MITRE ATT&CK Reference

ICS and Enterprise Matrices | ATT&CK v19.2 data (released August 2026) | Compiled September 28, 2026

Overview

What it is: MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a free, globally used knowledge base of adversary behavior built from real-world observations. It is not a regulation, a standard, or a compliance framework. It describes *how* attackers operate so defenders can test and prioritize their defenses against realistic behavior.

Structure: Tactics are the adversary's goal at each stage (the "why"). **Techniques** are how a goal is achieved, and **sub-techniques** are more specific variants. **Mitigations** are defensive measures mapped to techniques. **Groups** and **Software** link known threat actors and tools to the techniques they have used. ICS ATT&CK adds **Assets**, the OT device and system types that techniques target.

The matrices: Enterprise covers IT (Windows, Linux, macOS, cloud, identity, network devices, containers). **ICS** covers industrial control systems: PLCs, RTUs, HMIs, engineering workstations, historians, safety systems, and field devices. Real OT intrusions usually traverse both, starting in IT with Enterprise techniques and pivoting into OT with ICS techniques, so the two are meant to be used together.

This edition: ICS has 12 tactics, 79 techniques, and 18 sub-techniques, plus 52 mitigations, 18 asset types, and 14 tracked groups. Enterprise has 15 tactics, 222 techniques, and 475 sub-techniques. The Enterprise matrix in this release splits the former Defense Evasion tactic into **Stealth** and **Defense Impairment**.

Common uses: Threat-informed gap assessments (which techniques can you prevent, detect, or not see at all). Detection engineering and SIEM use-case coverage mapping. Purple-team and tabletop scenario design. Mapping incident findings to a common language for reporting. Evaluating vendor claims about OT monitoring coverage. Prioritizing mitigations by the techniques used against your sector.

Tips for water/wastewater OT work: Start with ICS Initial Access (especially External Remote Services, Internet Accessible Device, and Remote Services), plus Inhibit Response Function and Impair Process Control, which are where operational consequences occur. Build a coverage heat map in ATT&CK Navigator. Pair with CISA advisories, which cite ATT&CK technique IDs, and with SP 800-82 Rev 3 and ISA/IEC 62443 for control implementation.

Where to get it: attack.mitre.org (browsable site and ATT&CK Navigator); machine-readable STIX data on GitHub (mitre-attack/attack-stix-data); Excel exports are available from the site.

© The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation. Technique descriptions below are the first sentence of each official description; see attack.mitre.org for full details, procedure examples, and detection guidance.

Part 1 - ICS Matrix

Tactics at a glance

ID	Tactic	Techniques	Purpose
TA0108	**Initial Access**	12	The adversary is trying to get into your ICS environment. Initial Access consists of techniques that adversaries may use as entry vectors to gain an initial foothold within an ICS environment.
TA0104	**Execution**	10	The adversary is trying to run code or manipulate system functions, parameters, and data in an unauthorized way. Execution consists of techniques that result in adversary-controlled code running on a local or remote system, device, or other asset.
TA0110	**Persistence**	5	The adversary is trying to maintain their foothold in your ICS environment. Persistence consists of techniques that adversaries use to maintain access to ICS systems and devices across restarts, changed credentials, and other interruptions that could cut off their access.
TA0111	**Privilege Escalation**	2	The adversary is trying to gain higher-level permissions. Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network.
TA0103	**Evasion**	7	The adversary is trying to avoid security defenses. Evasion consists of techniques that adversaries use to avoid technical defenses throughout their campaign.
TA0102	**Discovery**	5	The adversary is locating information to assess and identify their targets in your environment. Discovery consists of techniques that adversaries use to survey your ICS environment and gain knowledge about the internal network, control system devices, and how their processes interact.
TA0109	**Lateral Movement**	6	The adversary is trying to move through your ICS environment. Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network.
TA0100	**Collection**	11	The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal. Collection consists of techniques adversaries use to gather domain knowledge and obtain contextual feedback in an ICS environment.
TA0101	**Command and Control**	3	The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment. Command and Control consists of techniques that adversaries use to communicate with and send commands to compromised systems, devices, controllers, and platforms with specialized applications used in ICS environments.
TA0107	**Inhibit Response Function**	13	The adversary is trying to prevent your safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state. Inhibit Response Function consists of techniques that adversaries use to hinder the safeguards put in place for processes and products.
TA0106	**Impair Process Control**	4	The adversary is trying to manipulate, disable, or damage physical control processes. Impair Process Control consists of techniques that adversaries use to disrupt control logic and cause determinantal effects to processes being controlled in the target environment.
TA0105	**Impact**	12	The adversary is trying to manipulate, interrupt, or destroy your ICS systems, data, and their surrounding environment. Impact consists of techniques that adversaries use to disrupt, compromise, destroy, and manipulate the integrity and availability of control system operations, processes, devices, and data.

TA0108 Initial Access

The adversary is trying to get into your ICS environment. Initial Access consists of techniques that adversaries may use as entry vectors to gain an initial foothold within an ICS environment.

ID	Technique	Description
T0817	**Drive-by Compromise**	Adversaries may gain access to a system during a drive-by compromise, when a user visits a website as part of a regular browsing session.
T0819	**Exploit Public-Facing Application**	Adversaries may leverage weaknesses to exploit internet-facing software for initial access into an industrial network.

ID	Technique	Description
T0866	**Exploitation of Remote Services**	Adversaries may exploit a software vulnerability to take advantage of a programming error in a program, service, or within the operating system software or kernel itself to enable remote service abuse.
T0822	**External Remote Services**	Adversaries may leverage external remote services as a point of initial access into your network.
T0883	**Internet Accessible Device**	Adversaries may gain access into industrial environments through systems exposed directly to the internet for remote access rather than through External Remote Services.
T0886	**Remote Services**	Adversaries may leverage remote services to move between assets and network segments.
T0847	**Replication Through Removable Media**	Adversaries may move onto systems, such as those separated from the enterprise network, by copying malware to removable media which is inserted into the control systems environment.
T0848	**Rogue Master**	Adversaries may setup a rogue master to leverage control server functions to communicate with outstations.
T0865	**Spearphishing Attachment**	Adversaries may use a spearphishing attachment, a variant of spearphishing, as a form of a social engineering attack against specific targets.
T0862	**Supply Chain Compromise**	Adversaries may perform supply chain compromise to gain control systems environment access by means of infected products, software, and workflows.
T0864	**Transient Cyber Asset**	Adversaries may target devices that are transient across ICS networks and external networks.
T0860	**Wireless Compromise**	Adversaries may perform wireless compromise as a method of gaining communications and unauthorized access to a wireless network.

TA0104 Execution

The adversary is trying to run code or manipulate system functions, parameters, and data in an unauthorized way. Execution consists of techniques that result in adversary-controlled code running on a local or remote system, device, or other asset.

ID	Technique	Description
T0895	**Autorun Image**	Adversaries may leverage AutoRun functionality or scripts to execute malicious code.
T0858	**Change Operating Mode**	Adversaries may change the operating mode of a controller to gain additional access to engineering functions such as Program Download.
T0807	**Command-Line Interface**	Adversaries may utilize command-line interfaces (CLIs) to interact with systems and execute commands.
T0871	**Execution through API**	Adversaries may attempt to leverage Application Program Interfaces (APIs) used for communication between control software and the hardware.
T0823	**Graphical User Interface**	Adversaries may attempt to gain access to a machine via a Graphical User Interface (GUI) to enhance execution capabilities.
T0874	**Hooking**	Adversaries may hook into application programming interface (API) functions used by processes to redirect calls for execution and privilege escalation means.
T0821	**Modify Controller Tasking**	Adversaries may modify the tasking of a controller to allow for the execution of their own programs.
T0834	**Native API**	Adversaries may directly interact with the native OS application programming interface (API) to access system functions.
T0853	**Scripting**	Adversaries may use scripting languages to execute arbitrary code in the form of a pre-written script or in the form of user-supplied code to an interpreter.
T0863	**User Execution**	Adversaries may rely on a targeted organizations user interaction for the execution of malicious code.

TA0110 Persistence

The adversary is trying to maintain their foothold in your ICS environment. Persistence consists of techniques that adversaries use to maintain access to ICS systems and devices across restarts, changed credentials, and other interruptions that could cut off their access.

ID	Technique	Description
T1694	**Insecure Credentials** T1694.001 Default Credentials T1694.002 Hardcoded Credentials	Adversaries may target insecure credentials as a means to persist on a system or device or move laterally from one system or device to another.
T1693	**Modify Firmware** T1693.001 System Firmware T1693.002 Module Firmware	Firmware is low-level software embedded in hardware that enables systems and devices to function properly and is commonly found in ICS environments.
T0889	**Modify Program**	Adversaries may modify or add a program on a controller to affect how it interacts with the physical process, peripheral devices and other hosts on the network.
T0873	**Project File Infection** T0873.001 Siemens Project File Format	Adversaries may attempt to infect project files with malicious code.
T0859	**Valid Accounts**	Adversaries may steal the credentials of a specific user or service account using credential access techniques.

