SANS INSTITUTE ICS Cyber Kill Chain

MITRE ATT&CK™

D3FEND™

SE TU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

Topic 2

SANS ICS Cyber Kill Chain MITRE ATT&CK & D3FEND for ICS

Dr Diarmuid Ó Briain

DEPARTMENT OF ELECTRONIC ENGINEERING & COMMUNICATIONS
SOUTH EAST TECHNOLOGICAL UNIVERSITY

20 Jan 2026

Version: 3.0.0

Licence

Learning objectives

- By the end of this topic you will be able to:
  - Understand and apply the SANS Cyber Kill Chain for Industrial Control Systems (ICS) and MITRE ATT&CK and D3FEND frameworks to analyse real-world Operational Technology (OT) cyberattacks.
  - Identify and analyse the unique cybersecurity challenges faced by OT systems.
  - Develop comprehensive threat models for OT systems to identify, prioritise, and mitigate potential attack vectors.
  - Evaluate the effectiveness of OT security controls in preventing and mitigating cyber threats.

Introduction to ICS Cyber Kill Chain & MITRE Frameworks

Framework	Primary Focus	Key Outcome
SANS ICS Kill Chain	Attack Lifecycle	Understanding the stages of an industrial cyber-attack.
MITRE ATT&CK	Adversary Behaviour	Identifying specific TTPs used by attackers.
MITRE D3FEND	Defensive Countermeasures	Implementing technical functions to negate or detect TTPs.

SANS ICS Kill Chain

What is a Kill Chain

- US Army doctrine F2T2EA, a structured procedure for identifying, engaging, and neutralising an enemy to achieve a desired outcome
  - **Find**: Locate suitable adversary targets for engagement
  - **Fix**: or pinpoint their exact location
  - **Track**: and monitor their movements
  - **Target**: Select the appropriate weapon or asset to produce the desired effects
  - **Engage**: the adversary
  - **Assess**: Evaluate the results.

Advanced Persistent Threats (APT)

- Meticulously planned and executed cyberattacks targeting specific organisations with sensitive information.
- Conventional tools, reliant on signatures and patterns to identify known vulnerabilities, are ineffective against APTs.
- APT attackers often employ zero-day exploits and custom malware to evade detection.
- Organisations need to adopt a more proactive and intelligence-driven approach to cyber defence.

Advanced Persistent Threats (APT)

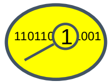
- Proactive approaches include:
  - Threat intelligence gathering
  - Network segmentation
  - Behavioural anomaly detection.

Intelligence-driven Computer Network Defence (CND)

- Leveraging adversary knowledge and Tactics, Techniques, and Procedures (TTP) for proactive defence.
- Understanding attack stages, mapping TTPs to defence measures, and identifying patterns.
- Proactive anticipation and neutralisation of attacks through continuous intelligence gathering.
- Reduced intrusion likelihood, informed resource allocation, and performance assessment.
- Addressing threat component of risk beyond vulnerability mitigation.

Intrusion Kill Chain

LOCKHEED MARTIN

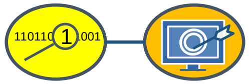


1) Reconnaissance

- Attacker gathers information about the target organisation and its systems.
- Info can be obtained from a variety of sources, such as public records, social media, and corporate websites.
- The goal is to identify vulnerabilities that the attacker can exploit to gain access to the target system.

Intrusion Kill Chain

LOCKHEED MARTIN



2) Weaponisation

- Develop a malicious payload.
- Code that will be used to exploit the vulnerabilities in the target system, such as a virus, worm, or Trojan horse.

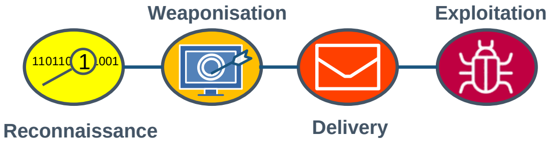
Intrusion Kill Chain

LOCKHEED MARTIN

3) Delivery

- Deliver the payload to the target system,such as through email, USB drive, or network exploitation.
- Get the payload onto the target system so that it can be executed.

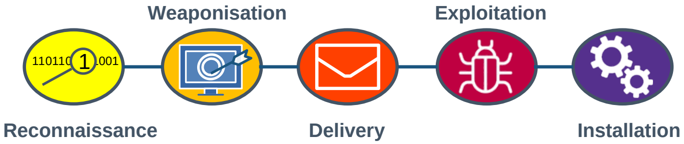
Intrusion Kill Chain



4) Exploitation

- Attempt to exploit the vulnerabilities that have been identified.
- Use the payload to execute malicious code and gain access to the system.

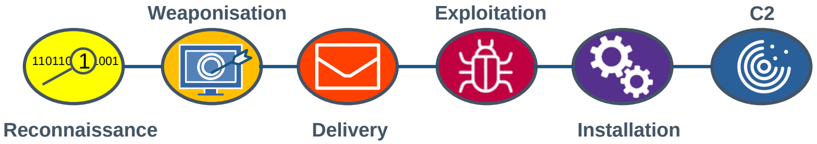
Intrusion Kill Chain



5) Installation

- Install malware or other malicious software.
- Gains control of the system to facilitate the carrying out of objectives.

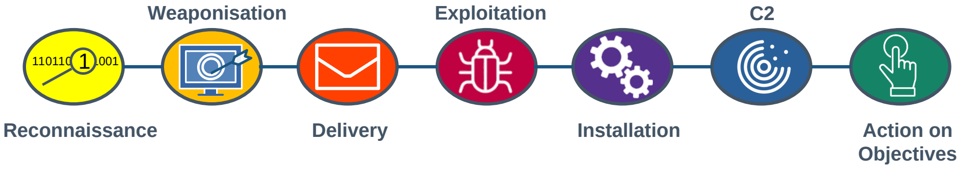
Intrusion Kill Chain



6) Command and Control (C2)

- Establish a communication channel with the compromised system for remote control.
- Facilitates the stealing of data, installation of more malware, or launch other attacks.

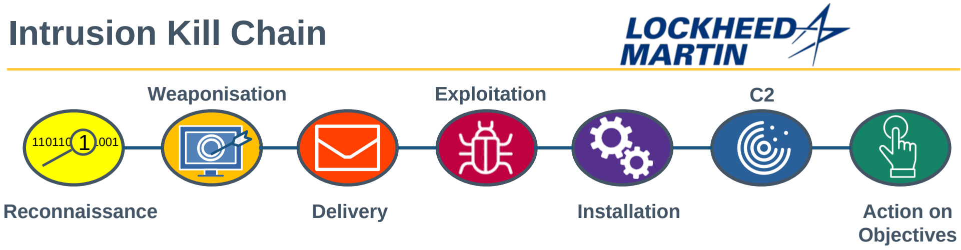
Intrusion Kill Chain



7) Actions on Objectives

- Carry out their objectives, such as stealing data, disrupting operations, or damaging the system.

Intrusion Kill Chain



- The intrusion kill chain can be used as a model for actionable intelligence by aligning enterprise defensive capabilities with the adversary's specific processes.
- Defenders can evaluate the performance and effectiveness of their defences by using the intrusion kill chain to track the adversary's progress through the attack lifecycle.
  - This approach allows defenders to identify capability gaps and devise investment roadmaps to address them.
- Intelligence-driven CND is based on a deep understanding of the adversary and enables informed security decisions and measurements.

SETU Ollscoil Teicneolaíochta an Oirdheisceirt South East Technological University

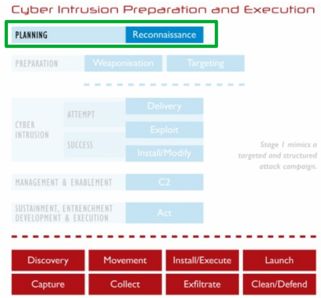
SANS

ICS Kill Chain

Stage 1

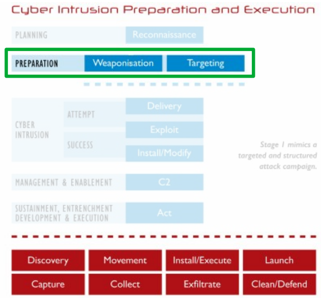
SANS Cyber Kill Chain for ICS – Stage 1

- **Planning Phase**
  - ***Reconnaissance***:
    - Gather info about the target.
  - ***Target Selection***
  - ***Developing Exploits***
  - ***Establish Command and Control (C2)***:
    - Establish comms channel with C2 server.



