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

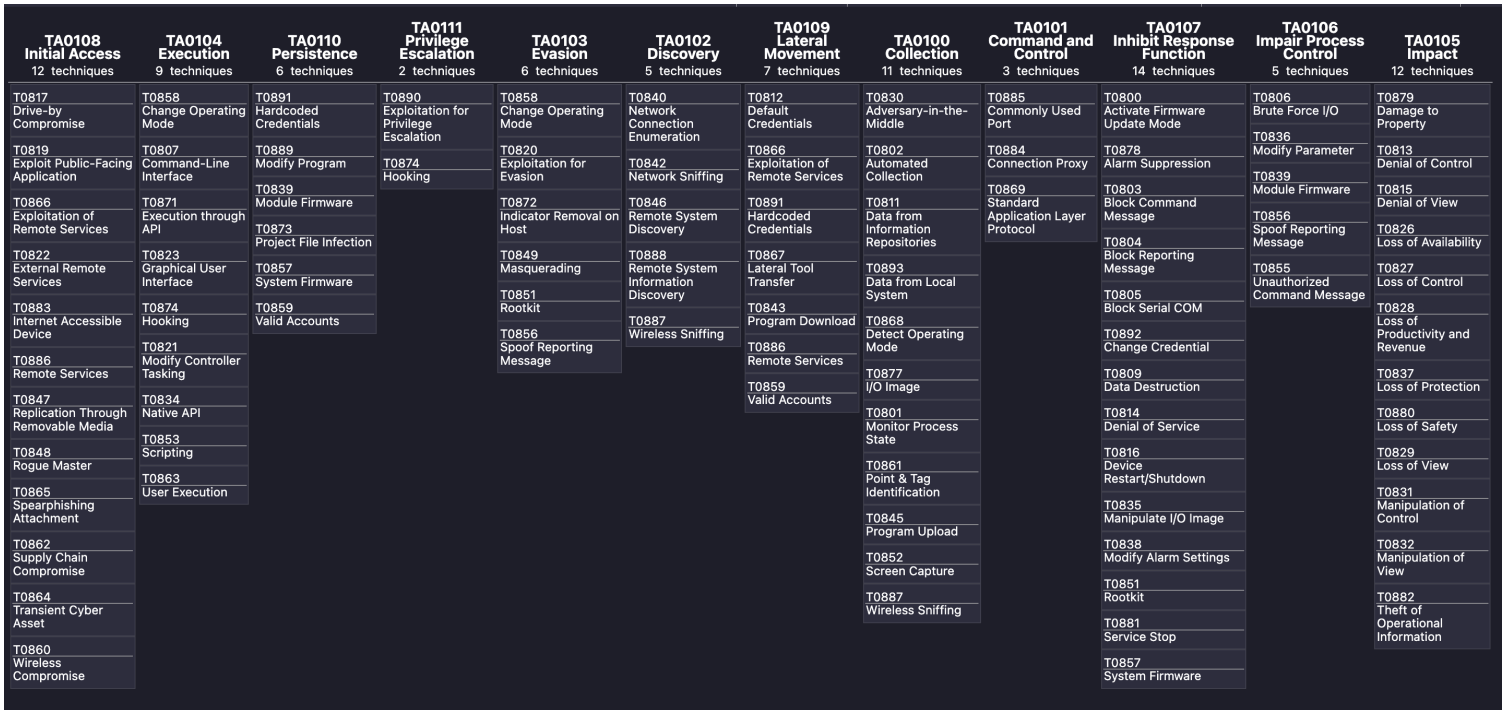
How Zero Trust Access and Protection Stops Threats

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.



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

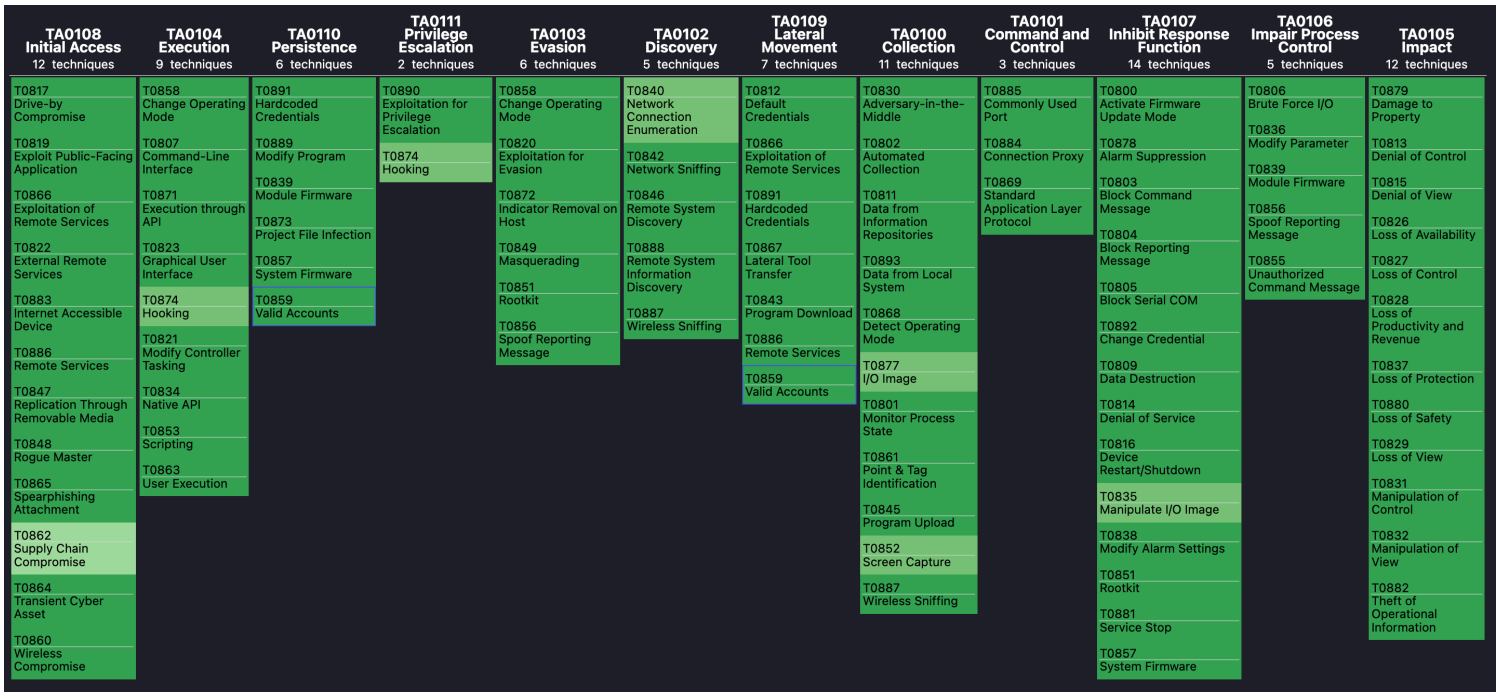
Real world circumstances like the rise of remote work, cloud, and bring-your-own-device policies, alongside the increasing overall complexity and economic importance of industrial systems, are driving the urgent need for zero trust architectures in ICS.

> ***"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.



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, using Xage.

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. Read More.

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.

Contact us 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.

xage SECURITY