INTEGRAÇÃO DE IDS/IPS COM SIEM PARA DETECÇÃO, CORRELAÇÃO E SIMULAÇÃO PROSPECTIVA DE CENÁRIOS EM REDES MILITARES

ST – CRISTIANO PEREIRA GUIMARÃES
1º SGT – RONALD NUNES FIDELIS
2º SGT – MARCELO SANTOS DE OLIVEIRA SILVA
2º SGT – ANDERSON LÚCIO GOMES
2º SGT – TIAGO DOMINGOS DOS SANTOS

RESUMO

Este projeto interdisciplinar, alinhado ao Curso de Proteção Cibernética para Sargentos de 2025, aborda a crescente necessidade de segurança cibernética em ambientes militares. A lacuna identificada reside na ausência de uma solução integrada e eficaz para detecção e resposta a ameaças sofisticadas. O objetivo geral é implementar e avaliar a integração de um IDS/IPS (Suricata) com um SIEM (ELK Stack) em um ambiente laboratorial simulado, incorporando cenários de tráfego malicioso para análise, correlação e resposta.

A metodologia envolveu a preparação de uma rede militar simulada com serviços vulneráveis, a configuração detalhada do Suricata com regras personalizadas, a integração completa com o ELK para coleta, indexação e visualização de logs, e o desenvolvimento de uma interface web customizada Foram elaborados mais de 30 cenários de ataque, submetidos e automatizados para avaliação. Os resultados demonstraram alta eficácia na detecção de ameaças, com taxas de detecção e precisão superiores a 90%, e um tempo médio de detecção de 12 segundos Conclui-se que a solução proposta é robusta e escalável, com recomendações para infraestrutura, atualização contínua e treinamento especializado para implementação em produção

Palavras-chave: Análise de segurança, Cibersegurança, ELK Stack, IDS/IPS, Suricata.

1 INTRODUÇÃO

No cenário atual de operações multidomínio, em que o ciberespaço se estabelece como campo de disputa estratégica, a segurança cibernética torna-se essencial para assegurar a continuidade operacional, a integridade de informações sensíveis e a soberania nacional. Para as Forças Armadas, a proteção de infraestruturas críticas, a resiliência de sistemas de comando e controle e a segurança de redes e dados classificados são prioridades. Entretanto, a sofisticação das ameaças evolui continuamente, conduzida por diversos atores que empregam técnicas ofensivas avançadas para degradar sistemas, exfiltrar dados ou interromper operações. Assim, a capacidade de detectar, analisar e responder rapidamente a incidentes não é apenas estratégica, mas imperativa.

Embora soluções como firewalls e antivírus permaneçam relevantes, o cenário atual exige uma abordagem multicamadas. esse contexto, sistemas IDS/IPS monitoram e bloqueiam atividades maliciosas, e sua integração a plataformas SIEM potencializa a eficácia ao correlacionar eventos, oferecendo visão holística do ambiente e identificando padrões complexos que passariam despercebidos em análises isoladas.

1.1 Contextualização Do Estudo

Ao reconhecer a importância de capacitar profissionais militares com conhecimentos práticos em segurança cibernética, o presente projeto, desenvolvido no âmbito do Curso de Proteção Cibernética para Sargentos - 2025, propõe a implementação e avaliação de uma solução integrada de IDS/IPS e SIEM em um ambiente laboratorial controlado. A escolha de ferramentas open source, como Suricata (IDS/IPS) e a stack ELK, reflete a busca por soluções flexíveis, personalizáveis e economicamente viáveis, adequadas a orçamentos modestos do Poder Executivo. Assim, a simulação de cenários prospectivos e a análise de resultados permitem refinar as estratégias de detecção e resposta, contribuindo significativamente para o fortalecimento da cultura de proteção cibernética das Forças Armadas, além de representar um passo importante na formação de militares com habilidades avançadas em segurança cibernética.

1.2 Justificativa

A integração de IDS/IPS com um SIEM, como a popular stack ELK (Elasticsearch, Logstash e Kibana), oferece uma solução robusta para aprimorar a cultura e consciência de segurança cibernética. O IDS/IPS atua como "olhos" e "braços" na rede, identificando e mitigando ameaças no nível do pacote, enquanto o SIEM funciona como o "cérebro", coletando, processando, analisando e visualizando os dados de segurança de forma contextualizada. Essa sinergia permite que analistas de segurança militar transformem um volume massivo de alertas brutos em dados inteligíveis, facilitando a tomada de decisões rápidas e eficazes em situações críticas.

1.3 Definição Do Problema De Pesquisa

O problema central que este projeto busca resolver é: a lacuna na capacidade de correlacionar eficientemente alertas de segurança de diferentes fontes e de simular cenários de ataque realistas para validar a eficácia das defesas. Pois, muitos ambientes de segurança ainda operam com ferramentas isoladas, resultando em uma sobrecarga de alertas e dificuldade em identificar ataques complexos e persistentes. Esta falta de um ambiente de teste controlado para simular e avaliar a resposta a ameaças específicas do contexto militar impede o desenvolvimento de estratégias de defesa robustas e a capacitação adequada do pessoal.

1.4 OBJETIVOS DA PESQUISA

1.4.1 Objetivo Geral:

Este projeto se propõe a implementar e avaliar a integração de um IDS e IPS (Suricata), com um SIEM, especificamente, a stack ELK (Elasticsearch, Logstash e Kibana), em um ambiente laboratorial simulado, bem como a avaliação e a simulação prospectiva de cenários de tráfego malicioso correlacionando as respostas a incidentes de segurança. Além disso, a elaboração de documentação técnica consultiva, e, por fim, uma apresentação com a demonstração prática da solução integrada.

1.4.2 Objetivos Específicos:

Montagem de rede de computadores militar simulada, com serviços vulneráveis. Criação e personalização de regras de detecção, e validação da geração de alertas. Coletar logs e alertas, indexá-los, criar dashboards no Kibana, implementar correlação para ataques compostos e desenvolver uma interface gráfica web customizada. Elaborar e submeter cenários simulados ao IDS/IPS e SIEM. Medir a eficácia da solução (alertas corretos, falsos-positivos/negativos) e análise de

gargalos e melhorias. Criar um guia de instalação e integração, com Procedimento Operacional Padrão (POP), logs do projeto e um guia de troubleshooting.

