

1. NIST Framework & Its 5 Core Functions:

The NIST Cybersecurity Framework is a guideline created by the U.S. National Institute of Standards and Technology (NIST) to help organizations manage and reduce cybersecurity risks.

It breaks security into 5 key functions that act as the backbone of any security program.

Analogy: "Securing a House"

Stage	House Analogy
Identify	Make a list of all your valuables
Protect	Lock the doors and install cameras
Detect	Use CCTV to catch intruders
Respond	Call the police and handle threat
Recover	Fix damage and improve security

1. **Identify:** Understand what needs to be protected.
 - a. **Goal:** Create visibility of all assets, risks, users, and systems.
 - b. **Includes:** Asset Management, Risk Assessments, Data Classification, Business Context Awareness
 - c. **Example:**
 - i. Inventory all laptops, servers, user accounts.
 - ii. Identify critical systems (e.g., Domain Controller, Finance DB).
2. **Protect:** Apply controls to protect your systems.
 - a. **Goal:** Limit or prevent cybersecurity events.
 - b. **Includes:** Firewalls, EDR, Antivirus, Multi-Factor Authentication (MFA), Data Encryption, Employee Awareness Training.
 - c. **Example:**
 - i. Enable MFA for all admins.
 - ii. Patch all critical systems.
 - iii. Use group policies to block USBs.
3. **Detect:** Identify cybersecurity events as early as possible.
 - a. **Goal:** Know when something suspicious happens.
 - b. **Includes:** SIEM (e.g., Microsoft Sentinel), EDR (e.g., Defender for Endpoint)
 - c. **Example:**
 - i. Sentinel detects "Multiple failed logins" from unknown IP.
 - ii. Defender flags a suspicious script execution.
4. **Respond:** Take action when a threat is detected.
 - a. **Goal:** Contain the threat, stop the spread, and start recovery.
 - b. **Includes:** Incident Response Playbooks, Threat Containment, Stakeholder Communication, Forensics & Investigation.
 - c. **Example:**
 - i. SOC isolates the infected host from the network.
 - ii. Reset user passwords involved in the attack.

- iii. Notify the leadership team about breach impact.
- 5. **Recover:** Restore operations and improve after the incident.
 - a. **Goal:** Minimize downtime and enhance future defenses.
 - b. **Includes:** System Restoration (Backups), Patch Management, Lessons Learned Review, Continuous Improvement
 - c. **Example:**
 - i. Restore server from clean backup.
 - ii. Patch the exploited vulnerability.
 - iii. Update detection rule in Sentinel.

Why is NIST CSF Important?

- Universal cybersecurity standard
- Helps prioritize security efforts
- Makes your SOC process more structured
- Enables better communication with leadership & audit teams
- Easily integrates with tools like Sentinel, Defender, Splunk, etc.

2. Incident Response Life Cycle (IRLC)

Incident Response is the process of identifying, handling, containing, and recovering from cybersecurity incidents like phishing, malware, brute force, ransomware, etc.

The goal is to minimize damage, restore systems, and learn from the attack to prevent it from happening again.

The 6 Phases of the Incident Response Life Cycle:

1. **Preparation:** Getting ready before an attack happens.
 - a. Key Actions:
 - i. Build an Incident Response Team (IRT/SOC)
 - ii. Create playbooks, SOPs, and escalation matrix
 - iii. Train staff on what to do in an incident
 - iv. Set up tools like SIEM, EDR, firewalls, and email security
 - b. Example:
 - i. You have a phishing playbook in place.
 - ii. You regularly conduct mock phishing simulations for employees.
2. **Identification:** Detecting that an incident has occurred (or is ongoing).
 - a. Key Actions:
 - i. Monitor SIEM/EDR for alerts
 - ii. Analyze logs for abnormal behavior
 - iii. Use threat intelligence to validate alerts
 - iv. Confirm whether it's a real incident (True Positive)
 - b. Example:
 - i. Sentinel alerts: 100+ failed login attempts in 5 minutes
 - ii. Defender flags: suspicious PowerShell by Excel

3. **Containment:** Stop the threat from spreading and limit the damage.
 - a. Key Actions:
 - i. Isolate infected machines from the network
 - ii. Revoke compromised credentials
 - iii. Block malicious IPs/domains
 - iv. Disable affected user accounts
 - b. Example:
 - i. You isolate a laptop spreading ransomware
 - ii. Block outbound traffic to attacker's command-and-control server
4. **Eradication:** Remove the threat completely from your systems.
 - a. Key Actions:
 - i. Delete malware, reverse changes
 - ii. Uninstall unauthorized software
 - iii. Patch exploited vulnerabilities
 - iv. Deep scan for persistence (e.g., registry, scheduled tasks)
 - b. Example:
 - i. Use Defender to remove malware
 - ii. Delete registry keys created by attacker
5. **Recovery:** Restore normal operations safely.
 - a. Key Actions:
 - i. Restore from backups
 - ii. Reconnect systems to the network
 - iii. Monitor systems for re-infection
 - iv. Validate that systems are clean
 - b. Example:
 - i. Restore the finance server from a backup
 - ii. Monitor user activity and system logs post-recovery
6. **Lessons Learned:** Review the incident to understand what went wrong and how to improve.
 - a. Key Actions:
 - i. Create an Incident Report
 - ii. Analyze root cause
 - iii. Update detection rules/playbooks
 - iv. Share learnings with the team
 - b. Example:
 - i. Found phishing email bypassed filters → tune email gateway
 - ii. Added new detection rule in Sentinel for the missed behavior

Real-World Scenario:

A phishing email bypassed email security and tricked a user into downloading a fake invoice. Defender detects malware behavior.

