SOC OPEN SOURCE

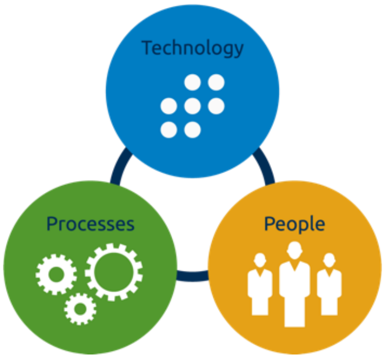
https://www.linkedin.com/in/joas-antonio-dos-santos

SOC

A security operations center (SOC) is responsible for performing attack detection and threats, analyze attacks and threats, assess their impacts, and respond to security incidents. Its structure is based on three main functions: People, Processes and Technology.

People

People are a key factor within a SOC, being an incident response professional or a Security Analyst. An incident responder is responsible for performing a detailed analysis of malicious events using research analysis, threat intelligence, malware analysis tools, and forensic techniques. While a security analyst collects security event data, machine log data, network logs and risk analysis to determine an impact of a threat.



Law Suit

To make the SOC effective, it is vital to define and document processes so that execution can be ensured according to the documented plan. The process ensures timely synchronization and execution of different events and activities performed by the SOC. It is through processes that the responsibilities of functions linked to a SOC will be delegated to a security analyst and an incident response professional in order to achieve the best results.

Technology

The technologies ensure that the SOC will have tools and controls to carry out the monitoring of critical environments, risk analysis and incident response, to avoid major impacts.

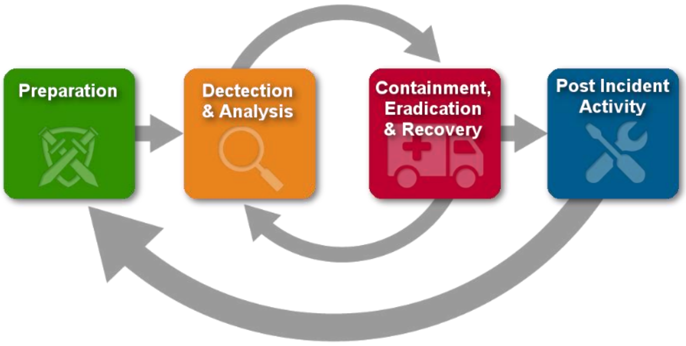
Based on these three functions, we will have:

- **Security Monitoring:** implementation and development of detection rules, analysis of security events and incidents.
- **Threat Hunting:** Active search for new threats and suspicious anomalies about events collected in monitoring tools.

- **Threat Intelligence:** Collecting information about threats and their motivations from external sources and in a community manner with other organizations.
- **Cyber Brand Protection:** Monitoring of external information sources in order to detect leaks of confidential data from patients and staff (login data, internal documents etc).
- **Incident Response:** Recommendations on how to go about resolving security incidents and helping to deal with them.

incident response

Incident response is a set of methodologies that aim to contain and minimize the impacts of a cyber incident, whether it is the result of an attack, misuse, or even a major disaster. The objective is to handle the situation in a way that limits damage and reduces recovery time and costs.



NIST: Incident Response Lifecycle

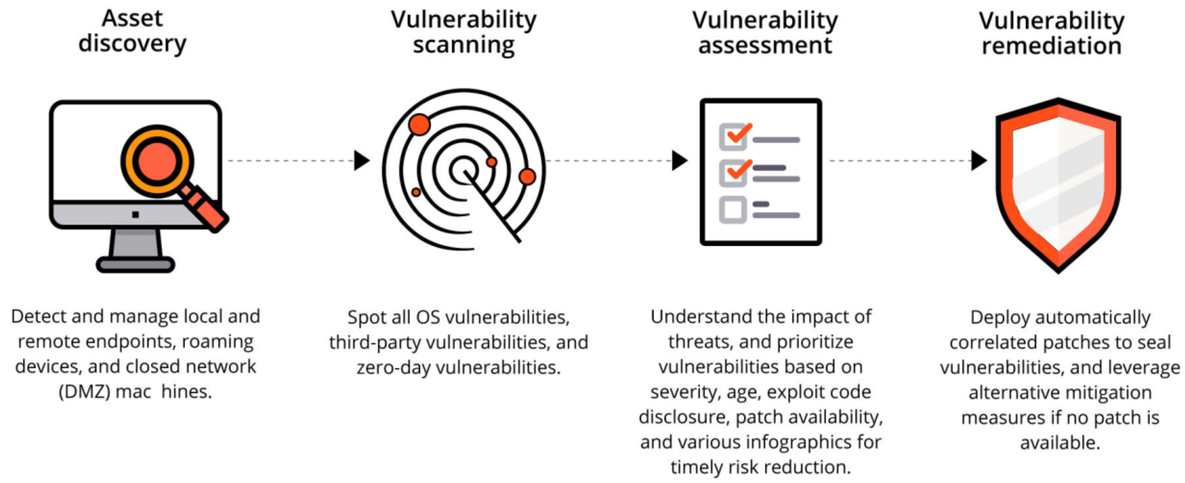
- **Preparation:** Constant study of new threats and methodologies, constant training of specialists, implementation and operation of technologies that allow us to act. Collecting and monitoring indicators to generate analytical and predictive reports.
- **Identification:** Screening of indicators in order to quantify, qualify and classify identified threats.
- **Containment:** Threat containment by isolating affected systems to prevent further damage and an appropriate response to each threat.
- **Eradication:** Elimination of identified threats as well as the location of flaws exposed to these threats.
- **Recovery:** Restore affected systems and threatened resources.
- **Lessons Learned:** Review and refinement of knowledge bases to improve responsiveness to future incidents.

