Topic 2

SANS ICS Cyber Kill Chain, and the MITRE ATT&CK & D3FEND Frameworks

Dr Diarmuid Ó Briain

Version: 3.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Illustration Index

Index of Tables

1 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.

2 Introduction

The SANS Cyber Kill Chain for ICS provides a foundational, seven-phase model (Reconnaissance through Actions on Objectives) tailored specifically to the unique operational requirements of industrial systems. While the Kill Chain offers a high-level view of an adversary's progression, it is effectively a specialised subset of the more expansive MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework. ATT&CK serves as a globally accessible knowledge base of adversary Tactics, Techniques, and Procedures (TTP), offering a granular, real-world perspective on how attackers navigate an environment.

To move from understanding the threat to active neutralisation, security professionals utilise the MITRE Detection, Denial, and Disruption Framework Empowering Network Defence (D3FEND) framework. While ATT&CK catalogues offensive maneuvers, D3FEND is a technical knowledge base of defensive countermeasure techniques. It maps directly to ATT&CK, allowing defenders to identify specific defensive verbs, such as Decoy, Isolate, or Harden, that can interrupt an attacker's progress at any stage of the Kill Chain. Together, these three frameworks allow OT security professionals to model threats, identify vulnerabilities, and deploy precise technical safeguards to ensure operational resilience.

Table 1: The SANS Kill chain, MITRE ATT&CK and D3FEND 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.

3 SANS Cyber Kill Chain for ICS

3.1 What is a Kill Chain

A kill chain is a structured procedure for identifying, engaging, and neutralising an enemy to achieve a desired outcome. The US Department of Defence (DoD) targeting doctrine outlines the phases of this process as Find, Fix, Track, Target, Engage, Assess (F2T2EA):

1. **Find**: Locate suitable adversary targets for engagement
2. **Fix**: or pinpoint their exact location
3. **Track**: and monitor their movements
4. **Target**: Select the appropriate weapon or asset to produce the desired effects
5. **Engage**: the adversary
6. **Assess**: Evaluate the results.

This is a comprehensive, end-to-end process that is often referred to as a "chain" because any one breakdown in the sequence can halt the entire operation.

3.2 Advanced Persistent Threats

Conventional network defence tools, such as Intrusion Detection Systems (IDS) and anti-virus software, are designed to detect and respond to known vulnerabilities in computer systems. However, the increasing sophistication and persistence of cyberattacks have rendered these traditional approaches ineffective against Advanced Persistent Threats (APT).

APTs are meticulously planned and executed cyberattacks that involve well-resourced and skilled adversaries. These attackers target specific organisations with highly sensitive information, such as intellectual property, customer data, or government secrets, and employ advanced tools and techniques to evade detection and maintain access for extended periods.

Conventional IDS and anti-virus software often rely on signatures or patterns to identify malicious activity. However, APT attacks often employ zero-day exploits, vulnerabilities that are not known to software vendors and are therefore not yet patched. Additionally, APT attackers often use custom malware that is specifically designed to bypass traditional security defences.

Traditional network defence approaches, which primarily focus on protecting against known vulnerabilities, are becoming increasingly ineffective in the face of sophisticated cyber threats such as APTs. Instead of relying solely on signatures and

patterns to identify malicious activity, organisations must adopt a more proactive and intelligence-driven approach to cyber defence.

Intelligence-driven Computer Network Defence (CND) leverages knowledge about adversaries and their TTPs to create a feedback loop that empowers defenders to gain an information advantage over attackers. By understanding the stages of an attack, mapping adversary TTPs to appropriate defence measures, identifying patterns that link individual intrusions to broader campaigns, and continuously gathering intelligence, defenders can proactively anticipate and neutralise attacks.

Institutionalising an intelligence-driven CND approach significantly reduces the likelihood of successful intrusions, informs investment decisions in network defence resources, and provides valuable metrics to assess performance and effectiveness. This intelligence-based approach is crucial in the face of APTs, as it goes beyond vulnerability mitigation to address the threat component of risk as well.

3.3 The Intrusion Kill Chain

The intrusion kill chain is a framework, developed at Lockheed Martin, for understanding and preventing cyberattacks. It breaks down the attack process into a series of stages, each of which represents a specific goal that the attacker must achieve in order to succeed [1].

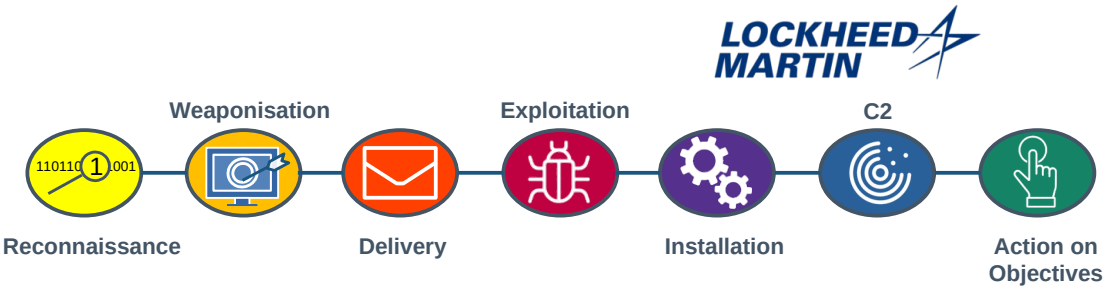


Figure 1: Intrusion Kill Chain

1. Reconnaissance

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

2. Weaponisation

Once the attacker has gathered enough information, they begin to develop a malicious payload. This payload is the code that will be used to exploit the vulnerabilities in the target system. The payload can be a variety of things, such as a virus, worm, or Trojan horse.

