



## Check Point + XM Cyber *Cybersecurity Controls Monitoring*

Organizations today use on average 80 security tools to implement, manage, and secure their data. Aligning these multiple security controls to security benchmarks, recommendations, regulations, and best practices can be quite chaotic. One solution for managing the chaos is adopting tools that work well together, something Gartner defines as a Cybersecurity Mesh Architecture (CSMA). A cybersecurity mesh enables tools to interoperate through several supportive layers, such as a consolidated policy management, security intelligence and identity fabric.

### Joint Solution

XM Cyber and Check Point Software seamlessly integrate, enabling enterprises to manage their cybersecurity environment while continuously monitoring their cyber security eco-system posture. XM Cyber continuously monitors Check Point Firewalls with IPS (intrusion prevention) and alert IT staff on key aspects and issues that could affect the entire organization.

XM Cyber can be deployed in a corporate network with a Check Point security infrastructure in a few hours providing:

- indicators of misconfigured tools and gaps in cybersecurity protection
- continuous and proactive recommendations for improving security status
- alerts in case of deviation from normal behavior

### Extensible, Agile Security Management

The solution is made possible by open APIs in the Check Point Security Management platform. The Check Point consolidated security management platform provides a single view into all security configurations, and delivers comprehensive visibility into all network traffic, applications, events and threats. Check Point management enables customers and third parties to customize the security management to fit their specific needs. This is achieved with a secure, trusted API architecture, allowing for web and command line management. These features create a truly consolidated security management solution with high operational efficiency, risk visibility and delegated security.

## XM Cyber Continuous Security Monitoring

XM Cyber Security Controls Monitoring is a single pane of glass cybersecurity orchestration management and awareness solution that continuously measures cybersecurity maturity and on-line status by retrieving and analyzing Critical Security Controls (CSCs) from the enterprise's security tools that are already deployed in the organization network. This empowers CISOs, Risk Officers, IT infrastructure managers and C-Level executives with alerts from an informative, continuous and comprehensive security-aware management knowledgebase.

### Use case #1 Firewall/IPS Configuration Issues

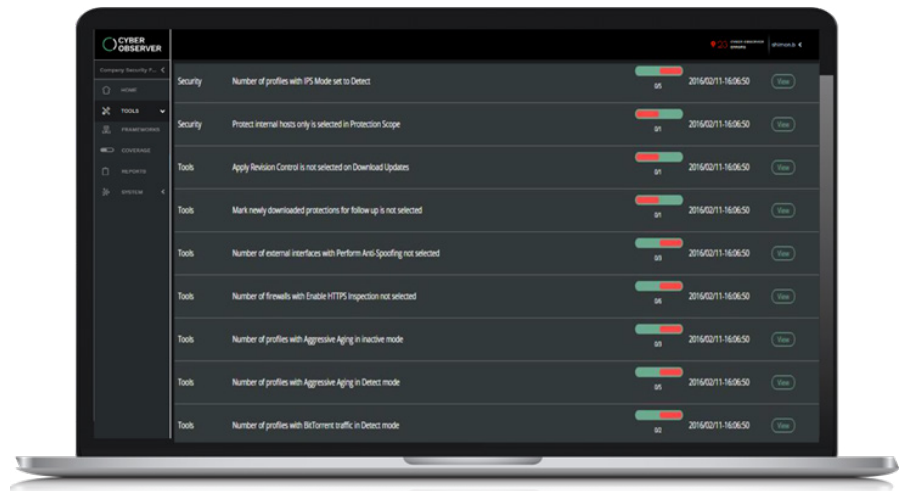
#### Key findings:

- Interfaces with Perform Anti-Spoofing not selected
- Accept stateful UDP replies for unknown services is turned on
- Drop out of state tcp packets is turned off

### Use case #2 Firewall Insecure Rules

#### Key findings:

- Telnet service accept rules found
- Any-Any accept rule(s) found
- Policies with cleanup rule not found



#### About Check Point

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)) is a leading provider of cyber security solutions to corporate enterprises and governments globally. Check Point Infinity's portfolio of solutions protects enterprises and public organizations from 5<sup>th</sup> generation cyber-attacks with an industry leading catch rate of malware, ransomware and other threats. Infinity comprises three core pillars delivering uncompromised security and generation V threat prevention across enterprise environments: Check Point Harmony, for remote users; Check Point CloudGuard, to automatically secure clouds; and Check Point Quantum, to protect network perimeters and datacenters, all controlled by the industry's most comprehensive, intuitive unified security management; Check Point Horizon, a prevention-first security operations suite. Check Point protects over 100,000 organizations of all sizes.

#### About XM Cyber

XM Cyber is a leading hybrid cloud security company that's changing the way organizations approach cyber risk. XM Cyber transforms exposure management by demonstrating how attackers leverage and combine misconfigurations, vulnerabilities, identity exposures, and more, across AWS, Azure, GCP and on-prem environments to compromise critical assets. With XM Cyber, you can see all the ways attackers might go, and all the best ways to stop them, pinpointing where to remediate exposures with a fraction of the effort. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, and Israel.