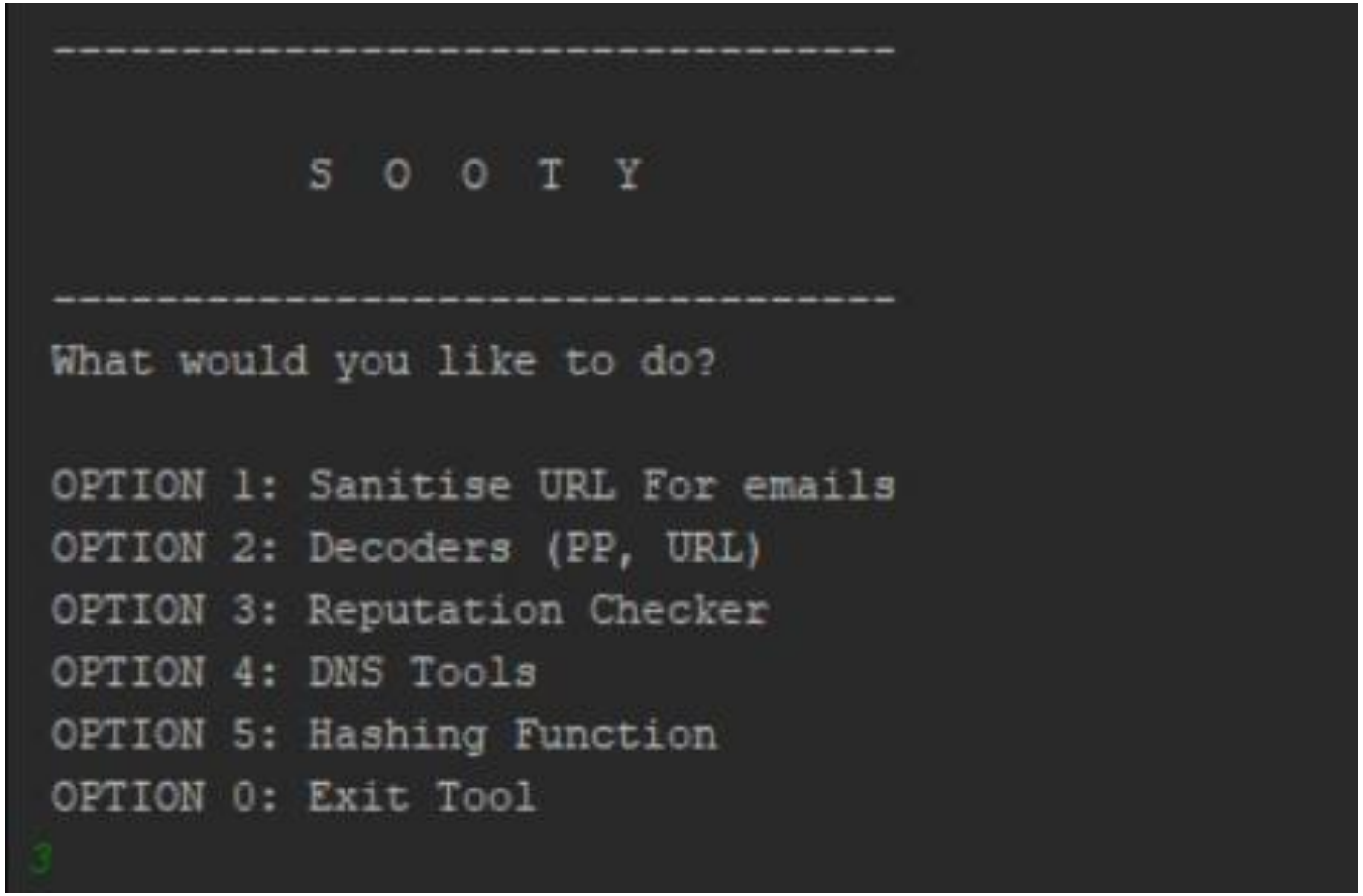
Security Operation Center – Operations Development

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

Security Operation Center Tools

Sooty

- Sooty is a tool developed with the task of aiding SOC analysts with automating part of their workflow. One of the goals of Sooty is to perform as many of the routine checks as possible, allowing the analyst more time to spend on deeper analysis within the same time-frame. Details for many of Sooty's features can be found below.
- https://github.com/TheresAFewConors/Sooty



Peepdf

- peepdf is a Python tool to explore PDF files in order to find out if the file can be harmful or not. The aim of this tool is to provide all the necessary components that a security researcher could need in a PDF analysis without using 3 or 4 tools to make all the tasks. With peepdf it's possible to see all the objects in the document showing the suspicious elements, supports the most used filters and encodings, it can parse different versions of a file, object streams and encrypted files. With the installation of **PyV8** and **Pylibemu** it provides Javascript and shellcode analysis wrappers too. Apart of this it is able to create new PDF files, modify existent ones and obfuscate them.
- https://eternal-todo.com/tools/peepdf-pdf-analysis-tool

```
Usage: ./peepdf.py [options] PDF_file

Options:
  -h, --help            show this help message and exit
  -i, --interactive     Sets console mode.
  -s SCRIPTFILE, --load-script=SCRIPTFILE
                        Loads the commands stored in the specified file and
                        execute them.
  -c, --check-vt        Checks the hash of the PDF file on VirusTotal.
  -f, --force-mode      Sets force parsing mode to ignore errors.
  -l, --loose-mode      Sets loose parsing mode to catch malformed objects.
  -m, --manual-analysis
                        Avoids automatic Javascript analysis. Useful with
                        eternal loops like heap spraying.
  -u, --update          Updates peepdf with the latest files from the
                        repository.
  -g, --grinch-mode     Avoids colorized output in the interactive console.
  -v, --version         Shows program's version number.
  -x, --xml             Shows the document information in XML format.
```

PyREBox

- PyREBox is a Python scriptable Reverse Engineering sandbox. It is based on QEMU, and its goal is to aid reverse engineering by providing dynamic analysis and debugging capabilities from a different perspective. PyREBox allows to inspect a running QEMU VM, modify its memory or registers, and to instrument its execution, by creating simple scripts in Python to automate any kind of analysis. It also offers a shell based on IPython that exposes a rich set of commands, as well as a Python API.
- https://talosintelligence.com/pyrebox

Fail2Ban

- Fail2ban scans log files (e.g. /var/log/apache/error_log) and bans IPs that show the malicious signs -- too many password failures, seeking for exploits, etc. Generally Fail2Ban is then used to update firewall rules to reject the IP addresses for a specified amount of time, although any arbitrary other action (e.g. sending an email) could also be configured. Out of the box Fail2Ban comes with filters for various services (apache, courier, ssh, etc).

- Fail2Ban is able to reduce the rate of incorrect authentications attempts however it cannot eliminate the risk that weak authentication presents. Configure services to use only two factor or public/private authentication mechanisms if you really want to protect services.
- https://www.fail2ban.org/wiki/index.php/Main_Page

OSSEC

- OSSEC is a full platform to monitor and control your systems. It mixes together all the aspects of HIDS (host-based intrusion detection), log monitoring and SIM/SIEM together in a simple, powerful and open source solution.

