SOLUTION BRIEF

CYBERX AND CYBERARK INTEGRATION

Secure Remote Access For Industrial Networks

Reducing OT Risk from Unauthorized Remote Access

The March 2018 FBI/DHS alert clearly documented how threat actors are leveraging compromised remote access credentials to access critical infrastructure networks via remote desktop and VPN connections. By using trusted connections, this approach easily bypasses any OT perimeter security. Credentials are typically stolen from privileged users — such as control engineers and third-party maintenance personnel — who require remote access to perform daily tasks.

Continuous Monitoring & Privileged Access Security for OT

As the trusted leader in Privileged Access Security, CyberArk offers a range of capabilities for securing privileged credentials and controlling remote access to critical assets such as engineering workstations and HMI's.

CyberX provides the most widely-deployed platform for continuously reducing ICS & IIoT risk, incorporating ICS-aware asset discovery, risk and vulnerability management, and continuous monitoring with behavioral anomaly detection.

HIGHLIGHTS

- Real-time alerting on unauthorized remote access
- Audit trail of all remote access sessions
- Investigations and forensic queries based on remote access protocols

BENEFITS

- Enable secure remote access by privileged users and third-party vendors
- Strengthen operational resilience
- Implement unified IT/OT security governance leveraging scarce security resources across both IT and OT

THE CYBERX PLATFORM

- Passive monitoring with optional selective probing (active component)
- Broadest & deepest understanding of ICS/SCADA protocols, devices, and applications — across all automation vendors (vendor-agnostic)
- Continuous ICS asset visibility, vulnerability management & threat monitoring

CYBERARK PRODUCTS + SOLUTIONS

- Core Privileged Access Security
- Privileged Session Manager
The integration of CyberX with CyberArk Privileged Account Security enables industrial organizations to:

- **Receive real-time alerts** whenever CyberX detects remote sessions that were not authorized by the CyberArk solution. Additionally, CyberX can immediately detect anomalous remote communication sessions indicating a potential breach of the OT network.

- **Continuously monitor and audit** privileged user sessions in the CyberX console, including which OT devices are being accessed and whether the session is being monitored and recorded by CyberArk Privileged Session Manager, which is part of the Core Privileged Access Solution.

- **Perform incident response, threat hunting & threat modeling**: SOC analysts can query the CyberX event timeline to identify all remote sessions based on forensic details such as access protocols (SSH, RDP, etc.) and source/destination details. SOC analysts can also leverage CyberX’s exclusive automated threat modeling to identify and proactively secure multi-step attack chains that rely on remote access connections to compromise critical OT assets.

### Common Use Cases

1. **Real-time alerting**: Whenever the CyberX platform identifies remote sessions that have not been authorized by CyberArk Privileged Session Manager, it will issue an “Unauthorized Remote Session” alert as shown in the screen shot. To facilitate immediate investigation, the alert also shows the IP addresses and names of the source and destination devices.
2. Event timeline: Whenever CyberArk Privileged Session Manager authorizes a remote connection, it will be documented and visible in the CyberX Event Log page, which shows a timeline of all alerts and notifications. This acts as an additional audit trail, as seen here:

3. Auditing and forensics: Administrators can also audit and investigate remote access sessions by querying the CyberX platform via its built-in data mining interface. This can be used to identify all remote access connections that have occurred including forensic details such as From/To devices, protocols (RDP, SSH, etc.), Source/Destination users, time-stamps, and whether the sessions were authorized using PSM.
ABOUT CYBERX

We know what it takes.

CyberX delivers the only industrial cybersecurity platform built by blue-team experts with a track record defending critical national infrastructure. That difference is the foundation for the most widely-deployed platform for continuously reducing IIoT and ICS risk and preventing costly production outages, safety failures, environmental incidents, and theft of sensitive intellectual property.

CyberX delivers the only IIoT & ICS security platform addressing all five requirements of the NIST CSF and all four requirements of Gartner’s Adaptive Security Architecture. CyberX is also the only IIoT & ICS security company to have been awarded a patent for its ICS-aware threat analytics and machine learning technology.

Notable CyberX customers include 2 of the top 5 US energy providers; a top 5 US chemical company; a top 5 global pharmaceutical company; and national electric and gas utilities across Europe and Asia-Pacific. Strategic partners include industry leaders such as Palo Alto Networks, IBM Security, Splunk, McAfee, Optiv Security, DXC Technology, and Deutsche-Telekom/T-Systems.

Customers choose CyberX because it’s the simplest, most mature, and most interoperable solution for auto-discovering their assets, identifying critical vulnerabilities and attack vectors, and continuously monitoring their ICS networks for malware and targeted attacks. What’s more, CyberX provides the most seamless integration with existing SOC workflows for unified IT/OT security governance.

For more information, visit CyberX.io or follow @CyberX_Labs.