TA0111 Privilege Escalation

The adversary is trying to gain higher-level permissions. Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network.

ID	Technique	Description
T0890	**Exploitation for Privilege Escalation**	Adversaries may exploit software vulnerabilities in an attempt to elevate privileges.
T0874	**Hooking**	Adversaries may hook into application programming interface (API) functions used by processes to redirect calls for execution and privilege escalation means.

TA0103 Evasion

The adversary is trying to avoid security defenses. Evasion consists of techniques that adversaries use to avoid technical defenses throughout their campaign.

ID	Technique	Description
T0858	**Change Operating Mode**	Adversaries may change the operating mode of a controller to gain additional access to engineering functions such as Program Download.
T0820	**Exploitation for Evasion**	Adversaries may exploit a software vulnerability to take advantage of a programming error in a program, service, or within the operating system software or kernel itself to evade detection.
T0872	**Indicator Removal on Host**	Adversaries may attempt to remove indicators of their presence on a system in an effort to cover their tracks.
T0849	**Masquerading**	Adversaries may use masquerading to disguise a malicious application or executable as another file, to avoid operator and engineer suspicion.
T0851	**Rootkit**	Adversaries may deploy rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components.
T0894	**System Binary Proxy Execution**	Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries.
T1692	**Unauthorized Message** T1692.001 Command Message T1692.002 Reporting Message	Adversaries may send unauthorized messages to ICS systems and devices to evade defenses or manipulate processes.

TA0102 Discovery

The adversary is locating information to assess and identify their targets in your environment. Discovery consists of techniques that adversaries use to survey your ICS environment and gain knowledge about the internal network, control system devices, and how their processes interact.

ID	Technique	Description
T0840	**Network Connection Enumeration**	Adversaries may perform network connection enumeration to discover information about device communication patterns.
T0842	**Network Sniffing**	Network sniffing is the practice of using a network interface on a computer system to monitor or capture information regardless of whether it is the specified destination for the information.
T0846	**Remote System Discovery** T0846.001 Port Scan T0846.002 Broadcast Discovery T0846.003 Multicast Discovery	Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for subsequent Lateral Movement or Discovery techniques.
T0888	**Remote System Information Discovery**	An adversary may attempt to get detailed information about remote systems and their peripherals, such as make/model, role, and configuration.
T0887	**Wireless Sniffing**	Adversaries may seek to capture radio frequency (RF) communication used for remote control and reporting in distributed environments.

TA0109 Lateral Movement

The adversary is trying to move through your ICS environment. Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network.

ID	Technique	Description
T0866	**Exploitation of Remote Services**	Adversaries may exploit a software vulnerability to take advantage of a programming error in a program, service, or within the operating system software or kernel itself to enable remote service abuse.
T1694	**Insecure Credentials** T1694.001 Default Credentials T1694.002 Hardcoded Credentials	Adversaries may target insecure credentials as a means to persist on a system or device or move laterally from one system or device to another.
T0867	**Lateral Tool Transfer**	Adversaries may transfer tools or other files from one system to another to stage adversary tools or other files over the course of an operation.
T0843	**Program Download** T0843.001 Download All T0843.002 Online Edit T0843.003 Program Append	Adversaries may perform a program download to transfer a user program to a controller.
T0886	**Remote Services**	Adversaries may leverage remote services to move between assets and network segments.
T0859	**Valid Accounts**	Adversaries may steal the credentials of a specific user or service account using credential access techniques.

TA0100 Collection

The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal. Collection consists of techniques adversaries use to gather domain knowledge and obtain contextual feedback in an ICS environment.

ID	Technique	Description
T0830	**Adversary-in-the-Middle**	Adversaries with privileged network access may seek to modify network traffic in real time using adversary-in-the-middle (AiTM) attacks.
T0802	**Automated Collection**	Adversaries may automate collection of industrial environment information using tools or scripts.
T0811	**Data from Information Repositories**	Adversaries may target and collect data from information repositories.
T0893	**Data from Local System**	Adversaries may target and collect data from local system sources, such as file systems, configuration files, or local databases.
T0868	**Detect Operating Mode**	Adversaries may gather information about a PLCs or controllers current operating mode.
T0877	**I/O Image**	Adversaries may seek to capture process values related to the inputs and outputs of a PLC.

ID	Technique	Description
T0801	**Monitor Process State**	Adversaries may gather information about the physical process state.
T0861	**Point & Tag Identification**	Adversaries may collect point and tag values to gain a more comprehensive understanding of the process environment.
T0845	**Program Upload**	Adversaries may attempt to upload a program from a PLC to gather information about an industrial process.
T0852	**Screen Capture**	Adversaries may attempt to perform screen capture of devices in the control system environment.
T0887	**Wireless Sniffing**	Adversaries may seek to capture radio frequency (RF) communication used for remote control and reporting in distributed environments.

TA0101 Command and Control

The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment. Command and Control consists of techniques that adversaries use to communicate with and send commands to compromised systems, devices, controllers, and platforms with specialized applications used in ICS environments.

ID	Technique	Description
T0885	**Commonly Used Port**	Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend in with normal network activity, to avoid more detailed inspection.
T0884	**Connection Proxy**	Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications.
T0869	**Standard Application Layer Protocol**	Adversaries may establish command and control capabilities over commonly used application layer protocols such as HTTP(S), OPC, RDP, telnet, DNP3, and modbus.

TA0107 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. Inhibit Response Function consists of techniques that adversaries use to hinder the safeguards put in place for processes and products.

ID	Technique	Description
T0800	**Activate Firmware Update Mode**	Adversaries may activate firmware update mode on devices to prevent expected response functions from engaging in reaction to an emergency or process malfunction.
T0878	**Alarm Suppression**	Adversaries may target protection function alarms to prevent them from notifying operators of critical conditions.
T1695	**Block Communications** T1695.001 Serial COM T1695.002 Ethernet T1695.003 Wi-Fi	Operational technology communications occur over serial COM, Ethernet, Wi-Fi, cellular (4G/5G), and satellite mediums.
T1691	**Block Operational Technology Message** T1691.001 Command Message T1691.002 Reporting Message	Adversaries may block messages between systems and devices in an OT/ICS environment to disrupt processes.
T0892	**Change Credential**	Adversaries may modify software and device credentials to prevent operator and responder access.
T0809	**Data Destruction**	Adversaries may perform data destruction over the course of an operation.
T0814	**Denial of Service**	Adversaries may perform Denial-of-Service (DoS) attacks to disrupt expected device functionality.
T0816	**Device Restart/Shutdown**	Adversaries may forcibly restart or shutdown a device in an ICS environment to disrupt and potentially negatively impact physical processes.
T0835	**Manipulate I/O Image**	Adversaries may manipulate the I/O image of PLCs through various means to prevent them from functioning as expected.
T0838	**Modify Alarm Settings**	Adversaries may modify alarm settings to prevent alerts that may inform operators of their presence or to prevent responses to dangerous and unintended scenarios.
T1693	**Modify Firmware** T1693.001 System Firmware T1693.002 Module Firmware	Firmware is low-level software embedded in hardware that enables systems and devices to function properly and is commonly found in ICS environments.

ID	Technique	Description
T0851	**Rootkit**	Adversaries may deploy rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components.
T0881	**Service Stop**	Adversaries may stop or disable services on a system to render those services unavailable to legitimate users.

TA0106 Impair Process Control

The adversary is trying to manipulate, disable, or damage physical control processes. Impair Process Control consists of techniques that adversaries use to disrupt control logic and cause determinantal effects to processes being controlled in the target environment.

ID	Technique	Description
T0806	**Brute Force I/O**	Adversaries may repetitively or successively change I/O point values to perform an action.
T1693	**Modify Firmware** T1693.001 System Firmware T1693.002 Module Firmware	Firmware is low-level software embedded in hardware that enables systems and devices to function properly and is commonly found in ICS environments.
T0836	**Modify Parameter**	Adversaries may modify parameters used to instruct industrial control system devices.
T1692	**Unauthorized Message** T1692.001 Command Message T1692.002 Reporting Message	Adversaries may send unauthorized messages to ICS systems and devices to evade defenses or manipulate processes.

TA0105 Impact

The adversary is trying to manipulate, interrupt, or destroy your ICS systems, data, and their surrounding environment. Impact consists of techniques that adversaries use to disrupt, compromise, destroy, and manipulate the integrity and availability of control system operations, processes, devices, and data.