3. Delivery

The next step is to deliver the payload to the target system. This can be achieved in a variety of ways, such as through email, flash-drive, or network exploitation. The goal of delivery is to get the payload onto the target system so that it can be executed.

4. Exploitation

Once the payload is on the target system, the attacker attempts to exploit the vulnerabilities that they have identified. This involves using the payload to execute malicious code and gain access to the system.

5. Installation

After gaining access to the system, the attacker installs malware or other malicious software. This software gives the attacker control of the system and allows them to carry out their objectives.

6. Command and Control

The attacker establishes a Command and Control (C2) communication channel with the compromised system so they can control it remotely. This allows the attacker to steal data, install more malware, or launch other attacks.

7. Actions on Objectives

The final stage of the intrusion kill chain is where the attacker carries out their objectives. This could involve stealing data, disrupting operations, or damaging the system.

By aligning enterprise defensive capabilities with the specific processes an adversary undertakes to target that enterprise, the intrusion kill chain transforms into a model for actionable intelligence. Defenders can evaluate the performance and effectiveness of these actions, and devise investment roadmaps to address any capability gaps. At its core, this approach is the perfect example of intelligence-driven CND, which hinges on informed security decisions and measurements based on a deep comprehension of the adversary.

3.4 SANS Cyber Kill Chain for ICS

The SANS Cyber Kill Chain for ICS builds upon the foundation of the Lockheed Martin Intrusion Kill Chain, providing a more specific and nuanced framework for understanding and preventing cyberattacks on ICS. It expands upon the seven phases of the original kill chain, tailoring them to the unique characteristics and vulnerabilities of ICS environments. This more granular approach allows security professionals to develop targeted mitigation strategies that effectively address the specific risks posed by ICS cyberattacks [2].

3.4.1 Stage 1

The initial phase of an ICS cyberattack, as illustrated in Figure 2, bears resemblance to espionage or intelligence operations. It shares parallels to the actions covered in Lockheed Martin's Cyber Kill Chain, often aiming to acquire knowledge about the ICS, understanding the system, and establishing methods to breach internal perimeter safeguards or gain access to production environments.

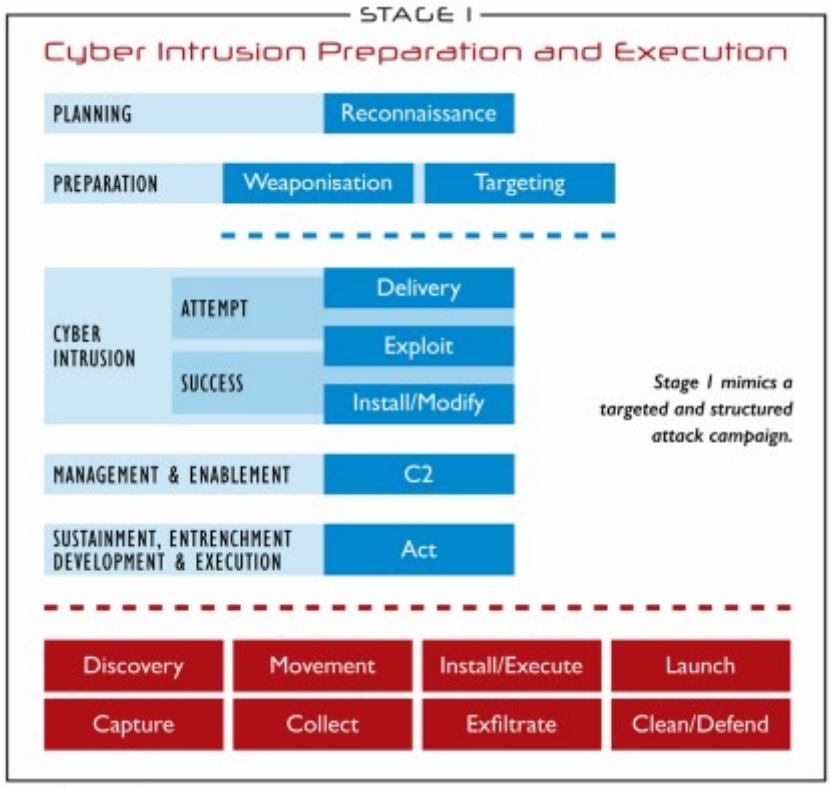


Figure 2: SANS Cyber Kill Chain - Stage 1

Planning phase: marks the commencement of the attack operation, initiated with reconnaissance efforts. Reconnaissance entails the meticulous gathering of information about the target, a process often facilitated by Open-Source INTelligence (OSINT) tools, such as Google and Shodan. These tools enable attackers to delve into publicly available data, including public announcements, social media profiles, and company websites.

The objective of this initial reconnaissance phase is to uncover weaknesses and identify information that can assist attackers in their subsequent targeting, delivery, and exploitation endeavours. This valuable information can encompass human, network, host, account, and protocol details, as well as insights into organisational policies, procedures, and processes.

