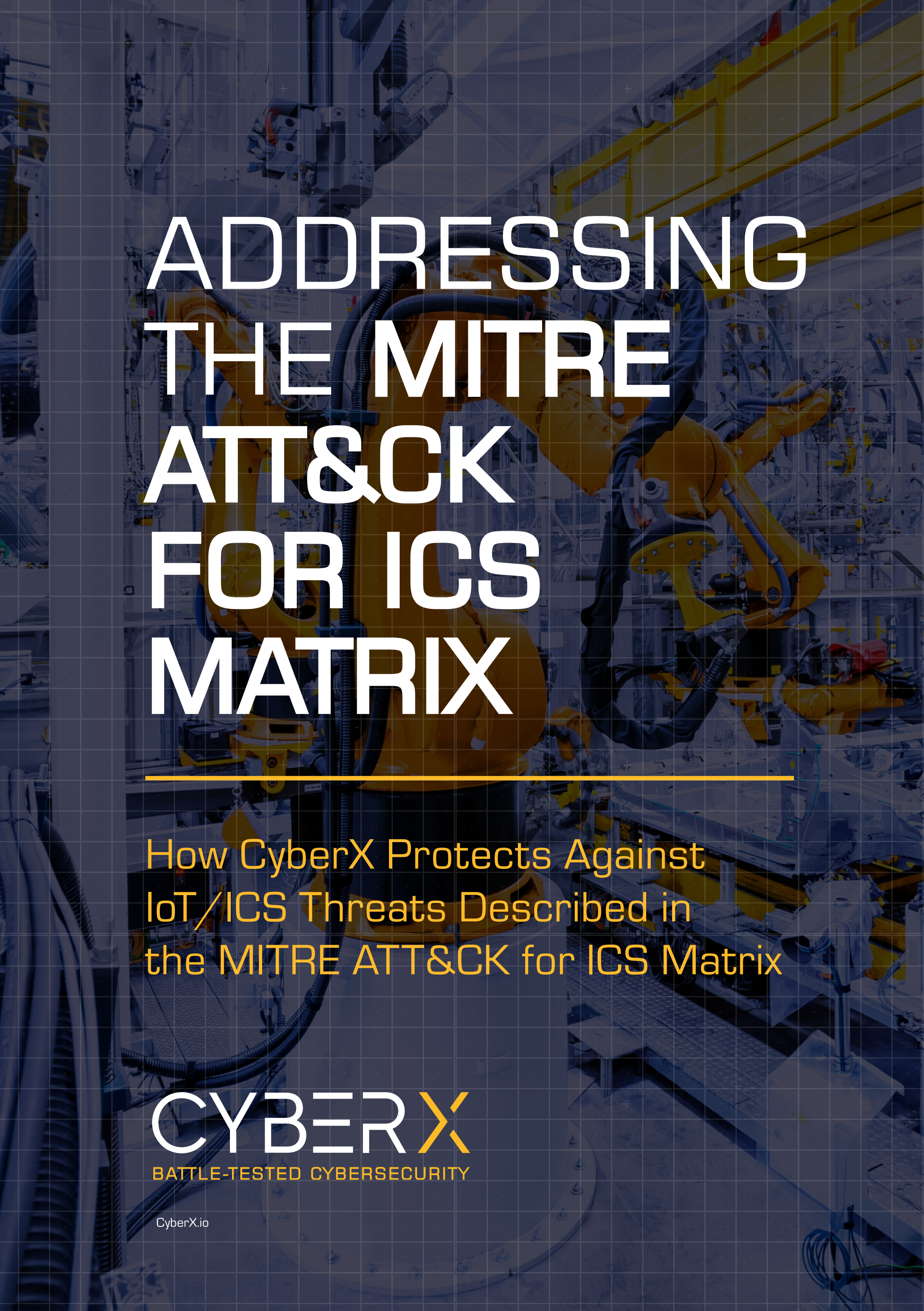


ADDRESSING THE **MITRE ATT&CK FOR ICS MATRIX**

How CyberX Protects Against IoT/ICS Threats Described in the MITRE ATT&CK for ICS Matrix

CYBERX
BATTLE-TESTED CYBERSECURITY

CyberX.io

Table of Contents

1.0

THE MITRE ATT&CK FOR ICS MATRIX

Modern IoT/ICS networks face adversaries that are often more sophisticated than those attacking IT networks. The MITRE ATT&CK for ICS Matrix provides a much-needed knowledge base of threat actor behavior – and as the simplest and most robust IoT/ICS security solution, CyberX's agentless platform is uniquely positioned to address these threats.

1.1 What is the MITRE ATT&CK Framework for ICS?

Many security professionals may already be familiar with the MITRE ATT&CK Framework. The original Framework is a detailed matrix of techniques used by threat actors to penetrate IT systems. While this is a thorough index of threats targeting IT systems, ICS systems are facing a very different set of risks and tactics. What's more, these systems can't be protected by traditional enterprise cybersecurity technologies such as vulnerability scanners (e.g., NESSUS) and agent-based endpoint security.

1.2 Why is the MITRE ATT&CK for ICS Matrix important, even beyond the industrial environment?

High-profile attacks like NotPetya, TRITON, and LockerGoga have proven that IoT/ICS security can have significant impacts on safety, revenue, and brand reputation. But effectively strengthening IoT/ICS security requires a purpose-built IoT/ICS security platform – one that is specifically tailored to the requirements, threats, and restrictions of an IoT/ICS environment.

This is why, in January 2020, MITRE released the MITRE ATT&CK for ICS Matrix: a matrix of tactics that threat actors use to compromise ICS networks. These techniques form an invaluable roadmap of risks that any successful IoT/ICS security platform must address.

While the framework is titled as being "for Industrial Control Systems," it's important to note that these tactics have impacts that reach far beyond ICS environments specifically. Many of the general techniques described in the framework still pose significant risk to any unmanaged device that doesn't fall within the traditional IT environment, including most IoT technology. For example, attackers can download malicious firmware into IoT devices like security cameras in the same way they can use this tactic to compromise PLCs.

The framework is divided into eleven tactics, which describe the steps of an IoT/ICS attack. Within each tactic, MITRE has identified specific techniques that threat actors use to accomplish their goals.

2.0

WHO SHOULD READ THIS DOCUMENT

This document is intended for any security practitioner who intends to use the MITRE ATT&CK for ICS Matrix to strengthen their IoT/OT security posture, or as a reference when initiating or strengthening an IoT/OT security program. This includes CISOs, IoT/OT security analysts, network managers, and other security and IT practitioners.

3.0

WHAT YOU WILL LEARN FROM THIS DOCUMENT

This document is an introduction to the unique ways in which adversaries compromise ICS environments.

It also describes how CyberX addresses every threat actor technique outlined in the MITRE ICS Framework.