ID	Technique	Description
T0879	**Damage to Property**	Adversaries may cause damage and destruction of property to infrastructure, equipment, and the surrounding environment when attacking control systems.
T0813	**Denial of Control**	Adversaries may cause a denial of control to temporarily prevent operators and engineers from interacting with process controls.
T0815	**Denial of View**	Adversaries may cause a denial of view in attempt to disrupt and prevent operator oversight on the status of an ICS environment.
T0826	**Loss of Availability**	Adversaries may attempt to disrupt essential components or systems to prevent owner and operator from delivering products or services.
T0827	**Loss of Control**	Adversaries may seek to achieve a sustained loss of control or a runaway condition in which operators cannot issue any commands even if the malicious interference has subsided.
T0828	**Loss of Productivity and Revenue**	Adversaries may cause loss of productivity and revenue through disruption and even damage to the availability and integrity of control system operations, devices, and related processes.
T0837	**Loss of Protection**	Adversaries may compromise protective system functions designed to prevent the effects of faults and abnormal conditions.
T0880	**Loss of Safety**	Adversaries may compromise safety system functions designed to maintain safe operation of a process when unacceptable or dangerous conditions occur.
T0829	**Loss of View**	Adversaries may cause a sustained or permanent loss of view where the ICS equipment will require local, hands-on operator intervention; for instance, a restart or manual operation.
T0831	**Manipulation of Control**	Adversaries may manipulate physical process control within the industrial environment.
T0832	**Manipulation of View**	Adversaries may attempt to manipulate the information reported back to operators or controllers.
T0882	**Theft of Operational Information**	Adversaries may steal operational information on a production environment as a direct mission outcome for personal gain or to inform future operations.

ICS Mitigations

ID	Mitigation	Description
M0800	**Authorization Enforcement**	The device or system should restrict read, manipulate, or execute privileges to only authenticated users who require access based on approved security policies.
M0801	**Access Management**	Access Management technologies can be used to enforce authorization polices and decisions, especially when existing field devices do not provide sufficient capabilities to support user identification and authentication.
M0802	**Communication Authenticity**	When communicating over an untrusted network, utilize secure network protocols that both authenticate the message sender and can verify its integrity.
M0803	**Data Loss Prevention**	Data Loss Prevention (DLP) technologies can be used to help identify adversarial attempts to exfiltrate operational information, such as engineering plans, trade secrets, recipes, intellectual property, or process telemetry.
M0804	**Human User Authentication**	Require user authentication before allowing access to data or accepting commands to a device.
M0805	**Mechanical Protection Layers**	Utilize a layered protection design based on physical or mechanical protection systems to prevent damage to property, equipment, human safety, or the environment.
M0806	**Minimize Wireless Signal Propagation**	Wireless signals frequently propagate outside of organizational boundaries, which provide opportunities for adversaries to monitor or gain unauthorized access to the wireless network.
M0807	**Network Allowlists**	Network allowlists can be implemented through either host-based files or system hosts files to specify what connections (e.g., IP address, MAC address, port, protocol) can be made from a device.
M0808	**Encrypt Network Traffic**	Utilize strong cryptographic techniques and protocols to prevent eavesdropping on network communications.
M0809	**Operational Information Confidentiality**	Deploy mechanisms to protect the confidentiality of information related to operational processes, facility locations, device configurations, programs, or databases that may have information that can be used to infer organizational trade-secrets, recipes, and other intellectual property (IP).
M0810	**Out-of-Band Communications Channel**	Have alternative methods to support communication requirements during communication failures and data integrity attacks.
M0811	**Redundancy of Service**	Redundancy could be provided for both critical ICS devices and services, such as back-up devices or hot-standbys.
M0812	**Safety Instrumented Systems**	Utilize Safety Instrumented Systems (SIS) to provide an additional layer of protection to hazard scenarios that may cause property damage.
M0813	**Software Process and Device Authentication**	Require the authentication of devices and software processes where appropriate.
M0814	**Static Network Configuration**	Configure hosts and devices to use static network configurations when possible, protocols that require dynamic discovery/addressing (e.g., ARP, DHCP, DNS) can be used to manipulate network message forwarding and enable various AiTM attacks.
M0815	**Watchdog Timers**	Utilize watchdog timers to ensure devices can quickly detect whether a system is unresponsive.
M0816	**Mitigation Limited or Not Effective**	This type of attack technique cannot be easily mitigated with preventative controls since it is based on the abuse of system features.
M0817	**Supply Chain Management**	Implement a supply chain management program, including policies and procedures to ensure all devices and components originate from a trusted supplier and are tested to verify their integrity.
M0818	**Validate Program Inputs**	Devices and programs designed to interact with control system parameters should validate the format and content of all user inputs and actions to ensure the values are within intended operational ranges.
M0913	**Application Developer Guidance**	This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.
M0915	**Active Directory Configuration**	Configure Active Directory to prevent use of certain techniques; use security identifier (SID) Filtering, etc.
M0916	**Vulnerability Scanning**	Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them.

ID	Mitigation	Description
M0917	**User Training**	Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction.
M0918	**User Account Management**	Manage the creation, modification, use, and permissions associated to user accounts.
M0919	**Threat Intelligence Program**	A threat intelligence program helps an organization generate their own threat intelligence information and track trends to inform defensive priorities to mitigate risk.
M0920	**SSL/TLS Inspection**	Break and inspect SSL/TLS sessions to look at encrypted web traffic for adversary activity.
M0921	**Restrict Web-Based Content**	Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc.
M0922	**Restrict File and Directory Permissions**	Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.
M0924	**Restrict Registry Permissions**	Restrict the ability to modify certain hives or keys in the Windows Registry.
M0926	**Privileged Account Management**	Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.
M0927	**Password Policies**	Set and enforce secure password policies for accounts.
M0928	**Operating System Configuration**	Make configuration changes related to the operating system or a common feature of the operating system that result in system hardening against techniques.
M0930	**Network Segmentation**	Architect sections of the network to isolate critical systems, functions, or resources.
M0931	**Network Intrusion Prevention**	Use intrusion detection signatures to block traffic at network boundaries.
M0932	**Multi-factor Authentication**	Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator.
M0934	**Limit Hardware Installation**	Block users or groups from installing or using unapproved hardware on systems, including USB devices.
M0935	**Limit Access to Resource Over Network**	Prevent access to file shares, remote access to systems, unnecessary services.
M0936	**Account Use Policies**	Configure features related to account use like login attempt lockouts, specific login times, etc.
M0937	**Filter Network Traffic**	Use network appliances to filter ingress or egress traffic and perform protocol-based filtering.
M0938	**Execution Prevention**	Block execution of code on a system through application control, and/or script blocking.
M0941	**Encrypt Sensitive Information**	Protect sensitive data-at-rest with strong encryption.
M0942	**Disable or Remove Feature or Program**	Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.
M0944	**Restrict Library Loading**	Prevent abuse of library loading mechanisms in the operating system and software to load untrusted code by configuring appropriate library loading mechanisms and investigating potential vulnerable software.
M0945	**Code Signing**	Enforce binary and application integrity with digital signature verification to prevent untrusted code from executing.
M0946	**Boot Integrity**	Use secure methods to boot a system and verify the integrity of the operating system and loading mechanisms.
M0947	**Audit**	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.
M0948	**Application Isolation and Sandboxing**	Restrict the execution of code to a virtual environment on or in-transit to an endpoint system.
M0949	**Antivirus/Antimalware**	Use signatures or heuristics to detect malicious software.
M0950	**Exploit Protection**	Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring.
M0951	**Update Software**	Perform regular software updates to mitigate exploitation risk.
M0953	**Data Backup**	Take and store data backups from end user systems and critical servers.
M0954	**Software Configuration**	Implement configuration changes to software (other than the operating system) to mitigate security risks associated with how the software operates.

