XM Cyber | SOLUTION BRIEF

Closing the Gap Between Exposure Discovery & Remediation

Drive efficient and effective exposure remediation with the evidence required to overcome the burden of proof

Security teams are drowning in context-less alerts that IT lacks the bandwidth to fix. Without proof of exploitability or a way to account for existing controls, organizations waste effort on low-risk patches while critical choke points remain open. This creates a burden of proof gap where remediation stalls, legacy systems remain exposed, and there is no automated way to verify if a fix actually worked.

XM Cyber closes this gap by using a digital twin to continuously validate exposures against real-world attack paths without risking production. It directs teams to high-impact choke points where a single fix severs multiple attack routes, providing IT with the step-by-step guidance and alternative mitigations needed to act. By integrating directly into workflows and providing automated remediation confirmation, it replaces guesswork with documented proof of risk reduction.

SOLUTION BENEFITS

See Every Exposure, Every Path

Uncover every possible path an attacker could take to compromise your critical assets and data, with continuous validation ensuring teams focus on exposures that are truly exploitable and impact the business.

Act for Impact, Not Just Severity

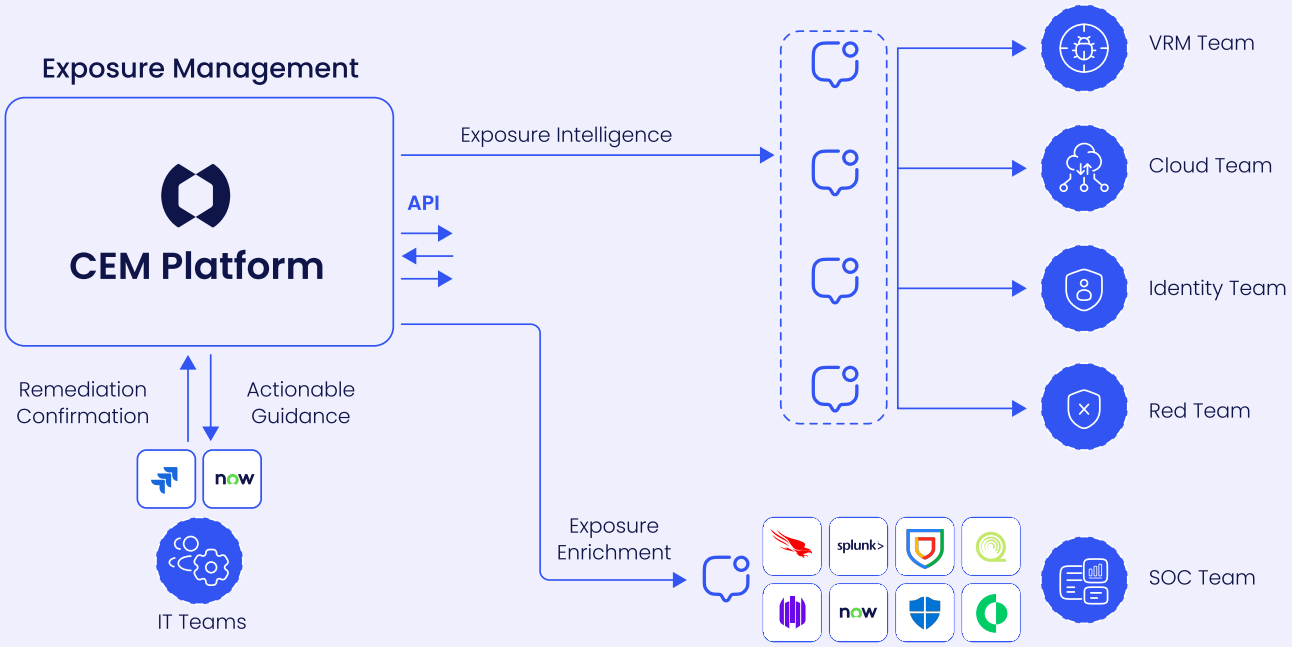
Focus remediation efforts on severing validated attack paths, targeting choke points to reduce the potential blast radius quickly and with the least amount of effort.

Articulate Risk, Drive Remediation

Continuously validate the impact of remediation teams, proving fixes have been implemented successfully and efforts have meaningfully improved the organization's security posture.

Exposure Findings You Can Trust

When XM Cyber suggests a fix, teams know it's been validated against real threats and existing security controls.



Prove Exploitability and Potential Impact to Drive Urgency

Continuous validation using a digital twin approach ensures every exposure is truly exploitable and suggested fixes will work.

Focus Remediation Efforts On Choke Points to Maximize Impact

Continuous validation using a digital twin approach ensures every exposure is truly exploitable and suggested fixes will work.

Fix What Matters, Even When a Patch Isn't Possible

Understand exactly how to eliminate risk with alternative mitigation options where fixes aren't possible or delayed.

Drive Autonomous Remediation with Actionable Exposure Intelligence

Drive actionability across your entire security stack by pushing exposure intelligence directly into the ITOps, AI SOC, or SOAR tools your teams use today.

Continuous Testing Confirms Fixes Are Successfully Implemented

Prove fixes worked as intended and confidently communicate progress in reducing risk across the organization.

Integrate Seamlessly with Existing Tooling and Workflows

Flexible, API-driven integrations with common security and ITOps tools help facilitate remediation operations and incident response workflows.

Learn more at xmcyber.com

XM Cyber