XM Cyber | INTEGRATION SOLUTION BRIEF

XM Cyber x Splunk

Streamlining Investigation and Accelerate Response by Enriching Splunk with Exposure Intelligence

Executive Summary

The challenge for Splunk users isn't a lack of data, it's a lack of actionable and context-enriched data. In a sea of logs and notable events, it is nearly impossible for SOC analysts to manually determine which threats represent a true existential risk to business continuity. This "context gap" leads to slow investigation times and reactive firefighting.

The XM Cyber App for Splunk bridges this gap by embedding Continuous Exposure Management (CEM) directly into the SOC analyst's natural workflow. By integrating real-time Attack Graph Analysis™ into the Splunk environment, organizations can move beyond basic alerts to a platform-centric approach. This integration allows teams to enrich incidents with business context, accelerate response times, and audit potential attack paths before they result in a breach.

The Need for Continuous Exposure Management

Traditional SIEM workflows focus on what happened in the past. To stay ahead of modern threats, SOC teams need a forward-looking view of where the business is currently exposed. By providing end-to-end visibility into the entire attack surface and an effectively-scoped assessment of validated exposures leading to critical business assets, XM Cyber provides the "connective tissue" that Splunk requires to prioritize what matters most.

The integration ensures that Splunk notable events are no longer viewed in isolation. By correlating raw telemetry with pre-validated attack paths, the SOC can focus on the exposures that actually put "crown jewel" assets at risk, drastically reducing the noise and increasing operational efficiency.

Introducing

splunk> a cisco company

Power your SecOps with AI-driven SIEM

Gain comprehensive visibility, accurate detections, and operational efficiency across your security operations.

XM Cyber

Prevent Attacks That Put Your Business At Risk

Get ahead of attackers by continuously discovering, prioritizing, and fixing every validated exposure in YOUR environment before it's exploited.

Solution Benefits by Use Case

Assess Your Defenses Against Validated Exposures and Real-World Threats

Align on what matters most to the business and what's truly possible.

Assess Defenses Against Real-World Threats

Use the Sensors Overview dashboard to identify and investigate gaps in security coverage, ensuring that your attack surface is fully monitored and protected.

Align on Potential Breach Points

Correlate Splunk notable events with XM Cyber "choke points" to see how an attacker could pivot from a detected event toward your most critical assets.

Context-Aware Detection Engineering and Incident Response

Empower SOC teams with business context directly within their investigation and IR workflow.

Context-Aware Investigation

Enrich Splunk incidents with real-time attack graph context, giving analysts the "So What?" needed to disposition alerts with certainty and speed.

Accelerate Incident Response

Streamline response workflows by bypassing manual evidence gathering. Use out-of-the-box dashboards to see the specific causes behind score changes and risk.

Operationalize Exposure Intelligence

Ensure continuous alignment between proactive and reactive security teams.

Audit Attack Scenario Logs

Save and analyze detailed audit logs from XM Cyber within Splunk to reconstruct potential breach steps and satisfy compliance requirements.

Impact-Driven Prioritization

Use the Entities Overview and Scenario Exposure dashboards to track the specific threats that put your crown jewels and choke points at risk.

Access Control and IAM	Endpoint Security	Data Protection	Network Security	Config Management
Email Security	Remote Access	Vuln Management	Device Management	Web Services
Virtualization	Security Rating	SSPM Cloud Services	**SIEM / SOC**	IT Management

XM Cyber

As the pioneer of exposure management, XM Cyber delivers a continuous and actionable understanding of cyber risk across the entire attack surface, including hybrid, cloud, on-prem, OT, legacy, AI, and container environments. Powered by proprietary Attack Graph Analysis™, the platform continuously validates exploitable exposures against a digital twin of your production environment, applying nearly a decade of offensive security expertise. By revealing the critical choke points where multiple attack scenarios converge, XM Cyber directs security teams to the remediation actions that eliminate the most risk with the least effort. The result is measurable improvement in security posture through prioritized, high-impact remediation, along with clear, business-contextual reporting that enables leaders to communicate risk effectively and demonstrate security ROI.