Awesome SOC

A collection of sources of documentation, and field best practices, to build and run a SOC (including CSIRT).

Those are my view, based on my own experience as SOC/CSIRT analyst and team manager, as well as well-known papers. Focus is more on SOC than on CERT/CSIRT.

My motto is: without reaction (response), detection is useless.

NB: Generally speaking, SOC here refers to detection activity, and CERT/CSIRT to incident response activity. CERT is a well-known (formerly) US trademark, run by CERT-CC, but I prefer the term CSIRT.

Table of Content

Must read

For a SOC

- MITRE, 11 strategies for a world-class SOC (or use local file): part 0 (Fundamentals).
- CMM, SOC-CMM
- LetsDefend SOC analyst interview questions
- FIRST, Building a SOC
- Gartner, SOC model guide
- NCSC, Building a SOC
- Splunk, State of Security 2023
- Rabobank CDC, DeTTECT

For a CERT/CSIRT

- FIRST, CERT-in-a-box
- FIRST, CSIRT Services Framework
- ENISA, Good practice for incident management
- EE-ISAC Incident Response whitepaper
- NIST, SP800-86, integration forensics techniques into IR
- Microsoft/EY/Edelman, Incident response reference guide

Globally (SOC and CERT/CSIRT)

- SentinelOne, What is SecOps
- Shubham, Security 360
- NIST, Cybersecurity framework
- ENISA, How to set-up a CSIRT and SOC
- NIST, SP800-61 rev2, incident handling guide
- MITRE, ATT&CK: Getting started
- Purp1eW0lf, Blue Team Notes
- ThreatConnect, SIRP / SOA / TIP benefits
- Gartner, Market Guide for Security Orchestration, Automation and Response Solutions
- PAN, Security orchestration for dummies
- FIRST, CVSS v3.1 specs
- OASIS Open, STIX
- FIRST, TLP (intelligence sharing and confidentiality)

- CIS, 18 critical security controls
- Gartner, Cybersecurity business value benchmark
- CyberArk: NIS2, how to address the security control gaps

Fundamental concepts

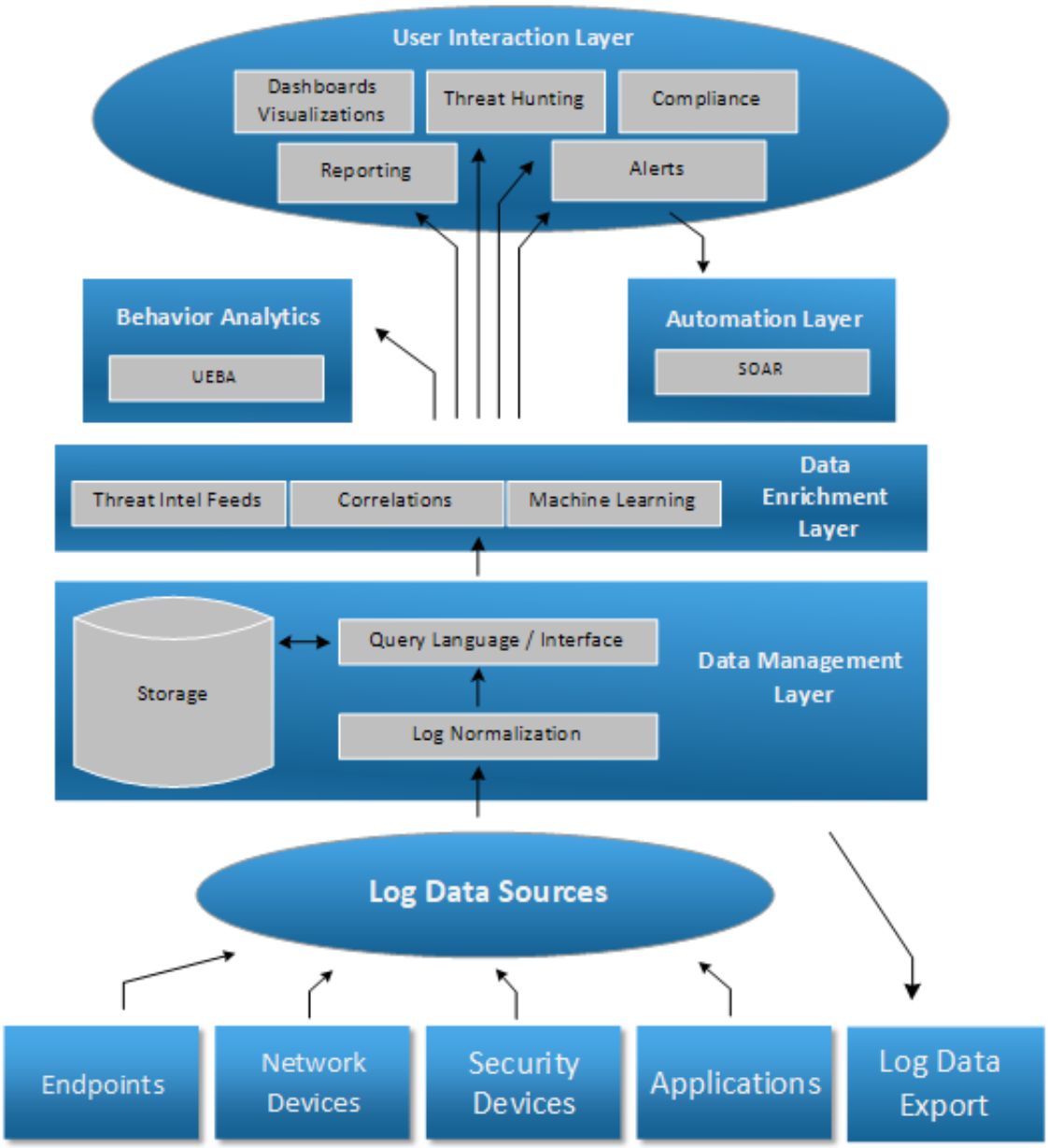
Concepts, tools, missions, attack lifecycle, red/blue/purple teams