One of the emerging areas of focus and investment is the concept of automation and security demand. This assumes increasing importance due to various trends in the sector.

- **Security Automation -** the use of information technology in place of manual processes for cyber incident response and security event management.
- **Security Orchestration -** an integration of security tools and information technology designed to streamline processes and drive security automation.

- **Threats and Vulnerability Management**

- Threat and vulnerability management prioritizes strengthening security with assessments and tests looking for threats that may impact certain environments. Conducting constant tests of the SOC defense mechanisms, in addition to testing the agility of the security team when detecting a threat and the efficiency of the incident response team. And for proper vulnerability management, the responsible professionals will deal with:



Detect and manage local and remote endpoints, roaming devices, and closed network (DMZ) mac hines.

Spot all OS vulnerabilities, third-party vulnerabilities, and zero-day vulnerabilities.

Understand the impact of threats, and prioritize vulnerabilities based on severity, age, exploit code disclosure, patch availability, and various infographics for timely risk reduction.

Deploy automatically correlated patches to seal vulnerabilities, and leverage alternative mitigation measures if no patch is available.

- Conducting regular penetration tests.
- Observe a consistent patch schedule.
- Account for all IT assets and networks.
- Get current threat feeds.
- Learn about current vulnerabilities and work to fix them.
- Visualize data for broad understanding.
- Check that the proper tools are used.

Add correction clauses to your service provider's policies and procedures.

- **Cyber Security Framework (CSF) – NIST**

Develop a SOC with the main market frameworks in mind

- The NIST cybersecurity framework, also called the NISTCyber Security Framework, provides a framework, based on existing standards, guidelines, and practices for organizations in the **private sector,** in order to better manage and reduce the cyber security risk. In addition to helping organizations prevent, detect and respond to cyber threats and cyber attacks, it is designed to improve cyber security communications and risk management among stakeholders internal and external.

- **C2M2**

- The Cybersecurity Maturity Model (C2M2) program is a public-private partnership effort was that was established as a result of Management's efforts to improve resources for cybersecurity in the electricity sector and expanded to health, in order to understand the cybersecurity posture of the network.

- The model focuses on implementing and managing cybersecurity practices associated with the operation and use of information technology and operational technology assets and the environments in which they operate. The goal is to support the ongoing development and measurement of cybersecurity capabilities in any organization.

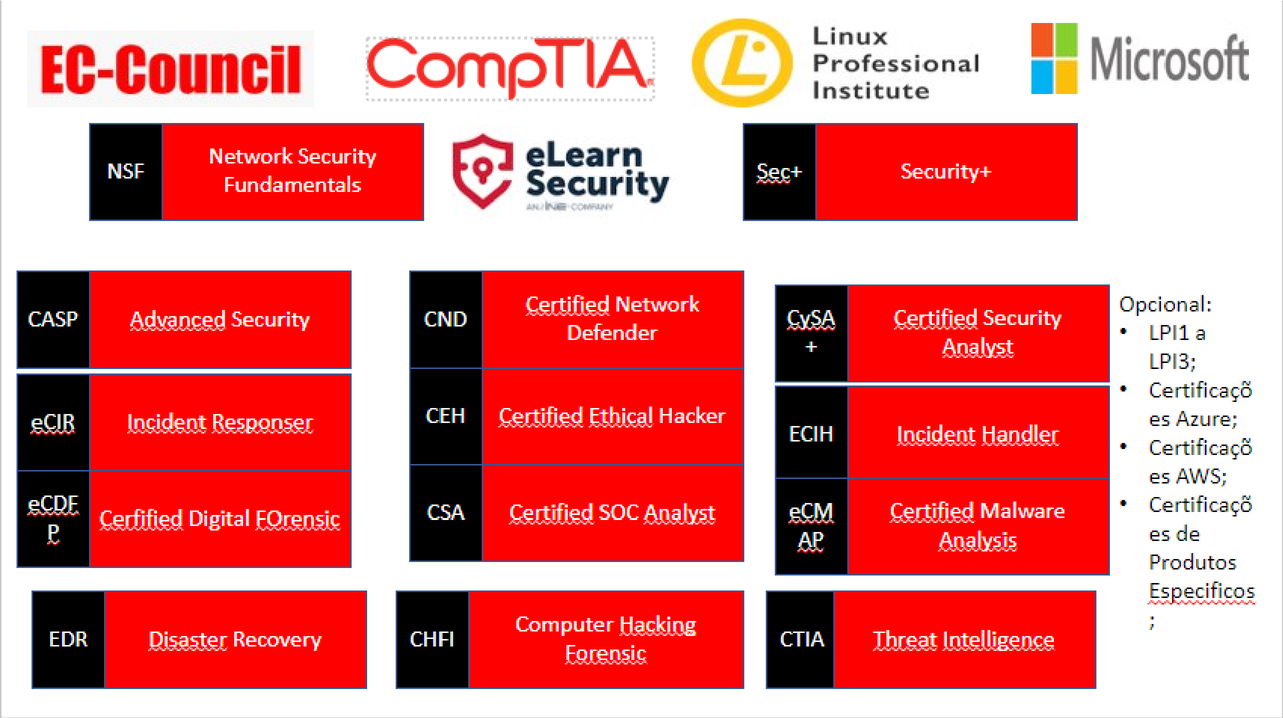
- **LGPD and GDPR**

The General Data Protection Act (BR) and the General Data Protection Regulation (EU), refers to the Processing of personal data, including in digital media, by a natural person or by a legal entity governed by public or private law, with the aim of protecting the fundamental rights of freedom and privacy and the free development of the natural person's personality. Including sensitive health data.