- https://github.com/ossec/ossec-hids
- https://www.ossec.net/

RKHunter and CHRookit

- http://rkhunter.sourceforge.net/
- http://chkrootkit.org/

Process Hacker

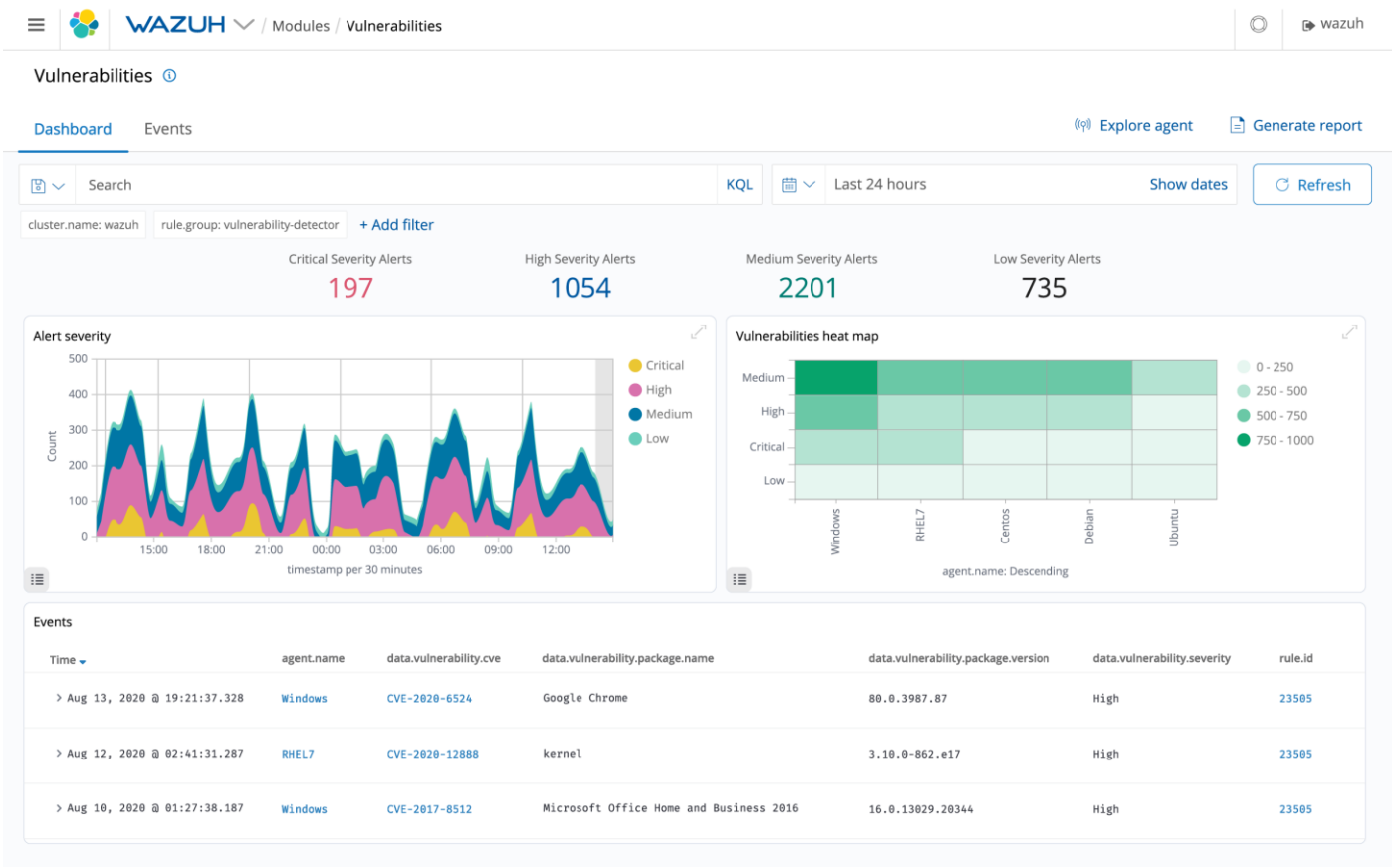
- Process Hacker, A free, powerful, multi-purpose tool that helps you monitor system resources, debug software and detect malware.
- https://processhacker.sourceforge.io/downloads.php

Splunk

- Its software helps capture, index and correlate real-time data in a searchable repository, from which it can generate graphs, reports, alerts, dashboards and visualizations. Splunk uses machine data for identifying data patterns, providing metrics, diagnosing problems and providing intelligence for business operations. Splunk is a horizontal technology used for application management, security and compliance, as well as business and web analytics.
- https://www.splunk.com/

Wazuh

- Wazuh is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance.
- https://wazuh.com/



TheHive

- A scalable, open source and free Security Incident Response Platform, tightly integrated with MISP (Malware Information Sharing Platform), designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly.
- https://thehive-project.org/

Security Onion

- Our products include both the Security Onion software and specialized hardware appliances that are built and tested to run Security Onion. Our appliances will save you and your team time and resources, allowing you to focus on keeping your organization secure.
- https://securityonionsolutions.com/

Caine

- CAINE (Computer Aided INvestigative Environment) is an Italian GNU/Linux live distribution created as a Digital Forensics project
- https://www.caine-live.net/

Caldera

What does CALDERA do?

- CALDERA helps cybersecurity professionals reduce the amount of time and resources needed for routine cybersecurity testing.
- CALDERA empowers cyber teams in three main ways:

Autonomous Adversary Emulation

- With CALDERA, your cyber team can build a specific threat (adversary) profile and launch it in a network to see where you may be susceptible. This helps with testing defenses and training blue teams on how to detect specific threats.

Autonomous Incident Response

- Enables your team to perform automated incident response on a given host, allowing them to find new ways to identify and respond to threats.

Manual Red-Team Engagements

- Helps your red team perform manual assessments with computer assistance by augmenting existing offensive toolsets. The framework can be extended with any custom tools you may have.
- https://caldera.mitre.org/

Atomic Red Team

https://atomicredteam.io/

Metta

Metta is an information security preparedness tool.

This project uses Redis/Celery, python, and vagrant with virtualbox to do adversarial simulation. This allows you to test (mostly) your host based instrumentation but may also allow you to test any network based detection and controls depending on how you set up your vagrants.

The project parses yaml files with actions and uses celery to queue these actions up and run them one at a time without interaction.

https://github.com/uber-common/metta

OSSIM

- AlienVault® OSSIM™, Open Source Security Information and Event Management (SIEM), provides you with a feature-rich open source SIEM complete with event collection, normalization and correlation. Launched by security engineers because of the lack of available open source products, AlienVault OSSIM was created specifically to address the reality many security professionals face: A SIEM, whether it is open source or commercial, is virtually useless without the basic security controls necessary for security visibility.
- https://cybersecurity.att.com/products/ossim

Prelude

- Prelude is a Universal "Security Information & Event Management" (SIEM) system. Prelude collects, normalizes, sorts, aggregates, correlates and reports all security-related events independently of the product brand or license giving rise to such events; Prelude is "agentless".
- As well as being capable of recovering any type of log (system logs, syslog, flat files, etc.), Prelude benefits from a native support with a number of systems dedicated to enriching information even further (snort, samhain, ossec, auditd, etc.).
- https://www.prelude-siem.org/

Nagios

- Nagios XI provides monitoring of all mission-critical infrastructure components including applications, services, operating systems, network protocols, systems metrics, and network infrastructure. Hundreds of third-party addons provide for monitoring of virtually all in-house and external applications, services, and systems.
- https://www.nagios.org/

Zabbix

Monitor any possible performance metrics and incidents in your network:

Network performance

- Network bandwidth usage
- Packet loss rate
- Interface errorrate
- High CPU or memory utilization
- Number of tcp connections is anomaly high for this day of the week
- Aggregate throughput of core routers is low

Network health

- Link is down
- System status is in warning/critical state
- Device temperature is too high / too low
- Power supply is in critical state
- Free disk space is low
- Fan is in critical state
- No SNMP data collection

Configuration changes

- New device added or removed
- Network module is added, removed or replaced
- Firmware has been upgraded
- Device serial number has changed
- Interface has changed to lower speed or half-duplex mode

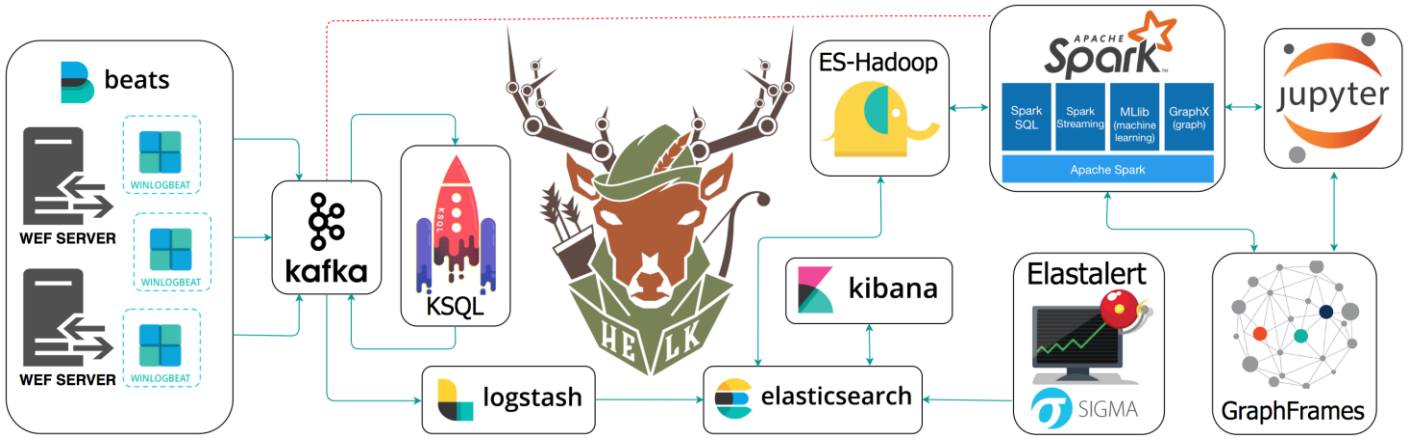
This is a sample list of network-related metrics and incidents, monitored by Zabbix out of the box. See the full list in template descriptions. You can extend/customize the scope of monitored objects by adding new items, writing custom data collection scripts, building custom templates, etc.