ICS Asset Types

ID	Asset	Description
A0001	**Workstation**	Workstations are devices used by human operators or engineers to perform various configuration, programming, maintenance, diagnostic, or operational tasks.
A0002	**Human-Machine Interface (HMI)**	Human-Machine Interfaces (HMIs) are systems used by an operator to monitor the real-time status of an operational process and to perform necessary control functions, including the adjustment of device parameters.
A0003	**Programmable Logic Controller (PLC)**	A Programmable Logic Controller (PLC) is an embedded programmable control device.
A0004	**Remote Terminal Unit (RTU)**	A Remote Terminal Unit (RTU) is a device that typically resides between field devices (e.g., PLCs, IEDs) and control/SCADA servers and supports various communication interfacing and data aggregation functions.
A0005	**Intelligent Electronic Device (IED)**	An Intelligent Electronic Device (IED) is a type of specialized field device that is designed to perform specific operational functions, frequently for protection, monitoring, or control within the electric sector.
A0006	**Data Historian**	Data historians, or historian, are systems used to collect and store data, including telemetry, events, alerts, and alarms about the operational process and supporting devices.
A0007	**Control Server**	Control servers are typically a software platform that runs on a modern server operating system (e.g., MS Windows Server).
A0008	**Application Server**	Application servers are used across many different sectors to host various diverse software applications necessary to supporting the ICS.
A0009	**Data Gateway**	Data Gateway is a device that supports the communication and exchange of data between different systems, networks, or protocols within the ICS.
A0010	**Safety Controller**	Safety controllers are typically a type of field device used to perform the safety critical function.
A0011	**Virtual Private Network (VPN) Server**	A VPN server is a device that is used to establish a secure network tunnel between itself and other remote VPN devices, including field VPNs.
A0012	**Jump Host**	Jump hosts are devices used to support remote management sessions into ICS networks or devices.
A0013	**Field I/O**	Field I/O are devices that communicate with a controller or data aggregator to either send input data or receive output data.
A0014	**Routers**	A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network.
A0015	**Switch**	A switch is a network device that connects endpoints (e.g., workstations, servers, HMIs, PLCs, etc.) so that they can communicate and share data and resources.
A0016	**Firewall**	A gateway that limits access between networks in accordance with local security policy.
A0017	**Distributed Control System (DCS) Controller**	A Distributed Control System (DCS) Controller is a microprocessor unit that is used to manage automation processes.
A0018	**Programmable Automation Controller (PAC)**	A Programmable Automation Controller (PAC) is an embedded programmable control device.

Groups Tracked in ICS ATT&CK

ID	Group	Description
G0032	**Lazarus Group** aka Labyrinth Chollima, HIDDEN COBRA, Guardians of Peace	Lazarus Group is a North Korean state-sponsored cyber threat group attributed to the Reconnaissance General Bureau (RGB).
G0034	**Sandworm Team** aka ELECTRUM, Telebots, IRON VIKING	Sandworm Team is a destructive threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455.
G0035	**Dragonfly** aka TEMP.Isotope, DYMALLOY, Berserk Bear	Dragonfly is a cyber espionage group that has been attributed to Russia's Federal Security Service (FSB) Center 16.
G0037	**FIN6** aka Magecart Group 6, ITG08, Skeleton Spider	FIN6 is a cyber crime group that has stolen payment card data and sold it for profit on underground marketplaces.

ID	Group	Description
G0046	**FIN7** aka GOLD NIAGARA, ITG14, Carbon Spider	FIN7 is a financially-motivated threat group that has been active since 2013.
G0049	**OilRig** aka COBALT GYPSY, IRN2, APT34	OilRig is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014.
G0064	**APT33** aka HOLMIUM, Elfin, Peach Sandstorm	APT33 is a suspected Iranian threat group that has carried out operations since at least 2013.
G0082	**APT38** aka NICKEL GLADSTONE, BeagleBoyz, Bluenoroff	APT38 is a North Korean state-sponsored threat group that specializes in financial cyber operations; it has been attributed to the Reconnaissance General Bureau.
G0088	**TEMP.Veles** aka XENOTIME	TEMP.Veles is a Russia-based threat group that has targeted critical infrastructure.
G0102	**Wizard Spider** aka UNC1878, TEMP.MixMaster, Grim Spider	Wizard Spider is a Russia-based financially motivated threat group originally known for the creation and deployment of TrickBot since at least 2016.
G0115	**GOLD SOUTHFIELD** aka Pinchy Spider	GOLD SOUTHFIELD is a financially motivated threat group active since at least 2018 that operates the REvil Ransomware-as-a Service (RaaS).
G1000	**ALLANITE** aka Palmetto Fusion	ALLANITE is a suspected Russian cyber espionage group, that has primarily targeted the electric utility sector within the United States and United Kingdom.
G1001	**HEXANE** aka Lyceum, Siamesekitten, Spirlin	HEXANE is a cyber espionage threat group that has targeted oil & gas, telecommunications, aviation, and internet service provider organizations since at least 2017.
G1027	**CyberAv3ngers** aka Soldiers of Soloman	The CyberAv3ngers are a suspected Iranian Government Islamic Revolutionary Guard Corps (IRGC)-affiliated APT group.

Part 2 - Enterprise Matrix

Tactics at a glance

ID	Tactic	Techniques	Purpose
TA0043	**Reconnaissance**	12	The adversary is trying to gather information they can use to plan future operations. Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting.
TA0042	**Resource Development**	9	The adversary is trying to establish resources they can use to support operations. Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting.
TA0001	**Initial Access**	11	The adversary is trying to get into your network. Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network.
TA0002	**Execution**	20	The adversary is trying to run malicious code. Execution consists of techniques that result in adversary-controlled code running on a local or remote system.
TA0003	**Persistence**	22	The adversary is trying to maintain their foothold. Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.
TA0004	**Privilege Escalation**	13	The adversary is trying to gain higher-level permissions. Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network.
TA0005	**Stealth**	30	The adversary is trying to hide and conceal their actions, appearing as normal behavior. Stealth consists of techniques that reduce the likelihood of detection by blending in with legitimate activity or minimizing observable signals.
TA0112	**Defense Impairment**	18	The adversary is trying to break security mechanisms, pipelines, and tooling so defenders can't see or trust what's happening. Defense Impairment consists of techniques that degrade, disable, or undermine the effectiveness and trustworthiness of security controls and monitoring mechanisms.
TA0006	**Credential Access**	17	The adversary is trying to steal account names and passwords. Credential Access consists of techniques for stealing credentials like account names and passwords.
TA0007	**Discovery**	34	The adversary is trying to figure out your environment. Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network.
TA0008	**Lateral Movement**	9	The adversary is trying to move through your environment. Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network.
TA0009	**Collection**	17	The adversary is trying to gather data of interest to their goal. Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives.
TA0011	**Command and Control**	18	The adversary is trying to communicate with compromised systems to control them. Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network.
TA0010	**Exfiltration**	9	The adversary is trying to steal data. Exfiltration consists of techniques that adversaries may use to steal data from your network.
TA0040	**Impact**	15	The adversary is trying to manipulate, interrupt, or destroy your systems and data. Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes.

TA0043 Reconnaissance

The adversary is trying to gather information they can use to plan future operations. Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting.

ID	Technique	Subs	Description
T1595	**Active Scanning**	3	Adversaries may execute active reconnaissance scans to gather information that can be used during targeting.
T1592	**Gather Victim Host Information**	4	Adversaries may gather information about the victim's hosts that can be used during targeting.

ID	Technique	Subs	Description
T1589	**Gather Victim Identity Information**	3	Adversaries may gather information about the victim's identity that can be used during targeting.
T1590	**Gather Victim Network Information**	6	Adversaries may gather information about the victim's networks that can be used during targeting.
T1591	**Gather Victim Org Information**	4	Adversaries may gather information about the victim's organization that can be used during targeting.
T1598	**Phishing for Information**	4	Adversaries may send phishing messages to elicit sensitive information that can be used during targeting.
T1682	**Query Public AI Services**	-	Adversaries may query publicly accessible artificial intelligence (AI) services, such as large language models (LLMs), to support targeting and operations.
T1597	**Search Closed Sources**	2	Adversaries may search and gather information about victims from closed (e.g., paid, private, or otherwise not freely available) sources that can be used during targeting.
T1596	**Search Open Technical Databases**	5	Adversaries may search freely available technical databases for information about victims that can be used during targeting.
T1593	**Search Open Websites/Domains**	3	Adversaries may search freely available websites and/or domains for information about victims that can be used during targeting.
T1681	**Search Threat Vendor Data**	-	Threat actors may seek information/indicators from closed or open threat intelligence sources gathered about their own campaigns, as well as those conducted by other adversaries that may align with their target industries, capabilities/objectives, or other operational concerns.
T1594	**Search Victim-Owned Websites**	-	Adversaries may search websites owned by the victim for information that can be used during targeting.

TA0042 Resource Development

The adversary is trying to establish resources they can use to support operations. Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting.

ID	Technique	Subs	Description
T1650	**Acquire Access**	-	Adversaries may purchase or otherwise acquire an existing access to a target system or network.
T1583	**Acquire Infrastructure**	8	Adversaries may buy, lease, rent, or obtain infrastructure that can be used during targeting.
T1586	**Compromise Accounts**	3	Adversaries may compromise accounts with services that can be used during targeting.
T1584	**Compromise Infrastructure**	8	Adversaries may compromise third-party infrastructure that can be used during targeting.
T1587	**Develop Capabilities**	4	Adversaries may build capabilities that can be used during targeting.
T1585	**Establish Accounts**	3	Adversaries may create and cultivate accounts with services that can be used during targeting.
T1683	**Generate Content**	2	Adversaries may create or generate content to support targeting and operations.
T1588	**Obtain Capabilities**	7	Adversaries may buy and/or steal capabilities that can be used during targeting.
T1608	**Stage Capabilities**	6	Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting.

TA0001 Initial Access

The adversary is trying to get into your network. Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network.

