SIEM - Gestão e Análise de Eventos de Segurança nas Organizações **(Parte I)**

Mestrado de Cibersegurança e Informática Forense
UC: Gestão e Análise de Relatórios de Segurança
Docente: Beatriz Piedade

Pedro Marques
Escola Superior de Gestão e Tecnologia
Instituto Politécnico de Leiria
Leiria, Portugal
2220562@my.ipleiria.pt

Filipe Bagagem
Escola Superior de Gestão e Tecnologia
Instituto Politécnico de Leiria
Leiria, Portugal
2220558@my.ipleiria.pt

***Abstract*— As SIEM's são responsáveis por recolher dados relevantes à segurança da informação, de forma centralizada para detetar ameaças ou incidentes. Este fornece recursos de análise de segurança em tempo real ou o histórico de eventos passados, correlacionando vários eventos de log.**

Keywords—SIEM, logs, incidents, segurança, análise, ataques

I. INTRODUÇÃO E ENQUADRAMENTO

Uma plataforma de gestão de informações e eventos de segurança (SIEM) é uma solução abrangente de segurança cibernética projetada para recolher, analisar e gerir dados de eventos de segurança de várias fontes na rede de uma organização.

O SIEM combina a gestão de informações de segurança (SIM) e a gestão de eventos de segurança (SEM) num único sistema de gestão de segurança.

As plataformas SIEM oferecem uma visão centralizada dos eventos de segurança, agregando dados de vários sistemas, como "firewalls", sistemas de deteção de intrusão, servidores entre outros equipamentos. Essa abordagem holística permite que as equipas de segurança detetem e respondam aos incidentes de segurança com eficácia. As plataformas SIEM utilizam análise avançada, "machine learning" e técnicas de correlação para identificar padrões, anomalias e potenciais ameaças, permitindo que a equipa de segurança priorize e investigue incidentes com eficiência. Os principais recursos de uma plataforma SIEM incluem gestão de "logs", correlação de eventos, monitorização em tempo real, integração de inteligência de ameaças e automação de resposta a incidentes. A gestão de log envolve recolher, armazenar e indexar "logs" de várias fontes, permitindo que as equipas de segurança pesquisem e analisem os dados facilmente. A correlação de eventos ajuda a identificar relacionamentos e dependências entre diferentes eventos, fornecendo uma compreensão mais abrangente do cenário de segurança. A monitorização em tempo real permite que as equipas de segurança detetem e respondam a incidentes de segurança à medida que ocorrem, reduzindo o impacto de possíveis ameaças. A integração de inteligência de ameaças enriquece os dados de eventos de segurança com "feeds" de ameaças externas, permitindo que as organizações se mantenham atualizadas sobre as mais recentes ameaças e vulnerabilidades conhecidas. A automação de resposta a incidentes ajuda a simplificar e acelerar o processo de resposta a incidentes, garantindo uma ação rápida e minimizando possíveis danos. As plataformas SIEM desempenham um papel crucial na estratégia de segurança de uma organização, fornecendo insights acionáveis, deteção rápida de incidentes e recursos de resposta eficazes. Aproveitando o poder da análise e automações avançadas, estas plataformas permitem que as equipas de segurança se defendam proativamente contra ameaças cibernéticas sofisticadas e protejam ativos críticos. Em resumo, as plataformas SIEM são ferramentas essenciais no cenário de segurança cibernética complexo e presentemente em constante evolução. Elas capacitam as organizações para gerir eventos de segurança, identificar ameaças em tempo real e responder rapidamente para mitigar potenciais riscos. Ao adotar uma plataforma SIEM, as organizações podem melhorar significativamente a sua resiliência geral de segurança e proteger os seus ativos digitais contra ameaças cibernéticas que são cada vez mais sofisticadas.

