XM Cyber | INTEGRATION SOLUTION BRIEF

XM Cyber x Google Security Operations

Modernizing Security Operations by Enriching Google Security Operations (SecOps) with Exposure Intelligence

Executive Summary

SOC teams using Google SecOps can search billions of logs in seconds, but speed doesn't solve the "priority" problem. Analysts still struggle to determine if a suspicious event actually leads to a business-critical asset. Without reachability context, teams risk wasting time on isolated noise while actual attack paths remain open.

The XM Cyber integration for Google Security Operations (SecOps) creates a bi-directional intelligence loop between continuous exposure data and live security telemetry. By embedding XM Cyber's Attack Graph Analysis™ directly into the Google SecOps interface, analysts can automatically prioritize alerts based on verified risk. This integration uses automated playbook actions to calculate risk scores, enrich entities with business context, and push live breach points into attack simulations, turning static logs into a dynamic map of your organization's resilience.

The Need for Continuous Exposure Management

In modern security operations, the challenge is no longer about finding the needle in the haystack, it's about knowing which needles are actually poisonous. While SIEM platforms are elite at indexing historical events, they often lack the forward-looking visibility required to see how a single event connects to a larger attack path.

Continuous Exposure Management (CEM) shifts the focus from individual events to validated reachability. By layering an attack graph over real-time telemetry, SOC teams can see the full threat landscape from all angles, understanding every possible route an adversary could take before an attack ever happens. This allows the SOC to move from a reactive posture to a risk-based posture, where they prioritize threats based on their proximity to the organization's most critical business assets.

Introducing

Google SecOps

Say Goodbye to Legacy Security Operations

Helping organizations transform cybersecurity with frontline intelligence, expertise, and AI-powered innovation.

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.

Identify Visibility Blind Spots

Detect unmanaged assets or "shadow IT" that aren't sending logs to Google SecOps, ensuring your detection coverage matches your actual attack surface.

Map Potential Impact

Instantly see if a flagged entity is a dead-end or a "choke point" gateway. Understand the full blast radius of a detection before an attacker moves laterally.

Context-Aware Detection Engineering and Incident Response

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

Enrich Discovery with Identity Data

Automatically pull deep metadata (MFA status, Admin roles, and privilege levels) into SecOps widgets to determine the "stakes" of an alert without manual research.

Automated Alert Disposition

Use risk scoring to auto-close low-risk noise and auto-escalate threats that have a verified route to your most sensitive data.

Operationalize Exposure Intelligence

Ensure continuous alignment between proactive and reactive security teams.

Prioritize by Business Risk

Shift the focus from "High Severity" logs to "High Risk" scenarios, ensuring the SOC is working on the alerts that actually threaten business continuity.

Close the Feedback Loop

Transform live detections into active simulations. Mark suspicious users as "Breach Points" in XM Cyber to test how your environment holds up against a real-world pivot.

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.