XM Cyber

Integration Solution Brief

XM Cyber
Security Controls Monitoring

For Cisco Firepower Threat Defense (FTD)

Executive Summary

To enable the modern business to be successful, IT services must enable the business to work at the speed they need, while optimizing service delivery and ensuring business continuity and customer satisfaction. To do this organizations must implement and maintain a complicated, and constantly developing connected IT infrastructure. As these services evolve and transform, they also suffer from the growing security risk.

To address this and better defend the business from threat actors and adversaries, while ensuring the smooth running of business-critical systems and services, many CISOs are seeking to understand and then improve the security posture of their attack surface.

Enabling this requires a centralized viewpoint of all their security systems, control policies, and processes, that provide awareness of the current state, and the guidance needed to implement more effective security, without causing unnecessary friction to the business. To do this, they need a Security Controls Monitoring platform that integrates seamlessly with their existing cybersecurity ecosystem, and provides unique insights to optimize their primary security solutions.

CISCO

+

Robust security monitoring to protect the network from cyber threats.

The Need For Comprehensive Security Controls Monitoring

When cybersecurity responsibilities are dispersed throughout the organization, it is nearly impossible to comprehend how secure your organization is. Aligning effective security controls to security benchmarks, recommendations, regulations, and best practices can be very complex. Maintaining business continuity while under constant and increasing risk in an ever-evolving threat landscape, further compounds the strain on IT Security resources and personnel.

Effective cybersecurity requires synergy between people, processes, and technology. As such the purpose of continuous security controls monitoring is to ensure that each component is operating effectively and aligned to the same outcomes. Achieving this requires the design, implementation and testing of Critical Security Controls (CSCs), across your security stack.

Together XM Cyber SCM and Cisco Firepower Threat Defense (FTD), extend the protection of your network infrastructure allowing you to rapidly detect and response to configuration issues that could threaten the security of your network infrastructure.

Introducing: CISCO

Cisco Firepower Threat Defense (FTD) is a next-generation firewall and intrusion prevention system designed to protect networks from cyber threats. It combines advanced threat intelligence, traffic inspection, and policy enforcement to defend against malware, exploits, and unauthorized access.

With features like intrusion prevention, application visibility, and access control, it provides robust security monitoring and enforcement across hybrid environments.

Introducing: XM Cyber

XM Cyber Security Controls Monitoring (XM SCM) solution is a cybersecurity awareness and compliance management platform that acts as a single source of truth for the security posture of your entire hybrid infrastructure. It provides visibility, validation and monitoring of all security tools, critical security controls (CSCs), and their alignment to common security frameworks and regulatory compliance standards.

Solution Benefits by Use Case:

Security Posture Management

Establish a security posture baseline for Cloud to Core infrastructure and security tools

Infrastructure Hardening

Firewall rules allowing unrestricted access to any destination, source, or port are identified. Policies permitting insecure protocols such as Telnet, FTP, SNMP, and NetBIOS traffic are monitored. Devices with critical status alerts and outdated applied policies are assessed for potential security risks.

Security Configuration Optimization

Disabled access rules and missing logging configurations are reviewed for visibility gaps. Intrusion, malware, and DNS policies are analyzed for changes that may impact threat detection. Identity policies and security policies are tracked to ensure proper enforcement of network access controls.

Safeguard Security Defences

Monitor divergence from security baseline to detect unwanted configuration changes

Configuration Drift Management

Modifications to security rules, including newly added, removed, or changed access control policies, are monitored. Updates to prefilter policies, intrusion detection policies, and malware protection settings are reviewed. Changes in user accounts and device inventory are tracked to identify shifts in administrative access and infrastructure components.

Anomaly Detection

Unusual firewall rule modifications, such as test policies and temporary rules, are assessed for unexpected access permissions. Atypical task failures and system health alerts are monitored to detect operational anomalies. Unplanned additions or removals of security devices or policies are analyzed for irregular activity patterns.

Continuous Compliance Reporting

Simplify and increase adherence to leading industry compliance and regulations

Audit Readiness

Access control, intrusion prevention, and malware detection policies are logged to support audit and compliance reviews. Device inventory updates, including additions, removals, and applied policy statuses, are documented. Historical changes in firewall rules, DNS policies, and identity policies provide visibility into security enforcement over time.

Compliance Risk Reporting

Risks associated with broad access permissions, missing security controls, and disabled protection mechanisms are identified. Policy enforcement inconsistencies, including gaps in monitoring and logging, are assessed for compliance alignment. Documentation of policy changes and device health ensures adherence to network security standards.

Access Control | Endpoint Security | Data Protections | **Network Security** | Config Management

Email Security | Remote Access | Vuln Management | Device Management | Web Services

Virtualization | Security Rating | CSPM & SSPM | SIEM / SOC | IT Management

Business Value Outcomes Of Technology Integration:

Ensure Continuous Security Posture Validation and Optimization for Cisco FTD:

Reduce Operational Overhead

Effectively align cybersecurity technology, people, and processes to remediate exposures and implement proactive critical security controls.

Identify, track, and validate CSC indicators across all cybersecurity tools to correct misconfiguration, malfunctions, or security gaps in critical functionality.

Increase Security Posture & Cyber Hygiene

Ensure effective cyber hygiene that minimizes an attacker's ability to gain unauthorized access to your network and applications.

Comprehensive and continuous analytics that detect deviations from normal behavior and align access control policies to your desired security state.

Accelerate Adherence to Compliance Frameworks

Understand & report your security risk posture, to ensure the of the adherence of your IPS configuration and security policies to common compliance frameworks.

Out-of-the box CSC's and reporting, that drive your alignment to regulatory compliance frameworks, to simplify audit readiness.

About Cisco

Cisco Systems, Inc. is the world's largest hardware and software supplier within the networking solutions sector. The secure, agile networks business contains switching, routing, and wireless solutions.

The hybrid work division has products for collaboration and contact center needs. The end-to-end security group has products spanning a variety of threat prevention necessities. The internet for the future division has routed optical networks, silicon, and optics. Optimized application experiences offer solutions such as full stack observability.

Services are Cisco's technical support and advanced services offerings. In collaboration with Cisco's initiative on growing software and services, its revenue model is focused on increasing subscriptions and recurring sales.

Find out more

About XM Cyber

XM Cyber is a leading Continuous Exposure Management company that transforms the way organizations approach cybersecurity risk mitigation.

Uniquely combine continuous security control validation with XM Attack Graph Analysis™ capability to discover CVEs, misconfigurations, and identity issues, along with weaknesses in cybersecurity posture across the full attack surface.

It analyses how attackers can chain exposures together, or evade security defences, to reach and then compromise critical assets. The platform then provides detailed remediation guidance and recommendations to increase security posture and reduce cyber risk, enabling security teams to prevent more attacks with 75% less remediation effort.

Find out more

Stop wasting time on fixes that don't impact risk

XM Cyber gives you the context you need to make faster and more confident decisions about your security posture. Understand what critical security controls you have in place and how they are helping you align to best practices and regulatory compliance frameworks.

Now you can achieve continuous compliance across your dynamic Infrastructure, helping you reduce operational overhead and more effectively align cybersecurity technology, people and processes to remediate misconfigurations and implement proactive critical security controls.

The platform enables you to report compliance risk, by first understanding and then validating your security risk posture and it's alignment to common compliance and regulatory frameworks. Which in turn minimizes the attackers' ability to evade your security defences and increases your overall security posture.

It's time to change how you work, by ensuring your IT and Security Operations teams have the guidance they need to design and optimize effective critical security controls, while also mobilizing effective remediation strategies, helping you

Fix Less. Prevent More.