Security Operation Center and Analysis

JOAS ANTONIO

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

INTRODUCTION

- A Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.
- A SOC acts like the hub or central command post, taking in telemetry from across an organization's IT infrastructure, including its networks, devices, appliances, and information stores, wherever those assets reside. The proliferation of advanced threats places a premium on collecting context from diverse sources. Essentially, the SOC is the correlation point for every event logged within the organization that is being monitored. For each of these events, the SOC must decide how they will be managed and acted upon.

10 key functions performed by the SOC

- **Take Stock of Available Resources**
  The SOC is responsible for two types of assets—the various devices, processes and applications they're charged with safeguarding, and the defensive tools at their disposal to help ensure this protection.

  • What The SOC Protects
  The SOC can't safeguard devices and data they can't see. Without visibility and control from device to the cloud, there are likely to be blind spots in the network security posture that can be found and exploited. So the SOC's goal is to gain a complete view of the business' threat landscape, including not only the various types of endpoints, servers and software on premises, but also third-party services and traffic flowing between these assets.

  • How The SOC Protects
  The SOC should also have a complete understanding of all cybersecurity tools on hand and all workflows in use within the SOC. This increases agility and allows the SOC to run at peak efficiency.

10 key functions performed by the SOC

Preparation and Preventative Maintenance
Even the most well-equipped and agile response processes are no match for preventing problems from occurring in the first place. To help keep attackers at bay, the SOC implements preventative measures, which can be divided into two main categories.

- **Preparation**
Team members should stay informed on the newest security innovations, the latest trends in cybercrime and the development of new threats on the horizon. This research can help inform the creation a security roadmap that will provide direction for the company's cybersecurity efforts going forward, and a disaster recovery plan that will serve as ready guidance in a worst-case scenario.

- **Preventative Maintenance**
This step includes all actions taken to make successful attacks more difficult, including regularly maintaining and updating existing systems; updating firewall policies; patching vulnerabilities; and whitelisting, blacklisting and securing applications.

10 key functions performed by the SOC

- **Continuous Proactive Monitoring**
  Tools used by the SOC scan the network 24/7 to flag any abnormalities or suspicious activities. Monitoring the network around the clock allows the SOC to be notified immediately of emerging threats, giving them the best chance to prevent or mitigate harm. Monitoring tools can include a SIEM or an EDR, the most advanced of which can use behavioral analysis to "teach" systems the difference between regular day-to-day operations and actual threat behavior, minimizing the amount of triage and analysis that must be done by humans.

- **Alert Ranking and Management**
  When monitoring tools issue alerts, it is the responsibility of the SOC to look closely at each one, discard any false positives, and determine how aggressive any actual threats are and what they could be targeting. This allows them to triage emerging threats appropriately, handling the most urgent issues first.

- **Threat Response**
  These are the actions most people think of when they think of the SOC. As soon as an incident is confirmed, the SOC acts as first responder, performing actions like shutting down or isolating endpoints, terminating harmful processes (or preventing them from executing), deleting files, and more. The goal is to respond to the extent necessary while having as small an impact on business continuity as possible.

10 key functions performed by the SOC

- **Recovery and Remediation**
  In the aftermath of an incident, the SOC will work to restore systems and recover any lost or compromised data. This may include wiping and restarting endpoints, reconfiguring systems or, in the case of ransomware attacks, deploying viable backups in order to circumvent the ransomware. When successful, this step will return the network to the state it was in prior to the incident.

- **Log Management**
  The SOC is responsible for collecting, maintaining, and regularly reviewing the log of all network activity and communications for the entire organization. This data helps define a baseline for "normal" network activity, can reveal the existence of threats, and can be used for remediation and forensics in the aftermath of an incident. Many SOCs use a SIEM to aggregate and correlate the data feeds from applications, firewalls, operating systems and endpoints, all of which produce their own internal logs.

- **Root Cause Investigation**
  In the aftermath of an incident, the SOC is responsible for figuring out exactly what happened when, how and why. During this investigation, the SOC uses log data and other information to trace the problem to its source, which will help them prevent similar problems from occurring in the future.