For ICS environments, reconnaissance extends beyond basic information gathering. Attackers may meticulously research ICS technical vulnerabilities and features, seeking to understand the susceptibility of the target's processes and operating model to exploitation. Passive reconnaissance techniques, often referred to as foot-printing, capitalise on the vast volumes of information available online to discreetly gather intelligence about the target. This may involve mapping publicly or privately accessible attack surfaces, analysing activity patterns, and determining operating system software versions via routine queries.

Attackers often attempt to blend into the background noise of routine Internet traffic to conceal their reconnaissance activities. The publicly available information about organisations plays a significant role in shaping the target options available to adversaries, and defenders have no control over whether their organisations are deemed worthy of attack. Therefore, proactive measures to minimise the exposure of sensitive information and strengthen security posture are crucial for ICS environments.

Preparatory phase: comprises two crucial aspects: weaponisation and targeting. Weaponisation involves the deliberate modification of innocuous files, such as documents, to enhance their malicious capabilities. This often involves embedding exploits within files such as Portable Document Format (PDF) files, but it can also extend to exploiting inherent file features, such as macros in Microsoft Word documents.

Target identification and selection also occur during this phase. In military language, targeting entails analysing and prioritising potential victims, then devising appropriate attack strategies to achieve specific objectives. Cyber attackers make calculated decisions about the attack method based on a cost-benefit analysis, considering the effort required, likelihood of success, and risk of detection.

Weaponisation and targeting are not always mutually exclusive. In certain cases, attackers may uncover valid credentials for direct network access, eliminating the need for weaponisation. Alternatively, adversaries may weaponise their capabilities to target a broad range of potential victims, delaying the selection of a specific target until initial access is gained. This strategy offers greater flexibility and adaptability in the attack plan.

Cyber Intrusion phase: In this phase the attacker will attempt to infiltrate the defender's network or system. This encompasses the delivery of malicious payloads, such as phishing emails or exploits for existing access vulnerabilities. Once initial access is gained, attackers install capabilities like remote access Trojans to establish a persistent presence. Defenders should adopt a threat-informed approach to identify and mitigate intrusions, recognising that malware is not always the sole method employed by attackers.

Management and Enablement phase: After gaining initial access the attacker will establish C2, using methods such as a connection to the previously installed capability or abusing trusted communications such as the Virtual Private Network (VPN). Capable and persistent actors often establish multiple C2 paths to ensure connectivity is not interrupted if one is detected or removed. It is important to note that C2 methods do not always require a direct connection that supports a high frequency of bidirectional communication. Some access to protected networks, for example, may rely on one-way communication paths and require more time to move information out and deliver commands or code in.

Attackers often establish C2 by hiding in normal outbound and inbound traffic, hijacking existing communications. In some cases, attackers establish C2 by implanting equipment to establish their own communication bridge. With managed and enabled access to the environment, the adversary can now begin to achieve his or her goal.

Sustainment, Entrenchment, Development, and Execution phase: The adversary acts to achieve their goals. This may involve gathering information, moving laterally within the network, installing additional capabilities, launching attacks, capturing data, exfiltrating data, and employing anti-forensic techniques.

3.4.2 Stage 1 summary

Stage 1 is the most direct mapping to a breach in traditional Information Technology (IT) networks and can be bypassed if defenders have Internet-facing ICS components or information from a compromised third-party. In stage 1 of an ICS cyber attack the attacker carries out reconnaissance, preparation activities and and cyber intrusion such that they can establish C2.

ICS cyber attacks are unique because ICS components are designed for specific engineering and process requirements, making it difficult for attackers to exploit them without extensive knowledge. However, connecting ICS to the Internet directly undermines the inherent security advantages of a properly architected ICS. Defenders must carefully design and integrate systems to maintain these advantages. For instance, integrating safety systems into the same network as operations significantly reduces the attacker's effort and detection opportunities. With a well-designed ICS, even those with limited security features, attackers can find it challenging to achieve their goals. This underscores the importance of ICS security in preventing disruptions and safeguarding critical infrastructure.

3.4.3 Stage 2

Stage 2, as illustrated in Figure 3, presents the attacker with the opportunity to use the knowledge gained in Stage 1 to develop and test specific meaningful attacks on the ICS. Unfortunately, due to sensitive equipment it is possible that Stage 1 operations could lead to an unintended attack. This is a significant risk for a nation-state cyber operation because such an attack may be perceived as intentional and have unforeseen consequences. For example, an attempt to actively discover hosts on an ICS network may disrupt necessary communications or cause communication cards to fail. Simple interactions with ICS applications and infrastructure elements may result in unintentional outcomes. This activity would still be contained within Stage 1 and be an unintended effect in the Sustainment, Entrenchment, Development, and Execution phase. Intentional attacks take place in Stage 2 and are illustrated in Figure 3.

