

SOC OPEN SOURCE

<https://www.linkedin.com/in/joas-antonio-dos-santos>

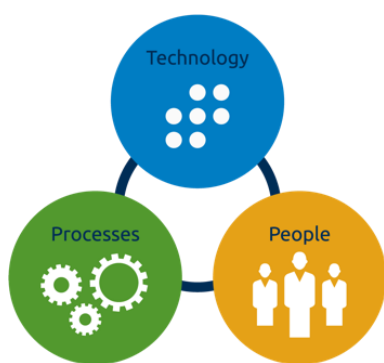
SOC

Um centro de operações de segurança (SOC) é responsável por realizar a detecção de ataques e ameaças, analisar os ataques e as ameaças, avaliar seus impactos e responder aos incidentes de segurança. Sua estrutura se baseia em três funções principais: Pessoas, Processos e Tecnologia.



Pessoas

As pessoas são um fator principal dentro de um SOC, sendo um profissional de resposta a incidentes ou um Analista de Segurança. Um profissional que responde a incidentes tem como responsabilidade a realização de uma análise detalhada de eventos maliciosos utilizando análise de pesquisa, inteligência de ameaças, ferramentas de análise de malware e técnicas forenses. Enquanto um analista de segurança coleta dados de eventos de segurança, dados de log de máquinas, logs de rede e análise de risco para determinar um impacto de uma ameaça.



Processos

Para tornar o SOC efetivo, é vital definir e documentar processos para que a execução possa ser assegurada de acordo com o plano documentado. O processo garante a sincronização e a execução oportuna de diferentes eventos e atividades executadas pelo SOC. É por meio de processos que será delegado as responsabilidades de funções atreladas a um SOC para um analista de segurança e um profissional de resposta a incidentes com o objetivo de alcançar os melhores resultados.

Tecnologia

As tecnologias garantem que o SOC possuirá ferramentas e controles para realizar o monitoramento de ambientes críticos, análises de risco e resposta a incidentes, para evitar grandes impactos.

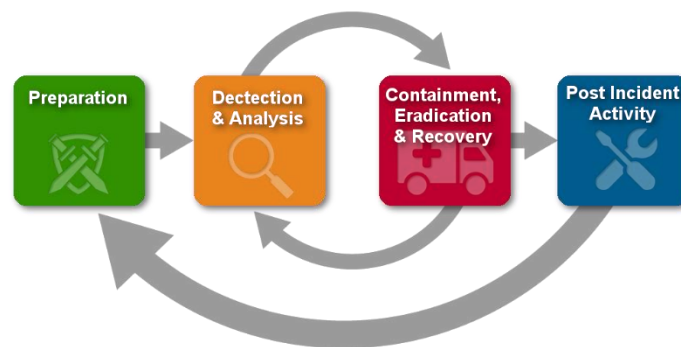
Com base nessas três funções, vamos possuir:

- **Monitoramento de segurança:** implementação e desenvolvimento de regras de detecção, análise de eventos e incidentes de segurança.
- **Threat Hunting:** Pesquisa ativa de novas ameaças e anomalias suspeitas sobre eventos coletados nas ferramentas de monitoramento.

- **Threat Intelligence:** Coletando informações sobre ameaças e as suas motivações em fontes externas e de maneira comunitária com outras organizações.
- **Cyber Brand Protection:** Monitoramento de fontes de informações externas com o objetivo de detectar vazamentos de dados confidenciais de pacientes e funcionários (dados de login, documentos internos etc).
- **Resposta a Incidente:** Recomendações sobre como proceder para solucionar incidentes de segurança e ajudar a lidar com eles.

Resposta a incidentes

A resposta a incidentes é um conjunto de metodologias que visam conter e minimizar os impactos de um incidente cibernético, sejam fruto de um ataque, mal uso, ou mesmo um desastre de grandes proporções. O objetivo é lidar com a situação de maneira a limitar os danos e reduzir o tempo e os custos de recuperação.