- https://www.zabbix.com/network_monitoring

Icinga

- Find answers, take actions and become a problem-solver. Be flexible and take your own ways. Stay curious, stay passionate, stay in the loop. Tackle your monitoring challenge.
- https://icinga.com/

Helk



- The Hunting ELK or simply the HELK is one of the first open source hunt platforms with advanced analytics capabilities such as SQL declarative language, graphing, structured streaming, and even machine learning via Jupyter notebooks and Apache Spark over an ELK stack. This project was developed primarily for research, but due to its flexible design and core components, it can be deployed in larger environments with the right configurations and scalable infrastructure.
- https://github.com/Cyb3rWard0g/HELK

CimSweep

- CimSweep is a suite of CIM/WMI-based tools that enable the ability to perform incident response and hunting operations remotely across all versions of Windows. CimSweep may also be used to engage in offensive reconnaisance without the need to drop any payload to disk. Windows Management Instrumentation has been installed and its respective service running by default since Windows XP and Windows 2000 and is fully supported in the latest versions of Windows including Windows 10, Nano Server, and Server 2016.
- https://github.com/PowerShellMafia/CimSweep

PowerForensics

- The purpose of PowerForensics is to provide an all inclusive framework for hard drive forensic analysis. PowerForensics currently supports NTFS and FAT file systems, and work has begun on Extended File System and HFS+ support.
- https://github.com/Invoke-IR/PowerForensics

RedLine

- Redline®, FireEye's premier free endpoint security tool, provides host investigative capabilities to users to find signs of malicious activity through memory and file analysis and the development of a threat assessment profile.

With Redline, you can:

- Thoroughly audit and collect all running processes and drivers from memory, file-system metadata, registry data, event logs, network information, services, tasks and web history.
- Analyze and view imported audit data, including the ability to filter results around a given timeframe using Redline's Timeline functionality with the TimeWrinkle™ and TimeCrunch™ features.
- Streamline memory analysis with a proven workflow for analyzing malware based on relative priority.
- Perform Indicators of Compromise (IOC) analysis. Supplied with a set of IOCs, the Redline Portable Agent is automatically configured to gather the data required to perform the IOC analysis and an IOC hit result review.
- https://www.fireeye.com/services/freeware/redline.html

Yara

- YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a. rule, consists of a set of strings and a boolean expression which determine its logic.
- https://github.com/VirusTotal/yara

Forager

- Do you ever wonder if there is an easier way to retrieve, store, and maintain all your threat intelligence data? Random user, meet Forager. Not all threat intel implementations require a database that is "correlating trillions of data points.." and instead, you just need a simple interface, with simple TXT files, that can pull threat data from other feeds, PDF threat reports, or other data sources, with minimal effort. With 15 pre-configured threat feeds, you can get started with threat intelligence feed management today
- https://github.com/opensourcesec/Forager

Threatbus

- Connect Open-Source Security Tools: Threat Bus is a pub-sub broker for threat intelligence data. With Threat Bus you can seamlessly integrate threat intel platforms like OpenCTI or MISP with detection tools and databases like Zeek or VAST.
- Native STIX-2: Threat Bus transports indicators and sightings encoded as per the STIX-2 open format specification.
- Plugin-based Architecture: The project is plugin-based and can be extended easily. Read about the different plugin types and how to write your own. We welcome contributions to adopt new open source tools!
- Official Plugins: We maintain many plugins right in the official Threat Bus repository. Check out our integrations for MISP, Zeek, CIFv3, and generally apps that connect via ZeroMQ, like vast-threatbus and our OpenCTI connector.
- Snapshotting: The snapshot feature allows subscribers to directly request threat intelligence data for a certain time range from other applications. Threat Bus handles the point-to-point communication of all involved apps.
- https://github.com/tenzir/threatbus

Threat Ingestor

- ThreatIngestor can be configured to watch Twitter, RSS feeds, or other sources, extract meaningful information such as malicious IPs/domains and YARA signatures, and send that information to another system for analysis.
- https://github.com/InQuest/ThreatIngestor

Misp

- User guide for MISP - The Open Source Threat Intelligence Sharing Platform. This user guide is intended for ICT professionals such as security analysts, security incident handlers, or malware reverse engineers who share threat intelligence using MISP or integrate MISP into other security monitoring tools. The user guide includes day-to-day usage of the MISP's graphical user interface along with its automated interfaces (API), in order to integrate MISP within a security environment and operate one or more MISP instances.
- https://github.com/MISP/misp-book

Malware-IOC

- Here are indicators of compromise (IOCs) of our various investigations. We are doing this to help the broader security community fight malware wherever it might be.
- .yar files are Yara rules
- .rules files are Snort rules
- samples.md5, samples.sha1 and samples.sha256 files are newline separated list of hexadecimal digests of malware samples
- If you would like to contribute improved versions please send us a pull request.
- If you've found false positives give us the details in an issue report and we'll try to improve our IOCs.
- These are licensed under the permissive BSD two-clause license. You are allowed to modify these and keep the changes to yourself even though it would be rude to do so.
- https://github.com/eset/malware-ioc

Cobalt Strike Scan

- Scan files or process memory for Cobalt Strike beacons and parse their configuration.
- CobaltStrikeScan scans Windows process memory for evidence of DLL injection (classic or reflective injection) and/or performs a YARA scan on the target process' memory for Cobalt Strike v3 and v4 beacon signatures.
- Alternatively, CobaltStrikeScan can perform the same YARA scan on a file supplied by absolute or relative path as a command-line argument.
- If a Cobalt Strike beacon is detected in the file or process, the beacon's configuration will be parsed and displayed to the console.
- https://github.com/Apr4h/CobaltStrikeScan

Harden Tools

- Hardentools is designed to disable a number of "features" exposed by operating systems (Microsoft Windows, for now) and some widely used applications (Microsoft Office and Adobe PDF Reader, for now). These features, commonly thought for enterprise customers, are generally useless to regular users and rather pose as dangers as they are very commonly abused by attackers to execute malicious code on a victim's computer. The intent of this tool is to simply reduce the attack surface by disabling the low-hanging fruit. Hardentools is intended for individuals at risk, who might want an extra level of security at the price of some usability. It is not intended for corporate environments.
- https://github.com/securitywithoutborders/hardentools

Windows Secure Host Baseline

- The Windows Secure Host Baseline (SHB) provides an automated and flexible approach for assisting the DoD in deploying the latest releases of Windows 10 using a framework that can be consumed by organizations of all sizes.

- The DoD CIO issued a memo on November 20, 2015 directing Combatant Commands, Services, Agencies and Field Activities (CC/S/As) to rapidly deploy the Windows 10 operating system throughout their respective organizations with the objective of completing deployment by the end of January 2017. The Deputy Secretary of Defense issued a memo on February 26, 2016 directing the DoD to complete a rapid deployment and transition to Microsoft Windows 10 Secure Host Baseline by the end of January 2017.
- https://github.com/nsacyber/Windows-Secure-Host-Baseline

Any Run

- It is not enough to run a suspicious file on a testing system to be sure in its safety. For some types of malware or vulnerabilities (e.g., APT), direct human interaction during analysis is required. A set of online malware analysis tools, allows you to watch the research process and make adjustments when needed, just as you would do it on a real system, rather than relying on a wholly automated sandbox.
- https://any.run/

Hybrid Analysis

- This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology.
- https://www.hybrid-analysis.com/

PSHunt

- PSHunt is a Powershell Threat Hunting Module designed to scan remote endpoints* for indicators of compromise or survey them for more comprehensive information related to state of those systems (active processes, autostarts, configurations, and/or logs).
- PSHunt began as the precurser to Infocyte's commercial product, Infocyte HUNT, and is now being open sourced for the benefit of the DFIR community.
- https://github.com/Infocyte/PSHunt

GoPhish

- Gophish is a powerful, open-source phishing framework that makes it easy to test your organization's exposure to phishing.
- https://getgophish.com/

Solar Winds

- The log manager gathers log messages from all over your system, consolidating the different formats they are written in to be stored and searched together. The dashboard shows all events live on the screen, and there is also an analytical tool that helps you search through stored log files for pertinent security information. The log manager also protects logfiles from tampering with a file integrity monitor.

- The Security Event Manager isn't just a SIEM. It includes a threat intelligence feed, which pools threat detection experiences from all of the clients of the SolarWinds system. The security system uses the guidance from the feed when searching through log messages for indicators of attack.
- https://www.solarwinds.com/security-event-manager

Cortex

- Cortex, an open source and free software, has been created by TheHive Project for this very purpose. Observables, such as IP and email addresses, URLs, domain names, files or hashes, can be analyzed one by one or in bulk mode using a Web interface. Analysts can also automate these operations thanks to the Cortex REST API.
- https://github.com/TheHive-Project/Cortex

HoneyPot Dionea

- Dionaea intention is to trap malware exploiting vulnerabilities exposed by services offered to a network, gaining a copy of the malware.
- https://dionaea.readthedocs.io/en/latest/index.html

IntelOwl

- IntelOwl is an Open Source Intelligence, or OSINT solution to get threat intelligence data about a specific file, an IP or a domain from a single API at scale
- https://intelowlproject.github.io/

Elastic EDR

- Elastic EDR prevents ransomware and malware, detects advanced threats, and arms responders with vital context. It’s free and open, ready for every endpoint.
- https://www.elastic.co/pt/endpoint-security/

OpenEDR

- OpenEDR is free and its source code is open to public. OpenEDR allows you to analyze what's happening across your entire environment at base-security-event level. This granularity enables accurate root-causes analysis needed for faster and more effective remediation. Proven to be the best way to convey this type of information, process hierarchy tracking provide more than just data, they offer actionable knowledge. It collects all the details on endpoints, hashes, and base and advanced events. You get detailed file and device trajectory information and can navigate single events to uncover a larger issue that may be compromising your system.

