ISACA Tunis Chapter · HAT Web Security Labs · devoteam · SECURAS TECHNOLOGIES · ANCS · RAISEGUARD · Smart Skills · Club DSI Tunisie · Polytechnique des Sciences Avancées Agrément N° 03-2001 · IT Advisory

I-PROTECT v8

SOC UNVEILED:

DECODING THE HEART OF CYBER DEFENSE

MONITORING CYBER TRAIN INTRUDERS

SPEAKER:

RIADH BRINSI

CYBERSECURITY MANAGER

WEDNESDAY 13 DEC,2023

8:00 PM

ONLINE

2023

Jagora Foundation · IEEE ENIS Computer Society · IEEE Cyber Security ENIS · IEEE Signal Processing Society Tunisia Chapter · IEEE Tunisia Section · Université de Sfax · Computational Intelligence Society Tunisia Chapter · ReGIM-Lab · ENIS · Tunisia Chapter

Table Of Content

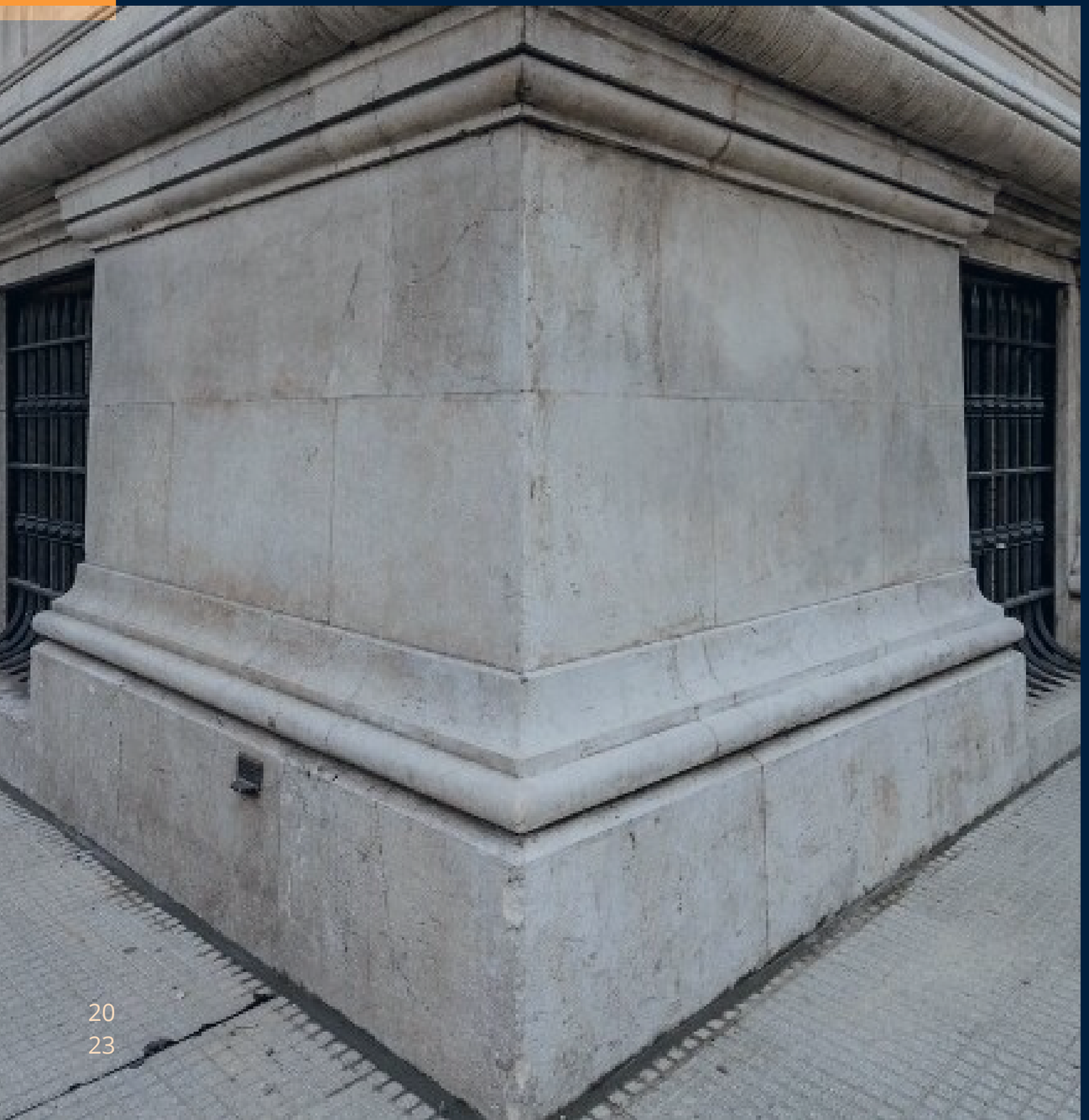
Riadh Brinsi

Cyber Security Manager | Air Force Veteran

WELCOME TO THE CYBERSECURITY

- **Cybersecurity:** the practice of protecting computer systems, networks, and digital data from unauthorized access, attacks, damage, or theft.
- **CIA:** Confidentiality, Integrity, Availability.
- **Cyber threats:** are malicious activities that aim to compromise digital systems and data.
- Cyber threats are diverse and evolving.
- Organizations face increasing risks.
- Robust cybersecurity measures are essential for protection.