NIST: Ciclo de vida de resposta a incidente

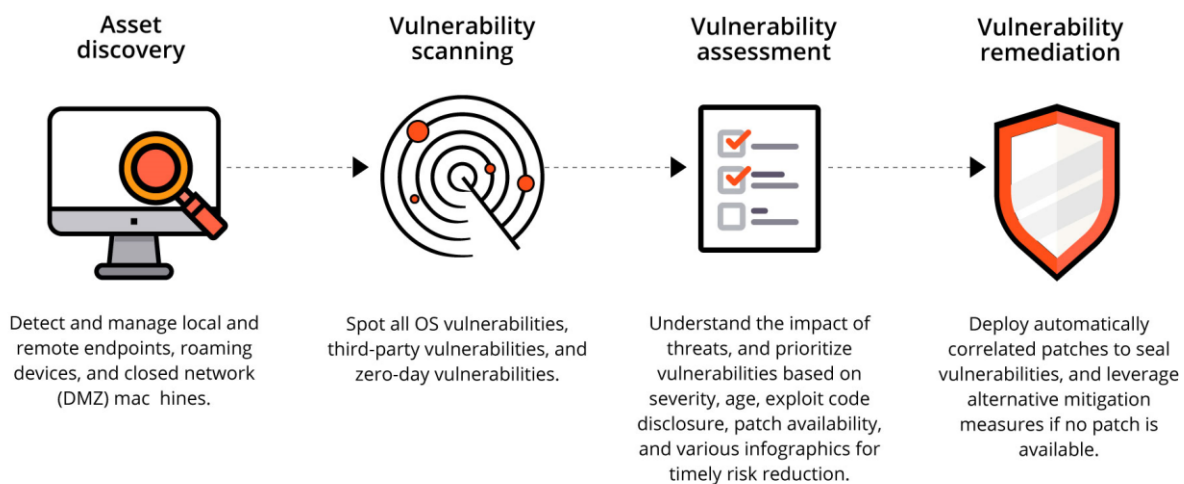
- **Preparação:** Estudo constante de novas ameaças e metodologias, treinamento constante de especialistas, implementação e operação de tecnologias que nos permitam atuar. Coletando e monitorando indicadores para gerar relatórios analíticos e preditivos.
- **Identificação:** Triagem de indicadores de forma a quantificar, qualificar e classificar as ameaças identificadas.
- **Contenção:** Contenção das ameaças por meio do isolamento dos sistemas afetados para evitar danos adicionais e uma reação apropriada para cada ameaça.
- **Erradicação:** Eliminação ameaças identificadas bem como a localização das falhas expostas a estas ameaças.
- **Recuperação:** Restabelecimento dos sistemas afetados e dos recursos ameaçados.
- **Lições aprendidas:** Revisão e aprimoramento das bases de conhecimento para aprimorar a capacidade de resposta a futuros incidentes.

Uma das áreas emergentes de foco e investimento é o conceito de automação e solicitação de segurança. Esta assume uma importância crescente devido a várias tendências do setor.

- **Automação de segurança** - o uso da tecnologia da informação no lugar de processos manuais para resposta a incidentes cibernéticos e gerenciamento de eventos de segurança.
- **Orquestração de segurança** - uma integração de ferramentas de segurança e tecnologia de informações projetadas para otimizar processos e direcionar uma automação de segurança.

▪ Ameaças e Gestão de Vulnerabilidades

- O gerenciamento de ameaças e vulnerabilidades prioriza reforçar a segurança com avaliações e testes a procura de ameaças que possam impactar determinados ambientes. Realizando testes constantes dos mecanismos de defesa do SOC, além de testar a agilidade do time de segurança ao detectar uma ameaça e a eficiência do time de resposta a incidentes. E para que tenha um gerenciamento de vulnerabilidades adequado, os profissionais responsáveis vão lidar com:



- Realização de testes regulares de invasão.
- Observar uma programação consistente de correções.
- Conta para todos os ativos e redes de TI.
- Obtenha os feeds atuais de ameaças.
- Aprenda sobre as vulnerabilidades atuais e trabalhe para corrigi-las.
- Visualize dados para amplo entendimento.
- Verifique se as ferramentas adequadas são usadas.

Adicione cláusulas de correção nas políticas e procedimentos do provedor de serviços.

▪ Cyber Security Framework (CSF) – NIST

Desenvolver um SOC pensando nos principais Frameworks de mercado



▪ O framework de segurança cibernética NIST, também chamado em inglês de NIST Cyber Security Framework, fornece uma estrutura, com base nos padrões, diretrizes e práticas existentes para organizações do **setor privado**, a fim de gerenciar e reduzir melhor o risco de segurança cibernética. Além de ajudar as organizações a prevenir, detectar e responder a ameaças cibernéticas e ataques cibernéticos, ele foi projetado para melhorar as comunicações de segurança cibernética e gerenciamento de riscos entre as partes interessadas internas e externas.

▪ C2M2

▪ O programa Modelo de Maturidade em Cibersegurança (C2M2) é um esforço de parceria público-privada que estabelecido como resultado dos esforços da Administração para melhorar os recursos de cibersegurança no setor elétrico e se expandido para a saúde, a fim de entender a postura de cibersegurança da rede.



foi

▪ O modelo se concentra na implementação e gerenciamento de práticas de segurança cibernética associadas à operação e uso de ativos de tecnologia da informação e tecnologia operacional e aos ambientes em que eles operam. O objetivo é apoiar o desenvolvimento e a medição contínuos dos recursos de cibersegurança em qualquer organização.