- https://openedr.com/

Vistumbler

- Vistumbler is a Windows wireless scanner. Vistumbler's main objective is to map and view access points around you using the collected wireless and GPS data.
- https://www.vistumbler.net/

Zeek

- Zeek is not an active security device, like a firewall or intrusion prevention system. Rather, Zeek sits on a “sensor,” a hardware, software, virtual, or cloud platform that quietly and unobtrusively observes network traffic. Zeek interprets what it sees and creates compact, high-fidelity transaction logs, file content, and fully customized output, suitable for manual review on disk or in a more analyst-friendly tool like a security and information event management (SIEM) system.
- https://zeek.org/

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 may be issued.
- https://metron.apache.org/

SIEMonster

- SIEMonster provides both a free SIEM and a paid solution. As is the case for many of the solutions used, the SIEMonster framework offers a centralized tool management interface for data analysis, threatening intelligence and various open source software. Your organization will host it on a cloud, unlike some other open source SIEM solutions.
- https://siemonster.com/

ClamAV

- ClamAV is an open source framework for antivirus mail gateway scanning and is available on Windows, OS X, Linux and BSD applications.
- https://www.clamav.net/

GRR Rapid Response

- The GRR Rapid Response of Google consists of two parts: a GRR client that is deployed to an investigated network and a GRR server that assists analysts in enforcing actions and in processing the data that are gathered.
- https://github.com/google/grr

Cyphon

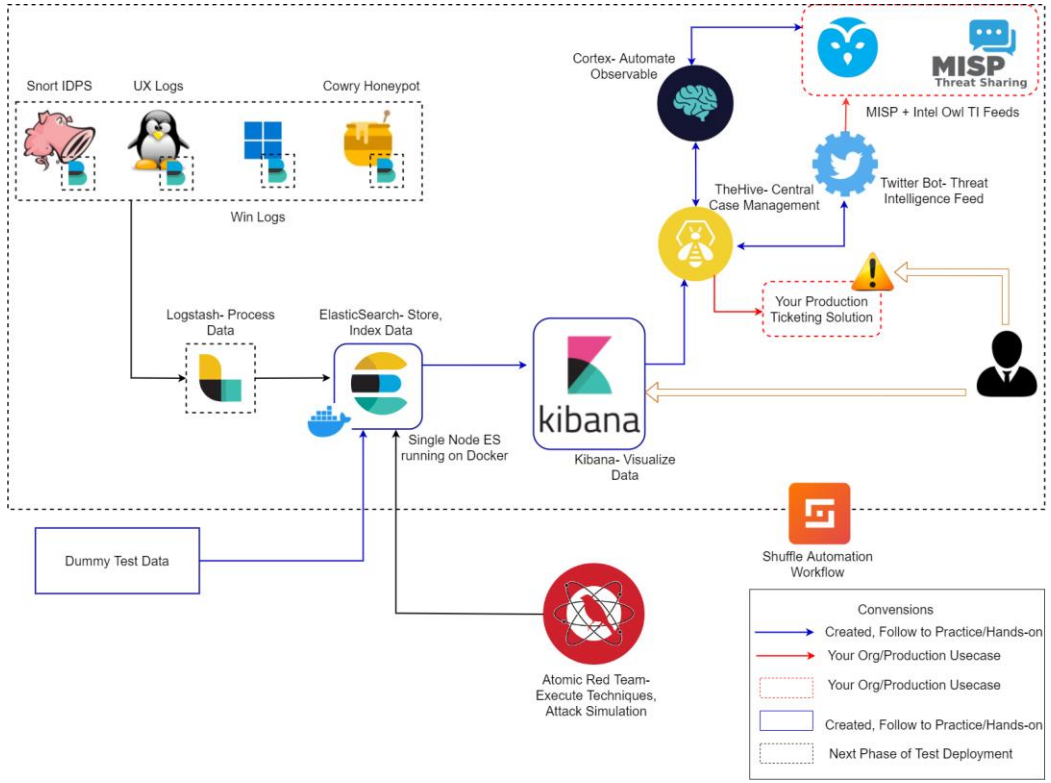
- Cyphon provides resources to capture, process, triage and incidents to analysts. It collects data, such as message logs, APIs which email – which makes it easy to analyze and collect as many or as little details as you want.
- https://www.cyphon.io/

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.
- https://github.com/abhinavbom/Threat-Intelligence-Hunter

