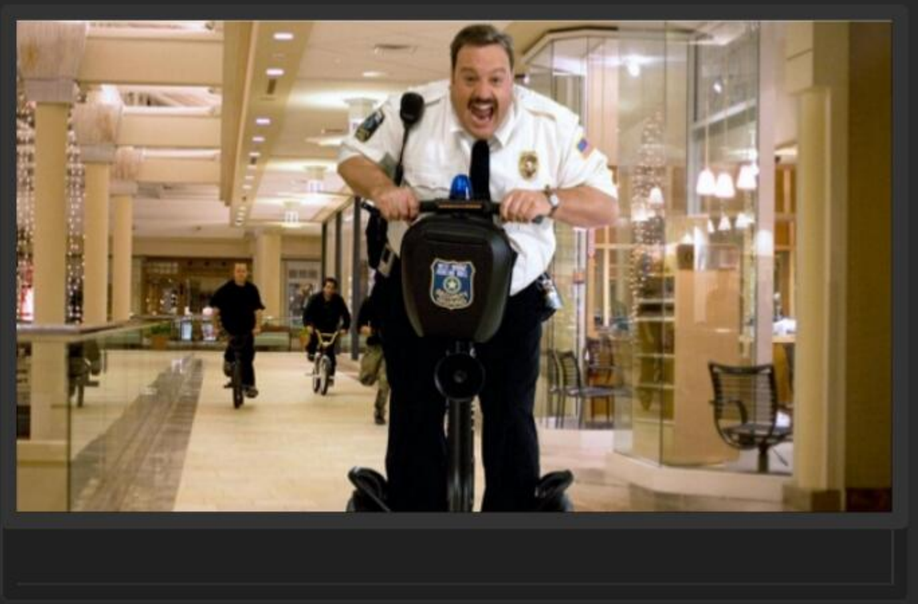
Security Operation Center

Career Secret Roadmap

Mohammad Khreesha
Senior Cybersecurity Director

Whoami



- 15+ Years of IT & Cybersecurity Experience.
- Cybersecurity Director & Trainer.
- ex-OWASP Amman Chapter Leader.
- Youtuber & Blogger.
- CEH, CHFI, ECSA, LPT master, OSCP, CRTP, eCPPT, eCPTX, eWPT, eWPTX, eMAPT, eCIR, eCTHP, eCMAP, eCDFP, & ISO 27001 LI.
- Top Arab Cybersecurity Social Media Influencer (2019, 2020, 2021, 2022, & 2023).