4.0

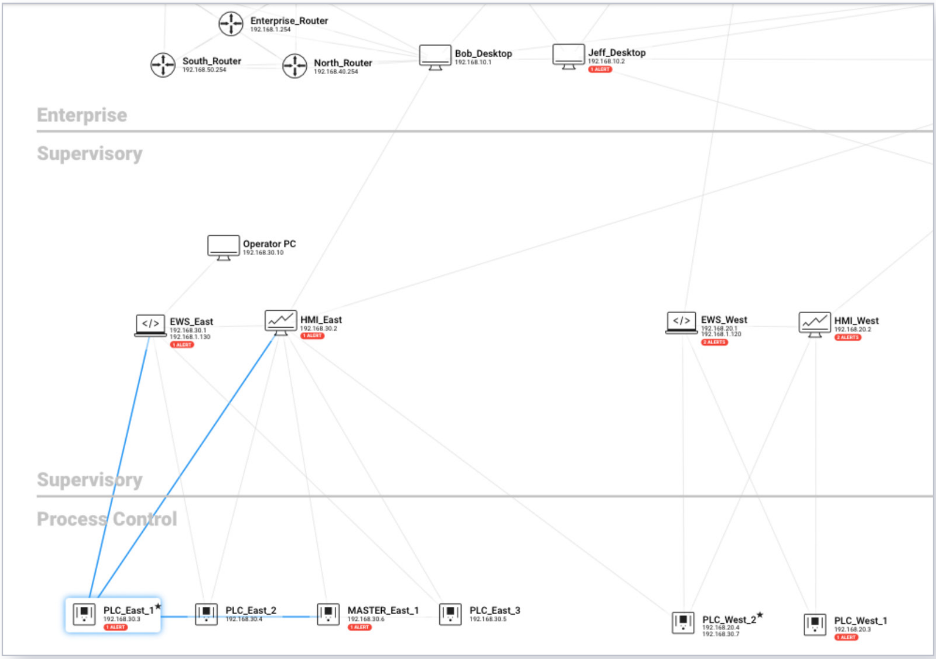
CYBERX VISIBILITY INTO IOT/ICS ASSETS, VULNERABILITIES & THREATS

As the simplest and most robust solution for IoT/ICS security, CyberX's agentless security platform is uniquely positioned to offer effective coverage across every technique in the framework. The platform addresses key challenges including:

IoT/ICS Asset Discovery:

Get immediate visibility into what devices are on your network and how they communicate with each other. This is a key capability when it comes to detecting any form of IoT/ICS threat.

- This asset visibility allows CyberX to immediately detect many MITRE Framework techniques, including examples such as Control Device Identification (T808), Internet Accessible Devices (T883), and Wireless Compromise (T860).



Example of automated asset discovery and network topology mapping

IoT/ICS Risk & Vulnerability Management:

Unlike active vulnerability scanning tools like NESSUS that can disrupt ICS devices, CyberX uses passive monitoring to understand top risks to your "crown jewel" assets and provide the answers you need to prioritize mitigation.

- CyberX gives you a unified view of IoT/ICS risks, including risks that threat actors will exploit in MITRE's techniques such as Default Credentials (T812), Exploitation for Evasion (T820), and Exploitation of Remote Services (T866).

Continuous IoT/ICS threat monitoring & incident response:

CyberX uses a combination of patented, ICS-aware behavioral analytics and proprietary ICS-specific threat intelligence to rapidly detect IoT/ICS threats. The platform also includes an event timeline, contextual alerts, and other sophisticated investigation tools to enable you to quickly respond to alerts.

- This even includes tactics that are often especially difficult to detect, including Alarm Suppression (T878), Serial Connection Enumeration (T854), and Man in the Middle (T830) attacks.

Detection of malfunctioning or misconfigured equipment:

In addition to alerting on cyber threats, CyberX identifies misconfigured or malfunctioning equipment and provides detailed information enabling you to perform root-cause analysis for any issues found.

- CyberX's ability to pinpoint malfunctioning devices also means it can quickly detect threat actor techniques such as Denial of Service (T814), System Firmware (T857), and Project File Injection (T873), as well as incidents that can cause safety issues such as Loss of Control (T827).

5.0

HOW CYBERX IS DIFFERENT

5.1 Fast and easy deployment

CyberX leverages a high degree of built-in automation to deliver granular visibility into assets, vulnerabilities, and threats — within minutes of being connected to the ICS network.

Unlike with other solutions, there's no need to manually configure policies or signatures, have any prior knowledge of the network, or rely on vendor product experts working in the background.

5.2 Choice of on-premises or cloud

Recognizing that sending data to the cloud can be problematic for many industrial and critical infrastructure organizations, CyberX offers a 100% on-premises solution via either physical or virtual appliances.

A cloud-based service is also available for clients monitoring network traffic that is less sensitive, such as traffic associated with BMS systems or generic IoT devices (printers, cameras, etc.).

5.3 Patented ICS-aware behavioral analytics with Layer 7 DPI

The CyberX platform incorporates the industry's only **patented IoT/ICS-aware behavioral analytics,** enabling it to identify threats faster and with more accuracy than generic baselining algorithms. This is because the platform's built-in machine learning has been specifically designed for the deterministic nature of IoT/ICS environments.

Additionally, unlike other solutions that only analyze superficial metadata about network traffic, the CyberX platform performs full Layer 7 deep packet inspection (DPI), enabling it to identify malicious PLC commands (like PLC-STOP commands) as well as malicious or unauthorized applications/services.

5.4 Automated IoT/ICS threat modeling

Unique in the industry, CyberX offers **automated IoT/ICS threat modeling** (attack vector simulation) that identifies and visualizes the most likely paths an attacker would take to compromise your most important assets (your "crown jewels").

This is especially useful for mitigating vulnerabilities an attacker would exploit during the "Initial Access" phase of the MITRE ATT&CK for ICS Matrix. Prioritization mitigation activities is key to a risk-based approach enabling you to make more effective use of limited people resources and narrow maintenance windows.

5.5 IoT/ICS-specific threat intelligence

Section 52, CyberX's threat intelligence team, is composed of world-class domain experts and data scientists who previously staffed a national military CERT defending against daily nation-state cyberattacks.

The team continuously tracks IoT/ICS-specific APT campaigns, malware, and adversaries targeting industrial organizations.

Section 52 uses Ganymede, an **automated, ML-based threat extraction system** and IoT/ICS-specific malware sandbox to collect and analyze data from a range of open and closed sources. The resulting Indicators of Compromise (IoCs) are continuously fed into the CyberX platform to enrich its built-in behavioral analytics.

5.6 Out-of-the-box integration with your existing IT security stack

CyberX provides out-of-the-box, API-level integration with existing IT security stacks — including SIEMs, SOAR, ticketing systems, CMDBs, firewalls and NAC solutions — enabling you to leverage existing SOC workflows, as well as demonstrate a unified IT/OT security monitoring and governance approach to auditors.

Deep integration with IT security tools also enables you to quickly correlate attacks that typically cross IT/OT boundaries.

These integrations include platforms such as Splunk, IBM QRadar, and ServiceNow, as well as firewalls from Palo Alto Networks, Fortinet, and Cisco.

5.7 Unified solution for both IoT and ICS security

CyberX offers a single-pane-of-glass solution for both ICS security (PLCs, HMIs, DCS, historians, etc.) and IoT security (cameras, BMS, printers, routers, Smart TVs, building access control, kiosks, etc.) — thereby reducing complexity and TCO.

5.8 Proven enterprise expertise and maturity

As the longest-standing pure-play provider of IoT/ICS security technology, CyberX has a deep understanding of the specialized protocols, devices, vulnerabilities, and behaviors found in ICS environments.

Deployed in some of the world's largest and most complex IoT/ICS environments, the platform is backed by IoT/ICS security experts with invaluable expertise about the best practices — both technical and organizational — required for successful enterprise-wide deployments.

6.0

HOW CYBERX ADDRESSES ATT&CK FOR ICS

Here are the 11 tactics described in MITRE's ATT&CK for ICS:

The 11 tactics described below are listed across the top column in the table on page 16. Beneath each column header are techniques used by attackers to perform the respective tactic. The techniques listed are not necessarily unique to any one specific tactic.

Tactic Name	Description
Collection	The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal.
Command and Control	The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment.
Discovery	The adversary is trying to figure out your ICS environment.
Evasion	The adversary is trying to avoid being detected.
Execution	The adversary is trying to run malicious code.
Impact	The adversary is trying to manipulate, interrupt, or destroy your ICS systems, data, and their surrounding environment.
Impair Process Control	The adversary is trying to manipulate, disable, or damage physical control processes.
Inhibit Response Function	The adversary is trying to prevent your safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state.
Initial Access	The adversary is trying to get into your ICS environment.
Lateral Movement	The adversary is trying to move through your ICS environment.
Persistence	The adversary is trying to maintain their foothold in your ICS environment.

