

**INTRODUCTION TO SOC AND CYBERSECURITY**  
**FUNDAMENTALS**



**WEEK 1: INTRODUCTION TO SOC  
AND CYBERSECURITY  
FUNDAMENTALS**

**SECURITY OPERATIONS  
CENTER - ASSIGNMENT**



***SIVA KRISHNA***

# **INTRODUCTION TO SOC AND CYBERSECURITY FUNDAMENTALS**

## **1.SCOPE:**

### **Definition:**

This week's assignments will learn about the basics of a Security Operations Center and its essential role in today's cybersecurity landscape. This will help distinguish a SOC from a NOC, analyze the difference in job roles within a SOC, work with core concepts in cybersecurity that you are more than likely to encounter (the CIA Triad), and use the MITRE ATT&CK framework to analyze several different attack vectors.

## **2.OBJECTIVE:**

### **Goal:**

The first objective is to have a general overview of SOC operations, roles, and critical cybersecurity principles. This includes How a SOC differs from a NOC, Tier-wise job responsibilities within a SOC, CIA Triad, and common attack vectors.

### **Learning outcomes:**

At the end of this assignment, you should be able to:

- ❖ Understand the purpose and function of SOC in an organizational context.
- ❖ Identify the Tier 1, Tier 2, and Tier 3 analyst roles and responsibilities within SOC.
- ❖ So, understand the fundamental meaning of the CIA Triad in cybersecurity.
- ❖ Admit new threats such as malware and phishing and determine their impact.
- ❖ Use the MITRE ATT&CK framework to investigate and document their attack vectors.

## **3.Procedure:**

### **Assignment 1: Research SOC Operations**

#### **What is a SOC (Security Operations Center)?**

A Security Operations Center, in simple terms, is the centralized team of the firm that protects and responds to incidents of cybersecurity threats. The SOC team uses technology, processes, and skilled people to protect the assets of the organization from various cyber threats. The assets comprise data, networks, applications, and devices.

#### **The purpose and objectives of a SOC:**

### **Continuous Screening:**

# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

The SOC runs 24/7, constantly monitoring the organization's IT environment for security threat identification in real time. This generally involves monitoring the data feed coming from various sources such as firewalls, intrusion detection systems (IDS), endpoint detection and response (EDR), and security information and event management (SIEM) tools.

### **Identify and analyze threats:**

The SOC can also detect the presence of malicious activity including unknown login attempts, malware infections, and network problems. Analysts use threat intelligence and more sophisticated tools to discover such activities at the earliest stages.

### **Incident Response:**

If the SOC team finds a security issue, it takes quick steps to control, mitigate, and remediate the threat. This can include isolating affected systems, removing malware, or blocking malicious IP addresses. Then, great efforts are made to cause minimal damage and resume normal operations as quickly as possible.

### **Proactive Threat Hunting:**

Beyond responding to notifications, a SOC team also practices proactive threat hunting. They seek threats that have evaded automated security controls and otherwise have relied on behavior-based analysis and anomaly detection.

### **Reporting and Compliance:**

SOC teams also provide reports in case of security incidents, emerging threat trends, and general security conditions. Such reports assist in observing the industry's rules and regulations and in abiding by the laws that are majorly GDPR, HIPAA, and PCI-DSS.

### **Key features of a SOC:**

**People:** The SOC team is a diverse group of workers, including security analysts, incident responders, threat hunters, and managers, performing their specific tasks - from alert watching to detailed forensic analysis.

**Processes:** Clear processes are very important to ensure the SOC is operating correctly. These plans include the incident response plan, procedures for escalation, and communications rules. These ensure immediate and reliable reactions by the team toward security incidents.

# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

**Technology:** A SOC depends upon an extensive array of security technologies, including:

**Security Information Event Management SIEM:** These systems collect and analyze logs from different places.

**IDS/IPS Intrusion Detection/Prevention Systems:** Identifies and prevents potential threats.

**Endpoint Detection and Response(EDR):** Actually, scans devices for anomalous activities.

**Firewalls and Anti-Virus Software:** First line of defense against known threats.

### **Why a SOC Is Important for Today's Organizations?**

More Cyber Threats Due to rising threats of complex cyber-attacks in the forms of ransomware, phishing, and Advanced Persistent Threats (APTs), organizations need a special team for some their valuable assets.

