DESENVOLVIMENTO E ANALISE DE GESTÃO DE INCIDENTES E SEGURANÇA
DESENVOLVIMENTO DE UMA FERRAMENTA DE GESTÃO DE INCIDENTES DE SEGURANÇA: ANÁLISE DO EMPREGO DA FERRAMENTA THEHIVE EM AMBIENTE SIMULADO

CAP LUÍS HENRIQUE ALVES **VIEIRA**
CAP HAMILTON RODRIGO GOMES DO AMARAL **SANTIAGO** DE ALMEIDA
CAP **FÁBIO** HENRIQUE **DATOLLA**

RESUMO

Este trabalho descreve o processo de desenvolvimento de uma ferramenta voltada para a gestão eficiente de incidentes de segurança da informação em ambientes corporativos. A crescente ameaça de ataques cibernéticos exige que as organizações adotem soluções para monitoramento, registro e mitigação de incidentes de maneira centralizada e eficaz. A ferramenta proposta inclui um sistema de monitoramento em tempo real, registro centralizado de incidentes, além de ferramentas para análise e respostas rápidas já pré estabelecidas. Os testes realizados em um ambiente simulado demonstraram a eficácia da solução em reduzir o tempo de resposta e melhorar a eficiência na gestão de incidentes.

***Palavras-chave**: Gestão de Incidentes, Segurança da Informação, Monitoramento, Resposta a Incidentes.*

1 INTRODUÇÃO

A transformação digital trouxe benefícios significativos, mas também aumentou as ameaças à segurança da informação, como ataques cibernéticos e vazamento de dados. Esses incidentes exigem respostas rápidas e eficazes, tornando essencial a implementação de ferramentas que auxiliem na gestão centralizada e organizada dos incidentes de segurança. Neste contexto cresce a importância da eficácia na gestão de incidentes, haja vista, a utilização massiva de serviços online de todas as naturezas que devem estar "expostos à internet", com disponibilidade diuturna e com informações precisas confiáveis e ágeis.

Muitas empresas enfrentam desafios para a adoção de soluções eficazes devido a custos elevados e falta de expertise, resultando em uma gestão fragmentada e reativa dos incidentes. Esse cenário aumenta os riscos de danos aos sistemas e dados corporativos, evidenciando a necessidade de ferramentas acessíveis e eficientes.

Este trabalho propõe o desenvolvimento de uma ferramenta que permita monitorar, registrar e responder a incidentes de segurança de forma centralizada e em tempo real. A ferramenta busca melhorar a eficiência na detecção e tratamento de incidentes, tornando o processo mais ágil e adequado às necessidades das empresas.

1.1 CONTEXTUALIZAÇÃO DO ESTUDO

Com o aumento da dependência tecnológica, as ameaças à segurança da informação têm crescido de forma alarmante. Empresas de diferentes setores enfrentam, diariamente, tentativas de ataques cibernéticos que podem comprometer a integridade de suas operações. Nesse cenário, a gestão de incidentes de segurança tornou-se um componente essencial da estratégia de proteção de ativos digitais. Entretanto, muitas organizações ainda carecem de ferramentas adequadas para monitorar e gerenciar esses incidentes de forma eficiente e centralizada.

1.2 JUSTIFICATIVA

A relevância de uma ferramenta de gestão de incidentes de segurança se justifica pela necessidade das organizações em melhorar sua capacidade de resposta a ataques. Muitas soluções no mercado apresentam limitações de custo e adaptabilidade para empresas de menor porte ou com infraestrutura heterogênea. A ferramenta proposta visa suprir essa lacuna, oferecendo uma alternativa eficaz e acessível para a detecção e tratamento de incidentes.

1.3 DEFINIÇÃO DO PROBLEMA DE PESQUISA

O problema central abordado por este estudo é a ausência de ferramentas acessíveis e eficientes que permitam a gestão integrada de incidentes de segurança em redes corporativas. A fragmentação de processos e a falta de um sistema de monitoramento contínuo levam a respostas ineficazes e, muitas vezes, tardias a incidentes de segurança.

1.4 OBJETIVOS DA PESQUISA

O objetivo geral deste trabalho é desenvolver uma ferramenta que centralize e otimize a gestão de incidentes de segurança. Os objetivos específicos incluem:

- Implementar um sistema de monitoramento em tempo real para detectar incidentes de segurança. De início, focando em um ponto específico de vulnerabilidade, de forma a iniciar e desenvolver esta ferramenta, para que se torne exequível no tempo disponível, funcional e prática.
- Desenvolver um módulo centralizador para registro e acompanhamento de incidentes.
- Definir procedimentos para a análise e tratamento de incidentes com base em níveis de criticidade.
- Avaliar o desempenho da ferramenta em um ambiente de testes simulados.

1.5 ESTRUTURA DO CONTEÚDO ESCRITO

Este trabalho está dividido nas seguintes seções:

- **Seção 1**: Introdução, onde são apresentados o contexto, a justificativa, a definição do problema e os objetivos do estudo.
- **Seção 2**: Desenvolvimento, que inclui a revisão da literatura, metodologia e análise de dados.
- **Seção 3**: Discussão dos resultados obtidos com a ferramenta desenvolvida.
- **Seção 4**: Conclusão, com as considerações finais e sugestões de futuras melhorias.