ID	Technique	Subs	Description
T1659	**Content Injection**	-	Adversaries may gain access and continuously communicate with victims by injecting malicious content into systems through online network traffic.
T1189	**Drive-by Compromise**	-	Adversaries may gain access to a system through a user visiting a website over the normal course of browsing.

ID	Technique	Subs	Description
T1190	**Exploit Public-Facing Application**	-	Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network.
T1133	**External Remote Services**	-	Adversaries may leverage external-facing remote services to initially access and/or persist within a network.
T1200	**Hardware Additions**	-	Adversaries may physically introduce computer accessories, networking hardware, or other computing devices into a system or network that can be used as a vector to gain access.
T1566	**Phishing**	4	Adversaries may send phishing messages to gain access to victim systems.
T1091	**Replication Through Removable Media**	-	Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes.
T1195	**Supply Chain Compromise**	3	Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.
T1199	**Trusted Relationship**	-	Adversaries may breach or otherwise leverage organizations who have access to intended victims.
T1078	**Valid Accounts**	4	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
T1669	**Wi-Fi Networks**	-	Adversaries may gain initial access to target systems by connecting to wireless networks.

TA0002 Execution

The adversary is trying to run malicious code. Execution consists of techniques that result in adversary-controlled code running on a local or remote system.

ID	Technique	Subs	Description
T1197	**BITS Jobs**	-	Adversaries may abuse BITS jobs to persistently execute code and perform various background tasks.
T1651	**Cloud Administration Command**	-	Adversaries may abuse cloud management services to execute commands within virtual machines.
T1059	**Command and Scripting Interpreter**	13	Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries.
T1609	**Container Administration Command**	-	Adversaries may abuse a container administration service to execute commands within a container.
T1610	**Deploy Container**	-	Adversaries may deploy a container into an environment to facilitate execution or evade defenses.
T1675	**ESXi Administration Command**	-	Adversaries may abuse ESXi administration services to execute commands on guest machines hosted within an ESXi virtual environment.
T1203	**Exploitation for Client Execution**	-	Adversaries may exploit software vulnerabilities in client applications to execute code.
T1574	**Hijack Execution Flow**	12	Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs.
T1674	**Input Injection**	-	Adversaries may simulate keystrokes on a victim's computer by various means to perform any type of action on behalf of the user, such as launching the command interpreter using keyboard shortcuts, typing an inline script to be executed, or interacting directly with a GUI-based application.
T1559	**Inter-Process Communication**	3	Adversaries may abuse inter-process communication (IPC) mechanisms for local code or command execution.
T1106	**Native API**	-	Adversaries may interact with the native OS application programming interface (API) to execute behaviors.
T1677	**Poisoned Pipeline Execution**	-	Adversaries may manipulate continuous integration / continuous development (CI/CD) processes by injecting malicious code into the build process.
T1053	**Scheduled Task/Job**	5	Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code.

ID	Technique	Subs	Description
T1648	**Serverless Execution**	-	Adversaries may abuse serverless computing, integration, and automation services to execute arbitrary code in cloud environments.
T1129	**Shared Modules**	-	Adversaries may execute malicious payloads via loading shared modules.
T1072	**Software Deployment Tools**	-	Adversaries may gain access to and use centralized software suites installed within an enterprise to execute commands and move laterally through the network.
T1569	**System Services**	3	Adversaries may abuse system services or daemons to execute commands or programs.
T1127	**Trusted Developer Utilities Proxy Execution**	3	Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads.
T1204	**User Execution**	5	An adversary may rely upon specific actions by a user in order to gain execution.
T1047	**Windows Management Instrumentation**	-	Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads.

TA0003 Persistence

The adversary is trying to maintain their foothold. Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.

ID	Technique	Subs	Description
T1098	**Account Manipulation**	7	Adversaries may manipulate accounts to maintain and/or elevate access to victim systems.
T1197	**BITS Jobs**	-	Adversaries may abuse BITS jobs to persistently execute code and perform various background tasks.
T1547	**Boot or Logon Autostart Execution**	14	Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems.
T1037	**Boot or Logon Initialization Scripts**	5	Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence.
T1671	**Cloud Application Integration**	-	Adversaries may achieve persistence by leveraging OAuth application integrations in a software-as-a-service environment.
T1554	**Compromise Host Software Binary**	-	Adversaries may modify host software binaries to establish persistent access to systems.
T1136	**Create Account**	3	Adversaries may create an account to maintain access to victim systems.
T1543	**Create or Modify System Process**	5	Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence.
T1546	**Event Triggered Execution**	18	Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events.
T1668	**Exclusive Control**	-	Adversaries who successfully compromise a system may attempt to maintain persistence by “closing the door” behind them – in other words, by preventing other threat actors from initially accessing or maintaining a foothold on the same system.
T1133	**External Remote Services**	-	Adversaries may leverage external-facing remote services to initially access and/or persist within a network.
T1525	**Implant Internal Image**	-	Adversaries may implant cloud or container images with malicious code to establish persistence after gaining access to an environment.
T1556	**Modify Authentication Process**	9	Adversaries may modify authentication mechanisms and processes to access user credentials or enable otherwise unwarranted access to accounts.
T1112	**Modify Registry**	-	Adversaries may interact with the Windows Registry as part of a variety of other techniques to aid in defense evasion, persistence, and execution.
T1137	**Office Application Startup**	6	Adversaries may leverage Microsoft Office-based applications for persistence between startups.
T1653	**Power Settings**	-	Adversaries may impair a system's ability to hibernate, reboot, or shut down in order to extend access to infected machines.
T1542	**Pre-OS Boot**	5	Adversaries may abuse Pre-OS Boot mechanisms as a way to establish persistence on a system.

ID	Technique	Subs	Description
T1053	**Scheduled Task/Job**	5	Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code.
T1505	**Server Software Component**	6	Adversaries may abuse legitimate extensible development features of servers to establish persistent access to systems.
T1176	**Software Extensions**	2	Adversaries may abuse software extensions to establish persistent access to victim systems.
T1205	**Traffic Signaling**	2	Adversaries may use traffic signaling to hide open ports or other malicious functionality used for persistence or command and control.
T1078	**Valid Accounts**	4	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.

TA0004 Privilege Escalation

The adversary is trying to gain higher-level permissions. Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network.

ID	Technique	Subs	Description
T1548	**Abuse Elevation Control Mechanism**	6	Adversaries may circumvent mechanisms designed to control privilege elevation to gain higher-level permissions.
T1134	**Access Token Manipulation**	5	Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls.
T1098	**Account Manipulation**	7	Adversaries may manipulate accounts to maintain and/or elevate access to victim systems.
T1547	**Boot or Logon Autostart Execution**	14	Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems.
T1037	**Boot or Logon Initialization Scripts**	5	Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence.
T1543	**Create or Modify System Process**	5	Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence.
T1484	**Domain or Tenant Policy Modification**	2	Adversaries may modify the configuration settings of a domain or identity tenant to evade defenses and/or escalate privileges in centrally managed environments.
T1611	**Escape to Host**	-	Adversaries may break out of a container or virtualized environment to gain access to the underlying host.
T1546	**Event Triggered Execution**	18	Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events.
T1068	**Exploitation for Privilege Escalation**	-	Adversaries may exploit software vulnerabilities in an attempt to elevate privileges.
T1055	**Process Injection**	12	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges.
T1053	**Scheduled Task/Job**	5	Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code.
T1078	**Valid Accounts**	4	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.

TA0005 Stealth

The adversary is trying to hide and conceal their actions, appearing as normal behavior. Stealth consists of techniques that reduce the likelihood of detection by blending in with legitimate activity or minimizing observable signals.

ID	Technique	Subs	Description
T1134	**Access Token Manipulation**	5	Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls.
T1197	**BITS Jobs**	-	Adversaries may abuse BITS jobs to persistently execute code and perform various background tasks.