Table of Contents

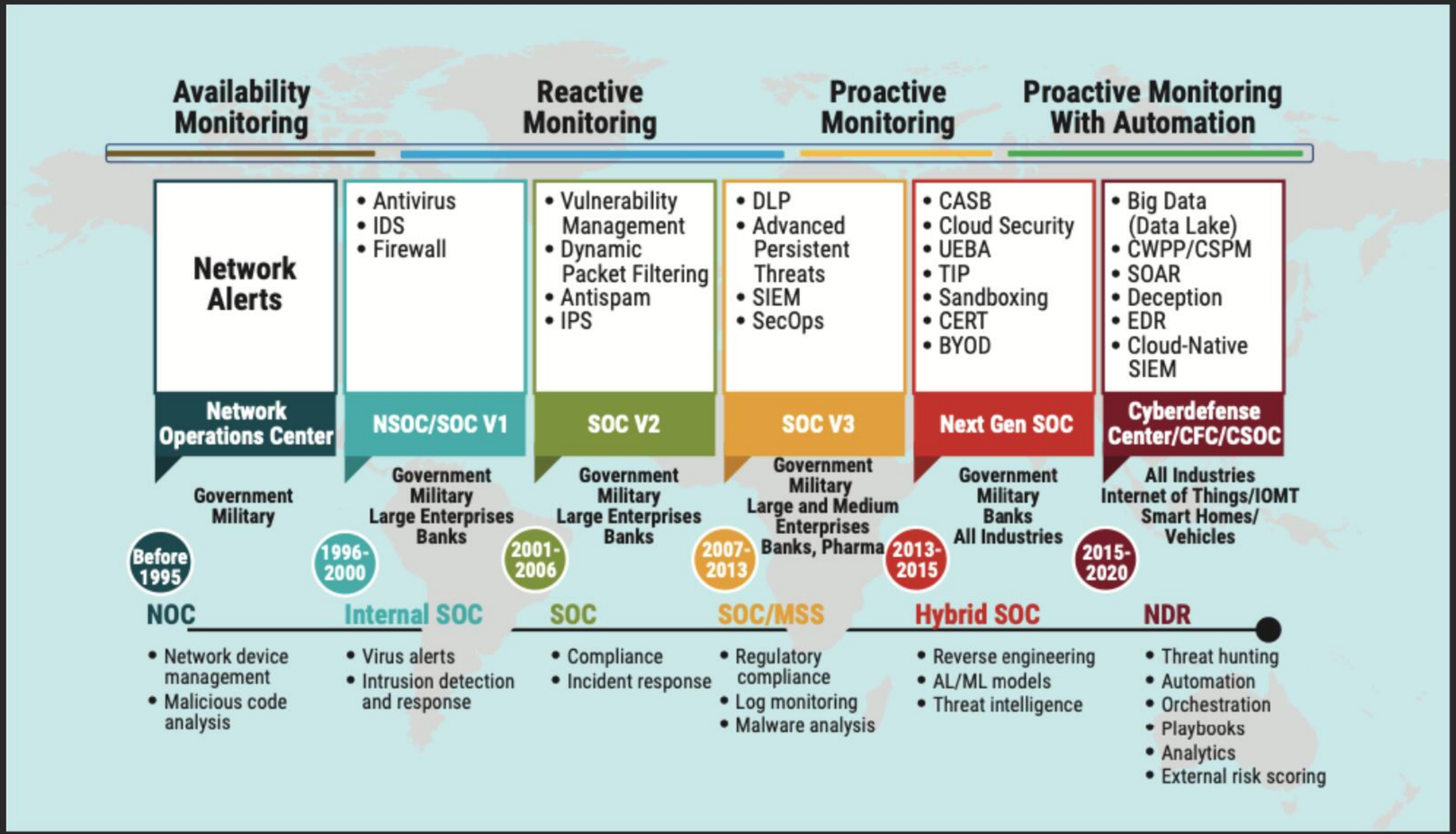
- Introduction to SOC
- The Road-map
  - Prerequisites
  - Main Skills
  - Advanced Skills
  - Certificates
- Learning Resources

What is a Security Operation Centre (SOC)