II. VANTAGENS E DESVANTAGENS EM UTILIZAR UMA SOLUÇÃO SIEM

As ferramentas de SIEM oferecem muitos benefícios que podem ajudar a reforçar a postura de segurança da organização, incluindo:

- Uma vista centralizada de potenciais ameaças
- Identificação e resposta a ameaças em tempo real
- Informações avançadas sobre ameaças
- Auditorias e relatórios de conformidade regulamentares
- Maior transparência de monitorização de utilizadores, aplicações e dispositivos

Desvantagens

- Os custos de implementação e manutenção podem ser significativos;

- O SIEM pode exigir uma equipa especializada para operar de forma eficaz;
- Os falsos alarmes podem causar uma sobrecarga desnecessária para a equipa de segurança.

A. Como implementar uma solução de SIEM

Organizações de todas as dimensões utilizam ou podem utilizar soluções de SIEM para mitigar os riscos de cibersegurança e cumprir as normas regulamentares em conformidade.

As boas práticas de implementação de um sistema de SIEM incluem:

- Definir muito bem os requisitos antes de implementar o SIEM
- Realizar muitos testes para minimizar os falsos alarmes
- Recolher dados relevantes para análise
- Documentar todos os processos e procedimentos
- Elaborar um plano de resposta a incidentes
- Melhorar/afinar continuamente o SIEM

B. Evolução dos SIEM's

Os sistemas de SIEM evoluíram ao longo do tempo para se tornarem soluções mais avançadas e integradas, capazes de lidar com os crescentes volumes de dados e as ameaças de segurança cada vez mais sofisticadas. As primeiras soluções de SIEM surgiram na década 90, em que o foco principal era recolher e analisar logs de sistemas e dispositivos de rede.

Uma década depois (2000), as soluções de SIEM começaram a incorporar recursos avançados de análise de segurança, como deteção de intrusões, correlação de eventos e análise comportamental dos utilizadores. Mais recentemente as soluções passaram a incluir tecnologias de machine learning e inteligência artificial, permitindo uma deteção e mitigação mais eficaz de ameaças.

C. Arquitetura dos SIEM's

A arquitetura dos sistemas de SIEM também evoluiu para suportar a integração com outras soluções de segurança, tanto de fornecedores internos como externos, criando um ecossistema de segurança mais completo e integrado. A infraestrutura da solução de SIEM geralmente consiste em três principais componentes:

- **Recolha de dados:** dispositivos responsáveis por recolher dados brutos de várias fontes, como logs de sistemas, tráfego de rede e dados de aplicações.
- **Armazenamento de dados:** uma infraestrutura de armazenamento dedicada para arquivar e analisar os dados recolhidos.
- **Motor de análise:** aplicar as tecnologias de machine learning e inteligência artificial sobre os dados recolhidos, permitindo a correlação de dados de diferentes fontes para detetar ameaças de segurança em tempo real.

D. Perspetivas Futuras

Com toda a certeza, a (IA) Inteligência Artificial terá um papel preponderante nas soluções SIEM. Algumas das perspetivas futuras para um SIEM:

- Integração com outras soluções de segurança: Alargar o leque de soluções com integração de diferentes fornecedores, criando uma rede integrada de proteção para a organização.
- Melhorias na inteligência artificial: Com a evolução da IA, é provável que os sistemas SIEM evoluam para fornecer análises e soluções ainda mais precisas e avançadas.
- Maior automação: O aumento da automação permitirá que as soluções SIEM identifiquem e resolvam ameaças automaticamente, sem a necessidade de uma intervenção humana constante.
- Integração com análise de Big Data: Com a quantidade de dados gerados a cada minuto, os provedores de soluções SIEM podem começar a integrar soluções de análise de Big Data para melhorar a inteligência de segurança das soluções.

O futuro dos sistemas SIEM será promissor e ao mesmo tempo muito exigente.

III. SISTEMAS DE SIEM DISPONÍVEIS NO MERCADO

Existem vários sistemas de SIEM disponíveis no mercado, cada um com as suas próprias características e recursos, bem como vantagens e desvantagens.