▪ LGPD e GDPR

A Lei Geral de Proteção de dados (BR) e o Regulamento Geral sobre Proteção de Dados (UE),

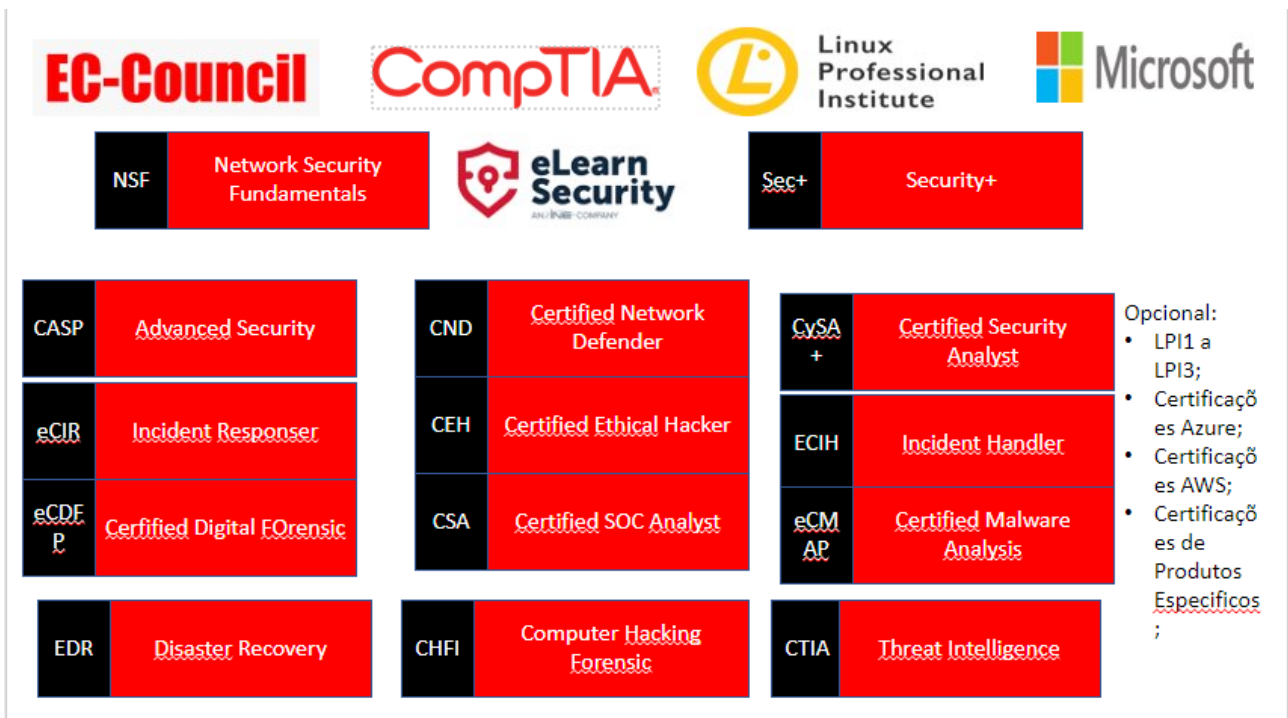


refere-se ao Tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Incluindo dados sensíveis referentes a saúde.

▪ Núcleo Acadêmico

▪ Treinamentos

Um programa de treinamento e com o objetivo de conferir aos profissionais das áreas para desenvolver suas habilidades na área de segurança da informação. Veja uma estrutura de certificações:



■ Machine Learning and Artificial Intelligence

Os volumes massivos e crescentes de dados desses dispositivos nos últimos anos tornaram cada vez mais difícil para as equipes de operações de segurança (SecOps) detectar, fazer a triagem, priorizar e responder às ameaças, resultando em maior exposição a riscos. Os sistemas tradicionais de gerenciamento de eventos e informações de segurança (SIEM) e outros mecanismos de alerta que usam regras e limites estáticos, embora eficazes contra ameaças conhecidas, enfrentaram desafios com ataques novos, baixos e direcionados.

A tendência para a rápida montagem de dados de alerta aumentou a necessidade de uma maneira automatizada para as organizações filtrarem rapidamente e identificarem ameaças profundamente ocultas. Isso precisa acontecer usando regras estáticas e procurando desvios do comportamento normal no tráfego.