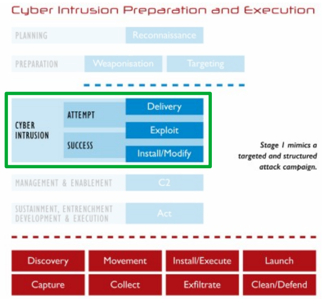
SANS Cyber Kill Chain for ICS – Stage 1

- **Preparatory phase**
  - ***Weaponisation***:
    - Modify innocuous files to embed exploits.
  - ***Target Identification***:
    - Analyse and prioritise potential victims.
  - ***Attack Strategy Development***:
    - Devise appropriate attack strategies.
  - ***Target Selection***:
    - Select the most suitable target.



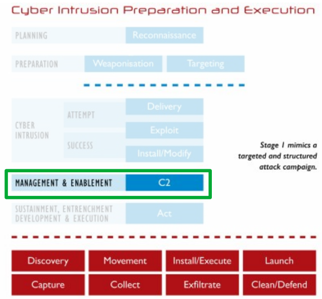
SANS Cyber Kill Chain for ICS – Stage 1

- **Cyber Intrusion phase**
  - ***Delivery***:
    - Deliver malicious payloads.
  - ***Exploitation***:
    - Exploit vulnerabilities in the target system.
  - ***Installation***:
    - Install malware or other tools.
  - ***Persistence***:
    - Take steps to ensure that access to the system is not easily detected or removed.



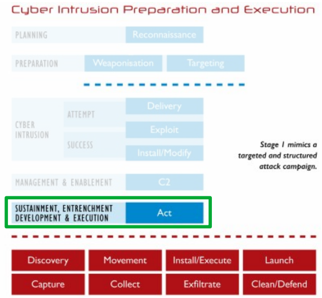
SANS Cyber Kill Chain for ICS – Stage 1

- **Management and Enablement phase**
  - ***Establishing C2***:
    - Establish a comms channel with the C2 server.
  - ***Maintaining C2***:
    - Establish multiple C2 paths.
  - ***Hiding C2***:
    - Hide C2 comms in normal outbound and inbound traffic.
  - ***Enabling access***:
    - Gain managed and enabled access to the environment.



SANS Cyber Kill Chain for ICS – Stage 1

- **Sustainment, Entrenchment, Development, and Execution phase**
  - Gather information
  - Move laterally within the network
  - Install additional capabilities
  - Launch attacks
  - Capture data
  - Exfiltrate data
  - Employ anti-forensic techniques.



SETU
Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

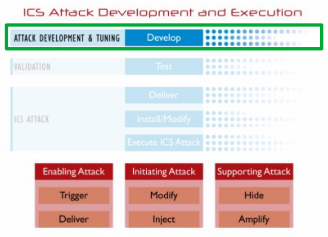
SANS

ICS Kill Chain

Stage 2

SANS Cyber Kill Chain for ICS – Stage 2

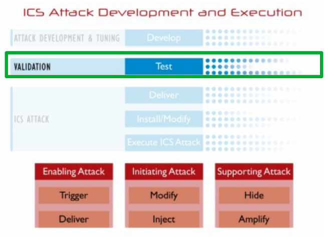
- **Attack Development and Tuning phase**
  - *Tailoring attack capabilities to specific vulnerabilities.*
  - *Utilising exfiltrated data to better understand the target system.*
  - *Limited live in-production testing due to the risk of detection.*
  - *The lack of live activity makes it difficult for defenders to detect adversary activities during Stage 2.*
  - *Delays between Stage 1 and Stage 2.*



Stage 2 shows the steps associated with a material attack that requires high confidence.

SANS Cyber Kill Chain for ICS – Stage 2

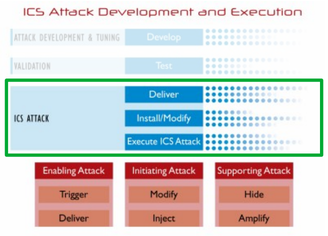
- **Validation phase**
  - *Attack code testing on similar or identically configured systems*.
  - *Importance of testing for precise timing and execution*.
  - *Physical ICS equipment or software component acquisition for complex attacks*.
  - *Difficulty of detecting attacker validation activities*.
  - *Government agencies' potential identification of unusual equipment acquisitions*.



Stage 2 shows the steps associated with a material attack that requires high confidence.

SANS Cyber Kill Chain for ICS – Stage 2

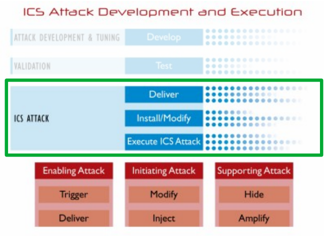
- **ICS Attack phase**
  - *Execution*.
  - *Attack components*.
  - *Spoofing state information*.
  - *Complexity of ICS attacks*.



Stage 2 shows the steps associated with a material attack that requires high confidence.

SANS Cyber Kill Chain for ICS – Stage 2

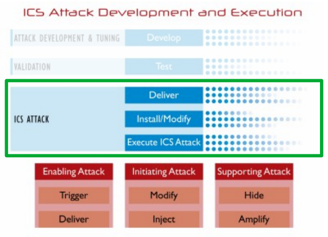
- **ICS Attack phase -** ICS attack types:
  - ***Loss***: Loss of view and of control.
  - ***Denial***: Denial of view, of control and of safety systems.
  - ***Manipulation***: Manipulation of view, of control, of sensors and instruments, and of safety systems.
  - ***Activation of safety systems***: Safety protocols are unconventionally triggered.



Stage 2 shows the steps associated with a material attack that requires high confidence.

SANS Cyber Kill Chain for ICS – Stage 2

- **ICS Attack phase –** Impact:
  - ***IT systems***: DoS attacks are disruptive to business operations.
  - ***ICS systems***: Manipulation of sensors or processes poses a significant threat to safety and human life.
  - ***Potential attack scenarios***:
    - Power grid failures
    - Dam overflows
    - Release of hazardous materials
    - Degradation of manufacturing products
    - Financial losses due to unusable product



Stage 2 shows the steps associated with a material attack that requires high confidence.

ICS Cyber Kill Chain summary

- A model that helps defenders understand the phases of an adversary's campaign into an ICS.
- Can be used to identify opportunities for detection, remediation, and defence.
- OT networks are more defensible than traditional IT networks, but it is important to maintain this defensible architecture by limiting the integration of safety systems with operations networks and removing ICS components from direct Internet access.

SANS Kill chain

According to the text, which of the following statements accurately describe the relationship between the SANS ICS Kill Chain, MITRE ATT&CK, and MITRE D3FEND frameworks? (Select all that apply)

□ MITRE D3FEND maps directly to ATT&CK to identify defensive verbs such as Decoy, Isolate, or Harden.

□ MITRE D3FEND focuses on the attack lifecycle to help understand the stages of an industrial cyber-attack.

□ MITRE ATT&CK provides a granular knowledge base of adversary Tactics, Techniques, and Procedures (TTP).

□ The SANS ICS Kill Chain is considered a specialised subset of the more expansive MITRE ATT&CK framework.

SANS Kill chain

According to the text, which of the following statements accurately describe the relationship between the SANS ICS Kill Chain, MITRE ATT&CK, and MITRE D3FEND frameworks? (Select all that apply)

- ☑ MITRE D3FEND maps directly to ATT&CK to identify defensive verbs such as Decoy, Isolate, or Harden.
- □ MITRE D3FEND focuses on the attack lifecycle to help understand the stages of an industrial cyber-attack.
- ☑ MITRE ATT&CK provides a granular knowledge base of adversary Tactics, Techniques, and Procedures (TTP).
- ☑ The SANS ICS Kill Chain is considered a specialised subset of the more expansive MITRE ATT&CK framework.

SANS Kill chain

Based on the description of Stage 2 of the SANS Cyber Kill Chain for ICS, which activities are typically performed by an adversary during this stage? (Select all that apply)

- □ Spoofing state information to maintain a facade of normality during execution.
- □ Validating attack code on similar or identically configured physical ICS equipment.
- □ Tailoring capabilities using exfiltrated data acquired during the first stage.
- □ Initial reconnaissance using OSINT tools like Google and Shodan.

