

Mastering MITRE ATT&CK for ICS with a Zero Trust Model

How Zero Trust Access and Protection Stops Threats

Introduction

In the rapidly evolving landscape of industrial control systems (ICS) security, understanding and mitigating potential threats is crucial. The MITRE ATT&CK for ICS Matrix offers a comprehensive framework for identifying and analyzing attacker tactics and techniques in ICS environments. However, merely understanding these threats is not enough. Implementing robust defense mechanisms is key. This is where Xage's Zero Trust Access Management and Asset Protection plays a pivotal role, blocking key attacks outlined in the MITRE ATT&CK ICS Matrix.

Understanding the MITRE ATT&CK ICS Matrix

The MITRE ATT&CK for ICS Matrix is a globally-recognized knowledge base used for understanding attacker behavior in the context of ICS. It categorizes real world cyberattacker tactics, techniques, and procedures—providing a structured approach to identifying security gaps and recommending detection and mitigation strategies. However, the complexity and sophistication of these attack tactics means that preventing them requires advanced security solutions.

| TA0108 Initial Access 12 techniques | TA0104 Execution 9 techniques | TA0110 Persistence 6 techniques | TA0111 Privilege Escalation 2 techniques | TA0103 Evasion 6 techniques | TA0102 Discovery 5 techniques | TA0109 Lateral Movement 7 techniques | TA0100 Collection 11 techniques | TA0101 Command and Control 3 techniques | TA0107 Inhibit Response Function 14 techniques | TA0106 Impair Process Control 5 techniques | TA0105 Impact 12 techniques |
|---|---|--|--|---|---|--|---|---|--|--|--|
| 12 techniques T0817 Drive-by Compromise T0819 Exploit Public-Facing Application 70886 Exploitation of Remote Services T0822 External Remote Services T0838 Internet Accessible Device T0886 Remote Services T0847 Replication Through Remote Services T0847 Replication Through Remote Services T0847 Regue Master T0848 Spearphishing Attachment T0868 Spearphishing Attachment T0864 Transient Cyber Asset T0860 Wireless | 9 techniques T0858 Change Operating Mode T0807 Command-Line Interface T0821 T0823 Graphical User Interface T0874 Hooking T0824 Modify Controller Tasking T0834 Native API T0853 Scripting T0863 User Execution | 6 techniques T0891 Hardcoded Credentials T0889 Modify Program T0839 Module Firmware T0873 Project File Infection T0857 System Firmware T0859 Valid Accounts | 2 techniques T0890 Exploitation for Privilege Escalation T0874 Hooking | b techniques T0858 Change Operating Mode T0820 T0820 T0820 T0872 Indicator Removal on Host T0849 Masquerading T0856 Spoof Reporting Message | b techniques T0840 Network Connection Enumeration T0842 Network Sniffing T0848 Remote System Discovery T0887 Wireless Sniffing | Techniques T0812 Default Credentials T0866 Exploitation of Remote Services T0881 Hardcoded Credentials T0887 Lateral Tool Transfer T0843 Program Download T0886 Remote Services T0859 Valid Accounts | 11 techniques T0830 Adversary-in-the- Middle Automated Collection T0802 Automated Collection T0811 Data from Local System T0868 Detect Operating Mode T0877 I/00 Detect Operating Mode T0801 Monitor Process State T0861 Point & Tag Identification T0845 Program Upload T0882 Screen Capture T0887 Wireless Sniffing | TO885 Commonly Used Port TO884 Connection Proxy TO889 Standard Application Layer Protocol | 14 techniques T0800 Activate Firmware Update Mode T0878 Alarm Suppression T0803 Block Command Message T0804 Block Reporting Message T0805 Block Reporting Change Credential T0809 Data Destruction T0814 Denial of Service T0816 Device Restart/Shutdown T0835 Manipulate I/O Image T0838 Modify Alarm Settings T0881 Service Stop T0857 | 5 techniques T0806 Brute Force I/O T0836 Modily Parameter T0839 Module Firmware T0856 Spoof Reporting Message T0855 Command Message | 12 techniques T0879 T0873 T0873 T0813 Denial of Control T0815 Denial of View T0826 Loss of Availability T0827 Loss of Control T0828 Loss of Productivity and Revenue T0837 T0829 Loss of View T0821 T0829 Loss of View T0831 Manipulation of View T0832 T0832 T0842 T0842 T0842 T0842 T0842 T0844 T0844 T0844 T0845 T084 |
| Compromise | | | | | | | | | System Firmware | | |

MITRE ATT&CK Framework for ICS.