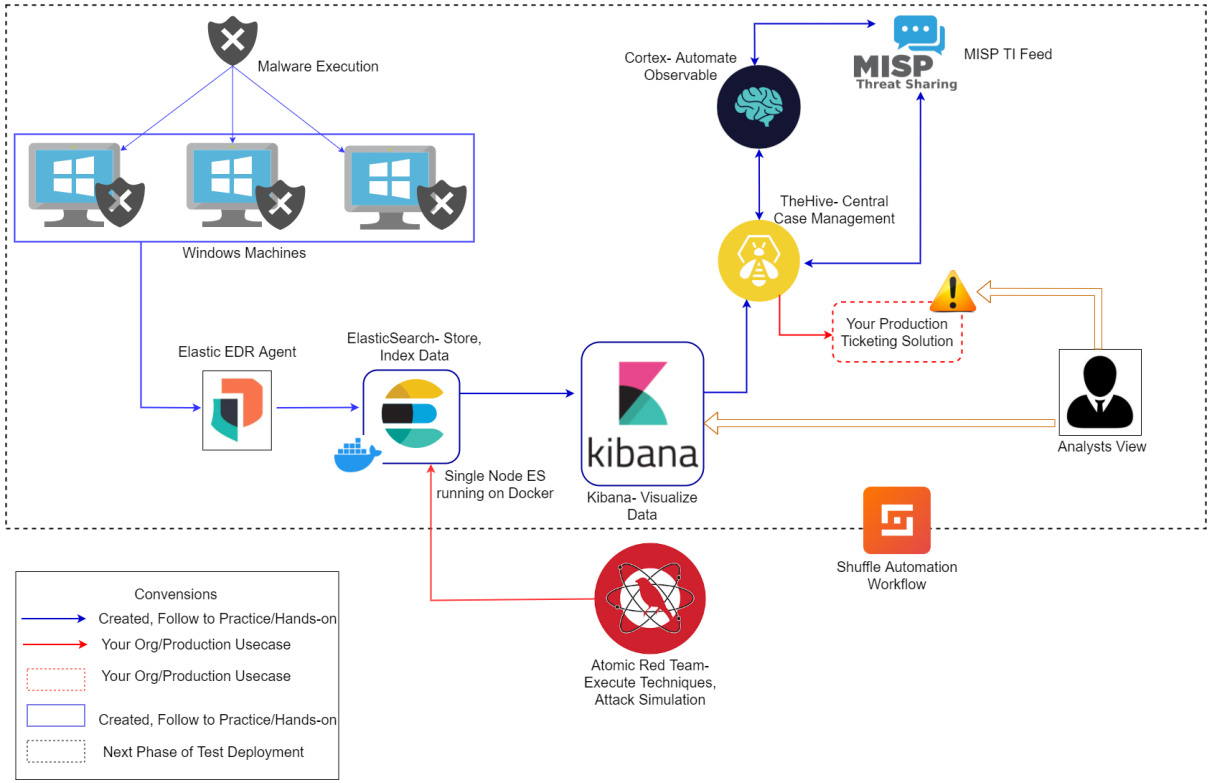
Security Operation Center Architecture

Example Architecture 1



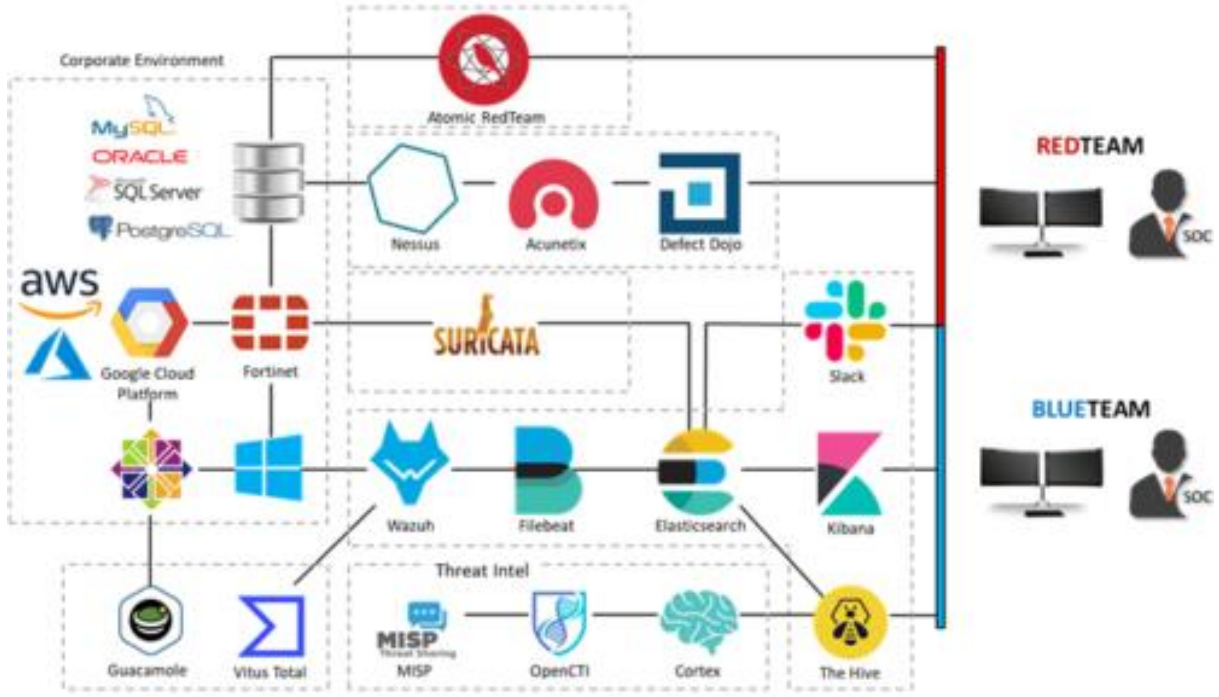
https://github.com/archanchoudhury/SOC-OpenSource

EDR Stack Architecture



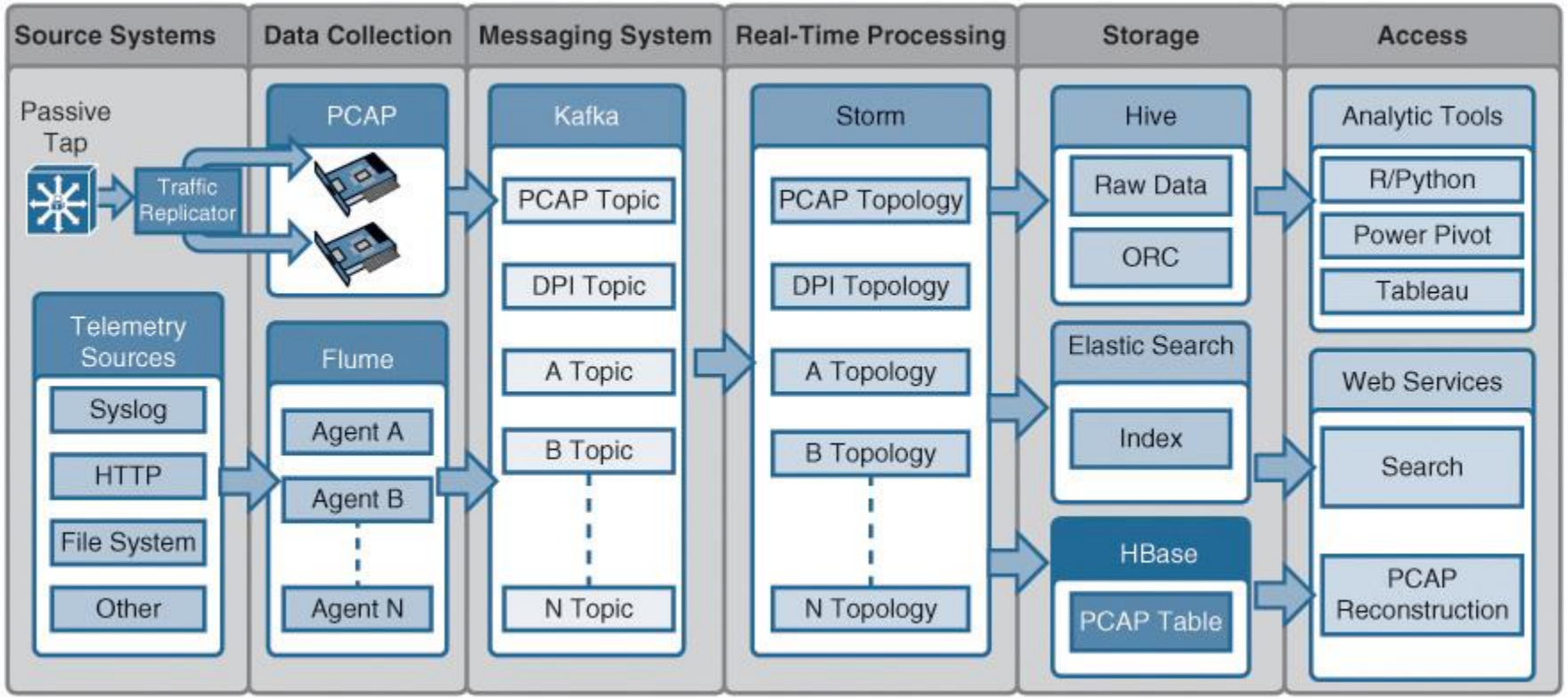
https://github.com/archanchoudhury/SOC-OpenSource