image : https://www.treuhandsuisse.ch/fr/la-protection-des-donnees-rendez-vous-avec-linformatique-avez-vous-deja-opte-pour-le-cryptage-ou



GRC: THE CORNERSTONE

- **Governance:** Ensure that IT goals, policies and processes are aligned with business objectives and leadership for ethical and strategic decision-making. **=>The direction**
- **Risk Management:** iterative process of identifying, assessing, and responding to risks related to financial, operational, and strategic objectives. **=>How to use the resources**
- **Compliance:** Ensuring adherence to applicable laws, regulations, and internal policies to avoid legal issues, financial penalties, and reputational damage. **=> Being ethical and within legal boundaries**

image: https://engineering.stanford.edu/magazine/article/what-s-around-corner-camera-technology

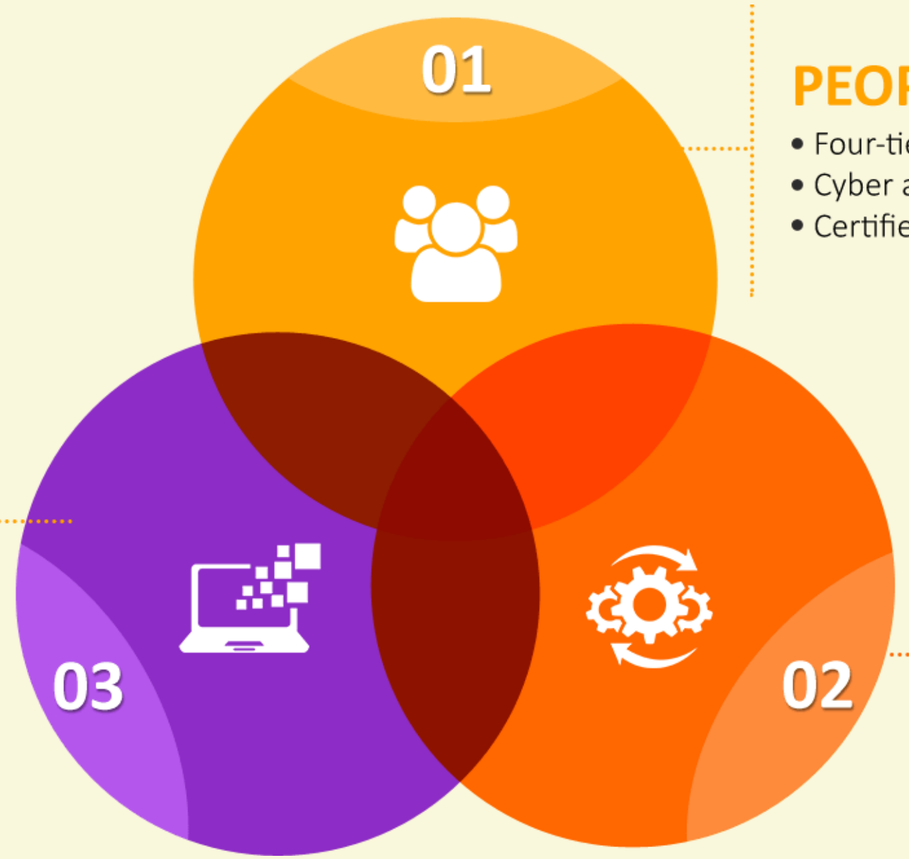
The SOC: the train controller

A Security Operations Center (SOC) is a centralized facility equipped to

to cybersecurity threats and incidents in real-time.

image 1 :AI generated
image 2 : https://docs.actzero.ai/

The Main Components of the SOC



PEOPLE

- Four-tier SOC team
- Cyber architectural engineers
- Certified risk professionals

PROCESS

- SOC Orchestration
- Threat detection
- Vulnerability scanning
- Network threat analytics

TECHNOLOGY

- Alert and reporting
- Alarms and escalation
- Defined use cases
- Automated ticketing
- Incident breach response
- Reporting and dashboards

image : https://cetark.com/soc.html

People

skilled cybersecurity professionals responsible for monitoring, analyzing, and responding to security incidents.

