

For a SOC

SOC build MITRE, [11 strategies for a world-class SOC](#) (or use [local file](#)): part 0 (Fundamentals).

- FIRST, [Building a SOC](#)
- NCSC, [Building a SOC](#)
- Gartner, [SOC model guide](#)
- Splunk, [State of Security 2023](#)
- Microsoft, [Secure your business with 365](#)
- SOC training/interview:
 - LetsDefend [SOC analyst interview questions](#)
- SOC management:
 - FIRST, [ISO 27035 Practical value for CSIRT and SOCs](#)
 - SANS, [2024 SOC survey](#)
- SOC assessment:
 - CMM, [SOC-CMM](#)
 - Rabobank CDC, [DeTTECT](#)

For a CERT/CSIRT

- CSIRT build:
 - FIRST, [CERT-in-a-box](#)
 - FIRST, [CSIRT Services Framework](#)
- Security incident response management:
 - ENISA, [Good practice for incident management](#)
 - EE-ISAC [Incident Response whitepaper](#)
 - LinkedIn Pulse, [Security incident management according to ISO 27005](#)
 - Microsoft/EY/Edelman, [Incident response reference guide](#)
 - Microsoft, [IR lessons on cloud ID compromise](#)
- Forensics:
 - NIST, [SP800-86, integration forensics techniques into IR](#)
 - [ForensicsArtefacts](#)
- Incident response playbooks:
 - Kaspersky, [Incident Response Playbook: Dark Web Breaches](#)
 - IncidentResponse.org, [IR playbooks](#)
 - SANS, [IR Mitigations tasks](#)

Globally (SOC and CERT/CSIRT)

- Terms and concepts:
 - Shubham, [Security 360](#)

- Vilnius Benetis, [CSIRT, SOC, ISAC and PSIRT definitions](#)
 - Thomas Roccia, [Visual Threat Intelligence](#)
 - SentinelOne, [What is SecOps](#)
 - Purp1eW0lf, [Blue Team Notes](#)
 - PAN, [Security orchestration for dummies](#)
 - ThreatConnect, [SIRP / SOA / TIP benefits](#)
 - Medium, [Compromise assessment methodology](#)
- SOC/CSIRT processes:
 - NIST, [SP800-61 rev3, incident handling guide](#)
- CSIRT build:
 - ENISA, [How to set-up a CSIRT and SOC](#)
- Frameworks and materials:
 - MITRE, [ATT&CK: Getting started](#)
 - NIST, [Cybersecurity framework](#)
 - FIRST, [CVSS v4 specs](#)
 - OASIS Open, [STIX](#)
 - FIRST, [TLP](#) (intelligence sharing and confidentiality), and [PAP](#)
 - CIS, [18 critical security controls](#)
- Security capabilities mappings:
 - CTID, [Mappings explorer](#)
- Threat matrix:
 - Push Security, [SaaS attack matrix](#)
 - Microsoft, [Threat Matrix for Azure Storage services](#)
 - MITRE, [Threat Matrix for AI-systems](#)
- SOAR solutions:
 - Swimlane, [Cyber Threat readiness report 2023](#);
 - Gartner, [Market Guide for Security Orchestration, Automation and Response Solutions](#)
- NIS2:
 - NIS2Directive: [NIS2 10 main requirements](#)
 - LinkedIn: [How will NIS2 impact your organization?](#)
 - CyberArk: [NIS2, how to address the security control gaps](#)
- Management:
 - Gartner, [Cybersecurity business value benchmark](#)
 - Forrester, [Best practices for automating SecOps workflow](#)
 - Microsoft, ["While the initial trigger event was a Distributed Denial-of-Service \(DDoS\) attack... initial investigations suggest that an error in the implementation of our defences amplified the impact of the attack rather than mitigating it"](#)
- SOP (Standard Operating Procedures):
 - [Antimalware check SOP](#)
 - [M365/Azure compromise assessment SOP](#)
 - [Web server compromise assessment](#)

Fundamental concepts

Concepts, tools, missions, attack lifecycle, red/blue/purple teams

MITRE references:

- [11 strategies for a world-class SOC](#), Strategy 5: Prioritize Incident Response, pages 101-123,

Prepare for handling incidents by defining incident categories, response steps, and escalation paths, and codifying those into SOPs and playbooks. Determine the priorities of incidents for the organization and allocate the resources to respond. Execute response with precision and care toward constituency mission and business.

Dedicated page

Cf.: [SOC/CSIRT Basic and fundamental concepts](#).