- ## Academic Nucleus

- ## Trainings

A training program aimed at providing professionals in the areas to develop their skills in the area of   information security. See a certification structure:



NSF Network Security Fundamentals

Sec+ Security+

CASP Advanced Security

eCIR Incident Responser

eCDFP Cerfified Digital FOrensic

CND Certified Network Defender

CEH Certified Ethical Hacker

CSA Certified SOC Analyst

CySA+ Certified Security Analyst

ECIH Incident Handler

eCMAP Certified Malware Analysis

EDR Disaster Recovery

CHFI Computer Hacking Forensic

CTIA Threat Intelligence

Opcional:

- LPI1 a LPI3;
- Certificações Azure;
- Certificações AWS;
- Certificações de Produtos Especificos;

- ## Machine Learning and Artificial Intelligence

The massive and growing volumes of data from these devices in recent years have made it increasingly difficult for security operations teams (SecOps) to detect, triage, prioritize and respond to threats, resulting in greater exposure to risk. Traditional security information and event management (SIEM) systems and other alerting mechanisms that use static rules and thresholds, while effective against known threats, have faced challenges with new, low-level, targeted attacks.

The trend toward rapid assembly of alert data has increased the need for an automated way for organizations to quickly filter and identify deeply hidden threats. This needs to happen using static rules and looking for deviations from normal traffic behavior.

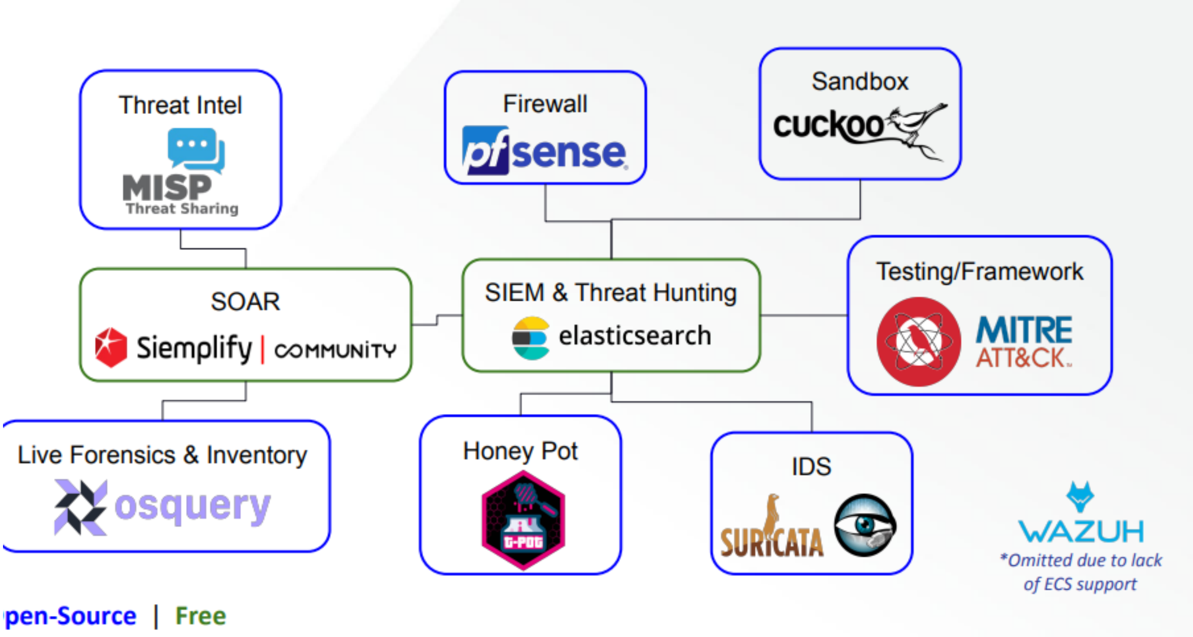
Some ML models are "supervised", while others are "unsupervised". Supervised ML involves learning by example from an existing dataset and then applying that knowledge to new data. For example, by analyzing data associated with known malware traffic, a supervised ML tool learns how traffic deviates from normal so that it can recognize the same pattern in new data without being explicitly programmed.

An unattended ML tool works by observing traffic over a period of time, learning what "normal" behavior on the network looks like, and investigating deviations from that baseline. Unattended ML "really shows its power" when it comes to finding insider threats, advanced persistent threats and other targeted attacks, Daigle said.

Unsupervised ML does not depend on rules and limits, but learns continuously and automatically based on data patterns and scale. This means that it can create a baseline for the "normal" behavior of every entity in an organization, rather than applying the same baseline to all.

ML's primary use case in threat detection is for automatically identifying activities that deviate from a baseline. Current estimates of demand for ML-enabled products and artificial intelligence to meet cybersecurity challenges tend to vary widely, but most point to strong growth in the coming years.