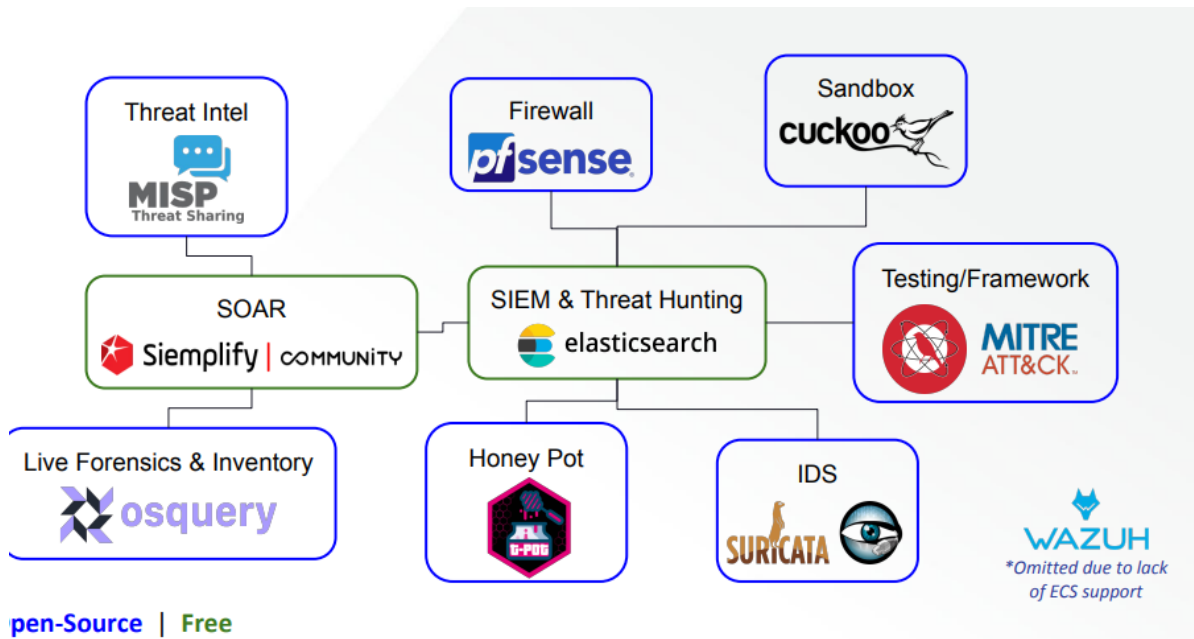
Alguns modelos de ML são "supervisionados", enquanto outros são "não supervisionados". O ML supervisionado envolve aprender por exemplo a partir de um conjunto de dados existente e depois aplicar esse conhecimento a novos dados. Por exemplo, ao analisar dados associados a tráfego de malware conhecido, uma ferramenta de ML supervisionada aprende como o tráfego se desvia do normal para que possa reconhecer o mesmo padrão em novos dados sem ser explicitamente programado.

Uma ferramenta de ML não supervisionada funciona observando o tráfego durante um período de tempo, aprendendo como é o comportamento "normal" na rede e investigando desvios dessa linha de base. O ML sem supervisão "realmente mostra seu poder" quando se trata de encontrar ameaças internas, ameaças persistentes avançadas e outros ataques direcionados, disse Daigle.

O ML não supervisionado não depende de regras e limites, mas aprende contínua e automaticamente com base nos padrões dos dados e em escala. Isso significa que ele pode criar uma linha de base para o comportamento "normal" de cada entidade em uma organização, em vez de aplicar a mesma linha de base a todas.

O principal caso de uso do ML na detecção de ameaças é para a identificação automática de atividades que se desviam de uma linha de base. As estimativas atuais da demanda por produtos habilitados para ML e inteligência artificial para enfrentar os desafios da segurança cibernética tendem a variar amplamente, mas a maioria aponta para um forte crescimento nos próximos anos.

▪ SOC Open Source



pen-Source | Free

Utilize Elastic Common Schema

- Combine registro, métricas e APM para adicionar maior observabilidade
- Alerta flexível em toda a pilha
- Links de reputação de IP - pesquisas personalizáveis
- 28 trabalhos de ML de detecção de anomalias focados em SIEM *
- 203 regras de detecção pré-construídas (mapeadas para MITER Att & Ck)
- Muitas visualizações pré-construídas

Beats Agents

Filebeat - File based logs & other data (has many modules)

Metricbeat - Metric (Infrastructure) data shipper

Packetbeat - Network data shipper

Winlogbeat - Windows Event Log data shipper

Auditbeat - Audit (Linux) data shipper

Heartbeat - Uptime Monitor

Functionbeat - Serverless shipper for Cloud data

MISP

- Plataforma de compartilhamento de informações sobre malware
- Plataforma de inteligência de ameaças de código aberto mantida pela CIRCL para armazenar, compartilhar, e colaborar em indicadores de segurança cibernética.
- Usa o protocolo de semáforo para classificação e compartilhamento
- Comunidades MISP
- O MISP tornará mais fácil para você compartilhar, mas também receber de pessoas confiáveis parceiros e grupos de confiança.
- Gerando regras Snort / Suricata / Bro / Zeek IDS, STIX, OpenIOC, texto ou csv exportações O MISP permite que você importe dados automaticamente em seus sistemas de detecção

Atomic Red Team

Atomic Red Team é uma biblioteca de testes simples que qualquer equipe de segurança pode executar para testar seus controles. Os testes são focados, têm poucas dependências e são definidos em um formato estruturado que pode ser usado por estruturas de automação.

