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.

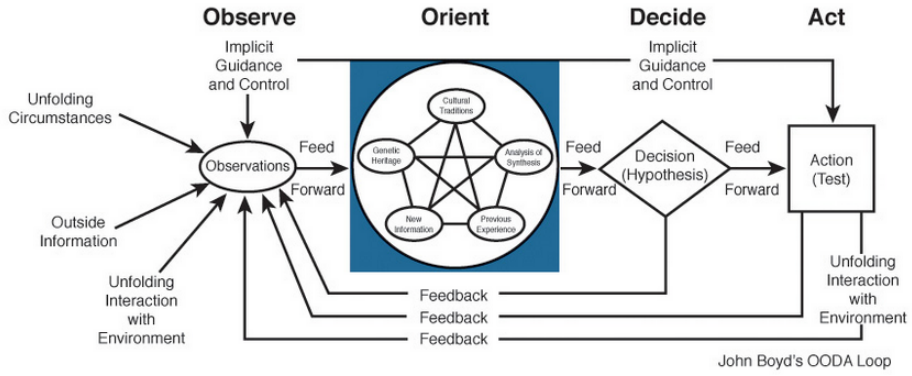

Figure 1: OODA Loop

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

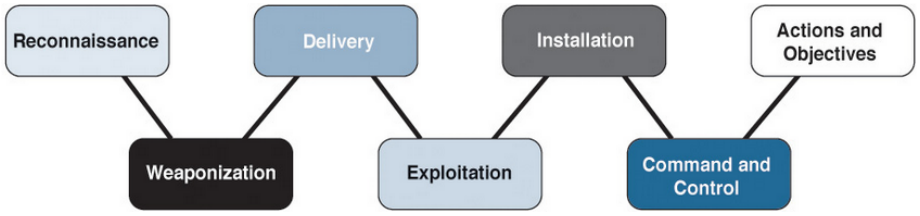

Figure 2: Cyber Kill Chain

- *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

Probability		Impact			
		Negligible	Marginal	Critical	Catastrophic
	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.

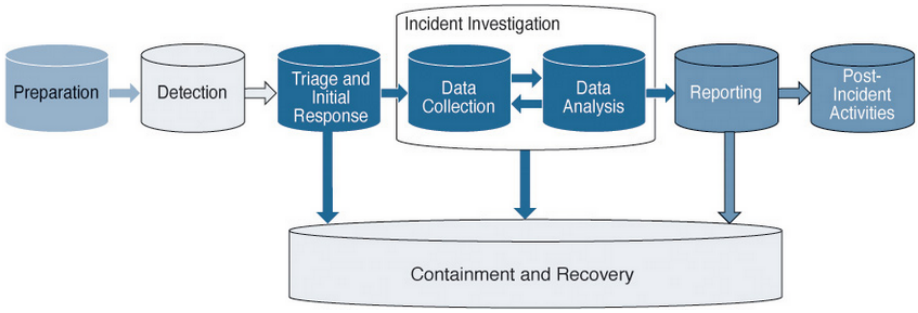

Figure 5: Incident Response Timeline

Incident Detection

SOC Generations

Characteristics of an Effective SOC

Introduction to Maturity Models

Applying Maturity Models to SOC

Phases of Building a SOC

Challenges and Obstacles

Summary