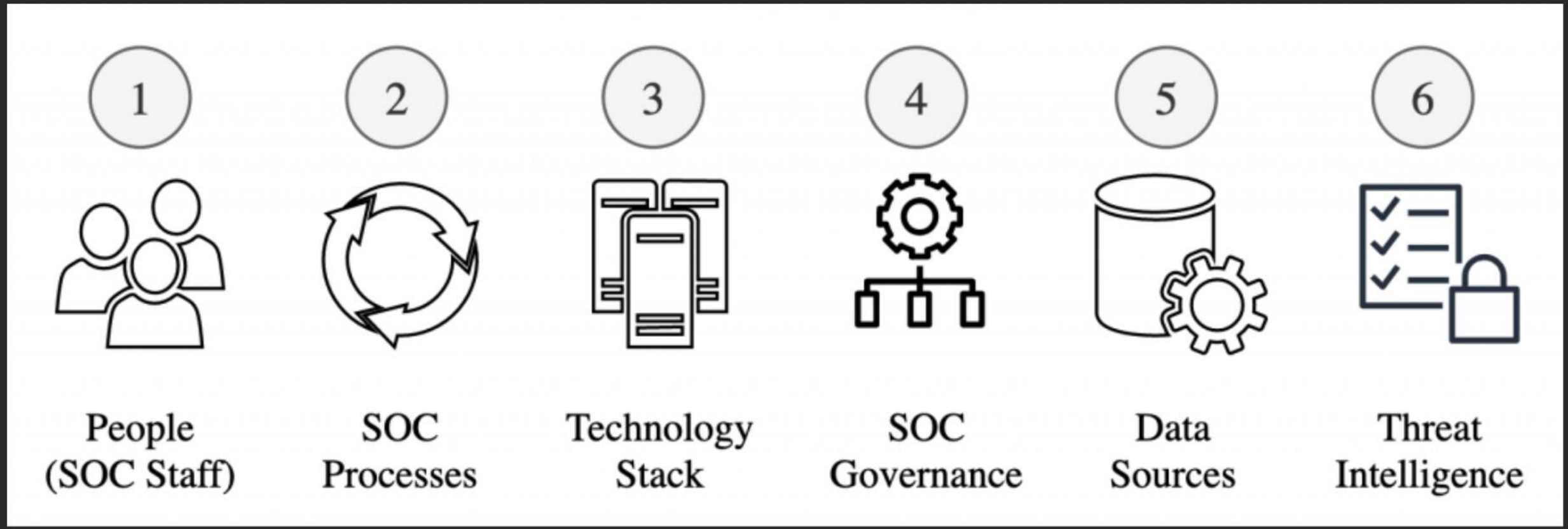
- A SOC is a centralized function within an organization that employs people, processes, and technology to continuously monitor and improve an organization’s security posture while preventing, detecting, analyzing, and responding to Cybersecurity incidents.

- A SOC is a centralized unit within any organization employing people, processes, and technology to continuously monitor and improve an organization's security visibility.

Evolution of SOC



Building Blocks of Modern SOC/CDC



Functions of SOC

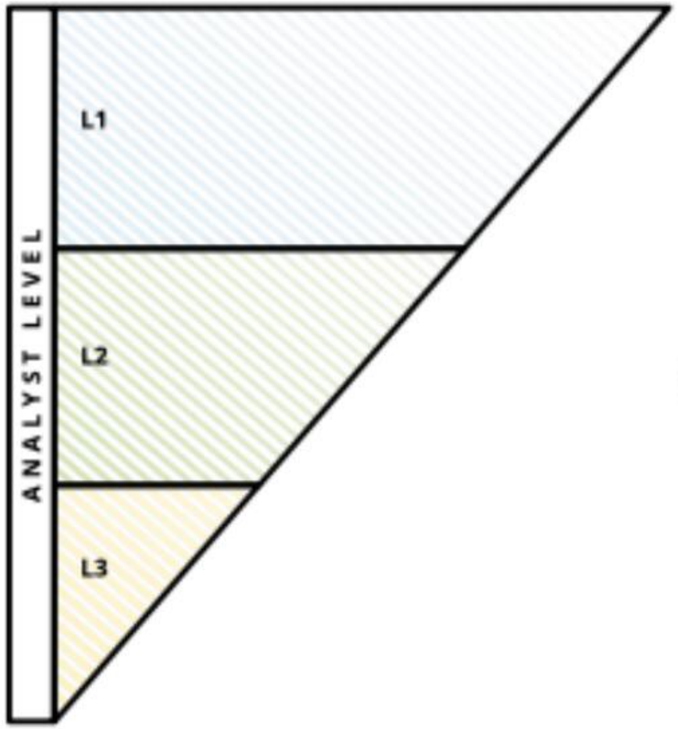
SOC Models

- ***In-house model*** requires you to fill all required positions for your security team internally.
- ***Outsources model*** rely on a managed security service provider (MSSP) to fill all of the roles of your security operations team.
- ***Hybrid model*** is a combination of in-house and outsourced employees.