Alguns dos mais populares incluem:

- Splunk
- IBM Qradar
- LogRhythm
- ArcSight
- McAfee Enterprise Security Manager
- AlienVault USM
- Elasticsearch
- Graylog
- Sumo Logic
- Securonix

Neste tipo de solução é importante avaliar cuidadosamente as necessidades da organização antes de escolher uma solução SIEM. Algumas das características importantes a serem consideradas incluem capacidade de análise de dados em tempo real, integração com outros sistemas de segurança e a capacidades de gerar relatórios.

As duas soluções que selecionámos para análise no âmbito do presente trabalho foram **Security Onion** e **OSSIM** (Open Source Security Information and Event Management).

IV. SIEM's SELECIONADOS

A. *SECURITY ONION*

O **Security Onion** é uma das distribuições mais populares disponíveis para construir um ambiente de segurança de rede. Ele contém ferramentas como Playbook, FleetDM, osquery, CyberChef, Elasticsearch, Logstash, Kibana, Suricata, Zeek, and Wazuh, o que o torna uma excelente escolha para analistas de segurança que querem detetar, analisar e monitorizar incidentes nas infraestruturas de rede à procura de atividades suspeitas e possíveis violações de segurança. [1]

Especificamente, o Security Onion é composto pelos seguintes componentes:

- **Sistema operativo:** O Security Onion é baseado no sistema operativo Ubuntu (Linux), que é altamente confiável e seguro.
- **Snort**: O Snort é um sistema de deteção de intrusos baseado em regras que monitoriza o tráfego de rede à procura de atividades suspeitas. O Snort é uma das principais ferramentas de segurança usadas no Security Onion.
- **Zeek**: O Zeek é um sistema de deteção de incidentes baseado em protocolos que monitoriza o tráfego de rede para detetar possíveis violações de segurança. O Zeek é complementar ao Snort e, juntos, tornam o Security Onion um poderoso sistema de deteção de incidentes.
- **Suricata**: O Suricata é outro sistema de deteção de incidentes que monitoriza o tráfego de rede e é capaz de detetar possíveis ameaças baseadas em comportamentos de rede.
- **Elasticsearch**: O Elasticsearch é um mecanismo de procura e análise de dados de código aberto que ajuda a indexar, analisar e pesquisar dados coletados pelo Security Onion.
- **Logstash**: O Logstash é uma ferramenta de processamento de dados que ajuda a centralizar, analisar e armazenar logs de várias fontes de dados.
- **Kibana**: O Kibana é uma interface de utilizador gráfica para analisar e visualizar dados coletados pelo Security Onion. Ele é utilizado para criar gráficos e visualizações personalizados para facilitar a compreensão dos dados.

Vantagens:

- Totalmente gratuito e de código aberto.
- Interfaces fáceis de utilizar e personalizar.
- Integração fácil com outros softwares de segurança.
- Excelente suporte para pesquisa e investigação forense.
- Capacidade de monitorizar vários tipos de logs e fontes de dados, como firewalls, IDS, servidores e aplicativos de rede.
- Inclui um conjunto completo de ferramentas de segurança, incluindo deteção de ameaças, análise comportamental e gestão de vulnerabilidades.

Desvantagens:

- Requer um conhecimento técnico avançado para configurar e gerir corretamente a solução.
- Pode consumir muitos recursos do sistema, especialmente em redes maiores com muitos dispositivos a gerar informação.
- Algum tempo para aprender a utilizar todas as suas funcionalidades e recursos.
- Pode gerar muitos falsos positivos caso não seja configurado corretamente.
- Tratando-se de um projeto de código aberto, mantido por uma comunidade, a qualidade do suporte técnico pode não ser a melhor.

B. *ALIEN VAULT OSSIM*

O SIEM (Security Information and Event Management) OSSIM (Open Source Security Information and Event Management) é um software de código aberto que fornece informações de segurança e recursos de gestão de eventos para monitorizar e analisar dados relacionados com a segurança em tempo real. Ele foi projetado para recolher, analisar e correlacionar dados de várias fontes, como dispositivos de segurança, servidores e infraestrutura de rede. [2]

O OSSIM SIEM fornece uma variedade de recursos, incluindo recolha de logs, correlação de eventos, descoberta de ativos, avaliação de vulnerabilidade e resposta a incidentes. Ele utiliza uma grande variedade de técnicas de análise de dados, como deteção baseada em assinatura, deteção de anomalias e análise comportamental para identificar possíveis ameaças à segurança.