See: SOC/CSIRT Basic and fundamental concepts.

SOC and CSIRT core

From logs to alerts: global generic workflow

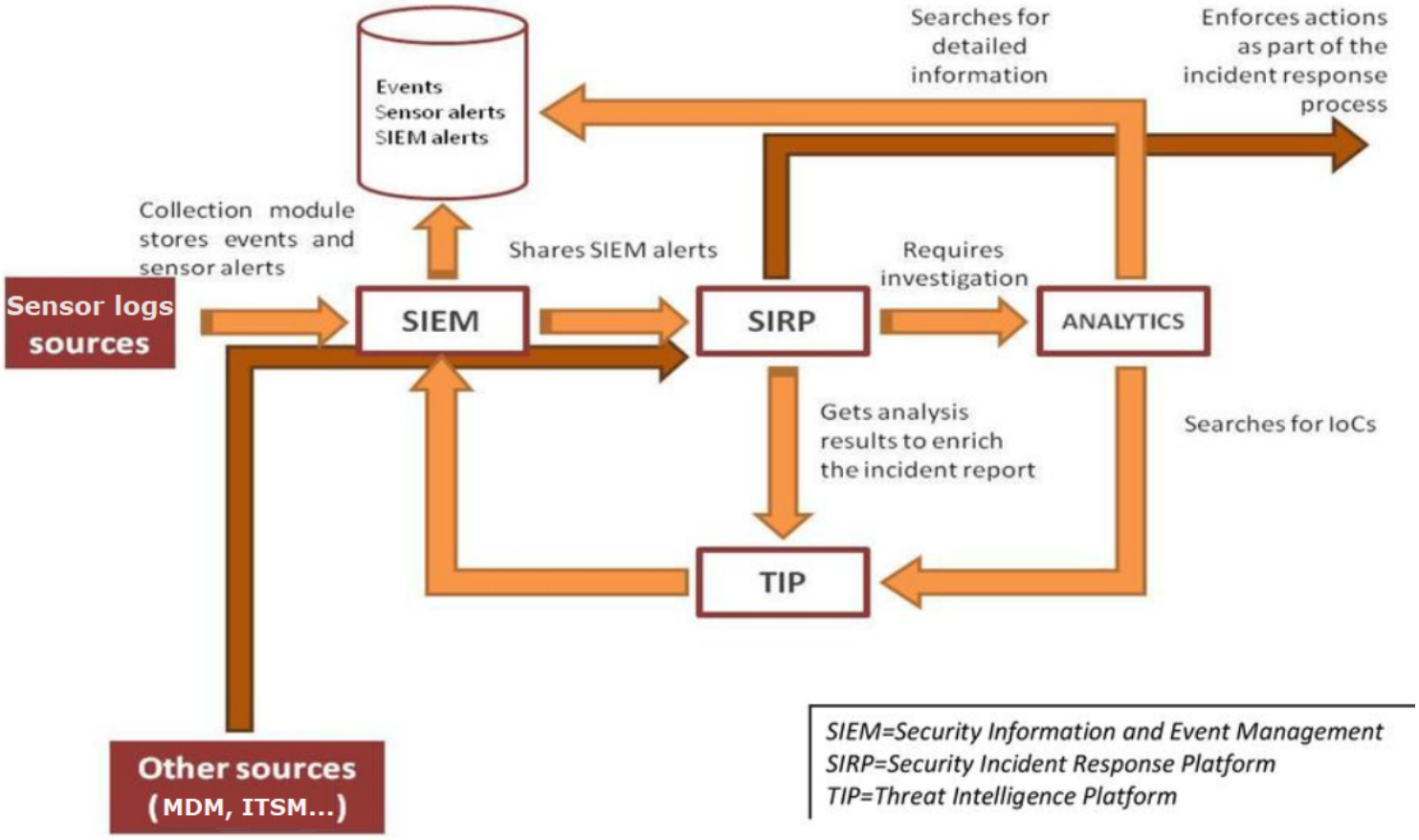
Quoted from this article:



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/CSIRT 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)

Critical tools for a SOC/CSIRT

- **SIEM**:
  - See Gartner magic quadrant
  - My recommendations: Microsoft Azure Sentinel, Sekoia.io XDR, Splunk.
- **SIRP**:
  - e.g.: IBM Resilient, TheHive, SwimLane, PAN Cortex XSOAR
  - My recommendations: TheHive, PAN Cortex XSOAR
- **SOA**:
  - e.g.: 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 and EDR differences table):
    - See Gartner magic quadrant
    - My recommendations: Microsoft Defender, ESET Nod32, BitDefender.
- **Endpoint Detection and Response**:
    - See Gartner magic quadrant and MITRE ENGENUITY
    - 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
- **Secure Web Gateway** (SWG) / Security Service Edge:
    - see Gartner magic quadrant
    - My recommendations: BlueCoat, CISCO, Zscaler, 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, I recommend: Semperis or PingCastle
- **EASM**: External Asset Security Monitoring / External Attack Surface Management:
    - My recommendations: Intrinsec (in French), Mandiant, Microsoft 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.
- **Deceptive technology:**
    - My recommendation: implement AD decoy acounts and AD DNS canary

Critical tools for CSIRT

- On-demand volatile data collection tool:
  - My recommendations: VARC, DFIR-ORC, FireEye Redline, ESET Sysinspector.
- 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 tracker:
  - My recommendation: Timesketch
- Scanners:
  - IOC scanners:
    - My recommendations: Loki, DFIR-ORC
- Log scanners: CrowdSec, DeepBlue
  - Offline antimalware scanners:
    - My recommendation: Windows Defender Offline, ESET SysRecue
  - 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

Other critical tools for a SOC and a CERT/CSIRT

- 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

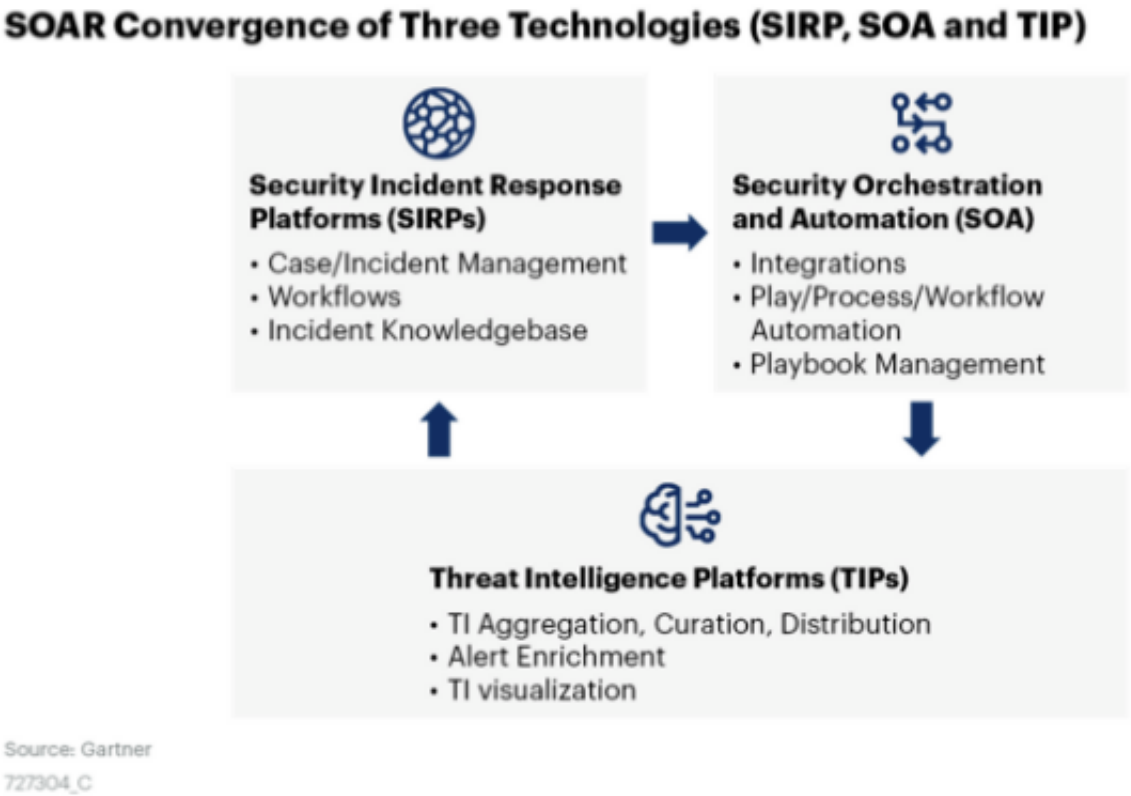
GitLab as a Wiki).