Open Source Threat Management



https://securityfirst.com.br/soc/

OpeN Source SOC

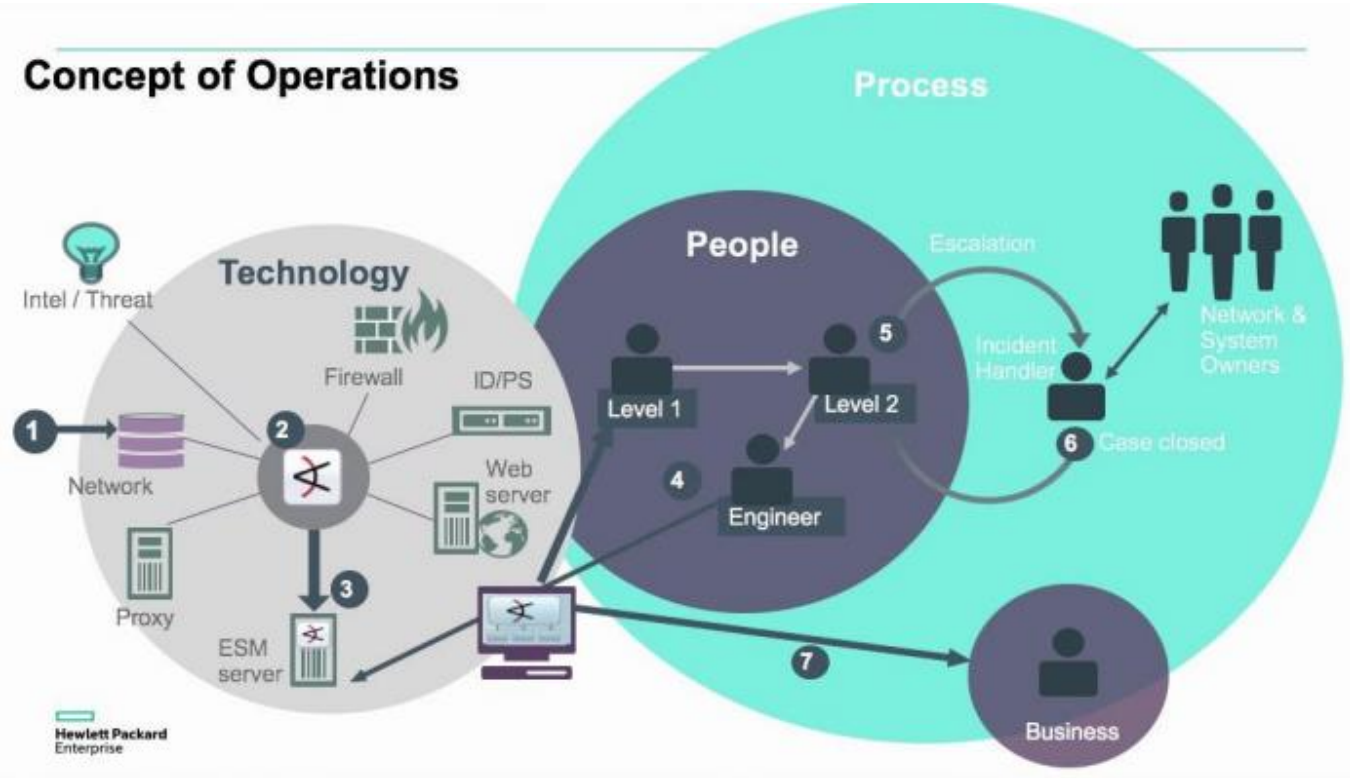


https://www.ciscopress.com/articles/article.asp?p=2455014

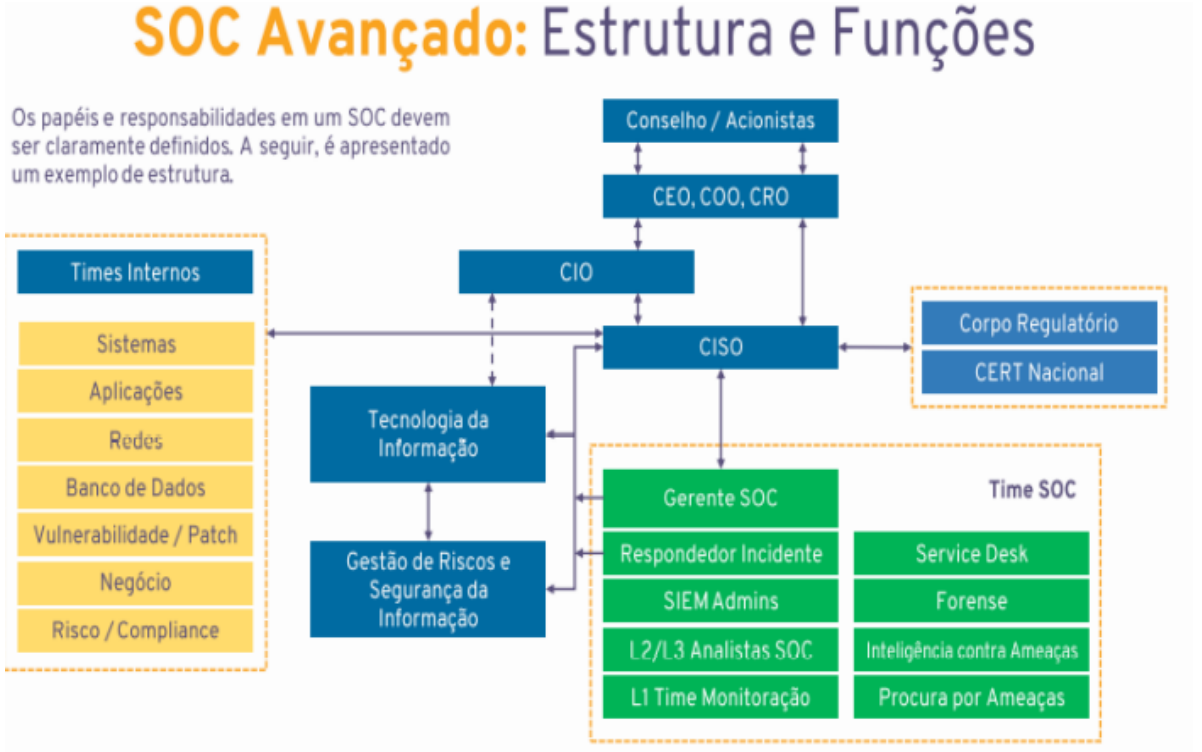
Security Operation Center

https://www.sketchbubble.com/en/presentation-security-operations-center.html

Security Operation Center - Concept

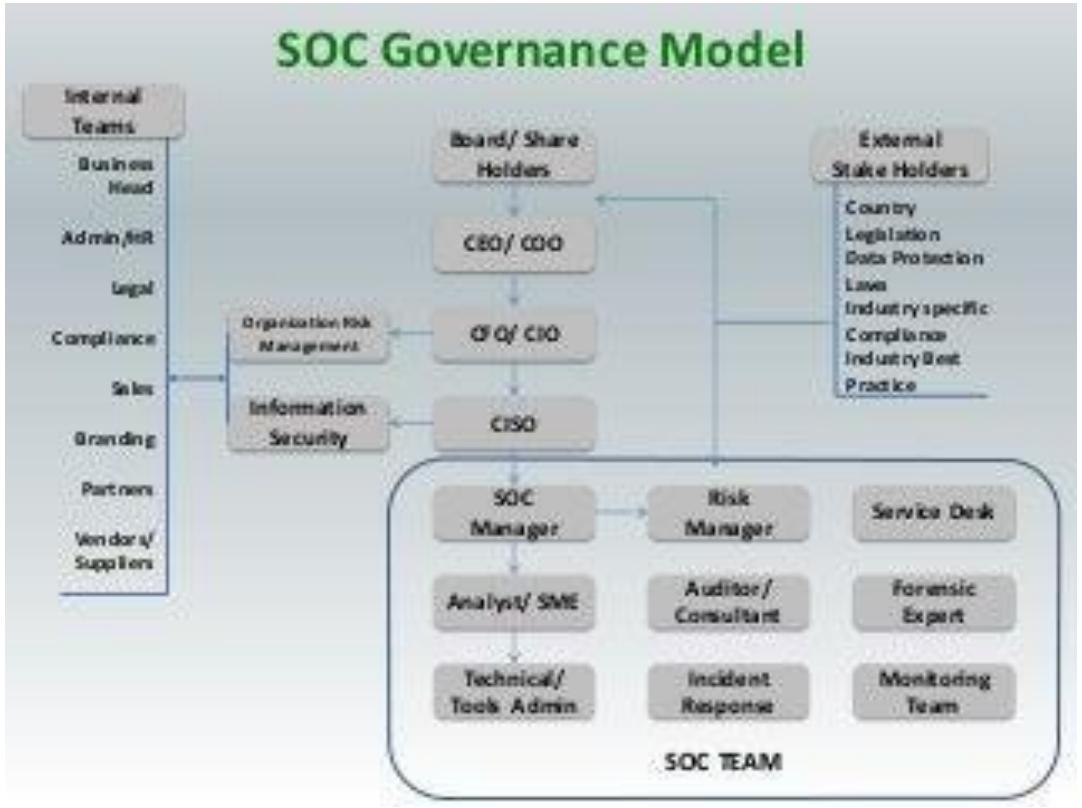


Security Operation Center - Concept

