How xenexSOS supports adaptive cybersecurity and delivers key elements of the NIST framework

The U.S. government recognizes that the national and economic security of the country depends on the reliable function of critical infrastructure.

Consequently, the federal government has identified 16 critical infrastructure sectors whose assets, systems and networks – both physical and virtual – are vital to the country.

The incapacitation or destruction of the systems and networks of these assets would have a debilitating effect on national security, the economy, and public health or safety.

According to the U.S. Department of Homeland Security, these 16 sectors include:

- Chemical and energy industries
- Commercial and government facilities
- Critical manufacturing
- Dams, water and wastewater systems

- Information technology and communications
- Nuclear reactors and waste
- Transportation

All of these sectors depend on information technology and industrial control systems to support business decisions and deliver critical services, which makes them vulnerable to cyberattacks.

To address these risks, an Executive Order in 2013 initiated the development of a voluntary risk-based cybersecurity framework. Drafted by the National Institute of Standards and Technology (NIST), the Framework for Improving Critical Infrastructure Cybersecurity provides organizations with a consistent, iterative, technology-neutral approach to identifying, assessing and managing cybersecurity risk.

The following sections highlight key components of the NIST cybersecurity framework and provide detail on how the xenexSOS® network-detection and response platform from XeneX® provides operators of critical infrastructure with continuous, automated threat surveillance and detection across the entire enterprise.

By automating threat detection and incident response, xenexSOS condenses weeks or months of work into minutes, enabling security teams to take action to prevent theft or damage.

Detect The detect function involves developing and implementing activities that enable the timely discovery of cybersecurity events. Key categories of the detect function include continuous monitoring, identification of anomalies and events, and detection processes.

Respond This function entails developing and implementing the appropriate activities to take action in response to a detected cybersecurity event. It supports the ability to contain the impact of a potential cybersecurity event, and encompasses categories such as

NIST framework implementation tiers Tiers describe the degree to which an organization’s cybersecurity risk management practices exhibit the characteristics defined in the framework – that is, risk and threat aware, repeatable, and adaptive.

The tiers provide a way for organizations to view and understand the characteristics of their approach to managing cybersecurity risk. Four tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed.

The NIST tiers are structured as follows:

- Tier 1 – Partial Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. An organization has no processes in place to coordinate or collaborate with external entities, such as partners.
- Tier 2 – Risk informed Risk management practices are approved by management but may not be established as organization-wide policy. Cybersecurity activities are prioritized based on an organization’s risk objectives, the threat environment, or business/mission requirements. There are no formalized capabilities to share cybersecurity information externally.

Framework overview The NIST cybersecurity framework is technology-neutral to ensure extensibility and enable technical innovation. It relies on standards, guidelines and practices that are developed, managed and updated by industry, with the goal of making cybersecurity tools and methods available that scale across borders and evolve with technological advances and business requirements.

The framework is designed to enable organizations to:

- Describe their current cybersecurity posture and target state
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process

- The framework core
- The framework profile
- The framework implementation tiers

The framework core The NIST core is a set of activities to achieve specific cybersecurity outcomes, and includes reference examples for achieving those outcomes that are common across critical infrastructure sectors.

The four elements of the core that work together are functions, categories, subcategories, and informative references. The framework core also defines five functions, subdivided into categories and subcategories of outcomes:

Identify The activities in the identify function are foundational for effective use of the framework, and help organizations develop an understanding of their business environment, the resources necessary to support critical functions, and how to manage cybersecurity risk to systems, assets, data, and capabilities.

Key categories encompassed by the identify function include asset management, governance, risk assessment, and risk management strategy.

Protect This function focuses on the development and implementation of appropriate safeguards. Key categories encompassed by the protect function include access control, data security, information protection processes and procedures, and protective technology.