10 key functions performed by the SOC

- **Security Refinement and Improvement**
  Cybercriminals are constantly refining their tools and tactics—and in order to stay ahead of them, the SOC needs to implement improvements on a continuous basis. During this step, the plans outlined in the Security Road Map come to life, but this refinement can also include hands-on practices such as red-teaming and purple-teaming.

- **Compliance Management**
  Many of the SOC's processes are guided by established best practices, but some are governed by compliance requirements. The SOC is responsible for regularly auditing their systems to ensure compliance with such regulations, which may be issued by their organization, by their industry, or by governing bodies. Examples of these regulations include GDPR, HIPAA, and PCI DSS. Acting in accordance with these regulations not only helps safeguard the sensitive data that the company has been entrusted with—it can also shield the organization from reputational damage and legal challenges resulting from a breach.

https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-soc.html

WHAT IS SOC

- https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/
- https://digitalguardian.com/blog/what-security-operations-center-soc
- https://www.eccouncil.org/what-is-soc/
- https://www.splunk.com/en_us/data-insider/what-is-a-security-operations-center.html
- https://www.techtarget.com/searchsecurity/definition/Security-Operations-Center-SOC
- https://www.paloaltonetworks.com/cyberpedia/what-is-a-soc
- https://www.fortinet.com/resources/cyberglossary/what-is-soc
- https://www.microfocus.com/en-us/what-is/security-operations-center
- https://www.servicenow.com/products/security-operations/what-is-soc.html
- https://www.logpoint.com/en/blog/security-operations-center/
- https://anysilicon.com/what-is-a-system-on-chip-soc/

WHAT IS SOC

- https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/
- https://digitalguardian.com/blog/what-security-operations-center-soc
- https://www.eccouncil.org/what-is-soc/
- https://www.splunk.com/en_us/data-insider/what-is-a-security-operations-center.html
- https://www.techtarget.com/searchsecurity/definition/Security-Operations-Center-SOC
- https://www.paloaltonetworks.com/cyberpedia/what-is-a-soc
- https://www.fortinet.com/resources/cyberglossary/what-is-soc
- https://www.microfocus.com/en-us/what-is/security-operations-center
- https://www.servicenow.com/products/security-operations/what-is-soc.html
- https://www.logpoint.com/en/blog/security-operations-center/
- https://anysilicon.com/what-is-a-system-on-chip-soc/

WHAT IS SOC 2.0

- https://securityintelligence.com/posts/soc-2-cybersecurity-hiring/
- https://www.imperva.com/learn/data-security/soc-2-compliance/
- https://secure.checkpoint.com/cloud-security/soc-20-a-guide-for-better-cloud-security-visibility-and-forensics
- https://www.computerworld.com/article/3427851/how-the-bank-of-england-built-its-soc-2-0.html
- https://titanwolf.org/Network/Articles/Article?AID=344fdef5-085b-4013-a523-2a080fcf3f4d
- https://www.securityweek.com/its-time-implement-soc-20
- https://cybersecurity.att.com/resource-center/solution-briefs/soc-2-compliance-alienvault-usm

ATTACK METHODOLOGY

- https://www.synack.com/blog/how-hackers-hack-attacker-methodology-and-exploitation-watch-the-demo/
- https://www.pearsonitcertification.com/articles/article.aspx?p=462199&seqNum=2
- https://geek-university.com/ccna-security/hacking-methodology/
- https://inldigitallibrary.inl.gov/sites/sti/sti/3494179.pdf
- https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html
- https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/
- https://www.ibm.com/topics/cyber-attack
- https://www.unisys.com/glossary/cyber-attack/
- https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/
- https://www.ncsc.gov.uk/information/how-cyber-attacks-work
- https://www.upguard.com/blog/cyber-attack
- https://www.techtarget.com/searchsecurity/definition/cyber-attack

