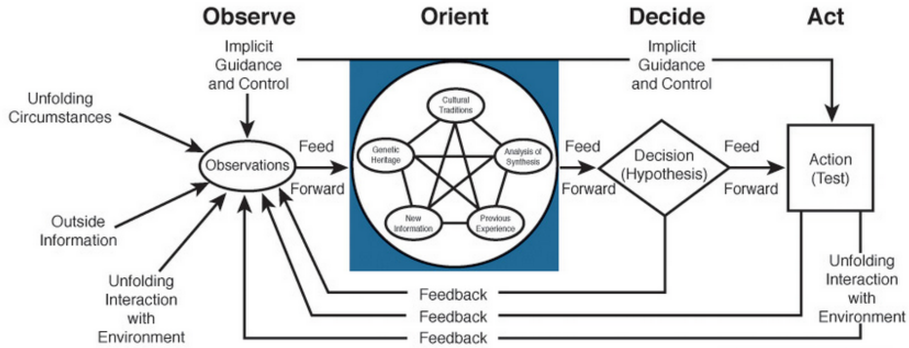
Chapter 1. Introduction to Security Operations and the SOC

Cybersecurity Challenges

As attacks become more sophisticated, intelligent monitoring integrated in a incident response program have to evolve.

To handle Cybersecurity threats and hacks, the cybersecurity industry has adopted a strategy called the **OODA Loop**.

- *Observe:* Monitor, collect and store data from various points in your network.
- *Orient:* Analyze collected data in search of suspicious activities.
- *Decide:* Determine an action course based on the results of the analysis phase and the experience you have gained from previous loop iterations.
- *Act:* Execute the action course you decided in the previous step.



John Boyd's OODA Loop

Figure 1: OODA Loop

To attack a target, the hackers follow another strategy, called the **Cyber Kill Chain**

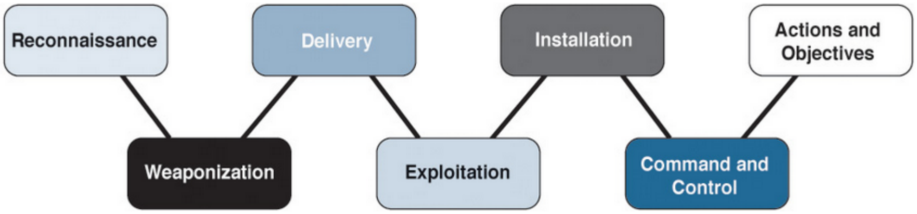


Figure 2: Cyber Kill Chain

- *Phase 1, Reconnaissance:* Research, Identification and selection of targets (Websites, Mailing lists…)

- *Phase 2, Weaponization:* Coupling a remote-access Trojan with an exploit into a deliverable payload.
- *Phase 3, Delivery:* Transmission of the weapon to the targeted environment.
- *Phase 4, Exploitation:* Triggers the intruder's code.
- *Phase 5, Installation:* Installation of a remote-access Trojan or back door. (To maintain persistence)
- *Phase 6, Command and Control:* Establish connection with C&C server
- *Phase 7, Actions and Objectives:* Intruders take actions to achieve their original objectives. (Collect sensitive information, cause damage, or move laterally, to access another system)

Attackers perform reconnaissance to identify the easiest and most effective way to breach a network. Defense teams using the OODA Loop can catch this behavior and proceed accordingly. The OODA Loop is a defense strategy against every phase of the cyber kill chain.

Threat Landscape

Breaches tend to happen very quickly and on average take a long time to be detected by the targeted organization.

Hackers and Cybersecurity experts are always going to play the cat and mouse game, because once one knows about the actions of another, it changes their own to bypass given actions.

Business Challenges

Legal and business-imposed decisions impact the way organizations operate information security. Examples of these decisions include:

- Moving Infrastructure to the cloud
- Proliferation of Bring Your Own Device
- Meeting company requirements

The Cloud

According to various studies, security is one of the top concerns of CIO to migrating to the Cloud but the Cloud is here to stay.

Compliance

Being compliant with mandatory or discretionary information security or privacy standards requires not only an investment in technology but also, in almost all cases, a fair amount of culture change.

Examples of security standards many organizations must comply with are:

- *Payment Card Industry Data Security Standard (PCI DSS)*
- *ISO/EIC 27001:*2013

Privacy and Data Protection

In addition to business-centric standards, companies must adhere to country-specific standards.