SOC core

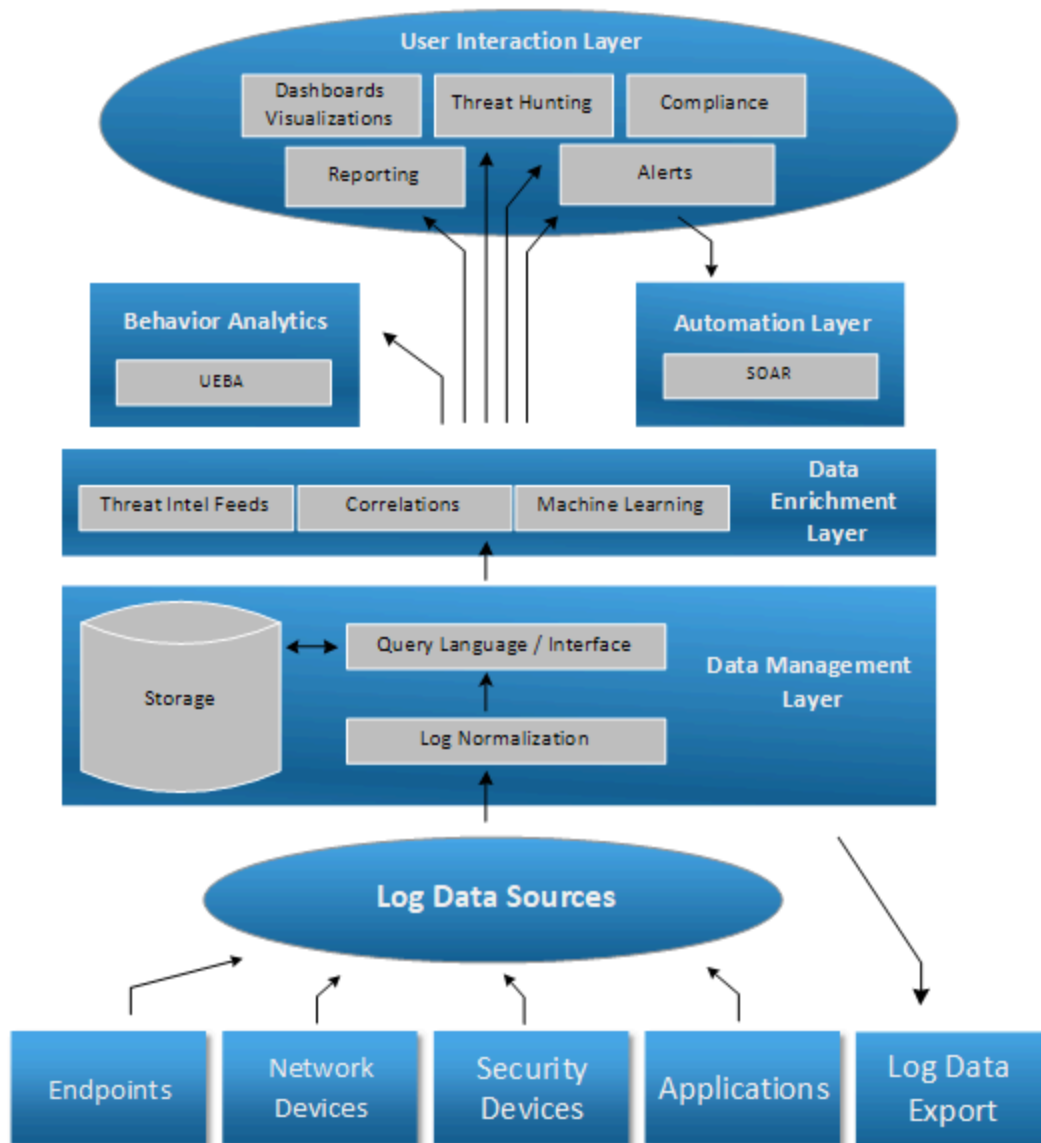
MITRE references:

- [11 strategies for a world-class SOC](#), Strategy 8: Leverage Tools to Support Analyst Workflow, pages 101-123,

Consolidate and harmonize views into tools and data and integrate them to maximize SOC workflow. Consider how the many SOC tools, including SIEM, UEBA, SOAR, and others fit in with the organization's technical landscape, to include cloud and OT environments