Cyber Kill Chain

- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- https://www.researchgate.net/figure/Lockheed-Martin-Cyber-Kill-Chain-CKC-22-seven-steps-The-part-that-is-specified-with_fig1_335024682
- https://www.computer.org/publications/tech-news/trends/what-is-the-cyber-kill-chain-and-how-it-can-protect-against-attacks
- https://www.varonis.com/blog/cyber-kill-chain/
- https://www.sciencedirect.com/topics/computer-science/cyber-kill-chain
- https://www.logsign.com/blog/7-steps-of-cyber-kill-chain/
- https://www.rapid7.com/blog/post/2021/05/27/kill-chains-part-1-strategic-and-operational-value/
- https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain
- https://www.proof.com.br/blog/o-que-e-cyber-kill-chain/

Case Study - Cryptomining

- https://www.accenture.com/_acnmedia/pdf-46/accenture-threat-analysis-monero-wannamine.pdf
- https://medium.com/ditto-trend-comms/case-study-monero-50d7ce705e37
- https://threatpost.com/monero-cybercrime-mining-malware/141116/
- https://www.zdnet.com/article/crypto-mining-malware-saw-new-life-over-the-summer-as-monero-value-tripled/

Case Study - Petya

- https://speakerdeck.com/hshrzd/notpetya-the-analysis-of-the-mysterious-malware-which-has-attacked-ukraine
- https://www.executech.com/insight/petya-cyber-attack-everything-need-know/
- https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/
- https://pt.slideshare.net/cpownall/maersk-notpetya-crisis-response-case-study
- https://www.mcafee.com/enterprise/pt-br/security-awareness/ransomware/petya.html
- https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how
- https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/

MITRE ATT&CK FRAMEWORK

- https://www.mcafee.com/enterprise/pt-br/security-awareness/cybersecurity/what-is-mitre-attack-framework.html
- https://www.exabeam.com/information-security/what-is-mitre-attck-an-explainer/
- https://www.rapid7.com/fundamentals/mitre-attack/
- https://logrhythm.com/solutions/security/mitre-attack-framework/
- https://www.f5.com/labs/articles/education/mitre-attack-what-it-is-how-it-works-who-uses-it-and-why
- https://www.cisco.com/c/en/us/products/security/what-is-mitre-attck.html
- https://www.threatq.com/mitre-attack/
- https://itegriti.com/2020/cybersecurity/what-is-the-mitre-attck-framework-and-why-is-it-important/
- https://www.secureworks.com/centers/mitre-attack
- https://www.csoonline.com/article/3267691/what-is-mitres-attandck-framework-what-red-teams-need-to-know.html
- https://www.cyberark.com/what-is/mitre-attack/
- https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-mitre-attck-framework/
- https://www.varonis.com/blog/mitre-attck/
- https://awakesecurity.com/glossary/mitre-attck-framework/
- https://www.bmc.com/blogs/mitre-attack-framework/
- https://attack.mitre.org/techniques/enterprise/

WINDOWS ENDPOINT

- https://docs.microsoft.com/pt-br/mem/endpoint-manager-overview
- https://www.veeam.com/br/windows-endpoint-server-backup-free.html
- https://www.sophos.com/en-us/support/documentation/endpoint-security-and-control-for-windows.aspx
- https://docs.microsoft.com/pt-br/windows/
- https://www.youtube.com/watch?v=88YI28GPwEg
- https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer
- https://www.onmsft.com/how-to/how-to-see-what-programs-are-running-in-windows-10
- https://www.howtogeek.com/405806/windows-task-manager-the-complete-guide/
- https://www.youtube.com/watch?v=E6ROLfd8RFo
- https://support.microsoft.com/en-us/windows/how-to-open-registry-editor-in-windows-10-deab38e6-91d6-e0aa-4b7c-8878d9e07b11
- https://docs.microsoft.com/pt-br/troubleshoot/windows-server/performance/windows-registry-advanced-users