SANS Kill chain

Based on the description of Stage 2 of the SANS Cyber Kill Chain for ICS, which activities are typically performed by an adversary during this stage? (Select all that apply)

- ☑ Spoofing state information to maintain a facade of normality during execution.
- ☑ Validating attack code on similar or identically configured physical ICS equipment.
- ☑ Tailoring capabilities using exfiltrated data acquired during the first stage.
- □ Initial reconnaissance using OSINT tools like Google and Shodan.

SANS Kill chain

Which of the following are recognised categories of ICS-specific attacks? (Select all that apply)

- □ Encryption of business databases for financial ransom.
- □ Loss of view where access to process information is prevented.
- □ Manipulation of sensors and instruments.
- □ Activation of safety systems through unconventional triggering of protocols.
- □ Distributed Denial-of-Service (DDoS) against the corporate marketing website.
- □ Exfiltration of customer credit card data from a retail server.

SANS Kill chain

Which of the following are recognised categories of ICS-specific attacks? (Select all that apply)

- ☐ Encryption of business databases for financial ransom.
- ☑ Loss of view where access to process information is prevented.
- ☑ Manipulation of sensors and instruments.
- ☑ Activation of safety systems through unconventional triggering of protocols.
- ☐ Distributed Denial-of-Service (DDoS) against the corporate marketing website.
- ☐ Exfiltration of customer credit card data from a retail server.

MITRE ATT&CK™ and D3FEND™

Introduction to MITRE frameworks

- MITRE US federally funded research organisation to solve complex national security and technical challenges since 1958.
- **ATT&CK**: a global knowledge base of real-world adversary TTPs to understand the "how" of cyberattacks.
- **D3FEND**: Provides a technical framework for Detection, Denial, and Disruption to map specific defensive actions against known threats.
- Together, these frameworks create a standardised language that allows organisations to bridge the gap between threat intelligence and active network defense.

Introduction to MITRE frameworks

Feature	MITRE ATT&CK	MITRE D3FEND
Focus	Adversary behaviour (offensive)	Defensive countermeasures (defensive)
Purpose	Understand how attackers operate	Understand how to defend against those operations
Content	TTPs of adversaries	Defensive techniques and countermeasures
Goal	Identify threats, assess risk, simulate attacks	Implement defences, mitigate attacks, improve posture
Perspective	Attacker's playbook	Defender's playbook

MITRE ATT&CK™ for ICS

setu.ie
INSPIRING FUTURES

Introduction to MITRE ATT&CK framework

- Developed by MITRE in 2013, to consider each stage of the cyberattack lifecycle from the perspective of the attacker
- Globally accessible knowledge base of adversary TTPs based on real-world observations
- Used as a foundation for the development of specific threat models and methodologies.

MITRE ATT&CK phases

- Reconnaissance
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Lateral Movement
- Collection
- Exfiltration

MITRE ATT&CK Reconnaissance phase

- **Discovery**
  - The attacker discovers information about the target and its environment.
- **Weaponisation**
  - The attacker prepares malware or exploits.
- **Delivery**
  - The attacker delivers the malware or exploit to the target.

MITRE ATT&CK Discovery tactic

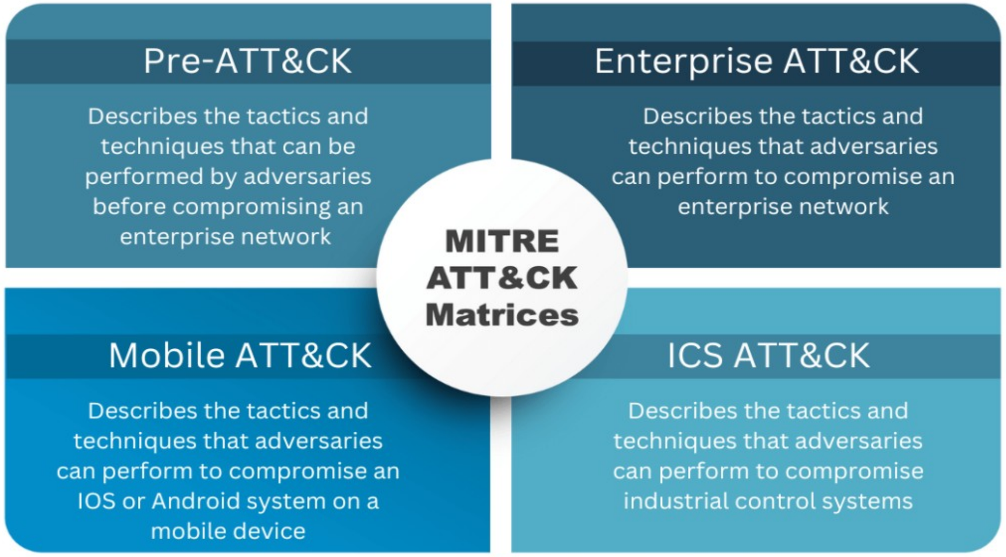
- **Network Mapping**
  - The attacker maps the target's network.
- **Data Credential Discovery**
  - The attacker discovers data and credentials.
- **Domain Discovery**
  - The attacker discovers the target's domain structure.

Benefits of using the MITRE ATT&CK framework

- Improved threat awareness
- Better threat detection
- More effective threat response
- Improved communication about threats.

The MITRE ATT&CK framework can be used for

- Threat modelling
- Threat intelligence
- Vulnerability assessment
- Incident response.



MITRE ATT&CK Matrices

Pre-ATT&CK

Describes the tactics and techniques that can be performed by adversaries before compromising an enterprise network

Enterprise ATT&CK

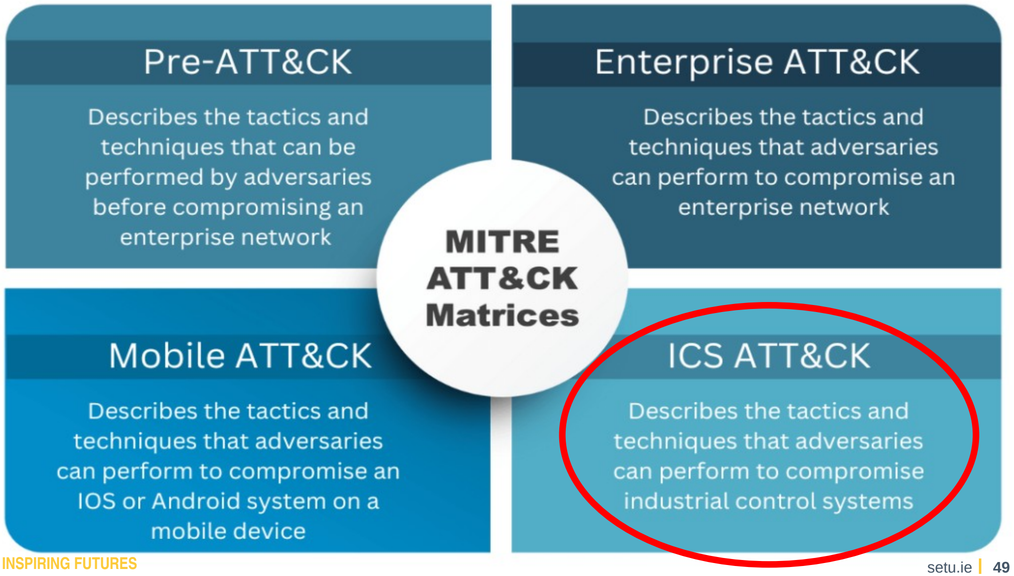
Describes the tactics and techniques that adversaries can perform to compromise an enterprise network

Mobile ATT&CK

Describes the tactics and techniques that adversaries can perform to compromise an IOS or Android system on a mobile device

ICS ATT&CK

Describes the tactics and techniques that adversaries can perform to compromise industrial control systems



Pre-ATT&CK

Describes the tactics and techniques that can be performed by adversaries before compromising an enterprise network

Enterprise ATT&CK

Describes the tactics and techniques that adversaries can perform to compromise an enterprise network

MITRE ATT&CK Matrices

Mobile ATT&CK

Describes the tactics and techniques that adversaries can perform to compromise an IOS or Android system on a mobile device

ICS ATT&CK

Describes the tactics and techniques that adversaries can perform to compromise industrial control systems