The original table from MITRE, with a detailed description of each technique, can be found here: **collaborate.mitre.org/attackics/index.php/Main_Page**

The techniques that CyberX detects immediately are in green boxes. The techniques that CyberX can detect after the initial compromise or where CyberX can detect via integration and correlation with other security technologies, such as SIEMs, are in tan boxes.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
🟩 Data Historian Compromise	🟩 Change Program State	⬜ Hooking	⬜ Exploitation for Evasion	🟩 Control Device Identification	🟩 Default Credentials	🟩 Automated Collection	🟩 Commonly Used Port	🟩 Activate Firmware Update Mode	⬜ Brute Force I/O	⬜ Damage to Property
🟩 Drive-by Compromise	⬜ Command-Line Interface	🟩 Module Firmware	🟩 Indicator Removal on Host	🟩 I/O Module Discovery	🟩 Exploitation of Remote Services	⬜ Data from Information Repositories	🟩 Connection Proxy	🟩 Alarm Suppression	🟩 Change Program State	⬜ Denial of Control
⬜ Engineering Workstation Compromise	🟩 Execution through API	🟩 Program Download	🟩 Masquerading	🟩 Network Connection Enumeration	🟩 External Remote Services	🟩 Detect Operating Mode	🟩 Standard Application Layer Protocol	🟩 Block Command Message	🟩 Masquerading	⬜ Denial of View
⬜ Exploit Public-Facing Application	🟩 Graphical User Interface	⬜ Project File Infection	🟩 Rogue Master Device	🟩 Network Service Scanning	🟩 Program Organization Units	🟩 Detect Program State		🟩 Block Reporting Message	🟩 Modify Control Logic	⬜ Loss of Availability
🟩 External Remote Services	🟩 Man in the Middle	🟩 System Firmware	⬜ Rootkit	🟩 Network Sniffing	🟩 Remote File Copy	⬜ I/O Image		⬜ Block Serial COM	🟩 Modify Parameter	⬜ Loss of Control
🟩 Internet Accessible Device	🟩 Program Organization Units	⬜ Valid Accounts	🟩 Spoof Reporting Message	🟩 Remote System Discovery	⬜ Valid Accounts	⬜ Location Identification		🟩 Data Destruction	🟩 Module Firmware	⬜ Loss of Productivity and Revenue
⬜ Replication Through Removable Media	🟩 Project File Infection		🟩 Utilize/Change Operating Mode	🟩 Serial Connection Enumeration		🟩 Monitor Process State		🟩 Denial of Service	🟩 Program Download	⬜ Loss of Safety
⬜ Spear-phishing Attachment	⬜ Scripting					🟩 Point & Tag Identification		🟩 Device Restart/ Shutdown	🟩 Rogue Master Device	⬜ Loss of View
🟩 Supply Chain Compromise	🟩 User Execution					🟩 Program Upload		🟩 Manipulate I/O Image	🟩 Service Stop	🟩 Manipulation of Control
🟩 Wireless Compromise						🟩 Role Identification		🟩 Modify Alarm Settings	⬜ Spoof Reporting Message	🟩 Manipulation of View
						⬜ Screen Capture		🟩 Modify Control Logic	⬜ Unauthorized Command Message	⬜ Theft of Operational Information
								🟩 Program Download		
								⬜ Rootkit		
								🟩 System Firmware		
								🟩 Utilize/Change Operating Mode		

🟩 CyberX detects technique immediately

⬜ CyberX detects technique after the learning period, or detects via integration and correlation with other security technologies such as SIEMs.

Following are a selection of ATT&CK tactics along with a description of how CyberX detects and/or responds to the presence of that particular tactic.

6.1 Initial Access

ATT&CK Tactic	Initial Access
T810: Data Historian Compromise	CyberX's patented IoT/ICS-aware behavioral analytics engines identify abnormal traffic, communication, and machine behavior that indicates a threat actor is trying to compromise — or has already compromised — the Data Historian, a critical component of any ICS environment.
T817: Drive-by Compromise	CyberX's threat intelligence feeds are continuously updated by Section 52, CyberX's threat intelligence team. These feeds identify known-malicious destinations and malware IOCs. CyberX alerts when a device attempts to communicate with these sites, or when a connection exhibits known IOCs. CyberX also alerts on any "new" connection outside of that device's baseline.
T818: Engineering Workstation Compromise	CyberX's patented behavioral analytics identify any unusual behavior from an Engineering Workstation, such as communication using unusual protocols or communication with unexpected devices. This behavior may indicate that this cyber-physical network asset (PLC, HMI, sensor, or actuator) has been compromised.
T819: Exploit Public-Facing Application	CyberX continuously monitors systems hosting public-facing applications to detect vulnerabilities that would allow a threat actor to cross into the ICS environment — ensuring that public-facing systems can't be exploited to get to the ICS networks. Section 52 reported one such vulnerability for a GE CIMPLICITY system: us-cert.gov/ics/advisories/ICSA-17-278-01A CyberX also detects abusive connections that indicate attempts to exploit public-facing applications, such as brute force attacks.
T822: External Remote Services	CyberX passively monitors device communications, identifying all active ports, services, and protocols. CyberX alerts whenever it observes a device utilizing unauthorized services, or when it observes abnormal new connections for an unknown source. In addition, CyberX alerts when it detects an inbound connection from the internet.

ATT&CK Tactic	Initial Access
T883: Internet Accessible Device	CyberX alerts on devices that have a connection to the internet.
T847: Replication Through Removable Media	CyberX's behavioral analytics engines detect malware that is transferred via removable media. CyberX alerts on both preliminary indicators that malware is active, as well as any malicious activity that takes place as a result of malware attempting to communicate to the network from the infected host.
T865: Spear-phishing Attachment	CyberX detects and alerts on attempts to access malicious command and control servers. It will also detect malicious network behavior caused by malware packaged in a spear-phishing attack. Section 52, CyberX's threat intelligence team, also provides early warnings against spear-phishing campaigns.
T862: Supply Chain Compromise	CyberX passively monitors all device-to-device communications – at all network layers, and in all production segments. Using patented IoT/ICS-aware behavioral analytics, CyberX baselines "known good activity" and alerts on suspicious anomalies that indicate potential supply chain compromise.
T860: Wireless Compromise	CyberX automatically discovers the wired and wireless infrastructure of an ICS environment, and will alert on unauthorized devices that connect to the network or perform malicious wireless activity.