ID	Technique	Subs	Description
T1612	**Build Image on Host**	-	Adversaries may build a container image directly on a host to bypass defenses that monitor for the retrieval of malicious images from a public registry.
T1622	**Debugger Evasion**	-	Adversaries may employ various means to detect and avoid debuggers.
T1678	**Delay Execution**	-	Adversaries may employ various time-based methods to evade detection and analysis.
T1140	**Deobfuscate/Decode Files or Information**	-	Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis.
T1006	**Direct Volume Access**	-	Adversaries may directly access a volume to bypass file access controls and file system monitoring.
T1480	**Execution Guardrails**	2	Adversaries may use execution guardrails to constrain execution or actions based on adversary supplied and environment specific conditions that are expected to be present on the target.
T1211	**Exploitation for Stealth**	-	Adversaries may exploit vulnerabilities to evade detection by hiding activity, suppressing logging, or operating within trusted or unmonitored components.
T1564	**Hide Artifacts**	14	Adversaries may attempt to hide artifacts associated with their behaviors to evade detection.
T1574	**Hijack Execution Flow**	12	Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs.
T1070	**Indicator Removal**	8	Adversaries may selectively delete or modify artifacts generated to reduce indications of their presence and blend in with legitimate activity.
T1202	**Indirect Command Execution**	-	Adversaries may abuse utilities that allow for command execution to bypass security restrictions that limit the use of command-line interpreters.
T1036	**Masquerading**	12	Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools.
T1027	**Obfuscated Files or Information**	18	Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit.
T1542	**Pre-OS Boot**	5	Adversaries may abuse Pre-OS Boot mechanisms as a way to establish persistence on a system.
T1055	**Process Injection**	12	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges.
T1620	**Reflective Code Loading**	-	Adversaries may reflectively load code into a process in order to conceal the execution of malicious payloads.
T1014	**Rootkit**	-	Adversaries may use rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components.
T1679	**Selective Exclusion**	-	Adversaries may intentionally exclude certain files, folders, directories, file types, or system components from encryption or tampering during a ransomware or malicious payload execution.
T1684	**Social Engineering**	2	Adversaries may use social engineering techniques to influence users to take actions that result in unauthorized access, approval of changes, disclosure of sensitive information, or execution of adversary-supplied instructions (i.e., introduction of malicious payloads or software), while minimizing technical indicators.
T1218	**System Binary Proxy Execution**	14	Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries.
T1216	**System Script Proxy Execution**	2	Adversaries may use trusted scripts, often signed with certificates, to proxy the execution of malicious files.
T1221	**Template Injection**	-	Adversaries may create or modify references in user document templates to conceal malicious code or force authentication attempts.
T1205	**Traffic Signaling**	2	Adversaries may use traffic signaling to hide open ports or other malicious functionality used for persistence or command and control.
T1127	**Trusted Developer Utilities Proxy Execution**	3	Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads.
T1535	**Unused/Unsupported Cloud Regions**	-	Adversaries may create cloud instances in unused geographic service regions in order to evade detection.

ID	Technique	Subs	Description
T1078	**Valid Accounts**	4	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
T1497	**Virtualization/Sandbox Evasion**	3	Adversaries may employ various means to detect and avoid virtualization and analysis environments.
T1220	**XSL Script Processing**	-	Adversaries may bypass application control and obscure execution of code by embedding scripts inside XSL files.

TA0112 Defense Impairment

The adversary is trying to break security mechanisms, pipelines, and tooling so defenders can't see or trust what's happening. Defense Impairment consists of techniques that degrade, disable, or undermine the effectiveness and trustworthiness of security controls and monitoring mechanisms.

ID	Technique	Subs	Description
T1686	**Disable or Modify System Firewall**	3	Adversaries may disable or modify host-based or network firewalls to impair defensive mechanisms and enable further action.
T1685	**Disable or Modify Tools**	6	Adversaries may disable, degrade, or tamper with security tools or applications (e.g., endpoint detection and response (EDR) tools, intrusion detection systems (IDS), antivirus, logging agents, sensors, etc.) to impair or reduce visibility of defensive capabilities.
T1484	**Domain or Tenant Policy Modification**	2	Adversaries may modify the configuration settings of a domain or identity tenant to evade defenses and/or escalate privileges in centrally managed environments.
T1689	**Downgrade Attack**	-	Adversaries may downgrade or use a version of system features that may be outdated, vulnerable, and/or does not support updated security controls.
T1687	**Exploitation for Defense Impairment**	-	Adversaries may exploit vulnerabilities in security software, infrastructure, or defensive components to degrade, disable, or otherwise continue to impair their ability to prevent, detect, or respond to malicious activity.
T1222	**File and Directory Permissions Modification**	2	Adversaries may modify file or directory permissions/attributes to evade access control lists (ACLs) and access protected files.
T1556	**Modify Authentication Process**	9	Adversaries may modify authentication mechanisms and processes to access user credentials or enable otherwise unwarranted access to accounts.
T1578	**Modify Cloud Compute Infrastructure**	5	An adversary may attempt to modify a cloud account's compute service infrastructure to evade defenses.
T1666	**Modify Cloud Resource Hierarchy**	-	Adversaries may attempt to modify hierarchical structures in infrastructure-as-a-service (IaaS) environments in order to evade defenses.
T1112	**Modify Registry**	-	Adversaries may interact with the Windows Registry as part of a variety of other techniques to aid in defense evasion, persistence, and execution.
T1601	**Modify System Image**	2	Adversaries may make changes to the operating system of embedded network devices to weaken defenses and provide new capabilities for themselves.
T1599	**Network Boundary Bridging**	1	Adversaries may bridge network boundaries by compromising perimeter network devices or internal devices responsible for network segmentation.
T1647	**Plist File Modification**	-	Adversaries may modify property list files (plist files) to enable other malicious activity, while also potentially evading and bypassing system defenses. macOS applications use plist files, such as the info.plist file, to store properties and configuration settings that inform the operating system how to handle the application at runtime.
T1690	**Prevent Command History Logging**	-	Adversaries may impair command history logging to hide commands they run on a compromised system.
T1207	**Rogue Domain Controller**	-	Adversaries may register a rogue Domain Controller to enable manipulation of Active Directory data.
T1688	**Safe Mode Boot**	-	Adversaries may abuse Windows safe mode to disable endpoint defenses.
T1553	**Subvert Trust Controls**	6	Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs.
T1600	**Weaken Encryption**	2	Adversaries may compromise a network device's encryption capability in order to bypass encryption that would otherwise protect data communications.

TA0006 Credential Access

The adversary is trying to steal account names and passwords. Credential Access consists of techniques for stealing credentials like account names and passwords.

ID	Technique	Subs	Description
T1557	**Adversary-in-the-Middle**	4	Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing, Transmitted Data Manipulation, or replay attacks (Exploitation for Credential Access).
T1110	**Brute Force**	4	Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained.
T1555	**Credentials from Password Stores**	6	Adversaries may search for common password storage locations to obtain user credentials.
T1212	**Exploitation for Credential Access**	-	Adversaries may exploit software vulnerabilities in an attempt to collect credentials.
T1187	**Forced Authentication**	-	Adversaries may gather credential material by invoking or forcing a user to automatically provide authentication information through a mechanism in which they can intercept.
T1606	**Forge Web Credentials**	2	Adversaries may forge credential materials that can be used to gain access to web applications or Internet services.
T1056	**Input Capture**	4	Adversaries may use methods of capturing user input to obtain credentials or collect information.
T1556	**Modify Authentication Process**	9	Adversaries may modify authentication mechanisms and processes to access user credentials or enable otherwise unwarranted access to accounts.
T1111	**Multi-Factor Authentication Interception**	-	Adversaries may target multi-factor authentication (MFA) mechanisms, (i.e., smart cards, token generators, etc.) to gain access to credentials that can be used to access systems, services, and network resources.
T1621	**Multi-Factor Authentication Request Generation**	-	Adversaries may attempt to bypass multi-factor authentication (MFA) mechanisms and gain access to accounts by generating MFA requests sent to users.
T1040	**Network Sniffing**	-	Adversaries may passively sniff network traffic to capture information about an environment, including authentication material passed over the network.
T1003	**OS Credential Dumping**	8	Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password.
T1528	**Steal Application Access Token**	-	Adversaries can steal application access tokens as a means of acquiring credentials to access remote systems and resources.
T1539	**Steal Web Session Cookie**	-	An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials.
T1649	**Steal or Forge Authentication Certificates**	-	Adversaries may steal or forge certificates used for authentication to access remote systems or resources.
T1558	**Steal or Forge Kerberos Tickets**	5	Adversaries may attempt to subvert Kerberos authentication by stealing or forging Kerberos tickets to enable Pass the Ticket.
T1552	**Unsecured Credentials**	8	Adversaries may search compromised systems to find and obtain insecurely stored credentials.

TA0007 Discovery

The adversary is trying to figure out your environment. Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network.

ID	Technique	Subs	Description
T1087	**Account Discovery**	4	Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment.
T1010	**Application Window Discovery**	-	Adversaries may attempt to get a listing of open application windows.
T1217	**Browser Information Discovery**	-	Adversaries may enumerate information about browsers to learn more about compromised environments.