MITRE ATT&CK – Tactics

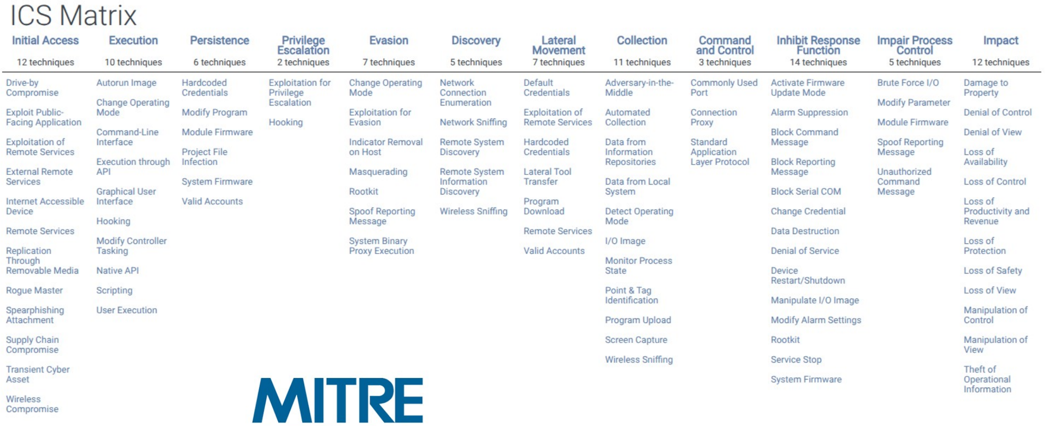
- 12 tactics employed in the framework
  - Each tactic cover the ***why*** of an attack
  - Tactics serve as a higher-level notation for the actions being carried out during an attack.

- TA0108 – Initial Access
- TA0104 – Execution
- TA0110 – Persistence
- TA0111 – Privilege Escalation
- TA0103 – Evasion
- TA0102 – Discovery
- TA0109 – Lateral Movement
- TA0100 – Collection
- TA0101 – Command and Control
- TA0107 – Inhibit Response Function
- TA0106 – Impair Process Control
- TA0105 – Impact

Ref: https://attack.mitre.org/matrices/ics/

MITRE ATT&CK – Techniques, Procedures & mitigations

- **Techniques**: Techniques cover the how and what an adversary gains when carrying out an action and can often be a single step in a string of activities to achieve goal.
- **Sub-Techniques**: Sub-techniques offer a granular description of a technique, are more specific in description and often platform or OS specific.
- **Procedures**: Procedures offer particular instances of how a technique or sub-technique has been used and can offer several additional behaviours in the way they are performed.
- **Mitigations**: Mitigations offer what to do when under attack so are countermeasures that may help prevent the adversary from achieving their goal.

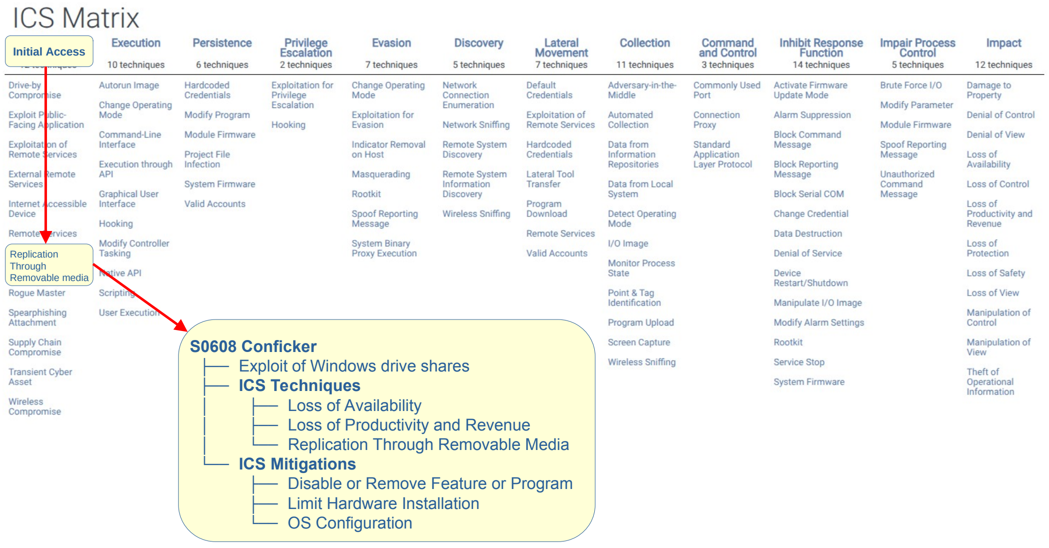


ICS Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

MITRE ATT&CK™ ICS

https://attack.mitre.org/matrices/ics/



ICS Matrix

Initial Access	Execution 10 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 7 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

S0608 Conficker

- Exploit of Windows drive shares
- **ICS Techniques**
  - Loss of Availability
  - Loss of Productivity and Revenue
  - Replication Through Removable Media
- **ICS Mitigations**
  - Disable or Remove Feature or Program
  - Limit Hardware Installation
  - OS Configuration

ATT&CK Example - Techniques

- Techniques of the tactic - TA0108 – Initial Access

- T0817 – Drive-by Compromise
- T0819 – Exploit Public-Facing Application
- T0866 – Exploitation of Remote Services
- T0822 – External Remote Services
- T0883 – Internet Accessible Device
- T0886 – Remote Services
- ***T0847 – Replication Through Removable Media***
- T0848 – Rogue Master
- T0865 – Spear-phishing Attachment
- T0862 – Supply Chain Compromise
- T0864 – Transient Cyber Asset
- T0860 – Wireless Compromise

ATT&CK Example - Procedures

- The ***T0847 – Replication Through Removable Media*** technique has two ***Procedures***
  - **S0608 – *Conficker, an exploit of Windows drive shares***
  - S0603 – Stuxnet, able to self-replicate by being spread through removable drives.

ATT&CK Example - Techniques

- The ***S0608 – Conficker, an exploit of Windows drive shares*** has three techniques associated with it for ICS
  - ICS T0826 – Loss of Availability
  - ICS T0828 – Loss of Productivity and Revenue
  - ICS T0847 – Replication Through Removable Media

ATT&CK Example - Mitigations

- The ***T0847 – Replication Through Removable Media*** technique can be mitigated by:
  - M0942 – Disable or Remove Feature or Program
    - Disable AutoRun
  - M0934 – Limit Hardware Installation
    - Limit hardware such as USB drives
  - M0928 – OS Configuration

ATT&CK Example - Detection

- The ***T0847 – Replication Through Removable Media*** exploit can be detected by:
  - DET0733 – Detection of Replication Through Removable Media
    - Analysis AN1866
      - Monitor for newly executed processes that execute from removable media after it is mounted or when initiated by a user. If a remote access tool is used in this manner to move laterally, then additional actions are likely to occur after execution, such as opening network connections for C2 and system and network information Discovery.
      - Monitor for newly constructed files copied to or from removable media.
      - Monitor for newly constructed drive letters or mount points to removable media.
      - Monitor for files accessed on removable media, particularly those with executable content.

Ollscoil Teicneolaíochta an Oirdheiscirt
SE TU
South East Technological University

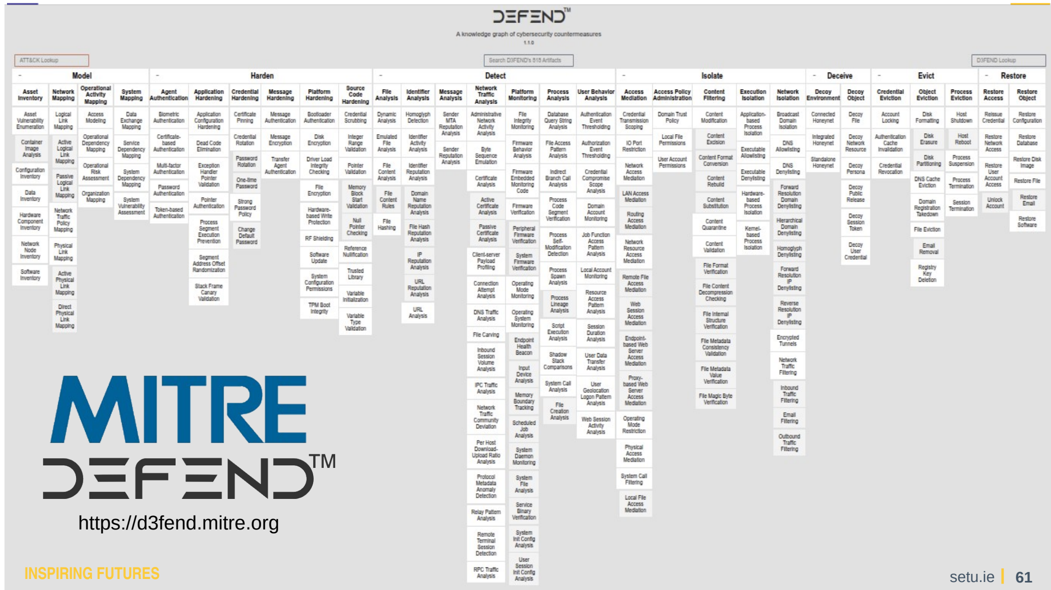
MITRE
D3FEND™

Introduction to MITRE **D3FEND** framework

- Developed by MITRE, and launched in 2025, as a knowledge graph of defensive cybersecurity countermeasures, complementing the ATT&CK framework.
- Provides a structured, systematic approach to implementing defensive measures that directly counter observed adversary TTPs.
- Used to design, implement, and validate threat-informed defence strategies, enhancing security posture and operational efficiency.