The MITRE ATT&CK for ICS Matrix is divided into twelve tactic categories: Initial Access, Execution, Persistence, Privilege Escalation, Evasion, Discovery, Lateral Movement, Collection, Command and Control, Inhibit Response Function, Impair Process Control, and Impact. Each tactic category contains anywhere from 2 to 14 techniques.

For example, the Initial Access technique (TA0108) contains a dozen techniques, including Exploitation of Remote Services (T0866), Internet Accessible Device (T0883), and more. Each technique then lists specific procedures that have been used to execute the technique in real-world cyberattacks.

The Rise of Zero Trust in ICS Environments

Real world circumstances like the rise of remote work, cloud, and bring-your-own-device policies, alongside the increasing overall complexity and economic importance of industrial systems, are driving the urgent need for zero trust architectures in ICS.

"Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources...Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established." - NIST 800-207 Zero Trust Architecture

Logging into a corporate account should not grant access to every asset inside the corporate network. Logging into an engineering workstation at a factory should not grant access to every remote terminal unit, sensor and actuator on the site. Instead, they must verify anything and everything trying to connect to its systems before granting access. In the context of ICS, where the stakes involve critical infrastructure and industrial operations, zero trust isn't just a recommendation—it's a necessity.

Xage's Zero Trust Approach to Blocking ICS Threats

Xage provides secure access and asset protection solutions with zero trust built in, specifically tailored for ICS environments. Xage provides mitigations for over 90% of the techniques in the MITRE ATT&CK for ICS framework, across all twelve tactic categories. The following is a subset of examples of how Xage protects against key high risk tactics, techniques, and procedures.

| TA0108 Initial Access | TA0104 Execution | TA0110 Persistence | TA0111 Privilege Escalation | TA0103 Evasion | TA0102 Discovery | TA0109 Lateral Movement | TA0100 Collection | TA0101 Command and Control | TA0107 Inhibit Response Function | TA0106 Impair Process Control | TA0105 Impact |
|--------------------------|---------------------|------------------------|-----------------------------------|----------------------|---------------------|-------------------------------|----------------------------|----------------------------------|--|-------------------------------------|---------------------|
| 12 techniques | 9 techniques | 6 techniques | 2 techniques | 6 techniques | 5 techniques | 7 techniques | 11 techniques | 3 techniques | 14 techniques | 5 techniques | 12 techniques |
| T0817 | T0858 | T0891 | T0890 | T0858 | T0840 | T0812 | T0830 | T0885 | товоо | T0806 | T0879 |
| Drive-by | Change Operating | Hardcoded | Exploitation for | Change Operating | Network | Default | Adversary-in-the- | Commonly Used | Activate Firmware | Brute Force I/O | Damage to |
| Compromise | Mode | Credentiais | Escalation | wode | Enumeration | Credentials | Middle | Port | opuate Mode | т0836 | Property |
| T0819 | T0807 | T0889 | | T0820 | | T0866 | T0802 | T0884 | T0878 | Modify Parameter | T0813 |
| Exploit Public-Facing | Command-Line | Modify Program | T0874 | Exploitation for | T0842 | Exploitation of | Automated | Connection Proxy | Alarm Suppression | | Denial of Control |
| Application | Interface | T0830 | Hooking | Evasion | Network Sniffing | Remote Services | Collection | 70869 | T0803 | 10839 Module Eirmware | T0815 |
| т0866 | T0871 | Module Firmware | | T0872 | T0846 | T0891 | T0811 | Standard | Block Command | Woddie Firmware | Denial of View |
| Exploitation of | Execution through | | | Indicator Removal on | Remote System | Hardcoded | Data from | Application Layer | Message | T0856 | |
| Remote Services | API | T0873 | | Host | Discovery | Credentials | Information | Protocol | | Spoof Reporting | T0826 |
| тороо | T0922 | Project File Infection | | T0940 | 70000 | 70967 | Repositories | | T0804 Block Departing | Message | Loss of Availabilit |
| External Remote | Graphical User | T0857 | | Masquerading | Remote System | Lateral Tool | T0893 | | Message | T0855 | T0827 |
| Services | Interface | System Firmware | | macqueraamy | Information | Transfer | Data from Local | | moodage | Unauthorized | Loss of Control |
| | | | | T0851 | Discovery | | System | | T0805 | Command Message | |
| T0883 | T0874 | T0859 | | Rootkit | 70007 | T0843 | TODGO | | Block Serial COM | | T0828 |
| Device | Hooking | valid Accounts | | T0856 | Wireless Sniffing | Program Download | Detect Operating | | T0892 | | Productivity and |
| Device | T0821 | | | Spoof Reporting | Mileless chilling | T0886 | Mode | | Change Credential | | Revenue |
| T0886 | Modify Controller | | | Message | | Remote Services | | | | | |
| Remote Services | Tasking | | | | | 70050 | T0877 | | T0809 | | T0837 |
| T0947 | T0924 | | | | | 10859 Valid Accounts | I/O Image | | Data Destruction | | Loss of Protection |
| Replication Through | Native API | | | | | Valid Accounts | T0801 | | T0814 | | т0880 |
| Removable Media | | | | | | | Monitor Process | | Denial of Service | | Loss of Safety |
| | T0853 | | | | | | State | | | | |
| T0848 | Scripting | | | | | | T0061 | | T0816 | | T0829 |
| Rogue Master | T0863 | | | | | | Point & Tag | | Restart/Shutdown | | Loss of view |
| T0865 | User Execution | | | | | | Identification | | | | T0831 |
| Spearphishing | | | | | | | | | T0835 | | Manipulation of |
| Attachment | | | | | | | T0845 | | Manipulate I/O Image | | Control |
| T0862 | | | | | | | Program Opload | | T0838 | | T0832 |
| Supply Chain | | | | | | | T0852 | | Modify Alarm Settings | | Manipulation of |
| Compromise | | | | | | | Screen Capture | | | | View |
| 70004 | | | | | | | 70007 | | T0851 | | TODOO |
| Transient Cuber | | | | | | | 10887 Wiroloss Spiffing | | ROOTKIT | | Thoft of |
| Asset | | | | | | | Wireless Shiring | | T0881 | | Operational |
| | | | | | | | | | Service Stop | | Information |
| T0860 | | | | | | | | | | | |
| Wireless | | | | | | | | | T0857 | | |
| Compromise | | | | | | | | | System Firmware | | |