- Vizualization tool for OSINT search and IOC:
  - My recommendation: OSINTracker

SOAR

What is SOAR?

As per Gartner definition:



Hence 3 critical tools (see above): SIRP, TIP, SOA, on top of SIEM.

And in my view, SOAR is more an approach, a vision, based on technology and processes, than a technology or tool per say.

Simple and commonly needed automation tools

- Online automated hash checker (script):

    - my recommendation: Munin, or with PowerShell Posh-VT
- Online URL automated analysis:
    - my recommendation: CyberGordon, URLScan.io
- Online automated sample analyzer:
    - my recommendation, via script and without sample submission: Malwoverview;
    - my recommendations for online dynamic analysis: Hybrid-Analysis, Joe's sandbox
- Offline automated sample analyzer:
    - My recommendation: Qu1cksc0pe
- (pure) Windows tasks automation:
    - My recommendations: AutoIT, Chocolatey
- SaaS-based (and partly free, for basic stuff) SOA:
    - Shuffle

Common automations

My recommendations for detection (alerts handling):

Try to implement at least the following automations, leveraging the SOA/SIRP/TIP/SIEM capabilities:

- Make sure all the context from any alert is being automatically transfered to the SIRP ticket, with a link to the SIEM alert(s) in case of.
    - Leverage API (through SOA) if needed to retrieve the missing context info, when using built-in integrations.
- Automatically query the TIP for any artefacts or even IOC that is associated to a SIRP ticket.
- Automatically retrieve the history of antimalware detections for an user and/or endpoint, that is associated to a SIRP ticket.
- Automatically retrieve the history of SIEM detections for an user and/or endpoint, that is associated to a SIRP ticket.
- Automatically retrieve the history of SIRP tickets for an user and/or endpoint, that is

associated to a new SIRP ticket.

- Automatically query AD or the assets management solution, for artefact enrichment (user, endpoint, IP, application, etc.).

My recommendations for response (incident response, containment/eradication steps):

- Block an IP on all firewalls (including VPN), SWG and CASB.
- Block an URL on SWG.
- Block an email address (sender) on SEG.
- Block an exe file (by hash) on endpoints (leveraging antimalware/EDR or AppLocker).
- Block an exe file (by hash) on gateways and CASB: SWG, SEG, CASB.
- Reset an AD account password.
- Disable an AD account (both user and computer, since computer account disabling will block authentication with any AD account on the endpoint, thus preventing from lateral movement or priv escalation).
- Report a (undetected) sample to security vendors, via email. Here are a few addresses, in case of:
  - Files samples (to be attached in a password-protected Zip file, with 'infected' as password): samples@eset.com, newvirus@kaspersky.com, report@sentinelone.com, virus_submission@bitdefender.com, vsamples@f-secure.com, virus_malware@avira.com, submitvirus@fortinet.com, virus_research@avertlabs.com, virus_doctor@trendmicro.com
  - URL/IP samples: samples@eset.com, samples@kaspersky.com, report@sentinelone.com, virus_submission@bitdefender.com, vsamples@f-secure.com, phish@office365.microsoft.com, report@openphish.com, reportphishing@apple.com, abuse@clean-mx.de, datasubmission@mcafee.com
- Report a false positive to security vendors, via email;
  - You may want to have a look at this page to know the required email address.
- Report a malicious URL (for instance, phishing) to a security vendor for takedown steps
  - My recommendation: Netcraft via API, or PhishReport.
- Block an IP address on web servers, linux firewalls, etc. based on community-driven CTI:
  - My recommendation: CrowdSec bouncer

IT/security Watch (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:
  - CISA catalog
  - CVETrends
- 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
- Other interesting websites:
  - e.g.: ISC, ENISA, ThreatPost ...