Três crenças principais constituíram o estatuto da Equipe Vermelha Atômica:









As equipes precisam ser capazes de testar tudo, desde controles técnicos específicos até resultados. Nossas equipes de segurança não querem operar com uma atitude de “esperança e oração” em relação à detecção. Precisamos saber o que nossos controles e programas podem detectar e o que não podem. Não temos que detectar todos os adversários, mas acreditamos em conhecer nossos pontos cegos.

<https://atomicredteam.io/>

Devemos ser capazes de executar um teste em menos de cinco minutos. A maioria dos testes de segurança e ferramentas de automação levam muito tempo para instalar, configurar e executar. Criamos o termo "testes atômicos" porque sentimos que havia uma maneira simples de decompor os testes para que a maioria pudesse ser executada em alguns minutos.










O melhor teste é aquele que você realmente executa.

Precisamos continuar aprendendo como os adversários estão operando. A maioria das equipes de segurança não tem o benefício de ver uma grande variedade de tipos e técnicas de adversário cruzando sua mesa todos os dias. Mesmo nós da Red Canary só encontramos uma fração das técnicas possíveis sendo usadas, o que torna o trabalho conjunto da comunidade essencial para nos tornarmos melhores.

	SaaS	On-Premise	Open-Source
 PatrOwl	✓	✓	✓
 spiderfoot	✓	✓	✓
 kenna	✓	✗	✗
 NormShield	✓	✗	✗
 Greenbone Sustainable Resilience	✗	✓	✓
 Qualys	✓	✓	✗
 SecurityCenter SC	✗	✓	✗
 tenable .io	✓	✗	✗

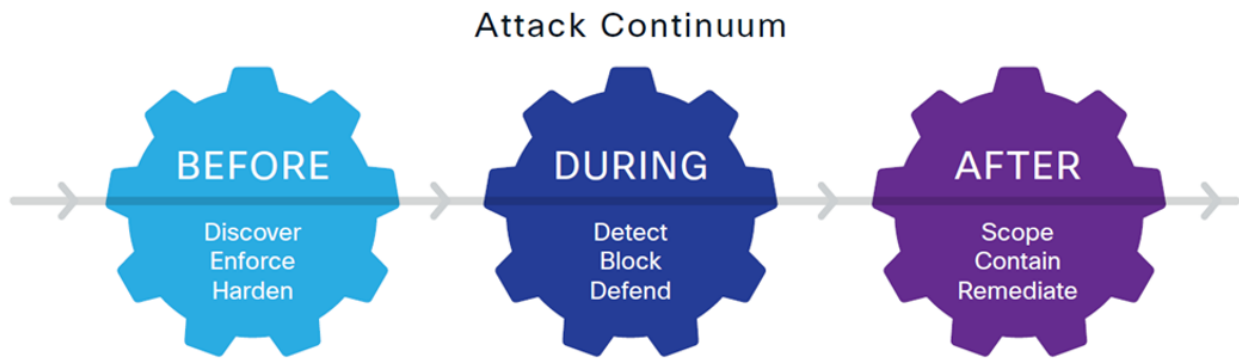
10 Best Free and Open-Source SIEM Tools

What You Need to Know

OSSIM		Offers both server-agent and serverless modes, with log analysis for mail servers, databases, and more.
Sagan		Real-time log analysis and correlation tool that's compatible with graphic consoles like Snorby and EveBox.
Splunk Free		Free version of Splunk tool that lets you index up to 500 MB daily for real-time data indexing and alerts.
Snort		Analyzes network traffic in real time, but features make it best-suited for experienced IT professionals.
Elasticsearch		Combine log search types and easily scan through large volumes of logs with this basic tool.
MozDef		A microservices-based tool that can integrate with third-party platforms for straightforward security insights.
ELK Stack		Combines Elasticsearch with tools like Kibana, Beats, and Logstash, for a fuller SIEM solution.
Wazuh		An on-premises tool that offers threat detection, incident response, and compliance support.
Apache Metron		Combines security operations center functions into one centralized, dynamic tool for catching threats.

- OSSIM
- OSSEC
- Sagan
- Splunk Free
- Snort
- Elasticsearch
- MozDef
- ELK Stack
- Wazuh
- Apache Metron