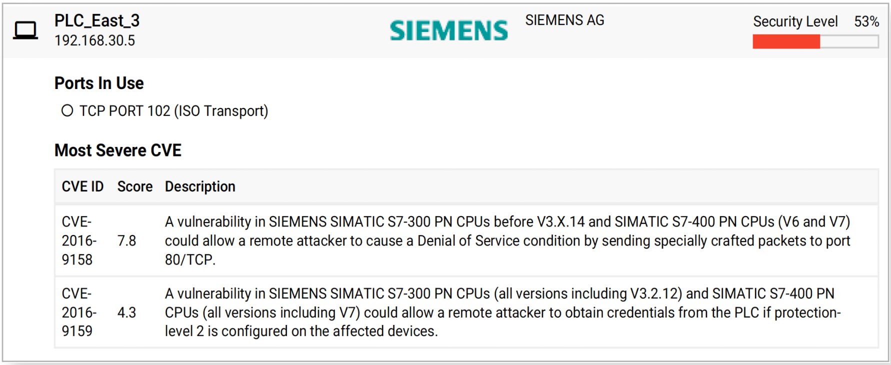
6.2 Execution

ATT&CK Tactic	Execution
T875: Change Program State	CyberX monitors the state of a control device and will identify when it is sent commands that alter its state (such as a STOP command or any other specific protocol command). In addition, CyberX alerts on any communication that violates ICS protocol specifications — detecting when threat actors try to embed their code into a PLC or exploit protocol vulnerabilities, for example.
T807: Command-Line Interface	CyberX monitors what devices are allowed to communicate to a PLC via SSH, Telnet and RDP. These protocols are likely to be used by attackers who are attempting to access ICS environments via the command-line interface. CyberX can alert on unusual activity and excessive brute force connection attempts that are outside the baseline — for example, when remote access is observed for the first time.
T871: Execution through API	CyberX alerts on unusual API activity, and will include the source address of the API call if it is outside of baseline behavior.
T823: Graphical User Interface	CyberX monitors device-to-device communication patterns as well as protocols like VNC and RDP, which are typically used to access Graphical User interfaces. CyberX detects abnormal traffic to GUI machines, which can indicate that a threat actor is attempting to access a GUI. In addition, CyberX also detects exploit attempts on RDP such as BlueKeep and DejaBlue.
T830: Man in the Middle	CyberX monitors all device communications. This includes network traffic characteristics such as ARP traffic, TCP options, and abnormal TCP resets. Studying this traffic with patented behavioral analytics allows CyberX to detect anomalies that indicate a Man-in-the-Middle attack. In addition, CyberX's unique protocol violation analytics engine detects network traffic that does not adhere to ICS protocol specifications — another potential indication of a Man-in-the-Middle attack.
T844: Program Organization Units	CyberX detects and alerts on a wide range of PLC-specific network traffic and programming downloads. These include the commands related to changing the program on a device. CyberX can also show the before/after differences when new programming code is transmitted over the network.

ATT&CK Tactic	Execution
T873: Project File Infection	CyberX detects when a PLC has been reprogrammed and alert on that activity. In addition, CyberX alerts if the device is programmed from an unauthorized device.
T853: Scripting	CyberX's patented behavioral analytics detect all anomalous or unauthorized behavior. If a malicious script is used to attack or alter a device, CyberX alerts on this behavior. CyberX also tracks all programming events in the environment.
T863: User Execution	CyberX detects and alerts on abnormal system behavior that indicates compromise via user execution, including activity such as PLC resets and configuration changes.

6.3 Persistence

ATT&CK Tactic	Persistence
T874: Hooking	CyberX's monitoring and patented IoT/ICS-aware analytics allow it to detect when a system has been compromised. CyberX would first alert on the programming change that occurred, and then alert on the Hooking, which establishes an illegal function call outside of the ICS protocol specification. Another alert is generated if the redirected API calls across the network show the system acting abnormally, outside the normal baseline of activity.
T839: Module Firmware	CyberX detects and alerts when firmware is downloaded to PLCs. In addition, CyberX's analytics will alert if this new firmware causes the PLC behavior to change outside of its baseline activity. CyberX also depicts an index of all firmware versions on every device, as well as a visual timeline of any firmware changes that have taken place on the network.
T843: Program Download	CyberX detects program downloads to PLCs, and will alert if the new program causes abnormal PLC behavior.
T873: Project File Infection	CyberX detects when a PLC has been reprogrammed. If that device changes in behavior from its normal baseline or attempts to contact any malicious domains, then CyberX will alert on that activity as well.
T857: System Firmware	CyberX's monitoring capabilities can determine the current version of system firmware on each device. Based on this information, CyberX identifies known threat CVEs to the firmware and and generates a risk report with risk scoring so customers can manage their upgrade and/or patching strategy. CyberX also can detect when a PLC firmware has been changed by either an authorized or unauthorized device, and alert on that activity.
T859: Valid Accounts	CyberX's patented behavioral analytics detect abnormal account behavior, such as the behavior changes that would be a result of a threat actor taking over a valid account. CyberX will also alert on abnormal network connections. All of this activity is also logged in a complete audit trail for forensic investigation, as well as fed into any SIEM such as Splunk or IBM QRadar.



PLC_East_3
192.168.30.5

SIEMENS AG

Security Level 53%

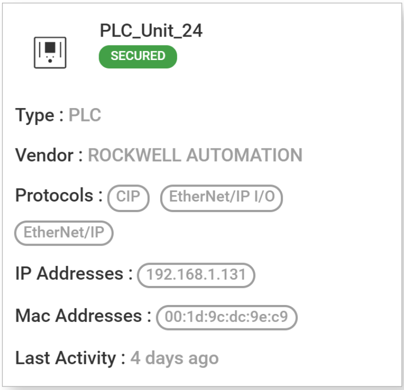
Ports In Use

○ TCP PORT 102 (ISO Transport)

Most Severe CVE

CVE ID	Score	Description
CVE-2016-9158	7.8	A vulnerability in SIEMENS SIMATIC S7-300 PN CPUs before V3.X.14 and SIMATIC S7-400 PN CPUs (V6 and V7) could allow a remote attacker to cause a Denial of Service condition by sending specially crafted packets to port 80/TCP.
CVE-2016-9159	4.3	A vulnerability in SIEMENS SIMATIC S7-300 PN CPUs (all versions including V3.2.12) and SIMATIC S7-400 PN CPUs (all versions including V7) could allow a remote attacker to obtain credentials from the PLC if protection-level 2 is configured on the affected devices.

Known vulnerabilities (CVEs) for a Siemens PLC (embedded device). The Industroyer/CrashOverride grid attack exploited a similar Denial-of-Service (DoS) vulnerability in Siemens relays.



PLC_Unit_24
SECURED

Type : PLC

Vendor : ROCKWELL AUTOMATION

Protocols : CIP EtherNet/IP I/O EtherNet/IP

IP Addresses : 192.168.1.131

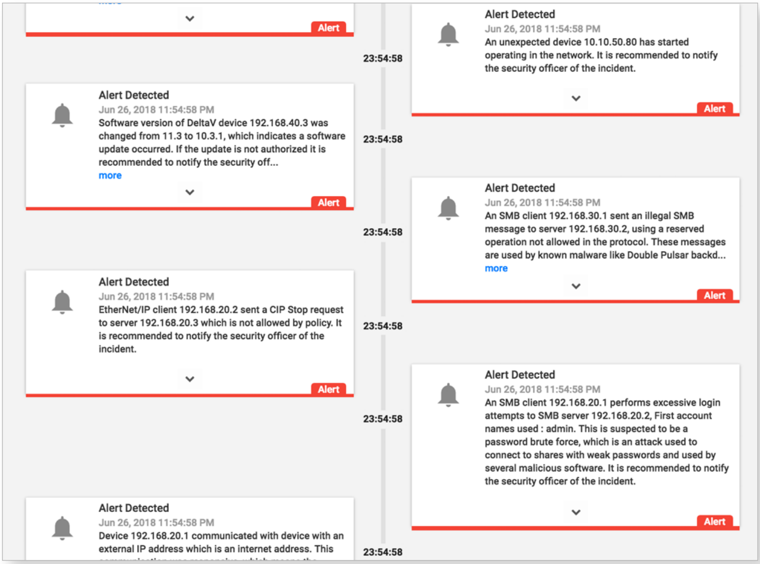
Mac Addresses : 00:1d:9c:dc:9e:c9

Last Activity : 4 days ago

Detailed device information obtained by right-clicking on network topology map.