Detection engineering

Cf. detection engineering page.

Threat intelligence

Cf. threat intelligence page.

Management

Cf. management page.

HR and training

Cf. HR and training page.

IT achitecture

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

As per NCSC website:

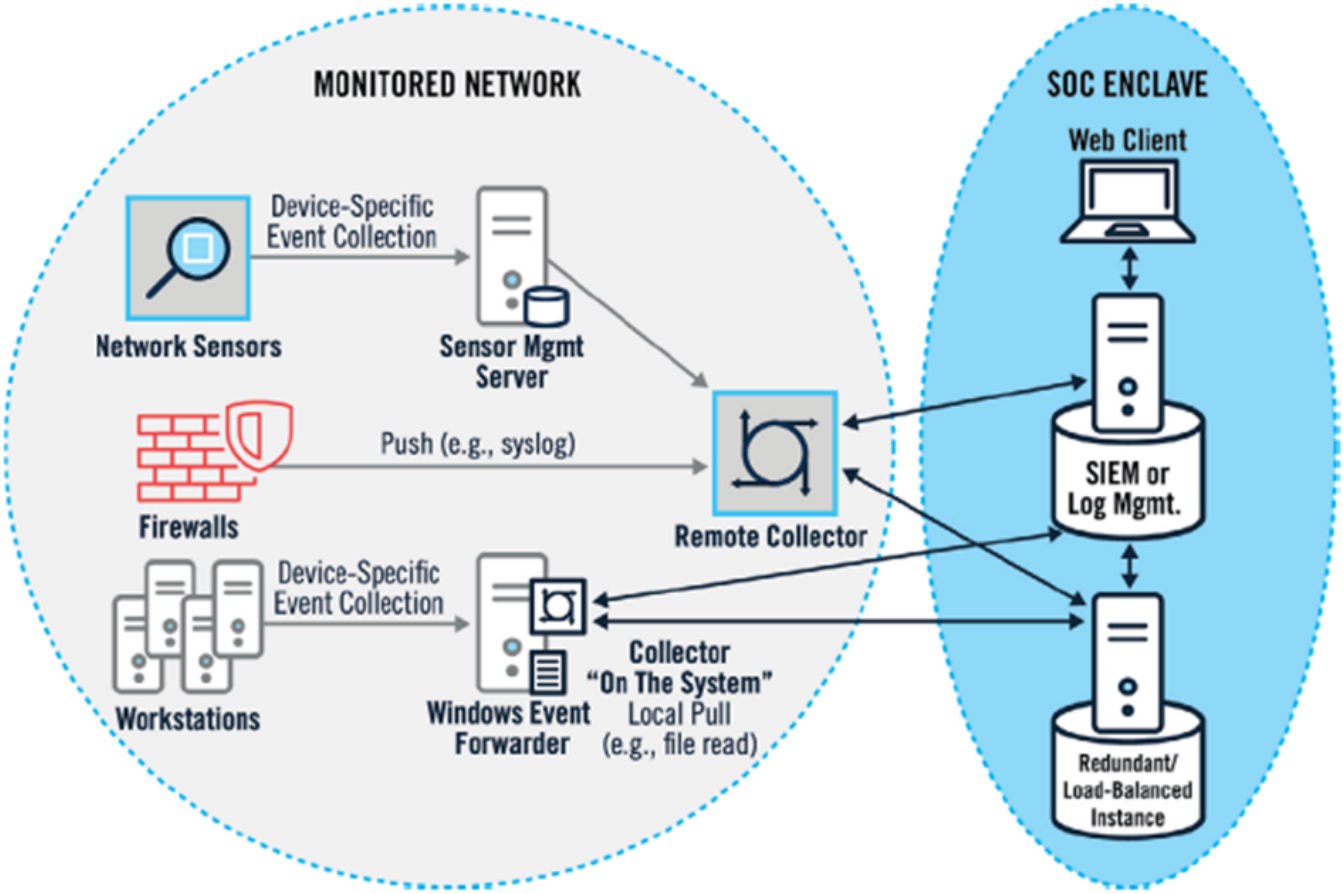
> Indications of an attack will rarely be isolated events on a single system component or system. So, where possible, having a single platform where analysts have the ability to see and query log data from all of your onboarded systems is invaluable. Having access to the log data from multiple (or all) 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 mange 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?