1. Zero Trust Identity and Access Management: Xage enforces strict identity verification for every device and user, ensuring that only authenticated and authorized entities can access system components. This directly counters techniques like 'Valid Accounts' and 'User Execution' listed in the MITRE matrix.



2. Least Privilege Access: By implementing least privilege access controls, Xage ensures that even authenticated users are only given access to resources essential for their tasks. This limits the potential impact of numerous techniques in the tactic categories of Privilege Escalation (TA0111), Lateral Movement (TA0109), and Persistence (TA0110). These tactic categories, and particularly the technique of abusing Valid Accounts (T0859), have been used in some of the biggest cyberattacks of the last several years.



3. Continuous Monitoring and Breach Prevention: Xage's system continuously monitors network access events, identifying and preventing attempted policy violations in real-time. Xage also logs all access events and provides screen recordings of each session for rapid investigation and incident response. This capability is crucial for detecting and mitigating Command and Control (TA0101) tactics and Evasion (TA0103) techniques.



4. Encryption, Data Integrity, and Data Access Control: Within Xage, all communications within the ICS network are encrypted, and data integrity checks are a standard. All data access and data transfer is controlled based on centrally-managed least privilege policies. This combats Adversary-in-the-Middle (T0830) and Data Destruction (T0809) threats and prevents data from being exfiltrated or shared with the wrong parties either maliciously or by accident.



5. Segmentation and Microsegmentation: Xage creates secure zones within the ICS network, isolating critical components. This segmentation is vital for protecting against a dozen techniques contained in the Target Discovery and Lateral Movement (TA0109) tactic categories and reducing the blast radius of any potential breach.

Real-World Outcomes in ICS Security

Multiple industrial organizations have adopted Xage's Zero Trust Access and Protection solutions, witnessing significant enhancements in their security posture. A major energy company eliminated risk against thousands of user accounts that had access to critical assets. The United States Space Force is achieving the goals of the Department of Defense's Zero Trust Roadmap, <u>using Xage.</u>

The Department of Energy's National Renewable Energy Lab tested Xage's ability to block critical, real-world MITRE techniques, using a realistic cyber range emulating actual power utility environments. Xage prevented numerous MITRE techniques pulled straight from recent, attacks against critical energy infrastructure. <u>Read More.</u>

MITRE-Enhanced Security with Xage

The MITRE ATT&CK ICS Matrix provides a valuable framework for understanding potential threats in ICS environments. However, the real game-changer is implementing a robust defense mechanism against these threats. Xage's Zero Trust solutions demonstrate a proactive and effective approach to securing ICS infrastructure while still enabling access and ease-of-use, offering a much-needed shield in an increasingly hostile digital landscape.

<u>Contact us</u> for further information about the MITRE ATT&CK ICS Matrix and how Xage's Zero Trust Access and Protection solutions provide protection across every Tactic category in the framework and robust attack prevention against the most common and devastating techniques.