6.4 Evasion

ATT&CK Tactic	Evasion
T820: Exploitation for Evasion	CyberX detects and alerts on behavioral changes indicating that a device has been exploited for evasion. CyberX's event timeline provides a forensic audit trail, which is invaluable in diagnosing and mitigating potential exploitations. CyberX also proactively identifies software vulnerabilities, enabling organizations to quickly remediate vulnerable devices, isolate these devices, and mitigate risks before they can be exploited.
T872: Indicator Removal on Host	CyberX provides a complete, unaltered history of all network activity and device behavior. If a threat actor attempts to remove log files or otherwise cover their tracks, CyberX offers a forensically sound audit trail that cannot be altered and tracks their attempts at obfuscation.
T849: Masquerading	CyberX continuously monitors the behavior of every device to detect and alert on abnormal behavior by passively listening to the activity of these devices "out of band." Specifically, CyberX monitors the behavior of the device, not the files executed on the system. This visibility cuts through attackers' masquerading techniques.
T848: Rogue Master Device	CyberX detects and alerts when a device communicates with a rogue master device, as well as discovers all new devices that were not previously authorized to be active in the network. If a device communicates with a rogue master device, CyberX can alert on this activity as well as discover devices which were previously not authorized to be active in the network.
T851: Rootkit	CyberX immediately identifies abnormal behavior indicating a potential rootkit. If a threat actor is attempting to install a rootkit on a PLC, CyberX detects when the configuration and firmware have been altered and alert on this activity.
T856: Spoof Reporting Message	CyberX detects abnormal message traffic which may indicate message spoofing.
T858: Utilize/ Change Operating Mode	CyberX monitors and alerts on PLC mode changes. CyberX's patented M2M behavioral analytics recognizes any unexpected anomalies within the ICS system, including those pertaining to operating nodes.



Alert

23:54:58

Alert Detected
Jun 26, 2018 11:54:58 PM
An unexpected device 10.10.50.80 has started operating in the network. It is recommended to notify the security officer of the incident.

Alert

23:54:58

Alert Detected
Jun 26, 2018 11:54:58 PM
Software version of DeltaV device 192.168.40.3 was changed from 11.3 to 10.3.1, which indicates a software update occurred. If the update is not authorized it is recommended to notify the security off...
more

Alert

23:54:58

Alert Detected
Jun 26, 2018 11:54:58 PM
An SMB client 192.168.30.1 sent an illegal SMB message to server 192.168.30.2, using a reserved operation not allowed in the protocol. These messages are used by known malware like Double Pulsar backd...
more

Alert

23:54:58

Alert Detected
Jun 26, 2018 11:54:58 PM
EtherNet/IP client 192.168.20.2 sent a CIP Stop request to server 192.168.20.3 which is not allowed by policy. It is recommended to notify the security officer of the incident.

Alert

23:54:58

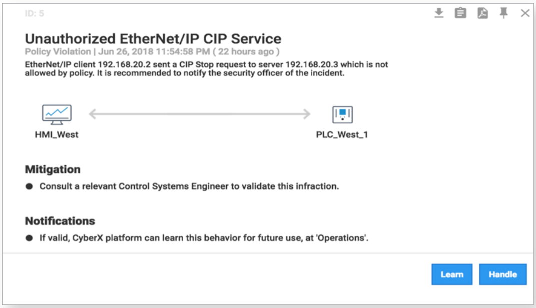
Alert Detected
Jun 26, 2018 11:54:58 PM
An SMB client 192.168.20.1 performs excessive login attempts to SMB server 192.168.20.2, First account names used : admin. This is suspected to be a password brute force, which is an attack used to connect to shares with weak passwords and used by several malicious software. It is recommended to notify the security officer of the incident.

Alert

23:54:58

Alert Detected
Jun 26, 2018 11:54:58 PM
Device 192.168.20.1 communicated with device with an external IP address which is an internet address. This

Incident responders use the Event Timeline to quickly investigate incidents.



ID: 5

Unauthorized EtherNet/IP CIP Service
Policy Violation | Jun 26, 2018 11:54:58 PM (22 hours ago)
EtherNet/IP client 192.168.20.2 sent a CIP Stop request to server 192.168.20.3 which is not allowed by policy. It is recommended to notify the security officer of the incident.

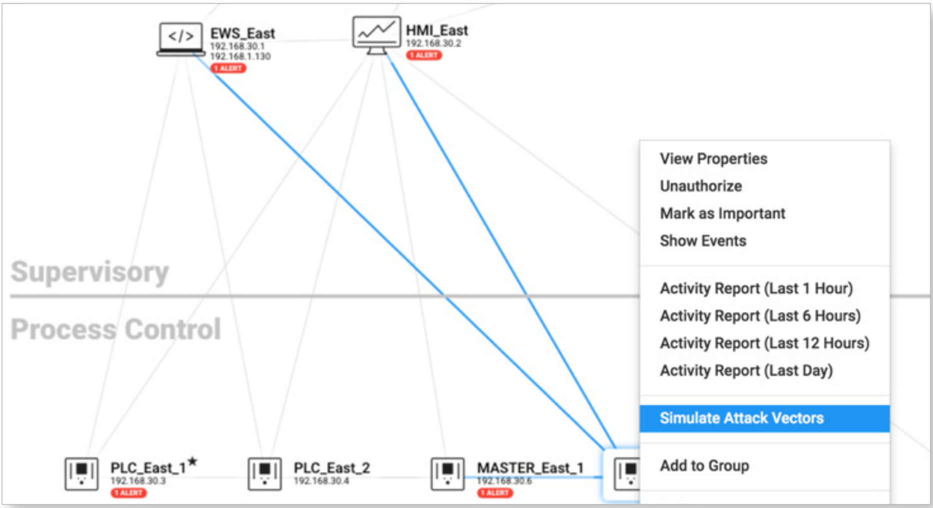
Mitigation
- Consult a relevant Control Systems Engineer to validate this infraction.

Notifications
- If valid, CyberX platform can learn this behavior for future use, at 'Operations'.

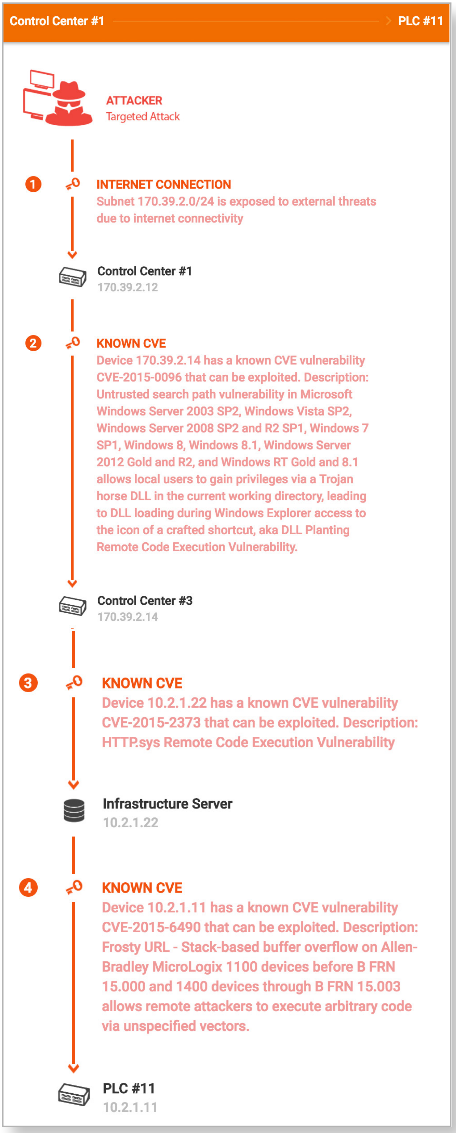
Example of contextual alert showing identification of unauthorized activity at the application layer.