From logs to alerts: global generic workflow

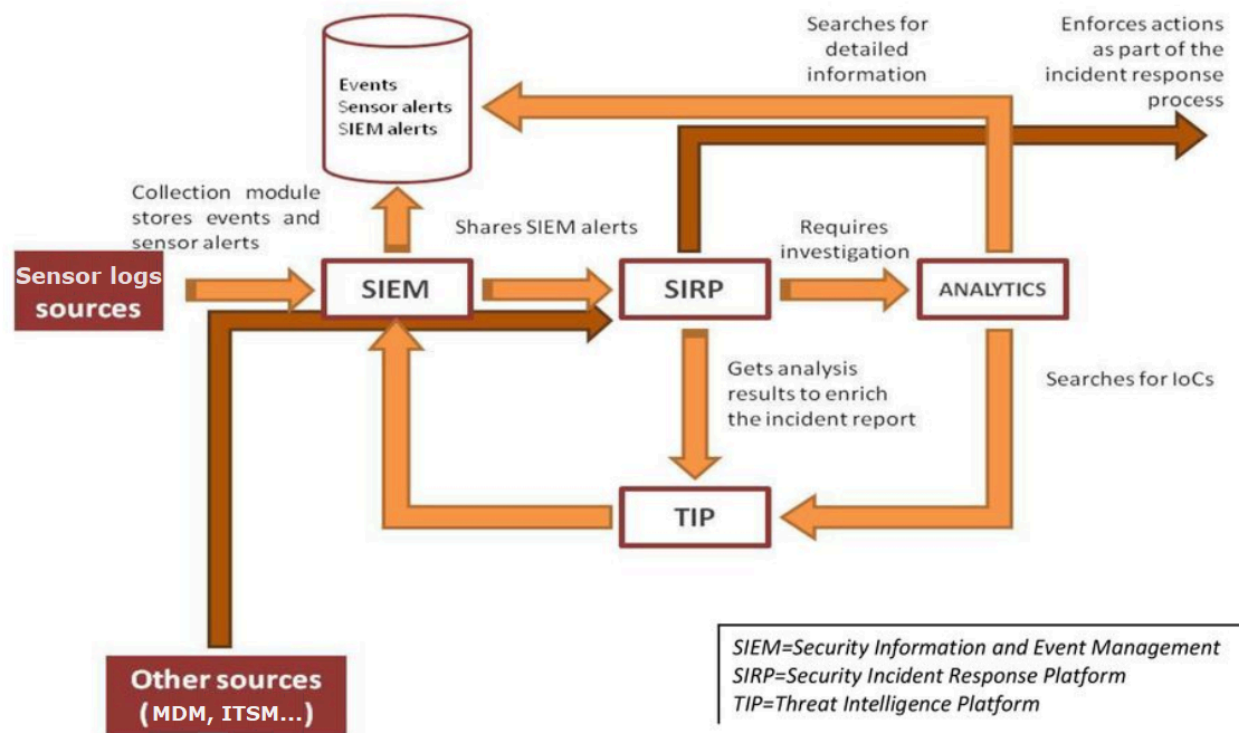
Quoted from [this article](#):



Following the arrows, we go from log data sources to data management layer, to then data enrichment layer (where detection happens), to end-up in behavior analytics or at user interaction layer (alerts, threat hunting...). All of that being enabled and supported by automation.

SOC architecture of detection

Based on [CYRAIL's paper drawing](#), that I've slightly modified, here is an example of architecture of detection (SIEM, SIRP, TIP interconnections) and workflow:



- Sensors log sources are likely to be: audit logs, security sensors (antimalware, FW, NIDS, proxies, EDR, NDR, CASB, identity threat detection, honeypot...).

Mission-critical means (tools/sensors)

MITRE references

- [11 strategies for a world-class SOC](#), Strategy 7: Select and Collect the Right Data, pages 101-123,

Choose data by considering relative value of different data types such as sensor and log data collected by network and host systems, cloud resources, applications, and sensors. Consider the trade-offs of too little data and therefore not having the relevant information available and too much data such that tools and analysts become overwhelmed.

Critical tools for a SOC/CSIRT

- [SIEM](#):
 - See [Gartner magic quadrant](#) and [Gartner critical SIEM capabilities](#)
 - My recommendations: [Microsoft Azure Sentinel](#), [Sekoia.io XDR](#), [Splunk](#), [Graylog](#).