Staffing model	Pros	Cons
In-house	• Quick communication • Can have higher accuracy • All data is kept internally • Your team can apply their knowledge of the organisation in their work	• Generally, the most expensive model • Can take longer to reach maturity • Potential to lose knowledge with a team member • High total cost of ownership to manage a 24x7 operation
Outsourced	• Service level agreements (SLAs) make the scope and budgeting for the services well-defined • Easy to implement and short ramp up time • Access to 24x7 operations, monitoring, detection and threat intelligence • Reduced operating cost	• Difficult to move in-house from this model • MSSPs need time to understand your organisation • Increased risk associated with data being stored outside of your organisation • Requires vendor management
Hybrid	• Double checking for certain alerts • Your team can get cross-training from experts outside of your organisation • Can help you achieve 24x7 operations without staffing during less desirable times	• Model may be costly over time • Increased risk associated with data being stored outside of your organisation • May require you to set up additional hardware

SOC Types

Tier-based SOC



Current tier-based model reduces the amount of judgment calls made by analysts as their technical experience increases.

Technology enablement

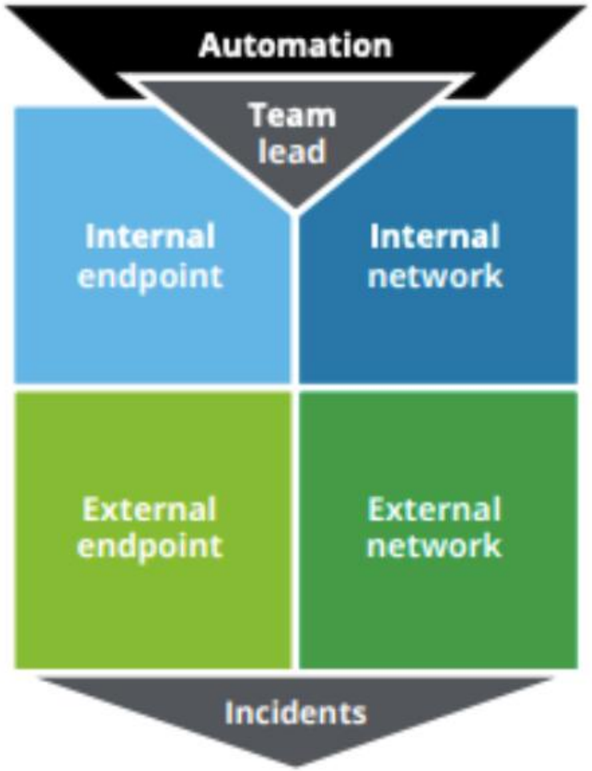
ENRICHMENT

AUTOMATION

CURATION

Technology empowers analysts to be more meaningful and efficient in their judgment calls.

Skills-based SOC



Appropriate subject matter expertise, coupled with automation, provides an appropriate level of context to judgment calls.

SOC Team Members

- Chief Information Security Officer (CISO) :
  - Defines the security operations of the organization.
  - Interacts with management about security issues and compliance tasks.
  - Gives a final look at policies, strategies, and procedures relating to the organization’s Cybersecurity
  - Has a primary role in compliance, risk management, and implement policies to meet particular security demands
- SOC Manager :
  - Manages the security operations team and reports to the CISO.
  - Controls the security team, give technical guidance, and also maintain financial activities.
  - Supervises the activities of the SOC team, including hiring, training, and assessing staff.

Continue..

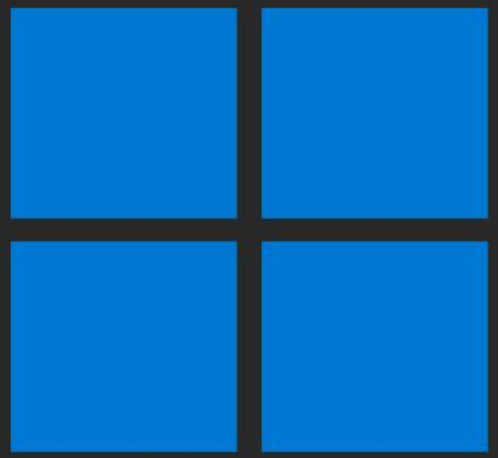
- SOC Engineer/Architect :
  - Maintains and suggests monitoring and analysis tools.
  - Builds a security architecture and work with developers to secure this architecture.
  - Gives appropriate attention to security aspects when producing information systems.
  - Produces tools and solutions that allow organizations to respond efficiently to attacks.
- SOC Analyst (Tier 1) :
  - Monitors user activity, network events and signals from security tools to identify events.
  - Is responsible for determining which alerts and other abnormal activity represent real threats.