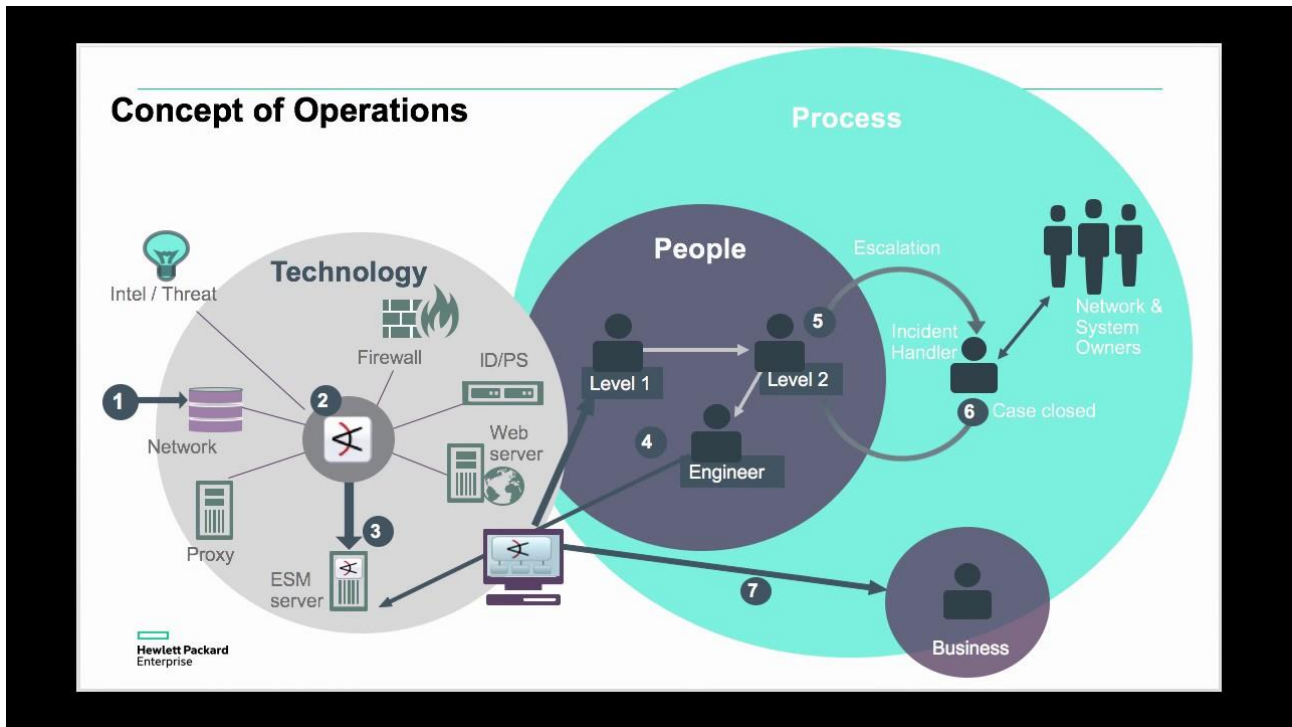
Exemplo: Design Security Operation Center



Firewall	VPN	NGIPS	Advanced Malware Protection
NGFW	UTM	Email Security	Network Behaviour Analysis
NAC & Identity Services		Web Security	Adv. Malware Sandboxing



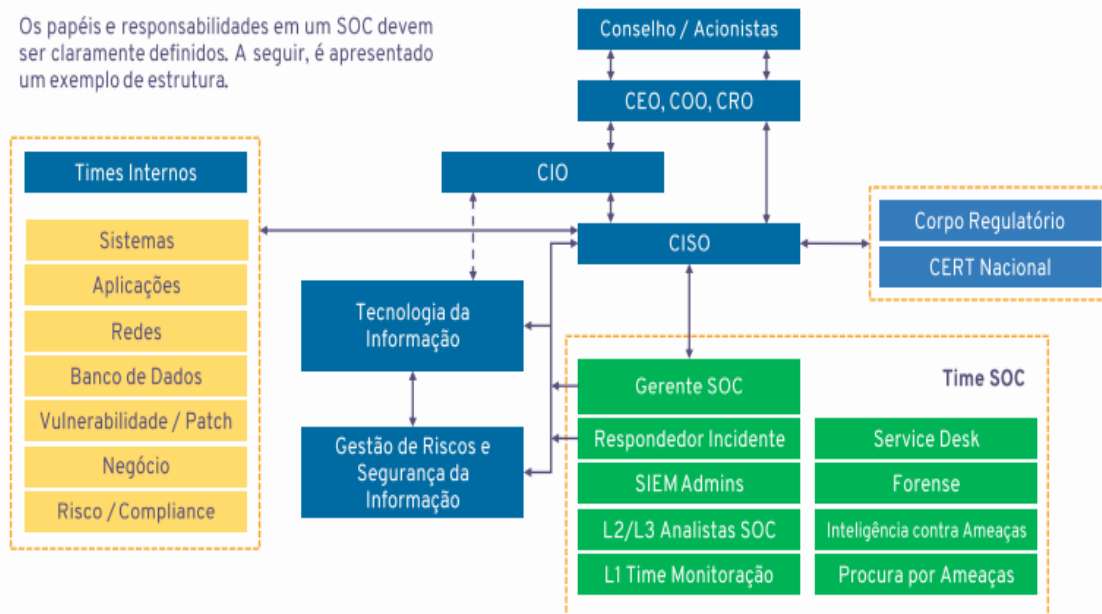
Conceitos da Operação



Exemplo: Estrutura e Funções

SOC Avançado: Estrutura e Funções

Os papéis e responsabilidades em um SOC devem ser claramente definidos. A seguir, é apresentado um exemplo de estrutura.