2. DESENVOLVIMENTO

A gestão de incidentes de segurança é uma atividade fundamental em um cenário digital cada vez mais vulnerável a ataques cibernéticos. As instituições enfrentam grandes dificuldades para identificar e reagir a incidentes, em razão do aumento contínuo de dados gerados por sistemas de vigilância e da sofisticação das ameaças atuais. Nesse cenário, a automação da resposta a incidentes se torna indispensável, possibilitando que as equipes de segurança atuem de maneira rápida e eficiente, reduzindo os efeitos adversos de possíveis falhas. Ferramentas como TheHive e Cortex surgem como soluções inovadoras que aprimoram os fluxos de trabalho e fortalecem a colaboração entre os especialistas em segurança.

O TheHive proporciona uma plataforma colaborativa que simplifica a gestão de incidentes, possibilitando que as equipes troquem informações em tempo real e tratem casos de maneira organizada. Sua interface amigável torna a criação e a atribuição de tarefas mais eficazes. O Cortex, funcionando como o “cérebro” do TheHive, automatiza análises e respostas, conectando diversas APIs e serviços que asseguram uma rápida ação em face de ameaças. Essa integração entre as duas ferramentas não só facilita uma resposta mais rápida, mas também permite uma análise mais detalhada dos incidentes, com a

coleta de dados relevantes de forma automática, promovendo decisões embasadas. Ademais, a colaboração e a troca de conhecimento são essenciais para o aprimoramento contínuo das práticas de segurança. A utilização do TheHive e do Cortex não só potencializa a resposta a incidentes, mas também cria um ambiente propício para que as equipes aprendam com cada evento, registrando e analisando ocorrências anteriores. Essa metodologia contribui para o desenvolvimento de um banco de dados de conhecimento que pode ser consultado em situações futuras, aumentando a prontidão e resiliência das organizações diante de novas ameaças.

Assim, a adoção dessas ferramentas representa um avanço significativo na gestão de segurança, garantindo que as empresas estejam melhor equipadas para enfrentar os desafios do cenário digital contemporâneo.

2.1 REVISÃO DA LITERATURA

A automatização da resposta a incidentes de cibersegurança tem sido destacada na literatura acadêmica, refletindo o aumento das ameaças digitais e a necessidade de processos de segurança mais eficazes. A resposta a incidentes visa identificar, analisar, mitigar e prevenir eventos que possam afetar a integridade, segurança e disponibilidade da informação dentro das organizações. Inicialmente, estes processos eram manuais, com analistas investigando os incidentes separadamente, resultando muitas vezes em respostas lentas e ineficazes. No entanto, a crescente complexidade dos ataques e o aumento do volume de dados processados exigiram o desenvolvimento de modelos de resposta automatizados.

A literatura enfatiza a importância do ciclo de vida da resposta a incidentes, incluindo as fases de preparação, identificação de ameaças, contenção, remoção e recuperação. Este modelo é essencial para coordenar esforços durante e após um incidente, promovendo uma abordagem estruturada para minimizar os danos. Killcrece et al (2003) sugerem que a integração de tecnologias no ciclo de vida de resposta a incidentes é importante para aumentar a eficiência. A automação surge assim como uma ferramenta capaz não só de acelerar estes processos, mas também de garantir maior precisão e consistência na resposta a incidentes. À medida que a frequência e a complexidade dos ataques cibernéticos aumentaram, a automação tornou-se uma necessidade, especialmente devido à falta de profissionais de segurança qualificados.

De acordo com Grobauer et al. (2010),a automação permite que tarefas operacionais e repetitivas sejam executadas de forma mais rápida e com menos erros, permitindo que os analistas de segurança se concentrem em atividades mais estratégicas.

A literatura discute frequentemente plataformas de automação de segurança e resposta a incidentes (SOAR), que integram diferentes ferramentas e processos em uma única interface. Estas plataformas permitem uma detecção e resposta mais rápida às ameaças, otimizando a detecção (MTTD) e o tempo de resposta (MTTR),conforme destacado pela Gartner (2017).

Entre as soluções SOAR descritas na literatura, a integração das ferramentas TheHive e Cortex vem ganhando atenção. O TheHive é uma plataforma de gerenciamento de incidentes e o Cortex automatiza a análise e execução de ações em resposta a incidentes. Estas ferramentas são particularmente valorizadas pela sua natureza de código aberto, flexibilidade e ampla capacidade de integração com outras soluções de segurança, conforme discutido pelo OpenSOC (2019). TheHive e Cortex se diferenciam de outras plataformas proprietárias pela capacidade de serem customizadas e adaptadas a uma variedade de ambientes empresariais, sejam eles de grande ou médio porte.