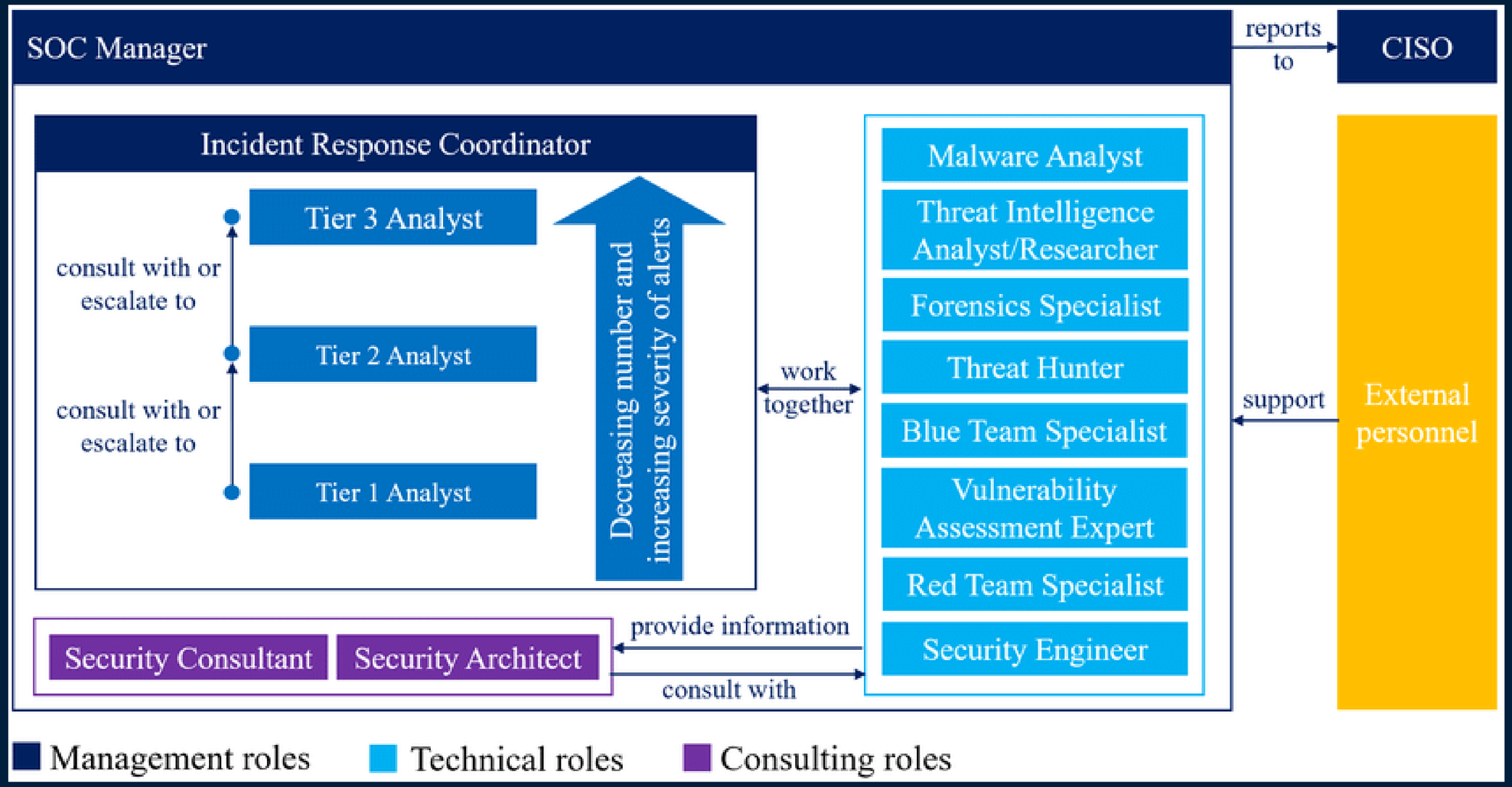


image : https://www.researchgate.net/figure/Interaction-of-different-roles-within-a-SOC-79_fig4_347520429

Process

the development and implementation of effective procedures, workflows, and protocols for incident detection, analysis, and response. It ensures a systematic and organized approach to managing cybersecurity incidents within the SOC.