MITRE D3FEND™

Ref: https://d3fend.mitre.org



D3FEND™

A knowledge graph of cybersecurity countermeasures

1.1.0

ATT&CK Lookup

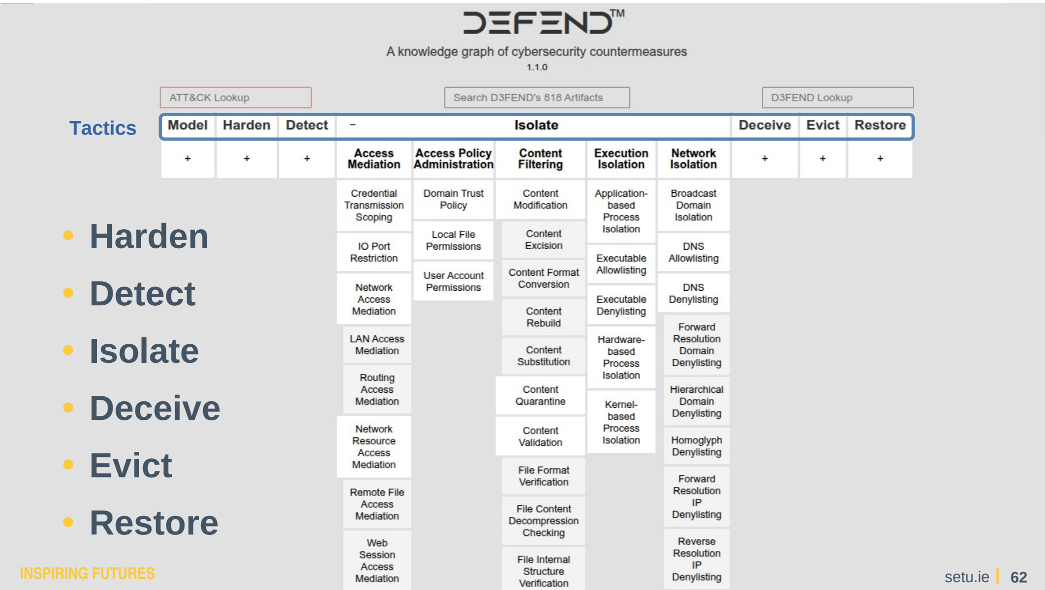
Search D3FEND's 818 Artifacts

D3FEND Lookup

- Model
  - **Asset Inventory**: Asset Vulnerability Enumeration; Container Image Analysis; Configuration Inventory; Data Inventory; Hardware Component Inventory; Network Node Inventory; Software Inventory
  - **Network Mapping**: Logical Link Mapping; Active Logical Link Mapping; Passive Logical Link Mapping; Network Traffic Policy Mapping; Physical Link Mapping; Active Physical Link Mapping; Direct Physical Link Mapping
  - **Operational Activity Mapping**: Access Modeling; Operational Dependency Mapping; Operational Risk Assessment; Organization Mapping
  - **System Mapping**: Data Exchange Mapping; Service Dependency Mapping; System Dependency Mapping; System Vulnerability Assessment
- Harden
  - **Agent Authentication**: Biometric Authentication; Certificate-based Authentication; Multi-factor Authentication; Password Authentication; Token-based Authentication
  - **Application Hardening**: Application Configuration Hardening; Dead Code Elimination; Exception Handler Pointer Validation; Pointer Authentication; Process Segment Execution Prevention; Segment Address Offset Randomization; Stack Frame Canary Validation
  - **Credential Hardening**: Certificate Pinning; Credential Rotation; Password Rotation; One-time Password; Strong Password Policy; Change Default Password
  - **Message Hardening**: Message Authentication; Message Encryption; Transfer Agent Authentication
  - **Platform Hardening**: Bootloader Authentication; Disk Encryption; Driver Load Integrity Checking; File Encryption; Hardware-based Write Protection; RF Shielding; Software Update; System Configuration Permissions; TPM Boot Integrity
  - **Source Code Hardening**: Credential Scrubbing; Integer Range Validation; Pointer Validation; Memory Block Start Validation; Null Pointer Checking; Reference Nullification; Trusted Library; Variable Initialization; Variable Type Validation
- Detect
  - **File Analysis**: Dynamic Analysis; Emulated File Analysis; File Content Analysis; File Content Rules; File Hashing
  - **Identifier Analysis**: Homoglyph Detection; Identifier Activity Analysis; Identifier Reputation Analysis; Domain Name Reputation Analysis; File Hash Reputation Analysis; IP Reputation Analysis; URL Reputation Analysis; URL Analysis
  - **Message Analysis**: Sender MTA Reputation Analysis; Sender Reputation Analysis
  - **Network Traffic Analysis**: Administrative Network Activity Analysis; Byte Sequence Emulation; Certificate Analysis; Active Certificate Analysis; Passive Certificate Analysis; Client-server Payload Profiling; Connection Attempt Analysis; DNS Traffic Analysis; File Carving; Inbound Session Volume Analysis; IPC Traffic Analysis; Network Traffic Community Deviation; Per Host Download-Upload Ratio Analysis; Protocol Metadata Anomaly Detection; Relay Pattern Analysis; Remote Terminal Session Detection; RPC Traffic Analysis
  - **Platform Monitoring**: File Integrity Monitoring; Firmware Behavior Analysis; Firmware Embedded Monitoring Code; Firmware Verification; Peripheral Firmware Verification; System Firmware Verification; Operating Mode Monitoring; Operating System Monitoring; Endpoint Health Beacon; Input Device Analysis; Memory Boundary Tracking; Scheduled Job Analysis; System Daemon Monitoring; System File Analysis; Service Binary Verification; System Init Config Analysis; User Session Init Config Analysis
  - **Process Analysis**: Database Query String Analysis; File Access Pattern Analysis; Indirect Branch Call Analysis; Process Code Segment Verification; Process Self-Modification Detection; Process Spawn Analysis; Process Lineage Analysis; Script Execution Analysis; Shadow Stack Comparisons; System Call Analysis; File Creation Analysis
  - **User Behavior Analysis**: Authentication Event Thresholding; Authorization Event Thresholding; Credential Compromise Scope Analysis; Domain Account Monitoring; Job Function Access Pattern Analysis; Local Account Monitoring; Resource Access Pattern Analysis; Session Duration Analysis; User Data Transfer Analysis; User Geolocation Logon Pattern Analysis; Web Session Activity Analysis
- Isolate
  - **Access Mediation**: Credential Transmission Scoping; IO Port Restriction; Network Access Mediation; LAN Access Mediation; Routing Access Mediation; Network Resource Access Mediation; Remote File Access Mediation; Web Session Access Mediation; Endpoint-based Web Server Access Mediation; Proxy-based Web Server Access Mediation; Operating Mode Restriction; Physical Access Mediation; System Call Filtering; Local File Access Mediation
  - **Access Policy Administration**: Domain Trust Policy; Local File Permissions; User Account Permissions
  - **Content Filtering**: Content Modification; Content Excision; Content Format Conversion; Content Rebuild; Content Substitution; Content Quarantine; Content Validation; File Format Verification; File Content Decompression Checking; File Internal Structure Verification; File Metadata Consistency Validation; File Metadata Value Verification; File Magic Byte Verification
  - **Execution Isolation**: Application-based Process Isolation; Executable Allowlisting; Executable Denylisting; Hardware-based Process Isolation; Kernel-based Process Isolation
  - **Network Isolation**: Broadcast Domain Isolation; DNS Allowlisting; DNS Denylisting; Forward Resolution Domain Denylisting; Hierarchical Domain Denylisting; Homoglyph Denylisting; Forward Resolution IP Denylisting; Reverse Resolution IP Denylisting; Encrypted Tunnels; Network Traffic Filtering; Inbound Traffic Filtering; Email Filtering; Outbound Traffic Filtering
- Deceive
  - **Decoy Environment**: Connected Honeynet; Integrated Honeynet; Standalone Honeynet
  - **Decoy Object**: Decoy File; Decoy Network Resource; Decoy Persona; Decoy Public Release; Decoy Session Token; Decoy User Credential
- Evict
  - **Credential Eviction**: Account Locking; Authentication Cache Invalidation; Credential Revocation
  - **Object Eviction**: Disk Formatting; Disk Erasure; Disk Partitioning; DNS Cache Eviction; Domain Registration Takedown; File Eviction; Email Removal; Registry Key Deletion
  - **Process Eviction**: Host Shutdown; Host Reboot; Process Suspension; Process Termination; Session Termination
- Restore
  - **Restore Access**: Reissue Credential; Restore Network Access; Restore User Account Access; Unlock Account
  - **Restore Object**: Restore Configuration; Restore Database; Restore Disk Image; Restore File; Restore Email; Restore Software