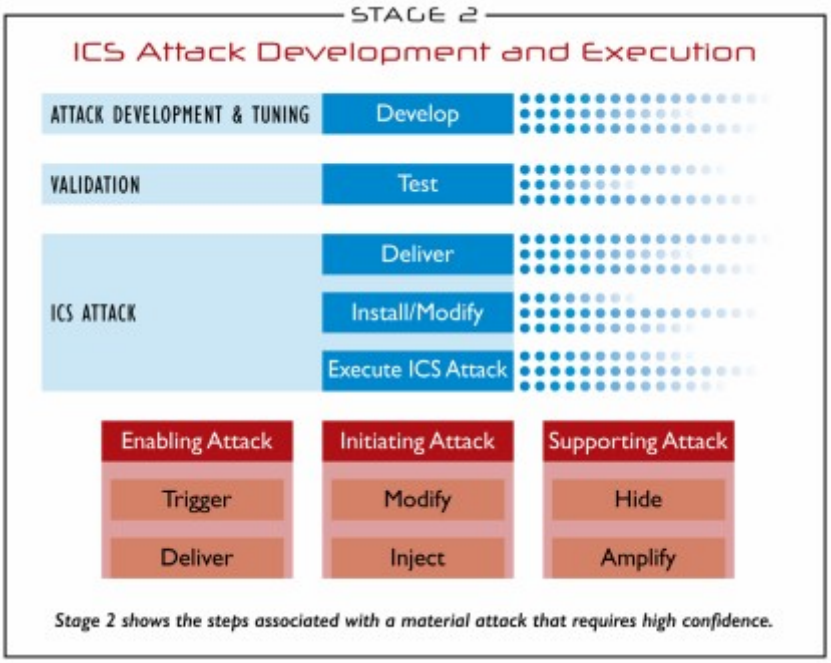


Figure 3: SANS Cyber Kill Chain - Stage 2

Attack Development and Tuning phase: Stage 2 of an ICS cyber attack involves attack development and tuning, where the attacker tailors their capabilities to exploit specific vulnerabilities in the target system and achieve their desired objectives. This development is often conducted using exfiltrated data, acquired during the first stage. Only highly confident attackers, with a low perception of defender awareness, will engage in live in-production testing of their attack code. This makes it challenging for defenders to detect adversary activities during this stage. Additionally, due to the need for extensive development and testing, there may be significant delays between the completion of Stage 1 and the initiation of Stage 2 operations.

Validation phase: After developing their attack capability, the attacker enters the Validation phase, where they test their code on similar or identically configured systems to ensure its effectiveness and reliability. This is crucial for attacks that require precise timing and execution, such as Denial-of-Service (DOS) attacks. For more complex or impactful attacks, the adversary may acquire physical ICS equipment or software components to conduct thorough testing. While this level of validation may be difficult for typical defenders to detect, government agencies with access to industry sources can potentially identify unusual equipment acquisitions, which could signal the start of Stage 2 operations following an established Stage 1 intrusion.

ICS Attack phase: The final stage of an ICS cyber attack is the Execution phase, where the adversary unleashes their tailored capabilities to achieve their desired objectives. This may involve multiple attack components, such as enabling, initiating, or supporting actions, to manipulate specific elements of the ICS process. Attackers may utilise tactics, such as spoofing state information, to deceive plant operators and maintain a facade of normality while carrying out their malicious activities.

The complexity of ICS attacks varies based on system security, process type, safety measures, and attacker objectives. Simple DoS attacks are easier, while manipulation and re-attacks are more difficult. Attackers aim to cause physical harm, equipment damage, formula modifications, or recipe manipulations.

Attacks on ICS systems can be categorised into four main types:

- **Loss**
  - **of view**: access is prevented to process information
  - **of control**: unintended process changes are caused
- **Denial**
  - **of view**: process information is misrepresented
  - **of control**: preventing manipulation of process parameters
  - **of safety systems**: prevention of safety systems activation
- **Manipulation**
  - **of view**: process information is altered
  - **of control**: specific process changes are forced
  - **of safety systems**: the modification of safety parameters
  - **of sensors and instruments**
- **Activation**
  - **of safety systems:** unconventional triggering of safety protocols

The impacts of ICS attacks differ from those on traditional IT systems. In IT, DoS can be disruptive to business operations, but in ICS, manipulation of sensors or processes can pose a significant threat to safety and human life.

ICS operations must understand the full range of potential attack scenarios, which extend beyond power grid failures and dam overflows. Attacks could also include the release of hazardous materials, degradation of manufacturing products, or financial losses due to unusable product. A proactive approach to the identification and assessment of potential attack scenarios is crucial for the development of effective mitigation strategies and minimising the impact of potential attacks.

3.5 Summary

The ICS Cyber Kill Chain is a model that helps defenders understand the phases of an adversary's campaign into an ICS. This model can be used to identify opportunities for detection, remediation, and defence. ICS 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.

4 The MITRE Corporation

The MITRE is a not-for-profit organisation that operates US federally funded research and development centres (FFRDC) for various U.S. government agencies. It was established in 1958 as a spin-off from Massachusetts Institute of Technology (MIT) Lincoln Laboratory, MITRE plays a role in advancing US national security, aviation, healthcare, and cybersecurity, among other fields. They are known for providing objective, data-driven solutions and technical expertise without commercial conflicts of interest, often tackling complex challenges that require a deep understanding of systems engineering and cutting-edge technology. Through initiatives such as the widely adopted Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and Detection, Denial, and Disruption Framework Empowering Network Defence (D3FEND) frameworks, MITRE has significantly contributed to the cybersecurity community by providing standardised knowledge bases that help organisations understand and defend against real-world adversarial behaviours.