**Real-Time Threat Detection:** A SOC will help one access or spot threats in the quickest way possible with their response. This reduces chances of data breaches and minimizes the potential damage by cyber incidents.

**Enhanced Incident Response:** A SOC can deliver the capability of clear, effective incident response for organizations, serving a significant reduction of the effects of cyber-attacks.

**Regulatory Compliance:** Many industries have strict rules about data security. A SOC helps organizations follow these rules, preventing expensive fines and harm to their reputation.

**Purpose:** A SOC is the heart of an organization that uses people, processes, and technology to protect and enhance the security of an organization. In a way, it seeks to prevent, detect, analyze, and respond to cybersecurity problems. The ultimate purpose of a SOC is to detect threats early enough so that it can counter them even before they are allowed to do harm.

# **INTRODUCTION TO SOC AND CYBERSECURITY FUNDAMENTALS**



## **Difference Between SOC and NOC:**

<b>Feature</b>	<b>SOC (Security Operations Center)</b>	<b>NOC (Network Operations Center)</b>
<b>Primary Focus</b>	Cybersecurity and threat management	Network performance and availability
<b>Main Goal</b>	Protecting against cyber threats like malware, phishing, and DDoS attacks	Ensuring network uptime, reliability, and optimization
<b>Key Activities</b>	Threat detection, incident response, vulnerability management	Network monitoring, bandwidth management, troubleshooting
<b>Core Tools</b>	SIEM, IDS/IPS, EDR, threat intelligence platforms	Network monitoring systems, routers, switches, load balancers
<b>Skill Sets</b>	Cybersecurity analysis, forensics, incident handling	Network engineering, system administration, network optimization

# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

### **What is a SOC?**

A Security Operations Center (SOC) is a centralized unit responsible for monitoring and managing an organization's security posture. Its primary focus is on preventing, detecting, analyzing, and responding to cyber security incidents. SOC teams continuously monitor networks, systems, and applications for suspicious activities or security breaches. They employ various technologies like SIEM (Security Information and Event Management), threat intelligence, and advanced analytics to safeguard against cyber threats.

### **What is a NOC?**

A Network Operations Center (NOC) is another centralized unit tasked with overseeing and managing an organization's network infrastructure. NOC teams are responsible for monitoring network performance, troubleshooting issues, and ensuring uninterrupted network availability. They use network monitoring tools, performance metrics, and automation to identify and address network-related issues promptly. NOC plays a critical role in maintaining the reliability and efficiency of network operations.

#### **1. Main Focus**

SOC: Cybersecurity-(protection of organization against, e.g. malware, hacking, and data breaches).

NOC: The working of the network, with a focus on optimization and removing technical problems in order to avoid downtime.

#### **2. Primary Goal**

SOC: Protect sensitive data, detect threats, and respond to security incidents.

NOC: Maintain dependable, available, and efficient performance of the network and IT infrastructure.

#### **3. Activities**

SOC: Monitors for suspicious activities, investigates security alerts, handles cybersecurity incidents, and actively hunts for potential threats.

NOC: Watches over network health, does bandwidth monitoring, provides maintenance, and offers troubleshooting to keep the entire system up.

**4. Tools Used SOC:** Use of security tools, such as SIEM-I (Security Information and Event Management), IDS (Intrusion Detection Systems), firewalls, and EDR (Endpoint Detection and Response).



# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

NOC: Use of tools for network monitoring, performance analysis, routers, switches, and load balancers.

### **5. Skills Required**

SOC: Knowledge in cybersecurity, threat analysis, incident response, and forensics Engineering is valued for NOC: expert knowledge in network engineering, system administration, and troubleshooting network issues.

### **6. Threats vs. Performance**

SOC: Preventing and detecting cyber threats.

NOC: Performance and constantly maintaining system availability.

### **7. Members of the Team**

SOC: Security analyst, incident responder, and threat hunter.

NOC: Network engineer, system administrator, and network support specialist.

### **In summary,**

SOC protection against attacks within a cybersecurity context.

NOC performance of the network in order to keep the system operational fully. Hence, both of these are very important for the IT infrastructure of an organization as they deal with various points and focus on different objectives and responsibilities.

