# AVALIAÇÃO DE SISTEMAS DE DETECÇÃO DE INTRUSOS NA COMPUTAÇÃO EM NUVEM

Mateus Kenzo Iochimoto (IC) e Charles Boulhosa Rodamilans (Orientador)

**Apoio:PIBIC CNPq**

## RESUMO

Motivados pelo crescimento dos tráfegos de rede e pelos ataques direcionados as organizações (que vão desde empresas até instituições governamentais), estas necessitam implementar mecanismos de defesa para sua rede, sendo uma delas sendo o Sistema de Detecção de Intrusos (IDS). Com a existência de diversas tecnologias que atuam como IDSs, existe a necessidade de identificar qual sistema implantar e utilizar; os motivos para decidir vão desde o quão performático o sistema é, até o quanto esse sistema pode oferecer em benefícios baseando-se no seu custo e/ou outras características. Neste estudo, uma pesquisa foi realizada levantado diversos serviços tradicionais de detecção de intrusos, como Suricata e Snort, como também IDSs baseados na nuvem, como o AWS GuardDuty e o Google Cloud IDS, com intuito de identificar características fundamentais utilizadas para escolha dos serviços, determinar as vantagens (e desvantagens) de cada sistema, para finalmente fazer uma comparação objetiva desses sistemas. Os principais resultados encontrados estão relacionados às situações em que esses dois tipos de sistemas são mais recomendados para serem usados em pequenas e grandes empresas, o qual inferiu-se, com base no custo, que os IDSs baseados na nuvem são mais recomendados do que os tradicionais para empresas pequenas, enquanto o contrário também foi observado para empresas grandes, em que concluímos que os sistemas tradicionais são mais vantajosos. Esses resultados se mostram de grande valor, em especial para as organizações que precisam implementar um sistema de detecção de intrusos e, portanto, precisam de um direcionamento para a escolha desses serviços.

**Palavras-chave:** Sistema de Detecção de Intrusos (IDS). Computação em Nuvem. Avaliação de Sistemas.

**ABSTRACT**

Motivated by the growth of network traffic and attacks directed at organizations (ranging from companies to government institutions), these need to implement defense mechanisms for their network, one of them being the Intrusion Detection System (IDS). With the existence of several technologies that act as IDSs, there is a need to identify which system to deploy and use; the reasons for deciding can range from how performant system is, to how much this system can offer in benefits based on its cost and/or other characteristics. In this study, research was carried out on several traditional intrusion detection services, such as Suricata and Snort, as well as cloud-based IDSs, such as AWS GuardDuty and Google Cloud IDS, in order to identify fundamental characteristics used to choose services, determine the advantages (and disadvantages) of each system, to finally make an objective comparison of these systems. The main results found are related to situations in which these two types of systems are more recommended for use in small and large companies, which inferred, based on cost, that cloud-based IDSs are more recommended than traditional systems for small companies, while the opposite was also observed for large companies, in which we concluded that traditional systems more advantageous. These results prove to be of great value, especially for organizations that need to implement an intrusion detection system and, therefore, need guidance for choosing these services.

**Keywords:** Intrusion Detection System (IDS). Cloud Computing. System evaluation.

## 1. INTRODUÇÃO

Atualmente é cada vez mais notório e relevante a atuação da área da segurança de sistemas. A necessidade cada vez mais crescente de defendermos os dados, desde os nossos próprios, de conhecidos ou até mesmo de clientes.

Um caso recente registrado por Poder360 (2021), acerca de ataques hackers em sites e aplicativos do Ministério da Saúde, que acarretou na exclusão de milhões de dados desse sistema além de que muitos dados desses usuários foram feitos como reféns, esse mesmo grupo também atacou o sistema do Mercado Livre, NVIDIA, Localiza e Samsung. Esses casos são para mostrar que até mesmo as maiores empresas e até governos precisam se preocupar com a segurança de seus sistemas.

Os sistemas de detecção de instrução tradicionais (Khan, 2016) são normalmente instalados e utilizados nas empresas (ex. snort, suricata) podem ser instalados em máquinas virtuais na nuvem computacional para reduzir os custos da empresa. As empresas também podem optar pela utilização dos serviços de IDS oferecidos pela própria nuvem. A AWS oferece o IDS chamado de GuardDuty - usa *feeds* de inteligência contra ameaças, como listas de endereços IP e domínios maliciosos e aprendizado de máquina para identificar atividades inesperadas e potencialmente não autorizadas e maliciosas e outro serviço de segurança chamado Amazon Detective, que funciona por meio de uma Inteligência artificial que coleta automaticamente dados de log para criar um conjunto de dados vinculados que permite realizar facilmente investigações de segurança mais rápidas e eficientes. O Microsoft Azure possui o Azure Defender - ele encontra pontos fracos em sua configuração de nuvem, ajuda a fortalecer a postura geral de segurança do seu ambiente e pode proteger cargas de trabalho em ambientes multi nuvem e híbridos contra ameaças em evolução; e também o Microsoft Sentinel, que dá uma visão geral da empresa usando *machine learning.*