4.1 MITRE ATT&CK and D3FEND Frameworks

The MITRE ATT&CK and D3FEND are two complementary cybersecurity frameworks each with a distinct focus.

4.1.1 MITRE ATT&CK

ATT&CK is a globally accessible knowledge base of adversary TTPs based on real-world observations. It describes how attackers operate across various stages of an intrusion (e.g., Initial Access, Execution, Persistence, Exfiltration). It's essentially a comprehensive "playbook" of what adversaries do.

The ATT&CK framework is applied by:

- **Red Teams/Penetration Testers**: to simulate real-world attacks and test an organisation's defences.
- **Threat Intelligence Analysts**: to understand adversary behaviour, enrich threat intelligence feeds, and identify specific threat actor groups and their methods.
- **Security Operations Centre (SOC) Analysts**: For intrusion detection, threat hunting, and correlating suspicious activities to known adversary techniques.
- **Security Architects and Engineers**: To assess security posture, identify defensive gaps, and prioritise security investments based on common attack vectors.
- **Incident Responders**: To quickly understand the methods used in an attack and guide response actions.
- **Risk Management Professionals**: To assess the likelihood and impact of specific attack techniques.

4.1.2 MITRE D3FEND

D3FEND is a knowledge graph of defensive cybersecurity countermeasures. It provides a structured, systematic approach to implementing defensive measures to counteract the adversarial TTPs documented in ATT&CK. It describes how defenders can respond to or prevent specific attacks.

Who should apply it:

- **Security Architects and Engineers**: To design and build robust defences, identify the appropriate defensive techniques for specific threats, and ensure comprehensive coverage against ATT&CK techniques.
- **Blue Teams/Defensive Security Teams**: To implement and optimise security controls, develop detection rules, and create SOC playbooks that directly counter observed or anticipated adversary behaviours.
- **Detection Engineers**: To map defensive capabilities to specific adversary tactics and techniques, pinpointing gaps in current defensive measures.
- **Organisations developing security products/solutions**: To standardise the vocabulary for describing defensive capabilities and to align their offerings with known threats.
- **Anyone seeking to establish a threat-informed defence**: By using D3FEND in conjunction with ATT&CK, organisations can build security strategies that are directly aligned with real-world threat behaviours.

Table 2: Comparison of MITRE ATT&CK and D3FEND 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

5 MITRE ATT&CK for ICS

5.1 What is ATT&CK?

ATT&CK is a framework that categorises cyber attacks into TTPs, specific actions or steps that attackers take to achieve their goals [3]. The framework offers extensive information that previously was only available from documented APTs or through the experiences that security personnel had gained from lived incidents [4].

ATT&CK is organised into eight phases:

- **Reconnaissance**: The attacker gathers information about the target.
- **Initial Access**: The attacker gains access to the target's network or system.
- **Execution**: The attacker executes code on the target's system.
- **Persistence**: The attacker makes sure that they can maintain access to the target's system.
- **Privilege Escalation**: The attacker gains higher levels of access on the target's system.
- **Lateral Movement**: The attacker moves laterally within the target's network.
- **Collection**: The attacker collects data from the target's system.
- **Exfiltration**: The attacker exfiltrates data from the target's system.

Each phase of the ATT&CK framework is divided into tactics, which are high-level goals that attackers pursue. For example, the **Reconnaissance phase** has the following tactics:

- **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.

Each tactic is then divided into techniques, which are specific actions or steps that attackers take to achieve their goals. For example, the **Discovery tactic** has the following techniques:

- **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.

There are many benefits to using ATT&CK, including:

- **Improved threat awareness**: ATT&CK can help organisations to understand the TTPs that attackers use, which can help them to identify and defend against attacks.
- **Better threat detection**: ATT&CK can be used to develop threat detection signatures and rules.
- **More effective threat response**: ATT&CK can be used to develop incident response playbooks.
- **Improved communication about threats**: ATT&CK is a common language that can be used to communicate about threats between different organisations.

ATT&CK can be used for:

- **Threat modelling**: ATT&CK can be used to model the threats that an organisation faces.
- **Threat intelligence**: ATT&CK can be used to collect and analyse threat intelligence.
- **Vulnerability assessment**: ATT&CK can be used to assess an organisation's vulnerabilities to specific TTPs.
- **Incident response**: ATT&CK can be used to guide incident response activities.