COMMAND PROMPT

- https://www.thomas-krenn.com/en/wiki/Cmd_commands_under_Windows
- https://www.makeuseof.com/tag/15-cmd-commands-every-windows-user-know/
- https://docs.microsoft.com/pt-br/windows-server/administration/windows-commands/windows-commands
- https://www.lifewire.com/list-of-command-prompt-commands-4092302
- https://ss64.com/nt/
- https://www.ionos.com/digitalguide/server/know-how/windows-cmd-commands/
- https://www.computerhope.com/issues/chusedos.htm
- https://helpdeskgeek.com/help-desk/21-cmd-commands-all-windows-users-should-know/
- https://dev.to/iamprogrammmer/command-prompt-basic-commands-you-should-know-cmd-4aj
- https://www.howtogeek.com/235101/10-ways-to-open-the-command-prompt-in-windows-10/
- https://www.wired.com/story/6-windows-command-prompt-clever-tips/
- https://www.businessinsider.com/command-prompt-commands
- https://bytescout.com/blog/windows-command-prompt-commands.html
- https://www.pcworld.com/article/394613/6-command-prompt-commands-you-should-still-be-using.html

POWERSHELL

- https://docs.microsoft.com/pt-br/powershell/
- https://github.com/MicrosoftDocs/PowerShell-Docs
- https://www.windowscentral.com/how-create-and-run-your-first-powershell-script-file-windows-10
- https://www.tutorialspoint.com/powershell/powershell_scripting.htm
- https://www.varonis.com/blog/windows-powershell-tutorials/
- https://adamtheautomator.com/run-powershell-script/
- https://www.dummies.com/computers/operating-systems/windows-xp-vista/create-run-powershell-script/
- https://www.scriptrunner.com/
- http://underpop.online.fr/w/windows-power-shell/como-criar-e-executar-um-script-microsoft-windows-powershell.htm
- https://www.dirceuresende.com/blog/powershell-script-para-listar-e-exportar-para-csv-todos-os-arquivos-um-diretorio-com-atributos-nome-diretorio-tamanho-e-duracao/

SHELL SCRIPTING

- https://www.shellscript.sh/
- https://www.devmedia.com.br/introducao-ao-shell-script-no-linux/25778
- https://www.tutorialspoint.com/unix/shell_scripting.htm
- https://devhints.io/bash
- https://developers.redhat.com/cheat-sheets/bash-shell-cheat-sheet
- https://devdojo.com/bobbyiliev/the-only-bash-scripting-cheat-sheet-that-you-will-ever-need
- https://www.zero2devops.com/blog/bash-scripting-cheat-sheet
- https://github.com/LeCoupa/awesome-cheatsheets/blob/master/languages/bash.sh
- https://monovm.com/blog/bash-scripting-cheat-sheat/
- https://www.ullright.org/ullWiki/show/bash-shell-scripting-cheat-sheet
- https://shellmagic.xyz/
- https://www.youtube.com/watch?v=wsh64rjnRas
- https://www.youtube.com/watch?v=aaEoyVIowk8
- https://www.youtube.com/watch?v=v_1zB2WNN14
- https://www.tutorialspoint.com/linux_admin/index.htm

Network Services Administration

- https://medium.com/dont-code-me-on-that/tryhackme-network-services-room-writeup-e00f88b7b599
- https://docs.oracle.com/cd/E19455-01/806-0916/6ja85398c/index.html
- https://www.systemsengineering.com/managed-it/network-administration/
- https://pt.slideshare.net/UcMan/system-and-network-administration-network-services-54603810
- https://dynamixsolutions.com/network-and-server-administration/
- https://www.youtube.com/watch?v=qI-N4J2Xl5w
- https://www.youtube.com/watch?v=qcvZ2Jm8fPU

ELK and SYSLOG

- https://sematext.com/blog/logstash-alternatives/
- https://logz.io/learn/complete-guide-elk-stack/
- https://stackshare.io/stackups/logstash-vs-rsyslog
- https://www.elastic.co/pt/blog/how-to-centralize-logs-with-rsyslog-logstash-and-elasticsearch-on-ubuntu-14-04
- https://www.trustradius.com/compare-products/logstash-vs-solarwinds-kiwi-syslog-server
- https://maddevs.io/insights/blog/log-collecting-with-elk-and-rsyslog/
- https://www.elastic.co/pt/what-is/elk-stack
- https://sematext.com/guides/elk-stack/#:~:text=Thus%2C%20ELK%20is%20a%20log,visualize%20it%20in%20real%20time.
- https://www.cprime.com/resources/blog/log-management-elk-and-why-you-should-care/
- https://medium.com/@vitalypanukhin/elasticsearch-elk-stack-for-log-management-8f4e61a60239