Pelo advento do crescimento das redes de comunicações e do crescimento de atacantes ativos globalmente, o tema de cibersegurança se tornou muito importante, e, as tecnologias de defesa (como os sistemas de detecção de intrusos) tem sido fundamentais para a segurança da organização. Por existirem diversos serviços de IDS sendo disponibilizados, o usuário/organização fica em dúvida de qual ferramenta/serviço utilizar: seria um serviço que oferece funcionalidades que facilitam a sua utilização e manutenção? Ou um serviço que proporciona uma alta performance a um elevado custo seria uma melhor opção? Estas questões acerca do tema evidenciou a importância de um estudo comparativo dos sistemas de IDS e com a intenção de qualificar esses sistemas por meio das suas funcionalidades e de suas capacidades, em uma perspectiva envolvendo sistemas de dois tipos: tradicionais e os baseados em nuvem. O estudo também tem como intenção entender

as vantagens (e desvantagens) de usar serviços que não cobram por licença, e serviços que cobram pelo sua utilização mas possuem inúmeras funcionalidades que facilitam a sua implantação e manutenção.

O objetivo deste trabalho é comparar os sistemas de deteção de intrusos tradicionais (instalados na própria empresa) e serviços de detecção de intrusos oferecidos pela nuvem, analisando suas funcionalidades e custos.

## 2. REFERENCIAL TEÓRICO

### 2.1. Sistema de Detecção de Intruso (IDS)

Para diminuir o número desses casos foram criados sistemas de detecção de intrusos (Intrusion Detection System - IDS) (Kurose, 2015) - sistemas computacionais para detecção de possíveis invasores na organização. Esses sistemas monitoram o tráfego de rede e/ou eventos dos computadores procurando por atividades suspeitas e ameaças conhecidas e podem lançar um alerta quando encontra. Existem duas variantes para esse tipo de sistema: os baseados em rede (Network Intrusion Detection System - NIDS) e os baseados em hosts (Host Intrusion Detection System - HIDS).

### 2.2.1 Tipos de IDS

Os sistemas de detecção de intrusos baseados em rede (NIDS), são um tipo de IDS baseado em rede, controlando o tráfego que flui pela rede, analisando pacotes em tempo real, procurando padrões ou assinaturas que correspondam a padrões de ataque conhecidos ou comportamento anormal. O NIDS pode ser implementado como dispositivos de hardware ou soluções de software executados em servidores dedicados ou dispositivos de rede.

Já os sistemas de detecção baseado em host (HIDS), concentram-se no monitoramento das atividades em sistemas host individuais, como servidores ou *endpoints*. Ao contrário do NIDS, o HIDS opera no nível do host e pode monitorar logs do sistema, integridade de arquivos e outros dados específicos do sistema.

Algumas soluções de segurança modernas combinam elementos de NIDS e HIDS para criar um sistema de prevenção e detecção de intrusos (IDPS) mais abrangente. Esses sistemas híbridos oferecem uma abordagem mais holística para monitoramento de rede e host, fornecendo uma ampla gama de cobertura de segurança e insights mais profundos sobre possíveis ameaças.

### 2.2.2 Ferramentas de ids

SURICATA

O Suricata (Suricata, 2023) é um sistema de detecção e prevenção de intrusos de alto desempenho e mecanismo de monitoramento de segurança de rede, desenvolvido pela Open Information Security Foundation (OISF). Ele foi projetado para inspecionar o tráfego de rede em tempo real e pode detectar uma ampla gama de ameaças, incluindo invasões, malware e outras atividades maliciosas. Suricata usa um modelo de detecção baseado em regras, semelhante ao Snort, mas também possui suporte para ameaças emergentes e outros conjuntos de regras. O Suricata é conhecido por sua implementação que usa o *multithreading*, que permite lidar com tráfego de rede de alta velocidade de maneira eficaz. É frequentemente usado como um componente essencial em Centros de Operações de Segurança (SOCs) e infraestruturas de segurança de rede.

SNORT

O Snort (Snort, 2023) é um dos sistemas de detecção de intrusos de código aberto mais antigos e amplamente utilizados. Foi projetado por Martin Roche em 1998 e agora é administrado pela Cisco. O Snort funciona analisando o tráfego de rede em relação a um conjunto de regras. Essas regras são definidas para identificar padrões ou assinaturas específicas associadas a ameaças conhecidas, como malware, ataques de rede e outras atividades maliciosas. O Snort pode ser usado no modo IDS (detectando possíveis ameaças) e no modo IPS (bloqueando o tráfego caso necessário). Esse sistema é altamente escalável e expansível, tornando-se popular para redes pequenas e grandes.