Exemplo: Ferramentas Open Sources para SOC

SIEM

Apache Metron: A estrutura Cisco Open SOC desenvolveu o Apache Metron. Como o SIEMonster, várias soluções de código aberto também estão conectadas em uma rede centralizada. O Apache Metron pode usar a linguagem JSON padrão para analisar e normalizar eventos de segurança para uma análise fácil. Além disso, podem ser emitidos avisos de segurança, enriquecimento de dados e rotulagem.

AlienVault OSSIM: A AT&T Cybersecurity fornece o AlienVault OSSIM, uma ferramenta de código aberto SIEM baseada em sua solução USM da AlienVault. O AlienVault OSSIM reúne muitos projetos de código aberto em um único pacote, próximo às entradas acima. O AlienVault OSSIM também permite o rastreamento e registro de aplicativos.

MozDef: Construído com o Mozilla para simplificar o tratamento de acidentes de segurança, o MozDef oferece escalabilidade e resiliência. MozDef fornecerá correlação de eventos e avisos de segurança com uma arquitetura baseada em microsserviços. Isso também pode ser incorporado com outros terceiros.

OSSEC: Tecnicamente, OSSEC é um sistema de detecção de intrusão de código aberto, em vez de uma solução SIEM. No entanto, ele ainda oferece um agente host para coleta de logs e um aplicativo central para processar esses logs. No geral, essa ferramenta monitora os arquivos de log e a integridade dos arquivos em busca de ataques cibernéticos em potencial. Ele pode realizar análises de log de vários serviços de rede e fornecer à sua equipe de TI inúmeras opções de alerta.

Wazuh: Na verdade, o Wazuh evoluiu de outra solução SIEM, a saber, OSSEC, de código aberto. No entanto, o Wazuh é uma opção especial para si agora. Isso facilita o armazenamento de dados baseado em agente e a recuperação de syslogs. O Wazuh também pode rastrear dispositivos facilmente no local. Possui uma interface web dedicada e diretrizes detalhadas para o controle rápido do administrador de TI.

Prelude OSS: Prelude OSS oferece a solução Prelude SIEM com uma versão de código aberto. Isso ajuda você a trabalhar com uma grande variedade de formatos de log e outros recursos. Ele também pode normalizar dados de eventos em uma linguagem comum, que pode oferecer suporte a outras ferramentas e soluções de segurança cibernética. O Prelude OSS também lucra com o crescimento contínuo, enquanto mantém a ameaça de inteligência atual.

Snort: Snort também oferece monitoramento de log como outro sistema de detecção de intrusão de código aberto; também realiza análises de tráfego de rede em tempo real para identificar possíveis perigos. O Snort também pode visualizar o tráfego ou fluxos de despejo de pacotes em um arquivo de log. Além disso, os plug-ins de saída podem ser usados para decidir como e onde o conjunto de dados é salvo.

Sagan: Sagan opera quase inteiramente como um fórum para o dispositivo SIEM Snort, que é complementar ao Sagan e segue os princípios do Snort. Sagan é leve e pode gravar em bancos de dados no snort. Pode ser outro recurso útil para quem gostaria de colaborar com o Snort.

ELK Stack: Existem produtos SIEM gratuitos na solução ELK Stack. Por exemplo, ELK pode compilar logs de quase todas as fontes de dados usando componentes Logstash embutidos. Portanto, esses dados de log podem ser combinados em uma ampla variedade de plug-ins, embora regras de segurança manuais sejam necessárias. ELK Stack também pode exibir dados com uma parte específica.

SIEMonster: SIEMonster fornece um SIEM grátis e uma solução paga. Como é o caso de muitas das soluções usadas, o framework SIEMonster oferece uma interface de gerenciamento de ferramenta centralizada para análise de dados, inteligência ameaçadora e vários softwares de código aberto. Sua organização o hospedará em uma nuvem, ao contrário de algumas outras soluções SIEM de código aberto.

IDS/IPS

Snort: Snort é a solução IDPS de código aberto mais conhecida para Windows e Unix, que fornece revisão de intrusos, monitoramento de pacotes e recursos completos de prevenção de intrusão em tempo real.

Suricata: Suricata é um IDPS e motor de controle de segurança de rede com uma rede de alto desempenho. Uma vez que é multi-threaded, a carga de processamento em um sensor é balanceada em uma instância.

OSSEC: Este sistema combina análise de log, gerenciamento de integridade de arquivo, rastreamento de registro do Windows, implementação central de política, identificação de rootkits, avisos em tempo real e resposta ativa.