BEST PRACTICES LOG MANAGEMENT

- https://www.rapid7.com/blog/post/2015/10/15/10-best-practices-for-log-management-and-analytics/
- https://www.loggly.com/use-cases/what-is-log-management-short-guide-and-best-practices/
- https://www.dnsstuff.com/log-management-best-practices
- https://www.tek-tools.com/apm/log-management-best-practices
- https://www.darkreading.com/edge/theedge/9-modern-day-best-practices-for-log-management/b/d-id/1340591
- https://www.graylog.org/post/what-is-log-management-a-complete-logging-guide
- https://wisdomplexus.com/blogs/log-management-best-practices/
- https://csrc.nist.gov/publications/detail/sp/800-92/final

SIEM/SEM

- https://medium.com/@ronanthewriter/5-best-practices-for-successful-siem-implementations-e45d184386e5
- https://www.bmc.com/blogs/siem-best-practices/
- https://blog.netwrix.com/2021/05/05/siem-use-cases/
- https://www.toolbox.com/it-security/siem/blogs/7-best-practices-for-successful-siem-implementation-and-adoption-112018/
- https://www.n-able.com/blog/siem-logging-best-practices
- https://www.dnsstuff.com/common-siem-alerts
- https://anlyz.co/blog/best-practices-of-how-to-implement-siem-software/
- https://www.linkedin.com/pulse/best-practices-successful-siem-implementation-ina-nikolova-ph-d-/
- https://www.eventsentry.com/resources/siem-bestpractices.pdf
- https://www.gartner.com/reviews/market/security-information-event-management
- https://www.exabeam.com/library/2021-gartner-magic-quadrant-for-siem/
- https://www.securonix.com/resources/2021-gartner-magic-quadrant-for-siem/
- https://techbeacon.com/security/how-use-siem-hunt-techniques-prepare-cyber-threats
- https://www.fireeye.com/products/helix/what-is-siem-and-how-does-it-work.html

VULNERABILITY MANAGEMENT

- https://cybersecurity.att.com/blogs/security-essentials/vulnerability-management-explained
- https://www.qualys.com/apps/vulnerability-management/
- https://www.youtube.com/watch?v=DcwBn9nOmiE
- https://www.gartner.com/reviews/market/vulnerability-assessment
- https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html
- https://www.crowdstrike.com/cybersecurity-101/vulnerability-management/

EDR

- https://www.trendmicro.com/pt_br/business/products/detection-response/edr-endpoint-sensor.html
- https://www.securityreport.com.br/overview/endpoint-detection-and-response-edr-o-caso-do-contexto/
- https://www.mcafee.com/enterprise/pt-br/security-awareness/endpoint/what-is-endpoint-detection-and-response.html
- https://en.wikipedia.org/wiki/Endpoint_detection_and_response
- https://www.techtarget.com/searchsecurity/definition/endpoint-detection-and-response-EDR
- https://digitalguardian.com/blog/what-endpoint-detection-and-response-definition-endpoint-detection-response
- https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/
- https://www.cynet.com/endpoint-protection-and-edr/top-6-edr-tools-compared/
- https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-detection-and-response-edr
- https://www.varonis.com/blog/edr-security/

REGEX

- https://regexr.com/
- https://www.computerhope.com/jargon/r/regex.htm
- https://medium.com/factory-mind/regex-tutorial-a-simple-cheatsheet-by-examples-649dc1c3f285
- https://developer.mozilla.org/en-US/docs/Web/JavaScript/Guide/Regular_Expressions
- https://www.geeksforgeeks.org/write-regular-expressions/
- https://www.regular-expressions.info/tutorial.html
- https://www.smashingmagazine.com/2009/05/introduction-to-advanced-regular-expressions/
- https://www.rexegg.com/regex-quickstart.html