6 MITRE ATT&CK Matrices

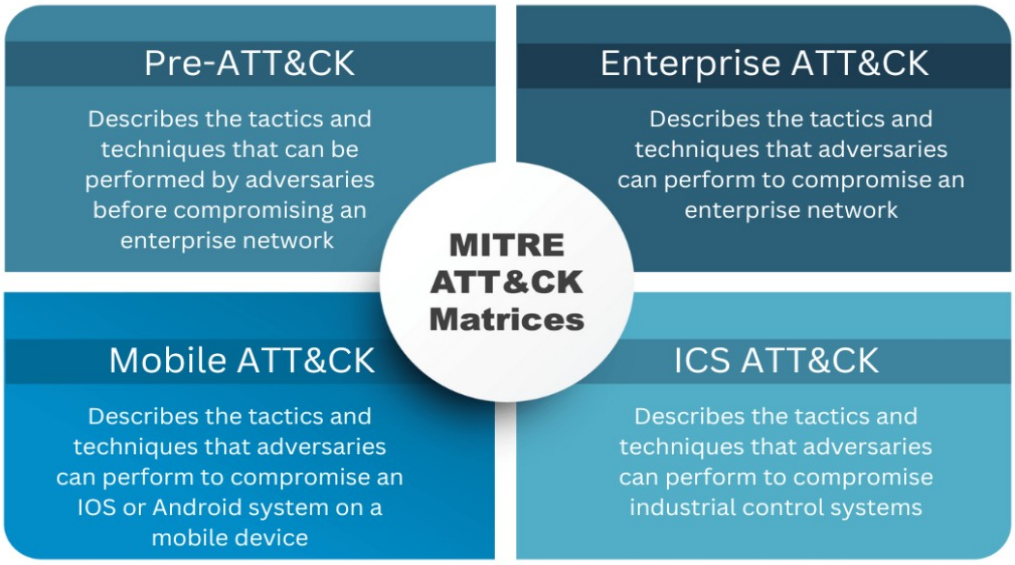


Figure 4: MITRE ATT&CK Matrices

Figure 4 is a diagram that illustrates the different types of cyber attacks. It is divided into four main categories:

1. **Pre-ATT&CK** describes the tactics and techniques that can be performed by adversaries before compromising an enterprise network. This includes things such as reconnaissance, weaponisation, and delivery.
2. **Enterprise ATT&CK** describes the tactics and techniques that adversaries can perform to compromise an enterprise network. This includes things such as exploitation, installation, persistence, and credential access.
3. **Mobile ATT&CK** describes the tactics and techniques that adversaries can perform to compromise an iOS or Android system on a mobile device. This includes things such as reconnaissance, exploitation, and credential access.
4. **ICS ATT&CK** describes a specialised version of the MITRE ATT&CK framework that is designed for understanding and defending against cyberattacks on ICS.

The MITRE ATT&CK framework and matrices are valuable tools for understanding cyber attacks. It can help organisations to identify and defend against attacks by providing a common language and taxonomy for discussing threat intelligence.

6.1 Pre-ATT&CK

The attacker begins by gathering information about the target, such as their network infrastructure, security posture, and employee habits. To achieve this social engineering techniques may be employed to trick employees into revealing sensitive information or clicking on malicious links. Once enough information has been gathered, the attacker will prepare the attack through activities such as developing malware, creating phishing emails, or exploiting vulnerabilities in the target's systems.

6.2 Enterprise ATT&CK

The attacker delivers their attack to the target's network or system, typically through phishing emails, exploiting vulnerabilities, or using stolen credentials. Once access has been gained to the target's system, they will try to establish persistence. This means making sure that they can maintain access to the system even after the initial attack.

The next step for the attacker is to try escalate privileges. This means gaining higher levels of access to the system, such as administrator privileges facilitating movement laterally within the target's network, moving from one system to another without being detected.

At this stage the attacker will then collect data from the target's system, typically including sensitive information such as personal data, financial data, or intellectual property.

As a final step data will be exfiltrated from the target's system. This may be achieved by sending it to a remote server or copying it to a removable storage device.

6.3 Mobile ATT&CK

Similarly to the Enterprise ATT&CK, the attacker begins by gathering information about the target's mobile device. This may include the device's model, operating system, and applications. Again, as with enterprise systems, once the attacker has gathered enough information, they will prepare the attack typically by developing malware, creating phishing emails, or exploiting vulnerabilities in the device's operating system.

The attack is then delivered to the target's mobile device, typically through phishing emails, exploiting vulnerabilities, or using stolen credentials. Once access has been gained access to the target's device, the attacker will try to establish persistence by making sure that they can maintain access to the device even after the initial attack.

The attacker will then try to escalate to root privileges and with this level of access, they will then move laterally within the device, moving from one app to another without being detected.

The attacker will then collect data such as personal data, financial data, or location data, from the device.

Finally, the attacker will exfiltrate the data from the device by sending it to a remote server or copying it to a removable storage device.

7 MITRE ATT&CK for ICS[1]

MITRE ATT&CK for ICS is the subject of this topic [5] [6]. The ATT&CK framework for ICS environment is separate to the enterprise level framework as the technologies employed are different. Attacks, on ICS, follow a different methodology and motivation from enterprise attackers. ATT&CK for ICS was initially released in January 2020, with the current version 14 released on October 31st, 2023. This offers focus on 12 separate tactics, 81 techniques as well as 52 different mitigations. Here is a list of the 12 tactics employed in the framework:

- 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

Each Tactic cover the ***why*** of an attack, the objective of performing an attack. Tactics serve as a higher-level notation for the actions being carried out during an attack, such as privilege escalation. Each tactic has documented Techniques and Procedures to implement the tactic and mitigations to prevent the attack.

- **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. Each tactic category contains multiple techniques being used to gain the tactical advantage.
- **Sub-Techniques:** Sub-techniques offer a granular description of a technique, are more specific in description and often platform or operating system 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.

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

- **Mitigations:** Mitigations offer ***what to do*** when under attack so are countermeasures that may help prevent the adversary from achieving their goal.