A integração das ferramentas TheHive e Cortex é amplamente reconhecida por melhorar a automação da resposta a incidentes de segurança cibernética. Semelhante a Binalay et al (2018),esta integração fornece uma solução robusta para gerenciar e processar as grandes quantidades de dados gerados durante a resposta a incidentes. O Cortex tem a capacidade de realizar ações automatizadas em escala, facilitando a análise de arquivos

suspeitos, a verificação da reputação de domínios e endereços IP e a execução de manuais automatizados de prevenção de ameaças em tempo real. Outro aspecto relacionado é a capacidade de personalizar modelos de incidentes no TheHive. Isto padroniza o processo de resposta, melhora a colaboração entre as equipes de segurança e ajuda a criar uma base de conhecimento baseada em incidentes anteriores. Vilasa et al. (2020) descobriram que automatizar e integrar o Cortex com outros sistemas de segurança, como firewalls e soluções de inteligência contra ameaças, pode expandir ainda mais a capacidade de resposta de uma organização e permitir uma defesa mais proativa e eficaz.

Apesar dos benefícios, a literatura também identifica desafios na implementação da automação da resposta a incidentes. Um dos principais problemas está na configuração das ferramentas de automação. Schreiber (2021) aponta que uma configuração inadequada pode resultar em falsos positivos ou falsos positivos, reduzindo a eficiência do sistema e expondo as organizações a riscos adicionais. Esse problema pode ocorrer devido a regras mal definidas ou soluções desajustadas e pode impactar diretamente sua capacidade de detectar e conter ameaças. Outro desafio diz respeito à dependência excessiva da automação. Embora as ferramentas automatizadas reduzam os tempos de resposta e aumentem a consistência, enquanto While et al (2019) argumentam que a intervenção humana ainda é essencial para a tomada de decisões críticas em incidentes mais complexos. A automação deve, portanto, ser vista como um complemento ao trabalho humano, e não como uma substituição total. A expertise dos analistas ainda é necessária para interpretar os dados e tomar decisões estratégicas, especialmente em cenários que exigem análises mais profundas e contextuais.

A revisão da literatura também revelou diversas lacunas que merecem atenção. Uma delas é a falta de pesquisas sobre a eficácia da integração do TheHive com o Cortex e outras ferramentas integradas em instituições de médio porte. A maioria dos estudos concentra-se em grandes empresas com extensos recursos de TI. No entanto, há pouca pesquisa sobre como usar essas ferramentas de forma eficiente em ambientes com poucos recursos. Outro aspecto pouco discutido é o impacto da automação na formação das equipes de segurança cibernética. Embora a automação reduza as cargas de trabalho manuais, ela pode criar dependências técnicas e reduzir a capacidade do analista de responder a incidentes de forma autônoma.

Automatizar a resposta a incidentes de segurança, especialmente usando ferramentas como TheHive junto ao Cortex, *MISP* e *Wazuh*; pode melhorar significativamente a velocidade e a eficiência das operações de segurança. As plataformas SOAR fornecem um ambiente unificado de detecção e resposta a ameaças, oferecendo benefícios como padronização de processos e tempos de resposta mais rápidos. No entanto, a automação também traz desafios, como a necessidade de configuração cuidadosa e equilíbrio entre tecnologia e intervenção humana. Este estudo visa explorar essas questões mais profundamente, focando na aplicabilidade dessas ferramentas em ambientes de diversos portes.

2.2 MÉTODOS DE PESQUISA

Este estudo visa investigar e analisar o processo de automação de resposta a incidentes de segurança da informação utilizando as ferramentas *TheHive* com *Cortex*, *MISP* e *Wazuh* em um ambiente simulado, aplicando esses conceitos na prática dentro de uma organização de médio porte. Para alcançar os objetivos propostos, foi adotado um método de pesquisa exploratória com uma abordagem mista, envolvendo tanto métodos qualitativos quanto quantitativos.

O estudo foi conduzido em duas etapas principais: uma etapa inicial de pesquisa bibliográfica e uma etapa de experimentação prática. A primeira etapa teve como objetivo revisar a literatura existente sobre a automação de respostas a incidentes de segurança e o uso das ferramentas TheHive juntos com outras ferramentas complementares. Já a segunda etapa consistiu na implementação e avaliação prática das ferramentas em um ambiente de laboratório, simulando cenários de incidentes de segurança para testar a eficiência e eficácia do sistema.

A pesquisa concentrou-se na automação e orquestração de respostas a incidentes em um cenário controlado, permitindo a observação detalhada de como as ferramentas atuam na coleta e análise de dados, na interação com sistemas de terceiros e na execução de tarefas de mitigação e resposta.

A amostra de incidentes de segurança cibernética foi composta por cenários criados artificialmente em um ambiente de laboratório. Esses cenários simulam tentativas de invasão e atividades maliciosas em rede, entre outros tipos de ameaças comuns no ambiente corporativo. Os incidentes foram gerados e configurados para replicar as condições que as ferramentas *TheHive* com *Cortex*, *MISP* e *Wazuh* enfrentaram em um cenário real de resposta a incidentes. Cada incidente foi tratado e analisado pelas ferramentas de forma automatizada, com o objetivo de avaliar sua eficiência e eficácia.

