CONTINUOUS IOT/OT THREAT MONITORING FOR AZURE SENTINEL

Rapidly detect and respond to IoT/OT threats with automation and integration. Gain the benefits of CyberX’s agentless security platform and IoT/OT-aware behavioral analytics – combined with Azure Sentinel’s cloud-native scalability, simplicity, and machine learning.

The IoT/OT Security Challenge

As organizations connect massive numbers of IoT/OT devices to their networks to optimize operations, boards and management teams are increasingly concerned about the expanding attack surface and corporate liability they represent.

Because these connected devices can’t easily be protected by agent-based technologies — and are often unpatched or misconfigured — they can be compromised by adversaries to pivot deeper into corporate networks to threaten safety, disrupt operations, steal intellectual property, and siphon resources for DDoS botnets and cryptojacking.

Addressing the Challenge with Robust, Agentless IoT/OT Security

CyberX’s agentless IoT/OT security platform is easy to deploy and provides real-time visibility to all unmanaged IoT/OT devices, vulnerabilities, and threats — within minutes of being connected to the network.

Leveraging multiple threat detection mechanisms including the industry’s only patented, IoT/OT-aware behavioral analytics — eliminating the need to configure any rules or signatures — CyberX continuously monitors IT/OT networks for unauthorized or anomalous activities.

Your Bird’s-Eye View Across the Enterprise

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

The integration of CyberX and Azure Sentinel brings additional context, speed, and precision to threat investigation and threat hunting, enabling defenders to be more nimble and efficient in mitigating threats that frequently cross IT/IoT/OT boundaries.
Leveraging Azure Sentinel’s machine learning and artificial intelligence, CyberX’s IoT/OT threat alerts and deep contextual information can now be correlated and analyzed alongside diverse sources of security intelligence including Microsoft Defender Advanced Threat Protection (formerly Windows Defender ATP) and other Microsoft Threat Protection solutions, plus Azure Security Center for IoT, Azure AD, Office 365, and more.

In addition, there are built-in connectors to the broader security ecosystem from other Microsoft Intelligent Security Association partners such as Check Point, Cisco, F5, Fortinet, Palo Alto Networks and Symantec, as well as broader ecosystem partners such as ServiceNow.

LEFT: CyberX’s integration with Azure Sentinel is configurable and out-of-the-box. Note that encrypted communication using SSL/TLS 1.2 can also be enabled on this screen.

About CyberX

We know what it takes.

Funded by Norwest Venture Partners, Qualcomm Ventures, and other leading venture firms, CyberX delivers the only cybersecurity platform built by blue-team experts with a track record of defending critical national infrastructure. That difference is the foundation for the most widely deployed platform for continuously reducing IoT/OT risk and preventing costly outages, safety and environmental incidents, theft of intellectual property, and operational inefficiencies. For more information, visit CyberX.io or follow @CyberX_Labs.