ID	Technique	Subs	Description
T1580	**Cloud Infrastructure Discovery**	-	An adversary may attempt to discover infrastructure and resources that are available within an infrastructure-as-a-service (IaaS) environment.
T1538	**Cloud Service Dashboard**	-	An adversary may use a cloud service dashboard GUI with stolen credentials to gain useful information from an operational cloud environment, such as specific services, resources, and features.
T1526	**Cloud Service Discovery**	-	An adversary may attempt to enumerate the cloud services running on a system after gaining access.
T1619	**Cloud Storage Object Discovery**	-	Adversaries may enumerate objects in cloud storage infrastructure.
T1613	**Container and Resource Discovery**	-	Adversaries may attempt to discover containers and other resources that are available within a containers environment.
T1622	**Debugger Evasion**	-	Adversaries may employ various means to detect and avoid debuggers.
T1652	**Device Driver Discovery**	-	Adversaries may attempt to enumerate local device drivers on a victim host.
T1482	**Domain Trust Discovery**	-	Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments.
T1083	**File and Directory Discovery**	-	Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system.
T1615	**Group Policy Discovery**	-	Adversaries may gather information on Group Policy settings to identify paths for privilege escalation, security measures applied within a domain, and to discover patterns in domain objects that can be manipulated or used to blend in the environment.
T1680	**Local Storage Discovery**	-	Adversaries may enumerate local drives, disks, and/or volumes and their attributes like total or free space and volume serial number.
T1654	**Log Enumeration**	-	Adversaries may enumerate system and service logs to find useful data.
T1046	**Network Service Discovery**	-	Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation.
T1135	**Network Share Discovery**	-	Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement.
T1040	**Network Sniffing**	-	Adversaries may passively sniff network traffic to capture information about an environment, including authentication material passed over the network.
T1201	**Password Policy Discovery**	-	Adversaries may attempt to access detailed information about the password policy used within an enterprise network or cloud environment.
T1120	**Peripheral Device Discovery**	-	Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system.
T1069	**Permission Groups Discovery**	3	Adversaries may attempt to discover group and permission settings.
T1057	**Process Discovery**	-	Adversaries may attempt to get information about running processes on a system.
T1012	**Query Registry**	-	Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.
T1018	**Remote System Discovery**	-	Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system.
T1518	**Software Discovery**	2	Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment.
T1082	**System Information Discovery**	-	An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture.
T1614	**System Location Discovery**	1	Adversaries may gather information in an attempt to calculate the geographical location of a victim host.
T1016	**System Network Configuration Discovery**	2	Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems.

ID	Technique	Subs	Description
T1049	**System Network Connections Discovery**	-	Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.
T1033	**System Owner/User Discovery**	-	Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system.
T1007	**System Service Discovery**	-	Adversaries may try to gather information about registered local system services.
T1124	**System Time Discovery**	-	An adversary may gather the system time and/or time zone settings from a local or remote system.
T1673	**Virtual Machine Discovery**	-	An adversary may attempt to enumerate running virtual machines (VMs) after gaining access to a host or hypervisor.
T1497	**Virtualization/Sandbox Evasion**	3	Adversaries may employ various means to detect and avoid virtualization and analysis environments.

TA0008 Lateral Movement

The adversary is trying to move through your environment. Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network.

ID	Technique	Subs	Description
T1210	**Exploitation of Remote Services**	-	Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network.
T1534	**Internal Spearphishing**	-	After they already have access to accounts or systems within the environment, adversaries may use internal spearphishing to gain access to additional information or compromise other users within the same organization.
T1570	**Lateral Tool Transfer**	-	Adversaries may transfer tools or other files between systems in a compromised environment.
T1563	**Remote Service Session Hijacking**	2	Adversaries may take control of preexisting sessions with remote services to move laterally in an environment.
T1021	**Remote Services**	8	Adversaries may use Valid Accounts to log into a service that accepts remote connections, such as telnet, SSH, and VNC.
T1091	**Replication Through Removable Media**	-	Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes.
T1072	**Software Deployment Tools**	-	Adversaries may gain access to and use centralized software suites installed within an enterprise to execute commands and move laterally through the network.
T1080	**Taint Shared Content**	-	Adversaries may deliver payloads to remote systems by adding content to shared storage locations, such as network drives or internal code repositories.
T1550	**Use Alternate Authentication Material**	4	Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls.

TA0009 Collection

The adversary is trying to gather data of interest to their goal. Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives.

ID	Technique	Subs	Description
T1557	**Adversary-in-the-Middle**	4	Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing, Transmitted Data Manipulation, or replay attacks (Exploitation for Credential Access).
T1560	**Archive Collected Data**	3	An adversary may compress and/or encrypt data that is collected prior to exfiltration.
T1123	**Audio Capture**	-	An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information.

ID	Technique	Subs	Description
T1119	**Automated Collection**	-	Once established within a system or network, an adversary may use automated techniques for collecting internal data.
T1185	**Browser Session Hijacking**	-	Adversaries may take advantage of security vulnerabilities and inherent functionality in browser software to change content, modify user-behaviors, and intercept information as part of various browser session hijacking techniques.
T1115	**Clipboard Data**	-	Adversaries may collect data stored in the clipboard from users copying information within or between applications.
T1074	**Data Staged**	2	Adversaries may stage collected data in a central location or directory prior to Exfiltration.
T1530	**Data from Cloud Storage**	-	Adversaries may access data from cloud storage.
T1602	**Data from Configuration Repository**	2	Adversaries may collect data related to managed devices from configuration repositories.
T1213	**Data from Information Repositories**	6	Adversaries may leverage information repositories to mine valuable information.
T1005	**Data from Local System**	-	Adversaries may search local system sources, such as file systems, configuration files, local databases, virtual machine files, or process memory, to find files of interest and sensitive data prior to Exfiltration.
T1039	**Data from Network Shared Drive**	-	Adversaries may search network shares on computers they have compromised to find files of interest.
T1025	**Data from Removable Media**	-	Adversaries may search connected removable media on computers they have compromised to find files of interest.
T1114	**Email Collection**	3	Adversaries may target user email to collect sensitive information.
T1056	**Input Capture**	4	Adversaries may use methods of capturing user input to obtain credentials or collect information.
T1113	**Screen Capture**	-	Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation.
T1125	**Video Capture**	-	An adversary can leverage a computer's peripheral devices (e.g., integrated cameras or webcams) or applications (e.g., video call services) to capture video recordings for the purpose of gathering information.

TA0011 Command and Control

The adversary is trying to communicate with compromised systems to control them. Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network.

ID	Technique	Subs	Description
T1071	**Application Layer Protocol**	5	Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic.
T1092	**Communication Through Removable Media**	-	Adversaries can perform command and control between compromised hosts on potentially disconnected networks using removable media to transfer commands from system to system.
T1659	**Content Injection**	-	Adversaries may gain access and continuously communicate with victims by injecting malicious content into systems through online network traffic.
T1132	**Data Encoding**	2	Adversaries may encode data to make the content of command and control traffic more difficult to detect.
T1001	**Data Obfuscation**	3	Adversaries may obfuscate command and control traffic to make it more difficult to detect.
T1568	**Dynamic Resolution**	3	Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations.
T1573	**Encrypted Channel**	2	Adversaries may employ an encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol.
T1008	**Fallback Channels**	-	Adversaries may use fallback or alternate communication channels if the primary channel is compromised or inaccessible in order to maintain reliable command and control and to avoid data transfer thresholds.

ID	Technique	Subs	Description
T1665	**Hide Infrastructure**	-	Adversaries may manipulate network traffic in order to hide and evade detection of their C2 infrastructure.
T1105	**Ingress Tool Transfer**	-	Adversaries may transfer tools or other files from an external system into a compromised environment.
T1104	**Multi-Stage Channels**	-	Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions.
T1095	**Non-Application Layer Protocol**	-	Adversaries may use an OSI non-application layer protocol for communication between host and C2 server or among infected hosts within a network.
T1571	**Non-Standard Port**	-	Adversaries may communicate using a protocol and port pairing that are typically not associated.
T1572	**Protocol Tunneling**	-	Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems.
T1090	**Proxy**	4	Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure.
T1219	**Remote Access Tools**	3	An adversary may use legitimate remote access tools to establish an interactive command and control channel within a network.
T1205	**Traffic Signaling**	2	Adversaries may use traffic signaling to hide open ports or other malicious functionality used for persistence or command and control.
T1102	**Web Service**	3	Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system.

TA0010 Exfiltration

The adversary is trying to steal data. Exfiltration consists of techniques that adversaries may use to steal data from your network.

ID	Technique	Subs	Description
T1020	**Automated Exfiltration**	1	Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection.
T1030	**Data Transfer Size Limits**	-	An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds.
T1048	**Exfiltration Over Alternative Protocol**	3	Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel.
T1041	**Exfiltration Over C2 Channel**	-	Adversaries may steal data by exfiltrating it over an existing command and control channel.
T1011	**Exfiltration Over Other Network Medium**	1	Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel.
T1052	**Exfiltration Over Physical Medium**	1	Adversaries may attempt to exfiltrate data via a physical medium, such as a removable drive.
T1567	**Exfiltration Over Web Service**	4	Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel.
T1029	**Scheduled Transfer**	-	Adversaries may schedule data exfiltration to be performed only at certain times of day or at certain intervals.
T1537	**Transfer Data to Cloud Account**	-	Adversaries may exfiltrate data by transferring the data, including through sharing/syncing and creating backups of cloud environments, to another cloud account they control on the same service.