Em resumo, Suricata e Snort são ferramentas valiosas no gerenciamento de segurança de rede e detecção de intrusão. Cada um tem seus pontos fortes e a escolha da implementação depende dos dados usados, dos requisitos de rede e da quantidade a ser analisada.

## 2.3 Computação em Nuvem

A computação em nuvem é a disponibilidade sob demanda de recursos computacionais pela Internet (Qian, 2009) - você pode usufruir de recursos sem necessariamente ter a máquina física. Como por exemplo, você pode utilizar máquinas virtuais (MVs) remotamente, cada uma com sistemas operacionais diferentes. A computação em nuvem normalmente usa

um modelo de "*pay-as-you-go*", que ajuda a reduzir despesas de capital inicial da empresa. Pelo sistema da nuvem ser de fácil acesso e oferecer diversos serviços é que cada vez ela é mais relevante e bastante utilizada. Os dois provedores de nuvem atuais líderes de mercados são o da Amazon Web Services (AWS) e Microsoft Azure.

### 2.3.1 Serviços de ids na nuvem

AWS GuardDuty

O AWS GuardDuty (AWS, 2023b) é um serviço de detecção de ameaças gerenciado pela AWS projetado para proteger seus recursos na nuvem contra atividades maliciosas e comportamentos suspeitos. Lançado em 2017, o GuardDuty utiliza a inteligência artificial, aprendizado de máquina e análise de dados em tempo real para monitorar continuamente a atividade em suas contas da AWS e identificar possíveis ameaças de segurança. O serviço opera em uma variedade de fontes de dados, incluindo logs de fluxo de rede, registros de DNS e registros de autenticação, para analisar padrões de tráfego, comunicações e interações com recursos da AWS.

Quando o GuardDuty identifica uma ameaça potencial, ele gera alertas detalhados, notificando os usuários através do console da AWS, e-mail ou integrações com serviços de gerenciamento de incidentes, permitindo aos administradores e equipes de segurança poderem tomar medidas imediatas para mitigar as ameaças antes que elas causem danos significativos aos recursos na nuvem.

Uma das principais vantagens do AWS GuardDuty é a sua capacidade de ser facilmente integrado com outros serviços da AWS, como o AWS CloudTrail, CloudWatch e o Amazon Macie, para fornecer uma solução de segurança holística e abrangente para ambientes na nuvem. Além disso, como é um serviço gerenciado, a AWS cuida das atualizações, manutenção e escalabilidade, permitido que os usuários se concentrem na análise das ameaças e na proteção de seus recursos.

Google Cloud IDS

O Google Cloud IDS (Google, 2023) é um serviço gerenciado de detecção de intrusos nativo da nuvem que cria uma rede gerenciada pelo Google com instâncias de máquina virtual (VM), possuindo também um grande suporte a muitos requisitos de compliance de empresas. O tráfego na rede é espelhado e inspecionado pelo Palo Alto Networks Next-Generation Firewall (NGFW) para fornecer detecção avançada de ameaças.

É importante ressaltar que a Azure (Microsoft) que também é um grande nome nesse modelo de negócios, também possui serviços de IDS próprios, porém, nesse trabalho por uma questão de acessibilidade acabamos optando por usar o AWS GuardDuty e o Google Cloud IDS como representantes dos IDS nativos da nuvem.

## 3. METODOLOGIA

Este estudo tem por finalidade compreender e comparar IDSs para auxiliar na escolha de qual sistema utilizar e também para saber em qual situação esse sistema é o mais recomendado.

A classificação dessa pesquisa quanto aos seus objetivos, é dada por exploratória, visto que esse estudo teve um grande enfoque na compreensão das vantagens e desvantagens entre IDSs de dois modelos de negócios diferentes, tradicionais e baseados em nuvem, assim, disponibilizando mais informações sobre um caso pouco estudado.

Os procedimentos de coleta dos dados, que serão citados posteriormente, foram feitos através de uma pesquisa bibliográfica e documental, com abordagem qualitativa, com o intuito de relacionar os dados, levantar suas particularidades e então fazer uma interpretação deles, tendo como foco o estudo dos sistemas de detecção de intrusos tradicionais, como o Suricata e o Snort, e os baseados na nuvem, como o AWS GuardDuty e o Google Cloud IDS.

