Palo Alto Networks and CyberX

ICS/SCADA Threat Detection and Prevention

Benefits of the Integration

The CyberX platform uniquely combines:

- Deep understanding of industrial devices, protocols, and applications
- Continuous monitoring and ICS-aware behavioral analytics
- Asset and network topology discovery
- Risk and vulnerability management
- Automated threat modeling and threat intelligence

Palo Alto Networks Next-Generation Firewalls provide:

- Highly granular visibility into traffic at application and user levels
- The ability to apply these parameters in policy

The Challenge

Companies with critical industrial infrastructure are increasingly concerned about ICS/SCADA cyberattacks by nation-states and cybercriminals.

As Information Technology (IT) and Operational Technology (OT) networks have become increasingly connected to support digitalization and collection of real-time intelligence from production operations, the attack surface has increased, and with it the risk of both targeted attacks and malware infection.

While downtime in a traditional IT environment can interrupt business continuity, breaches in OT environments can have far more devastating effects, including costly production outages, catastrophic safety failures, environmental damage, and theft of corporate intellectual property.

CyberX

The CyberX platform provides continuous monitoring with specialized behavioral analytics purpose-built to detect unauthorized or suspicious ICS/SCADA traffic. The platform incorporates patented, ICS-aware self-learning engines that automatically inventory and profile assets, identify vulnerabilities, and detect a wide range of threats in real time without relying on rules or signatures, specialized skills, or prior knowledge of the environment. Plus, it uses passive monitoring to ensure zero impact on the ICS/SCADA network.

Palo Alto Networks

Palo Alto Networks Next-Generation Firewalls offer a prevention-focused architecture that is easy to deploy and operate. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere. Next-Generation Firewalls inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. The user, application, and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies as well as write rules that are easy to understand and maintain.

Palo Alto Networks and CyberX

Palo Alto Networks and CyberX have integrated an off-the-shelf solution that leverages Panorama™ network security management to automatically create new policies in Palo Alto Networks Next-Generation Firewalls based on contextual information the CyberX platform provides. A one-click "confirmation mode" prompt ensures a human in the loop at all times.

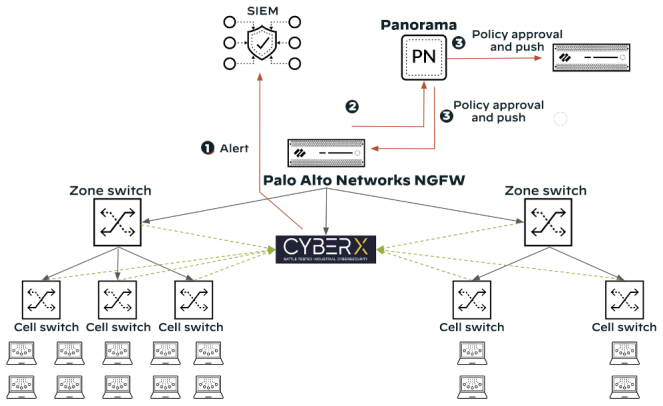

Figure 1: Rapidly blocking sources of malicious traffic in an ICS/SCADA network with CyberX and Panorama

Key Use Cases for Prevention

This integration supports an array of use cases, including:

- **Unauthorized PLC changes:** An update to the ladder logic or firmware of a device can represent a legitimate activity or an attempt to compromise the device by inserting malicious code, such as a RAT, or parameters that may causing a physical process—such as a spinning turbine—to malfunction.
- **Protocol violation:** A non-permitted packet structure or a field value that violates the protocol specification can represent a misconfigured application, but it may also indicate a malicious attempt to compromise the device by, for example, causing a buffer overflow condition.
- **PLC stop:** A command that causes a device to stop functioning puts at risk the physical process that the programmable logic controller (PLC) is controlling.
- **Malware in the ICS network:** ICS-specific malware, such as TRITON or Industroyer, can manipulate ICS devices via their native protocols. CyberX detects IT malware that moves laterally into an ICS/SCADA environment, such as Conficker, WannaCry, or NotPetya.
- **Scanning malware:** Reconnaissance tools let attackers collect data about system configurations during a pre-attack phase. For example, the Havex Trojan scans industrial networks for devices using Open Platform Communications (OPC), a standard protocol used by Windows®-based SCADA systems to communicate with ICS devices.

Rapid Creation of Asset-Based Policies

CyberX has also developed an integration with the Palo Alto Networks Security Operating Platform® that facilitates automatic creation of fine-grained, ICS-aware policy templates using tags based on the type of asset.

Using passive network traffic analysis (NTA), the CyberX platform automatically discovers all assets and their communication behavior, fingerprinting the asset type and associated properties (e.g., protocol, vendor, firmware revision level). By automatically tagging devices with their discovered properties (e.g., device type) and whether or not they are authorized devices, the CyberX application enables administrators to rapidly create asset-based policies. Administrators can also rapidly create Dynamic Address Groups (DAGs) using these asset-based tags.

Examples of ICS-aware policies include:

- "Unauthorized devices are not allowed to communicate between subnets"
- "HMIs can only communicate with PLCs using the MODBUS protocol"
- "Only engineering workstations are allowed to program PLCs"

About CyberX

Founded by military cyber-experts with nation-state expertise defending critical infrastructure, CyberX provides the most widely-deployed platform for continuously reducing ICS/SCADA/OT risk.

Our ICS-aware self-learning engines deliver immediate insights about assets, vulnerabilities, and threats—in less than an hour—without relying on rules or signatures, specialized skills, or prior knowledge of the environment.

CyberX is a member of the Palo Alto Networks Application Framework Community and the IBM Security App Exchange Community, and has partnered with premier solution providers and MSSPs worldwide including Optiv Security, DXC Technology, Wipro, and Deutsche-Telekom/T-Systems.

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. Find out more at www.paloaltonetworks.com.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com