STREAMING DEFENSE

a new dimension in cybersecurity

Streaming Defense- aligning to the NIST Cybersecurity Framework

WHITEPAPER

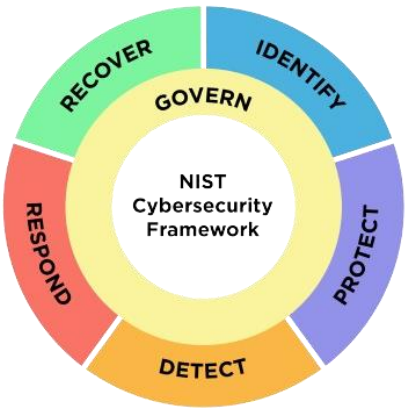
Contents

01

Introduction

The NIST Cybersecurity Framework, developed by the National Institute of Standards and Technology (NIST), serves as a comprehensive guide for organizations to bolster their cybersecurity defenses. Structured around five key functions—Identify, Protect, Detect, Respond, and Recover—the framework outlines essential steps for managing cybersecurity risk effectively.

NIST has recently introduced a sixth function, termed "govern," which addresses how organizations can internally formulate and implement decisions to uphold their cybersecurity strategy. This function highlights cybersecurity as a significant enterprise risk, standing on par with legal, financial, and other considerations, thereby underlining its importance for senior leadership.



Within each function, the framework provides categories and subcategories, offering detailed guidance on cybersecurity activities. This granularity allows organizations to assess their current cybersecurity practices, identify gaps, and develop targeted strategies for improvement.

A core strength of the NIST Cybersecurity Framework lies in its emphasis on collaboration and information sharing. By fostering a culture of cooperation, it enables organizations to leverage collective expertise and insights to strengthen their cybersecurity defenses.

Moreover, the framework's adaptability makes it suitable for organizations of all sizes, industries, and cybersecurity maturity levels. Its customizable nature allows entities to tailor their cybersecurity strategies to their specific needs and risk profiles.

The widespread adoption of the NIST Cybersecurity Framework underscores its relevance and efficacy in today's cyber landscape. Organizations globally recognize its value in guiding strategic cybersecurity investments, enhancing resilience, and mitigating risks effectively. By providing a structured and adaptable framework for managing cybersecurity risk, NIST empowers organizations to navigate the complex cybersecurity landscape with confidence and resilience.

02

How Streaming Defense Aligns to the NIST Cybersecurity Framework

Streaming Defense aligns closely with the NIST Cybersecurity Framework, excelling in the Detect and Respond functions with advanced technologies like wire-speed processing, AI, and ML for real-time threat detection and immediate response. It analyzes data at high speeds to identify and mitigate threats, minimizing damage and maintaining security.

Additionally, Streaming Defense supports the Identify and Protect functions by continuously monitoring for vulnerabilities and proactively mitigating threats.

This comprehensive approach enhances the overall cybersecurity posture, ensuring all critical aspects of cybersecurity are addressed and aligning with the NIST framework's strategy for managing and reducing cybersecurity risk.

DETECT

The DETECT module in the NIST Cybersecurity Framework focuses on identifying cybersecurity events quickly. It involves continuous monitoring of networks and systems, anomaly detection to spot unusual activities, and the use of Security Information and Event Management (SIEM) tools to analyze security data.

It also includes integrating threat intelligence and maintaining incident response plans to ensure swift and effective responses to any detected threats or incidents.

Detecting Anomalies and Events:

Real-Time Threat Detection:	Streaming Defense excels in real-time threat detection, identifying and flagging unusual activities and potential threats as they occur.
Behavioural Analytics:	The platform continuously monitors network traffic and user behaviour to detect anomalies that may indicate security incidents.

Security Continuous Monitoring:

Continuous Monitoring:	Streaming Defense provides continuous monitoring of network activities, ensuring that threats are detected promptly.
Full Visibility:	The solution offers a comprehensive and real time visibility into network traffic and potential threats, enhancing situational awareness.

Summary

Streaming Defense excels in detection with real-time threat intelligence and instant cyberattack neutralization. By integrating real-time threat intelligence feeds, it identifies emerging threats swiftly, keeping organizations ahead of evolving cyber risks. Its ability to neutralize cyberattacks at wire speed is invaluable, preventing data breaches and system compromises, safeguarding critical assets, and operations in real-time.

RESPOND

The Respond function in the NIST Cybersecurity Framework involves planning and implementing activities to address detected cybersecurity incidents effectively. Streaming Defense aligns closely with this function by utilizing advanced technologies such as AI and machine learning to provide real-time threat detection and immediate response capabilities.

It ensures that organizations can communicate effectively during incidents, analyze incident data to understand impacts and causes, and mitigate the effects promptly.

Additionally, Streaming Defense helps improve future incident responses by offering insights and analytics that inform continuous improvement efforts, thereby enhancing the overall security posture and resilience of the organization.

Response Planning:

Proactive Threat Mitigation	Streaming Defense is designed to not only detect but also respond to threats in real-time, allowing for immediate threat neutralization before they escalate into breaches.
Mitigation:	The platform continuously monitors network traffic and user behaviour to detect anomalies that may indicate security incidents.

Response Planning:

Proactive Threat Mitigation	Streaming Defense is designed to not only detect but also respond to threats in real-time, allowing for immediate threat neutralization before they escalate into breaches.