- [SIRP](#):
 - e.g.: [IBM Resilient](#), [TheHive](#), [SwimLane](#), [PAN Cortex XSOAR](#)
 - My recommendations: [TheHive](#), [PAN Cortex XSOAR](#)
- [SOA](#):
 - I recommend to read the SoftwareReview's [SOAR Data quadrant awards](#)
 - e.g. of solutions: [IBM Resilient](#), [SwimLane](#), [TheHive](#), [PAN Cortex XSOAR](#), [Microsoft Logic Apps](#)
 - My recommendations: [SwimLane](#), [TheHive](#), [PAN Cortex XSOAR](#)
- [TIP](#):
 - See [Threat intel page](#)

Critical sensors for a SOC

- Antimalware/antivirus (you may want to have a look at my antivirus vs. EDR comparison):
 - See [Gartner magic quadrant](#) or [Forrester Wave](#)
 - My recommendations: [Microsoft Defender](#), [ESET Nod32](#), [BitDefender](#), [WithSecure Elements EPP](#)
- [Endpoint Detection and Response](#):
 - See [Gartner magic quadrant](#), [MITRE ENGenuity](#), and [Forrester Wave](#)
 - My recommendations: [SentinelOne](#), [Microsoft Defender for Endpoint](#), [Harfanglab](#), [ESET XDR](#), [WithSecure Elements EDR](#), [CrowdStrike Falcon EDR](#), [Tanium](#), [Wazuh](#)
- [Secure Email Gateway](#) (SEG):
 - See [Gartner reviews and ratings](#)
 - My recommendations: [Microsoft Defender for Office365](#), [ProofPoint](#), [Mimecast](#), [WithSecure Elements Collaboration Protection](#)
- [Secure Web Gateway](#) (SWG) / Security Service Edge:
 - see [Forrester wave for SSE](#)
 - My recommendations: [BlueCoat Edge SWG](#), [CISCO SASE](#), [Zscaler Cloud proxy](#), [Netskope](#).
- [Identity Threat Detection and Response](#) (ITDR) for identity and AD/AAD security (audit logs, or specific security monitoring solutions):
 - My recommendations: [Semperis Directory Services Protector](#)
 - for a one-shot security assessment of AD and Entra ID, I recommend: [Semperis Purple Knight](#) or [PingCastle](#)
- EASM: External Asset Security Monitoring / External Attack Surface Management:
 - My recommendations: [Intrinsec \(in French\)](#), [Mandiant](#), [Qualys EASM](#)
 - for a security check-up:
 - quick security assessment of your website: [ImmuniWeb](#)
 - AWS/Azure/GCP security assessment (community tool): [ScootSuite](#)
- CASB: [Cloud Access Security Broker](#), if company's IT environment uses a lot of external services like SaaS/IaaS:
 - See [Gartner magic quadrant](#)

- My recommendations: [Microsoft MCAS](#), [Zscaler](#), [Netskope](#).
- Mobile Threat Defense:
 - See the [latest Forrester Wave about MTD](#)
 - my recommendation : [Zimperium MTD](#)

Critical tools for CSIRT

- Compromise assessment tools:
 - My recommendations:
 - Paid ones:
 - [Thor Cloud lite](#);
 - [WithSecure Elements EDR](#);
 - free ones:
 - for Linux:
 - WithSecure [Cat-Scal](#);
 - [UAC](#);
 - for Windows:
 - simple but efficient ESET [Sysinspector](#);
 - [Velociraptor](#);
 - [DFIR-ORC](#);
 - [Sysmon](#):
 - install it (if not done already, let it run for a few hours/days), with [Olaf Hartong's config](#);
 - then investigate its log with a regular SIEM or with [Zircolite](#)
 - For AD:
 - simple but efficient [ADRecon](#);
 - [Semperis Purple Knight](#);
 - [BloodHound Community](#)
 - For MS Entra ID & M365:
 - [CrowdStrike Reporting Tool for Azure](#)
 - [Semperis Purple Knight](#);
 - [365Inspect](#);
 - [Azure AD Incident Response Powershell](#)
 - For Azure / GCP / AWS:
 - [ScootSuite](#)
- On-demand volatile data collection tool:
 - My recommendations: [FastIR](#), [VARC](#), [FireEye Redline](#), [DFIR-ORC](#);
- Remote action capable tools (ie.: remote shell or equivalent):
 - My recommendations: [CIMSweep](#), [Velociraptor](#), [CrowdStrike Falcon Toolkit](#) but it relies on CrowdStrike EDR, [GRR](#) but it needs an agent to be installed.
- On-demand sandbox:
 - My recommendations for online ones: [Joe's sandbox](#), [Hybrid Analysis](#), etc;
 - My recommendation for local one: Windows 10 native Sandbox, with [automation](#).