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 Forensocs Incident Response Git
- Austin Songer
- 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
- SOCTOM

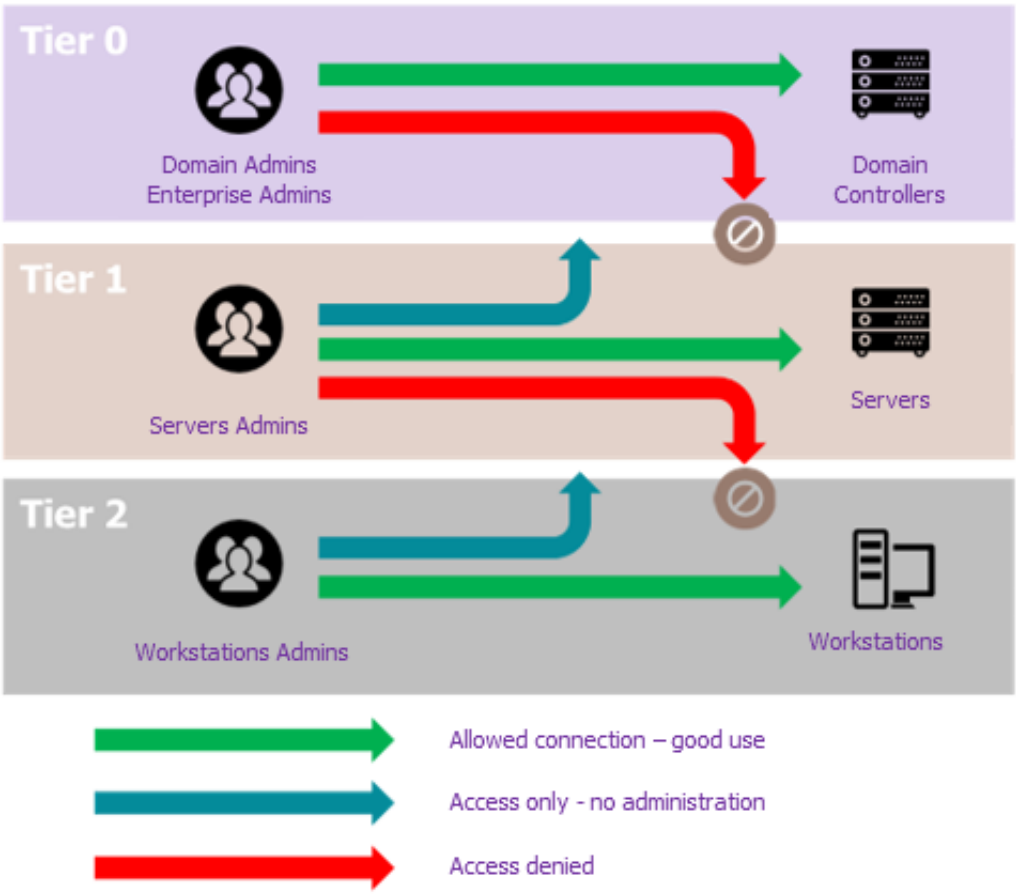
SOC sensors, nice to have

- (full-featured) Honeypot:
  - My recommendation: Canary.tools
  - Or, have a look at (Awesome honeypots Git](https://github.com/paralax/awesome-honeypots)
- NIDS:
  - My recommendation: Crowdsec
- Phishing and brand infringement protection (domain names):
  - My recommendation: PhishLabs, Netcraft
- NDR:
  - My recommendation: Gatewatcher
- MDM:
  - My recommendation: Microsoft Intune
- 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

Appendix

License

CC-BY-SA

Special thanks

Yann F., Wojtek S., Nicolas R., Clément G., Alexandre C., Jean B., Frédérique B., Pierre d'H., Julien C., Hamdi C., Fabien L., Michel de C., Gilles B., Olivier R., Jean-François L., Fabrice M., Pascal R., Florian S., Maxime P., Pascal L., Jérémy d'A., Olivier C. x2, David G., Guillaume D., Patrick C., Lesley K., Gérald G., Jean-Baptiste V., Antoine C. ...