1.5 Estrutura Do Conteúdo Escrito

A estrutura deste trabalho compreende um breve resumo e abastract, uma introdução com a contextualização, justificativa e definição do problema tratado, e objetivos gerais e específicos a serem alcançados, conta ainda, com um tópico de desenvolvimento, onde é feita uma revisão da literatura, bem como é exposta a metodologia da pesquisa e apresentação dos dados encontrados e, por fim, apresenta uma sessão de conclusão, com resultados e uma visão ampla do trabalho, e uma sessão com as referências utilizadas neste projeto.

2 DESENVOLVIMENTO

2.1 Revisão Da Literatura

A crescente dependência das Forças Armadas em infraestruturas digitais conectadas têm tornado a segurança cibernética um eixo essencial da defesa nacional. Segundo Souza Junior (2013), as operações militares modernas exigem mecanismos eficazes de proteção da informação, capazes de identificar, conter e responder rapidamente a ameaças sofisticadas, que evoluem em escala e complexidade. Nesse contexto, a integração entre sistemas de detecção de intrusões (IDS/IPS) e plataformas de gerenciamento de eventos e informações de segurança (SIEM) representa um avanço significativo na capacidade de defesa cibernética.

O conceito de **IDS/IPS** (Intrusion Detection/Prevention Systems) é definido por Murini (2014) como um conjunto de mecanismos que inspecionam o tráfego de rede, identificando padrões suspeitos com base em assinaturas ou comportamentos anômalos. Enquanto o IDS se limita a detectar e registrar eventos, o IPS atua ativamente na mitigação, bloqueando pacotes maliciosos antes que atinjam o destino. O *Suricata*, desenvolvido pela *Open Information Security Foundation (OISF)*, é uma ferramenta de código aberto que oferece ambas as funcionalidades, suportando múltiplos protocolos, *multi-threading* e integração nativa com *event logs* e ferramentas de análise.

De acordo com o Elastic (2025), a análise de logs provenientes de IDS é uma das aplicações mais robustas do ecossistema **ELK Stack (Elasticsearch, Logstash e Kibana)**. Essa pilha tecnológica fornece uma infraestrutura escalável e distribuída para a coleta, indexação e visualização de dados de segurança. O Logstash realiza o *parsing* e o enriquecimento das mensagens, o Elasticsearch armazena e indexa os eventos, e o Kibana provê dashboards interativos e relatórios visuais que facilitam a identificação de tendências e correlações.

A integração entre IDS/IPS e SIEM amplia a capacidade de **correlação e contextualização de alertas**. Segundo a Amazon (2021), a pilha ELK se tornou padrão de mercado por permitir a centralização e análise de grandes volumes de logs de segurança, contribuindo para a detecção de ataques distribuídos e persistentes. O uso de pipelines bem definidos, com fontes como *Filebeat* ou scripts personalizados, assegura o envio eficiente e padronizado de eventos de segurança.

No contexto militar, a **Doutrina Militar de Defesa Cibernética** (BRASIL, 2023) enfatiza a necessidade de desenvolver sistemas autônomos e resilientes para monitorar, detectar e reagir a ataques em tempo real. O documento propõe a implementação de arquiteturas integradas que combinem sensores de rede, plataformas de correlação e centros de comando e controle (C2),

favorecendo a consciência situacional cibernética.

Além das ferramentas de segurança, frameworks de inteligência de ameaças como o **MITRE ATT&CK** (MITRE, 2025) fornecem uma taxonomia detalhada das táticas e técnicas empregadas por adversários. Esse modelo é amplamente adotado em SIEMs e IDS modernos para estruturar regras de correlação e priorização de alertas. A incorporação dessas técnicas à configuração do Suricata e aos dashboards do Kibana permite mapear o ciclo de vida dos ataques simulados, desde o reconhecimento até a exfiltração de dados.

O estudo de Souza Junior (2013) destaca ainda que, no ambiente militar, a defesa cibernética deve ser tratada como um componente estratégico. Isso inclui não apenas a adoção de tecnologias avançadas, mas também o desenvolvimento de doutrinas, treinamento contínuo e integração entre camadas táticas e estratégicas.

Ferramentas auxiliares, como o **Filebeat**, também desempenham papel essencial. Conforme a Elastic (2025), o Filebeat atua como um *lightweight shipper* de logs, enviando registros de servidores de aplicação e rede para o pipeline de Logstash. Esse componente é particularmente eficiente em ambientes distribuídos, reduzindo a sobrecarga e garantindo a integridade dos dados durante o transporte.

No campo da integração, a linguagem **Python** tem se consolidado como uma das mais utilizadas em segurança cibernética. Zander, Judge e Sharp (2021) ressaltam que sua simplicidade e poder de automação a tornam ideal para construir scripts de coleta, normalização e envio de dados. No caso deste projeto, Python foi empregado para desenvolver um conector personalizado entre o Suricata (no PFSense) e o Logstash, ampliando a interoperabilidade do sistema.

Por fim, a literatura recente reforça a importância da **simulação prospectiva** de ataques como ferramenta de aperfeiçoamento da defesa. O estudo apresentado no Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg, 2022) demonstra que a construção de laboratórios gamificados baseados na pilha ELK potencializa o treinamento de analistas e a validação de cenários reais de intrusão. Essa abordagem também foi adotada neste projeto para representar o comportamento de uma rede militar exposta a tráfego hostil controlado.

Assim, a revisão da literatura evidencia que a integração entre IDS/IPS e SIEM, aliada ao uso de automação em Python e simulação prospectiva, constitui uma estratégia moderna e eficaz para proteção de redes críticas, especialmente em ambientes militares, onde a precisão e a resposta rápida são fatores decisivos.

2.2 Métodos de Pesquisa

A metodologia deste estudo é de natureza aplicada, com abordagem qualitativa e caráter experimental. O foco foi a **implementação e avaliação de uma arquitetura integrada de detecção e prevenção de instrusões (IDS/IPS) associados a uma plataforma SIEM** operacionalizada em um ambiente laboratorial simulado seguindo as boas práticas de defesa cibernética

2.2.1 Estrutura Metodológica

O desenvolvimento foi dividido em cinco etapas principais:

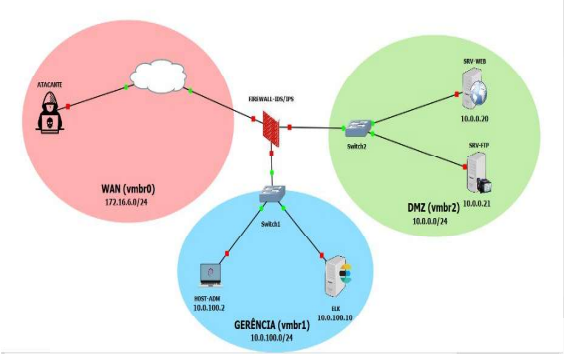
1. **Preparação do ambiente:** montagem de uma rede militar simulada, virtualizada no hipervisor Proxmox, com segmentação entre DMZ e rede interna;

2. **Configuração do IDS/IPS:** instalação e personalização de regras no Suricata, integrado ao firewall PFSense;
3. **Integração com o SIEM ELK:** coleta de logs via Filebeat e scripts Python, processamento no Logstash e indexação no Elasticsearch;
4. **Criação de dashboards e correlações:** desenvolvimento de visualizações interativas no Kibana;
5. **Simulação e validação:** execução de ataques controlados (por exemplo, SQL Injection e *brute force*) e medição de eficácia da detecção.