SOC Open Source



Use Elastic Common Schema

- Combine logging, metrics and APM to add greater observability
- Flexible alerting across the entire stack
- IP reputation links - customizable searches
- 28 ML anomaly detection jobs focused on SIEM *
- 203 pre-built detection rules (mapped to MITERAtt & Ck)
- Many prebuilt views

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

- Malware Information Sharing Platform
- Open source threat intelligence platform maintained by CIRCL to store, share, and collaborate on cybersecurity metrics.
- Use semaphore protocol for sorting and sharing
- MISP Communities
- MISP will make it easier for you to share, but also receive trusted partners and trust groups from trusted people.
- Generating rules Snort / Suricata / Bro / Zeek IDS, STIX, OpenIOC, text or csv exports MISP allows you to automatically import data into your detection systems

Atomic Red Team

Atomic Red Team is a simple test library that any security team can run to test their controls. Tests are focused, have few dependencies, and are defined in a structured format that can be used by automation frameworks.

Three main beliefs constituted the statute of the Atomic Red Team:

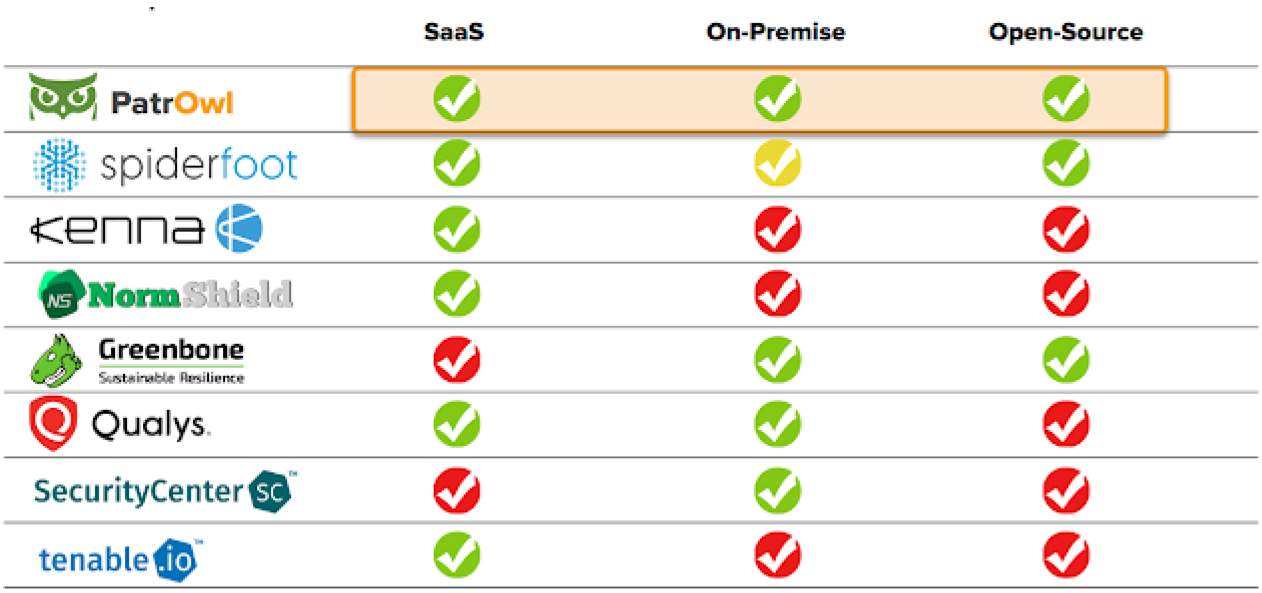
Teams need to be able to test everything from specific technical controls to results. Our security teams do not want to operate with a “hope and prayer” attitude towards detection. We need to know what our controls and programs can detect and what they can't. We don't have to detect every opponent, but we believe in knowing our blind spots.

https://atomicredteam.io/

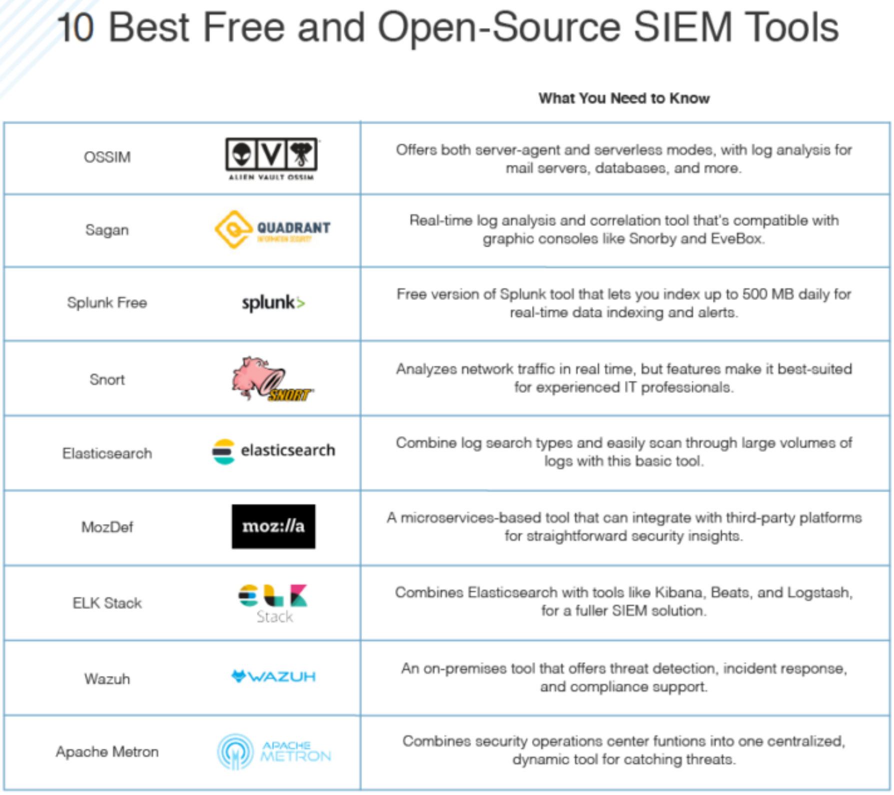
We should be able to run a test in less than five minutes. Most security testing and automation tools take a long time to install, configure and run. We coined the term "atomic tests" because we felt there was a simple way to break down the tests so that most could be run in a few minutes.