Para a nossa pesquisa bibliográfica e documental, utilizamos como base o artigo de Khan *et al.* (2016) para basear algumas das nossas métricas utilizadas, como, “escalabilidade”, “tipos de detecção”. Já no artigo de Park *et al.* (2017), os autores tratam sobre a utilização de recursos das IDSs tradicionais, e por isso utilizamos os resultados obtidos desse estudo para basear a nossa métrica de “utilização de recursos”. Para as funcionalidades como “facilidade de operação”, “atualização de assinaturas” e “integração”, foram feitas pesquisas nos próprios documentos dessas ferramentas quanto a essas capacidades (AWS)(Google Cloud).

## 4. RESULTADO

Nesta seção, iremos apresentar os resultados encontrados referente ao objetivo do dado artigo, que é afinal comparar IDSs tradicionais e nativos da nuvem, por meio de análises criteriosas sobre suas funcionalidades e custos. Para tanto, foi primeiro levantada uma comparação mais focada entre os IDS de nuvem em si, comparando as funcionalidades do AWS GuardDuty com o Google Cloud IDS, sintetizados na **Tabela 1**, para então chegar em uma comparação entre os IDS tradicionais e os nativos de nuvem que foram sintetizados na

**Tabela 2**. Finalizando então com uma última comparação dos ataques entre os sistemas tradicionais e nativos de nuvem para saber se são ou não capazes de detectar os ataques mais populares de hoje em dia, em que foi montado a **Tabela 3** com os resultados.

### 4.1 Comparação de ids somente de Nuvem

Realizou-se a comparação dos IDS para detecção voltado para Nuvem, com funcionalidades especificas de Nuvem. As funcionalidades analisadas foram:

- **Detecção em tempo real:** A detecção em tempo real é uma capacidade fundamental para sistemas de segurança na nuvem. Isso significa que eles podem identificar e alertar sobre atividades maliciosas em potencial à medida em que ocorrem, permitindo que as equipes de segurança tomem medidas imediatas para mitigar os riscos.
- **Detecção em máquinas virtuais:** Essa funcionalidade é essencial para identificar tentativas de intrusões e comportamentos maliciosos em instâncias de VMs (Virtual Machines), ajudando a manter a segurança das cargas de trabalho.
- **Detecção de escalonamento de privilégios na rede:** O escalonamento de privilégios é uma técnica comum usada por invasores para obter acesso não autorizado a sistemas.
- **Análise de logs:** É o processo de detecção em que os sistemas utilizam logs e eventos gerados em suas plataformas para identificar atividades maliciosas, como tráfego incomum e outras anomalias que possam indicar intrusão.
- **Correlação de eventos:** A correlação é uma técnica usada para aumentar a precisão da detecção de ameaças.
- **Integração com ferramentas de gestão e de resposta de incidentes:** Essa integração permite que as equipes de segurança tomem medidas rápidas e coordenadas para conter e responder a ameaças em tempo hábil.
- **Personalização das regras:** É uma capacidade importante para adequar a detecção de ameaças às necessidades específicas de cada organização.
- **Detecção de ameaças em ambientes híbridos:** Esse é o potencial de detecção para as organizações que utilizam tanto recursos em nuvem quanto recursos locais, importantíssimo para empresas que mantêm uma infraestrutura distribuída que precisa de soluções abrangentes de segurança.
- **Detecção de ameaças em aplicativos e serviços da nuvem:** Essa funcionalidade é crucial para garantir a segurança dos dados e operações na nuvem.

- **Detecção de ameaças em dispositivos de borda:** Essa funcionalidade é a capacidade do serviço de ser configurado para monitorar dispositivos de borda em ambientes híbridos, permitindo a detecção de atividades maliciosas nos pontos de entrada da rede, proporcionando uma camada adicional de segurança.

| | AWS Guardduty | Google cloud IDS |
|---|---|---|
| Detecção em tempo real | X | X |
| Detecção em máquinas virtuais | X | X |
| Detecção de escalonamento de privilégios na rede | X | X |
| Análise de logs | X | X |
| Correlação de eventos | X | X |
| Integração com ferramentas de gestão e de resposta a incidentes | X | X |
| Personalização das regras | X | X |
| Detecção de ameaças em ambientes híbridos | X | X |
| Detecção de ameaça em aplicativos e serviços de nuvem | X | X |
| Detecção de ameaça em dispositivos de borda | | X |

Tabela 1 sobre as funcionalidades que o AWS GuardDuty e o Google Cloud IDS oferecem.

Fonte: autoria própria.

Por meio dessas funcionalidades levantadas foi possível montar uma Tabela 1 de comparação de ambos AWS GuardDuty e Google Cloud IDS, e notou-se como que ambos os serviços fornecem praticamente as mesmas funcionalidades, mostrando realmente como essas funcionalidades são essenciais para sistemas de detecção de intrusos específicos da

nuvem. A diferença foi na funcionalidade *detecção de ameaça de em dispositivos de borda*, fornecendo uma vantagem para Google Cloud IDS.