Introduction to information assurance

- *Information Assurance:* Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Different countries have different definitions of Information Assurance, so it is necessary to know your countries definition.

Information Security is a subset of Information Assurance. (IA takes into consideration human error, like loosing a USB stick, while IS does not, and is threat-centric)

Introduction to risk management

- *Risk:* The probability of a threat executing on vulnerability and the impact resenting from successful exploitation
- *Risk Assessment:* The process of assigning some value to risk associated with assets. (To make informed decisions like: *mitigate, transfer, accept, avoid*)
- *Risk Management:* Combining the output of risk assessment with the decision on how to address risk.

A popular Risk Assessment Methodology is: **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation).

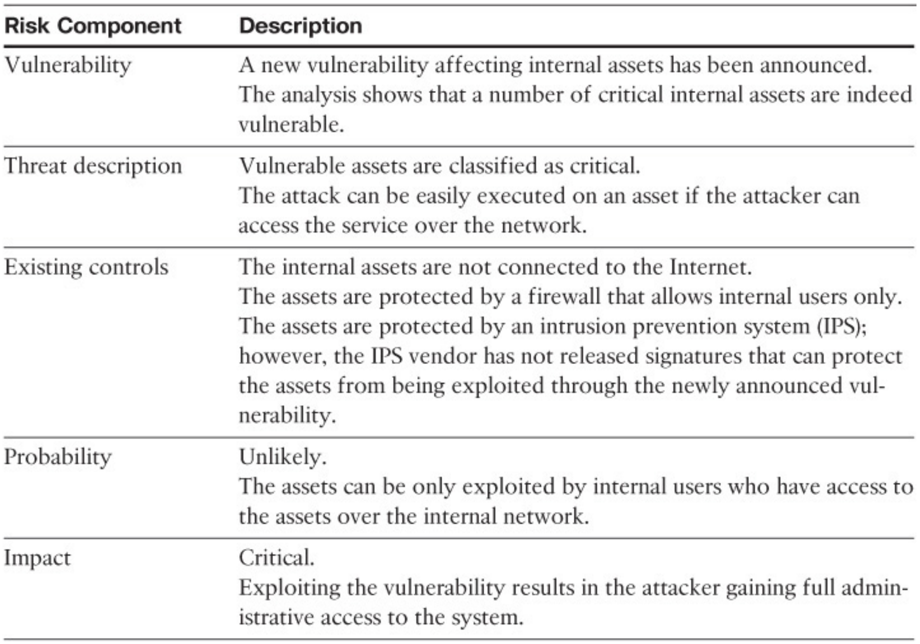
Based on the probability and Impact values generated for the specific event, we can now match the event to a cell in the Risk Heat Map, and act upon it if according to our pre-specified Risk Mitigation policy.

Information Security Incident Response

The team assigned to security operations is expected to monitor the organization's assets within scope and react to security events and incidents, including the detection and investigation of what would be considered indicators of compromise (IOC). A example of a IOC might be a USB being connected to the System when the security policy specifies otherwise.

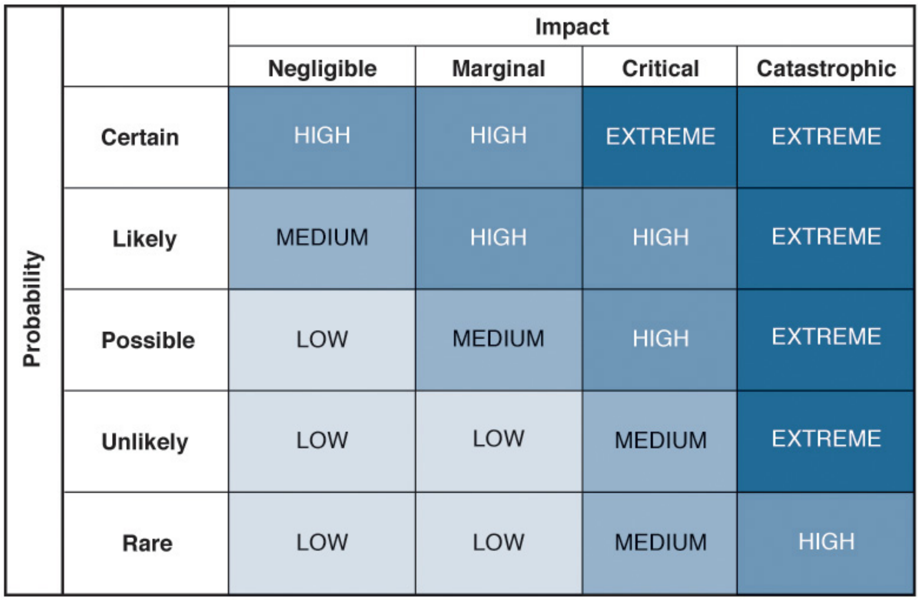
Responding to incidents starts by first detecting that an incident has actually occurred.