MITRE
D3FEND™

https://d3fend.mitre.org



D3FEND™

A knowledge graph of cybersecurity countermeasures

1.1.0

ATT&CK Lookup

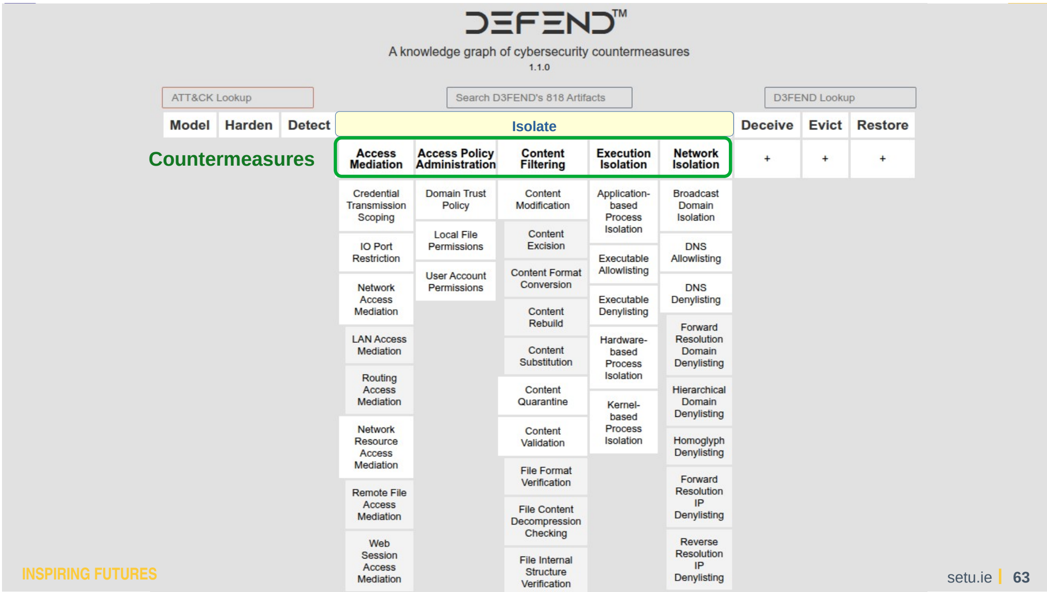
Search D3FEND's 818 Artifacts

D3FEND Lookup

Tactics

- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore

Model	Harden	Detect	Isolate					Deceive	Evict	Restore
+	+	+	**Access Mediation**	**Access Policy Administration**	**Content Filtering**	**Execution Isolation**	**Network Isolation**	+	+	+
			Credential Transmission Scoping	Domain Trust Policy	Content Modification	Application-based Process Isolation	Broadcast Domain Isolation			
			IO Port Restriction	Local File Permissions	Content Excision	Executable Allowlisting	DNS Allowlisting			
			Network Access Mediation	User Account Permissions	Content Format Conversion	Executable Denylisting	DNS Denylisting			
			LAN Access Mediation		Content Rebuild	Hardware-based Process Isolation	Forward Resolution Domain Denylisting			
			Routing Access Mediation		Content Substitution	Kernel-based Process Isolation	Hierarchical Domain Denylisting			
			Network Resource Access Mediation		Content Quarantine		Homoglyph Denylisting			
			Remote File Access Mediation		Content Validation		Forward Resolution IP Denylisting			
			Web Session Access Mediation		File Format Verification		Reverse Resolution IP Denylisting			
					File Content Decompression Checking					
					File Internal Structure Verification					



D3FEND™

A knowledge graph of cybersecurity countermeasures

1.1.0

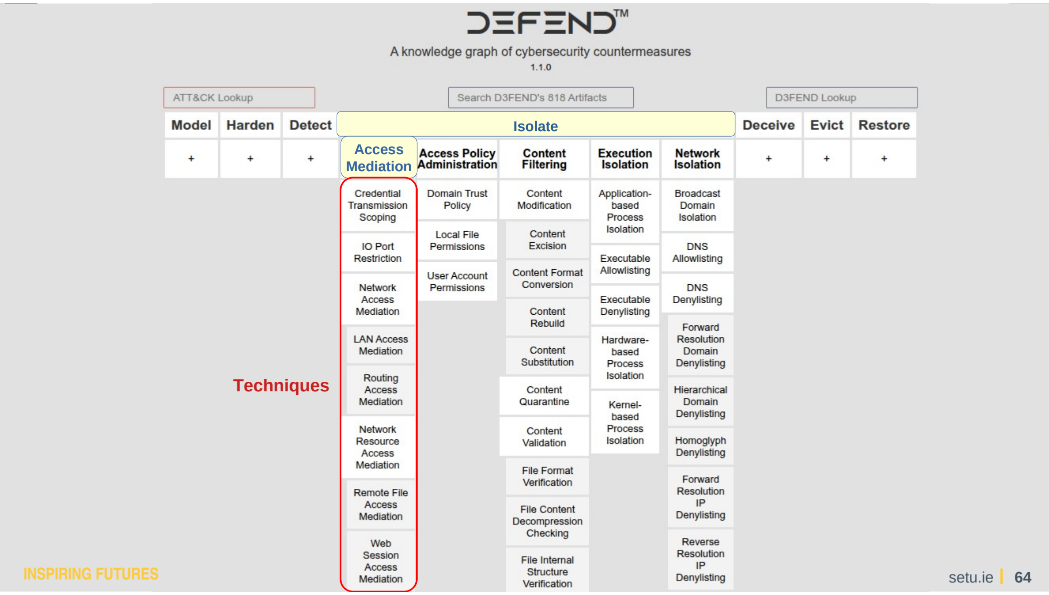
ATT&CK Lookup

Search D3FEND's 818 Artifacts

D3FEND Lookup

Countermeasures

Model	Harden	Detect	Isolate					Deceive	Evict	Restore
			Access Mediation	**Access Policy Administration**	**Content Filtering**	**Execution Isolation**	**Network Isolation**	+	+	+
			Credential Transmission Scoping	Domain Trust Policy	Content Modification	Application-based Process Isolation	Broadcast Domain Isolation			
			IO Port Restriction	Local File Permissions	Content Excision	Executable Allowlisting	DNS Allowlisting			
			Network Access Mediation	User Account Permissions	Content Format Conversion	Executable Denylisting	DNS Denylisting			
			LAN Access Mediation		Content Rebuild	Hardware-based Process Isolation	Forward Resolution Domain Denylisting			
			Routing Access Mediation		Content Substitution	Kernel-based Process Isolation	Hierarchical Domain Denylisting			
			Network Resource Access Mediation		Content Quarantine		Homoglyph Denylisting			
			Remote File Access Mediation		Content Validation		Forward Resolution IP Denylisting			
			Web Session Access Mediation		File Format Verification		Reverse Resolution IP Denylisting			
					File Content Decompression Checking					
					File Internal Structure Verification					