- Forensics and reverse-engineering tools suite:
 - My recommendations: [SIFT Workstation](#), or [Tsurugi](#);
 - My recommendation for reverse engineering and malware analysis, under Windows: [FireEye Flare-VM](#);
 - My recommendation for pure malware analysis, under Linux: [Remnux](#).
- Incident management tracker:
 - My recommendations: [Timesketch](#), [DFIR IRIS](#)
- Scanners:
 - IOC scanners:
 - My recommendations: [Loki](#), [DFIR-ORC](#)
 - For smartphones: [Tiny Check](#)
 - IOC repos for scanners:
 - Google [CTI's repo](#): Yara rules for Cobalt Strike and others.
 - [Yara-rules GitHub repo](#): multiple Yara rules types.
 - Spectre [Yara rules repo](#)
 - Neo23x0 [Community Yara rules](#)
 - and those listed here, [Awesome threat intel](#)
 - Offline antimalware scanners:
 - My recommendation: [Windows Defender Offline](#), [ESET SysRecue](#)
- Logs analyzers with detection capabilities:
 - My recommendations:
 - Paid ones: [Sekoia XDR](#),
 - Community-provided / free ones: [Zircolite](#), [DeepBlue](#), [CrowdSec](#)

Other critical tools for a SOC and a CERT/CSIRT

- Secure secrets sharing:
 - [OneTimeSecret](#)
- Data analysis tools:
 - My recommendations: [CyberChef](#), [Notepad++](#)
- Admin tools:
 - My recommendations for (free) admin tools: [Azure AD Internals suite](#), [SysInternals Suite](#), [MRemoteNG](#)
 - My recommendations for (free) remote deployment tools: [EMCO Remote installer](#)
- Internal ticketing system (NB: not SIRP, not for incident response!):
 - My recommendation: [GitLab](#)
- Knowledge sharing and management tool:
 - My recommendations: [Microsoft SharePoint](#), Wiki (choose the one you prefer, or [use GitLab as a Wiki](#)).
- Visualization tool for OSINT search and IOC:
 - My recommendation: [OSINTTracker](#)

IT/security Watch

MITRE reference

- [11 strategies for a world-class SOC](#), Strategy 6: Illuminate Adversaries with Cyber Threat Intelligence, pages 101-123,

Tailor the collection and use of cyber threat intelligence by analyzing the intersection of adversary information, organization relevancy, and technical environment to prioritize defenses, monitoring, and other actions.

Recommended sources

- SIEM rules publications:
 - [Sigma HQ \(detection rules\)](#)
 - [Splunk Security content \(free detection rules for Splunk\)](#)
 - [SOC Prime](#)
 - [Michel De Crevoisier's Git](#)
- Known exploited vulnerabilities +0days:
 - [CISA catalog](#)
 - [CVETrends](#)
 - [Top 0days "in the wild"](#)
- LinkedIn / Twitter:
 - e.g.: [LinkedIn Information Security Community group](#)
- RSS reader/portal:
 - e.g.: [Netvibes](#)
- Government CERT, industry sector related CERT...
 - e.g.: [CERT-FR](#), [CERT-US](#)
- Newsletters:
 - e.g.: [TheRecord.media](#), [Intrinsec Threat Landscape](#)
- Podcasts:
 - WithSecure [Xposed](#)
- Other interesting websites:
 - e.g.: [ISC](#), [ENISA](#), [ThreatPost](#) ...

SOAR

MITRE references

- [11 strategies for a world-class SOC](#), Strategy 8: Leverage Tools to Support Analyst Workflow, pages 101-123,

Consolidate and harmonize views into tools and data and integrate them to maximize SOC workflow. Consider how the many SOC tools, including SIEM, UEBA, SOAR, and others fit in with the organization's technical landscape, to include cloud and OT environments.

Dedicated page

Cf. [SOAR page](#)

Detection engineering

MITRE reference

- [11 strategies for a world-class SOC](#), Strategy 1: Know What You Are Protecting and Why, pages 101-123,

Develop situational awareness through understanding the mission; legal regulatory environment; technical and data environment; user, user behaviors and service interactions; and the threat. Prioritize gaining insights into critical systems and data and iterate understanding over time.

- [11 strategies for a world-class SOC](#), Strategy 7: Select and Collect the Right Data, pages 101-123,

Choose data by considering relative value of different data types such as sensor and log data collected by network and host systems, cloud resources, applications, and sensors. Consider the trade-offs of too little data and therefore not having the relevant information available and too much data such that tools and analysts become overwhelmed.

- [11 strategies for a world-class SOC](#), Strategy 11: Turn up the Volume by Expanding SOC Functionality, pages 101-123,

Enhance SOC activities to include threat hunting, red teaming, deception, malware analysis, forensics, and/or tabletop exercises, once incident response is mature. Any of these can improve the SOC's operating ability and increase the likelihood of finding more sophisticated adversaries.