SOC Team:

- Identifies the alert
- Contains the infected machine
- Removes the malware
- Recovers from backup
- Updates the email filter
- Documents the entire incident.

3. SOC Fundamentals: IOC, IOA, TP, FP, FN, TN + Logs, Alerts & Incidents

1. IOC – Indicator of Compromise:

- a. An IOC is proof that an attack has already happened. It's a forensic clue that something bad occurred.
- b. Example:
 - i. Malicious file hash (e.g., MD5, SHA256)
 - ii. Known malware domain (e.g., xyzmalware[.]com)
 - iii. Suspicious IP addresses
 - iv. Unusual registry changes
 - v. Unexpected service creation
- c. Real Scenario: Defender finds a process that matches a known ransomware hash → IOC match → Malware confirmed.

2. IOA – Indicator of Attack:

- a. An IOA is behavior that suggests an attack is happening right now. Focuses on the "how" attacker's intent and method.
- b. Example:
 - i. Word launching PowerShell
 - ii. 50+ failed login attempts in a minute
 - iii. User suddenly accessing 10,000 files
 - iv. Abnormal login from a new country
- c. Real Scenario: Sentinel detects user logged in from India, then 3 mins later from Russia → Behavioral anomaly → IOA.

3. True Positive (TP):

- a. An alert is raised and the threat is real
- b. Example:
 - i. Sentinel alert for brute-force → Analyst checks logs → Confirmed multiple failed logins → It's real.

4. False Positive (FP):

- a. Alert is triggered but there's no real threat
- b. Example:
 - i. Geo-login alert fires, but the user was using a VPN — nothing malicious.

5. True Negative (TN):

- a. No alert is raised, and there's no threat.

b. Examples of IOCs:

i. Users logged in normally from the office network — nothing suspicious, and no alert fired.

6. **False Negative (FN):**

a. No alert is raised, but an attack actually happened

b. Example:

i. Attacker used a zero-day exploit → bypassed all detection → no alerts in SIEM.

7. **Logs:**

a. Raw data generated by systems, devices, apps, etc. They capture who did what, when, and how.

b. Example Logs:

i. Windows Event Logs (ID 4625 = failed login)

ii. Firewall logs (blocked IPs)

iii. Proxy logs (web access)

iv. VPN logs (logon attempts)

8. Alerts:

a. Notifications triggered by correlation rules based on log behavior. These indicate potential threats.

b. Examples of Alerts:

i. "Multiple failed logins from same IP"

ii. "Unusual PowerShell command detected"

iii. "Connection to known malicious domain"

9. Incidents:

a. Confirmed security events that need action or investigation. They require containment, documentation, or escalation.

b. Examples of Incidents:

i. Malware infection

ii. Phishing attack

iii. Unauthorized access

iv. Lateral movement within the network

How it works:

[Logs]



[SIEM Correlates Behavior]



[Alert Generated]



[SOC Analyst Investigates]



[Confirmed = Incident]

4. MITRE ATT&CK Framework

- MITRE Adversarial Tactics, Techniques, and Common Knowledge

- It's a globally used framework that documents real-world attacker behavior — from the moment they enter your network to the damage they do.
- The attacker's playbook → so we (defenders) can detect, prevent, and respond better.
- **Why is MITRE Important in SOC?**
 - Helps understand attacker steps clearly
 - Maps alerts to tactics/techniques
 - Helps build use cases, detections, and playbooks
 - Used in SIEMs (Sentinel), EDRs (Defender), Threat Intel tools

MITRE ATT&CK Framework – All 14 Tactics:

1. Initial Access:
 - a. Definition: How an attacker enters the target environment.
 - b. Example: Phishing email with a malicious Word document.
2. Execution:
 - a. Definition: How an attacker runs malicious code inside the system.
 - b. Example: Macro inside Word launches PowerShell to drop malware.
3. Persistence:
 - a. Definition: How an attacker maintains access after reboot/logoff.
 - b. Example: Creates a scheduled task to auto-start malware on login.
4. Privilege Escalation:
 - a. Definition: How an attacker gains higher-level (admin/system) access.
 - b. Example: Exploits unpatched vulnerability to become local admin.
5. Defense Evasion:
 - a. Definition: How an attacker hides from security tools.
 - b. Example: Obfuscates PowerShell script and disables antivirus.
6. Credential Access:
 - a. Definition: How an attacker steals usernames, passwords, or tokens.
 - b. Example: Uses Mimikatz to dump credentials from LSASS memory.
7. Discovery:
 - a. Definition: How an attacker maps and explores the environment.
 - b. Example: Runs net user /domain to list all domain users.
8. Lateral Movement:
 - a. Definition: How an attacker moves across systems in the network.
 - b. Example: Uses stolen admin credentials to RDP into another server.
9. Collection:
 - a. Definition: How an attacker gathers sensitive data before stealing it.
 - b. Example: Zips documents from HR and Finance folders.
10. Exfiltration:
 - a. Definition: How an attacker transfers stolen data out of the environment.
 - b. Example: Uploads ZIP file to attacker's server over HTTPS.
11. Command and Control (C2):
 - a. Definition: How an attacker maintains remote access and issues commands.

- b. Example: Infected host connects to attacker's C2 via DNS tunneling.

12. Impact:

- a. Definition: How an attacker disrupts operations or damages systems.
- b. Example: Deploys ransomware to encrypt critical files.

13. Reconnaissance:

- a. Definition: How an attacker gathers information externally before the attack.
- b. Example: Scans LinkedIn to identify key IT staff in the company.

14. Resource Development:

- a. Definition: How an attacker builds tools and infrastructure before launching an attack.
- b. Example: Registers fake domains and develops phishing kits.