Automate Remediation of XM Cyber Attack Path Discovery with Cortex XSOAR

Discover & Disrupt Active Attack Paths

Continuous Attack Path Management and Risk Prioritization Increases Productivity

For most security professionals, simulating attacks comes down to just testing basic security controls. While testing is an important part of SOC upkeep, security teams need to verify that their defenses are hardened against all types of threats. For example: misconfigurations, unpatched vulnerabilities, and overly permissioned accounts are pervasive across most enterprise security environments. The ability to continuously map possible attack paths to your network assets is critical for revealing the current threat vectors and exploits that can be used by your adversaries, and will help prioritize what to fix first.

Leveraging insights from XM Cyber in Cortex XSOAR helps your team gain context to better understand alerts and security controls, so they can continuously improve your network defenses. Your security team can also use Cortex XSOAR and XM Cyber to simulate attacks that reflect your environment to discover and prioritize real exposures in your network and model new attack paths to your critical assets.

Benefits of the Integration

Understand risk:
Increased visibility for your business critical assets helps you understand your overall security posture and prioritize remediation.

Gain actionable intelligence:
Access contextual information on an operating exploit or attack technique, including a list of assets that may be directly or indirectly compromised.

Streamline remediation:
Receive prioritized response advice that requires less effort from your security team during an incident.

The XM Cyber Content Pack

XM Cyber delivers continuous visibility and proactive insight to enterprises through a risk-free solution that automatically identifies threats to critical business assets. By adding attack-centric intelligence and context to your recommended remediation steps, your security team can optimize resources and focus on the most important incidents.

Cortex XSOAR unifies case management, automation, real-time collaboration, and threat intelligence management to transform every stage of the incident lifecycle, resulting in significantly faster responses that require less manual effort and review.

The XM Cyber content pack for Cortex XSOAR provides full coverage of attack pathing, enabling your SOC to automate meaningful testing. Your team can use this powerful integration to:

- Identify successful attack vectors to your systems and label techniques by name.
- Enrich endpoints and IP addresses with impacted entities and assets, including a complexity of compromise summary, and more.
- Scan and isolate threats, with the option to take immediate action during incidents.

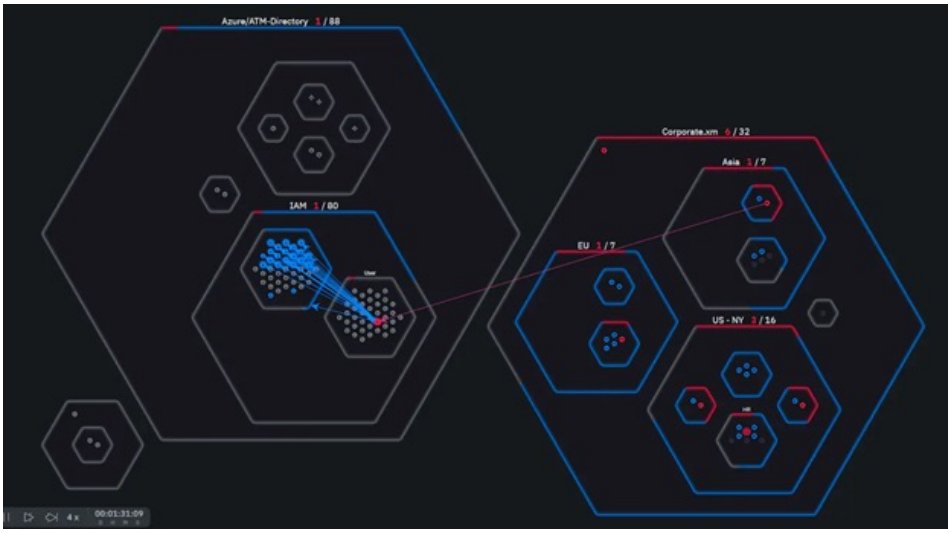

Figure 1- XM Cyber Battleground visualizes all possible attack paths to your critical assets

Cortex XSOAR Marketplace is a digital storefront for discovering turn-key security orchestration content packs centrally within Cortex™ XSOAR.

Content packs are prebuilt bundles of integrations, playbooks, dashboards, fields, subscription services, and all the dependencies needed to support specific security orchestration use cases.

The XM Cyber pack allows the SOC to see more attack context and automatically respond to incidents, leveraging attack-centric data to provide prioritized remediation.

Core content pack includes:

3 classifiers **28** incident fields **5** incident types **1** integration **3** layouts **4** playbooks

The XM Cyber content pack is easily deployed with a single click from the online Marketplace, giving you all the content needed to understand your risk and prioritize what to fix first with Cortex XSOAR.

