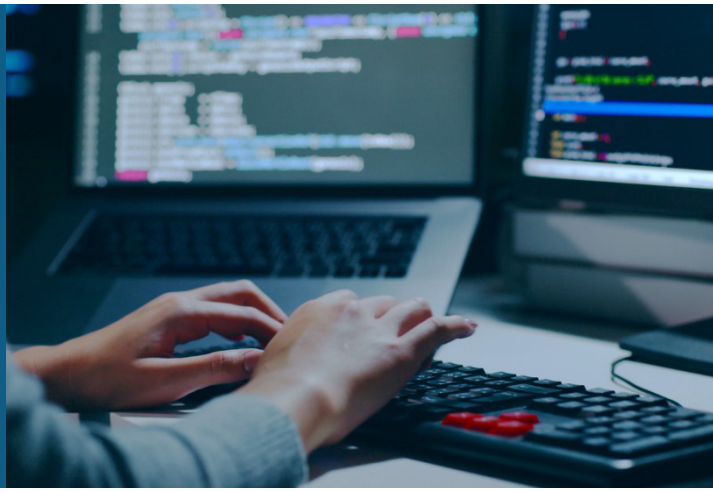
CYLERA™ | MITRE | ATT&CK®

SOLUTION BRIEF

Cylera and the MITRE ATT&CK for ICS Model

Detect Adversary Tactics, Techniques, and Procedures Faster

Improved cyber attack detection and investigations for healthcare delivery organizations



What Is the MITRE ATT&CK Model?

MITRE ATT&CK™ is a globally-accessible model that includes a knowledge base of adversary tactics and techniques based on real-world observations.

MITRE ATT&CK™ was started in 2013 to catalogue observed tactics, techniques, and procedures (TTPs) in use by advanced persistent threats (APTs) around the world. Many of the TTPs included in the knowledge base are in use by far less sophisticated attackers as well, and the structure of the model is usable by organizations of all sizes and security postures for identifying gaps in security coverage.

Since sophisticated TTPs that work well tend to enter the mainstream attack vernacular, the ATT&CK™ matrix offers enduring value for companies looking to vet and improve their detection and investigation coverage.

How Cylera Helps

The Cylera platform — along with the numerous security controls Cylera can identify for healthcare IT and clinical networks — can detect adversary techniques that correspond with each of the 11 tactics in the MITRE ATT&CK for ICS framework.

In addition to support for the MITRE ATT&CK for ICS model, Cylera also provides comprehensive healthcare IoT and connected medical device security and controls across the entire healthcare cybersecurity program spectrum. For example, the Cylera platform also aligns with guidelines set forth by NIST and other regulatory frameworks that follow the Identify, Protect, Detect, Respond, Recover, and Govern lifecycle.

MITRE ATT&CK for ICS Matrix Uses

- Identify threats
- Plan strategy
- Build defenses
- Assess and close gaps
- Monitor attack trends

Cylera Detection Capabilities

Cylera helps detect TTPs for healthcare IoT and connected medical devices per the MITRE ATT&CK for ICS model. Most of these techniques can be detected directly, while others can be detected indirectly via collateral efforts. The table below illustrates these capabilities for each technique and corresponding tactic.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command & 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 Ports	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 Later 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 Organizational 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 & Revenue
Replication Through Removeable Media	Project File Injection		Utilize Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing 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		

Reference

Cylera can detect technique directly

Cylera can detect technique indirectly

Cylera provides the easiest, most accurate and extensible platform for healthcare IoT intelligence and security to optimize patient care, service availability, and cyber defenses across diverse connected medical device and healthcare environments. The Cylera platform accurately discovers, categorizes, assesses, and monitors known and unknown assets with high fidelity to deliver unparalleled asset inventory, usage telemetry, risk prioritization, analytics, and guided threat remediation. Cylera integrates with popular IT and healthcare systems to allow organizations to advance cyber program maturity, increase operational efficiency,mitigate cyber threats, and enable compliance readiness.

CYLERA™

www.cylera.com