7.1 Example

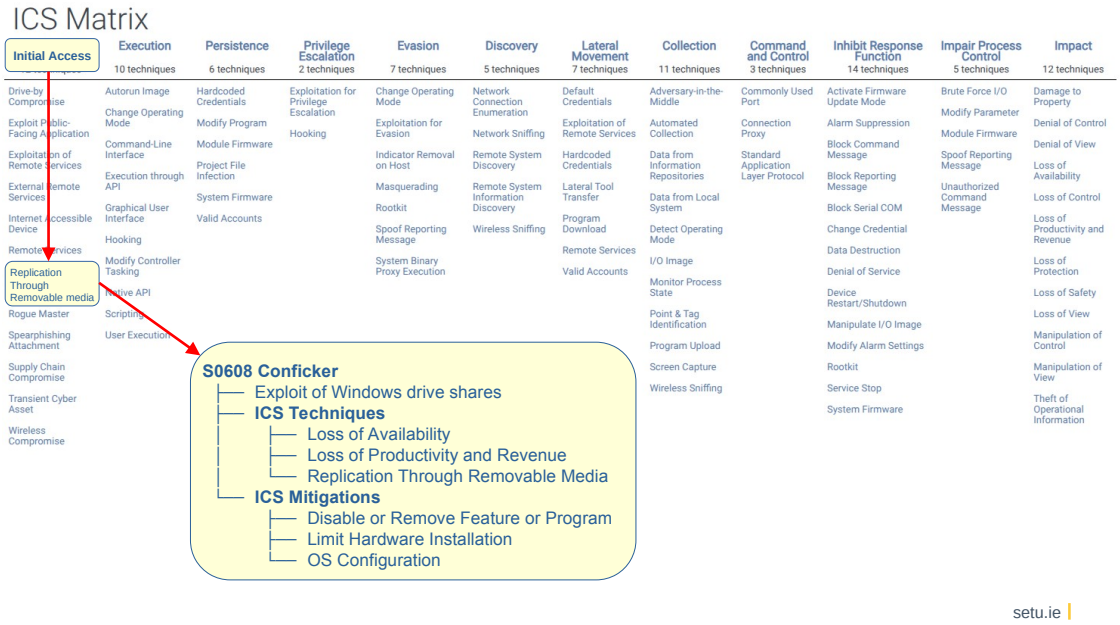


Figure 5: ATT&CK for ICS Matrix

Taking the ***TA0108 – Initial Access***, consider the ***Techniques*** used for this Tactic.

- 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

From these Techniques explore the ***T0847 – Replication Through Removable Media*** procedures. There are two, for the purpose of the exercise select:

- ***S0608 – Conficker, an exploit of Windows drive shares***
- S0603 – Stuxnet, able to self-replicate by being spread through removable drives.

Information on this computer worm can be accessed. Three techniques, within the ICS domain, can be found:

- ICS T0826 – Loss of Availability
- ICS T0828 – Loss of Productivity and Revenue
- ICS T0847 – Replication Through Removable Media

For example, ICS T0847 was the cause of a shutdown of the Gundremmingen nuclear power plant in Germany in 2016, on Chernobyl's 30th anniversary. RWE, the plant's operator, shut down the power plant as a precaution. On this occasion, the malware affected only the computer IT systems and not the ICS or Supervisory Control and Data Acquisition (SCADA) equipment that interacts with the nuclear fuel.

This **Conficker exploit** 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

If it does happen, a **Conficker attack** 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.

8 MITRE D3FEND[2]

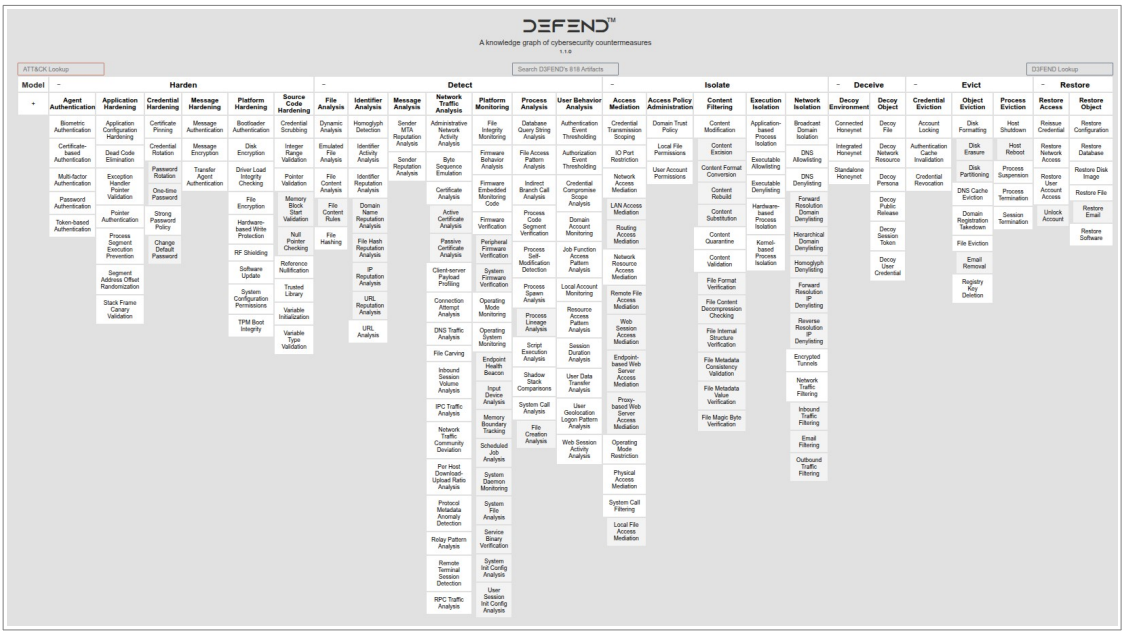


Figure 6: MITRE D3FEND Framework

8.1 What is D3FEND?

D3FEND is a framework that categorises defensive cybersecurity countermeasures into a knowledge graph, detailing specific defensive techniques and their relationships to adversarial actions. The framework offers extensive information that previously was only available from documented security best practices or through the experiences that security personnel had gained from implementing defences in lived incidents.