Dedicated page

Cf. [detection engineering page](#).

Threat intelligence

MITRE reference

- [11 strategies for a world-class SOC](#), Strategy 6: Illuminate Adversaries with Cyber Threat Intelligence, pages 101-123,

Tailor the collection and use of cyber threat intelligence by analyzing the intersection of adversary information, organization relevancy, and technical environment to prioritize defenses, monitoring, and other actions.

Dedicated page

Cf. [threat intelligence page](#).

Management

MITRE reference

- [11 strategies for a world-class SOC](#), Strategy 1: Know What You Are Protecting and Why, pages 101-123

Develop situational awareness through understanding the mission; legal regulatory environment; technical and data environment; user, user behaviors and service interactions; and the threat. Prioritize gaining insights into critical systems and data and iterate understanding over time.

- [11 strategies for a world-class SOC](#), Strategy 3: Build a SOC Structure to Match Your Organizational Needs, pages 101-123

Structure SOC by considering the constituency, SOC functions and responsibilities, service availability, and any operational efficiencies gained by selecting one construct over another

- [11 strategies for a world-class SOC](#), Strategy 9: Communicate Clearly, Collaborate Often, Share Generously, pages 101-123

Engage within the SOC, with stakeholders and constituents, and with the broader cyber community to evolve capabilities and contribute to the overall security of the broader community.

- [11 strategies for a world-class SOC](#), Strategy 10: Measure Performance to Improve Performance, pages 101-123

Determine qualitative and quantitative measures to know what is working well, and where to improve. A SOC metrics program includes business objectives, data sources and collection, data synthesis, reporting, and decision-making and action

- [11 strategies for a world-class SOC](#), Strategy 11: Turn up the Volume by Expanding SOC Functionality, pages 101-123

Enhance SOC activities to include threat hunting, red teaming, deception, malware analysis, forensics, and/or tabletop exercises, once incident response is mature. Any of these can improve the SOC's operating ability and increase the likelihood of finding more sophisticated adversaries.

Dedicated page

Cf. [management page](#).

HR and training

MITRE reference

- [11 strategies for a world-class SOC](#), Strategy 4: Hire AND Grow Quality Staff, pages 101-123

Create an environment to attract the right people and encourage them to stay through career progression opportunities and great culture and operating environment. Plan for turnover and build a pipeline to hire. Consider how many personnel are needed for the different SOC functions.

Dedicated page

Cf. [HR and training page](#).

IT achitecture of a SOC

Have a single and centralized platform ('single console')

As per [NCSC website](#):

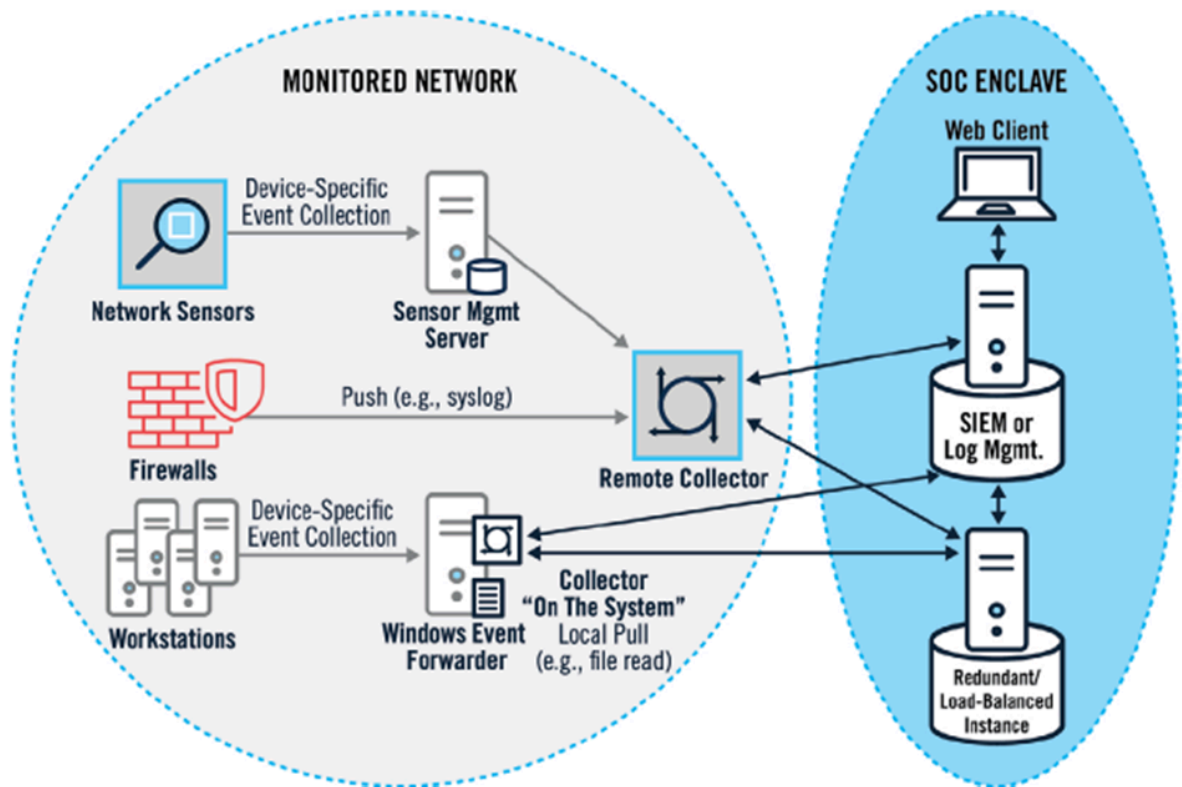
Indications of an attack will rarely be isolated events on a single system component or system. So, where possible, having a single platform where analysts have the ability to see and query log data from all of your onboarded systems is invaluable. Having access to the log data from multiple (or all) components, will enable analysts to look for evidence of attack across an estate and create detection use-cases that utilise a multitude of sources. By creating temporal (actions over a period of time) and spatial (actions across the estate) use-cases, an organisation is better prepared to address cyber security attacks that occur system wide.