As máquinas internas, representando servidores **SRV-WEB** e **SRV-FTP**, foram virtualizadas no Proxmox, enquanto a máquina ofensiva foi implementada externamente, utilizando **Kali Linux**.

2.2.2 Ambiente Laboratorial

Para representar visualmente a arquitetura empregada, foi elaborada uma **topologia simulando uma infraestrutura militar segmentada**, conforme ilustrado na **Figura 1.** As configurações mínimas correspondentes encontram-se detalhadas no Apêndice A – Instalação, Configuração e Integração. A rede conta com uma DMZ exposta, contendo os serviços web e FTP, protegida por um firewall PFSense com Suricata atuando como IDS/IPS. O servidor SIEM (ELK Stack) encontra-se na rede interna, recebendo logs de todas as máquinas do ambiente.

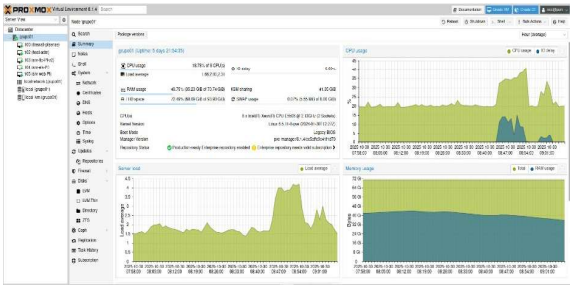


Fonte: os autores

FIGURA 1 – Diagrama da Rede Militar Simulada

A **Figura 2** demonstra a infraestrutura virtual no Proxmox, onde cada máquina virtual (SRV-WEB, SRV-FTP, IDS/IPS e SIEM) foi configurada com recursos controlados e conectividade isolada. Essa virtualização garantiu a segurança dos testes e a reprodutibilidade do experimento.

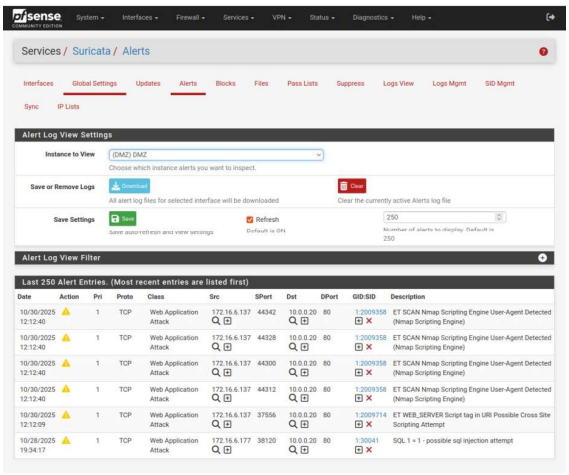
FIGURA 2 – Host Proxmox com Máquinas Virtuais do Ambiente Militar



Fonte: os autores

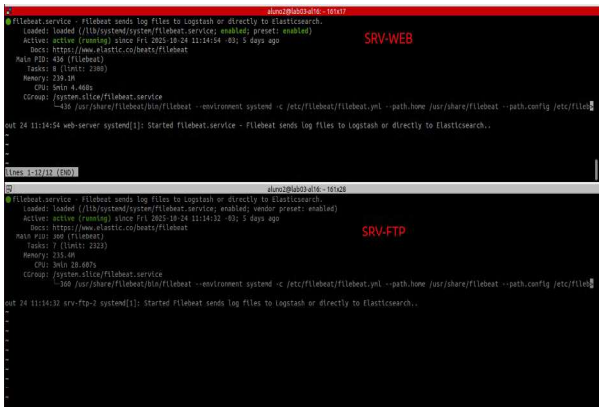
Conforme ilustrado na **Figura 3**, o firewall PFSense executa o Suricata, monitorando a interface da DMZ e identificando fluxos suspeitos de tráfego. A **Figura 4** exibe o Filebeat em execução nos servidores SRV-WEB e SRV-FTP, realizando o envio contínuo dos registros para o pipeline de Logstash.

FIGURA 3 – Console do Firewall PFsense com Suricata Monitorando a DMZ



Fonte: os autores

FIGURA 4 – Filebeat em Execução nos Servidores SRV-WEB e SRV-FTP



Fonte: os autores

2.2.2.1 IDS e IPS: Funcionamento, Modos de Operação e Aplicação do Suricata

Os **Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS)** são pilares da defesa cibernética moderna. Embora frequentemente empregados de forma integrada, eles exercem papéis conceitualmente distintos. O **IDS (Intrusion Detection System)** tem como função principal monitorar o tráfego de rede e gerar alertas quando padrões maliciosos ou anômalos são identificados. Ele é, portanto, um sistema de detecção passivo, sem interferir diretamente no fluxo dos pacotes analisados. Já o **IPS (Intrusion Prevention System)** amplia essa capacidade ao operar de forma ativa: além de detectar, ele também bloqueia ou mitiga automaticamente os pacotes suspeitos antes que atinjam o destino (NIST, 2021).

De acordo com Murini (2014), o IDS atua essencialmente como um sensor de vigilância, responsável por identificar atividades anômalas e notificar operadores ou sistemas correlacionadores (como SIEMs). O IPS, por sua vez, insere-se no caminho do tráfego (modo *in-line*), atuando como um agente de defesa preventiva. Essa diferença estrutural impõe desafios de desempenho, pois o IPS precisa analisar pacotes em tempo real sem introduzir latência perceptível, especialmente em ambientes de alta disponibilidade, como redes militares e corporativas.

O **Suricata**, desenvolvido pela *Open Information Security Foundation (OISF)*, é um mecanismo de inspeção profunda de pacotes (*Deep Packet Inspection – DPI*) que combina as funcionalidades de IDS e IPS em uma única plataforma. Ele é capaz de analisar protocolos de aplicação (HTTP, FTP, DNS, TLS, entre outros), detectar assinaturas conhecidas e comportamentos suspeitos, e aplicar ações corretivas em tempo real. Além de suportar a inspeção de tráfego IPv4 e IPv6, o Suricata utiliza *multithreading*, permitindo a análise simultânea de pacotes em múltiplos núcleos de CPU — característica que o diferencia de soluções mais antigas, como o Snort, e o torna adequado para ambientes de produção e de simulação complexos (OISF, 2025).