Bridge gaps and advance the maturity of your security program by tapping into the fastest-growing community of security experts. To discover new SOAR content, visit paloaltonetworks.com/cortex/xsoar/marketplace.

Solution:

If you want to improve your team's response times and reduce the effort it takes to discover and investigate threats, you can leverage the XM Cyber content pack to automate attack path discovery, incident handling, and response within Cortex XSOAR. The XM Cyber Attack Path Management solution provides visibility and intelligence to discover how attackers would pivot across your cloud or on-premise environments to breach your critical assets. This integration also provides context enrichment for prioritized remediation such as identification and placement of devices and entities that are at risk of being attacked.

Benefit:

Automate the continuous assessment of your ecosystem's risk exposures and enable a prioritized remediation plan with Cortex XSOAR and XM Cyber to scale your organization's security posture without adding any new staff or expertise to your current SOC team.

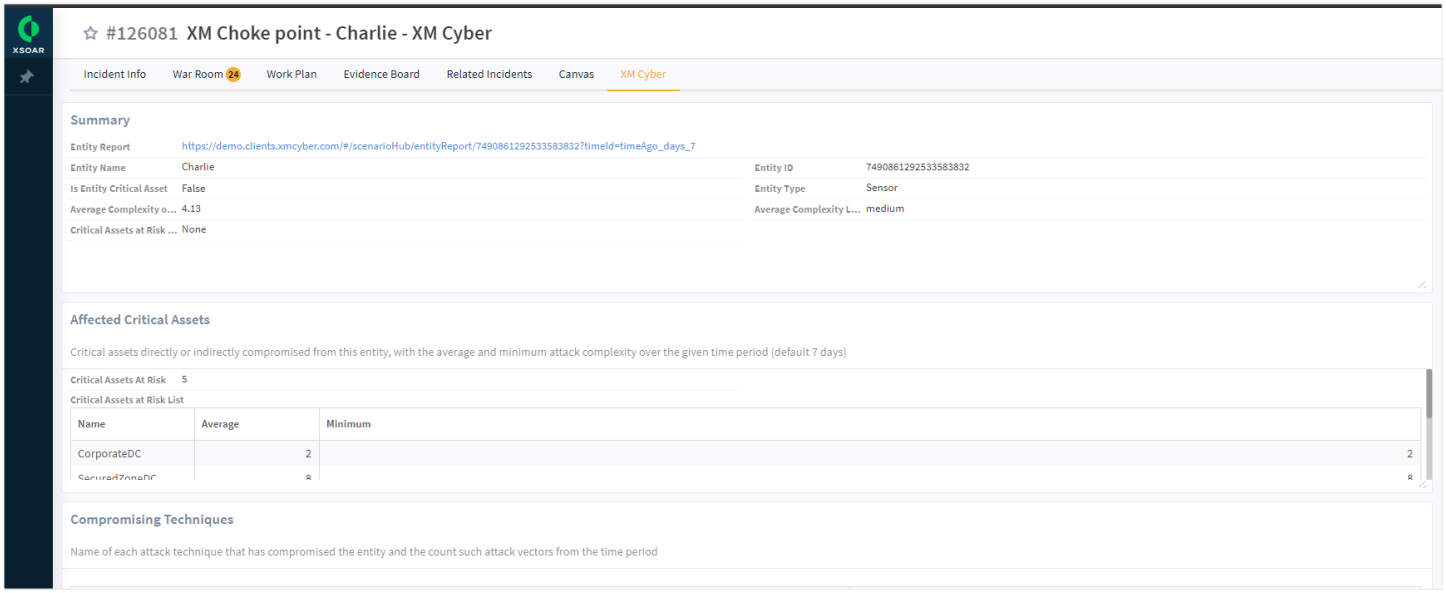

Figure 2 – Access a detailed report of attack techniques from within Cortex XSOAR

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

About XM Cyber

XM Cyber is the global leader in attack path management. The XM Cyber platform enables companies to rapidly respond to cyber risks affecting their business-sensitive systems by continuously finding new exposures, including exploitable vulnerabilities and credentials, misconfigurations, and user activities. XM Cyber constantly simulates and prioritizes the attack paths putting mission-critical systems at risk, providing context-sensitive remediation options. XM Cyber was founded by top executives from the Israeli cyber intelligence community and has offices in North America, Europe, and Israel.

For more information, go to xmcyber.com and follow us on Twitter @XMCyber_ and LinkedIn.com/company/xm.

XM CYBER

Tel Aviv +972 3 978 6668
New York +1 866 598 6170
London +44 203 322 3031
Munich +49 163 6288041
info@xmcyber.com