O OSSIM SIEM é uma ferramenta poderosa para organizações que procuram melhorar a sua infraestrutura de segurança obtendo melhor visibilidade no seu ambiente de TI. Esta ferramenta pode ajudar as organizações a detetar e responder a incidentes de segurança mais rapidamente, reduzir o risco de violações de dados e garantir a conformidade com as diretivas. Além disso, por ser de código aberto, o OSSIM SIEM pode ser personalizado e estendido para atender a necessidades organizacionais específicas.

O OSSIM SIEM é composto por vários módulos que trabalham juntos para fornecer informações de segurança abrangentes e recursos de gestão de eventos. Esses módulos incluem:

Fontes de dados: Este módulo é responsável por recolher dados de segurança de várias fontes, incluindo dispositivos de segurança, servidores e infraestrutura de rede.

Processamento de dados: Este módulo é responsável por processar e normalizar os dados recolhidos, garantindo que estejam num formato que possa ser analisado e correlacionado.

Mecanismo de análise: Este módulo é responsável por analisar os dados processados e gerar alertas quando são detetadas possíveis ameaças à segurança.

Mecanismo de correlação: Este módulo é responsável por correlacionar eventos de segurança em várias fontes de dados, permitindo identificar ameaças de segurança mais complexas.

Relatórios: Este módulo é responsável por gerar relatórios e dashboards que fornecem informações sobre a postura de segurança de uma organização.

Resposta a incidentes: Este módulo é responsável por automatizar os processos de resposta a incidentes, permitindo que as organizações respondam rapidamente a incidentes de segurança.

No geral, esses módulos trabalham juntos para fornecer às organizações uma visão centralizada e em tempo real da sua postura de segurança, permitindo que detetem e respondam às ameaças de segurança com mais eficiência.

Arquitetura OSSIM

A arquitetura OSSIM SIEM é baseada em um modelo cliente-servidor, onde o servidor OSSIM realiza a maior parte do processamento e análise, enquanto o agente OSSIM é instalado nos dispositivos a monitorizar para recolher e encaminhar dados de segurança para o servidor. O servidor pode ser implantado localmente ou na cloud e pode ser acedido através de uma interface baseada na web.

O servidor é composto por vários módulos, incluindo o módulo de fontes de dados, módulo de processamento de dados, mecanismo de análise, mecanismo de correlação, módulo de relatórios e módulo de resposta a incidentes. Esses módulos trabalham juntos para fornecer informações de segurança abrangentes e recursos de gestão de eventos.

A interface cliente fornece acesso ao servidor, permitindo que os utilizadores visualizem eventos de segurança, analisem dados, gerem relatórios e gerenciem incidentes. Além disso, a interface do cliente fornece acesso a uma variedade de opções de configuração, permitindo que os utilizadores personalizem o sistema para atender às suas necessidades específicas.

No geral, a arquitetura OSSIM SIEM foi projetada para ser escalável, flexível e personalizável, fornecendo às organizações uma ferramenta poderosa para melhorar sua postura de segurança.

Vantagens:

- **Código aberto:** OSSIM SIEM é uma solução de código aberto, o que significa que seu uso é gratuito e pode ser personalizado para atender a necessidades organizacionais específicas.
- **Monitorização centralizada:** Com o OSSIM SIEM, as organizações podem recolher e analisar dados de segurança de várias fontes de forma centralizada, fornecendo uma visão única da postura de segurança da organização.
- **Deteção de ameaças em tempo real:** o OSSIM SIEM usa uma variedade de técnicas de análise de dados para detetar possíveis ameaças à segurança em tempo real, permitindo que as organizações respondam rapidamente aos incidentes.
- **Recursos de segurança abrangentes:** OSSIM SIEM inclui uma variedade de recursos de segurança, como recolha de logs, correlação de eventos, descoberta de ativos, avaliação de vulnerabilidades e resposta a incidentes.
- **Conformidade:** O OSSIM SIEM pode ajudar as organizações a cumprir os regulamentos do setor.