6.5 Discovery

ATT&CK Tactic	Discovery
T808: Control Device Identification	CyberX detects port scans, abnormal network traffic, and device API requests coming from non-engineering workstations, which may indicate an attempt at conducting control device identification by a threat actor.
T824: I/O Module Discovery	CyberX's deep packet inspection monitors protocol functions and identifies backplane modules within ICS systems, which includes functions to enumerate I/O modules that are connected to the device. CyberX will also monitor network traffic and will detect when a threat actor attempts to conduct input/output discovery.
T840: Network Connection Enumeration	CyberX monitors all device communications and will alert on unauthorized network scans, high connection rates, and many other indicators of network connection enumeration.
T841: Network Service Scanning	CyberX alerts on a device port scanning to identify network services, and identifies any devices attempting to scan the network.
T842: Network Sniffing	CyberX will identify and alert when data is exfiltrated from the network via network sniffing, as well as when data is exfiltrated to the internet.
T846: Remote System Discovery	CyberX will identify threat actors' attempts to perform remote system discovery, such as port scanning from tools such as Nmap. This activity is detected as unauthorized or abnormal network traffic, and alerted upon immediately.
T854: Serial Connection Enumeration	Because CyberX identifies all unauthorized or abnormal network behavior, it will alert when a threat actor queries a device for its serial connection information over the network.



The first step in threat modeling is identifying your "crown jewel" assets. These are the assets whose compromise would have a major impact on your organization, such as by taking down production for a major revenue-generating product or causing a major safety incident.



Control Center #1 > PLC #11

ATTACKER
Targeted Attack

1 INTERNET CONNECTION
Subnet 170.39.2.0/24 is exposed to external threats due to internet connectivity

Control Center #1
170.39.2.12

2 KNOWN CVE
Device 170.39.2.14 has a known CVE vulnerability CVE-2015-0096 that can be exploited. Description: Untrusted search path vulnerability in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, leading to DLL loading during Windows Explorer access to the icon of a crafted shortcut, aka DLL Planting Remote Code Execution Vulnerability.

Control Center #3
170.39.2.14

3 KNOWN CVE
Device 10.2.1.22 has a known CVE vulnerability CVE-2015-2373 that can be exploited. Description: HTTP.sys Remote Code Execution Vulnerability

Infrastructure Server
10.2.1.22

4 KNOWN CVE
Device 10.2.1.11 has a known CVE vulnerability CVE-2015-6490 that can be exploited. Description: Frosty URL - Stack-based buffer overflow on Allen-Bradley MicroLogix 1100 devices before B FRN 15.000 and 1400 devices through B FRN 15.003 allows remote attackers to execute arbitrary code via unspecified vectors.

PLC #11
10.2.1.11

Once you've identified your "crown jewel" assets, use automated threat modeling to identify the most likely paths an attacker would take to compromise them. In this example, the targeted device (PLC #11) controls a major revenue-generating production line or a physical process whose compromise could cause a major safety or environmental incident.

This is also an example of lateral movement as described in Section 6.6.

6.6 Lateral Movement

ATT&CK Tactic	Lateral Movement
T812: Default Credentials	CyberX's visibility into network traffic will identify devices and the credentials they are using. In addition, CyberX monitors device connections to determine whether other devices are using these credentials, indicating potential default credentials.
T866: Exploitation of Remote Services	CyberX detects when a device uses remote services, and will identify if these services are used in an unusual or anomalous manner that could indicate lateral movement to infect other devices.
T822: External Remote Services	CyberX profiles the activity of each device, including the external remote services that are used. CyberX will alert if an external remote service comes from the internet. In addition, CyberX can identify any other abnormal or suspicious behavior from these services.
T844: Program Organization Units	CyberX detects and alerts when a PLC download or reprogramming occurs, as well as provide a review of the specific program changes.
T867: Remote File Copy	CyberX detects when a system is remotely copying files, as well as when excessive bandwidth is used on the network.
T859: Valid Accounts	CyberX's network monitoring and patented behavioral anomaly detection analytics engine detects when an unusual number of network connections are made. This can indicate that an adversary is using valid accounts to conduct lateral movement outside of the normal behavior for the legitimate account holder devices.

6.7 Collection

ATT&CK Tactic	Collection
T802: Automated Collection	CyberX will identify and alert on the use of tools or scripts used by threat actors for automated collection. CyberX alerts on all unusual network activity, including OPC protocol activity and other types of programming/scanning.
T811: Data from Information Repositories	When a threat actor attempts to connect to information repositories, CyberX will alert on these unauthorized or unusual connection attempts – such as abnormal MySQL connections, for example.
T868: Detect Operating Mode	CyberX identifies and alerts on PLC-specific commands, including those related to the PLC status (such as Start and Stop, for example).
T870: Detect Program State	CyberX identifies and alerts on PLC-specific commands, including those related to the PLC state.
T877: I/O Image	CyberX identifies and alerts on authorized or unauthorized connections to ICS devices which would be utilized to extract I/O images.
T825: Location Identification	CyberX identifies and alerts on authorized or unauthorized connections to ICS and ICS network infrastructure devices. These could be used to identify the device location.
T801: Monitor Process State	CyberX identifies and alerts on unauthorized connections to ICS devices which could be used to detect the device process state. In addition, CyberX alerts on process states that have not been authorized.
T861: Point & Tag Identification	CyberX identifies and alerts on network traffic that would be generated by threat actors querying devices for their point and tag information.
T845: Program Upload	CyberX monitors device communications and can alert whenever unauthorized program upload occurs, including presentation showing the specifics of the reprogramming that were performed.

ATT&CK Tactic	Collection
T850: Role Identification	CyberX monitors device communications and can be configured to alert when unusual connections are made to the network in an attempt to conduct reconnaissance for role identification, such as master or outstation devices.
T852: Screen Capture	CyberX identifies unauthorized remote connections such as RDP and VNC, which can be used on HMI systems to capture screen images of control system processes. CyberX can also identify unauthorized file transfers, such as when a device is attempting to exfiltrate a screen capture.

6.8 Command and Control

ATT&CK Tactic	Command and Control
T885: Commonly Used Port	CyberX's anomaly detection will identify when a commonly used port is being utilized outside of that port's protocol specification.
T884: Connection Proxy	CyberX monitors device communications and can alert (or and automatically block communications, via integration with firewall rules) when a device tries to connect to any malicious site on the internet, or if it uses an unauthorized connection proxy.
T869: Standard Application Layer Protocol	If a threat actor attempts to establish command and control over commonly used protocols, CyberX will identify and alert on this unusual behavior, which violates the normal baseline activity within the control system environment.

6.9 Inhibit Response Function

ATT&CK Tactic	Inhibit Response Function
T800: Activate Firmware Update Mode	CyberX monitors and alerts on PLC specific commands, including those relating to firmware loads or updates.
T878: Alarm Suppression	CyberX monitors and alerts on PLC alterations changes or behavior outside of normal operations, which may indicate that an adversary is attempting to suppress the device alarm. CyberX can also alert on custom values in industrial protocols independent of the monitored system.
T803: Block Command Message	CyberX monitors and alerts on PLC alterations changes or behavior outside of normal operations, which may indicate that an adversary is attempting to block command messages. In addition, CyberX alerts on a device being unresponsive to another device in the process control network.
T804: Block Reporting Message	CyberX monitors and alerts on PLC alterations changes or behavior outside of normal operations, which may indicate that an adversary is attempting to block reporting messages. In addition, CyberX alerts on a device being unresponsive to another device in the process control network.
T805: Block Serial COM	CyberX identifies and alerts on an unusual amount of connections to a serial to ethernet converter, which could indicate an attempt to Block Serial COM connections.
T809: Data Destruction	CyberX identifies and alerts on abnormal network traffic associated with data destruction commands, such as drop table or delete, within a data historian.
T814: Denial of Service	CyberX is able to detect denial of service attacks launched via a number of methods, including ping sweeps, high connection rates, excessive bandwidth and other indicators and techniques. CyberX's alert threshold for these events can also be customized.