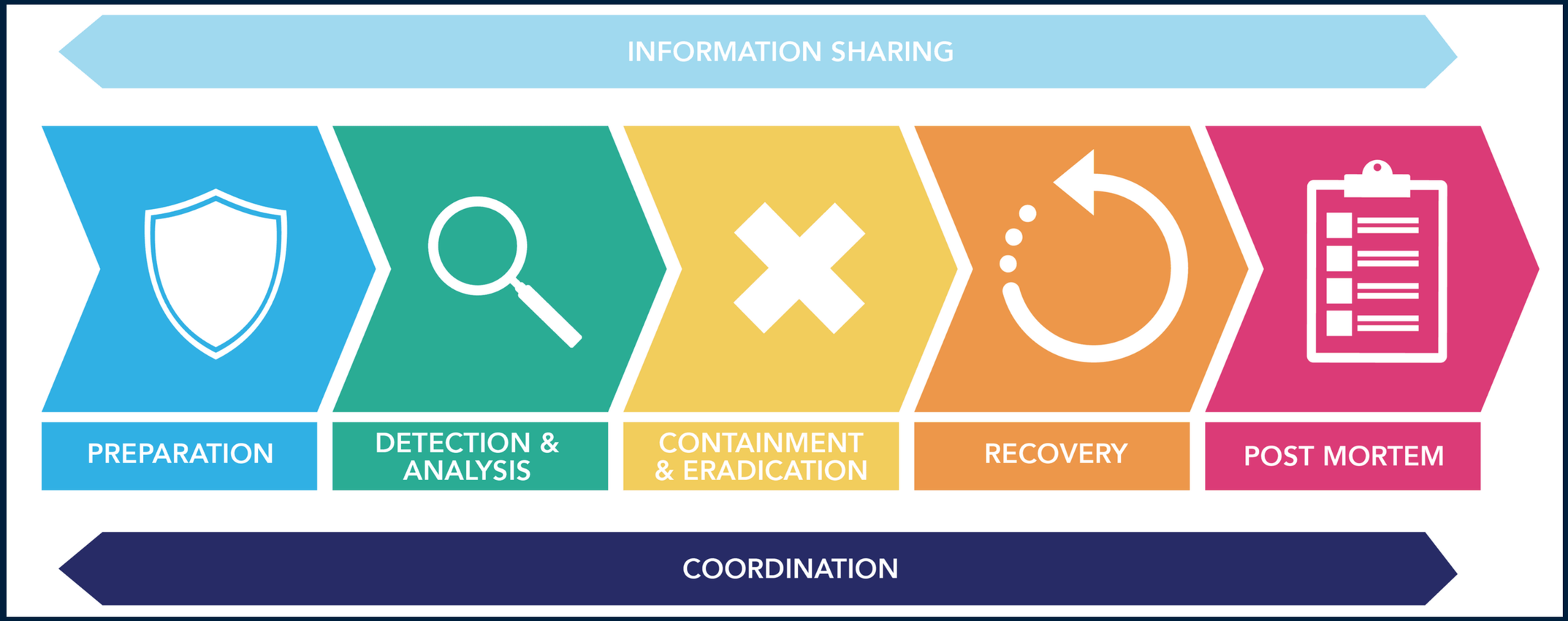


image : https://www.polymerhq.io/blog/how-to-apply-incident-response-for-saas/

Technology

the tools, technologies, and infrastructure used to monitor networks, analyze security data, and respond to incidents.
Good technology needs good people