### 4.2 Comparação de IDS tradicional (opensource) e de Nuvem

No cenário de segurança cibernética em constante mudança, as organizações enfrentam uma batalha constante contra agentes mal-intencionados que procuram invadir em suas redes e comprometer dados confidenciais. Os dois principais tipos de soluções IDS são sistemas locais tradicionais (*on-premise*), que no dado trabalho serão representados por Suricata e Snort, e soluções baseadas em nuvem, das quais o AWS GuardDuty e o Google Cloud IDS serão usados para comparação neste trabalho.

As características analisadas foram: Atualização de assinaturas, utilização de recursos, privacidade dos dados, integração, capacidade de detecção, facilidade de operação, preço, escalabilidade. Na **Tabela 2** serão postas essas características de maneira mais simples, possuindo uma explicação mais detalhada nas próximas subseções.

| | Tradicional | | Nuvem | |
|---|---|---|---|---|
| | Suricata | Snort | Google Cloud IDS | AWS GuardDuty |
| Atualização de assinaturas | Não possui | Não possui | Existe | Existe |
| Utilização de recursos | Possui | Possui | Não possui | Não possui |
| Integração | Possui | Possui | Possui | Possui |
| Tipos de detecção | Assinatura e anomalia | Assinatura e anomalia | Assinatura, anomalia, outras | Assinatura, anomalia, outras |
| Facilidade de operação | Difícil | Difícil | Fácil | Fácil |
| Escalabilidade | Possui | Possui | Possui | Possui |

Tabela 2 simplificada utilizando os critérios levantados para comparação tradicional x nuvem.

Fonte: Autoria Própria.

#### 4.2.1 Atualizações de assinaturas

A Atualização de assinaturas é um critério sobre o quão fácil/prático é para manter e trocar as assinaturas, conjunto de regras usado nos sistemas para detectar as ameaças.

Classificou-se como:

- Possui: a atualização é realizada de forma automática.
- Não possui: a atualização deve ser feita de forma manual.

**IDS tradicionais:** Quando usados, é preciso que os operadores desses sistemas regularmente e manualmente atualizem os códigos e as assinaturas dos sistemas para sempre se manterem à frente das atividades maliciosas. As ferramentas Suricata e Snort não possuem funcionalidades que atualizam suas assinaturas de forma automática e por isso precisam ser atualizadas manualmente.

**IDS baseado em cloud:** Em contrapartida das soluções tradicionais, as baseadas em nuvem se beneficiam disso, pelo fato de terem atualizações automatizadas diretamente do provedor, garantindo um acesso fácil a uma ferramenta atualizada das ameaças mais recentes. Como o Google Cloud IDS e AWS GuardDuty.

### 4.2.2 Utilização de recursos

A Utilização de recursos é a característica para dizer o quanto que o sistema utiliza dos recursos da máquina em que ele está sendo utilizado.

Classificou-se como:

- Possui: requer um hardware físico para ser utilizado.
- Não possui: não utiliza os recursos do hardware do usuário, visto que esses recursos estão sendo utilizados na nuvem.

**IDS tradicionais:** Nesses sistemas é necessário ter um hardware dedicado ou máquinas virtuais com capacidade de processamento, memória e armazenamento suficientes. As ferramentas Suricata e Snort ainda que possuam um baixo uso desses recursos isso segundo

o estudo de Hoover (2022), ainda sim possuem uma certa utilização, o que não ocorre para os sistemas baseados na nuvem.

**IDS baseado em cloud:** Essas soluções não precisam de servidor, maximizando os recursos com base nos serviços de nuvem, reduzindo a carga de hardware e infraestrutura derivado das soluções tradicionais. O que é verdade para o AWS GuardDuty e o Google Cloud IDS.

### 4.2.3 Integração

A Integração é a característica que diz sobre a capacidade desses sistemas de poderem se integrarem a outros serviços/sistemas para auxiliar na análise, gerenciamento, entre outros, das informações que os IDS detectam.

Classificou-se como:

- Possui: possui sistemas/serviços disponíveis para se integrar.
- Não possui: não existem serviços/sistemas para se integrarem a esses sistemas.

**IDS tradicionais:** Esses sistemas podem ser combinados com outras ferramentas de segurança e sistemas de segurança de informação e gerenciamento de eventos (SIEM) (IBM, 2023) para uma avaliação abrangente das ameaças. O Suricata e Snort podem ser facilmente integrados ao Splunk, QRADAR (IBM), ArcSight, e outros. Por essa grande quantidade de serviços que podem ser integrados, ambos sistemas foram qualificados como possui na Tabela 2.