Preparing a SOC to manage incidents extends to cover people, processes, and, of course, technology. A SOC is expected to educate users of the security measures



Risk Component	Description
Vulnerability	A new vulnerability affecting internal assets has been announced. The analysis shows that a number of critical internal assets are indeed vulnerable.
Threat description	Vulnerable assets are classified as critical. The attack can be easily executed on an asset if the attacker can access the service over the network.
Existing controls	The internal assets are not connected to the Internet. The assets are protected by a firewall that allows internal users only. The assets are protected by an intrusion prevention system (IPS); however, the IPS vendor has not released signatures that can protect the assets from being exploited through the newly announced vulnerability.
Probability	Unlikely. The assets can be only exploited by internal users who have access to the assets over the internal network.
Impact	Critical. Exploiting the vulnerability results in the attacker gaining full administrative access to the system.

Figure 3: Risk Assessment Exercise



		Impact			
		Negligible	Marginal	Critical	Catastrophic
Probability	Certain	HIGH	HIGH	EXTREME	EXTREME
	Likely	MEDIUM	HIGH	HIGH	EXTREME
	Possible	LOW	MEDIUM	HIGH	EXTREME
	Unlikely	LOW	LOW	MEDIUM	EXTREME
	Rare	LOW	LOW	MEDIUM	HIGH

Figure 4: Risk Heat Map

they have to take, and update channels available for the users to report perceived security incidents. A typical Incident-Handling process follows the list of steps presented in the Incident Response Timeline.

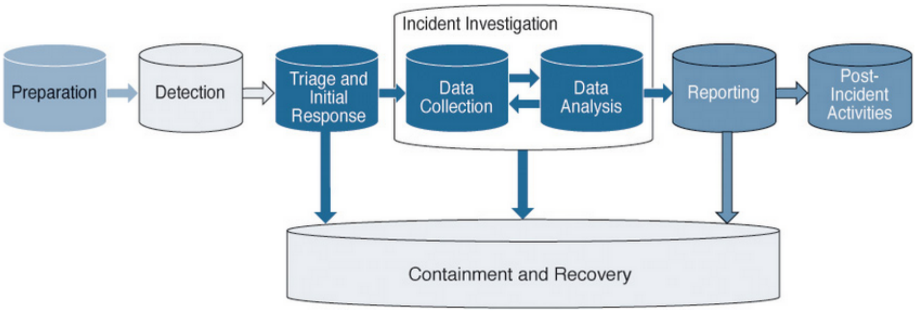


Figure 5: Incident Response Timeline

Incident Detection

- *Detection:* The phase in which an incident is observed and reported by people or technology, and the process that handles reporting aspects.

For the process to be effective, the following must be documented and formalized.