ATT&CK Tactic	Inhibit Response Function
T816: Device Restart/ Shutdown	CyberX's deep packet inspection and monitoring identifies commands to shut down and restart a device. This includes PLC Stop and DNP3 Reset, as well as many others.
T835: Manipulate I/O Image	CyberX's deep packet inspection of ICS protocols detects when a PLC has been altered via authorized or unauthorized commands. This allows CyberX to detect when a threat actor may be attempting to manipulate the device I/O image.
T838: Modify Alarm Settings	CyberX will identify any modification in PLC commands or programming that may be used by a threat actor to modify alarm settings.
T833: Modify Control Logic	CyberX will identify any PLC modification used by a threat actor to modify control logic.
T843: Program Download	CyberX detects PLC modifications from authorized or unauthorized devices, which a threat actor may use to modify the program running in the PLC.
T851: Rootkit	CyberX immediately identifies abnormal behavior indicating a potential rootkit. If a threat actor is attempting to install a rootkit on a PLC, CyberX will detect when the configuration and firmware have been altered and alert on this activity.
T857: System Firmware	CyberX alerts on a wide variety of PLC commands, including updates or changes to the device firmware.
T858: Utilize/ Change Operating Mode	CyberX alerts on a wide variety of PLC commands, including those that change the device operating mode.

6.10 Impair Process Control

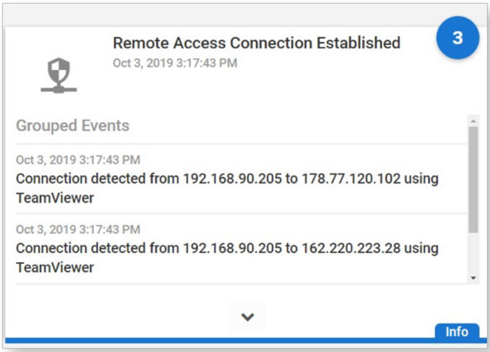
ATT&CK Tactic	Impair Process Control
T806: Brute Force I/O	CyberX's visibility and analytics identify abnormal network traffic, which includes I/O activity indicating a potential brute force I/O attack.
T875: Change Program State	CyberX monitors the state of a control device and will identify any state-alerting commands sent to a PLC.
T849: Masquerading	CyberX continuously monitors the behavior of every device to detect and alert on abnormal behavior by passively listening to the activity of these devices "out of band." Specifically, CyberX monitors the behavior of the device, not the files executed on the system. This visibility cuts through attackers' masquerading techniques.
T833: Modify Control Logic	CyberX identifies any PLC modification which may be used by an adversary to modify the control logic.
T836: Modify Parameter	CyberX alerts on a number of PLC commands. This includes configure commands, which change device configuration.
T839: Module Firmware	CyberX detects and alerts when firmware is downloaded to PLCs. In addition, CyberX's analytics will alert if this new firmware causes the PLC behavior to change outside of its baseline activity. CyberX also depicts provides an index of all firmware versions on every device, as well as a visual timeline of any firmware changes that have taken place on the network.
T843: Program Download	CyberX detects PLC modification from authorized or unauthorized devices, which includes program downloads onto a certain PLC.
T848: Rogue Master Device	CyberX alerts when a device communicates with a rogue master device, as well as discovers all new devices that were not previously authorized to be active in the network.

ATT&CK Tactic	Execution
T881: Service Stop	CyberX detects and alerts on a number of PLC commands. This includes "STOP" commands, which are used to stop device services.
T856: Spoof Reporting Message	CyberX detects abnormal message traffic, which may indicate report message spoofing.
T855: Unauthorized Command Message	CyberX will identify and alert if command messages are transmitted by unauthorized devices.

6.11 Impact

ATT&CK Tactic	Impact
T879: Damage to Property	CyberX identifies vulnerabilities and risks in the ICS environment which allows customers to take proactive steps to mitigate risks. By proactively remediating the issues found to prevent a successful attack, it can prevent damage to property. If devices begin to act outside of their normal baseline of activity, alerts will be generated, and if acted upon in a timely manner, this can prevent any damage to property.
T813: Denial of Control	CyberX indentifies and alerts on the device messages required to prevent ICS devices from attempting to communicate with its controllers. CyberX also monitors device polling periods and will alert if the devices don't maintain the same interval of communications.
T815: Denial of View	CyberX alerts where there is a communication failure between a device and its control source. In addition, CyberX's passive network monitoring identifies when a device has last appeared on the network.
T826: Loss of Availability	CyberX's network monitoring, behavioral baselining, vulnerability & risk assessments, and asset discovery benefits enable organizations to secure their IoT/ICS networks, detect and prevent any malicious attackers, and quickly diagnose any malicious attempts to disrupt operations.
T827: Loss of Control	CyberX's network monitoring, behavioral baselining, vulnerability & risk assessments, and asset discovery benefits enable organizations both to proactively secure their IoT/ICS networks, and, in the face of an attack, immediately detect and mitigate any malicious attempts to commandeer control.
T828: Loss of Productivity and Revenue	CyberX's network monitoring, behavioral baselining, vulnerability & risk assessments, and asset discovery benefits enable organizations to secure their IoT/ICS networks, detect any attempts to harm productivity, and quickly diagnose costly downtime.
T880: Loss of Safety	CyberX's network monitoring, behavioral baselining, vulnerability & risk assessments, and asset discovery benefits enable organizations to secure their IoT/ICS networks and detect malicious attacks. The result is the early detection and mitigation of any attempts to endanger lives.

ATT&CK Tactic	Impact
T829: Loss of View	CyberX provides detailed information on each asset. This includes information such as when the asset was last seen on the network, other device connections, the asset's last risk score, and mitigation steps to improve risk score. With this data and context, organizations can prioritize restoration activities to prevent a loss of view to the ICS environment.
T831: Manipulation of Control	CyberX identifies and alerts on changes in values, tags, or other parameters that threat actors will attempt to manipulate.
T832: Manipulation of View	CyberX provides detailed information on each asset and changes to that asset. This includes information such as when the asset was last seen on the network, other device connections, the asset's last risk score, and mitigation steps to improve risk score.
T882: Theft of Operational Information	CyberX's combination of monitoring and analytics enable the detection of data theft. CyberX alerts when an unauthorized device connects to the network, and upon the detection of anomalies that indicate data exfiltration (such as bandwidth spikes, or network assets creating connections to new hosts).



Remote Access Connection Established

Oct 3, 2019 3:17:43 PM

Grouped Events

Oct 3, 2019 3:17:43 PM
Connection detected from 192.168.90.205 to 178.77.120.102 using TeamViewer

Oct 3, 2019 3:17:43 PM
Connection detected from 192.168.90.205 to 162.220.223.28 using TeamViewer