### **Real-World Examples**

- ❖ Online retailers and law firms, which operate outside normal business hours, may require a NOC to ensure network functionality.
- ❖ Businesses with dedicated internal IT teams may choose to establish a NOC for full-service network assistance, while those requiring exclusive security assistance may opt for a SOC.

### **SOC and NOC: Key Challenges**

Both the Security Operations Center (SOC) and the Network Operations Center (NOC) are essential to the operational integrity and security of an organization's IT infrastructure. However, they face unique challenges that can impact their effectiveness. Understanding these challenges is vital for enhancing the performance and collaboration between these two critical teams.

### **Challenges Faced by Network Operations Center (NOC)**

Increasing Complexity of Network Infrastructure: As technology evolves, organizations are adopting complex systems such as cloud computing, virtualization, and software-defined networking. NOC professionals must

# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

continuously adapt to these changes, often requiring new skills and knowledge to effectively monitor and manage diverse environments.

**High Volume of Network Traffic:** The exponential growth of data and network activity can overwhelm NOC teams. Managing large traffic volumes requires efficient monitoring tools and processes to ensure that performance issues can be promptly identified and addressed.

**Resource Constraints:** NOC teams often operate under tight budgets and limited staffing, which can restrict their ability to respond to incidents effectively and maintain proactive monitoring practices.

**Service Level Agreement (SLA) Management:** Meeting SLAs can be challenging, especially when unexpected outages or performance issues occur. NOC teams must quickly resolve issues to ensure compliance, which can be difficult amidst the increasing complexity of network systems.

### **Challenges Faced by the Security Operations Center (SOC)**

#### **Evolving Threat Landscape:**

Cyber threats constantly evolve, with attackers using sophisticated techniques to infiltrate systems. SOC teams must stay ahead of these developments, which require ongoing training and implementing advanced security technologies.

**Resource Allocation and Staffing:** Like NOC teams, SOC teams often face challenges with staffing and budget constraints. Finding qualified security professionals is a significant hurdle, and high turnover rates can disrupt continuity and knowledge retention.

**Data Overload:** SOC teams are inundated with data from various sources, including logs, alerts, and threat intelligence feeds. Analyzing this vast amount of information to identify genuine threats while minimizing false positives is complex.

**Integration of Security Tools:** The effectiveness of a SOC relies on integrating multiple security tools and technologies. However, disparate systems can lead to inefficiencies and gaps in security coverage, making it difficult to respond to threats in a timely manner.

**Interdepartmental Communication:** Effective communication and collaboration between SOC and other departments, including the NOC, are



# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

crucial for a holistic security approach. Challenges in coordinating efforts and sharing information can lead to delays in incident response and increased vulnerability.

### **Conclusion:**

A Security Operations Center (SOC) is crucial for modern organizations to defend against the ever-growing landscape of cyber threats. By having a dedicated team focused on cybersecurity, organizations can protect their sensitive data, ensure business continuity, and maintain compliance with regulatory requirements. The SOC is the heart of an organization's security strategy, providing round-the-clock protection against cyber threats.

This comprehensive understanding of SOC should impress your professor by highlighting not only what a SOC is but also its significance, operations, and differentiating factors compared to other IT functions like a NOC.

### **Assignment 2 : Job Role Analysis**

#### **SOC Tiers and Responsibilities:**

##### **Tier 1: Security Analyst (Frontline)**

##### **Responsibilities:**

- ❖ Monitor alerts coming from SIEM and other security tools.
- ❖ Perform initial analysis and triage of events to determine the severity of an incident.
- ❖ Forward confirmed incidents to the higher tiers.

##### **Monitoring and Sorting Alerts:**

Keep a close watch on security alerts from SIEM (Security Information and Event Management) systems and other security tools.

Identify and classify potential security threats by the severity level and the type of warning.

##### **First Look:**

Do some basic checks on suspicious activities to see if they are wrong alerts or really dangers.

Check the logs, network traffic, and endpoint data for any signs of malware, unauthorized access, or harmful activity. Escalation:

# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

Refer verified or hard cases to Tier 2 analysts for validation or follow-up.  
Document findings and keep thorough records of incidents for reference purposes.

### **Skills Required:**

- ❖ Basic understanding of cybersecurity concepts.
- ❖ Some understanding of SIEM tools and knowledge of network protocols and log analysis.
- ❖ Strong analytical and problem-solving skills.