Desvantagens:

- **Implementação complexa**: A implementação e configuração do OSSIM SIEM pode ser complexa e demorada, exigindo um alto nível de conhecimento técnico.
- **Suporte limitado**: Como o OSSIM SIEM é uma solução de código aberto, o suporte geralmente é fornecido pela comunidade, que pode não ser tão abrangente quanto as soluções comerciais.
- **Escalabilidade**: OSSIM SIEM pode não ser tão escalável quanto as soluções comerciais, tornando-o menos adequado para organizações maiores com ambientes de TI complexos.
- **Altos falsos positivos**: OSSIM SIEM pode gerar um alto número de alertas falsos positivos, que podem levar muito tempo para serem investigados e resolvidos.
- **Manutenção**: OSSIM SIEM requer manutenção contínua, incluindo atualizações de software, correções de bugs e alterações de configuração, que podem consumir muito tempo e exigir uma equipa de TI dedicada.

O OSSIM SIEM pode ser integrado a uma ampla variedade de dispositivos e tecnologias de segurança para fornecer recursos abrangentes de monitorização e análise de segurança. Algumas integrações comuns incluem:

- **Dispositivos de segurança:** O OSSIM SIEM pode ser integrado com uma grande variedade de dispositivos de segurança, como firewalls, sistemas de deteção de intrusão e software antivírus, para recolha de dados de segurança e gerar alertas.
- **Scanners de vulnerabilidade:** O OSSIM SIEM pode ser integrado com scanners de vulnerabilidade, como Nessus e OpenVAS, para identificar e priorizar vulnerabilidades no ambiente de TI.

- **Sistemas de gerenciamento de log**: O OSSIM SIEM pode ser integrado com sistemas de gestão de logs, como o syslog-ng, para recolher e analisar dados de log de várias fontes.
- **Sistemas de tickets:** O OSSIM SIEM pode ser integrado a sistemas de tickets, como JIRA e ServiceNow, para automatizar os processos de resposta a incidentes.
- **Feeds de inteligência de ameaças:** o OSSIM SIEM pode ser integrado com feeds de inteligência de ameaças, como Open Threat Exchange (OTX) e AlienVault Labs, para aprimorar os seus recursos de deteção de ameaças.
- **Plataformas Cloud:** O OSSIM SIEM pode ser integrado com plataformas cloud, como Amazon Web Services (AWS) e Microsoft Azure, para monitorizar e analisar dados de segurança em ambientes cloud.

O OSSIM SIEM tem a capacidade de se integrar a uma ampla variedade de tecnologias permite que ele forneça recursos abrangentes de monitorização e análise de segurança para organizações de todos os tamanhos.

V. SELEÇÃO DO SISTEMA DE SIEM

Optámos pela escolha do **Security Onion** pelas seguintes razões:

- **Open Source** - O Security Onion é baseado em software livre, o que significa que ele pode ser descarregado e utilizado gratuitamente.
- **Conjunto de ferramentas** - O Security Onion inclui um conjunto completo de ferramentas para a monitorização de segurança, análise de log, deteção de anomalias e resposta a incidentes.
- **Integração com outras ferramentas** - O Security Onion é compatível com uma grande variedade de outras ferramentas de segurança, incluindo IDS / IPS, firewalls, proxys e gestores de logs.
- **Escalabilidade** - O Security Onion pode ser dimensionado para responder às necessidades de qualquer empresa, independentemente do tamanho da empresa. A solução suporta a recolha e análise de dados de segurança em tempo real de grandes volumes de dados.
- **Fácil de utilizar** - O Security Onion é fácil de instalar, configurar e usar. Isto significa que pequenas e médias empresas podem implementar o Security Onion com pouco esforço quando comparado com outras soluções.
- **Comunidade ativa** - O Security Onion tem uma grande comunidade de utilizadores e programadores que estão constantemente a melhorar a solução. Isto garante que o Security Onion se encontre atualizado com as últimas tendências de segurança.