**IDS baseado em cloud:** Podem ser integradas a outros serviços de segurança da própria provedora de nuvem, para fornecer uma plataforma centralizada de gerenciamento de segurança. O AWS GuardDuty e o Google Cloud IDS podem se integrar uma variedade de serviços, que podem ser desde sistemas de gerenciamento de identidade e acesso (IAM), como AWS IAM e Google Cloud Identity and Access Management, firewalls de rede, como AWS WAF e o Google Cloud Firewall, SIEMs, como o Splunk, o AWS Security Command Center e o Google Cloud Security Command Center, entre muitos outros serviços. Por essa grande quantidade de serviços que podem ser integrados, ambos sistemas foram qualificados como *possui* na Tabela 2.

### 4.2.4 Tipos de detecção

Os Tipos de detecção se dão pelo conjunto de técnicas de detecção que os sistemas IDS analisados utilizam para realizar suas detecções.

**Detecção baseada em assinatura (signature-based) (Mishra, 2017):** Ambas soluções nativas e não-nativas de nuvem utilizam esse modelo de detecção para identificar ameaças conhecidas com base em padrões predefinidos. Sistemas: Suricata, Snort, AWS GuardDuty, Google Cloud IDS.

**Detecção baseada em anomalia (anomaly-based)(Mishra, 2017):** Embora os sistemas tradicionais possam ser mais limitados a algumas técnicas baseadas em anomalia, os IDSs baseados na nuvem geralmente resultam de uma junção de dados e algoritmos avançados de aprendizado de máquina. Sistemas: Suricata, Snort, AWS GuardDuty, Google Cloud IDS.

**Detecção de ameaças em nuvem:** As soluções IDS baseadas na nuvem possuem uma vantagem natural na detecção de ameaças específicas da nuvem, como por exemplo na detecção de tentativas não autorizadas de desabilitar o AWS CloudTrail logging, a iniciação de instâncias em regiões não usuais e até tentativas de login suspeitas nos bancos de dados. Sistemas: AWS GuardDuty, Google Cloud IDS.

### 4.2.5 Escalabilidade:

A Escalabilidade descreve a capacidade do sistema de manter seu desempenho ao aumentar seu volume de trabalho.

Classificou-se como:

- Possível: para as situações em que os sistemas têm grande capacidade de serem escalados, seja pela sua arquitetura ou pelo seu modelo de negócios.
- Não possível: para as situações em que os sistemas não podem ser escalados.

**IDS tradicionais:** A escalabilidade nesses sistemas pode ser limitada por recursos de hardware e alterações manuais na configuração. O Suricata e o Snort, ambos possuem capacidades de aumentar sua escalabilidade com a utilização dos seus recursos *multithreading*, aumentando sua performance e assim também sua escalabilidade, porém, suas capacidades de escalabilidade podem também ser limitadas aos recursos de suas máquinas, ainda assim possuem a possibilidade de serem implementados em ambientes virtuais na nuvem, e por isso foram classificados como escalabilidade alta na Tabela 2.

**IDS baseada em cloud:** Já nesses sistemas, por se tratar de um serviço baseado na nuvem, existe uma maior escalabilidade dinâmica, em que os recursos vão se alterando conforme os requisitos também se alteram. O AWS GuardDuty e o Google Cloud IDS não possuem nenhum limitador físico na questão da sua escalabilidade, sem considerar os custos para manter esse serviço, por isso a escalabilidade foi considerada como alta na Tabela 2.

#### 4.2.6 Facilidade de operação:

A Facilidade de operação descreve a facilidade para administrar e analisar esses sistemas.

Classificou-se como:

- Difícil: para as situações em que os sistemas são complexos de se utilizar, requerendo um conhecimento aprofundado à sua utilização.
- Fácil: para as situações em que os sistemas possuem suporte de fácil acesso à sua utilização, funcionalidades já prontas, o que faz com que esses sistemas sejam mais simples de administrar.

**IDS tradicional:** As soluções de IDS tradicionais requerem monitoramento manual e revisão por profissionais de segurança experientes. O Suricata e o Snort são ferramentas mais difíceis de se utilizar, na medida em que é preciso de um profissional de segurança experiente para manejar essas ferramentas, por esse motivo, a gestão usabilidade dessas ferramentas foi classificada como difícil na Tabela 2.

**IDS baseada em cloud:** As soluções IDS baseadas em nuvem geralmente vêm com interfaces e automações fáceis de usar, tornando-as mais acessíveis a um público mais amplo. O AWS GuardDuty e o Google Cloud IDS possuem interfaces mais fáceis de

compreender e funcionalidades que tornam o manejo dessas ferramentas por pessoas menos qualificadas mais acessível.

