics/security/what-is-soar>.

22 WHAT Is XDR? Extended Detection and Response | Trellix. Disponível em: <https://www.trellix.com/security-awareness/endpoint/what-is-xdr/>.

23 IT, I. *SIEM, SOAR e XDR: Escolha a solução certa para sua empresa*. abr. 2023. Disponível em: <https://www.internationalit.com/post/siem-soar-e-xdr-escolha-a-soluÃğÃčo-certa-para-sua-empresa>.

24 SILVA, G. Z. d. *SIEM vs. SOAR: Qual é a diferença?* jul. 2022. Disponível em: <https://blogs.manageengine.com/portugues/2022/07/26/siem-vs-soar-qual-e-a-diferenca.html>.

25 RED Team vs Blue Team vs Purple Team. nov. 2021. Disponível em: <https://br.claranet.com/blog/o-que-e-red-team-blue-team-e-purple-team-cyber-security>.

26 O que é o NIST Cybersecurity Framework? | IBM. Disponível em: <https://www.ibm.com/br-pt/topics/nist>.

27 CICHONSKI, P.; MILLAR, T.; GRANCE, T.; SCARFONE, K. *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*. [S.l.], ago. 2012. NIST SP 800–61r2 p. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>.

28 TEBALDI, P. C. *MSPs | O que são Managed Service Providers e como trabalham?* set. 2017. Disponível em: <https://www.opservices.com.br/msps-managed-service-providers/>.

29 WHAT is UEBA (User and Entity Behavior Analytics)? | IBM. Disponível em: <https://www.ibm.com/topics/ueba>.

30 HS. *O que é Threat Intelligence?* jan. 2023. Disponível em: <https://hackersec.com/o-que-e-threat-intelligence/>.

31 CROWLEY, C. Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey. 2019.

32 6 ataques cibernéticos mais frequentes em 2023 (até agora). out. 2023. Section: Tecnologia. Disponível em: <https://www.startse.com/artigos/ataques-ciberneticos-mais-frequentes-em-2023>.

33 SOC Metrics: Security Metrics & KPIs for Measuring SOC Success. Disponível em: <https://www.splunk.com/en_us/blog/learn/security-operations-metrics.html>.