### **Current Skills Match:**

Basic understanding of SIEM and network protocols.

### **Tier 2: Incident Responder, Detailed Analyst**

#### **Responsibilities:**

- ❖ **In-Depth Analysis:**
- ❖ Conduct thorough investigations of incidents escalated by Tier 1 analysts to determine the scope and impact.
- ❖ Perform root cause analysis to identify how an attack occurred and which systems were affected.
- ❖ **Incident Response and Containment:**
- ❖ Develop and execute incident response plans to contain and mitigate threats.
- ❖ Implement containment measures such as isolating compromised systems, blocking malicious IP addresses, or removing malware.
- ❖ **Threat Intelligence and Reporting:**
- ❖ Leverage threat intelligence to understand the attacker's tactics, techniques, and procedures (TTPs).
- ❖ Generate detailed reports on incidents, including recommendations for improving security controls.

#### **Tasks:**

- ❖ To examine, closely, cases that Tier 1 has forwarded.
- ❖ Conduct root cause analysis and implement threat containment.
- ❖ Develop and implement an incident response strategy.

### **Skills Used:**

- ❖ Good understanding of cybersecurity threats and ways attackers operate.

# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

- ❖ Proficient in malware analysis, digital evidence investigation, and threat detection.
- ❖ Familiarity with the IDS/IPS and EDR tools.

### **Current Skills Match:**

Basic Understanding of Malware Analysis.

### **Tier 3: Threat Hunter / SOC Manager**

### **Responsibilities:**

#### **Proactive threat hunting:**

- ❖ Identify hidden risks and signs of compromise (IOCs) in the organization's environment.
- ❖ Advanced methods include behavior studies and unusual activity to uncover complex attacks which may evade automated security tools.

#### **Incident Management and Remediation:**

- ❖ This support will assist in responding to critical security incidents through coordination with internal and external partners.
- ❖ Long-term plans to prevent future attacks and make the security of the organization much stronger.

#### **Safety Plan and Improvement:**

- ❖ Create and implement security policies, playbooks, and standard operating procedures (SOPs) for the Security Operations Center (SOC). Do regular security checks, look for weaknesses, and test for breaks to find and fix security problems. Support and train Tier 1 and Tier 2 analysts.

### **Tasks:**

- ❖ Actively seek potential risks as informed by threat intelligence.
- ❖ Heavily leads incident response and threat mitigation activities.
- ❖ Design security policies, guidelines, and SOC procedures.

### **Technical Requirements:**

- ❖ Knowledge in understanding threats, searching for threats, and designing security systems.
- ❖ Very good leadership and planning abilities.
- ❖ Penetration testing and vulnerability assessment have evolved.

### **Current Skills Match:**

Basic skills and knowledge about Penetration Testing.

# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

### **Summary of SOC Tiers and Their Roles**

SOC Tier	Role Title	Key Focus	Responsibilities
<b>Tier 1</b>	Security Analyst	Real-time monitoring and alert triage	Monitor alerts, perform basic analysis, escalate incidents.
<b>Tier 2</b>	Incident Responder	In-depth investigation and incident response	Conduct detailed analysis, contain threats, generate reports.
<b>Tier 3</b>	Threat Hunter / SOC Manager	Proactive threat hunting and SOC management	Hunt for hidden threats, lead incident management, optimize security strategy

By having these three distinct tiers, SOC's ensure that they have the right level of expertise and focus at every stage of threat detection and response, thereby providing a robust defense against cyber threats.

### **Assignment 3: Cybersecurity Concepts Exercise**

#### **CIA Triad: Backbone of Cybersecurity**

The CIA Triad is the foundational model in cybersecurity, mirroring three interrelated critical principles: Confidentiality, Integrity, and Availability. As a result, these can be referred to as the cornerstones upon which information systems protect themselves, standing firm in guiding design, implementation, and management as far as security policies and practices are concerned. Success in the operation of a SOC largely emanates from how well the CIA Triad works to ensure comprehensive protection against cyber threats.

#### **Confidentiality**

**Definition:** Confidentiality ensures that sensitive information is only available to authorized users and is protected from unauthorized access or disclosure.

**Example:** This includes encrypting data, managing password strength, and implementing access controls to prevent unauthorized users from accessing

# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

sensitive files.