Continue..

- Incident Responder (Tier 2) :
  - Remediates attacks intensified from Tier 1 Analysts.
  - Collects data for more analysis, evaluate the attack, identify the root of the attack, implement required security actions to counter the attack, and restore system operations.
  - Responsible for investigating and generating reports on information security issues.
- Threat Hunters (Tier 3) :
  - Works proactively to explore the weaknesses in IT infrastructure.
  - Performs penetration tests and review vulnerability assessments.
  - Maintains security systems up to date and contribute to ongoing security approaches to secure the organization against further attacks.

The Road-map : Prerequisites

IT Fundamentals



Windows

Linux

Networking

Scripting

Database

Cybersecurity

The Road-map : Main Skills

Building Home Lab

Working with SIEM

Log Analysis

Network Analysis

Pentesting

Incident Handling

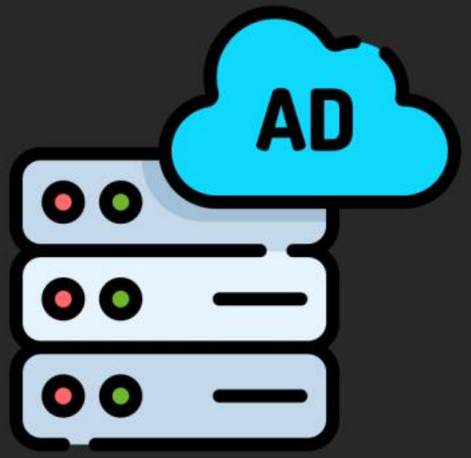
DFIR

Threat Hunting

Malware Analysis

Threat Intelligence

The Road-map : Advanced Skills