The best test is the one you actually run.

We need to keep learning how adversaries are operating. Most security teams don't have the benefit of seeing a wide variety of opponent types and techniques crossing their table every day. Even we at Red Canary have only found a fraction of the possible techniques being used, which makes working together as a community essential to making ourselves better.



	SaaS	On-Premise	Open-Source
PatrOwl	🟢	🟢	🟢
spiderfoot	🟢	🟡	🟢
kenna	🟢	🔴	🔴
NormShield	🟢	🔴	🔴
Greenbone Sustainable Resilience	🔴	🟢	🟢
Qualys.	🟢	🟢	🔴
SecurityCenter SC	🔴	🟢	🔴
tenable.io	🟢	🔴	🔴

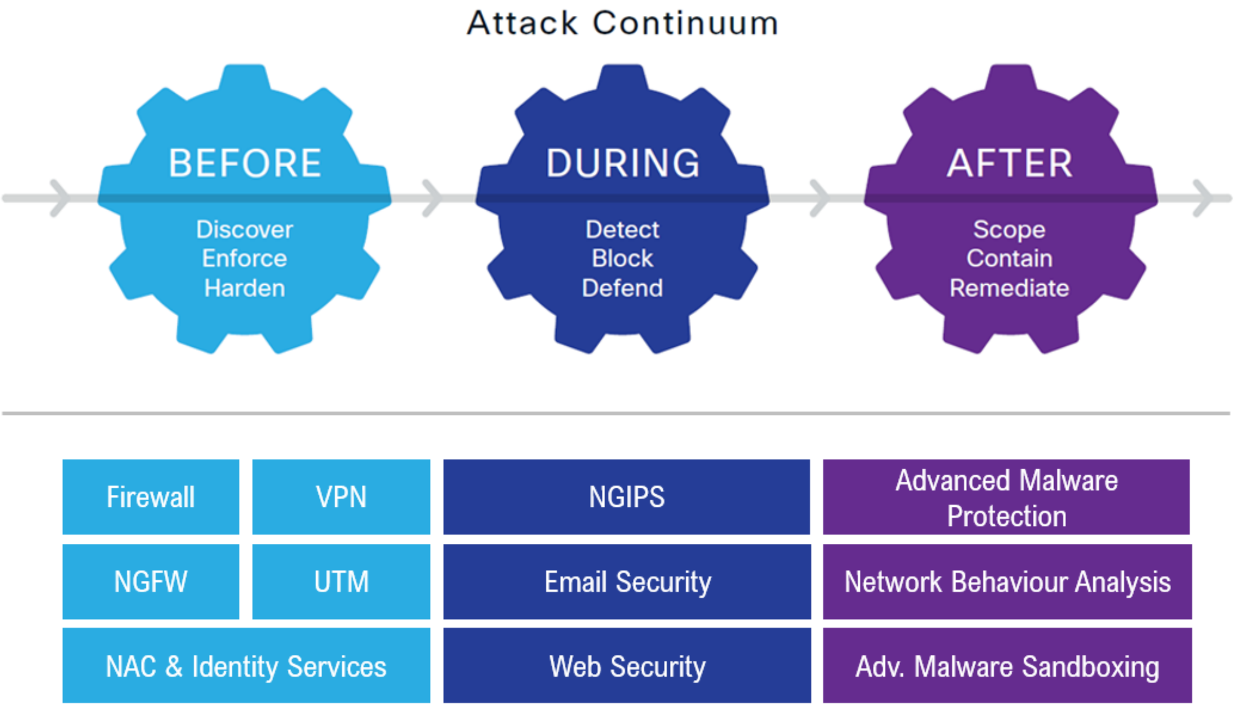