VI. INFRAESTRUTURA TECNOLÓGICA A UTILIZAR

Para utilizar Security Onion, é necessário ter uma infraestrutura tecnológica adequada, que inclui:

Hardware:

Servidor com processador de 64 bits, de preferência multi-core (quad-core ou superior) e suporte para a virtualização

Mínimo de 8 GB de memória RAM (recomenda-se 16 GB ou mais)

Disco rígido com no mínimo 500 GB de espaço livre para os logs e armazenamento de pacotes capturados

Software:

Sistema operacional Ubuntu 18.04 LTS (ou superior)

VirtualBox, VMware ou outro software de virtualização compatível com o Ubuntu

Rede:

Rede dedicada para o tráfego de pacotes de dados a ser analisado

Router com capacidade de espelhamento de portas para a captura de pacotes

Serviço DHCP para atribuir automaticamente endereços IP aos dispositivos que serão monitorizados

Ligação à internet:

Ligação de alta velocidade (recomenda-se no mínimo 10 Mbps) para atualizar as ferramentas e bibliotecas do SO e do Security Onion

Endereço IP público para acesso remoto, através de uma VPN.

Tendo em conta os requisitos recomendados, a nossa proposta para a implementação do Security Onion para a segunda fase do trabalho, está ilustrado na figura 1.

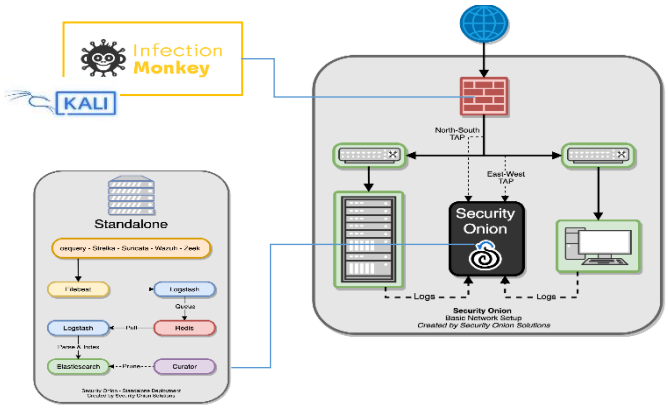

Figura 1 - Cenário a implementar

A implementação consiste na instalação de uma infraestrutura baseada em servidores virtuais que compreende um servidor santadalone "Security Onion", um servidor baseado em Windows Server com Serviços Web (IIS Server), um router com ligação à internet, um switch/hub e uma máquina baseada em Kali Linux com o Infection Monkey a

gerar simulações de ataques para conseguirmos gerar tráfego e recolher logs válidos como ameaças.

I. Conclusão

Em conclusão, uma plataforma de gestão de informações e eventos de segurança (SIEM) é um componente vital da infraestrutura de segurança de uma organização. Ela fornece uma visão centralizada e holística dos eventos de segurança, permitindo que as equipas de segurança monitorizem, detetem e respondam às ameaças de forma eficaz. Ao alavancar análises avançadas, "machine learning" e automação, as plataformas SIEM permitem que as organizações fiquem à frente das ameaças cibernéticas e protejam os seus ativos valiosos. Com a crescente complexidade e frequência das ameaças cibernéticas, as organizações não podem confiar apenas nas medidas de segurança tradicionais. As plataformas SIEM fornecem uma abordagem mais abrangente ao nível da segurança dos sistemas, recolhendo e analisando dados de várias fontes, permitindo a identifação de padrões e anomalias que podem indicar possíveis ameaças. Além disso, as plataformas SIEM facilitam a conformidade com os requisitos regulamentares, fornecendo recursos detalhados de registo, auditoria e geração de relatórios. Eles ajudam as organizações a atender às exigências dos regulamentos e padrões do setor, como o Regulamento Geral de Proteção de Dados (RGPD). Ao investir numa plataforma SIEM, as organizações podem fortalecer a sua postura de segurança, melhorar os tempos de resposta a incidentes e minimizar o impacto potencial de violações de segurança. Essas plataformas fornecem as ferramentas e informações necessárias para aprimorar a deteção de ameaças, a investigação de incidentes e a coordenação de respostas, resultando num ambiente mais resiliente e seguro. Num mundo onde as ameaças cibernéticas continuam a evoluir, as organizações precisam de soluções robustas e avançadas para proteger seus dados e sistemas críticos. As plataformas SIEM oferecem a tecnologia e os recursos necessários para ficar à frente dos cibercriminosos, permitindo que as organizações protejam sua reputação, confiança do cliente e continuidade dos negócios. A adoção de uma plataforma SIEM é um passo proativo em direção à segurança cibernética abrangente e tranquilidade num mundo cada vez mais interligado.