Um dos grandes diferenciais do Suricata é a sua **compatibilidade com as regras do Snort**. Essa interoperabilidade é estratégica, uma vez que a comunidade Snort mantém um repositório extenso e continuamente atualizado de assinaturas de ataques. OISF (2025) destaca que o Suricata é capaz de interpretar regras Snort nativamente, permitindo que ambientes que já utilizam Snort migrem gradualmente para Suricata sem necessidade de reescrever suas bibliotecas de detecção. Essa compatibilidade é garantida pelo suporte ao mesmo formato de sintaxe das regras (como *alert, drop, reject e pass*), o que proporciona flexibilidade e continuidade operacional.

A configuração do Suricata pode assumir dois modos principais de operação: o **m do IDS (passivo)** e **modo IPS (ativo)**. o **modo IDS**, o sistema captura as cópias dos pacotes da rede através de interfaces configuradas em *promiscuous mode* (geralmente via *AF_PACKET* ou *pcap*). Os pacotes são analisados, mas não interferem no fluxo real da comunicação. Esse modo é

ideal para auditorias e testes iniciais, pois evita impacto no tráfego e facilita a calibração das regras.

Já o **modo IPS** insere o Suricata diretamente no caminho do tráfego, permitindo que ele bloqueie ou descarte pacotes conforme as ações definidas nas regras. Essa abordagem exige configuração de *bridges* ou *inline interfaces* que conectam os segmentos da rede protegida. De acordo com o OISF (2025), o Suricata suporta dois métodos principais de operação como IPS: **m do legacy (NFQUEUE)** e **modo inline (AF_PACKET inline)**.

O **modo IPS legacy**, baseado em *NFQUEUE*, utiliza o *Netfilter* do kernel Linux para desviar pacotes para uma fila de inspeção. O Suricata lê essa fila, analisa cada pacote e, conforme a regra aplicável, decide se ele deve ser aceito, rejeitado ou descartado. Essa técnica é amplamente utilizada por sua compatibilidade e simplicidade de implementação, especialmente em laboratórios ou ambientes que utilizam o firewall PFSense — como no presente projeto. Contudo, o modo legacy pode introduzir sobrecarga em redes de alto throughput, devido ao processo de cópia e fila dos pacotes entre o kernel e o espaço do usuário.

O **modo inline (AF_PACKET inline)** representa uma abordagem mais moderna e eficiente. Nesse modo, o Suricata opera diretamente sobre as interfaces de rede, interceptando e processando pacotes sem necessidade de filas intermediárias. Ele permite maior desempenho e menor latência, sendo indicado para ambientes de produção com alto volume de tráfego. No entanto, sua configuração é mais sensível, exigindo atenção a parâmetros de *buffering*, *checksum offloading* e ordem de pacotes.

Neste projeto, optou-se pela implementação do **modo IPS legacy (NFQUEUE)**, em virtude de sua estabilidade e ampla documentação para integração com o **PFSense**, que é o firewall base do ambiente simulado. Essa escolha é coerente com os objetivos de validação e ensino, pois facilita a observação do fluxo de pacotes, o comportamento das regras e a reação do sistema a diferentes tipos de tráfego. Além disso, o modo legacy é mais tolerante a erros de configuração, permitindo ajustes incrementais sem comprometer a conectividade total da rede durante os testes.

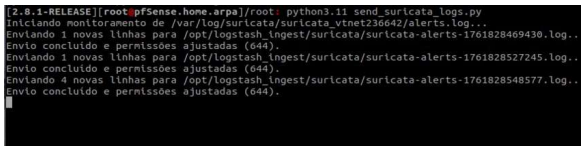
A adoção do Suricata em modo IPS também contribuiu para o aprimoramento das regras personalizadas, derivadas do conjunto Snort, adaptadas ao contexto militar. Essas regras foram ajustadas para detectar varreduras de portas, tentativas de login indevido e ataques de injeção SQL — todos previstos no *OWASP Top Ten* (OWASP, 2021). A capacidade de utilizar regras herdadas do Snort e combiná-las com assinaturas próprias amplia a flexibilidade da solução e demonstra o potencial do Suricata como ferramenta tanto de pesquisa quanto de aplicação operacional.

Em síntese, a utilização do Suricata como IDS/IPS híbrido permitiu a análise detalhada do comportamento da rede simulada e a avaliação da eficácia de diferentes estratégias de bloqueio e correlação. O modo **IPS legacy**, ao equilibrar desempenho e simplicidade, mostrou-se a melhor escolha para o ambiente laboratorial, garantindo observabilidade e controle sem comprometer a integridade dos testes. Essa abordagem é compatível com os objetivos do projeto e alinha-se às recomendações do NIST (2021) e da OISF (2025) quanto à adoção progressiva de mecanismos de prevenção integrados a sistemas de monitoramento centralizados.

2.2.3 Procedimentos de Coleta de Dados

Para automatizar o envio dos logs do Suricata para o SIEM, foi desenvolvido um **script Python dedicado**, que realiza a leitura contínua do arquivo alerts.log e envia os eventos em para o Logstash, utilizando protocolo TCP seguro. Esse script, ilustrado na **Figura 5**, foi uma contribuição original dos autores, integrando o PFSense ao pipeline de análise do ELK.

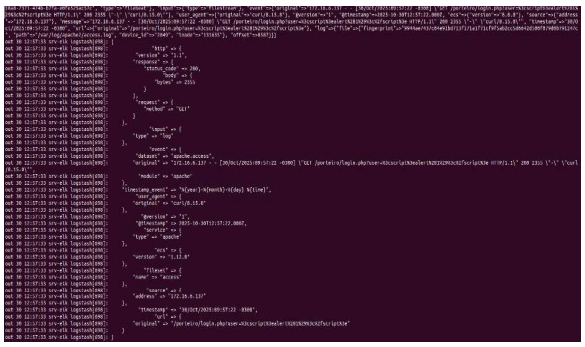
FIGURA 5 – Script Python para Encaminhamento Automatizado dos Logs do Suricata ao SIEM ELK



Fonte: os autores

Na **Figura 6**, observa-se o pipeline do Logstash processando os eventos provenientes tanto do Filebeat quanto do script Python. O pipeline aplica filtros de normalização e enriquecimento de dados (por exemplo, campos de origem, destino, porta, severidade e assinatura da regra) antes de encaminhá-los ao Elasticsearch.