D3FEND™

A knowledge graph of cybersecurity countermeasures

1.1.0

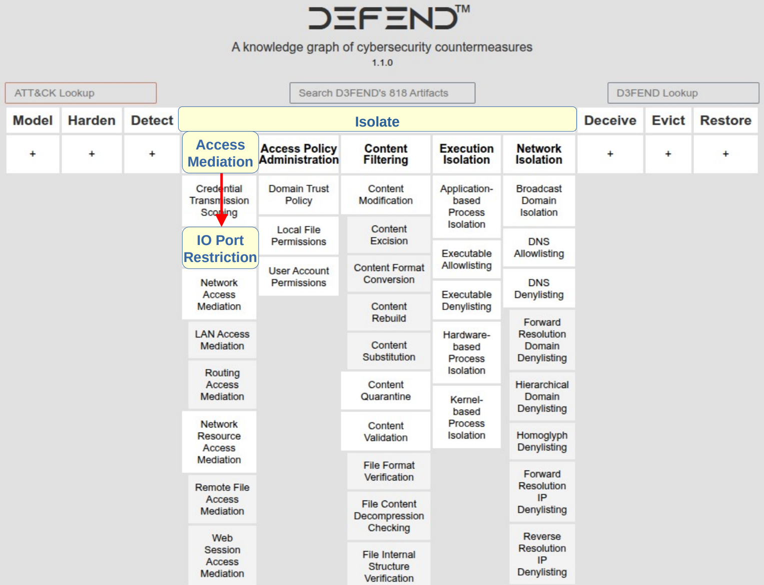
ATT&CK Lookup

Search D3FEND's 818 Artifacts

D3FEND Lookup

Techniques

Model	Harden	Detect	Isolate					Deceive	Evict	Restore
+	+	+	**Access Mediation**	**Access Policy Administration**	**Content Filtering**	**Execution Isolation**	**Network Isolation**	+	+	+
			Credential Transmission Scoping	Domain Trust Policy	Content Modification	Application-based Process Isolation	Broadcast Domain Isolation			
			IO Port Restriction	Local File Permissions	Content Excision	Executable Allowlisting	DNS Allowlisting			
			Network Access Mediation	User Account Permissions	Content Format Conversion	Executable Denylisting	DNS Denylisting			
			LAN Access Mediation		Content Rebuild	Hardware-based Process Isolation	Forward Resolution Domain Denylisting			
			Routing Access Mediation		Content Substitution	Kernel-based Process Isolation	Hierarchical Domain Denylisting			
			Network Resource Access Mediation		Content Quarantine		Homoglyph Denylisting			
			Remote File Access Mediation		Content Validation		Forward Resolution IP Denylisting			
			Web Session Access Mediation		File Format Verification		Reverse Resolution IP Denylisting			
					File Content Decompression Checking					
					File Internal Structure Verification					



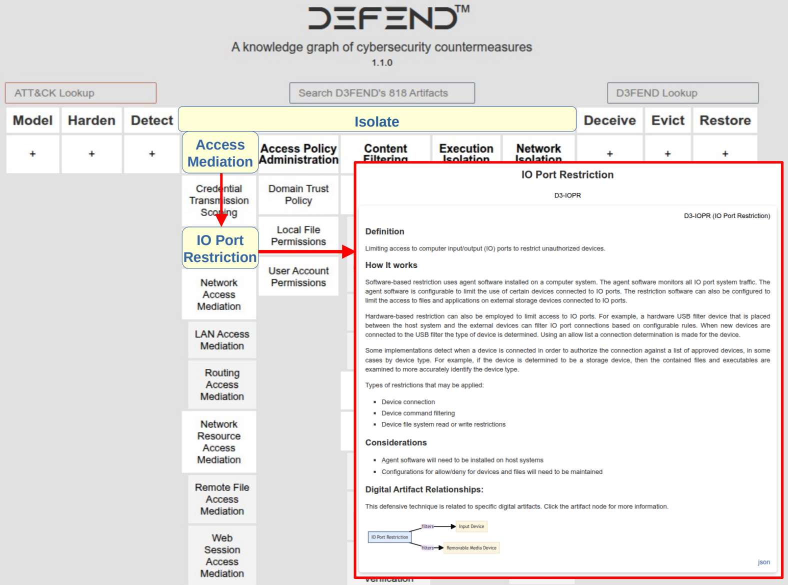
D3FEND™

A knowledge graph of cybersecurity countermeasures

1.1.0

ATT&CK Lookup | Search D3FEND's 818 Artifacts | D3FEND Lookup

Model	Harden	Detect	Isolate					Deceive	Evict	Restore
+	+	+	Access Mediation	Access Policy Administration	Content Filtering	Execution Isolation	Network Isolation	+	+	+
			Credential Transmission Scoping	Domain Trust Policy	Content Modification	Application-based Process Isolation	Broadcast Domain Isolation			
			IO Port Restriction	Local File Permissions	Content Excision	Executable Allowlisting	DNS Allowlisting			
			Network Access Mediation	User Account Permissions	Content Format Conversion	Executable Denylisting	DNS Denylisting			
			LAN Access Mediation		Content Rebuild	Hardware-based Process Isolation	Forward Resolution Domain Denylisting			
			Routing Access Mediation		Content Substitution	Kernel-based Process Isolation	Hierarchical Domain Denylisting			
			Network Resource Access Mediation		Content Quarantine		Homoglyph Denylisting			
			Remote File Access Mediation		Content Validation		Forward Resolution IP Denylisting			
			Web Session Access Mediation		File Format Verification		Reverse Resolution IP Denylisting			
					File Content Decompression Checking					
					File Internal Structure Verification					



D3FEND™

A knowledge graph of cybersecurity countermeasures

1.1.0

ATT&CK Lookup | Search D3FEND's 818 Artifacts | D3FEND Lookup

Model | Harden | Detect | Isolate | Deceive | Evict | Restore

Access Mediation | Access Policy Administration | Content Filtering | Execution Isolation | Network Isolation

Credential Transmission Scoping | Domain Trust Policy

IO Port Restriction | Local File Permissions

Network Access Mediation | User Account Permissions

LAN Access Mediation

Routing Access Mediation

Network Resource Access Mediation

Remote File Access Mediation

Web Session Access Mediation

IO Port Restriction

D3-IOPR

D3-IOPR (IO Port Restriction)

Definition

Limiting access to computer input/output (IO) ports to restrict unauthorized devices.

How It works

Software-based restriction uses agent software installed on a computer system. The agent software monitors all IO port system traffic. The agent software is configurable to limit the use of certain devices connected to IO ports. The restriction software can also be configured to limit the access to files and applications on external storage devices connected to IO ports.

Hardware-based restriction can also be employed to limit access to IO ports. For example, a hardware USB filter device that is placed between the host system and the external devices can filter IO port connections based on configurable rules. When new devices are connected to the USB filter the type of device is determined. Using an allow list a connection determination is made for the device.

Some implementations detect when a device is connected in order to authorize the connection against a list of approved devices, in some cases by device type. For example, if the device is determined to be a storage device, then the contained files and executables are examined to more accurately identify the device type.

Types of restrictions that may be applied:

- Device connection
- Device command filtering
- Device file system read or write restrictions

Considerations

- Agent software will need to be installed on host systems
- Configurations for allow/deny for devices and files will need to be maintained

Digital Artifact Relationships:

This defensive technique is related to specific digital artifacts. Click the artifact node for more information.

Map ATT&CK Mitigation to D3FEND Technique

MITRE ATT&CK™ ICS

M0934

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. This includes disabling USB ports, restricting driver installation, and implementing endpoint security tools to monitor and block unapproved devices. This mitigation can be implemented through the following measures:

ID: M1034

Version: 1.1

Created: 11 June 2019

Last Modified: 18 December 2024

MITRE D3FEND™

D3-IOPR

IO Port Restriction

Definition

Limiting access to computer input/output (IO) ports to restrict unauthorized devices.

How It works

Software-based restriction uses agent software installed on a computer system. The agent software monitors all IO port system traffic. The agent software is configurable to limit the use of certain devices connected to IO ports. The restriction software can also be configured to limit the access to files and applications on external storage devices connected to IO ports.

Hardware-based restriction can also be employed to limit access to IO ports. For example, a hardware USB filter device that is placed between the host system and the external devices can filter IO port connections based on configurable rules. When new devices are connected to the USB filter the type of device is determined. Using an allow list a connection determination is made for the device.

Some implementations detect when a device is connected in order to authorize the connection against a list of approved devices, in some cases by device type. For example, if the device is determined to be a storage device, then the contained files and executables are examined to more accurately identify the device type.