O Security Onion e o AlienVault OSSIM são soluções populares de segurança de código aberto que fornecem recursos de gestão de eventos e informações de segurança (SIEM). No entanto, existem algumas diferenças importantes entre eles, na arquitetura, O Security Onion é focado principalmente na monitorização e análise de segurança de rede. Ele é baseado no sistema operativo Ubuntu e combina várias ferramentas de código aberto, incluindo Elasticsearch, Logstash, Kibana e Suricata, para fornecer visibilidade de rede abrangente e deteção de ameaças. Por outro lado, o AlienVault OSSIM é uma solução mais completa que inclui monitorização de segurança de rede, deteção de intrusão baseada em host, avaliação de vulnerabilidade e gerenciamento de logs. Ele utiliza a sua própria plataforma AlienVault USM unificada, que inclui componentes proprietários. Na facilidade de utilização, o Security Onion requer algum conhecimento técnico para instalar e configurar devido à sua arquitetura modular e integração de várias ferramentas. É adequado para profissionais de segurança ou organizações com equipas de segurança dedicadas. O AlienVault OSSIM, por outro lado, visa fornecer uma experiência mais amigável ao oferecer uma interface unificada e controlos de segurança pré-configurados. Ele foi projetado para ser mais acessível a utilizadores com menos experiência técnica. No suporte à comunidade, tanto o Security Onion quanto o AlienVault OSSIM têm comunidades de utilizadores ativas e fóruns de suporte. No entanto, o Security Onion tem uma comunidade maior e mais estabelecida com uma maior riqueza de documentação, tutoriais e conteúdo de contribuição da comunidade. Isso pode ser útil para solucionar problemas e obter assistência para problemas específicos. No âmbito dos recursos e capacidades, embora ambas as soluções ofereçam funcionalidades básicas de SIEM, como gestão de logs, correlação de eventos e deteção de ameaças, há diferenças nos recursos específicos que elas fornecem. O Security Onion destaca-se na monitorização de segurança de rede, oferecendo recursos robustos de captura e análise de pacotes. Ele permite a integração com sistemas de deteção de intrusão de código aberto, como o Suricata e o Snort.

O AlienVault OSSIM, por outro lado, oferece uma gama mais ampla de recursos, incluindo avaliação de vulnerabilidade, descoberta de ativos e deteção de intrusão baseada em host.

Em última análise, a escolha entre o Security Onion e o AlienVault OSSIM depende das necessidades e preferências específicas da organização. O Security Onion é adequado para monitorização de segurança com foco em rede, enquanto o AlienVault OSSIM oferece um conjunto mais abrangente de recursos de segurança.

Considerar fatores como experiência técnica, recursos desejados e o nível de suporte da comunidade pode ajudar a tomar uma decisão.

II. Referências

[1] S. Onion, "securityonion.net," [Online]. Available: https://docs.securityonion.net/en/2.3/.

[2] alienvault, "alienvault.com," [Online]. Available: https://success.alienvault.com/s/topic/0TO0Z000000oRS3WAM/ossim.