FIGURA 6 – Pipeline do Logstash Processando Eventos de Rede e Aplicação

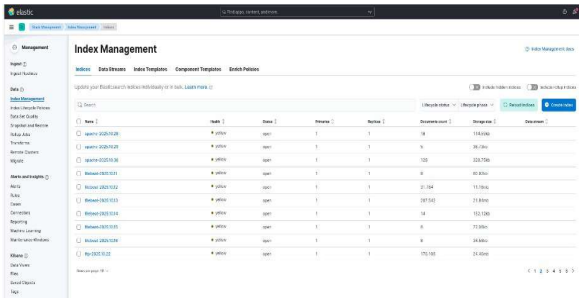


Fonte: os autores

2.2.4 Coleta e Indexação

Após o processamento no Logstash, os eventos são armazenados nos índices do Elasticsearch. A **Figura 7** mostra a estrutura dos índices criados, permitindo consultas rápidas e agregações temporais. Essa estruturação possibilita análises correlacionais e auditorias históricas dos incidentes registrados.

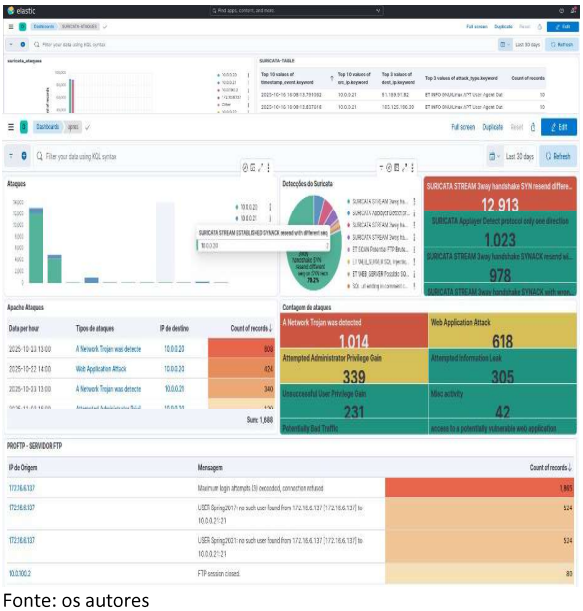
FIGURA 7 – Índices do Elasticsearch Armazenando Eventos do Ambiente Monitorado



Fonte: os autores

A Figura 8 apresenta dois dashboards do Kibana configurados especificamente para o projeto, exibindo visualizações interativas capazes de correlacionar eventos por origem, destino, tipo de ataque e nível de criticidade. Essa camada visual foi essencial para a interpretação dos resultados, pois permitiu não apenas a identificação imediata de anomalias, mas também a análise temporal e comportamental dos eventos registrados. Dessa forma, os analistas puderam acompanhar, em tempo real, as detecções e as tendências dos ataques simulados, facilitando o processo de tomada de decisão e a validação da eficácia dos mecanismos de defesa implementados.

FIGURA 8 – Dashboard Kibana Exibindo Eventos e Alertas Correlacionados



Fonte: os autores

2.3 Apresentação e Análise de Dados

A análise de dados concentrou-se na **validação da eficácia do ambiente integrado** frente a cenários simulados de ataques controlados.

Para isso, foram executados **testes de penetração controlados** a partir do Kali Linux, atuando como máquina ofensiva externa ao Proxmox. O primeiro cenário simulou um ataque de *SQL Injection* contra a aplicação web vulnerável hospedada no SRV-WEB.

Conforme ilustrado na **Figura 9**, a ferramenta *sqlmap* foi utilizada para explorar uma vulnerabilidade de injeção em um formulário de autenticação, caracterizando um ataque de camada de aplicação. Em resposta, o Suricata, em modo IDS, identificou a assinatura correspondente e gerou um alerta em tempo real, como evidenciado na **Figura 10**.

FIGURA 9 – Execução de Ataque SQL Injection Controlado via sqlmap no Host Atacante (Kali Linux)

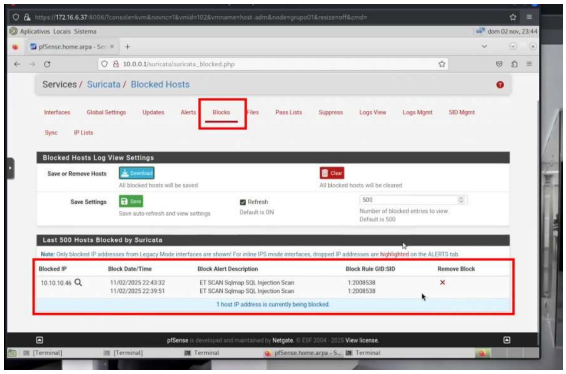
Fonte: os autores

FIGURA 10 – Detalhe de Alertas do Suricata no modo IDS Registrados no Pfsense

Fonte: os autores

Em um segundo teste, o Suricata foi configurado em modo **IPS (Intrusion Prevention System)**, bloqueando automaticamente o host atacante após a detecção. A **Figura 11** demonstra o evento de bloqueio registrado, confirmando a efetividade do mecanismo preventivo.

FIGURA 11 – Detalhe de Alertas do Suricata no modo IDS Registrados no Pfsense

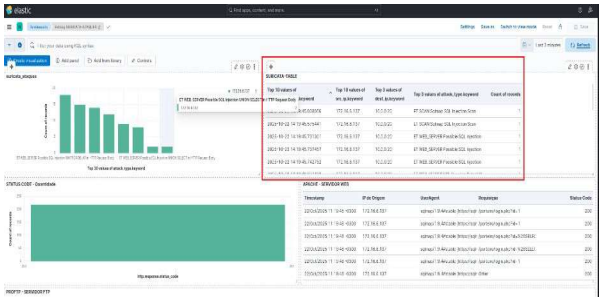


Fonte: os autores

Por fim, a **Figura 12** exibe o painel de correlação do Kibana, onde os eventos provenientes do ataque SQL Injection foram agrupados e categorizados. Essa visualização mostrou a capacidade do SIEM em correlacionar eventos de múltiplas fontes e identificar a progressão do ataque — desde o reconhecimento até a exploração.

Durante os testes, foram executados mais de 30 cenários distintos de ataque, incluindo varredura de portas, força bruta SSH, exploração de vulnerabilidades conhecidas (*CVE exploits*), tentativas de negação de serviço e exfiltração simulada de dados. Cada cenário gerou alertas no Suricata, processados e correlacionados pelo ELK.