10 Best Free and Open-Source SIEM Tools

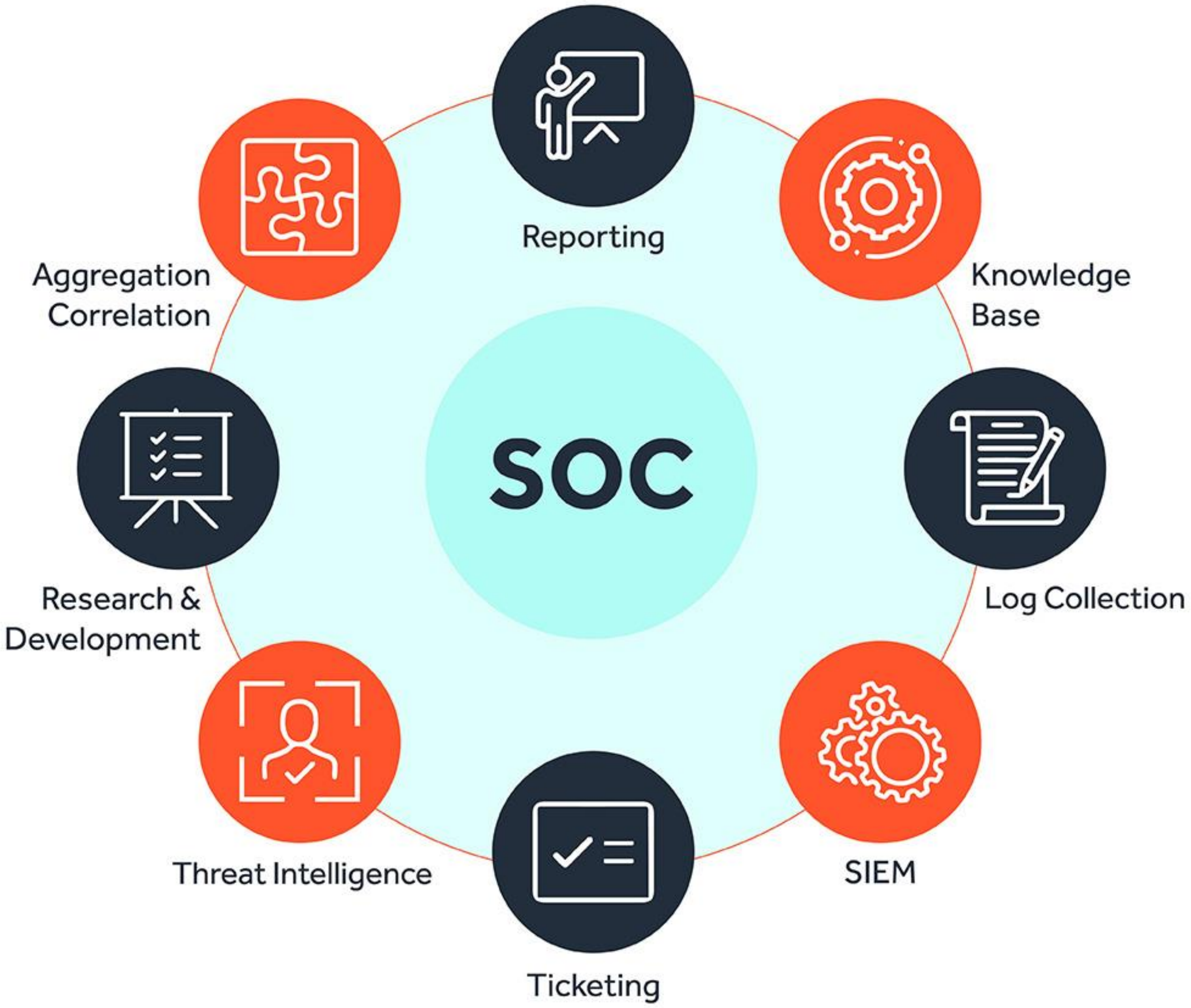
		What You Need to Know
OSSIM	ALIEN VAULT OSSIM	Offers both server-agent and serverless modes, with log analysis for mail servers, databases, and more.
Sagan	QUADRANT	Real-time log analysis and correlation tool that's compatible with graphic consoles like Snorby and EveBox.
Splunk Free	splunk>	Free version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

- SO
- OSSEC
- Sagan
- Splunk Free
- Snort
- elasticsearch
- MozDef
- ELK Stack
- Wazuh
- Apache Metron

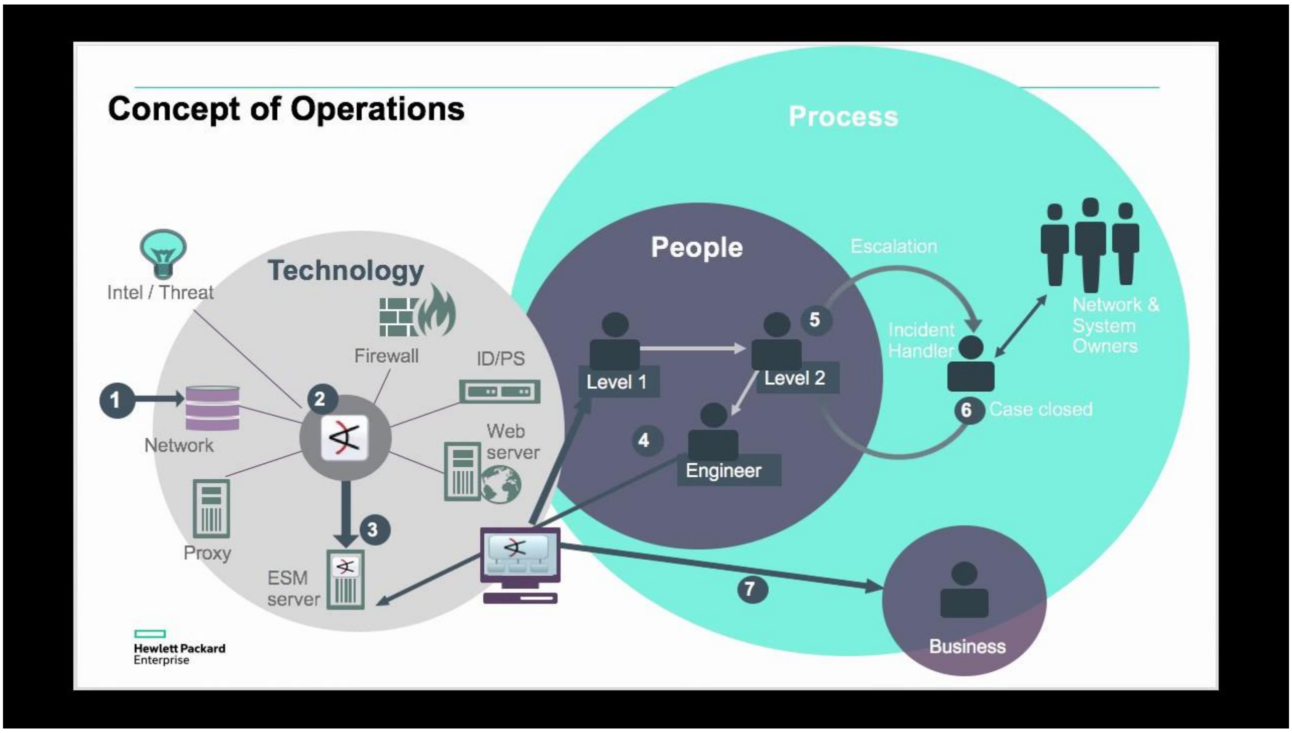
Example: Design Security Operation Center