### **Importance in SOC:**

SOC teams monitor and protect data to prevent breaches that could expose sensitive information like customer data, intellectual property, or financial records. It helps defend against attacks like data breaches, phishing, and unauthorized access.

### **Integrity**

**Definition:** Integrity refers to the accuracy, consistency, and trustworthiness of data throughout its lifecycle. This includes preventing unauthorized data alterations, whether intentional (e.g., cyberattacks) or accidental (e.g., human error).

**Example:** Implementing hash functions, digital signatures, and checksums adds an extra layer of defense by detecting unauthorized changes to data files.

### **Importance in SOC:**

Ensures that data remains unaltered during storage, transmission, and processing. SOC teams use integrity checks to quickly identify tampering, data corruption, or unauthorized modifications caused by malware, ensuring that critical systems and data remain reliable.

### **Availability**

**Definition:** Availability ensures that information and resources are accessible to authorized users whenever needed, focusing on minimizing downtime and keeping systems, applications, and data operational to support business processes.

**Example:** Utilizing redundancy, backup systems, and robust disaster recovery plans to keep services operational during cyber-attacks or technical failures.

### **Importance in SOC:**

SOC teams monitor systems to detect and mitigate threats like Distributed Denial-of-Service (DDoS) attacks, which can disrupt services. This approach guarantees business continuity by proactively addressing potential issues that could cause outages or delays.

# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

### **Why the CIA Triad is Fundamental to SOC Operations**

The principles of the CIA Triad serve as key pillars guiding the Security Operations Center (SOC) in its mission to protect an organization's digital assets.

- ❖ **Holistic Defense:** By focusing on confidentiality, integrity, and availability, SOC teams provide a comprehensive defense against a broad range of cyber threats, including preventing data breaches, ensuring data integrity, and maintaining system uptime.
- ❖ **Incident Response:** During a security incident, SOC analysts evaluate how the CIA principles are affected. For instance, if malware compromises data confidentiality or integrity, the SOC must respond quickly to contain the damage and restore normal operations.
- ❖ **Risk Management:** The CIA Triad assists SOC teams in prioritizing risks and allocating resources effectively. For example, systems handling sensitive customer data might prioritize stronger confidentiality measures, while critical applications may focus on availability.
- ❖ **Regulatory Compliance:** Many regulations and standards, such as GDPR, HIPAA, and PCI-DSS, are based on the CIA principles. SOC teams play a crucial role in ensuring compliance by safeguarding sensitive data, maintaining data integrity, and ensuring service availability.

### **CIA Triad Overview:**

#### **Confidentiality:**

- ❖ Ensuring that sensitive information is accessible only to authorized users.
- ❖ Methods include encryption, access controls, and data classification.
- ❖ SOC Relevance: Prevents data breaches and unauthorized access.

#### **Integrity:**

- ❖ Protecting data from being altered or tampered with by unauthorized users.
- ❖ Methods include hashing, digital signatures, and version control.

#### **SOC Relevance:**

- ❖ Ensures that critical data remains accurate and trustworthy.



# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

### **Availability:**

- ❖ Ensuring that information and resources are available to authorized users when needed.
- ❖ Methods include redundancy, failover mechanisms, and DDoS protection.

### **SOC Relevance:**

Maintains system uptime and service reliability.

### **Recent Examples of Cyber Attacks:**

#### **Confidentiality Breach:**

- ❖ *Attack:* 2023 MOVEit Transfer breach exploited a zero-day vulnerability, leaking sensitive data from multiple organizations.
- ❖ *Impact:* Compromised PII (Personally Identifiable Information) of millions.

#### **Integrity Violation:**

- ❖ *Attack:* SolarWinds Supply Chain Attack (2020), where attackers injected malicious code into a software update, affecting the integrity of thousands of systems.
- ❖ *Impact:* Manipulated data and software configurations.

#### **Availability Disruption:**

- ❖ *Attack:* 2022 Costa Rica Ransomware Attack, which targeted government institutions, crippling their operations.
- ❖ *Impact:* Caused significant service outages and operational delays.

**In summary**, the CIA Triad serves as a guiding framework for SOC operations, helping to ensure that an organization's systems and data are secure, reliable, and accessible. By focusing on confidentiality, integrity, and availability, SOC teams can effectively defend against cyber threats, maintain trust, and support the organization's overall security strategy.