- Tier 3 – Repeatable There is an organization-wide approach to manage cybersecurity risk, and risk management practices are formally approved and expressed as policy. Dependencies are understood and information is received from partners that enables collaboration and risk-based management decisions in response to events.
- Tier 4 – Adaptive Cybersecurity risk management is part of the organizational culture

Organizations manage risk and actively share information with partners to improve cybersecurity before an event occurs.

Framework profile A profile can be characterized as the alignment of standards, guidelines and practices to the framework core in a particular implementation scenario. To develop a profile, review all of the core categories and subcategories and, based on business drivers and a risk assessment, determine which are most important.

Organizations can use profiles to identify opportunities for improving cybersecurity posture by comparing a current profile with a target profile. In addition, profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

Successful implementation of the cybersecurity framework is based on achieving the outcomes described in an organization's target profile.

xenexSOS supports automated detection and adaptive cybersecurity The xenexSOS network-detection and response platform from XeneX augments cybersecurity teams and enables organizations to achieve a Tier 4 adaptive security implementation.

xenexSOS correlates security-enriched metadata with other data sources, automatically surfaces hidden attacks in real time, and enables security analysts to perform conclusive threat hunting and incident investigations.

By providing continuous, non-stop network traffic monitoring, threat detection, triage, and incident reporting, xenexSOS automatically hunts down threats across the enterprise network, from cloud and data center workloads to user and IoT devices.

xenexSOS employs machine learning and attacker behavior analytics to automatically hunt down threats across the entire enterprise, from cloud and data center workloads to user and IoT devices.

- Continuous monitoring and analysis of all network traffic, including internal network traffic, Internet- bound traffic and internal traffic between physical and virtual hosts with an IP address – for example, laptops, servers, printers, BYOD/personal smart-devices, and IoT devices – regardless of the operating system or application.
- Real-time visibility into network traffic by extracting metadata from packets rather than performing deep packet inspection, enabling protection without prying.
- Analysis of metadata from captured packets with behavioral detection algorithms that spot hidden and unknown attackers, whether traffic is encrypted or not.
- Store and interact with security-enriched metadata to hunt for threats retrospectively and accelerate incident investigations.
- Deterministic identification of attack behaviors, including the use of remote access Trojans, encrypted tunnels, botnet behaviors, and reconnaissance tools. xenexSOS persistently tracks threats over time and across all phases of an attack, ranging from command and control (C&C), internal reconnaissance, lateral movement, and data exfiltration behaviors.
- Automatic correlation of threats with host devices under attack and threat detection details that include host context, packet captures, the seriousness of the threat, and certainty scores.
- Support for adaptive cybersecurity through an ongoing process of improvement that leverages the work of the XeneX Threat Labs™, a group of highly-skilled security researchers, as well as behavioral detection algorithms that constantly learn from the local environment and from global trends.

Framework core – Detect Automated threat detection is central to the xenexSOS platform. xenexSOS provides continuous monitoring and automated threat surveillance across the entire enterprise, providing a robust foundation for adaptive threat management.

xenexSOS gives IT security teams real-time visibility into all network traffic, analyzes that

Anomalies and events – DE.AE Anomalous activity is detected in a timely manner and the potential impact of events is understood.

Subcategory xenexSOS capability

- DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

Through a combination of supervised and unsupervised machine learning applied to the local network, xenexSOS develops the baseline of appropriate and approved behavior.

- DE.AE-2: Detected events are analyzed to understand attack targets and methods.

Metadata is analyzed with behavioral detection algorithms to identify hidden and unknown attackers. For example, supervised machine learning lets xenexSOS find the hidden traits that all threats have in common, while unsupervised machine learning reveals attack patterns.

- DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.

xenexSOS condenses thousands of events and network traits to a single detection using machine learning techniques that automate threat detection based on the characteristics of network traffic.

- DE.AE-4: Impact of events is determined. Automated scoring of hosts reveals the overall risk to the network based on threat and certainty.