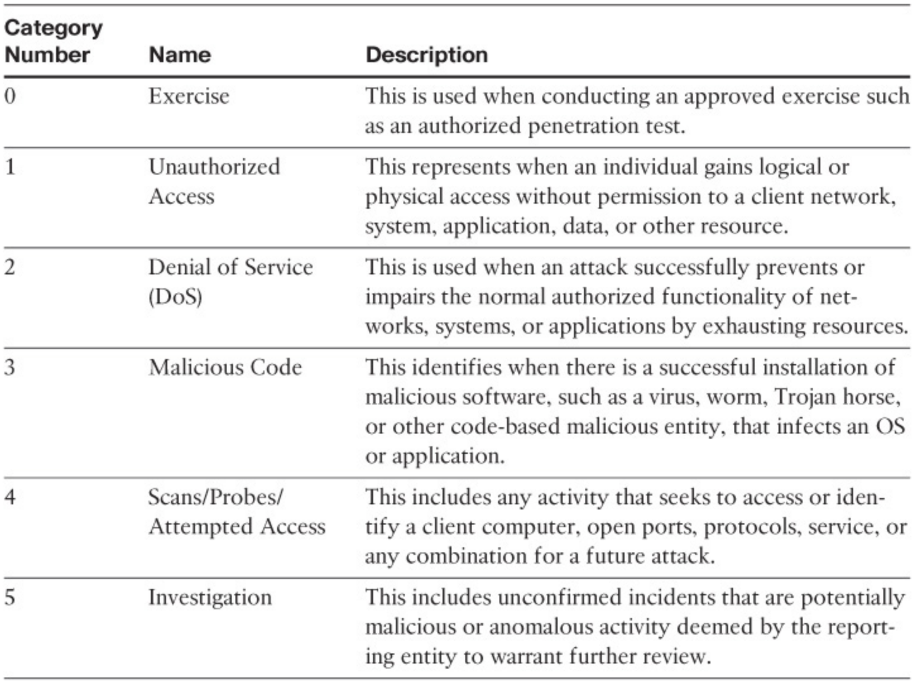
- *Identify sources:* People/technology responsible for detecting and reporting computer security incidents.
- *Identify channels:* through which computer security incidents should be reported.
- *Identify steps:* taken to accept and process computer security incident reports.
- *Identify requirements:* on people and technology for the process to work.

Incident Triage

- *Incident Triage:* represents the initial actions taken on a detected event that is used to determine the remaining steps according to the incident response plan.

This phase consists of three sub-phases, *verification, initial classification, assignment.* So that the organization might better understand incidents and categorize them.

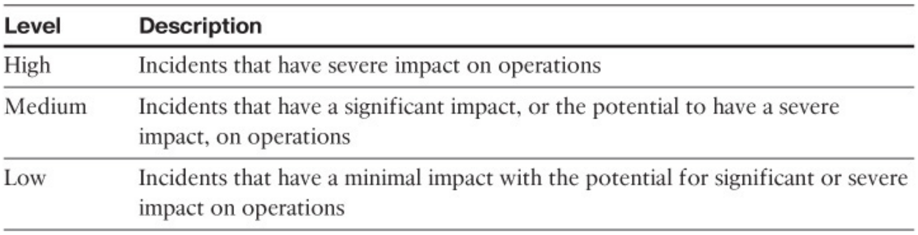
Incident Categories The category value identifies the type of the incident and its potential type of impact. Assigning a category value helps the SOC allocate the appropriate resources to analyze and investigate a computer security incident.



Category Number	Name	Description
0	Exercise	This is used when conducting an approved exercise such as an authorized penetration test.
1	Unauthorized Access	This represents when an individual gains logical or physical access without permission to a client network, system, application, data, or other resource.
2	Denial of Service (DoS)	This is used when an attack successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources.
3	Malicious Code	This identifies when there is a successful installation of malicious software, such as a virus, worm, Trojan horse, or other code-based malicious entity, that infects an OS or application.
4	Scans/Probes/ Attempted Access	This includes any activity that seeks to access or identify a client computer, open ports, protocols, service, or any combination for a future attack.
5	Investigation	This includes unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Figure 6: Computer Security Incident Table

Incident Severity Based on the expected or observed impact of an incident. Used for the prioritization of the incident.



Level	Description
High	Incidents that have severe impact on operations
Medium	Incidents that have a significant impact, or the potential to have a severe impact, on operations
Low	Incidents that have a minimal impact with the potential for significant or severe impact on operations

Figure 7: Incident Severity Levels

Once the incident has been categorized and it's severity level established, you can decide how to resolve the incident.

Incident Resolution The objective OD this phase is to discover the root cause of the incident while working on containing the incident at the earliest stage possible.

The analysis and investigation phase involves:

- Identifying compromised systems and accounts
- Understanding the impact of the computer security incident
- Identifying unauthorized access attempts to confidential data
- Understanding the chain of events that have lead to the computer security incident

The containment phase involves the actions performed to quickly stop a computer security incident from escalating or spreading to other systems.

Incident Closure Refers to the eradication phase in which all incident traces have been cleansed. If the incident has violated regulatory requirements, you should notify external entities.

Post-incident The "Lessons-learned" phase. This phase is aimed at feeding back useful knowledge obtained through the previous phases.