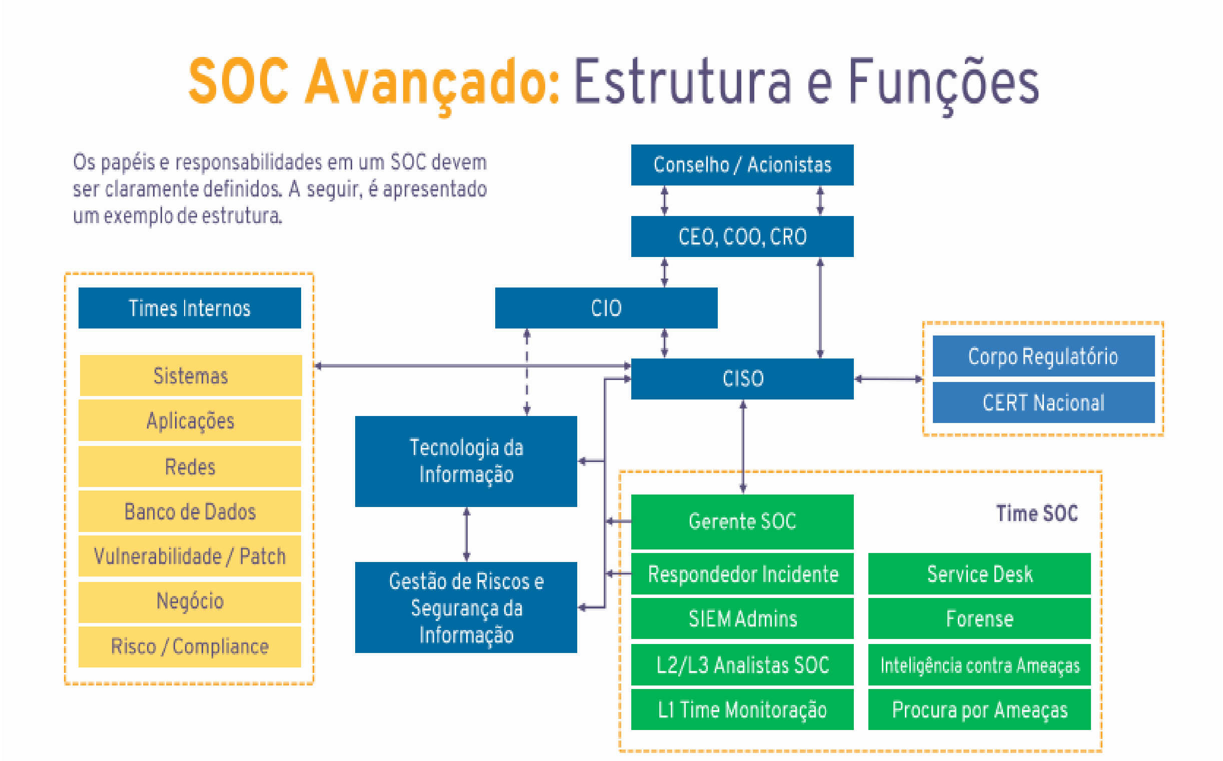
Firewall	VPN	NGIPS	Advanced Malware Protection
NGFW	UTM	Email Security	Network Behaviour Analysis
NAC & Identity Services		Web Security	Adv. Malware Sandboxing


Reporting
Aggregation Correlation
Knowledge Base
SOC
Research & Development
Log Collection
Threat Intelligence
SIEM
Ticketing

Operation Concepts



Example: Structure and Functions



SOC Avançado: Estrutura e Funções

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

Conselho / Acionistas

CEO, COO, CRO

CIO

CISO

Times Internos

- Sistemas
- Aplicações
- Redes
- Banco de Dados
- Vulnerabilidade / Patch
- Negócio
- Risco / Compliance

Tecnologia da Informação

Gestão de Riscos e Segurança da Informação

Corpo Regulatório

CERT Nacional

Time SOC

- Gerente SOC
- Respondedor Incidente
- SIEM Admins
- L2/L3 Analistas SOC
- L1 Time Monitoração
- Service Desk
- Forense
- Inteligência contra Ameaças
- Procura por Ameaças

Example: Open Sources Tools for SOC

SIEM

Apache Metron: The Cisco Open SOC framework developed Apache Metron. Like SIEMonster, several open source solutions are also connected in a centralized network. Apache Metron can use standard JSON language to parse and normalize security events for easy analysis. In addition, safety warnings, data enrichment and labeling can be issued.