STIX AND TAXII

- https://www.anomali.com/resources/what-are-stix-taxii
- https://oasis-open.github.io/cti-documentation/taxii/intro.html
- https://www.eclecticiq.com/stix-taxii
- https://threatconnect.com/stix-taxii/
- https://socradar.io/what-you-need-to-know-about-stix-and-taxii/
- https://www.plixer.com/blog/stix-taxii-threat-intelligence/
- https://medium.com/sekoia-io-blog/stix-and-taxii-c1f596866384

IoCs and IoAs

- https://www.trendmicro.com/vinfo/us/security/definition/indicators-of-compromise
- https://en.wikipedia.org/wiki/Indicator_of_compromise
- https://digitalguardian.com/blog/what-are-indicators-compromise
- https://encyclopedia.kaspersky.com/glossary/indicator-of-compromise-ioc/
- https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/
- https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/ioa-vs-ioc/
- https://www.logsign.com/blog/what-is-ioc-in-cyber-security/
- https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/fortiguard-indicators-of-compromise-service
- https://github.com/sroberts/awesome-iocs
- https://www.cytomic.ai/threat-hunting/iocs-ioas-what-difference/
- https://www.rocketcyber.com/blog-threat-detection-ioa-vs-ioc.html
- https://www.linkedin.com/pulse/iocs-e-ioas-conhecimento-vapt-vupt-paulo-henrique-dias-de-oliveira/?originalSubdomain=pt

Incident Response and Detection

- https://www.rapid7.com/blog/post/2016/03/29/what-is-incident-detection-and-response/#:~:text=Incident%20detection%20and%20response%20%2C%20also,threat%2C%20and%20removing%20their%20foothold.
- https://www.rapid7.com/solutions/incident-detection-and-response/
- https://www.cynet.com/incident-response/nist-incident-response/
- https://www.sciencedirect.com/topics/computer-science/incident-response-process
- https://digitalguardian.com/blog/five-steps-incident-response
- https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/incident-response-tools
- https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/incident-response-tools
- https://www.securitymetrics.com/blog/6-phases-incident-response-plan
- https://kemptechnologies.com/blog/incident-detection-response/
- https://github.com/meirwah/awesome-incident-response
- https://github.com/pain0x0/awesome-incident-response
- https://github.com/cloudsecurityalliance/CSA-Guidance/blob/master/Domain%209-%20Incident%20Response.md
- https://github.com/OWASP/samm/blob/master/Current%20Releases/head/core/operations/o-incident-management.md
- https://github.com/veeral-patel/incidents
- https://github.com/easttimor/aws-incident-response
- https://github.com/hsainnos/LICSTER

Computer Forensic

- https://github.com/topics/digital-forensics
- https://github.com/sepinf-inc/IPED
- https://github.com/mesquidar/ForensicsTools
- https://github.com/asiamina/A-Course-on-Digital-Forensics
- https://www.cipsec.eu/content/introduction-digital-forensics
- https://resources.infosecinstitute.com/topic/computer-forensics-multimedia-content-forensics/
- https://githubmemory.com/repo/fiuderazes/awesome-forensics
- https://github.com/cugu/awesome-forensics

Threat Hunting and Intelligence

- https://www.activecountermeasures.com/threat-intel-versus-threat-hunting-whats-the-difference/
- https://www.ibm.com/topics/threat-hunting
- https://redteam.pl/en/threat-hunting-intelligence.html
- https://www.recordedfuture.com/solutions/threat-hunting/
- https://nethemba.com/threat-hunting-and-threat-intelligence-services/
- https://blog.apnic.net/2021/10/21/how-to-threat-hunting-and-threat-intelligence/
- https://www.viavisolutions.com/pt-br/node/63435
- https://github.com/OTRF/ThreatHunter-Playbook
- https://github.com/Cyb3r-Monk/Threat-Hunting-and-Detection
- https://github.com/SoulSec/resource-threat-hunting
- https://github.com/osintbrazuca/OSINT-Brazuca
- https://github.com/Datalux/Osintgram
- https://github.com/jivoi/awesome-osint
- https://github.com/lockfale/OSINT-Framework