SOC Generations

Characteristics of an Effective SOC

- *Executive Sponsorship:* High-level roles in the organization (CEO, CIO) sign and sponsor the program
- *Governance:* Establish metrics to measure the effectiveness of the SOC capabilities

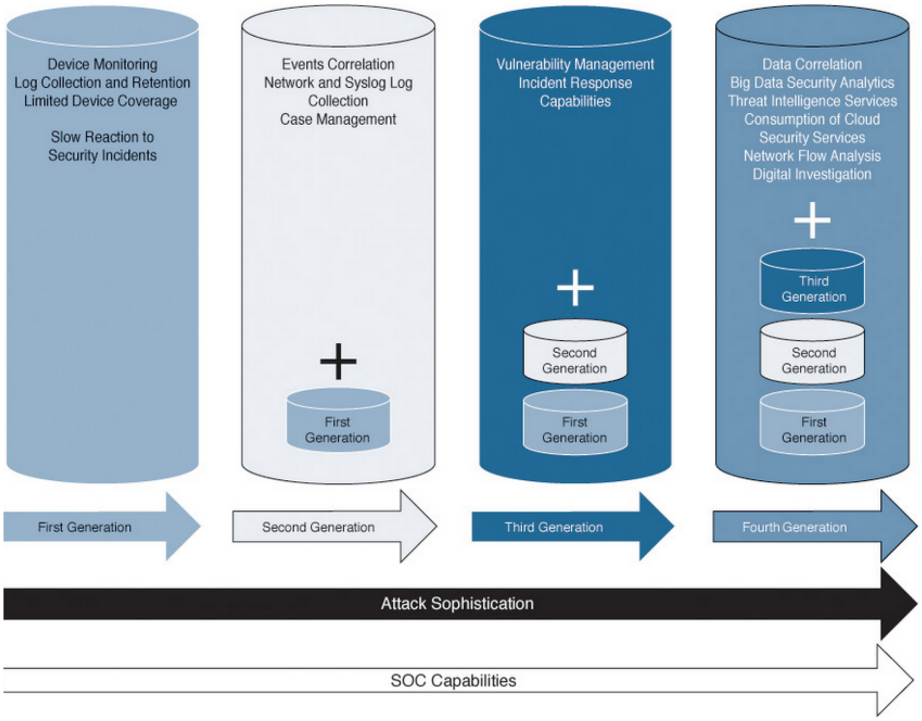


Figure 8: SOC Generations

- *Operate SOC as a program:* Elevates the importance of the SOC, and allows it to be implemented in different areas/projects of the company
- *Collaboration:* Different units of the program must collaborate during the plan, design, build and operate phases of the SOC
- *Access to data and systems:* Must be provided to the SOC team so they can perform their task
- *Applicable processes and procedures:* The team must be equipped with established knowledge and procedures
- *Skill set and experience:* The team must be equipped with the necessary skill set that enables them to do their task
- *Budget:* needed based on factors such as: In-house vs SOC outsourcing, The service provided by the SOC, The SOC operation hours, The skill set gap

Introduction to Maturity Models

- *Maturity Models:* Are IT governance tools used to describe management processes with respect to standardization, repeatable processes and results, and measurement of effectiveness.

Scores for the maturity model are based on an assignment of a 0-5 score. Using a maturity model helps you measure your current capabilities and track progress against goals.

Applying Maturity Models to SOC

Proposed SOC capabilities in three areas:

- People
  - Structure
  - Relative SOC Knowledge and experience
  - Training and awareness
- Process
  - Incident triage
  - Incident reporting
  - Incident analysis
  - Incident closure
  - Post-incident
  - Vulnerability discovery
  - Vulnerability remediation
- Technology
  - Network infrastructure readiness
  - Event collection, correlation, and analysis
  - Security monitoring
  - Security control
  - Log management
  - Vulnerability assessment