A coleta de dados foi realizada em duas frentes: revisão de literatura e experimentação prática. Na revisão de literatura, foram identificados artigos, livros e relatórios relevantes para o estudo das ferramentas de automação de resposta a incidentes, abordando a utilização de *TheHive* integrados com outras ferramentas, as melhores práticas de segurança cibernética e os desafios enfrentados na automação de respostas. Na fase experimental, foi criado um ambiente de laboratório com as ferramentas *TheHive* com *Cortex*, *MISP* e *Wazuh* instaladas e configuradas para simular incidentes de segurança comuns, como tentativas de invasão, vazamentos de dados e atividades maliciosas em rede. Foram gerados incidentes de segurança de forma artificial, que foram posteriormente tratados pelas ferramentas de maneira automatizada. Os dados coletados incluem tempo de resposta, precisão das análises, taxa de sucesso nas ações de mitigação e nível de colaboração entre as equipes, medido por meio de questionários aplicados aos participantes.

A análise dos dados coletados foi dividida em duas partes. A primeira parte, referente à revisão da literatura, foi conduzida por meio de uma análise qualitativa. Os artigos e publicações foram revisados e categorizados de acordo com temas principais, como "Automação de Respostas a Incidentes", "Ferramentas de SOAR", "Integração de TheHive com *Cortex*, *MISP* e *Wazuh*" e "Melhores Práticas em Segurança da Informação". Essa análise permitiu identificar lacunas no conhecimento e direcionar o estudo para aspectos ainda não completamente explorados. A segunda parte da análise, baseada na experimentação prática, seguiu um método quantitativo. Para isso, foram coletados dados referentes ao desempenho das ferramentas, como o tempo de resposta para cada incidente, o número de incidentes resolvidos sem intervenção humana e a quantidade de falsos positivos detectados. Esses dados foram analisados utilizando estatísticas descritivas, com o objetivo de verificar a eficácia das ferramentas na automação de respostas.

Além disso, foi realizada uma análise qualitativa dos feedbacks fornecidos pelos analistas participantes ao final do experimento. Esses feedbacks foram projetados para obter percepções subjetivas sobre a usabilidade das ferramentas, sua eficácia em comparação com processos manuais e as dificuldades encontradas pelos usuários.

Os métodos descritos neste estudo foram detalhados com o intuito de permitir que outros pesquisadores possam reproduzir a pesquisa em diferentes contextos. A instalação e configuração das ferramentas *TheHive* com *Cortex*, *MISP* e *Wazuh* foram documentadas passo a passo, incluindo as configurações de ambiente de rede, os testes utilizados para a geração dos incidentes simulados e as métricas aplicadas para análise de desempenho. Os incidentes simulados foram configurados para representar cenários de ataque realistas, e as ferramentas foram avaliadas em um ambiente controlado, o que permite que esses experimentos sejam replicados em diferentes organizações ou ambientes de teste, ajustando apenas as variáveis conforme necessário.

Espera-se que este trabalho possa contribuir para o avanço do conhecimento na área de gestão eficiente de incidentes de segurança da informação, além de fornecer um

modelo experimental que possa ser utilizado por outras organizações que desejam implementar ou melhorar suas práticas de segurança cibernética com o uso de ferramentas SOAR.

2.3 APRESENTAÇÃO E ANÁLISE DE DADOS

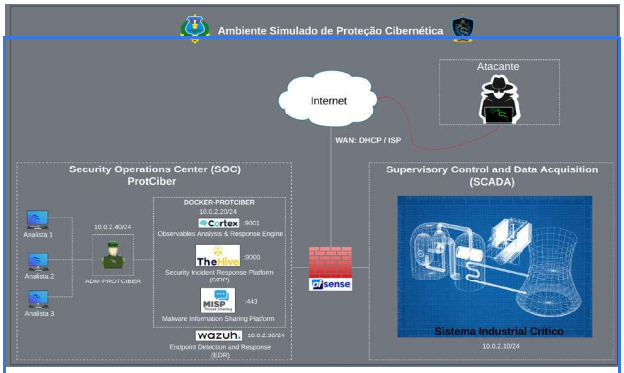
Nesta seção, são apresentados e analisados os dados coletados durante o estudo, que visa avaliar a eficácia da integração da ferramenta *TheHive* com *Cortex*, *MISP* e *Wazuh* em um ambiente simulado de gestão de incidentes de segurança cibernética. O ambiente foi cuidadosamente configurado para refletir um cenário realista, com um Sistema Industrial Crítico (SCADA) e um Security Operations Center (SOC), representando uma estrutura de defesa que monitora e protege ativos sensíveis contra possíveis ameaças externas e internas.

O ambiente simulado, conforme apresentado na figura do estudo, é composto por um SOC com três analistas e ferramentas integradas para detecção e resposta a incidentes. As ferramentas incluem:

- **TheHive**: plataforma central de resposta a incidentes.
- **Cortex**: engine para análise de observáveis, suportando automação de tarefas.
- **MISP**: plataforma para compartilhamento de informações sobre malwares e ameaças.
- **Wazuh**: solução de detecção e resposta a incidentes em endpoints.

Essas ferramentas foram integradas para monitorar, registrar e responder a incidentes de segurança no ambiente simulado, buscando replicar um SOC funcional e interativo.