Mitigation:

Immediate Termination of Threats:	Streaming Defense provides continuous monitoring of network activities, ensuring that threats are detected promptly.
Adaptive Response:	Leveraging AI and ML, Streaming Defense adapts its response strategies based on evolving threats, ensuring effective mitigation.

Analysis:

Incident Analysis:	Post-detection, the platform aids in the detailed analysis of security incidents, helping organizations understand the nature and impact of the threats.

Summary

Streaming Defense is also robust in its response capabilities. It promptly reacts to detected cyber threats, initiating immediate actions to mitigate potential damage.

By leveraging real-time analytics and automated response mechanisms, it ensures rapid and effective responses to cyber incidents.

This capability is invaluable in minimizing the impact of cybersecurity events, restoring normal operations swiftly, and preventing further harm.

Additionally, Streaming Defense facilitates post-incident analysis, offering insights to improve response strategies and enhance overall cybersecurity resilience.

IDENTIFY

The NIST Cybersecurity Framework's Identify function aims to understand an organization's environment to manage cybersecurity risks effectively. It includes inventory management, understanding the organization's mission and stakeholders, establishing governance policies, conducting risk assessments, developing risk management strategies, and managing third-party risks. This function helps organizations prioritize resources and cybersecurity activities, forming the foundation for effective risk management and protection efforts.

Asset Management:

Comprehensive Monitoring:	Streaming Defense's continuous monitoring capabilities ensure that all network assets are accounted for and protected, contributing to effective asset management.

Risk Assessment:

Risk Identification:	By identifying and flagging potential threats in real-time, Streaming Defense helps organizations assess risks promptly and accurately.

Summary

Streaming Defense provides comprehensive insights into organizational cybersecurity through advanced analytics and continuous monitoring. It identifies vulnerabilities and risks across networks and systems, strengthening security postures, prioritizing resources, and pre-emptively mitigating risks. Additionally, Streaming Defense supports the establishment of governance frameworks and risk management strategies, ensuring alignment with organizational goals and regulations. By understanding an organization's risk posture, including software zero-day exploits, IT and non-IT systems, OT, exposed services, and supplier chain risks, it enables organizations to prioritize their efforts in line with their risk management objectives.

PROTECT

The Protect function in the NIST Cybersecurity Framework focuses on implementing measures to safeguard critical infrastructure services and minimize the impact of cybersecurity events. This involves activities such as access control, employee training, data security, maintenance processes, protective technology deployment, and regular updates to mitigate vulnerabilities and enhance overall cybersecurity.

Information Protection Processes and Procedures:

Proactive Measures:	The platform's ability to detect and neutralize threats in real-time supports the implementation of robust information protection processes and procedures.
Protective Technology:	Advanced Technologies: Streaming Defense leverages cutting-edge technologies, including AI and ML, to protect against sophisticated cyber threats.

Summary

In the protection realm, Streaming Defense excels by implementing robust measures to safeguard organizational assets and operations. Through advanced technologies like encryption and access controls, it fortifies defenses against potential cyber threats. Proactive vulnerability monitoring and patching mitigate risks effectively, while comprehensive training programs bolster overall security posture.

This multifaceted approach helps organizations maintain resilience and safeguard critical assets against evolving cyber threats.

More about Streaming Defense

Streaming Defense revolutionizes threat response by combining wire speed, in-memory, and AI processing to instantly provide security operators with threat intelligence.

This empowers them to respond faster and more effectively than ever before. Unlike alternatives that write data to disk, our solution offers analysts the unique capability to immediately terminate threats.

This new dimension in cybersecurity ensures superior security outcomes, enhances analyst experience, reduces bottlenecks, and significantly minimizes dwell time and risk.

Key Features and Benefits

Real-Time Threat Detection: Streaming Defense provides real-time monitoring and analysis of network traffic, enabling the immediate identification of attacks and threats.

Full Visibility of Threats: Streaming Defense provides comprehensive visibility into network activities, enabling organizations to detect and respond to threats swiftly and accurately.

Proactive Threat Mitigation: Streaming Defense enables organizations to take proactive measures at wire-speed to mitigate risks, such as blocking suspicious transactions, terminating unauthorized sessions, and alerting security teams to potential threats.

Continuous Adaptation: Leveraging machine learning and AI-driven analytics, Streaming Defense continuously learns from security events and adapts its detection techniques to detect emerging fraud trends and evolving attack techniques.

Exfiltration Detection: Streaming Defense includes advanced capabilities for detecting data exfiltration attempts, enabling organizations to identify and prevent unauthorized data transfers, mitigating the risk of data breaches and intellectual property theft.

Integration Capabilities: Streaming Defense seamlessly integrates with existing fraud prevention systems and security tools, enabling organizations to orchestrate coordinated response efforts and enhance overall fraud defense capabilities.

Scalability and Flexibility: Designed to scale with the growing needs of organizations, Streaming Defense offers flexibility in deployment options and licensing models, ensuring seamless integration into existing security infrastructures and workflows.

In Summary

Streaming Defense predominantly operates within the Detect and Respond functions of the NIST Cybersecurity Framework, but it also makes substantial contributions to the Identify and Protect functions. Its real-time threat detection, continuous monitoring, proactive mitigation, and advanced analytics capabilities significantly enhance an organization's ability to detect and respond to cyber threats swiftly and effectively.

By leveraging these capabilities, organizations can bolster their overall cybersecurity posture, ensuring resilience against evolving cyber threats and maintaining the integrity of their systems and data.

See the Attack – Contain the Attack – Kill the Attack