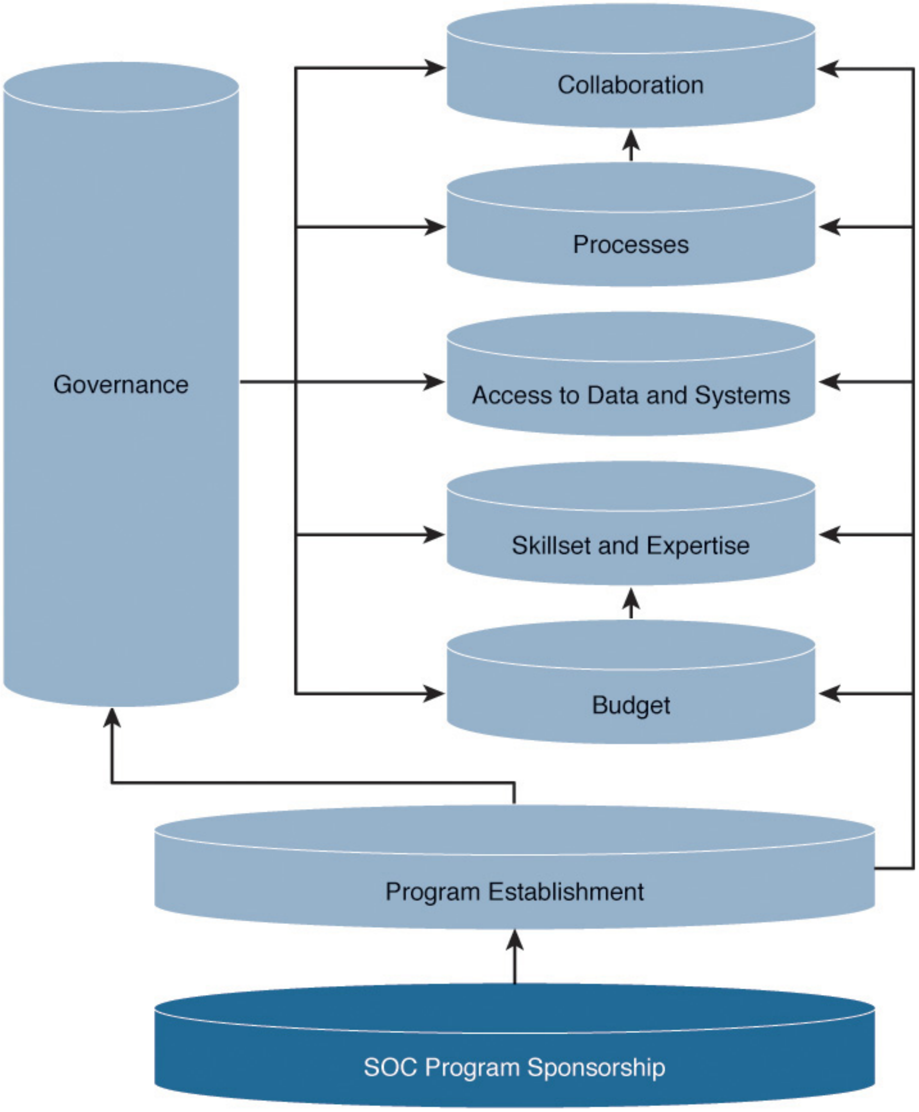
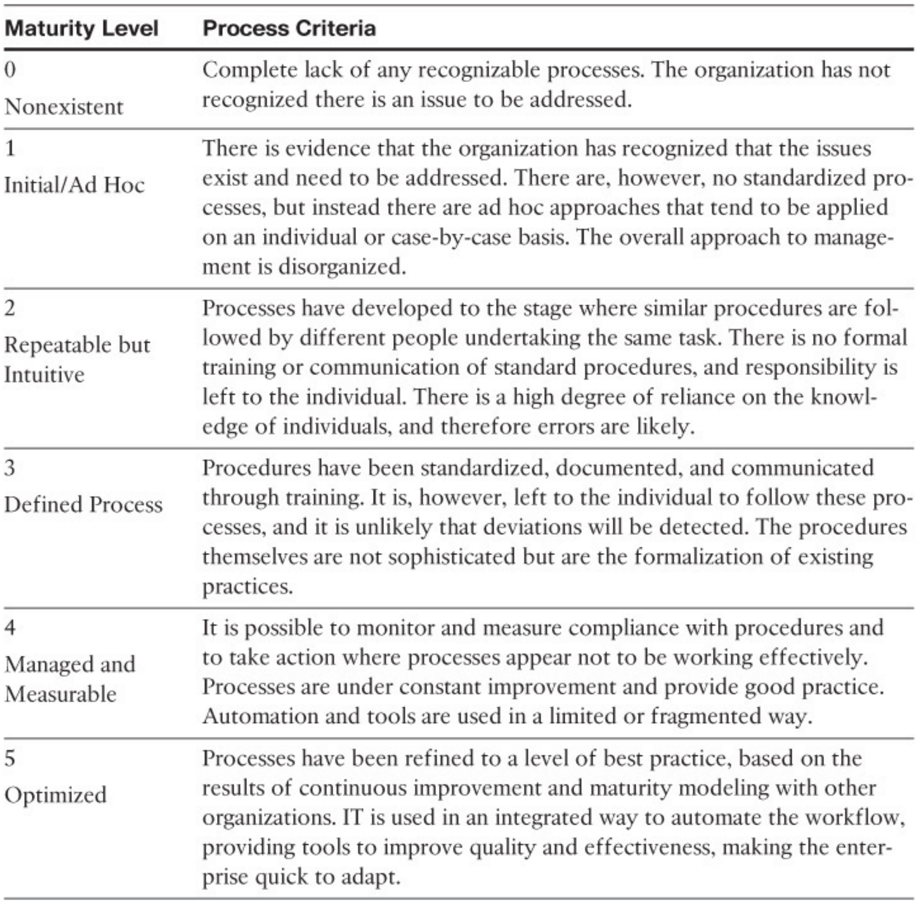