FIGURA 1 – Ambiente simulado

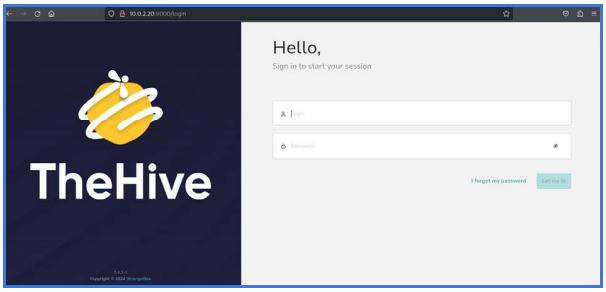


Fonte: os autores

De acordo com Strangebee (2024), o TheHive é uma plataforma abrangente de Resposta a Incidentes de Segurança (SIRP) 4-em-1, projetada para Centros de Operações de Segurança (SOCs), Equipes de Resposta a Incidentes de Segurança de Computadores (CSIRTs), Equipes de Resposta a Emergências de Computadores (CERTs) e profissionais de segurança da informação. Ela oferece um conjunto robusto de recursos que simplificam os fluxos de trabalho de resposta a incidentes, aprimoram a colaboração e permitem uma investigação e mitigação eficazes de ameaças.

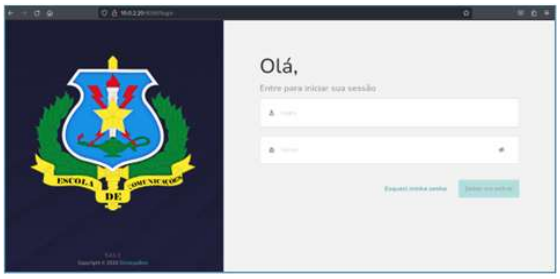
Além disso, o TheHive oferece a possibilidade de adicionar um caso, tarefas, campos personalizados e páginas para organizar e detalhar melhor os incidentes, permitindo uma investigação estruturada e eficiente. Ele facilita a colaboração entre equipes de segurança e fornece uma interface intuitiva para o acompanhamento de atividades e incidentes, tornando-se uma ferramenta essencial para resposta a incidentes e inteligência de ameaças, possibilitando inclusive um histórico dos incidentes existentes na instituição.

FIGURA 2 – Tela de login do TheHive



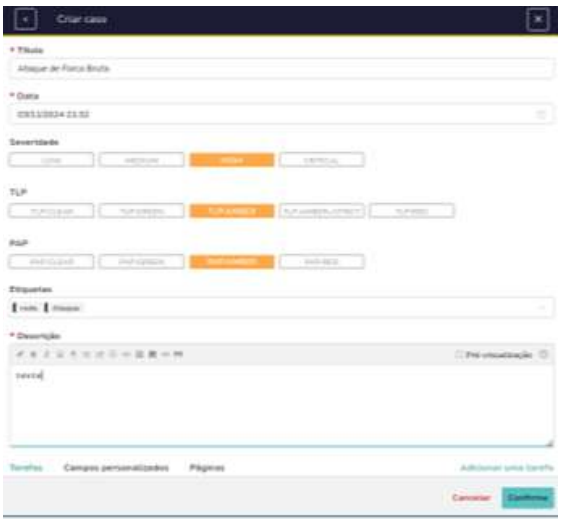
Fonte: os autores

FIGURA 3 – Tela de login do TheHive *customizado*



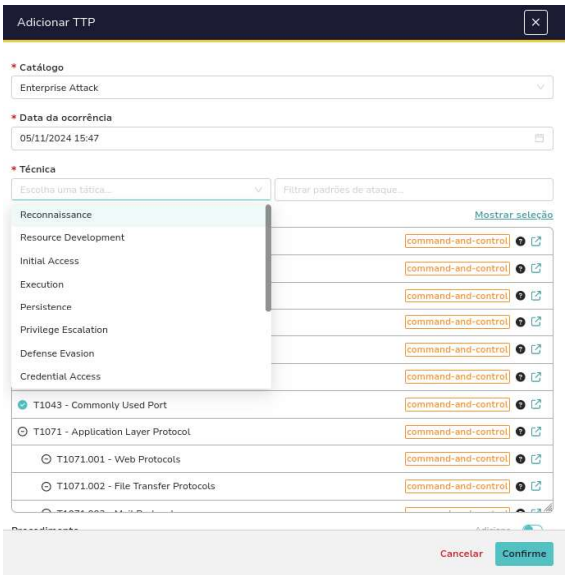
Fonte: os autores

FIGURA 4 – Inserção de incidente no *TheHive*



Fonte: os autores

FIGURA 5 – especificação de TTP no *TheHive*



Fonte: os autores

FIGURA 6 – alertas de incidentes no Sistema SCADA

Fonte: os autores

Durante o período de testes, foram registrados diversos incidentes de segurança, abrangendo tentativas de acesso não autorizado, falhas de autenticação, tentativas de exploração de vulnerabilidades e inúmeros outros incidentes.