Disconnect (as much as possible) SOC from monitored environment

The goal is to prevent an attacker from achieving lateral movement from a compromised monitored zone, to the SOC/CSIRT work zone.

Enclave:

- Implement SOC enclave (with network isolation), as per MITRE paper drawing:



- only log collectors and WEF should be authorized to send data to the SOC/CSIRT enclave. Whenever possible, the SOC tools pull the data from the monitored environment, and not the contrary;
 - on top of a SOC enclave, implement at least a [level 2 of network segmentation](#);
- SOC's assets should be part of a separate [restricted AD forest](#), to allow AD isolation with the rest of the monitored AD domains.

Endpoints hardening:

- SOC/CSIRT's endpoints should be hardened with relevant guidelines;
 - My recommendations: [CIS benchmarks](#), [Microsoft Security Compliance Toolkit](#)

To go further

Must read

- MITRE, [11 strategies for a world-class SOC \(remaining of PDF\)](#)
- CISA, [Cyber Defense Incident Responder role](#)
- FireEye, [Purple Team Assessment](#)

- Kaspersky, [AV / EP / EPP / EDR / XDR](#)
- Wavestone, [Security bastion \(PAM\) and Active Directory tiering mode: how to reconcile the two paradigms?](#)
- MalAPI, [list of Windows API and their potential use in offensive security](#)
- FireEye, [OpenIOC format](#)
- Herman Slatman, [Awesome Threat Intel](#)
- Microsoft, [SOC/IR hierarchy of needs](#)
- Betaalvereniging, [TaHiTI \(threat hunting methodology\)](#)
- ANSSI (FR), [EBIOS RM methodology](#)
- GMU, [Improving Social Maturity of Cybersecurity Incident Response Teams](#)
- J0hnbX, [RedTeam resources](#)
- Fabacab, [Awesome CyberSecurity BlueTeam](#)
- Microsoft, [Windows 10 and Windows Server 2016 security auditing and monitoring reference](#).
- iDNA, [how to manage FP in a SOC?](#), in FR
- Soufiane Tahiri, [Playbook for ransomware incident response](#), in FR
- PwnDefend, [AD post-compromise checklist](#)
- Gartner, [Market guide for NDR](#)
- Rawsec, [Resources inventory](#)
- Quest, [Best practices for AD disaster recovery](#)
- Microsoft, [Isolate Tier 0 assets with group policy](#)
- Securenvoy, [How to be compliant with NIS2?](#)
- CyberVigilance, [Mitre Engenuity Evaluations 2022 review](#)