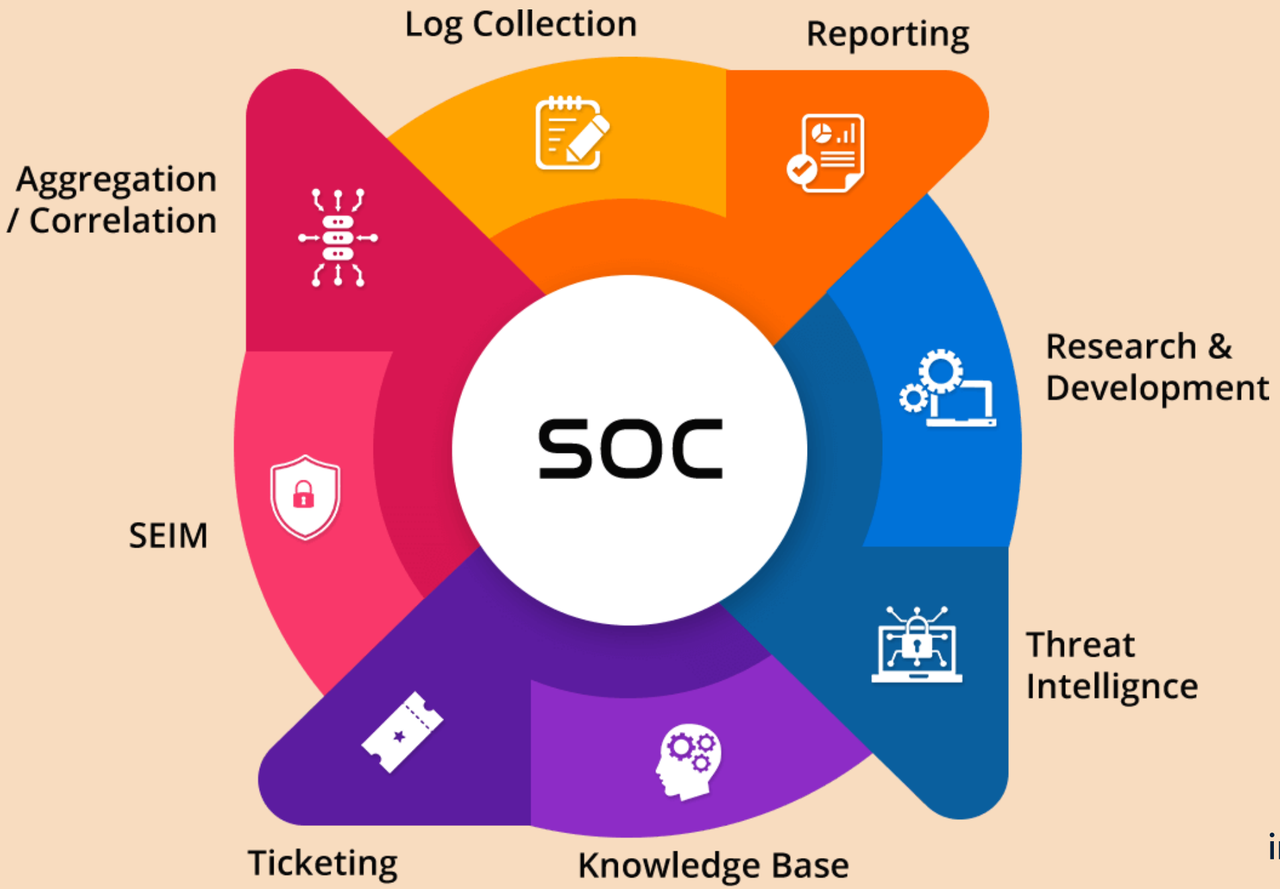


image : https://cetark.com/soc.html

The Models of SOC (1/2)

SOC-as-a-Service

Customer Target:
Small to mid-sized organizations.
Pros:

- Cost-effective with a subscription-based model.
- Access to specialized security expertise.
- Scalability without the need for in-house infrastructure.

Cons:

- Limited control over the security infrastructure.
- Potential concerns about data confidentiality.

Co-Managed SOC

Customer Target:
Organizations with an existing internal SOC collaborating with a third-party provider.
Pros:

- Utilizes both in-house and external expertise.
- Enhanced 24/7 monitoring and response capabilities.
- Collaboration allows for knowledge exchange.

Cons:

- Requires effective coordination between internal and external teams.
- Potential challenges in aligning processes and workflows.

The Models of SOC (2/2)

Multifunction SOC / NOC

Customer Target:
Larger organizations.
Pros:

- Comprehensive monitoring of both security and network operations.
- Improved coordination between security and IT operations.
- Efficient use of resources for organizations with both functions.

Cons:

- Complexity in managing diverse tasks.
- Potential challenges in maintaining expertise in both areas.

Dedicated SOC

Customer Target:
Large enterprises with significant security needs and resources.
Pros:

- Complete control over security infrastructure and operations.
- Tailored to the specific needs and risks of the organization.
- Direct oversight of all security processes.

Cons:

- High upfront and operational costs.
- Resource-intensive to establish and maintain.
- May require ongoing investments in training and technology.

Command SOC

Customer Target:
Government agencies, critical infrastructure providers, or large enterprises with extremely high-security requirements.
Pros:

- Operates at the highest level of security and authority.
- Coordinates responses to complex, large-scale cyber threats.
- Typically involves collaboration with law enforcement and intelligence agencies.

Cons:

- High costs associated with maintaining a Command SOC.
- Requires stringent adherence to regulatory and compliance standards.

SOC Maturity Levels

Non-existent: the aspect is nit present in the SOC

Initial: The aspect is delivered in an ad-hoc fashion

Defined: The aspect is documented and delivered consistently

Managed: The aspect is managed using ad-hoc feedback on the quality and timeliness of deliverables

Quantitatively Managed: The aspect is systematically being measured for quality, quantity and timeliness of deliverables