De acordo com Wazuh (2024), o Wazuh é uma plataforma de segurança open-source projetada para monitoramento, detecção e resposta a ameaças. Ele oferece uma variedade de recursos que permitem o monitoramento de integridade de arquivos, a análise de logs, a detecção de intrusões e a resposta a incidentes, sendo amplamente utilizado por equipes de segurança da informação para proteger e monitorar infraestruturas de TI.

O teste apresentado evidencia um alerta gerado pelo sistema Wazuh, originado do agente identificado como "SISTEMA-SCADA", conforme registrado na plataforma TheHive. Esse alerta sinaliza a adição de um novo arquivo ao sistema monitorado, o que pode representar uma potencial ameaça, dependendo do contexto operacional. Além disso, o alerta é classificado como uma nova ocorrência, gerada há poucos segundos, sugerindo a detecção recente da atividade. A severidade foi designada com uma classificação de severidade média.

FIGURA 7 – Alerta do Wazuh

Fonte: os autores

Um segundo teste foi realizado, apresentando um alerta gerado pelo sistema Wazuh e originado do agente identificado como "SISTEMA-SCADA", conforme registrado na plataforma TheHive. Esse alerta indica que o serviço Netcat está em escuta para conexões de entrada, o que pode representar uma potencial ameaça, dependendo do contexto operacional. Além disso, o alerta é classificado como uma nova ocorrência, gerada há aproximadamente um minuto, sugerindo a detecção recente da atividade. A severidade foi designada como média.

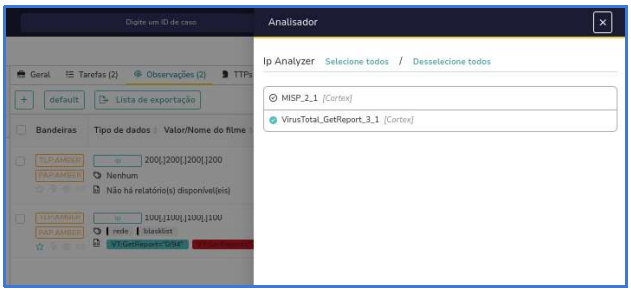
FIGURA 8 – Alerta do Wazuh

Fonte: os autores

De acordo com Strangebee (2024), o Cortex é uma ferramenta complementar ao TheHive que permite a análise automática de indicadores de compromissos e eventos de segurança. Ele fornece uma plataforma para executar uma ampla variedade de análises e gerar relatórios detalhados, facilitando a investigação de incidentes e a resposta a ameaças por parte das equipes de segurança.

Foi realizado um teste onde foi identificado um caso registrado na plataforma TheHive, relacionado ao sistema "SISTEMA-SCADA". Na aba de observáveis, foram analisados dados de IP e domínios através de ferramentas como "MISP 2.1" e "VirusTotal_GetReport_1.1". Essa análise mostra que o sistema está monitorando eventos e ameaças potenciais associadas ao SCADA, com os detalhes do alerta indicando uma atividade monitorada e categorizada recentemente. Esse processo permite avaliar a gravidade e tomar medidas de resposta rápida para mitigar possíveis riscos operacionais ao sistema.

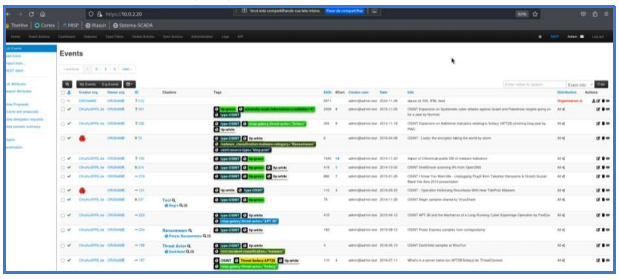
FIGURA 9 – Integração *TheHive* com *Cortex*



Fonte: os autores

De acordo com o MISP Project (2024), o MISP (Malware Information Sharing Platform) é uma plataforma de compartilhamento de informações sobre ameaças de segurança cibernética, que permite a coleta, o armazenamento e a distribuição de indicadores de comprometimento e inteligência de ameaças. Ele é amplamente utilizado por organizações e equipes de segurança para colaborar no combate a ameaças, oferecendo recursos para enriquecer e automatizar a troca de informações sobre ameaças.

FIGURA 10 – Intergração *TheHive* com *MISP*



Fonte: os autores

A imagem apresenta a interface da plataforma MISP (Malware Information Sharing Platform) na seção de eventos, exibindo informações importadas da comunidade para auxiliar na análise e priorização das ações de resposta para os eventos criados no TheHive. Esse monitoramento contínuo permite a identificação de padrões e ameaças recorrentes, promovendo uma postura de defesa mais proativa no sistema SCADA.

A combinação das plataformas TheHive, Cortex, MISP e Wazuh desempenhou um papel essencial na centralização e automação das respostas a incidentes. Quando o Wazuh identifica uma ameaça, ele envia um aviso automaticamente ao TheHive, documentando o caso como um incidente. O Cortex realiza análises automáticas dos dados observáveis e fornece informações pertinentes ao MISP, aumentando assim a base de conhecimento sobre ameaças. Esse processo assegura uma resposta rápida e eficaz, possibilitando que os analistas se concentrem em tarefas mais importantes e diminuindo o tempo de resposta.

