CyberX
Trusted. Industrial. Cybersecurity.

CYBERARK®

CyberX and CyberArk Integration

Ensuring secure remote access for industrial networks

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 zero impact on production OT networks
- Physical or virtual appliances
- No rules, signatures, or agents
- Broadest and deepest understanding of ICS/SCADA protocols, devices, and applications— across all automation vendors (vendor-agnostic)
- Continuous ICS asset visibility, vulnerability management & threat monitoring
- Native integration with SIEMs and firewalls

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 Account 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 HMIs.

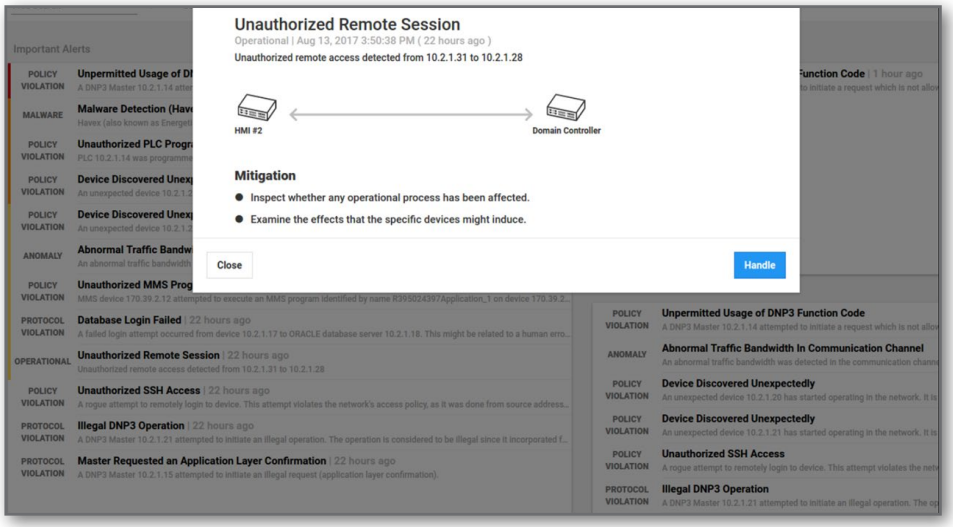
CyberX provides the most widely-deployed platform for continuously reducing ICS & IIoT risk, incorporating ICS-aware asset discovery, risk and vulnerability management, and continuous monitoring with behavioral anomaly detection.

The integration of CyberX with CyberArk Privileged Account Security enables industrial organizations to:

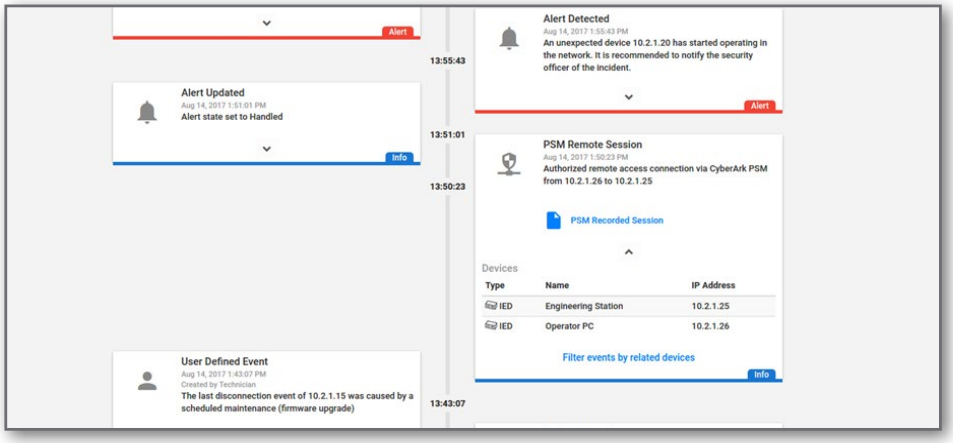
- **Receive real-time alerts** whenever CyberX detects remote sessions that were not authorized by the CyberArk solution. Additionally, CyberX can immediately detect anomalous remote communication sessions indicating a potential breach of the OT network.
- **Continuously monitor and audit** privileged user sessions in the CyberX console, including which OT devices are being accessed and whether the session is being recorded by CyberArk Privileged Session Manager (PSM).
- **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

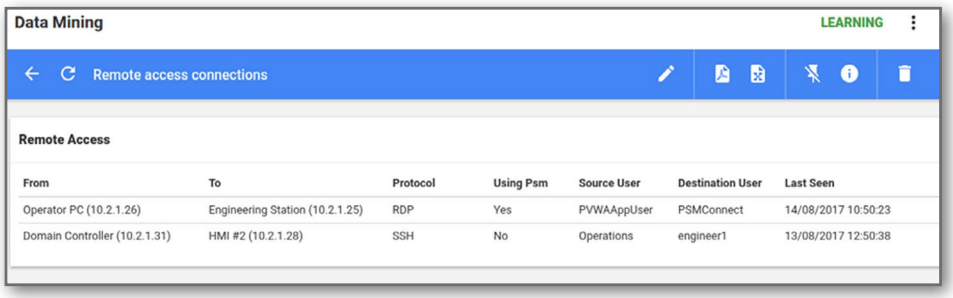
1. REAL-TIME ALERTING: Whenever the CyberX platform identifies remote sessions that have not been authorized by PSM, it will issue an "Unauthorized Remote Session" alert as shown in the screen shot. To facilitate immediate investigation, the alert also shows the IP addresses and names of the source and destination devices.



2. EVENT TIMELINE: Whenever PSM 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 & 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 the CyberX Platform

CyberX combines a deep, embedded understanding of industrial devices, protocols, and applications with continuous monitoring, ICS-aware behavioral analytics, and ICS threat intelligence. CyberX's proprietary, ICS-aware self-learning engines deliver immediately insights about OT assets, vulnerabilities, and threats – in less than an hour – without relying on rules or signatures, specialized skills, or prior knowledge of the environment.

About CyberX

Founded by military cyber experts with nation-state expertise defending critical infrastructure, CyberX provides the most widely-deployed platform for continuously reducing IIoT and ICS risk. CyberX is backed by elite investors including Norwest Venture Partners (NVP). The company is a member of the IBM Security App Exchange Community and the Palo Alto Networks Application Framework Community, and has partnered with other best-of-breed security suppliers including CyberArk. CyberX's partners also include premier solution providers and MSSPs worldwide including Optiv Security, DXC Technology, and Deutsche-Telekom/T-Systems.

CyberX
Trusted. Industrial. Cybersecurity.

CYBERARK