TA0040 Impact

The adversary is trying to manipulate, interrupt, or destroy your systems and data. Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes.

ID	Technique	Subs	Description
T1531	**Account Access Removal**	-	Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users.
T1485	**Data Destruction**	1	Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources.
T1486	**Data Encrypted for Impact**	-	Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources.
T1565	**Data Manipulation**	3	Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data.
T1491	**Defacement**	2	Adversaries may modify visual content available internally or externally to an enterprise network, thus affecting the integrity of the original content.
T1561	**Disk Wipe**	2	Adversaries may wipe or corrupt raw disk data on specific systems or in large numbers in a network to interrupt availability to system and network resources.
T1667	**Email Bombing**	-	Adversaries may flood targeted email addresses with an overwhelming volume of messages.
T1499	**Endpoint Denial of Service**	4	Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users.
T1657	**Financial Theft**	-	Adversaries may steal monetary resources from targets through extortion, social engineering, technical theft, or other methods aimed at their own financial gain at the expense of the availability of these resources for victims.
T1495	**Firmware Corruption**	-	Adversaries may overwrite or corrupt the flash memory contents of system BIOS or other firmware in devices attached to a system in order to render them inoperable or unable to boot, thus denying the availability to use the devices and/or the system.
T1490	**Inhibit System Recovery**	-	Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.
T1498	**Network Denial of Service**	2	Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users.
T1496	**Resource Hijacking**	4	Adversaries may leverage the resources of co-opted systems to complete resource-intensive tasks, which may impact system and/or hosted service availability.
T1489	**Service Stop**	-	Adversaries may stop or disable services on a system to render those services unavailable to legitimate users.
T1529	**System Shutdown/Reboot**	-	Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems.

Enterprise Mitigations

ID	Mitigation	Description
M1013	**Application Developer Guidance**	Application Developer Guidance focuses on providing developers with the knowledge, tools, and best practices needed to write secure code, reduce vulnerabilities, and implement secure design principles.
M1015	**Active Directory Configuration**	Implement robust Active Directory (AD) configurations using group policies to secure user accounts, control access, and minimize the attack surface.
M1016	**Vulnerability Scanning**	Vulnerability scanning involves the automated or manual assessment of systems, applications, and networks to identify misconfigurations, unpatched software, or other security weaknesses.
M1017	**User Training**	User Training involves educating employees and contractors on recognizing, reporting, and preventing cyber threats that rely on human interaction, such as phishing, social engineering, and other manipulative techniques.
M1018	**User Account Management**	User Account Management involves implementing and enforcing policies for the lifecycle of user accounts, including creation, modification, and deactivation.
M1019	**Threat Intelligence Program**	A Threat Intelligence Program enables organizations to proactively identify, analyze, and act on cyber threats by leveraging internal and external data sources.
M1020	**SSL/TLS Inspection**	SSL/TLS inspection involves decrypting encrypted network traffic to examine its content for signs of malicious activity.
M1021	**Restrict Web-Based Content**	Restricting web-based content involves enforcing policies and technologies that limit access to potentially malicious websites, unsafe downloads, and unauthorized browser behaviors.
M1022	**Restrict File and Directory Permissions**	Restricting file and directory permissions involves setting access controls at the file system level to limit which users, groups, or processes can read, write, or execute files.
M1024	**Restrict Registry Permissions**	Restricting registry permissions involves configuring access control settings for sensitive registry keys and hives to ensure that only authorized users or processes can make modifications.
M1025	**Privileged Process Integrity**	Privileged Process Integrity focuses on defending highly privileged processes (e.g., system services, antivirus, or authentication processes) from tampering, injection, or compromise by adversaries.
M1026	**Privileged Account Management**	Privileged Account Management focuses on implementing policies, controls, and tools to securely manage privileged accounts (e.g., SYSTEM, root, or administrative accounts).
M1027	**Password Policies**	Set and enforce secure password policies for accounts to reduce the likelihood of unauthorized access.
M1028	**Operating System Configuration**	Operating System Configuration involves adjusting system settings and hardening the default configurations of an operating system (OS) to mitigate adversary exploitation and prevent abuse of system functionality.
M1029	**Remote Data Storage**	Remote Data Storage focuses on moving critical data, such as security logs and sensitive files, to secure, off-host locations to minimize unauthorized access, tampering, or destruction by adversaries.
M1030	**Network Segmentation**	Network segmentation involves dividing a network into smaller, isolated segments to control and limit the flow of traffic between devices, systems, and applications.
M1031	**Network Intrusion Prevention**	Use intrusion detection signatures to block traffic at network boundaries.
M1032	**Multi-factor Authentication**	Multi-Factor Authentication (MFA) enhances security by requiring users to provide at least two forms of verification to prove their identity before granting access.
M1033	**Limit Software Installation**	Prevent users or groups from installing unauthorized or unapproved software to reduce the risk of introducing malicious or vulnerable applications.
M1034	**Limit Hardware Installation**	Prevent unauthorized users or groups from installing or using hardware, such as external drives, peripheral devices, or unapproved internal hardware components, by enforcing hardware usage policies and technical controls.
M1035	**Limit Access to Resource Over Network**	Restrict access to network resources, such as file shares, remote systems, and services, to only those users, accounts, or systems with a legitimate business requirement.
M1036	**Account Use Policies**	Account Use Policies help mitigate unauthorized access by configuring and enforcing rules that govern how and when accounts can be used.
M1037	**Filter Network Traffic**	Employ network appliances and endpoint software to filter ingress, egress, and lateral network traffic.

ID	Mitigation	Description
M1038	**Execution Prevention**	Prevent the execution of unauthorized or malicious code on systems by implementing application control, script blocking, and other execution prevention mechanisms.
M1039	**Environment Variable Permissions**	Restrict the modification of environment variables to authorized users and processes by enforcing strict permissions and policies.
M1040	**Behavior Prevention on Endpoint**	Behavior Prevention on Endpoint refers to the use of technologies and strategies to detect and block potentially malicious activities by analyzing the behavior of processes, files, API calls, and other endpoint events.
M1041	**Encrypt Sensitive Information**	Protect sensitive information at rest, in transit, and during processing by using strong encryption algorithms.
M1042	**Disable or Remove Feature or Program**	Disable or remove unnecessary and potentially vulnerable software, features, or services to reduce the attack surface and prevent abuse by adversaries.
M1043	**Credential Access Protection**	Credential Access Protection focuses on implementing measures to prevent adversaries from obtaining credentials, such as passwords, hashes, tokens, or keys, that could be used for unauthorized access.
M1044	**Restrict Library Loading**	Restricting library loading involves implementing security controls to ensure that only trusted and verified libraries (DLLs, shared objects, etc.) are loaded into processes.
M1045	**Code Signing**	Code Signing is a security process that ensures the authenticity and integrity of software by digitally signing executables, scripts, and other code artifacts.
M1046	**Boot Integrity**	Boot Integrity ensures that a system starts securely by verifying the integrity of its boot process, operating system, and associated components.
M1047	**Audit**	Auditing is the process of recording activity and systematically reviewing and analyzing the activity and system configurations.
M1048	**Application Isolation and Sandboxing**	Application Isolation and Sandboxing refers to the technique of restricting the execution of code to a controlled and isolated environment (e.g., a virtual environment, container, or sandbox).
M1049	**Antivirus/Antimalware**	Antivirus/Antimalware solutions utilize signatures, heuristics, and behavioral analysis to detect, block, and remediate malicious software, including viruses, trojans, ransomware, and spyware.
M1050	**Exploit Protection**	Deploy capabilities that detect, block, and mitigate conditions indicative of software exploits.
M1051	**Update Software**	Software updates ensure systems are protected against known vulnerabilities by applying patches and upgrades provided by vendors.
M1052	**User Account Control**	User Account Control (UAC) is a security feature in Microsoft Windows that prevents unauthorized changes to the operating system.
M1053	**Data Backup**	Data Backup involves taking and securely storing backups of data from end-user systems and critical servers.
M1054	**Software Configuration**	Software configuration refers to making security-focused adjustments to the settings of applications, middleware, databases, or other software to mitigate potential threats.
M1055	**Do Not Mitigate**	The Do Not Mitigate category highlights scenarios where attempting to mitigate a specific technique may inadvertently increase the organization's security risk or operational instability.
M1056	**Pre-compromise**	Pre-compromise mitigations involve proactive measures and defenses implemented to prevent adversaries from successfully identifying and exploiting weaknesses during the Reconnaissance and Resource Development phases of an attack.
M1057	**Data Loss Prevention**	Data Loss Prevention (DLP) involves implementing strategies and technologies to identify, categorize, monitor, and control the movement of sensitive data within an organization.
M1060	**Out-of-Band Communications Channel**	Establish secure out-of-band communication channels to ensure the continuity of critical communications during security incidents, data integrity attacks, or in-network communication failures.