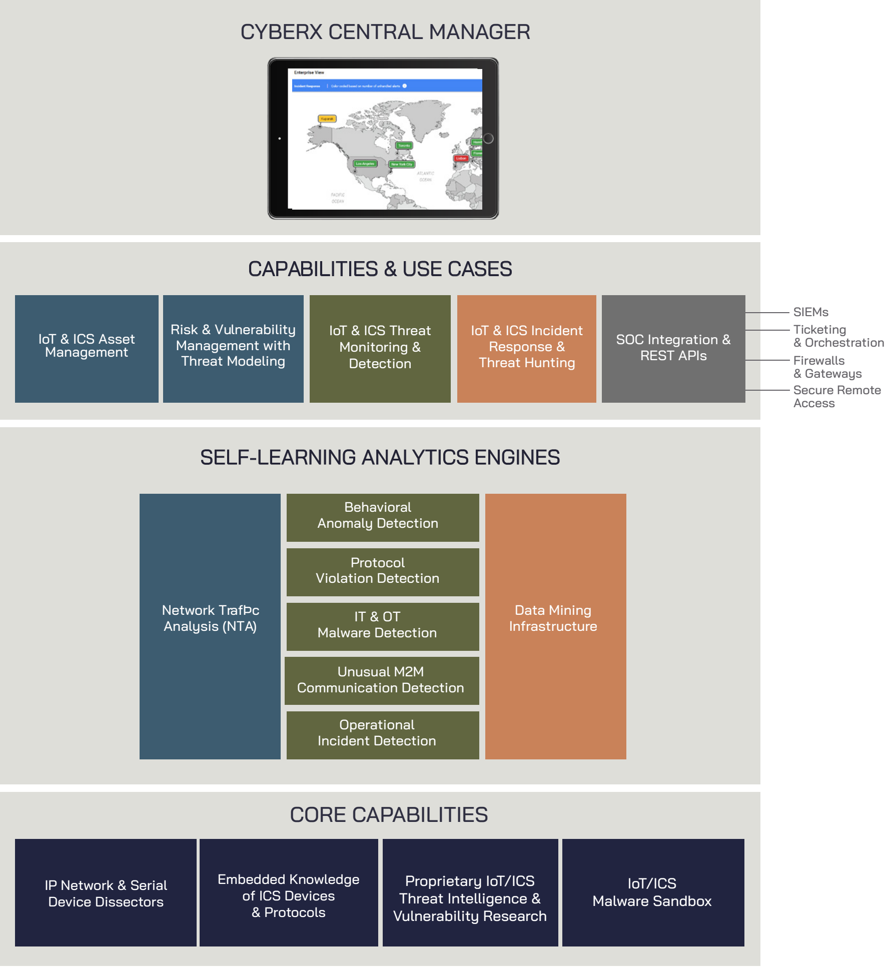
Alert message indicating the establishment of a remote access connection, which may or may not be authorized.

7.0

CYBERX ARCHITECTURE

5 Distinct Analytics Engines To Detect Anomalies Faster — With Fewer False Positives

Sophisticated attacks typically use multiple techniques to compromise OT networks, easily bypassing first-generation systems that look at baseline variations alone. That’s why CyberX identifies unusual or unauthorized behavior via five distinct analytics engines, while self-learning eliminates the need for configuring rules or signatures, specialized skills, or prior knowledge of the OT environment.



CYBERX CENTRAL MANAGER

CAPABILITIES & USE CASES

IoT & ICS Asset Management

Risk & Vulnerability Management with Threat Modeling

IoT & ICS Threat Monitoring & Detection

IoT & ICS Incident Response & Threat Hunting

SOC Integration & REST APIs

- SIEMs
- Ticketing & Orchestration
- Firewalls & Gateways
- Secure Remote Access

SELF-LEARNING ANALYTICS ENGINES

Network Traffic Analysis (NTA)

Behavioral Anomaly Detection

Protocol Violation Detection

IT & OT Malware Detection

Unusual M2M Communication Detection

Operational Incident Detection

Data Mining Infrastructure

CORE CAPABILITIES

IP Network & Serial Device Dissectors

Embedded Knowledge of ICS Devices & Protocols

Proprietary IoT/ICS Threat Intelligence & Vulnerability Research

IoT/ICS Malware Sandbox

Behavioral Anomalies

CyberX uses an innovative, patented technology called Industrial Finite State Modeling (IFSM) to quickly spot baseline deviations by modeling ICS networks as deterministic sequences of states and transitions.

Protocol Violations

Indicating the use of packet structures and field values that violate ICS protocol specifications as defined by ICS vendors. These indicate potential misuse of the ICS protocol to exploit device or network vulnerabilities.

Industrial Malware

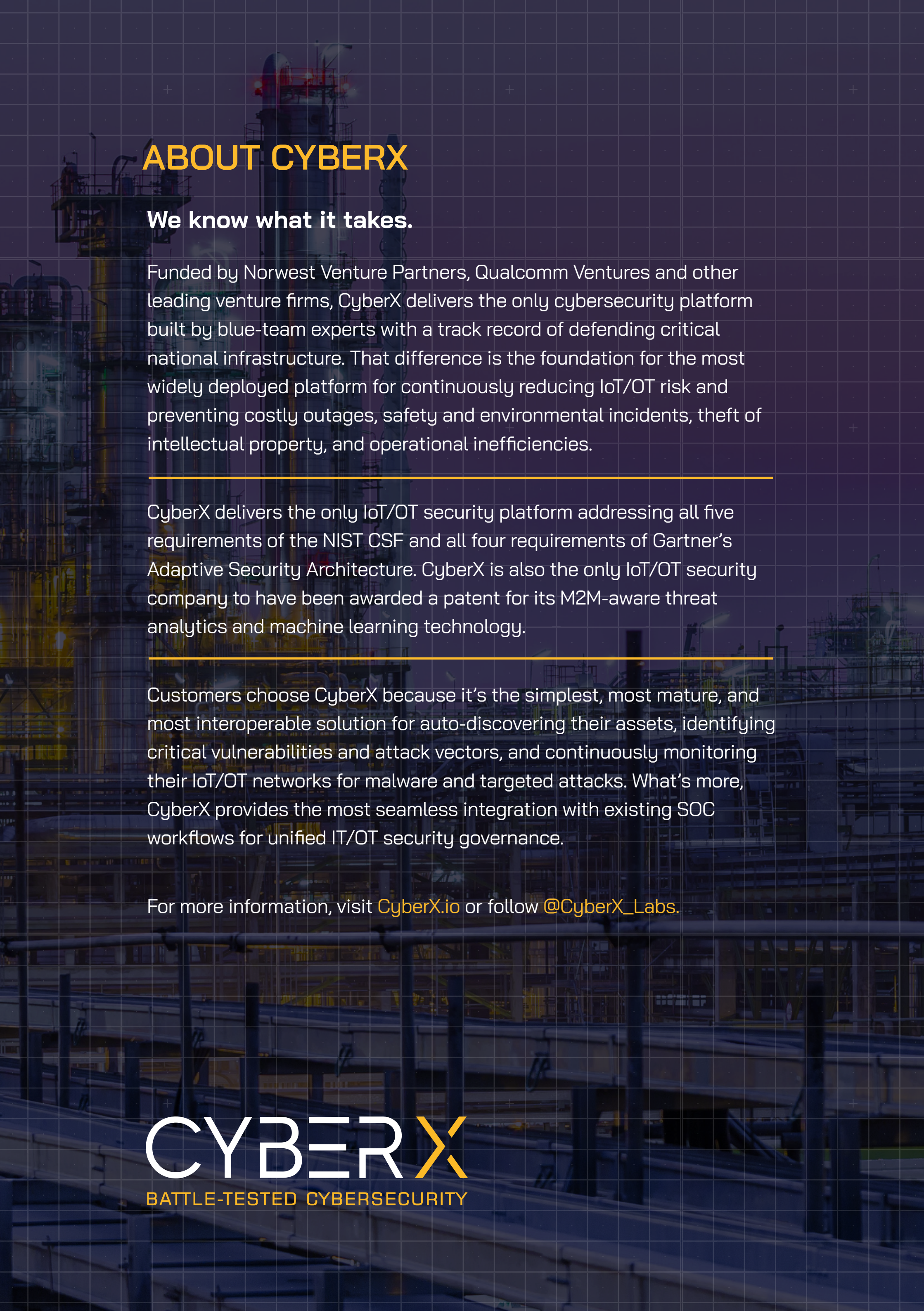
Behaviors indicating the presence of known malware such as WannaCry and NotPetya as well as purpose-built IoT and ICS malware such as TRITON and Industroyer.

Unusual Machine-To-Machine (M2M) Communications

Identified via ICS-aware heuristics such as PLCs should not typically be communicating with other PLCs.

Operational Issues

Such as intermittent connectivity indicating early signs of equipment failure.



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.

CyberX delivers the only IoT/OT 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 IoT/OT security company to have been awarded a patent for its M2M-aware threat analytics and machine learning technology.

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 IoT/OT 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.

CYBERX
BATTLE-TESTED CYBERSECURITY