# **INTRODUCTION TO SOC AND CYBERSECURITY FUNDAMENTALS**

## **Assignment 4: Attack Vector Exploration**

### **What is the MITRE ATT&CK Framework?**

The MITRE ATT&CK Framework (Adversarial Tactics, Techniques, and Common Knowledge) is a globally accessible knowledge base of cyber adversary tactics and techniques. It is used by organizations to understand and classify various cyber threats and improve their security posture. Developed by MITRE Corporation, this framework is widely recognized in the cybersecurity community for providing a structured approach to understanding how attackers operate.

The framework focuses on:

- **Tactics:** The "why" behind an attack (e.g., persistence, privilege escalation, data exfiltration).
- **Techniques:** The "how" of an attack (e.g., phishing, command-line interface, credential dumping).
- **Procedures:** Specific methods adversaries use to implement these techniques.

**MITRE**

**ATT&CK™**

attack.mitre.org

### Using Adversary Behavior to Strengthen Cyber Defense

No matter how strong your patching, compliance and security software, a determined cyber adversary can typically find a way into your network.

But how did the attacker get in? How are they moving around? And how can you use that knowledge to detect, mitigate and prevent future attacks? The MITRE ATT&CK™ framework answers those questions by providing a globally accessible knowledge base of adversary tactics and techniques that are based on real-world observations of adversaries' operations against computer networks. Armed with this knowledge, organizations and security vendors can work toward improving detection and prevention methods.

#### Pioneering with the Cyber Community for Collaborative Defense

ATT&CK was first created by a MITRE internal research program using our own data and operations. Now based on published, open source threat information, MITRE provides the framework as a resource to the cyber community. Anyone is free to leverage it, and everyone is free to use and contribute to ATT&CK.

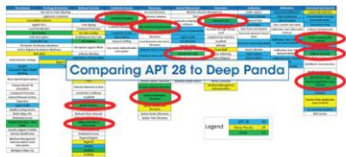
By making the ATT&CK knowledge base globally accessible, MITRE supports a growing community that is fostering innovation in open source tools, products and services based on the framework. ATT&CK is experiencing significant growth across the cybersecurity community, with wide adoption from industry, government and security vendors including organizations like Microsoft, IBM, USAA, JPMorgan Chase, and Palo Alto.

With the creation of ATT&CK, MITRE is partnering with the cyber community to fulfill its mission to solve problems for a safer world.

### Get Started with ATT&CK


#### Use ATT&CK for Cyber Threat Intelligence

Cyber threat intelligence comes from many sources, including knowledge of past incidents, commercial threat feeds, information-sharing groups, government threat-sharing programs, and more. ATT&CK gives analysts a common language to communicate across reports and organizations, providing a way to structure, compare, and analyze threat intelligence.




#### Use ATT&CK to Build Your Defensive Platform

ATT&CK includes resources designed to help cyber defenders develop analytics that detect the techniques used by an adversary. Based on threat intelligence included in ATT&CK or provided by analysts, cyber defenders can create a comprehensive set of analytics to detect threats.



#### Use ATT&CK for Adversary Emulation and Red Teaming

The best defense is a well-tested defense. ATT&CK provides a common adversary behavior framework based on threat intelligence that red teams can use to emulate specific threats. This helps cyber defenders find gaps in visibility, defensive tools and processes—and then fix them.



### Join the ATT&CK Community

MITRE encourages other researchers, analysts and cyber defenders to join our community and contribute new techniques and information.


#### MITRE ATT&CK Resources

**attack.mitre.org**

- Access ATT&CK technical information
- Contribute to ATT&CK
- Follow our blog
- Watch ATT&CK presentations

**@MITREattack**

Follow us on Twitter for the latest news.