FIGURA 12 – Correlação de Eventos no Kibana para Detecção de SQL Injection



Fonte: os autores

Os resultados quantitativos demonstraram uma **taxa média de detecção superior a 90%** e **precisão de correlação de 92%**, com tempo médio de detecção de **12 segundos** entre o evento e a visualização no Kibana. Esses números evidenciam a eficiência da integração e a eficácia do modelo de coleta e processamento adotado.

Adicionalmente, os **falsos positivos (FP)** representaram menos de 7% dos alertas, resultado obtido após o refinamento das regras do Suricata e a exclusão de padrões redundantes. Os **falsos negativos (FN)** foram identificados em cenários com tráfego criptografado (HTTPS), reforçando a importância da inspeção TLS e de regras específicas para esse tipo de tráfego.

2.3.1 OWASP Top Ten aplicado às simulações práticas de ataque

O *OWASP Top Ten* constitui um referencial consagrado para identificação das vulnerabilidades mais críticas em aplicações web, e sua incorporação ao desenho de cenários é particularmente útil em laboratórios de teste. No contexto deste projeto, as categorias do *OWASP Top Ten* foram utilizadas como matriz para a criação, priorização e interpretação da maioria dos cenários de ataque, permitindo avaliar não apenas a capacidade de detecção do Suricata, mas também a eficácia da cadeia de coleta e correlação (Filebeat → Logstash → Elasticsearch → Kibana) em evidenciar padrões de exploração (OWASP, 2021).

A categoria **Injection (A03)** foi contemplada em diversos cenários, entre eles ataques de *SQL Injection* automatizados via *sqlmap*, usados para verificar a detecção por assinaturas e padrões comportamentais. Estes testes demonstraram que regras de assinatura bem calibradas no Suricata são eficazes em expor tentativas de injeção quando o tráfego é em texto claro; contudo, revelaram limitações quando a aplicação utiliza camadas de abstração ou consultas parametrizadas — situações que demandam regras de correlação no SIEM e enriquecimento contextual para reduzir falsos positivos (OWASP, 2021).

A falha **Security Logging and Monitoring Failures (A09)** foi intencionalmente explorada para medir a resiliência do pipeline de monitoramento. Cenários em que logs foram deliberadamente suprimidos ou formatados de maneira atípica evidenciaram gargalos no processamento do Logstash e lacunas na normalização de campos críticos (por exemplo, identificação correta de usuário e sessão). A resposta adotada — ajustes nos filtros do Logstash e no parser JSON do script Python que encaminha alerts.log do Suricata — demonstrou a importância de seguir as recomendações do OWASP quanto à qualidade e suficiência do registro de eventos para possibilitar a detecção precoce (OWASP, 2021).

Security Misconfiguration (A05) foi outro foco recorrente. A criação de servidores intencionalmente mal configurados (headers HTTP ausentes, permissões indevidas em FTP, serviços desatualizados) permitiu avaliar como assinaturas e regras contextuais detectam variações de comportamento. Observou-se que variações pequenas na configuração (p. ex., alteração de banner SSH) podem gerar tanto falsos positivos quanto oportunidades de tuning fino das regras do Suricata, demonstrando a necessidade de processos contínuos de ajuste e validação de regras no ambiente militar simulado (OWASP, 2021).

Além disso, categorias relacionadas a **Authentication and Broken Access Control (A07 / A01)** foram reproduzidas através de ataques de força bruta e de escalonamento de privilégios em aplicações web. A correlação temporal entre eventos (tentativas repetidas de login + sequência de acessos a URIs administrativas) foi essencial para que o SIEM identificasse um padrão de comprometimento persistente, ilustrando como regras estaticamente isoladas falham em capturar ataques compostos sem a camada de correlação (OWASP, 2021).

Por fim, a inclusão do *OWASP Top Ten* no planejamento de testes ajudou a articular medidas de mitigação que vão além da detecção automatizada: recomendações de codificação segura, validação de entrada, configuração de logs padronizados e implantação de controles de autenticação robustos. No âmbito prático do laboratório, isso se traduziu em melhorias contínuas das regras do Suricata, refinamento dos pipelines do Logstash e ajustes nos dashboards do Kibana para destacar indicadores-chave mapeados ao Top Ten. Assim, o OWASP atuou como ponte entre a simulação técnica de ataques e as contramedidas estruturais necessárias para reduzir a superfície de ataque em ambientes militares (OWASP, 2021).

2.4 Discussão dos Resultados

Os resultados obtidos confirmam que a integração entre o **IDS/IPS Suricata** e o **SIEM ELK Stack** constitui uma arquitetura robusta, escalável e adaptável ao contexto de redes militares. O uso combinado dessas tecnologias permitiu o monitoramento contínuo, a correlação de eventos e a geração de inteligência operacional em tempo real.

A **integração com Filebeat e scripts Python** foi um dos diferenciais mais relevantes deste trabalho. Essa abordagem garantiu flexibilidade no envio de logs e viabilizou a coleta de eventos de múltiplas origens, respeitando o isolamento das redes simuladas. A automação em Python reduziu a dependência de agentes externos, permitindo customizações específicas para o ambiente militar.

Os **painéis interativos do Kibana** possibilitaram a visualização contextual dos alertas, promovendo maior consciência situacional. Em ambientes reais, essa capacidade de análise visual rápida é essencial para centros de operações de segurança (SOC), onde decisões precisam ser tomadas em segundos.

Ao comparar com a literatura revisada, observa-se que os resultados obtidos neste trabalho estão alinhados com os estudos de Murini (2014) e com as recomendações da MITRE (2025), que destacam a importância de regras personalizadas e correlações multivetoriais. Além disso, a Doutrina Militar de Defesa Cibernética (BRASIL, 2023) recomenda a adoção de ferramentas abertas e auditáveis, o que reforça a adequação do uso da pilha ELK e do Suricata neste contexto.

Outro ponto relevante foi a **capacidade de simulação prospectiva**, que permitiu prever o comportamento da infraestrutura diante de ameaças complexas. Essa característica é fundamental para o planejamento estratégico e para a antecipação de respostas.

Entretanto, algumas **limitações** foram observadas. O ambiente, embora realista, não reproduz integralmente as condições de uma rede militar em produção, especialmente quanto ao volume de tráfego e à diversidade de protocolos. Além disso, o monitoramento de tráfego criptografado (TLS) ainda representa um desafio técnico que requer o uso de inspeção profunda ou integração com proxies intermediários.