Optimizing: The aspect is continuously being optimized and improved

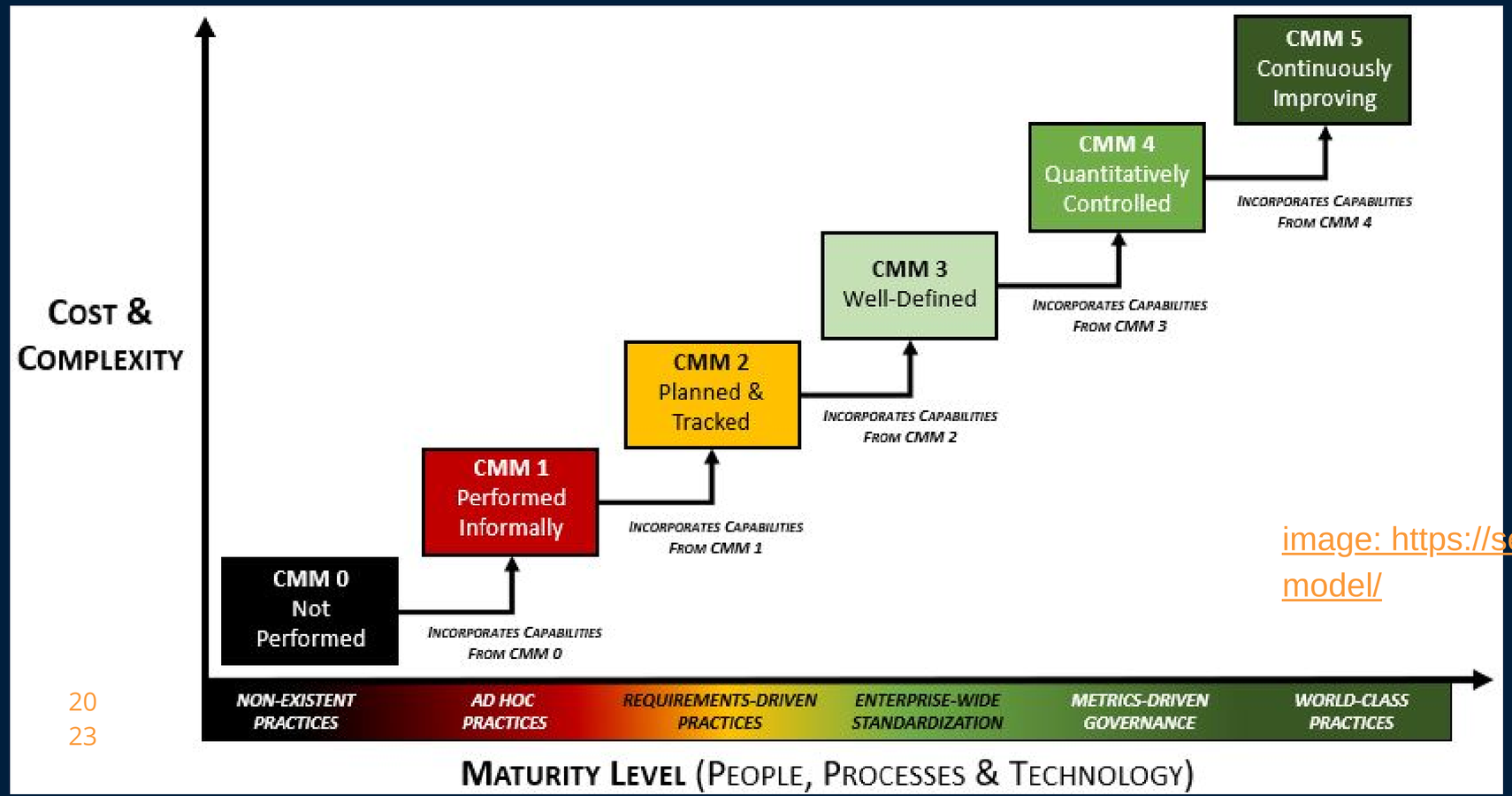


image: https://securecontrolsframework.com/capability-maturity-model/

Evolution of the SOC

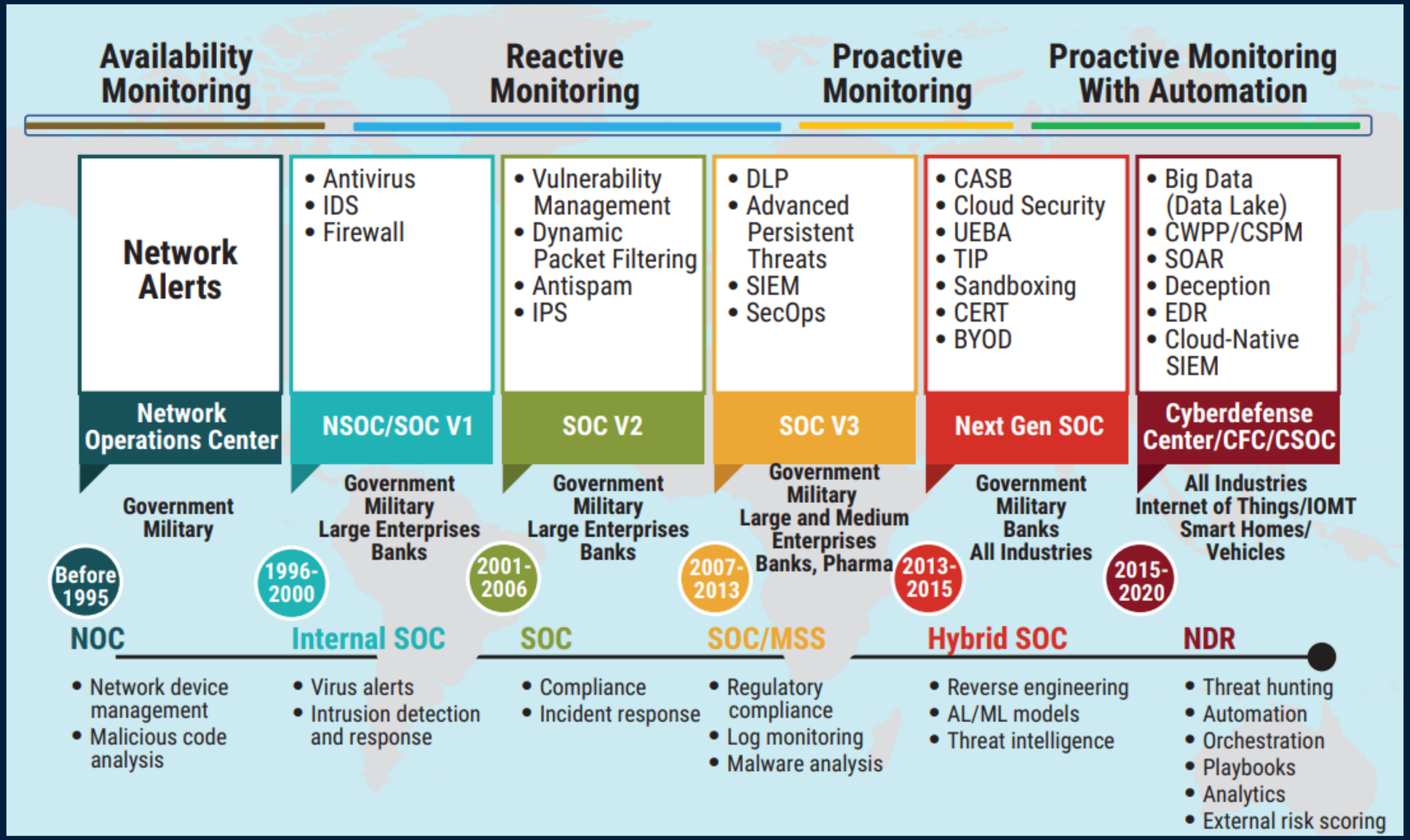


image: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc

Key Operational Components

Skilled Personnel

- The success of a SOC heavily relies on skilled individuals, including security analysts, incident responders, and SOC managers.
- Continuous training and development are crucial to keeping the team abreast of evolving threats and technologies.

Well defined Processes

- Effective SOC operations require well-defined processes and workflows to streamline incident response, threat intelligence integration, and continuous improvement.
- Processes ensure a systematic approach to managing cybersecurity incidents.

Technology

- SOCs leverage advanced tools such as Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Security Orchestration, Automation, and Response (SOAR).