A análise dos dados coletados confirma a eficácia do sistema de monitoramento em tempo real, em que todas as ferramentas operam de modo integrado para identificar, registrar e responder a incidentes de segurança. A concentração dos incidentes no TheHive simplificou a monitorização dos casos e a priorização dos mais críticos, com suporte adicional para análises mais aprofundadas e investigações pelo Cortex e MISP. No entanto, foi identificado que o processo ainda envolve intervenções manuais em certas etapas, como a revisão final dos incidentes pelos analistas.

Apesar da eficácia demonstrada por essa abordagem, existem oportunidades para aprimorar a eficiência e a velocidade de resposta.

2.4 DISCUSSÃO DOS RESULTADOS

Os resultados alcançados com a implementação da ferramenta TheHive, integrada ao Cortex, MISP e Wazuh, evidenciam que uma solução centralizada e automatizada para resposta a incidentes é viável e eficaz em um ambiente simulado. O estudo confirmou que, ao integrar essas ferramentas, foi possível identificar e responder a incidentes em tempo real, alcançando os objetivos de monitoramento contínuo e centralização de registros de incidentes. Esse alinhamento com a literatura existente ressalta a importância da automação e da centralização para aprimorar a eficiência nos centros de operações de segurança (SOCs).

A integração possibilitou uma resposta mais ágil e precisa, apresentando benefícios evidentes na priorização de incidentes de acordo com a criticidade, diminuindo a carga manual dos analistas. A utilização do TheHive como módulo centralizador facilitou o monitoramento dos casos, enquanto o Cortex e o MISP enriqueceram as análises com informações sobre ameaças, aprimorando a qualidade das respostas. Esse resultado contribui para o campo da segurança cibernética, demonstrando a eficácia da abordagem integrada para otimizar operações em SOCs.

No entanto, o estudo apresenta limitações. O TheHive, sem outras ferramentas integradas, possui utilidade limitada, funcionando apenas como um repositório de informações e uma plataforma de gestão de incidentes; contudo, quando integrado a outras ferramentas, torna-se uma solução mais robusta para o gerenciamento de incidentes de segurança. O ambiente simulado utilizado neste estudo é menos complexo que uma rede real, e a necessidade de intervenções manuais em certos processos de resposta aponta para oportunidades de melhoria em direção a uma automação mais completa. Além disso, a configuração das ferramentas exige conhecimentos técnicos especializados, o que pode restringir sua aplicabilidade para equipes de segurança com recursos limitados.

Para estudos futuros, recomendamos a avaliação dessa solução em redes maiores e mais complexas, a fim de testar sua escalabilidade e eficácia em ambientes reais. Outra direção relevante é o desenvolvimento de módulos que possibilitem uma automação completa, minimizando ainda mais a intervenção humana e ampliando a agilidade na resposta.

Em resumo, a integração entre TheHive, Cortex, MISP e Wazuh demonstrou ser promissora para a gestão de incidentes, resultando em ganhos significativos em eficiência e eficácia na resposta a incidentes em SOCs. Este estudo enfatiza a relevância da automação e da centralização no enfrentamento de ameaças cibernéticas, além de indicar direções para que investigações futuras expandam o alcance e a aplicabilidade desta solução.

3.1 RESULTADOS

Os resultados da pesquisa demonstram que a utilização integrada das ferramentas TheHive, Cortex, MISP e Wazuh foi efetiva na gestão de incidentes em um ambiente simulado de segurança cibernética. O principal propósito de implantar um sistema de monitoramento em tempo real foi alcançado, possibilitando a identificação e ação ágil diante de incidentes como tentativas de acesso não autorizado, ataques de força bruta e até Implantação de Carga Útil. Além disso, a implementação de um módulo centralizador com TheHive demonstrou-se eficaz para o registro e monitoramento de incidentes, simplificando o processo de priorização com base em sua criticidade. Os procedimentos para o tratamento de incidentes foram executados com êxito, possibilitando uma resposta organizada e eficaz. O desempenho global do sistema demonstrou ser satisfatório para o cenário simulado.

3.2 IMPLICAÇÕES PRÁTICAS E TEÓRICAS

Os resultados deste estudo apresentam implicações práticas e teóricas significativas no campo da segurança cibernética. Do ponto de vista prático, a incorporação de recursos como TheHive, Cortex, MISP e Wazuh evidencia uma estratégia eficaz para automatizar e consolidar a gestão de incidentes em SOCs, aprimorando a eficiência e a prontidão na resposta a ameaças.

Este modelo integrado pode ser implementado por instituições que visam aprimorar seus processos de segurança. No contexto teórico, a pesquisa ressalta a relevância da automação e centralização na mitigação de ameaças cibernéticas, agregando ao conhecimento ao demonstrar que ambientes simulados podem ser eficazes na avaliação do desempenho de soluções de segurança antes de sua implementação em redes reais.