Malware Analysis and Reverse Engineering

- https://www.youtube.com/watch?v=VOTnt2PdqNM
- https://www.youtube.com/watch?v=HtYlGdEo_9o
- https://www.youtube.com/watch?v=yZ6D4-Jz3Hc
- https://github.com/rshipp/awesome-malware-analysis
- https://github.com/CYB3RMX/Qu1cksc0pe
- https://github.com/hasherezade/malware_training_vol1
- https://github.com/crhenr/freki
- https://github.com/fwosar/malware-analysis-resources
- https://github.com/SafeEval/practical-malware-analysis
- https://github.com/rshipp/awesome-malware-analysis
- https://github.com/tylerha97/awesome-reversing
- https://githubmemory.com/repo/shadowce/awesome-reverse-engineering
- https://www.mentebinaria.com.br/studying-materials/registros/engenharia-reversa/
- https://www.mentebinaria.com.br/guia-de-estudos-e-profissoes/analista-de-malware-r2/

Network Monitor

- https://github.com/Enapiuz/awesome-monitoring
- https://www.cloudradar.io/blog/network-monitoring-best-practices
- https://www.whatsupgold.com/resources/best-practices/network-monitoring
- https://www.ninjaone.com/blog/network-monitoring-management-best-practices-for-beginners-2021/
- https://www.metricfire.com/blog/cisco-network-monitoring-6-best-practices/
- https://wisdomplexus.com/blogs/network-monitoring-best-practices/
- https://www.tek-tools.com/network/network-monitoring-guide-and-tools
- https://www.kaseya.com/blog/2020/06/29/effective-network-monitoring-5-best-practices/
- https://www.dnsstuff.com/network-monitoring
- https://solutionsreview.com/network-monitoring/category/best-practices/
- https://statseeker.technichegroup.com/seven-best-practices-for-network-monitoring-management/

ENDPOINT SECURITY

- https://www.mcafee.com/enterprise/pt-br/security-awareness/endpoint.html
- https://en.wikipedia.org/wiki/Endpoint_security
- https://www.citrix.com/pt-br/solutions/unified-endpoint-management/what-is-endpoint-security.html
- https://www.forcepoint.com/pt-br/cyber-edu/endpoint-security
- https://www.crowdstrike.com/cybersecurity-101/endpoint-security/
- https://www.cisco.com/c/en/us/products/security/endpoint-security/index.html

CLOUD SECURITY

- https://github.com/toniblyx/my-arsenal-of-aws-security-tools
- https://github.com/Funkmyster/awesome-cloud-security
- https://github.com/aquasecurity/cloudsploit
- https://github.com/owasp-cloud-security/owasp-cloud-security
- https://github.com/0xVariable/AWS-Security-Tools
- https://www.esecurityplanet.com/cloud/cloud-security-best-practices/
- https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/cloud-security-best-practices.html
- https://www.infosecurity-magazine.com/magazine-features/top-5-best-practices-for-cloud/
- https://thycotic.com/company/blog/2021/11/02/cloud-security-best-practices-checklist/
- https://solutionsreview.com/cloud-platforms/7-cloud-security-best-practices-to-keep-your-cloud-environment-secure/
- https://www.n-ix.com/cloud-security-best-practices/
- https://www.netwrix.com/cloud_security_best_practices.html

SOC CAREER

- https://www.cybrary.it/catalog/career-path/soc-analyst-level-1/
- https://www.cybrary.it/catalog/career-path/soc-analyst-level-2/
- https://www.cybrary.it/catalog/career-path/soc-analyst-level-3/
- https://www.eccouncil.org/build-a-rewarding-career-in-a-soc/
- https://www.seek.com.au/soc-analyst-jobs
- https://www.naukri.com/soc-jobs
- https://cyberdome.net/soc-career/
- https://kingslanduniversity.com/soc-analyst-career-path/
- https://www.cwjobs.co.uk/jobs/soc-analyst
- https://www.linkedin.com/jobs/soc-vagas/?originalSubdomain=br
- https://www.reddit.com/r/AskNetsec/comments/65540f/do_you_work_in_soc_career_advice_please/
- https://www.darkreading.com/careers-and-people/from-help-desk-to-head-of-soc-building-a-cybersecurity-career-on-empathy-and-candor
- https://www.cisecurity.org/blog/day-in-the-life-of-a-soc-analyst/