XM Cyber | INTEGRATION SOLUTION BRIEF

XM Cyber x Cortex XSOAR / XSIAM

Enrich Your SOC with the Context Needed to Make Informed, Autonomous Decisions

Executive Summary

The challenge for SOC teams 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 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 integration for XSOAR and XSIAM embeds continuous exposure management directly into your automated Cortex workflows. By seamlessly injecting attack surface and exposure intelligence into security teams' existing workflows can bridge the gap between reactive and proactive tooling and teams.

The Need for Continuous Exposure Management

Standard SOAR playbooks often trigger based on isolated alerts, leading to automated actions that may not address the root cause of a systemic risk. Modern SOC and IR teams need a proactive lens to understand the broader context of an incident. By mapping the entire attack surface and validating potential paths to your most critical assets, XM Cyber serves as the decision-support engine for Cortex.

This integration transforms how analysts manage XSOAR and XSIAM Incidents. Instead of responding to alerts in a vacuum, playbooks can now be enriched with pre-validated attack path data. By correlating real-time security events with exposure intelligence, your team can automate the prioritization of threats that have a viable route to your crown jewels, ensuring that your most powerful automation resources are always directed at the highest-impact risks.

Introducing

CORTEX BY PALO ALTO NETWORKS

Supercharge Incident Response Across Your SOC

Unleash machine speed and precision with the autonomous SOC built to stop tomorrow's threats.

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.

Seamless, Intuitive Analyst Experience

Incorporate exposure intelligence from the XM Cyber platform - including entity details, choke points, and risk scores - directly into the Cortex XSOAR War Room. This integration provides a unified interface for investigation, allowing analysts to triage incidents without context-switching.

Set Breach Points in Attack Graph Context

Understand instantly whether an affected asset sits on a validated attack path leading to critical business systems. This context allows for immediate Incident Mirroring, helping analysts determine if an alert requires urgent escalation or if the asset is effectively isolated from your crown jewels.

Context-Aware Detection Engineering and Incident Response

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

Context-Aware Investigation

Enrich XSOAR Incidents with real-time attack graph context. By correlating indicators of compromise (IOCs) with the attack surface, analysts gain the certainty needed to disposition alerts faster and prioritize remediation based on actual business risk.

Accelerate Incident Response

Streamline response workflows by automating evidence gathering through XSOAR playbooks. Use out-of-the-box dashboards and XM Cyber's exposure data to trigger automated containment actions at key choke points, stopping attackers before they reach a critical asset.

Operationalize Exposure Intelligence

Ensure continuous alignment between proactive and reactive security teams.

Audit Attack Scenario Logs

Ingest and analyze detailed audit and simulation logs from XM Cyber within Cortex to reconstruct potential breach steps. This provides a clear trail for post-incident reviews and ensures compliance requirements are met with validated exposure data.

Impact-Driven Prioritization

Leverage the Entities Overview and Scenario Exposure findings to drive your orchestration strategy. Focus your automated playbooks on the specific threats and weakest links that put your crown jewels at risk, ensuring a high-impact, low-noise security posture.

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.