Figure 9: SOC characteristics



Maturity Level	Process Criteria
0 Nonexistent	Complete lack of any recognizable processes. The organization has not recognized there is an issue to be addressed.
1 Initial/Ad Hoc	There is evidence that the organization has recognized that the issues exist and need to be addressed. There are, however, no standardized processes, but instead there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.
2 Repeatable but Intuitive	Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals, and therefore errors are likely.
3 Defined Process	Procedures have been standardized, documented, and communicated through training. It is, however, left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices.
4 Managed and Measurable	It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
5 Optimized	Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modeling with other organizations. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

Figure 10: COBIT Maturity Model

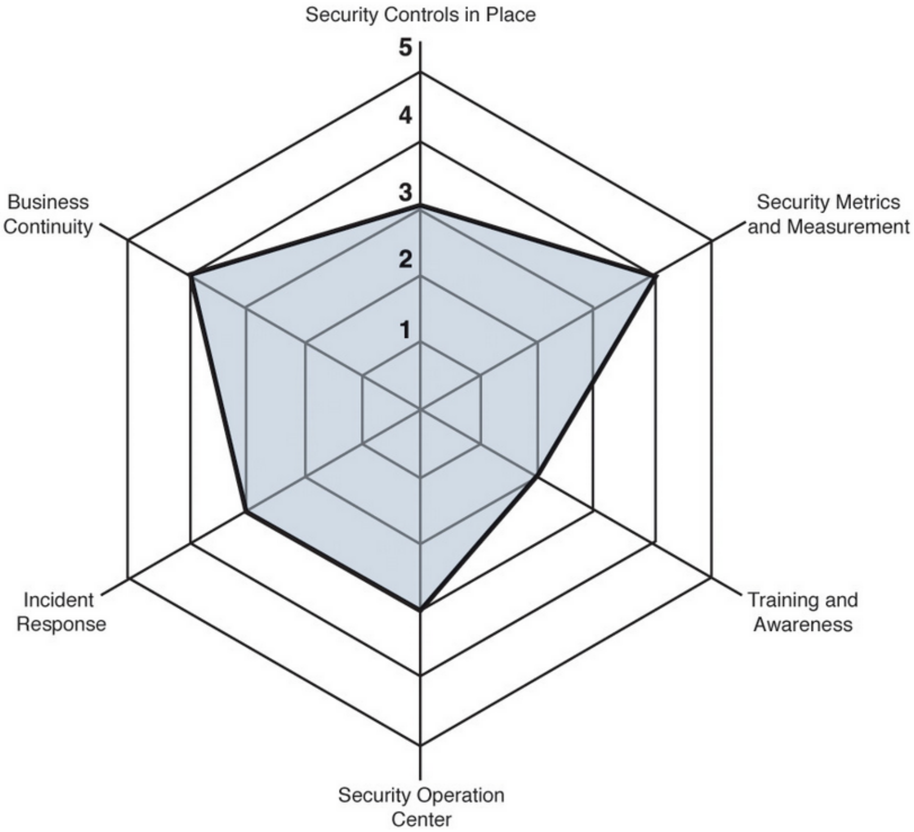


Figure 11: Capability Level: Security Operations

  - Vulnerability tracking
  - Threat intelligence

Graphically represented Process capabilities:

