XM Cyber | INTEGRATION SOLUTION BRIEF

XM Cyber x QRadar

Empowering the Modern SOC with Threat Visibility and Exposure Intelligence

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 App for IBM QRadar embeds continuous exposure management directly into your security operations. By integrating XM Cyber's comprehensive toolset into QRadar, security teams can leverage hybrid attack path data to bridge the gap between detection and remediation across cloud and on-premise environments.

The Need for Continuous Exposure Management

Standard SIEM operations are inherently reactive, focusing on historical logs. However, modern SOC teams require a proactive lens to identify where the organization is currently vulnerable. By mapping the entire attack surface and validating potential paths to your most critical assets, XM Cyber acts as the strategic intelligence layer for IBM QRadar.

This integration transforms how analysts handle QRadar Offenses. Rather than treating alerts as isolated incidents, the SOC can now contextualize every event within a pre-validated attack path. By syncing real-time telemetry with exposure data, your team can ignore the noise and focus exclusively on the threats that have a viable route to your crown jewels.

Introducing

QRadar®

Empowering the Modern SOC with Threat Visibility

Redefine SIEM to unleash analyst potential and outpace adversaries with speed, scale and accuracy.

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 QRadar interface for seamless, one-pane-of-glass investigations.

Set Breach Points in Attack Graph Context

Understand whether or not an affected asset sits on validated attack paths leading to critical assets, helping analysts with alert disposition and escalating incidents based on asset and business criticality.

Context-Aware Detection Engineering and Incident Response

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

Context-Aware Investigation

Enrich QRadar Offenses with real-time attack graph context, giving analysts the attack surface and exposure context 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 QRadar 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.