XM Cyber

NIST CSF

Framework Checklist

Organizations are constantly seeking innovative solutions to strengthen defenses and achieve greater resilience against cyber threats. While there are many ways to achieve this, The National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) has emerged as a leading guide for organizations to assess and improve their cybersecurity posture.

Understanding the NIST Cybersecurity Framework

NIST's CSF can be used by any organization looking to evaluate and improve its security posture. It helps understand and assess current security posture, organize and prioritize actions for managing risks, and communicate inside and outside the organization via a common language. Since its inception, the framework has become fundamental to enabling organizations to prepare for, and respond to, cyber threats and incidents.

The NIST CSF provides comprehensive guidelines, best practices, and recommendations to help organizations manage and mitigate cybersecurity risks. It comprises five core functions: Identify, Protect, Detect, Respond, and Recover. Each function encompasses several categories and subcategories, offering a granular approach to cybersecurity management.

1. Identify

□ Compile a comprehensive inventory of all devices, software, and information utilized, such as laptops, smartphones, tablets, and point-of-sale systems.

□ Establish and distribute a corporate cybersecurity guideline covering roles and duties for employees, vendors, and other individuals with access to confidential data.

□ Establish procedures for safeguarding against a breach and mitigating the impact if one occurs.

2. Protect

- □ Regulate access to your network and devices.
- □ Encrypt sensitive information while at rest and in transit.
- □ Utilize security programs to safeguard data.
- □ Regulate access to your network and devices.
- □ Regularly back up data.
- □ Keep security software up to date, and automate updates where feasible.
- □ Establish formal procedures for securely disposing of digital files and outdated devices.
- □ Educate all users on cybersecurity best practices to enhance understanding of personal risks and workplace responsibilities.

3. Detect

- □ Monitor your systems for unauthorized access, devices, and software.
- □ Investigate any unusual network or staff activities.
- □ Check for unauthorized users or connections on your network.

4. Respond

Develop a detailed plan for:

- □ Notifying individuals affected by data breaches.
- □ Ensuring continuous business operations.
- □ Informing law enforcement and relevant authorities about the breach.
- □ Investigating and containing security breaches.
- □ Updating cybersecurity policy and plan based on experiences.
- □ Preparation for unforeseen events that might jeopardize data.
- □ Then regularly test your plan.

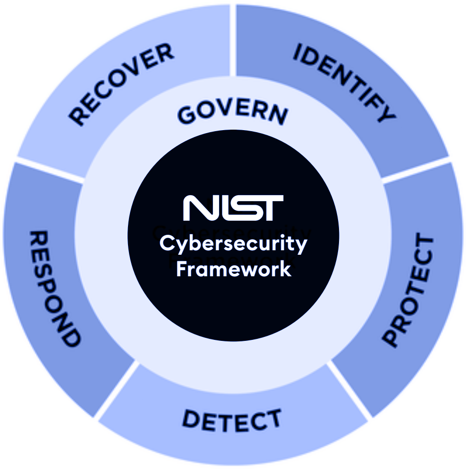
5. Recover

In the aftermath of an attack:

- □ Repair and recover any affected equipment and network components.
- □ Keep stakeholders informed about your response and recovery efforts.

Continuous Threat Exposure Management (CTEM) and CSF – Better Together

Introduced by Gartner in 2022, The Continuous Threat Exposure Management (CTEM) framework enables cybersecurity leaders to significantly enhance their organization's NIST CSF maturity. CTEM is a true paradigm shift in how organizations approach threat exposure management, as traditionally, they have relied on periodic vulnerability assessments and penetration testing to identify and remediate vulnerabilities. However, these methods offer only a snapshot in time and often need to catch up with the dynamic nature of cyber threats.



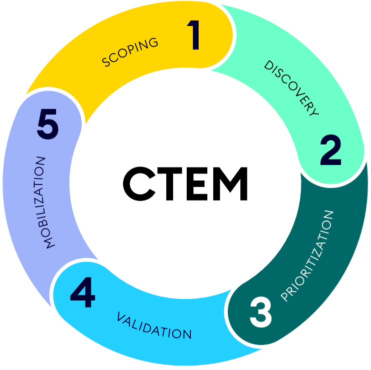
Steps for Creating & Using a CSF Organizational Profile

1. Scope the organizational profile.
2. Gather needed information.
3. Create the organizational profile.
4. Analize gops and create an action plan.
5. Implement action plan and update profile.

...Repeat

CTEM, on the other hand, provides continuous visibility into an organization's attack surface, enabling proactive identification and mitigation of vulnerabilities and exposures before attackers can exploit them. A comprehensive CTEM program combines advanced technologies such as external attack surface management, attack path modeling, and risk prioritization to provide a holistic view of an organization's security posture.

The 5 Stages of Continuous Threat Exposure Management



- **Stage 1 - Scoping**
  Scope scenarios to your threat landscape and critical assets
- **Stage 2 - Discovery**
  Discover CVEs, misconfigs, cloud, and identity risks across hybrid environments
- **Stage 3 - Prioritization**
  Prioritize threats "in the wild" and map attack paths to critical assets
- **Stage 4 - Validation**
  Validate exploitability and reachability to critical assets, to identify dead ends and choke points
- **Stage 5 - Mobilization**
  Mobilize teams around security risks with IT remediation guidance, ticketing, and progress tracking

CTEM Aligns Seamlessly With NIST CSF, to Benefit All 5 Core Functions:

01

Identify

CTEM enables organizations to comprehensively identify and inventory their assets, systems, and data. It also helps organizations discover unknown or forgotten assets that pose security risks by continuously monitoring the surface of external attacks. This enhanced visibility is crucial for establishing a strong foundation for cybersecurity management, as outlined in the Identify function of the NIST CSF.

02

Protect

CTEM strengthens the Protect function by proactively identifying vulnerabilities and misconfigurations before they can be exploited. By prioritizing risks based on their potential impact and likelihood of exploitation, CTEM enables organizations to focus on addressing the most critical vulnerabilities first. Additionally, CTEM's attack path modeling capabilities help organizations identify and mitigate potential attack paths, reducing the risk of compromise.

03

Detect

CTEM's continuous monitoring of the external attack surface enhances the Detect function by providing early warning of potential threats. By identifying changes in the attack surface, such as new vulnerabilities or exposed services, CTEM enables organizations to quickly detect and respond to possible attacks before they can cause significant damage.

04

Respond

In the event of a security incident, CTEM's risk prioritization capabilities help organizations prioritize their response efforts, ensuring that the most critical incidents are addressed first. Additionally, CTEM's attack path modeling can help organizations understand how attackers may have gained access to their systems, enabling them to take targeted actions to contain and eradicate the threat.

05

Recover

CTEM's continuous monitoring and risk prioritization capabilities also play a crucial role in the Recover function. By quickly identifying and addressing vulnerabilities, CTEM helps organizations minimize the impact of security incidents and accelerate recovery. Additionally, attack path modeling can help organizations identify and address weaknesses in their recovery processes, further enhancing their resilience against future attacks.

XM Cyber

XM Cyber is a leading Continuous Exposure Management company that transforms the way organizations approach cyber risk, enabling security teams to prevent more attacks with 75% less remediation effort. Its XM Attack Graph Analysis™ capability discovers CVEs, misconfigurations, and identity issues across on-premise and all major cloud environments. It analyzes how attackers can chain exposures together to reach critical assets, identifies key "choke points", and provides remediation guidance. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, Asia, and Israel.