AlienVault OSSIM: A AT&TCybersecurity provides AlienVault OSSIM, an open source SIEM tool based on its AlienVault USM solution. AlienVault OSSIM brings together many open source projects into a single package, close to the entries above. AlienVault OSSIM also allows application tracking and logging.

MozDef: Built with Mozilla to simplify the handling of safety incidents, MozDef offers scalability and resiliency. MozDef will provide event correlation and security warnings with an architecture based on microservices. This can also be incorporated with other third parties.

OSSEC: Technically, OSSEC is an open source intrusion detection system rather than a SIEM solution. However, it still provides a host agent to collect logs and a central application to process those logs. Overall, this tool monitors log files and file integrity for potential cyber attacks. It can perform log analysis of various network services and provide your IT staff with numerous alerting options.

Wazuh: In fact, oWazuh evolved from another SIEM solution, namely, OSSEC, which is open source. However, Wazuh is a special option for you now. This facilitates agent-based data storage and syslog retrieval. Wazuh can also easily track devices on site. It has a dedicated web interface and detailed guidelines for quick IT administrator control.

OSS Prelude: Prelude OSS offers the Prelude SIEM solution with an open source version. This helps you work with a wide variety of log formats and other features. It can also normalize event data into a common language, which can support other cybersecurity tools and solutions. Prelude OSS also profits from continued growth, while maintaining the current intelligence threat.

Snort: Snort also offers log monitoring as another open source intrusion detection system; it also performs real-time network traffic analysis to identify potential dangers. Snort can also view traffic or packet dump flows in a log file. In addition, output plugins can be used to decide how and where the dataset is saved.

Sagan: Sagan operates almost entirely as a forum for the SIEM Snort device, which is complementary to Sagan and follows Snort principles. Sagan is lightweight and can write to databases on snort. It can be another useful resource for anyone who would like to collaborate with Snort.

ELK Stack: There are free SIEM products in the ELK Stack solution. For example, ELK can compile logs from almost any data source using built-in Logstash components. Therefore, this log data can be combined into a wide variety of plug-ins, although manual security rules are required. ELK Stack can also display data with a specific part.

SIEMonster: SIEMonster provides a free SIEM and a paid solution. As is the case with many of the solutions used, the SIEMonster framework provides a centralized tool management interface for data analysis, threat intelligence and various open source software. Your organization will host it in a cloud, unlike some other open source SIEM solutions.

IDS/IPS

Snort: Snort is the most popular open source IDPS solution for Windows and Unix, providing intrusion review, package monitoring, and complete real-time intrusion prevention capabilities.

Meerkat: Suricata is an IDPS and network security control engine with a high performance network. Since it is multi-threaded, the processing load on a sensor is balanced on one instance.

OSSEC: This system combines log analysis, file integrity management, Windows registry tracking, central policy implementation, rootkit identification, real-time warnings and active response.

SecurityOnion: Security Onion is an open source intrusion detection tool, network monitoring protection system and log management distribution for enterprise security on Linux.

Bro Network Security Monitor: Bro is an open source network security platform that details network activity and can be used on a scale. It provides a robust forum for more general traffic analysis, which includes identifying incidents, detecting threats, and monitoring your security capabilities.

Vistumbler: Vistumbler is a Windows wireless scanner. The main purpose of Vistumbler is to map and visualize the access points around you using the collected wireless and GPS data.

Smoothwall Express: Smoothwall Express is an open source firewall that features an easy-to-use web interface and a separate, stable Linux operating system. The functionality involves LAN, DMZ and wireless network support, real-time content filtering and HTTPS filtering.

Untangle NG Firewall: NG Firewall is a next generation network application that simultaneously monitors network traffic. These applications are connected by a GUI, database and growing reports.

ClamAV: ClamAV is an open source framework for email gateway antivirus scanning and is available in Windows, OS X, Linux and BSD applications.

Incident Response Tool

GRR quick response: the quick response of Google's GRR consists of two parts: one GRR client deployed in an investigated network and a GRR server that assists analysts in applying actions and processing the collected data.

Cyphon: Cyphon provides capabilities to capture, process, triage and incidents for analysts. It collects data such as message logs, APIs that send email - which makes it easy to analyze and collect as much detail as you want.

Volatility: volatility is a forensic memory system that helps analysts in memory dumps analyze and explore information.

SIFT (Sans Investigative Forensics Toolkit) Workstation: SIFT Workstation is a Ubuntu tools with all the necessary analysis systems to conduct comprehensive digital forensics work.

The Hive Project: The Hive Project is a free, open source IR framework that allows many researchers to conduct incident investigations at the same time. This helps analysts produce new role assignment updates and display events and warnings from multiple sources, including SIEM alerts.

Malware Analysis Tools

Cuckoo Sandbox: Cuckoo Sandbox is a free malware analyze 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 Commitment 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. own set of indicators.

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

Machine Security Intelligence Collector: Machine 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.

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