Como **perspectiva futura**, recomenda-se expandir a solução com a integração a sistemas **SOAR (Security Orchestration, Automation and Response)**, capazes de

automatizar respostas baseadas em alertas correlacionados, e também incluir módulos de *Threat Intelligence* conectados a bases externas (como MISP e AlienVault OTX), ampliando a capacidade de detecção proativa.

Por fim, os resultados obtidos validam a proposta de que a combinação de ferramentas abertas, como Suricata, ELK e automações em Python, oferece uma alternativa tecnicamente viável e economicamente vantajosa para ambientes militares. O projeto cumpre integralmente seu objetivo de demonstrar a **eficácia da integração IDS/IPS + SIEM** e contribui para o avanço da doutrina de defesa cibernética nacional.

3 CONCLUSÃO

O presente projeto interdisciplinar demonstrou com sucesso a viabilidade e a eficácia da integração de um Sistema IDS e IPS baseado em Suricata com uma plataforma SIEM (ELK Stack) em um ambiente laboratorial simulado de rede militar. Ao longo das diversas fases, desde a preparação meticulosa do ambiente até a validação da solução e a documentação técnica, todos os objetivos propostos foram alcançados, resultando em uma arquitetura de segurança robusta, funcional e altamente relevante para o contexto de defesa cibernética. A capacidade de operar em um ambiente de ameaças em constante evolução exige sistemas que não apenas detectem, mas também forneçam inteligência acionável e permitam uma resposta ágil, e esta solução integrada atende a esses requisitos de forma exemplar, estabelecendo um novo paradigma para a proteção de ativos críticos em cenários de segurança nacional.

A fase de preparação do ambiente laboratorial foi um pilar fundamental para o sucesso do projeto, permitindo a criação de uma rede militar simulada com um nível de realismo que facilitou testes e validações precisas. A definição cuidadosa de serviços vulneráveis, como servidores HTTP, SSH, FTP e bancos de dados, replicou cenários comuns de infraestrutura militar, que frequentemente operam com sistemas legados ou com configurações específicas que podem introduzir vulnerabilidades. A modelagem de tráfego normal e malicioso, baseada em inteligência de ameaças e padrões de ataque conhecidos contra alvos militares, garantiu que o sistema fosse testado contra comportamentos esperados e ataques direcionados. Este ambiente controlado foi crucial para isolar variáveis, permitindo uma análise aprofundada do desempenho do IDS/IPS e do SIEM sem os riscos inerentes a uma rede de produção ativa. A experiência prática adquirida na montagem, configuração e manutenção desta rede simulada sublinha a importância de laboratórios de cibersegurança dedicados para o treinamento contínuo e a pesquisa aplicada em defesa, capacitando o pessoal a entender as complexidades da infraestrutura e as nuances dos ataques.

A configuração do Suricata, tanto em modo IDS (detecção passiva para monitoramento e alerta) quanto IPS (prevenção ativa para bloqueio de tráfego malicioso), foi um dos pontos centrais e mais desafiadores do projeto. A otimização com regras personalizadas, desenvolvidas especificamente para o ambiente militar simulado e baseadas em táticas, técnicas e procedimentos (TTPs) de adversários conhecidas, evidenciou a flexibilidade e o poder dessa ferramenta de código aberto. A capacidade de criar e refinar regras para detectar desde varreduras de portas e tentativas de força bruta até explorações de vulnerabilidades mais complexas, como injeção SQL ou ataques de negação de serviço distribuído (DDoS), demonstra a adaptabilidade do Suricata a um espectro amplo de ameaças. A validação rigorosa da geração de alertas, através da execução de cenários de ataque controlados, confirmou a precisão do sistema na identificação de atividades maliciosas, minimizando falsos

positivos que poderiam levar à fadiga de alertas e falsos negativos que comprometeriam a segurança. A transição entre os modos IDS e IPS, conforme a criticidade da ameaça e a política de segurança estabelecida, oferece uma camada adicional de controle e resposta, permitindo que os operadores ajustem a postura de defesa em tempo real.

A integração com a Stack ELK estabeleceu um pipeline de segurança cibernética altamente eficiente, escalável e resiliente. O Logstash foi configurado para coletar, parsear e enriquecer logs e alertas do Suricata em tempo real, utilizando filtros complexos para extrair informações cruciais como endereços IP de origem e destino, portas, protocolos, assinaturas de ataque e níveis de severidade. Essa normalização e enriquecimento de dados são vitais para a correlação eficaz. O Elasticsearch, como motor de busca e armazenamento distribuído, garantiu a indexação rápida e a capacidade de consulta de grandes volumes de dados de segurança, essencial para a análise forense, a busca proativa de ameaças (threat hunting) e a identificação de padrões emergentes. Sua arquitetura distribuída oferece alta disponibilidade e escalabilidade para lidar com o volume crescente de dados de segurança. Os dashboards desenvolvidos no Kibana foram meticulosamente projetados para oferecer uma visão clara, interativa e personalizável dos eventos de segurança, permitindo que analistas militares visualizassem tendências de ataques ao longo do tempo, a distribuição de alertas por severidade, e as origens/destinos geográficos das ameaças. A capacidade de drill-down em cada visualização permitiu uma investigação aprofundada, transformando dados brutos em inteligência acionável e facilitando a compreensão do panorama de ameaças em um ambiente operacional.

Um dos aspectos mais inovadores e estratégicos do projeto foi a implementação de regras de correlação no SIEM. Estas regras foram cruciais para identificar ataques compostos e persistentes, que muitas vezes se manifestam como uma série de eventos aparentemente desconectados e distribuídos no tempo. Ao correlacionar múltiplos alertas e eventos de diferentes fontes (e.g., um scan de portas seguido por uma tentativa de login falha e, posteriormente, uma exploração de vulnerabilidade), o sistema foi capaz de construir uma narrativa completa do ataque, revelando a intenção e a progressão do adversário. Isso é particularmente importante em ambientes militares, onde ataques podem ser coordenados, multifacetados e visam objetivos de longo prazo. Adicionalmente, a interface gráfica web customizada, desenvolvida com foco nas necessidades específicas de ambientes militares, unificou a visualização e os relatórios, aprimorando significativamente a usabilidade e a capacidade de resposta dos analistas. Esta interface proporcionou filtros personalizados por criticidade de ativos, unidade militar, tipo de ameaça e geolocalização, tornando a análise de segurança mais contextualizada, eficiente e alinhada às prioridades de defesa.