Active Directory

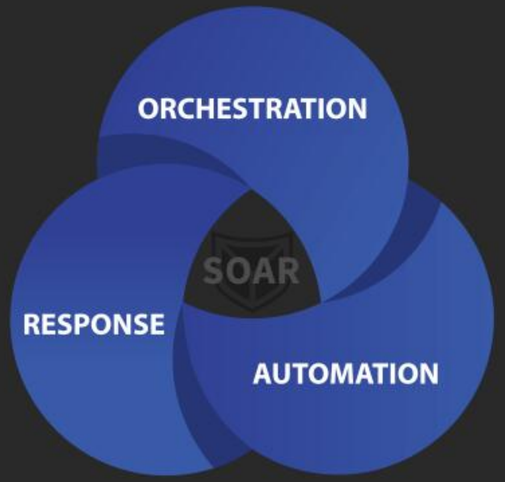
MITRE ATT&CK™

ATT&CK TTPs

Reverse Engineering

ASM

Assembly Language



SOAR

Cloud Security

Sigma Rules

Detection Engineering

The Road-map : Certificates

Entry Level

Intermediate Level

Advanced Level

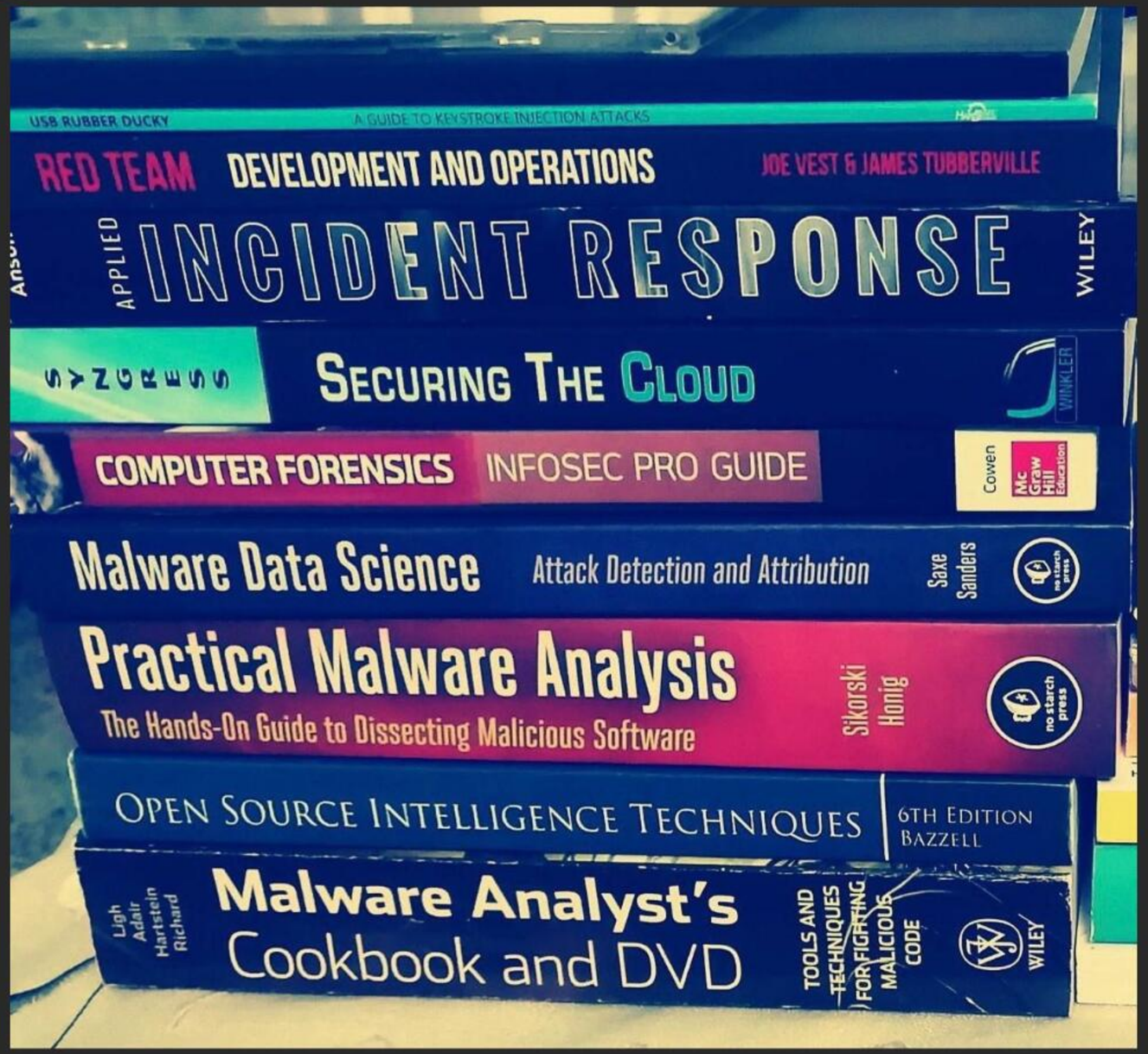
Golden Rule

“The best way to learn new things in your field is to teach them to others”

Learning Resources : Online

- https://www.youtube.com/@technawidotcom
- https://www.cyberdefenders.org
- https://app.hackthebox.com/sherlocks
- https://securityblue.team/
- https://wazuh.com/
- https://socprime.com
- https://github.com/cyb3rxp/awesome-soc
- https://github.com/LetsDefend/awesome-soc-analyst
- https://github.com/aboutsecurity/blueteam_homelabs

Learning Resources : Books



Any Questions, Comments or Concerns?

Thank you!

Website : https://www.technawi.net
Linkedin : https://www.linkedin.com/in/khreesha
Twitter: @banyrock
Facebook : http://www.fb.com/khreesha
Youtube : https://www.youtube.com/technawidotcom