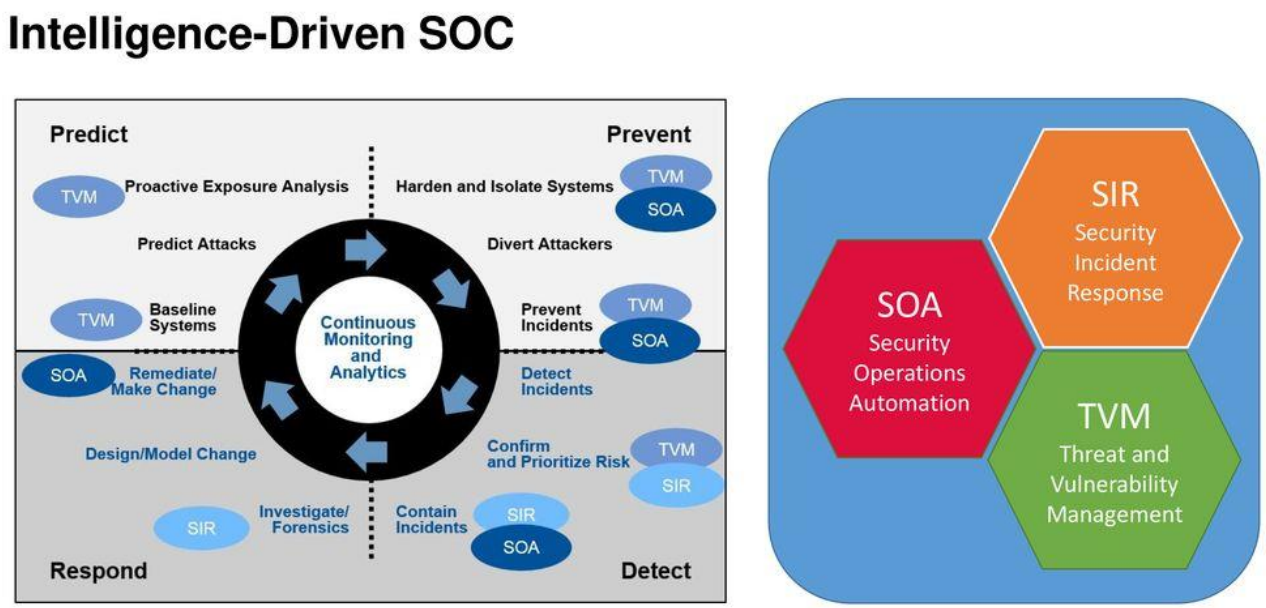


Security Operation Center - Triad

Security Operation Center Governance

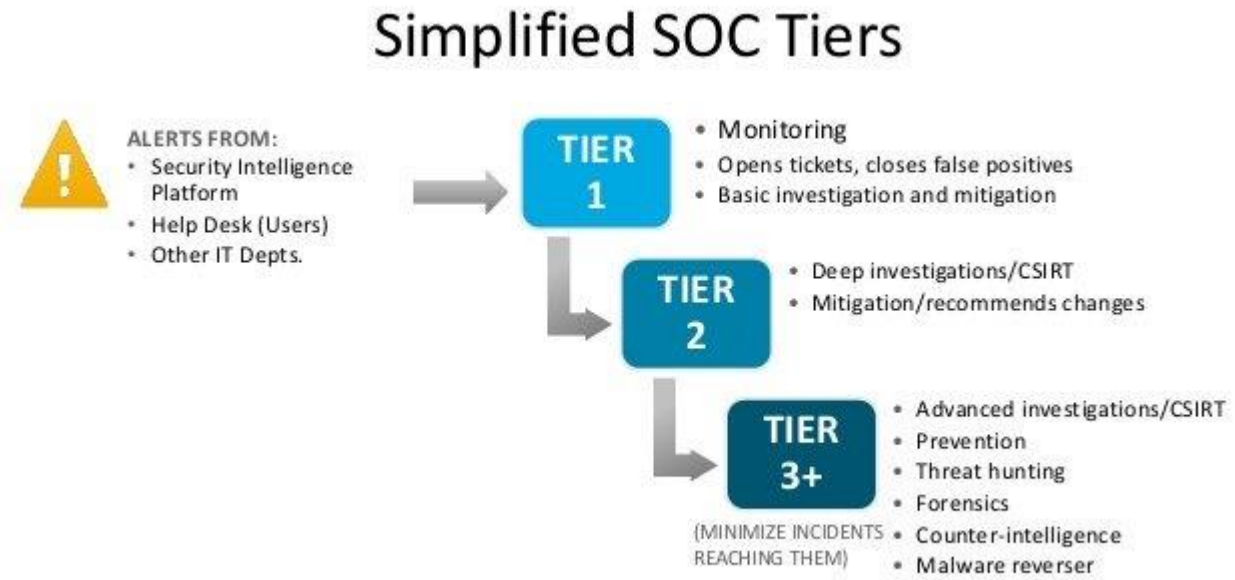


Intelligence-Driven SOC



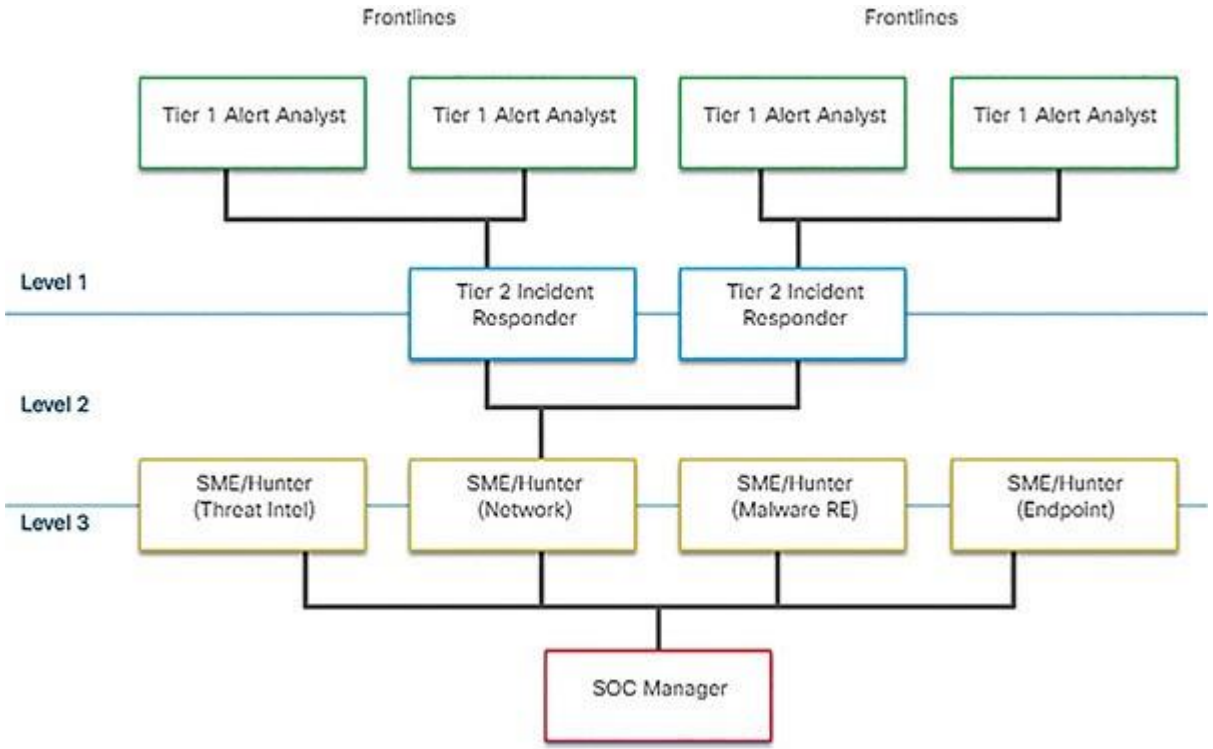
More information: The Five Characteristics of an Intelligence-Driven Security Operations Center, Gartner 2015

SOC Tiers



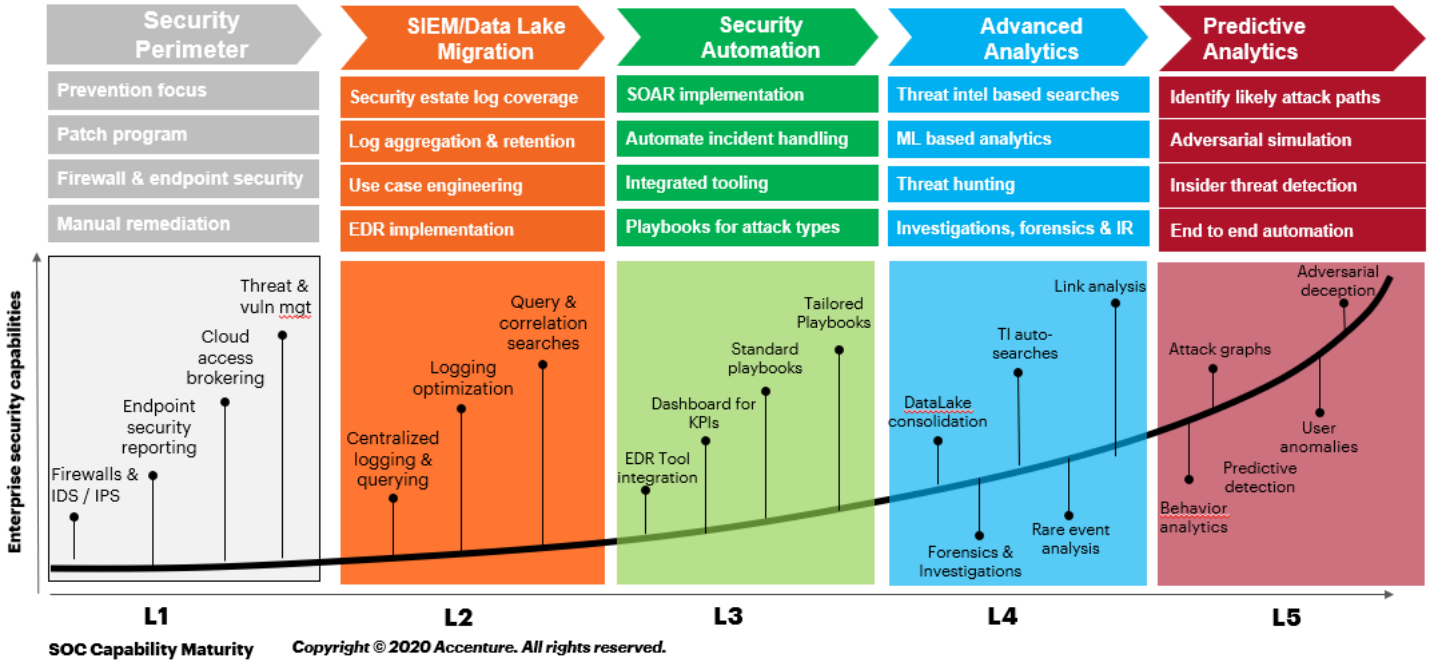
https://gbhackers.com/how-to-build-and-run-a-security-operations-center/