Security Onion: Security Onion é uma ferramenta de detecção de intrusão de código aberto, sistema de proteção de monitoramento de rede e distribuição de gerenciamento de log para segurança corporativa no Linux.

Bro Network Security Monitor: Bro é uma plataforma de código aberto de segurança de rede que detalha a atividade da rede e pode ser usada em uma escala. Ele fornece um fórum robusto para análise de tráfego mais geral, que inclui identificação de incidentes, detecção de ameaças e monitoramento de seus recursos de segurança.

Vistumbler: Vistumbler é um scanner sem fio do Windows. O objetivo principal do Vistumbler é mapear e visualizar os pontos de acesso ao seu redor usando os dados sem fio e GPS coletados.

Smoothwall Express: Smoothwall Express é um firewall de código aberto que apresenta uma interface da Web fácil de usar e um sistema operacional Linux estável e separado. A funcionalidade envolve suporte a LAN, DMZ e rede sem fio, filtrando conteúdo em tempo real e filtrando HTTPS.

Untangle NG Firewall: NG Firewall é uma próxima geração de aplicativos de rede que monitoram simultaneamente o tráfego da rede. Esses aplicativos são conectados por uma GUI, banco de dados e relatórios crescentes.

ClamAV: ClamAV é uma estrutura de código aberto para varredura antivírus de gateway de e-mail e está disponível em aplicativos Windows, OS X, Linux e BSD.

Ferramenta de Resposta a Incidentes

Resposta rápida de GRR: a resposta rápida de GRR do Google consiste em duas partes: um cliente GRR implantado em uma rede investigada e um servidor GRR que auxilia os analistas na aplicação de ações e no processamento dos dados coletados.

Cyphon: Cyphon fornece recursos para capturar, processar, fazer a triagem e incidentes para analistas. Ele coleta dados, como logs de mensagens, APIs que enviam e-mail - o que torna mais fácil analisar e coletar quantos detalhes você quiser.

Volatility: volatilidade é um sistema de memória forense que ajuda analistas em despejos de memória a analisar e explorar informações.

SIFT (Sans Investigative Forensics Toolkit) Workstation: SIFT Workstation é um kit de ferramentas Ubuntu com todos os sistemas de análise necessários para conduzir um trabalho forense digital abrangente.

The Hive Project: O Hive Project é uma estrutura de IR de código aberto e gratuita que permite que muitos pesquisadores realizem investigações de incidentes ao mesmo tempo. Isso ajuda os analistas a produzir novas atualizações de atribuição de função e exibir eventos e avisos de várias fontes, incluindo alertas SIEM.

Ferramentas de Análise de Malware

Cuckoo Sandbox: Cuckoo Sandbox is a free malware analyse tool that automates the task of analyzing any malicious file under Windows, macOS, Linux, and Android.

YARA: YARA is the name of the main method used for the analysis and identification of malware. It offers a regulatory method for generating malware family definitions based on textual or binary patterns.

GRR: Google Rapid Response's goal is to provide rapidly scalable support to forensics and investigation, so analysis can be conducted remotely and analyzed promptly.

The REMnux: The REMnux project provides a lightweight, malicious software Linux distribution for malware analysts.

Bro: Bro is a free and open-source software network analysis framework.

Threat Intelligence Tools

MISP: MISP (Malware information sharing platform) is a threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information.

TIH: TIH (Threat-Intelligence-Hunter) is an intelligence tool that helps you in searching for IOCs across multiple openly available security feeds and some well-known APIs. The idea behind the tool is to facilitate searching and storing of frequently added IOCs for creating your own set of indicators.

QTek/QRadio: QRadio is a tool/framework designed to consolidate cyber threats intelligence sources. The goal of the project is to establish a robust modular framework for extraction of intelligence data from vetted sources.

Machinae Security Intelligence Collector: Machinae is a tool for collecting intelligence from public sites/feeds about various security-related pieces of data: IP addresses, domain names, URLs, email addresses, file hashes and SSL fingerprints.

SOCRadar Community Edition: SOCRadar is a unified threat intelligence platform that tracks changes and risks on your digital assets, provides proactive protection to companies and provides information about attacks in the cyber world.

Web Application Firewalls

ModSecurity: ModSecurity is an open source, cross-platform web application firewall (WAF) module. It enables web application defenders to gain visibility into HTTP(S) traffic and provides a power rules language and API to implement advanced protections.

NAXSI: NAXSI is an acronym that stands for Nginx Anti Xss & Sql Injection. Its ultimate goal is to prevent any attacker from leveraging web vulnerabilities.

WebKnight: WebKnight is Open Source Web Application Firewall (WAF) for IIS.

Shadow Daemon: Shadow Daemon is a web application firewall that intercepts requests and filters out malicious parameters.