Subcategory xenexSOS capability

- DE.DP-4: Event detection information is communicated to appropriate parties. xenexSOS automated detection, triage and threat prioritization triggers real-time notifications to security teams. Notifications are delivered as one-page explanations attackers. Behavioral detection algorithms constantly learn from the local environment and from global trends. This continuous feedback loop drives dramatic improvements and allows for the tuning of existing algorithms in the customer's local environment.

Subcategory xenexSOS capability

- DE.CM-1: The network is monitored to detect potential cybersecurity events. Deployed inside the network, xenexSOS provides nonstop monitoring of all network traffic, including internal (east-west) and Internet-bound (north-south) traffic, to identify malicious attack behaviors that put in-scope assets at risk.
- DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events. xenexSOS tracks the internal Kerberos infrastructure to understand normal usage behaviors and detect when trusted user credentials are compromised by an attacker, including the misuse of administrative credentials and abuse of administrative protocols (e.g., IPMI).
- DE.CM-4: Malicious code is detected. xenexSOS provides multiple early-warning opportunities to detect ransomware, other malware variants, and malicious activity that precedes an attack on any network device, including devices that do not run antivirus software.
- DE.CM-5: Unauthorized mobile code is detected. xenexSOS continuously monitors and analyzes all network traffic, including internal traffic between physical and virtual hosts with an IP address, such as laptops, smartphones, BYOD and IoT devices, regardless of the operating system or application.
- DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.

xenexSOS continuously monitors and analyzes internal network traffic, Internet-bound traffic and data center traffic, including traffic between virtual workloads in the data center

Continuous security monitoring – DE.CM The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

Detection Processes – DE.DP Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Framework Core – Respond The timely communication of actionable detection information is critical to cybersecurity incident response. By automating the hunt for active threats, xenexSOS enables security teams to focus on high priority risks and respond rapidly to cybersecurity incidents.

xenexSOS provides a variety of communication and automated response mechanisms that improve situational awareness, expedite information sharing, and support response activities. These include:

- Displaying detection information via a simple dashboard that prioritizes compromised hosts that pose the highest risk, changes in a host's threat and certainty scores, and any key assets that show signs of attack. • Enabling security teams to easily share the same information on demand or on a set schedule using the highly customizable XeneX reporting engine. • Driving dynamic response rules or automatically triggering a response from existing security enforcement solutions.

Examples of supported security enforcement solutions:

- xenexSOS integrates with the Cisco Systems Identity Services Engine (ISE) to immediately isolate or quarantine a host.
- xenexSOS works with Carbon Black to rapidly isolate or quarantine a host device when a threat is detected and kill a malicious process.
- xenexSOS integrates with next-generation firewalls from Palo Alto Network, Cisco and Juniper Networks to block a compromised host device.

Subcategory xenexSOS capability

- RS.CO-2: Events are reported consistent with established criteria. xenexSOS provides consistent reporting of threat data to customers. Security teams receive one-page explanations of each attack detection, including possible triggers, root causes, business impacts, and steps to verify.
- RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.

Make the most of your security team Achieving an adaptive cybersecurity implementation entails a process of ongoing improvement and the ability to respond to sophisticated, evolving threats in a timely manner.

For organizations working toward achieving a NIST Tier 4 adaptive cybersecurity implementation, xenexSOS delivers an ongoing process of improvement that actively adapts to the changing cybersecurity landscape.

Achieving a NIST Tier 4 implementation is difficult, if not impossible, without automation. By providing continuous monitoring and automating threat detection and analysis, the xenexSOS platform is able to perform weeks or months of work in just minutes.

Instead of requiring additional headcount, xenexSOS augments an organization’s existing security team with the critical information it needs to make smarter, better-informed decisions. And by eliminating manual threat hunting and low-level threat analysis tasks, security teams can focus on rapid response and quick mitigation of cybersecurity incidents.

xenexSOS also enables organizations to get more value from their existing security investments by integrating with firewalls, endpoint detection, NAC, and other security enforcement points to block unknown and customized cyber-attacks.

12121 Wilshire Blvd., Suite 1111
Los Angeles, CA 90025
877-550-2568

Policy
Terms of
Service