XM Cyber | INTEGRATION SOLUTION BRIEF

XM Cyber x SentinelOne

Streamlining security operations by enriching Singularity Endpoint with attack graph analysis and exposure intelligence

Executive Summary

Despite massive advancements in threat detection and response tooling, many SOC teams still struggle with overwhelming alert volumes and false positives, leading to time wasted and downstream analyst fatigue.

XM Cyber and SentinelOne have joined forces to address this issue, seamlessly integrating real-time attack surface visibility and exposure intelligence into SentinelOne's Singularity Endpoint platform. This integration shifts SOC operations from reactive fire-fighting to proactive breach prevention by enriching detections with the context needed to make informed decisions quickly.

The Need for Continuous Exposure Management

The fundamental challenge SOC teams are facing is a lack of context; not only in terms of the attack surface, but also the business. Too often volume is a result of lacking or misaligned focus on what really matters, where the business is currently exposed and what's actually viable for potential threat actors to exploit. By providing end-to-end visibility into the entire attack surface, and an effectively-scoped assessment of validated exposures leading to critical business assets, Continuous Exposure Management (CEM) platforms serve as the foundation for delivering the exposure intelligence needed to fill in the context gaps.

The bi-directional integration between XM Cyber and SentinelOne ensures continuous alignment between security operations and risk management teams, ensuring that alert triage and incident response efforts are focused where they matter most. By seamlessly enriching alerts with exposure intelligence, SOC teams can quickly and easily prioritize the alerts related to pre-validated exposures and attack paths that put your critical assets and business at risk.

Introducing

SentinelOne

Stop Attacks with Unmatched Protection and Detection

AI-powered protection, detection, and response capabilities across endpoints, identities, and more.

XM Cyber

Prevent Attacks that Put Your Business At Risk

Continuously discover, prioritize and validate exposures across your entire hybrid attack surface.

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.

Align on Potential Breach Points

Identify and validate every potential attack path leading to critical assets that originate from compromised endpoints identified by SentinelOne.

Align on Potential Breach Points

Identify and validate every potential attack path leading to critical assets that originate from compromised endpoints identified by SentinelOne.

Context-Aware Detection Engineering and Incident Response

Empower SOC teams with business context directly within their EDR workflow.

Accelerate Incident Response

Drastically reduce investigation time by enriching every SentinelOne threat with XM Cyber's asset context to understand if a compromised asset is a stepping stone to your crown jewels.

Impact-Driven Prioritization

Understand the potential blast radius of an attack and whether a compromised asset identified by SentinelOne represents a choke point where multiple attack paths converge.

Operationalize Exposure Intelligence

Ensure continuous alignment between proactive and reactive security teams.

Automated Scenario Creation

Eliminate manual scenario configuration by using SentinelOne data to define the scope of exposure assessments, ensuring that validation efforts evolve dynamically alongside the threat landscape.

Shared Definition of Risk

Drive alignment between teams and effectively communicate your current risk posture and threat landscape to stakeholders across the organization.

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.