### 4.3 Comparação dos IDS quanto a deteção de Ataques Maliciosos

Realizou-se a comparação dos IDS para deteção de ataques específicos. Os ataques analisados foram:

- ***Phishing* (Khonji, 2013):** é uma técnica de ataque cibernético em que os atacantes tentam se passar por indivíduos ou entidades legítimas para induzir os usuários a revelarem informações confidenciais, como nomes de usuário, senhas, detalhes de cartão de crédito ou outros dados.
- **Cryptomining (Pastrana, 2019):** é um ataque em que os *hackers* usam de modo clandestino os recursos de computação da vítima para minerar criptomoedas. Os invasores infectam o computador ou a rede da vítima com malware de criptomineração, que consome energia do computador e eletricidade para minerar criptomoedas para os invasores sem o conhecimento ou consentimento da vítima.
- ***Bruteforce* (Najafabadi, 2014):** é um ataque que envolve tentar sistematicamente todas as combinações possíveis para nomes de usuários e senhas até que seja encontrada a certa. O invasor utiliza ferramentas automatizadas que geram e testam rapidamente essas combinações, tentando obter acesso não autorizado a contas ou sistemas de usuários.
- **DdoS (Kene, 2015):** o ataque Distributed Denial-of-Service (DDoS) (em português, Negação de Serviço Distribuída) é um ataque que envolve sobrecarregar um sistema de destino, como um site ou serviço online, utilizando um grande volume de tráfego de várias fontes simultaneamente. O objetivo é esgotar os recursos do alvo, causando interrupções no serviço e tornando-o indisponível para usuários legítimos.
- ***Port Scan* (Kene, 2015):** é uma das técnicas de reconhecimento usadas para identificar portas abertas em um sistema de destino. Os invasores usam ferramentas especializadas para sondar uma variedade de endereços IP e portas para descobrir possíveis pontos de entrada para explorar vulnerabilidades ou obter acesso não autorizado.
- ***SQL injection* (Halfond, 2006):** é um tipo de ataque de aplicações web que explora vulnerabilidades em sites ou aplicativos mal codificados. Os invasores inserem código SQL malicioso nos campos de entrada, na esperança de manipular o banco de dados utilizado.

- ***Ransomware* (Ng, 2018):** é um ataque que utiliza software malicioso para criptografar os arquivos de vítimas, tornando-os inacessíveis. Os invasores exigem um resgate, geralmente em criptomoeda, em troca do fornecimento da chave para decodificar para então ter acesso aos arquivos.

Os resultados são apresentados na Tabela 3. Foi observado que esses serviços estão bem equilibrados em questão de serem capazes de detectar essas ameaças mais comuns.

| | Tradicional | | Nuvem | |
|---|---|---|---|---|
| | Suricata | Snort | AWS GuardDuty | Google cloud IDS |
| Phishing/ Spear Phishing | X | X | X | X |
| Cryptomining | X | X | X | X |
| Bruteforce | X | X | X | X |
| DDoS | X | X | X | X |
| Port Scan | X | X | X | X |
| SQL Injection | X | X | X | X |
| Ransomware | X | X | X | X |

Tabela 3 que mostra os ataques que as IDSs tradicionais e de nuvem conseguem detectar.

Fonte: autoria própria.

## 5. CONSIDERAÇÕES FINAIS

Em conclusão, a escolha entre soluções IDS tradicionais (como Suricata e Snort) e soluções IDS baseadas em nuvem (como AWS GuardDuty e Google Cloud IDS) dependem muito das necessidades e requisitos específicos de segurança, políticas e considerações regulatórias de uma organização. Enquanto as soluções IDS tradicionais oferecem uma segurança local (*on-premise*) mais customizável, as soluções baseadas na nuvem trazem benefícios específicos para a nuvem, como, escalabilidade dinâmica, atualizações

automáticas, integração perfeita com serviços da nuvem. Em suma, a escolha do melhor serviço depende dos requisitos que a própria organização possui, em que para empresas menores, muitas vezes serviços de nuvem podem ser muito mais vantajosos do que os tradicionais, visto que para elas não existirá por exemplo o custo inicial da aquisição e manutenção das máquinas, quem sabe também em questão da qualificação profissional do time como um todo, em que esses sistemas requerem em geral uma menor experiência para sua compreensão entre outros motivos, ou então para empresas maiores, em que se pode inferir que para elas talvez os IDSs tradicionais sejam mais conta, pelo fato de geralmente já possuírem pessoas qualificadas e máquinas para manejar essas tecnologias, ou até pelo fato de que a quantidade dos dados analisados possa ser tão grande que acabe gerando um custo maior do que ter as máquinas físicas.