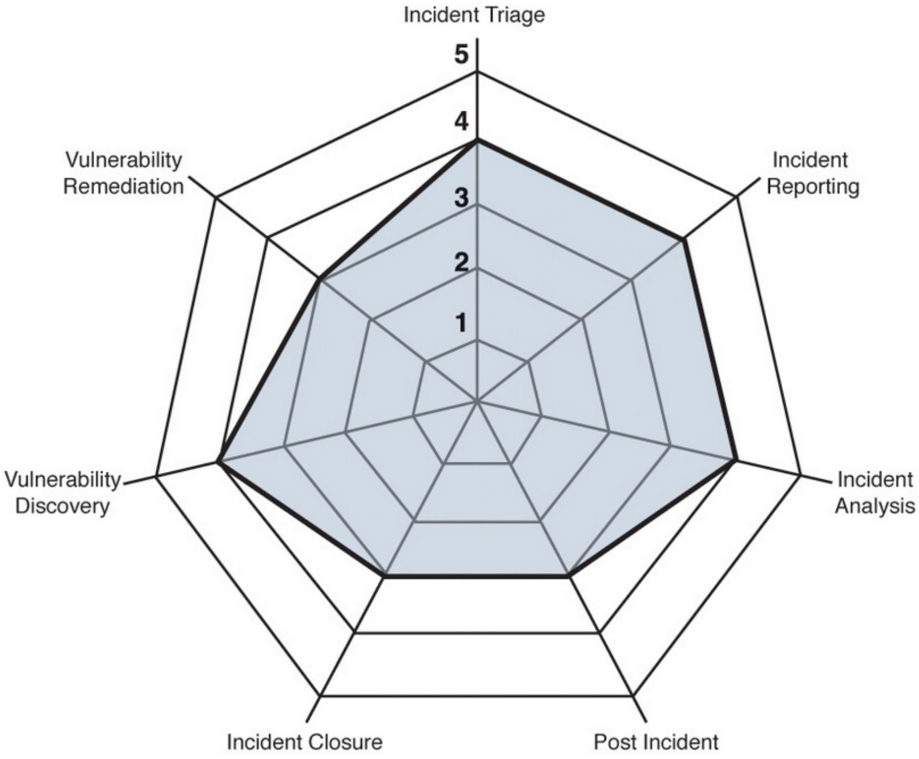


Figure 12: SOC Capabilities

Phases of Building a SOC

Most common phases of building a SOC: *Plan, Design, Build, Operate, Transfer*

Challenges and Obstacles

Establishing and maintaining a proper SOC relies heavily on proper planning, there are almost always challenges that are specific to the organization. These challenges are introduced because of issues related to governance, collaboration, skill sets, and so on.

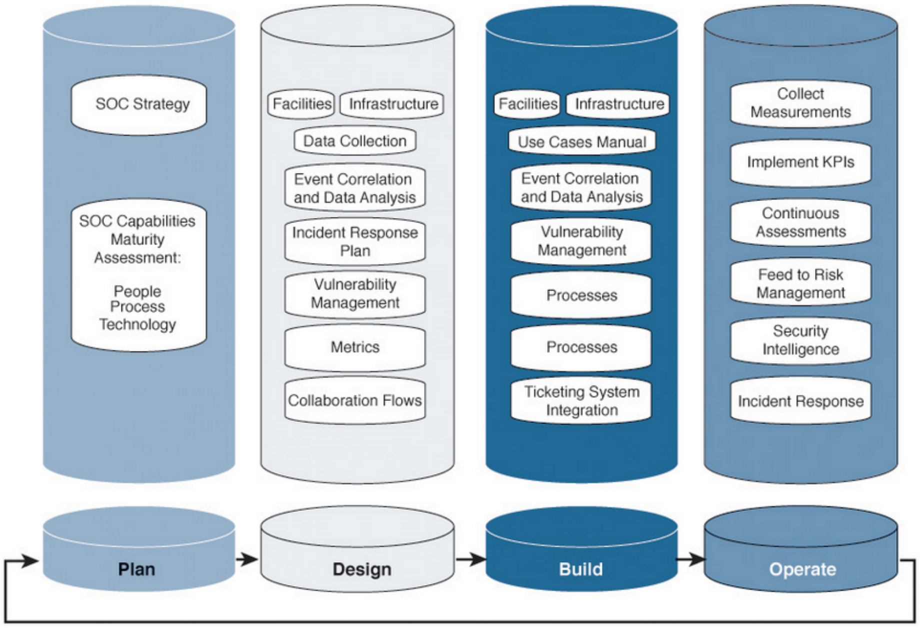


Figure 13: Phases of building a SOC