- Automation plays a pivotal role in enhancing operational efficiency by handling routine tasks and allowing analysts to focus on critical issues.

image: https://www.imio.be/imio-et-vous/nos-valeurs/innovation

Key Business Considerations

Costs and Budgeting

- Running a SOC involves operational costs, including personnel salaries, technology investments, and ongoing training.
- Budgeting is essential to allocate resources effectively and ensure sustained operations.

Return on Security Investment (ROSI)

- A well-functioning SOC delivers a strong ROSI by preventing and mitigating cyber threats, reducing the impact of security incidents on the organization.
- SOCs provide immeasurable value in protecting sensitive data, maintaining business continuity, and safeguarding organizational reputation.

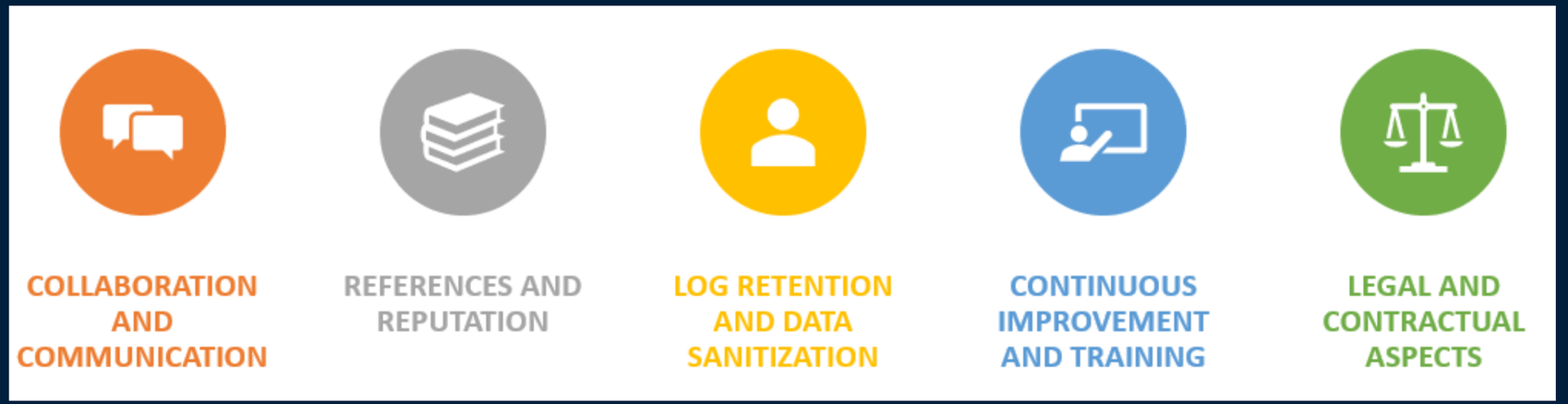
Key Performance Indicators (KPIs)