3.3 LIMITAÇÕES E CONSIDERAÇÕES

O estudo apresenta certas limitações metodológicas que necessitam ser levadas em consideração. Inicialmente, é importante ressaltar que o ambiente simulado não reflete completamente a complexidade de uma rede real, o que pode afetar a generalização dos resultados para contextos mais diversos e abrangentes. Ademais, a incorporação das ferramentas demanda conhecimento técnico especializado, o que pode representar um obstáculo à sua implementação em instituições com recursos limitados ou pequenas equipes. O estudo dependeu de intervenções manuais na resposta a incidentes, destacando a importância de uma maior automação para aumentar a independência e eficiência do sistema.

3.4 RECOMENDAÇÕES E DIREÇÕES FUTURAS

Com base nos resultados obtidos, recomendamos que as organizações interessadas em melhorar a gestão de incidentes considerem a implementação de um SOC utilizando uma ferramenta integrada como a utilizada neste estudo.

CERT.BR (2021) recomenda que organizações adotem boas práticas para tratamento de incidentes de segurança, como o uso de plataformas de automação, o que pode auxiliar na mitigação de riscos e no aperfeiçoamento das respostas a ameaças, minimizando impactos e permitindo um acompanhamento contínuo dos incidentes.

Recomendamos pesquisas futuras para avaliar a solução em redes reais e mais complexas e verificar a escalabilidade e robustez do sistema.

Além disso, o desenvolvimento de módulos que automatizam totalmente a resposta a incidentes sem a necessidade de intervenção manual pode melhorar ainda mais a eficácia do sistema.

Estudos comparativos com outras soluções de gerenciamento de incidentes fornecem informações valiosas sobre a relação custo-benefício e a adequação dessas ferramentas para diferentes situações organizacionais.

ABSTRACT

This work describes the development of an external tool for the efficient management of information security incidents in corporate environments. The rising threat of cyber-attacks necessitates that organizations adopt centralized and effective solutions for monitoring, recording, and mitigating incidents. The proposed tool includes a real-time monitoring system, centralized incident logging, and tools for analysis and rapid pre-configured responses. Tests conducted in a simulated environment demonstrated the solution's effectiveness in reducing response time and enhancing efficiency in incident management.

***Keywords**: Incident Management, Information Security, Monitoring, Incident Response.*

REFERÊNCIAS

BINALAY, A. et al. Cortex and TheHive: An Open-Source SOAR Platform for Incident Response Automation. In: *Proceedings of the 2018 International Conference on Cyber Security*, 2018. p. 112-125.

CERT.BR – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Guia de Boas Práticas para Tratamento de Incidentes de Segurança. 2021. Disponível em: https://www.cert.br/docs/guia/. Acesso em: 20 set. 2024.

GARTNER. Market Guide for Security Orchestration, Automation and Response (SOAR). *Gartner Research*, 2017. Disponível em: https://www.gartner.com/en/documents/3760482. Acesso em: 15 out. 2023.

GROBAUER, B.; WALLS, T.; STOECKER, S. Understanding Cloud Computing Vulnerabilities: Automated Incident Response and Security Challenges. *Journal of Information Security*, v. 6, n. 4, p. 298-309, 2010.

KILLCRECE, G. et al. Incident Management in Cybersecurity: Improving Response Efficiency. *Tech Report*, Carnegie Mellon University, 2003.

LOPES, R. V.; MONTONI, M. A. Gestão de Segurança da Informação com Base em ISO/IEC 27001. *Revista Tecnologia e Sociedade*, v. 8, n. 2, p. 43-58, 2013.

MEDEIROS, I. C.; COSTA, F. R.; VELOSO, P. A. S. Segurança em Redes de Computadores: Ataques, Ferramentas e Técnicas de Defesa. *Revista Brasileira de Computação Aplicada*, v. 4, n. 2, p. 89-101, 2012.

MISP PROJECT. MISP Documentation: Overview. Disponível em: https://www.misp-project.org/. Acesso em: 06 out. 2024.

OPENSOC. Open-Source Security Tools: Implementing TheHive and Cortex for Incident Management. *OpenSOC Workshop Report*, 2019. Disponível em: https://www.opensoc.com/report-2019. Acesso em: 20 set. 2023.

ROCHA, S. S.; SOARES, M. S.; ALVES, V. L. A Automação e Orquestração da Resposta a Incidentes com o Uso de TheHive e Cortex. *Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica*, v. 17, n. 3, p. 65-78, 2021.

SCHREIBER, M. Challenges in Automating Incident Response: The Human Factor in Security Automation. *Cyber Defense Review*, v. 6, n. 3, p. 101-119, 2021.

STRANGEBEE. TheHive Overview: Application Stack. Disponível em: https://docs.strangebee.com/thehive/overview/. Acesso em: 06 set. 2024.

VILAÇA, P.; RIBEIRO, T.; SANTOS, A. Enhancing Incident Response with TheHive and Cortex Integration. *Journal of Cybersecurity Engineering*, v. 12, n. 2, p. 55-72, 2020.

WAZUH. Wazuh Documentation: Overview. Disponível em: https://documentation.wazuh.com/. Acesso em: 06 set. 2024.

WHILE, P.; JONES, S.; MITCHELL, C. Human-Centric Incident Response: Limitations of Full Automation in Cybersecurity. *International Journal of Cyber Operations*, v. 8, n. 1, p. 34-49, 2019