# INTRODUCTION TO SOC AND CYBERSECURITY FUNDAMENTALS

## Why is the MITRE ATT&CK Framework Important?

The MITRE ATT&CK Framework is crucial for several reasons:

1. **Standardization:** It provides a common language for cybersecurity professionals to discuss and analyze threats, making collaboration more effective.
2. **Threat Detection and Response:** By understanding the tactics and techniques attackers use, organizations can develop better detection, prevention, and response strategies.
3. **Gap Analysis:** Organizations can use ATT&CK to identify gaps in their existing defenses. This helps in prioritizing security investments and focusing on areas where the organization is most vulnerable.
4. **Red Teaming and Penetration Testing:** Security teams can use the framework to simulate realistic attacks, allowing them to test the effectiveness of their security controls.
5. **Incident Response and Threat Hunting:** Helps security analysts in identifying indicators of compromise (IOCs) and understanding the progression of an attack, which is essential for faster incident response and effective threat hunting.

[illegible]

The MITRE ATT&CK™  
Enterprise Framework

[attack.mitre.org](https://attack.mitre.org)

© 2019 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case Number 15-1294

MITRE

# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

### **How Does the MITRE ATT&CK Framework Work?**

The framework is organized into different matrices, with the most popular one being the Enterprise ATT&CK Matrix, which covers various platforms like Windows, macOS, Linux, cloud environments, and more. Here's how it is structured:

#### **1. Tactics**

##### **What are Tactics?**

Tactics are the adversary's goals during an attack. They represent the why of an attack and are high-level objectives that attackers try to achieve.

##### **Examples of Tactics:**

Initial Access: Entering the target network.

Persistence: Maintaining access to the system after initial entry.

Privilege Escalation: Gaining higher-level permissions on a system.

Data Exfiltration: Stealing sensitive data from the target network.

#### **2. Techniques**

##### **What are Techniques?**

Techniques describe how adversaries achieve their objectives (tactics). They are more specific than tactics and represent the methods used in an attack.

##### **Examples of Techniques:**

Phishing (T1566): Using social engineering to trick users into revealing sensitive information.

Credential Dumping (T1003): Extracting password hashes from a system.

Command and Scripting Interpreter: PowerShell (T1059.001): Using PowerShell scripts to execute malicious commands.

#### **3. Sub-Techniques**

##### **What are Sub-Techniques?**

Sub-techniques are further breakdowns of techniques to provide a more granular understanding of attack methods.

**Example of a Sub-Technique:** Spear Phishing via Service (T1566.003): A targeted phishing attack using communication services like Slack or LinkedIn instead of traditional email.

# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

### **4. Procedures**

#### **What are Procedures?**

Procedures are specific implementations of techniques used by attackers. These are often tied to real-world attack campaigns.

#### **Example of a Procedure:**

APT29 (Cozy Bear) using PowerShell scripts to establish persistence in targeted networks.

#### **Example of How MITRE ATT&CK is Used**

Let's say a security team detects suspicious behavior on a network. They observe an attacker using PowerShell to download and execute a script.

By referencing the MITRE ATT&CK Framework:

#### **Tactic: Execution**

**Technique:** Command and Scripting Interpreter: PowerShell (T1059.001)

**Procedure:** They can correlate this activity with known attack groups that use similar techniques, helping them attribute the attack and respond more effectively.

#### **Summary Table**

<b>Component</b>	<b>Explanation</b>	<b>Examples</b>
Tactics	High-level goals of an attacker	Initial Access, Privilege Escalation, Data Exfiltration
Techniques	Methods to achieve those goals	Phishing, Credential Dumping, PowerShell
Sub-Techniques	More detailed breakdown of techniques	Spear Phishing via Service, LSASS Memory Dumping
Procedures	Specific implementations used by attackers	APT29 using PowerShell for persistence

The **MITRE ATT&CK** framework is a comprehensive, curated knowledge base of tactics and techniques used by adversaries to compromise systems. It provides a structured way to analyze attacks by categorizing them into various tactics (the "why") and techniques (the "how"). Below,

# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

I've documented **5 common attack vectors** using the MITRE ATT&CK framework, along with real-world examples where applicable.

### **Phishing (Technique: T1566)**

**Tactic:** Initial Access

**Description:** Phishing involves sending fraudulent emails or messages designed to trick users into revealing sensitive information or downloading malware. Attackers often use social engineering tactics to appear legitimate.

**Real-World Example:** In 2016, the Democratic National Committee (DNC) was targeted by Russian hackers using spear-phishing emails. This attack led to the breach of sensitive emails, which were later leaked, influencing the U.S. presidential election.

**Mitigation:**

Implement email filtering solutions to detect and block phishing attempts.

Train employees on recognizing phishing emails and suspicious links.

