ISSN: 2634 - 8853

Journal of Engineering and Applied Sciences Technology

SCIENTIFIC Research and Community

Review Article

Open Access

Comparative Study of CTEM Frameworks: NIST, MITRE, and Beyond

Santosh Kumar Kande

Senior Vulnerability Analyst, USA

ABSTRACT

The rapid increase in cyber threats and the evolving landscape of cybersecurity demand robust frameworks to manage and mitigate cyber risks effectively. Cyber Threat Exposure Management (CTEM) has emerged as a critical approach for organizations to continuously identify, assess, and remediate threats. This paper conducts a comparative study of prominent CTEM frameworks, including the NIST Cybersecurity Framework (CSF) and MITRE ATT&CK, while also exploring emerging frameworks that extend beyond these standards. The study aims to highlight their effectiveness, adaptability, and challenges in modern cybersecurity environments. Recommendations for harmonizing these frameworks to develop a comprehensive CTEM strategy are provided.

***Corresponding author**

Santosh Kumar Kande, Senior Vulnerability Analyst, USA.

Received: December 19, 2024; **Accepted:** December 23, 2024; **Published:** January, 02, 2025

Keywords: Cyber Threat Exposure Management (CTEM), NIST CSF, MITRE ATT&CK, Cybersecurity Frameworks, Risk Mitigation, Threat Intelligence

Introduction

The frameworks for cybersecurity give businesses organized ways to identify, assess, and minimize potential risks online. The sophisticated nature of cyberattacks has rendered traditional security management techniques inadequate. A proactive approach that enables constant monitoring and evaluation of potential threats is Cyber Threat Exposure Management (CTEM).

The National Institute of Standards and Technology (NIST) Cybersecurity Framework and MITRE ATT&CK have gained prominence for their structured approaches to cybersecurity. However, newer frameworks and hybrid methodologies are emerging to address limitations in adaptability and real-time threat intelligence.

This paper compares NIST CSF, MITRE ATT&CK, and emerging CTEM frameworks, analyzing their strengths, weaknesses, and practical applicability in contemporary cybersecurity practices.

Overview of Prominent CTEM Frameworks

NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework, introduced in 2014, provides a flexible approach to managing and reducing cybersecurity risks. The framework consists of five core functions:

- **Identify:** Understand systems, assets, and risks.
- **Protect:** Implement safeguards to mitigate risks.
- **Detect:** Develop capabilities to identify incidents.
- **Respond:** Contain and mitigate incidents.
- **Recover:** Restore capabilities and services.

Strengths: Universally accepted, comprehensive, and customizable.
Limitations: Static in nature; lacks real-time threat detection and continuous adaptation.

MITRE ATT&CK Framework

MITRE ATT&CK is a globally recognized knowledge base of adversary tactics and techniques based on real-world observations. It is widely used for threat modeling and incident detection.

Key components include:

- **Tactics:** The goals adversaries aim to achieve (e.g., persistence, privilege escalation).
- **Techniques:** Methods used to achieve those goals.
- **Procedures:** Specific implementation details for techniques.

Strengths: Granular threat modeling, detailed mapping of techniques.
Limitations: Requires significant expertise to implement effectively; focuses heavily on detection and less on proactive exposure management.

Emerging Frameworks: Beyond NIST and MITRE

Newer CTEM frameworks have emerged to address gaps in existing models. Examples include:

- **CISA Cybersecurity Performance Goals (CPGs) (2022):** Developed by the Cybersecurity and Infrastructure Security Agency to align with NIST CSF but with a performance-driven approach.
- **Gartner CTEM Framework (2022):** Focuses on continuous visibility and adaptive prioritization of cyber risks.

These frameworks emphasize real-time threat intelligence integration, automation, and continuous improvement.

Comparative Analysis

The comparative analysis evaluates these frameworks based on the following criteria:

- Scope and Coverage
- Integration of Threat Intelligence
- Adaptability to Emerging Threats
- Implementation Complexity
- Real-Time Monitoring and Automation

Criteria	NIST CSF	MITRE ATT&CK	Emerging Frameworks
Scope and Coverage	Broad, risk-based	Threat-focused, granular	Hybrid, holistic
Integration of Threat Intel	Limited	Extensive	Real-Time Integration
Adaptability	Static	Flexible but Reactive	Adaptive and proactive
Implementation Complexity	Low-Medium	High	Medium-High
Real-Time Monitoring	Minimal	Partial	Fully Integrated

Challenges and Gaps in Current Frameworks

While NIST and MITRE frameworks provide valuable guidance, they present challenges in modern cybersecurity environments:

- **Static Nature of NIST CSF:** Limited adaptability to rapidly evolving threats.
- **Complexity of MITRE ATT&CK:** Requires expertise and resources for effective implementation.
- **Lack of Automation:** Manual processes hinder real-time threat detection and response.

Emerging frameworks aim to bridge these gaps but remain nascent and require further industry adoption.

Harmonizing Frameworks for a Unified CTEM Approach

To achieve a robust CTEM strategy, organizations can harmonize these frameworks:

- **Adopt a Hybrid Approach:** Combine the flexibility of NIST CSF with the granular threat intelligence of MITRE ATT&CK.
- **Integrate Real-Time Threat Intelligence:** Leverage tools and platforms for automated threat exposure detection and prioritization.
- **Focus on Continuous Improvement:** Implement iterative assessments to adapt to emerging threats.

Conclusion

This paper highlights the strengths and weaknesses of NIST CSF, MITRE ATT&CK, and emerging frameworks in the context of Cyber Threat Exposure Management. While NIST and MITRE serve as foundational models, newer frameworks offer adaptive and automated solutions necessary for modern cybersecurity challenges. Organizations must adopt a hybrid approach that leverages the strengths of each framework while integrating real-time threat intelligence for effective CTEM [1-6].

References

1. NIST (2014) Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
2. (2020) MITRE ATT&CK Framework. MITRE https://attack.mitre.org/.
3. CISA (2022) Cybersecurity Performance Goals. Cybersecurity and Infrastructure Security Agency https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf.
4. (2022) Continuous Threat Exposure Management Framework. Gartner https://www.gartner.com/en/articles/how-to-manage-cybersecurity-threats-not-episodes.
5. Lewis JA, Ray D (2021) Adapting Cybersecurity Frameworks for Modern Threats. Journal of Cybersecurity Studies 8: 45-60.
6. Gartner (2022) Gartner Research: Cybersecurity Trends in 2022. Gartner Insights 18.