Nice to read

- NIST, [SP800-53 rev5 \(Security and Privacy Controls for Information Systems and Organizations\)](#)
- Amazon, [AWS Security Fundamentals](#)
- Microsoft, [PAW Microsoft](#)
- CIS, [Business Impact Assessment](#)
- Abdessabour Boukari, [RACI template \(in French\)](#)
- Trellix, [XDR Gartner market guide](#)
- Elastic, [BEATS agents](#)
- [V1D1AN's Drawing: architecture of detection](#),
- [RFC2350](#) (CERT description)
- [Awesome Security Resources](#)
- [Incident Response & Computer Forensics, 3rd ed](#)
- [GDPR cybersecurity implications \(in French\)](#)
- [SANS SOC survey 2022](#)
- Soufiane Tahiri, [Digital Forensics Incident Response Git](#)
- Austin Songer, [Incident playbook](#)
- CISA, [Cybersecurity incident and vulnerability response playbooks](#)
- Reprise99, [Microsoft Sentinel queries](#)

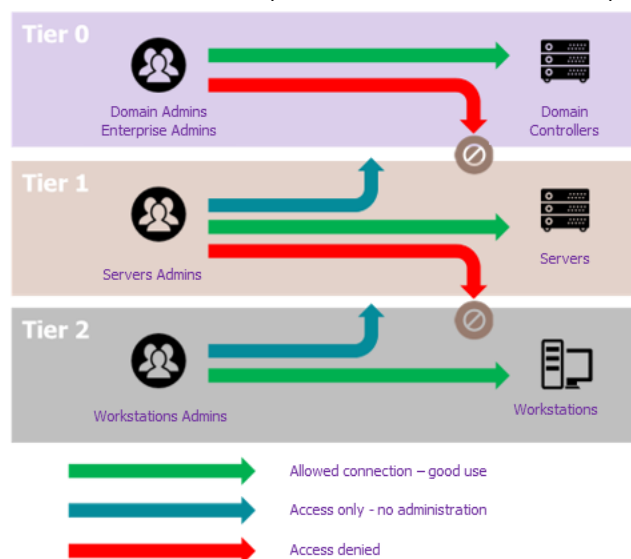
- MyFaberSecurity, [MS Sentinel architecture and recommendations for MSSP](#)
- Gartner, [PAM Magic Quadrant reprint](#)
- Rawsec, [Tools inventory](#)
- Microsoft, [command line reference](#)
- Microsoft, [Sentinel data collection scenarios](#)
- SOC CMM, [SOCTOM](#)
- [PTES](#)
- OWASP, [WSTG](#)
- BitDefender, [Analyzing MITRE ATT&CK evaluations 2023](#)
- Microsoft, [Licensing maps, eg. for Defender](#)

SOC sensors, nice to have

- Dark Web monitoring (data leaks, etc.)
 - My recommendation: [AIL Framework](#)
 - for paid SaaS solutions, I recommend to have a look at this [top 10](#)
- Deceptive technology:
 - My recommendation: implement [AD decoy accounts](#) and [AD DNS canary](#)
- WAF for internet-facing websites/apps:
 - My recommendations:
 - FOSS: [Crowdsec WAF](#), [Bunkerweb](#)
 - paid but good price: [CloudFlare](#)
- MDM:
 - My recommendation: [Microsoft Intune](#)
- (full-featured) Honeypot:
 - My recommendation: [Canary.tools](#)
 - Or, have a look at [Awesome honeypots Git](#)
- Phishing and brand infringement protection (domain names):
 - My recommendation: [PhishLabs](#), [Netcraft](#)
- NIDS:
 - My recommendation: [Crowdsec](#)
- NDR:
 - My recommendation: [Gatewatcher](#)
- DLP:
 - See [Gartner reviews and ratings](#)
- OT (industrial) NIDS:
 - My recommendation: [Nozomi Guardian](#)
- Network TAP:
 - My recommendation: [Gigamon](#)
- Mobile network security (2G/3G):
 - My recommendation: Dust Mobile.

Harden SOC/CSIRT environment

- Implement hardening measures on SOC workstations, servers, and IT services that are used (if possible).
 - e.g.: [CIS](#), [Microsoft Security Compliance Toolkit](#)
- Put the SOC assets in a separate AD forest, as [forest is the AD security boundary](#), for isolation purposes, in case of a global enterprise's IT compromise
- Create/provide a disaster recovery plan for the SOC assets and resources.
- Implement admin bastions and silo to administrate the SOC env (equipments, servers, endpoints):
 - My advice: consider the SOC environment as to be administrated by Tier 1, if possible with a dedicated admin bastion. Here is a generic drawing from Wavestone's article (see Must read references):



- Recommended technology choices: [Wallix PAM](#)
- Implement a [level 3 of network segmentation](#)
- You may want to use throwable machines (virtual machines) for incident response or specific artefacts analysis. Here are my recommendations:
 - [Microsoft Developer virtual machines](#);
 - Hardening [script](#);
 - If needed, [Flare-VM](#) framework to automate tools installation;