## 6. REFERÊNCIAS


ArcSight SIEM. Disponível em: <https://www.microfocus.com/en-us/cyberres/secops/arcsight-esm>. Acesso em: 16 de ago. 2023

AWS GuardDuty Amazon Web Services (AWS). Disponível em: <https://aws.amazon.com/guardduty/>. Acesso em: 16 de ago. 2023b.

AWS. **Amazon GuardDuty User Guide**. Disponível em: < https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html>. Acesso em: 16 de ago. 2023a.

Azure. Disponível em <https://azure.microsoft.com/en-us/>. Acesso em: 16 de ago. 2023

Google Cloud IDS. Disponível em: <https://cloud.google.com/intrusion-detection-system>. Acesso em: 16 de ago. 2023

Hoover, Cole. **Comparative study of snort 3 and suricata intrusion detection systems**. 2022. Acesso em: 16 de ago. 2023.

Halfond, W.G., Viegas, J. and Orso, A., 2006, March. **A classification of SQL-injection attacks and countermeasures**. In *Proceedings of the IEEE international symposium on secure software engineering* (Vol. 1, pp. 13-15). IEEE. Acesso em: 16 de ago. 2023

IBM. **O que é SIEM**. Disponível em: < https://www.ibm.com/br-pt/topics/siem>. Acesso em: 16 de ago. 2023

IBM. QRADAR. Disponível em: < https://www.ibm.com/qradar>. Acesso em: 16 de ago. 2023

Kene, S.G. and Theng, D.P., 2015. **A review on intrusion detection techniques for cloud computing and security challenges**. In *2015 2nd International Conference on Electronics and Communication Systems (ICECS)* (pp. 227-232). IEEE. Acesso em: 16 de ago. 2023

Khan, M.A. **A survey of security issues for cloud computing. *Journal of network and computer applications***. 2016. Acesso em: 16 de ago. 2023

Khonji, M., Iraqi, Y. and Jones, A., 2013. **Phishing detection: a literature survey**. *IEEE Communications Surveys & Tutorials*, *15*(4), pp.2091-2121. Acesso em: 16 de ago. 2023

Kurose, James, Keith Ross. **Redes de computadores e a Internet - uma abordagem top-down**. 6. ed. Pearson, 2015. Acesso em: 16 de ago. 2023

Mishra, P., Pilli, E.S., Varadharajan, V. and Tupakula, U., 2017. **Intrusion detection techniques in cloud environment**: A survey. *Journal of Network and Computer Applications*, *77*, pp.18-47. Acesso em: 16 de ago. 2023

Najafabadi, M.M., Khoshgoftaar, T.M., Kemp, C., Seliya, N. and Zuech, R., 2014. **Machine learning for detecting brute force attacks at the network level**. In *2014 IEEE International Conference on Bioinformatics and Bioengineering* (pp. 379-385). IEEE. Acesso em: 16 de ago. 2023

Ng, C.K., Pan, L., Xiang, Y., Ng, C.K., Pan, L. and Xiang, Y., 2018. Ramsonware and Honeypot. ***Honeypot Frameworks and Their Applications: A New Framework***, pp.75-78. Acesso em: 16 de ago. 2023

Open Information Security Foundation (OISF). **Suricata Documentation**. Disponível em <https://suricata.io/documentation/>. Acesso em: 16 de ago. 2023

Park, Wonhyung, and Seongjin Ahn, 2017. **Performance comparison and detection analysis in snort and suricata environment**. *Wireless Personal Communications* 94: 241-252. Acesso em: 16 de ago. 2023

Pastrana, S. and Suarez-Tangil, G., 2019, October. **A first look at the crypto-mining malware ecosystem: A decade of unrestricted wealth**. In *Proceedings of the Internet Measurement Conference* (pp. 73-86). Acesso em: 16 de ago. 2023

Poder360, 2021. **Sites do Ministério da Saúde sofrem ataque hacker e estão fora do ar**. Disponível em: <https://www.poder360.com.br/governo/sites-do-ministerio-da-saude-sofrem-ataque-hacker-e-estao-fora-do-ar/>. Acesso em: 16 de ago. 2023

Qian, L., Luo, Z., Du, Y.; Guo, L., 2009. **Cloud computing: An overview**. In *IEEE international conference on cloud computing*. Springer, Berlin, Heidelberg. Acesso em: 16 de ago. 2023

SNORT. Disponível em: <https://www.snort.org>. Acesso em: 16 de ago. 2023

Splunk. **What is Splunk & What Does It Do? An introduction To Splunk**. Disponível em: < https://www.splunk.com/en_us/blog/learn/what-splunk-does.html>. Acesso em: 16 de ago. 2023

SURICATA Open Information Security Foundation (OISF). Disponível em: <https://suricata.io>. Acesso em: 16 de ago. 2023

**Contatos:** mateus.iochimoto@gmail.com e charles.rodamilans@mackenzie.br