SOC Tiers 2



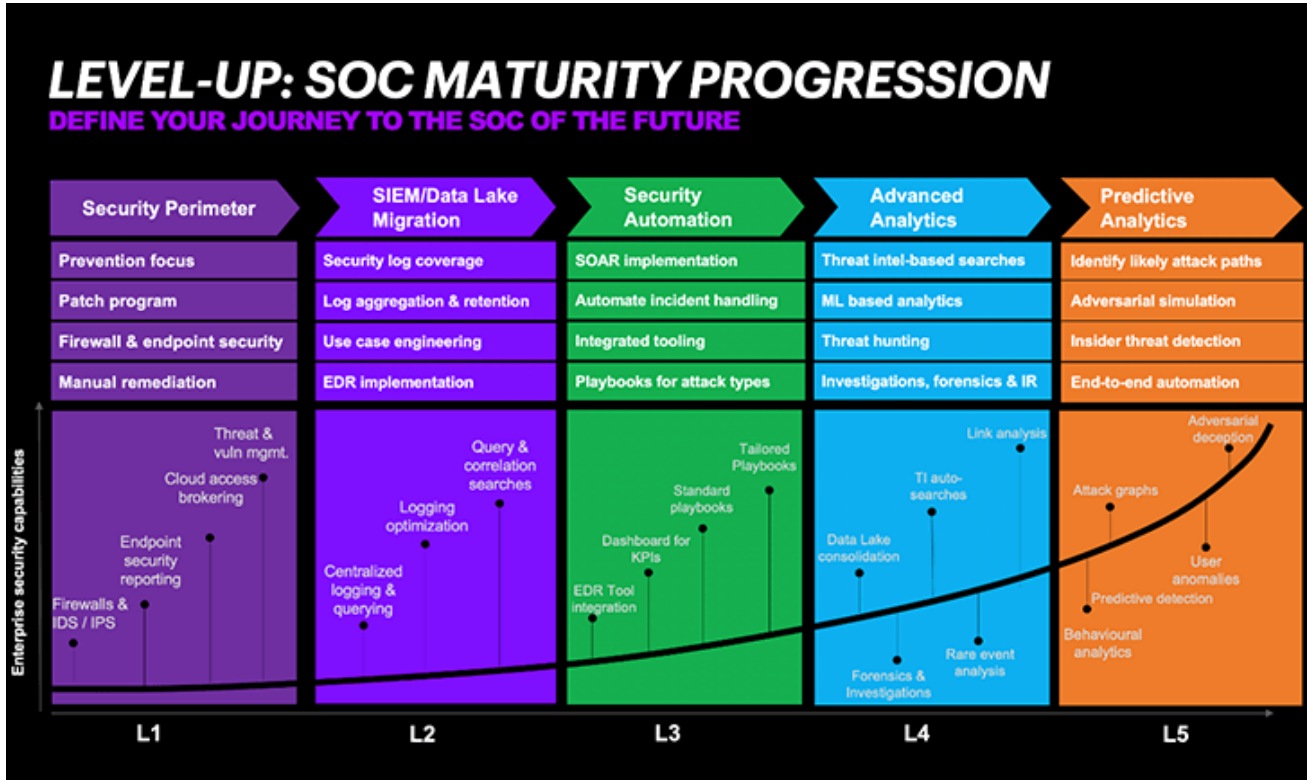
https://medium.com/predict/security-operations-center-soc-e5f47e277a35

SOC Tiers 3



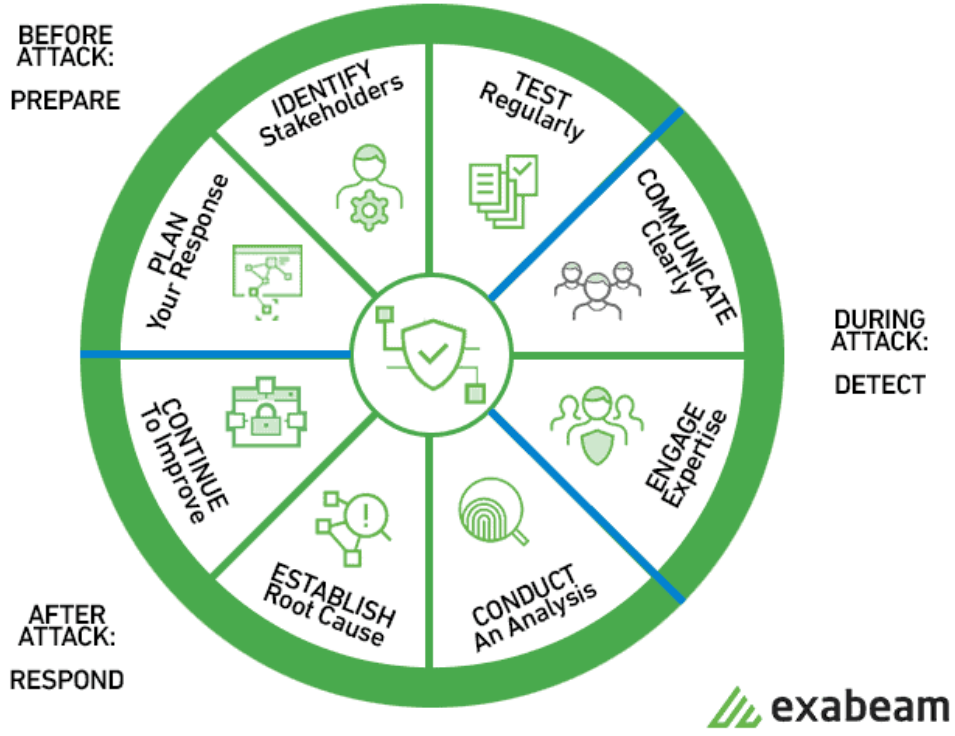
https://www.accenture.com/us-en/blogs/security/level-up-soc-game-one-logical-step-at-a-time

SOC Maturity Progression



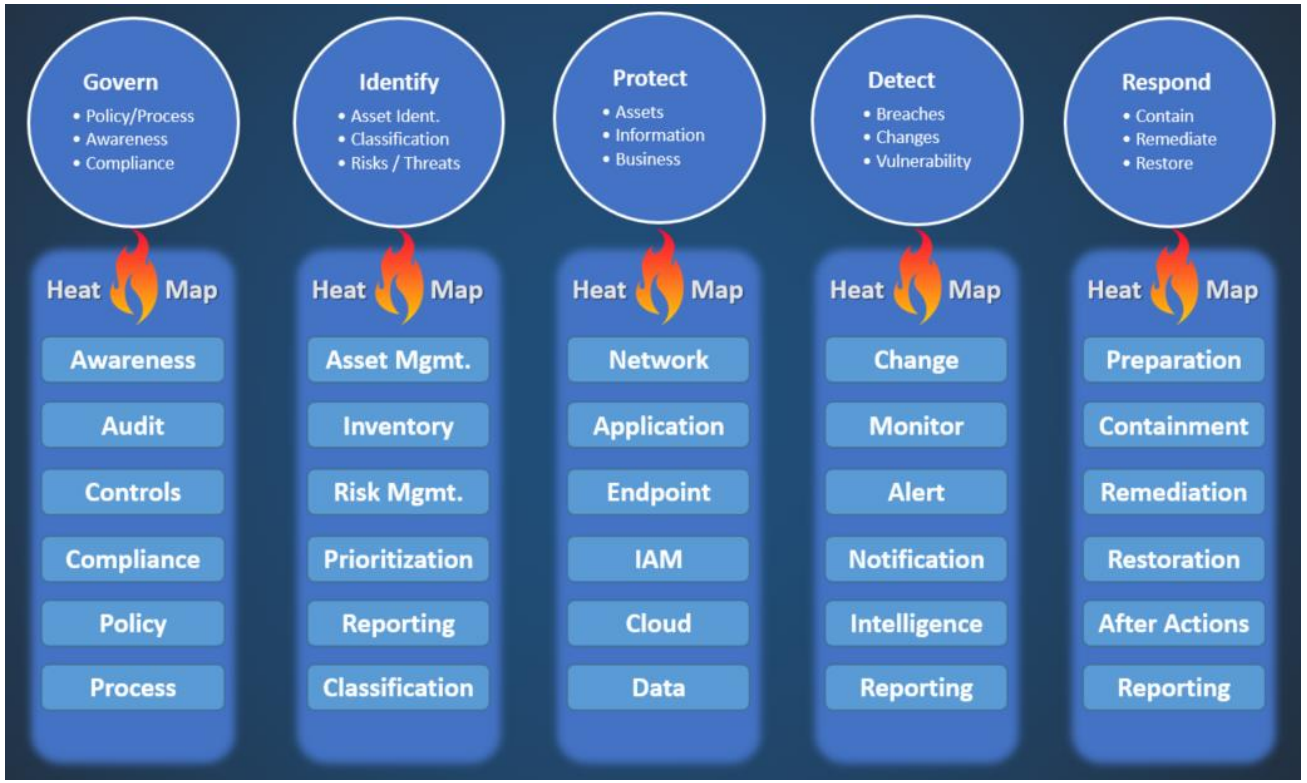
https://www.accenture.com/us-en/blogs/federal-viewpoints/leveling-up-your-cybersecurity-how-agencies-mature-security-programs

Incident Response



https://www.exabeam.com/incident-response/incident-response-plan/

Incident Response Organized



AWESOME!

- https://github.com/fabacab/awesome-cybersecurity-blueteam
- https://github.com/CyberSecurityUP/Awesome-Red-Team-Operations
- https://github.com/infosecn1nja/Red-Teaming-Toolkit
- https://github.com/an4kein/awesome-red-teaming
- https://socradar.io/how-to-build-a-soc-with-open-source-solutions/
- https://github.com/counteractive/incident-response-plan-template/blob/master/playbooks/playbook-ransomware.md
- https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-insightidr-ransomware-playbook.pdf
- https://cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099
- https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
- https://www.atlassian.com/incident-management/incident-response/how-to-create-an-incident-response-playbook
- https://frsecure.com/blog/incident-response-playbooks/
- https://www.youtube.com/watch?v=52HA_Y8A1Zs