- Measuring SOC performance involves tracking key metrics such as mean time to detect (MTTD), mean time to respond (MTTR), and the number of incidents resolved.
- KPIs contribute to demonstrating the tangible business impact of the SOC.

Compliance and Reporting

- SOCs play a critical role in ensuring compliance with industry regulations and standards.
- Accurate reporting and documentation are imperative for meeting regulatory requirements.

How to choose your SOC Partner/Provider



How to start a SOC analyst career

- **Networking and IT Fundamentals:** Linux, windows, cisco, Fortinet....
- **Cybersecurity Fundamentals:** Comptia security+
- **Learn Cloud Technologies:** AWS, GCP, Azure
- **Master a SIEM:** ELK stack, Qradar, Microsoft Sentinel, splunk
- **Create Your Own Lab**
- **Engage in Platforms and Challenges:** TryHackMe, Hack The Box, Let's Defend, and participate in Capture The Flag (CTF) challenges
- **Seek Professional Advice**
- **Apply for Internships or Entry-Level Positions**
- **Develop Soft Skills**

What Makes a Difference in your SOC? (1/2)

- Effective Leadership and Management
- Skilled and Well-Trained Personnel
- Well-Defined Processes and Workflows
- Advanced Technologies and Tools
- Proactive Threat Intelligence Integration
- Collaboration and Communication
- Continuous Monitoring and Analysis
- Incident Response Planning

What Makes a Difference in your SOC? (2/2)

- Regular Auditing and Compliance
- Investment in Automation and Orchestration
- Learning from Incidents
- Strong Relationships with External Entities
- Cybersecurity Awareness and Training
- Metrics and Key Performance Indicators (KPIs)
- Community Engagement and Information Sharing
- Ethical and Legal Considerations

image: https://nell-associes.com/formation/resolution-de-probleme-un-defi-creatif/

THANK YOU

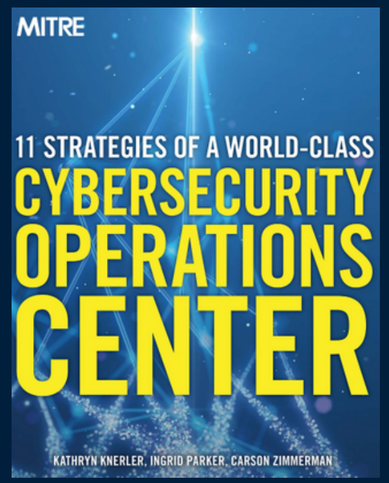
image: https://tunisie.co/article/15187/golf/reserver/la-neige-c-est-ain-drahem-120117

Riadh Brinsi

Cyber Security Manager | Air Force Veteran

Medium: https://medium.com/@br.riadh

References


MITRE
11 STRATEGIES OF A WORLD-CLASS
CYBERSECURITY
OPERATIONS
CENTER
KATHRYN KNERLER, INGRID PARKER, CARSON ZIMMERMAN


ISACA
ONLINE
EXCLUSIVE

Acronyms

- AI/ML: Artificial Intelligence/Machine Learning
- BYOD: Bring Your Own Device
- CASB: Cloud Access Security Broker
- CERT: Computer Emergency Response Team
- CFC: Cyber Fusion Center
- CSOC: Cyber Security Operations Center
- CSPM: Cloud Security Posture Management
- CWPP: Cloud Workload Protection Platform
- DLP: Data Loss Prevention
- EDR: Endpoint Detection and Response
- IOT/IOMT: Internet of Things/Internet of Medical Things
- IPS: Intrusion Prevention System
- SecOps: Security Operations
- SIEM: Security Information and Event Management
- SOAR: Security Orchestration, Automation, and Response
- TIP: Threat Intelligence Platform
- UEBA: User and Entity Behavior Analytics