### **2. Credential Dumping (Technique: T1003)**

**Tactic:** Credential Access

**Description:** Attackers extract credentials (usernames and passwords) from compromised systems. Tools like Mimikatz can be used to dump passwords stored in memory, cached credentials, or hashes.

**Real-World Example:** In the 2017 NotPetya ransomware attack, attackers used the EternalBlue exploit to spread laterally and used credential dumping to move between systems within organizations like Maersk and Merck.

**Mitigation:**

Use the latest security patches to protect against known vulnerabilities. Implement multi-factor authentication (MFA) to reduce the impact of credential theft.

### **3. PowerShell (Technique: T1059.001)**

**Tactic:** Execution

**Description:** PowerShell is a legitimate scripting language used for system administration. Attackers misuse PowerShell scripts to execute



# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

malicious commands or payloads without triggering traditional antivirus solutions.

**Real-World Example:** In the Sunburst (SolarWinds) supply chain attack of 2020, attackers used PowerShell scripts to establish persistence and execute remote commands on affected networks.

### **Mitigation:**

Disable or restrict PowerShell usage where possible.

Monitor PowerShell activity logs for suspicious behavior.

### **4. Exploitation of Remote Services (Technique: T1210)**

**Tactic:** Initial Access

**Description:** Attackers exploit vulnerabilities in remote services (e.g., RDP, VPN, web servers) to gain unauthorized access. This technique often leverages unpatched software or weak authentication.

**Real-World Example:** The ProxyLogon vulnerability (CVE-2021-26855) in Microsoft Exchange Servers was widely exploited by attackers to gain access to emails, upload web shells, and escalate privileges.

### **Mitigation:**

Regularly update and patch remote access software.

Use network segmentation and firewalls to restrict access to critical systems.

### **5. Data Encrypted for Impact (Technique: T1486)**

**Tactic:** Impact

**Description:** Attackers encrypt files on the victim's system, rendering data inaccessible. This is a common technique used in ransomware attacks, where the attacker demands a ransom for the decryption key.

**Real-World Example:** The WannaCry ransomware attack in 2017 targeted organizations worldwide, exploiting a Windows vulnerability (EternalBlue). It encrypted data and demanded payment in Bitcoin for decryption, affecting systems in over 150 countries.

### **Mitigation:**

Implement regular data backups and ensure they are isolated from the network.

Use endpoint protection solutions with ransomware detection capabilities.

# **INTRODUCTION TO SOC AND CYBERSECURITY**

## **FUNDAMENTALS**

### **4. Results/Findings**

#### **Analysis:**

- ❖ SOCs are crucial for proactive security monitoring, while NOCs focus on network health.
- ❖ Each SOC tier has specific skill requirements, and there's a clear pathway for skill development from Tier 1 to Tier 3.
- ❖ The CIA Triad serves as the foundation for assessing and mitigating cybersecurity risks.
- ❖ The MITRE ATT&CK framework offers a comprehensive catalog of tactics and techniques used by attackers.

### **5. Conclusion**

#### **Summary of Key Learnings:**

- ❖ Gained a clear understanding of SOC operations and the differentiation from NOC functions.
- ❖ Identified the specific skills required at each SOC tier, aiding in career path planning.
- ❖ Reinforced the significance of the CIA Triad in cybersecurity defense mechanisms.
- ❖ Learned to leverage the MITRE ATT&CK framework for mapping attack vectors.

#### **Future Considerations:**

- ❖ Further research on automated SOC tools (SIEM, SOAR) could enhance incident response.
- ❖ Develop hands-on skills in threat hunting and advanced threat detection.

#### **Action Points:**

- ❖ If in a real-world SOC, prioritize upskilling in Tier 2/3 skills.
- ❖ Implement phishing awareness training to reduce human error vulnerabilities.

# **INTRODUCTION TO SOC AND CYBERSECURITY FUNDAMENTALS**

## **6. Additional Notes**

### **Questions:**

- ❖ How can automation in SOC impact job roles and required skills?
- ❖ What are the emerging trends in SOC operations and technologies?

### **References for Further Reading:**

- ❖ ["The SOC Analyst's Guide to Cybersecurity" \(Book\).](#)
- ❖ [MITRE ATT&CK Framework Official Documentation.](#)