Types of restrictions that may be applied:

- Device connection
- Device command filtering
- Device file system read or write restrictions

SETU Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

MITRE Frameworks

In their capacity as planners and designers, how do Security Architects and Engineers utilise the MITRE ATT&CK and D3FEND frameworks according to the text? (Select all that apply)

- ☐ Assessing security posture and identifying defensive gaps.
- ☐ Designing and building robust defenses by identifying appropriate defensive techniques.
- ☐ Simulating real-world attacks to test an organisation's defenses.
- ☐ Ensuring comprehensive coverage against ATT&CK techniques by selecting specific countermeasures.
- ☐ Directly executing "Evict" tactics to remove adversaries from a compromised system.

MITRE Frameworks

In their capacity as planners and designers, how do Security Architects and Engineers utilise the MITRE ATT&CK and D3FEND frameworks according to the text? (Select all that apply)

- ☑ Assessing security posture and identifying defensive gaps.
- ☑ Designing and building robust defenses by identifying appropriate defensive techniques.
- ☐ Simulating real-world attacks to test an organisation's defenses.
- ☑ Ensuring comprehensive coverage against ATT&CK techniques by selecting specific countermeasures.
- ☐ Directly executing "Evict" tactics to remove adversaries from a compromised system.

MITRE Frameworks

Which of the following statements accurately describe the relationship between ATT&CK for ICS and D3FEND? (Select all that apply)

- ☐ D3FEND 1.0 includes additions for Operational Technology (OT) and source code hardening.
- ☐ There is a dedicated "D3FEND for ICS" matrix that mirrors the 12 ICS ATT&CK tactics.
- ☐ General D3FEND techniques such as anomaly detection and access control are often transferable to ICS environments.
- ☐ Organisations can leverage D3FEND by mapping its defensive techniques to specific ATT&CK for ICS techniques.

MITRE Frameworks

Which of the following statements accurately describe the relationship between ATT&CK for ICS and D3FEND? (Select all that apply)

- ☑ D3FEND 1.0 includes additions for Operational Technology (OT) and source code hardening.
- ☐ There is a dedicated "D3FEND for ICS" matrix that mirrors the 12 ICS ATT&CK tactics.
- ☑ General D3FEND techniques such as anomaly detection and access control are often transferable to ICS environments.
- ☑ Organisations can leverage D3FEND by mapping its defensive techniques to specific ATT&CK for ICS techniques.

MITRE Frameworks

In the context of the Stuxnet/Conficker example provided, which of the following are recognised methods for detecting or mitigating *Replication Through Removable Media* (TA0847)? (Select all that apply)

- ☐ Disabling AutoRun features (M0942).
- ☐ Implementing IO Port Restriction (D3-IOPR) to limit USB connectivity.
- ☐ Enforcing strong password complexity policies for local user accounts.
- ☐ Encrypting all files stored on the removable media.
- ☐ Monitoring for newly executed processes that run from removable media after mounting.

MITRE Frameworks

In the context of the Stuxnet/Conficker example provided, which of the following are recognised methods for detecting or mitigating *Replication Through Removable Media* (TA0847)? (Select all that apply)

- ☑ Disabling AutoRun features (M0942).
- ☑ Implementing IO Port Restriction (D3-IOPR) to limit USB connectivity.
- ☐ Enforcing strong password complexity policies for local user accounts.
- ☐ Encrypting all files stored on the removable media.
- ☑ Monitoring for newly executed processes that run from removable media after mounting.

Threat Modelling

Threat Model

- A threat model is a process that helps organisations identify, assess, and prioritise cybersecurity threats.
- It involves understanding the potential threats that an organisation faces, the likelihood of those threats being realised, and the potential impact of those threats if they are realised.
- Threat models can be used to inform security decisions, such as which security controls to implement and where to focus security resources.

Threat Models are used to

- Identifying and prioritising risks
- Developing security controls
- Communicating security risks
- Preparing for incidents.

Threat Models example

- Identify
  - Threat Actor(s)
    - Type
    - Motivation
    - Capabilities
  - Attack Vector
    - Method
    - Vulnerability
    - Exploit

Threat model
S0608 – *Conficker*, an exploit of Windows drive shares

Threat Actor

- **Type**: Advanced Persistent Threat (APT)
- **Motivation**: Gain unauthorised access to systems and networks to steal data, disrupt operations, or conduct espionage
- **Capabilities**: Highly skilled technical expertise, advanced tools and techniques, sophisticated attack methods

Attack Vector

- **Method**: Exploiting vulnerabilities in Windows drive shares
- **Vulnerability**: MS08-067, a vulnerability in the Server Message Block (SMB) protocol that allows attackers to execute arbitrary code on vulnerable systems
- **Exploit**: *Conficker*, a worm that exploits the MS08-067 vulnerability to spread to other systems through shared drives

Threat Models example

- Identify
  - Attack Path
    - Reconnaissance
    - Delivery
    - Exploitation
    - Installation
    - Persistence
    - Lateral Movement
    - Collection
    - Exfiltration

Attack Path

- **Reconnaissance:** The attacker gathers information about the target system, such as its network configuration and vulnerabilities.
- **Delivery**: The attacker sends a malicious file to the target system, often disguised as a legitimate file.
- **Exploitation**: When the victim opens the malicious file, the Conficker worm is executed, allowing the attacker to gain control of the system.
- **Installation**: The worm installs itself on the system and spreads to other systems through shared drives.
- **Persistence**: The worm creates persistence mechanisms to ensure that it remains active on the system even after reboots.
- **Lateral Movement**: The worm moves laterally through the network, infecting other systems and gaining access to sensitive data.
- **Collection**: The worm gathers sensitive data from the infected systems, such as personal information, financial data, and intellectual property.
- **Exfiltration**: The worm exfiltrates the stolen data to the attacker's command and control server.

Threat Models example

- Identify
  - Mitigation Strategies

Mitigation Strategies

- **Patch systems promptly**: Keep all systems patched with the latest security updates, including the MS08-067 patch.
- **Disable unnecessary shares**: Disable unnecessary network shares to reduce the attack surface.
- **Implement strong access controls**: Enforce strong access controls on shared drives, restricting access to authorised users only.
- **Use intrusion detection and prevention systems (IDS/IPS)**: Deploy IDS/IPS systems to detect and block malicious activity on the network.
- **Educate employees about cybersecurity threats**: Educate employees about cybersecurity threats and how to identify and avoid suspicious emails and attachments.
- **Implement a vulnerability management program**: Regularly scan systems for vulnerabilities and prioritise patching the most critical ones.
- **Use endpoint security solutions**: Deploy endpoint security solutions to detect and block malware infections.

Learning objectives

- Understand and apply the SANS Cyber Kill Chain for Industrial Control Systems (ICS) and MITRE **ATT&CK** and **D3FEND** frameworks to analyse real-world Operational Technology (OT) cyberattacks. ✓
- Identify and analyse the unique cybersecurity challenges faced by OT systems. ✓
- Develop comprehensive threat models for OT systems to identify, prioritise, and mitigate potential attack vectors. ✓
- Evaluate the effectiveness of OT security controls in preventing and mitigating cyber threats. ✓

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Exercise

Exercise 1: Applying ATT&CK

Student	Tactic	Technique
1	TA0108 – Initial Access	T0817 – Drive-by Compromise
2	TA0104 – Execution	T0807 – CLI
3	TA0110 – Persistence	T0889 – Modify Program
4	TA0111 – Privilege Escalation	T0890 – Exploit for Privilege Escalation
5	TA0103 – Evasion	T0820 – Exploit for Privilege Evasion
6	TA0102 – Discovery	T0842 – Network Sniffing
7	TA0109 – Lateral Movement	T0812 – Default Credentials
8	TA0100 – Collection	T0893 – Data from Local System
9	TA0101 – Command and Control	T0885 – Commonly Used Port
10	TA0107 – Inhibit Response Function	T0878 – Alarm Suppression
11	TA0106 – Impair Process Control	T0836 – Modify Parameter
12	TA0105 – Impact	T0815 – Denial of View
13	TA0108 – Initial Access	T0883 – Internet Accessible Device
14	TA0104 – Execution	T0823 – GUI
15	TA0110 – Persistence	T0873 – Project File Injection
16	TA0111 – Privilege Escalation	T0849 – Masquerading

Take Home

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

D +353 59 917 5000 | E diarmuid.obriain@setu.ie | **setu.ie**
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Thank you

engcore
advancing technology