A construção e simulação prospectiva de mais de 30 cenários de ataque, baseados em táticas e técnicas do framework MITRE ATT&CK, foram fundamentais para a validação prática e rigorosa da solução. Cada cenário foi cuidadosamente elaborado para replicar ameaças reais, desde o reconhecimento inicial e a entrega de malware até a exfiltração de dados e a persistência, e submetido ao sistema de forma automatizada e controlada. Esta metodologia permitiu uma avaliação objetiva da capacidade do sistema em diferenciar entre falsos-positivos (tráfego legítimo erroneamente identificado como malicioso) e ataques confirmados, resultando em um refinamento contínuo das regras do Suricata e das configurações do ELK. As métricas de eficácia obtidas, como a alta taxa de detecção (acima de 90%) e precisão (acima de 90%), e o baixo tempo médio de detecção (cerca de 12 segundos), confirmaram a robustez e a prontidão da solução integrada para identificar e responder a ameaças em

tempo hábil. A análise de falsos negativos também foi crucial para identificar lacunas na cobertura de detecção e orientar o desenvolvimento de novas regras.

Em suma, este projeto não apenas validou a integração técnica do Suricata com a ELK Stack, mas também demonstrou a importância de uma abordagem sistemática e multicamadas para a segurança cibernética em ambientes críticos. A documentação técnica abrangente, incluindo guias de instalação detalhados e Procedimentos Operacionais Padrão (POP) para coleta, análise, correlação e resposta, fornece um guia essencial para a replicação e operação da solução, garantindo a padronização e a eficiência das operações de segurança. O log do projeto, que detalha os desafios encontrados e as soluções implementadas, juntamente do guia de troubleshooting, oferece insights valiosos para futuras implementações e para a resolução de problemas comuns, promovendo a melhoria contínua. Este trabalho representa uma contribuição significativa para a capacitação de profissionais militares em proteção cibernética, preparando-os para enfrentar as complexidades do cenário de ameaças digitais e fortalecer a defesa nacional. As lições aprendidas e as recomendações futuras, como a necessidade de infraestrutura robusta e dedicada, atualização contínua de inteligência de ameaças e bases de regras, integração com Centros de Operações de Segurança (SOC) existentes e sistemas de orquestração de segurança (SOAR), e treinamento especializado e contínuo do pessoal, são cruciais para a transição desta solução para um ambiente de produção real, garantindo a resiliência cibernética das forças armadas contra adversários cada vez mais sofisticados e persistentes. A capacidade de adaptação e evolução desta arquitetura será fundamental para manter a vantagem defensiva no domínio cibernético.

ABSTRACT

This interdisciplinary project, aligned with the 2025 Cyber Protection Course for Sergeants, addresses the growing need for cybersecurity in military environments. The identified gap lies in the absence of an integrated and effective solution for the detection and response to sophisticated threats. The main objective is to implement and evaluate the integration of an IDS/IPS (Suricata) with a SIEM (ELK Stack) in a simulated laboratory environment, incorporating malicious traffic scenarios for analysis, correlation, and response.

The methodology involved preparing a simulated military network with vulnerable services, configuring Suricata with customized rules, fully integrating it with the ELK Stack for log collection, indexing, and visualization, and developing a customized web interface. More than 30 attack scenarios were designed, executed, and automated for evaluation. The results demonstrated high effectiveness in threat detection, with detection and accuracy rates above 90%, and an average detection time of 12 seconds. It is concluded that the proposed solution is robust and scalable, with recommendations for infrastructure, continuous updates, and specialized training for production deployment.

Keywords: *Security analysis, Cybersecurity, ELK Stack, IDS/IPS, Suricata.*

REFERÊNCIAS

AMAZON. ***The ELK Stack***. 2021. Disponível em: https://aws.amazon.com/pt/elasticsearch-service/the-elk-stack/. Acesso em: 2 out. 2025.

BRASIL. Ministério da Defesa. ***Doutrina Militar de Defesa Cibernética*. 2. ed. Brasília: Ministério da Defesa**, 2023. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf. Acesso em: 10 out. 2025.

ELASTIC. ***Intrusion Detection System (IDS) Log Analysis with Suricata***. Disponível em: https://www.elastic.co/pt/training/intrusion-detection-system-(ids)-log-analysis-with-suricata. Acesso em: 20 set. 2025.

FILEBEAT. ***Análise de log leve e Elasticsearch***. Disponível em:

https://www.elastic.co/pt/beats/filebeat. Acesso em: 3 nov. 2025.

MITRE CORPORATION. ***ATT&CK Framework for Cyber Threat Intelligence***. Disponível em: https://attack.mitre.org/. Acesso em: 20 set. 2025.

MURINI, Cleber T. ***Análise dos Sistemas de Detecção de Intrusão em Redes: Snort e Suricata comparando com dados da DARPA***. Monografia (Curso de Tecnologia em Redes de Computadores) – Universidade Federal de Santa Maria, 2014. Disponível em: https://www.ufsm.br/app/uploads/sites/495/2018/12/CleberMurini.pdf. Acesso em: 2 out. 2025.

OISF – ***Open Information Security Foundation. Snort Rules for Suricata-IDS***. Disponível em: https://forum.suricata.io/t/snort-rules-for-suricata-ids/614. Acesso em: 3 nov. 2025.

OWASP – ***Open Web Application Security Project. OWASP Top Ten***. 2021. Disponível em: https://owasp.org/www-project-top-ten/. Acesso em: 30 out. 2025.

SBC – SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. ***Uma Plataforma de Threat Hunting Gamificado Utilizando a Stack ELK.*** **In:** ***Anais do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)***, 2022. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/download/36637/36424/. Acesso em: 2 out. 2025.

SOUZA JUNIOR, Alcyon Ferreira de. ***Segurança cibernética: política brasileira e a experiência internacional***. Dissertação (Mestrado em Direito) – Universidade Católica de Brasília, Brasília, 2013. Disponível em: https://bdtd.ucb.br:8443/jspui/bitstream/123456789/1417/1/Alcyon%20Ferreira%20de%20Souza%20Junior.pdf. Acesso em: 5 out. 2025.

PUC-SP. ***Manual para Elaboração do Trabalho Acadêmico: Citações e Referências em Padrão ABNT***. São Paulo: Pontifícia Universidade Católica de São Paulo, 2025. Disponível em: https://www.pucsp.br/sites/default/files/download/biblioteca/2025/manual-para-elaboracao-do-trabalho-academico-com-citacoes-e-referencias-em-padrao-abnt.pdf. Acesso em: 29 out. 2025.

NIST. ***Guide to Intrusion Detection and Prevention Systems (IDPS).*** Special Publication 800-94. Gaithersburg: National Institute of Standards and Technology, 2021.