D3FEND is organised into seven high-level categories, or tactics, that align with the defensive lifecycle:

- **Model:** Generating a common understanding of systems, operations, users, and relationships that act as the foundation of other security and risk management activities.
- **Harden:** Techniques that reduce the attack surface and strengthen system configurations.
- **Detect:** Techniques that identify and alert on adversarial activity.
- **Isolate:** Techniques that contain or limit the impact of an attack.
- **Deceive:** Techniques that mislead or trick attackers.
- **Evict:** Techniques that remove adversaries from a compromised system or network.
- **Restore:** Techniques for returning the system to a better state after an incident.

2 https://d3fend.mitre.org

Each category of the D3FEND framework is divided into **defensive countermeasures**, which are high-level strategies for defence. For example, the Harden category has countermeasures such as:

- **Application Hardening:** Strengthening the security of software applications.
- **Operating System Hardening:** Securing the underlying operating system.
- **Network Hardening:** Improving the security of network infrastructure.

Each defensive countermeasure is then divided into **techniques**, which are specific actions or steps that defenders take to achieve their goals. For example, the Application Hardening countermeasure has the following techniques:

- **Executable Deny-listing:** Preventing the execution of unauthorised programs.
- **File Hashing:** Verifying the integrity of files.
- **Input Validation:** Ensuring that user input conforms to expected formats to prevent injection attacks.

There are many benefits to using D3FEND, including:

- **Improved defensive posture:** D3FEND can help organisations to understand and implement comprehensive defensive measures against known adversary TTPs.
- **Better security control mapping:** D3FEND can be used to map existing security controls to specific defensive techniques, identifying gaps in coverage.
- **More effective security architecture:** D3FEND can be used to design security architectures that are directly informed by threat intelligence.
- **Improved communication about defences:** D3FEND is a common language that can be used to communicate about defensive capabilities within and between organisations.

D3FEND can be used for:

- **Threat-informed defence:** D3FEND can be used in conjunction with ATT&CK to build defences directly aligned with adversary behaviours.
- **Security control gap analysis:** D3FEND can be used to identify where defensive measures are lacking.
- **Defensive playbook development:** D3FEND can be used to guide the creation of playbooks for various defensive scenarios.
- **Cybersecurity education and training:** D3FEND provides a structured way to understand and teach defensive concepts.

8.2 D3FEND and ICS

D3FEND's primary focus is on **enterprise defence**, and its techniques are generally applicable across various IT environments. However, D3FEND 1.0, released in 2021, did include some **additions for operational technology (OT)** and concepts such as source code hardening, which indicates an awareness and consideration of ICS-related defensive needs.

While there isn't a dedicated "D3FEND for ICS" matrix, organisations working with ICS environments can still leverage the existing D3FEND framework by:

- **Mapping to ATT&CK for ICS:** The core idea of D3FEND is to provide countermeasures for ATT&CK techniques. Therefore, when a specific ATT&CK for ICS technique is identified that an adversary might use, the general D3FEND framework can be considered for corresponding defensive techniques that could mitigate or prevent that attack, even if those D3FEND techniques aren't specifically labelled "for ICS".
- **General Applicability:** Many defensive techniques described in D3FEND, such as network hardening, anomaly detection, and access control, are highly relevant and transferable to ICS environments, even if their implementation details might differ due to the unique characteristics of OT.
- **Community and Future Development:** MITRE is an evolving organisation, and frameworks like D3FEND are continuously updated based on community feedback and emerging threats. It's possible that a more explicit "D3FEND for ICS" matrix could be developed in the future if there's sufficient demand and research.

In essence, while ATT&CK explicitly differentiates between enterprise and ICS attack patterns, D3FEND aims for a more universal set of defensive principles that can be applied across different environments, with an increasing awareness of OT considerations.

8.2.1 D3FEND against an ATT&CK Technique

Consider the ATT&CK technique **T0847 – Replication Through Removable Media** that was looked at earlier.

ATT&CK Technique

T0847 – Replication Through Removable Media

Adversaries may replicate themselves on removable media (e.g., USB sticks, external hard drives) to propagate across systems when the media is connected to other computers. This often involves placing malicious files or autorun configurations on the media.

The adversary’s goal is to gain initial access to new systems, establish persistence, or move laterally within air-gapped or segmented networks.

This technique has a mitigation **M0934 - Limit Hardware Installation**.

Consider a D3FEND technique that addresses the ATT&CK mitigation **M0934**. One of the most effective ways to counter T0847 is through prevention and reduction of the attack surface, which aligns perfectly with the D3FEND **Isolate** tactic.

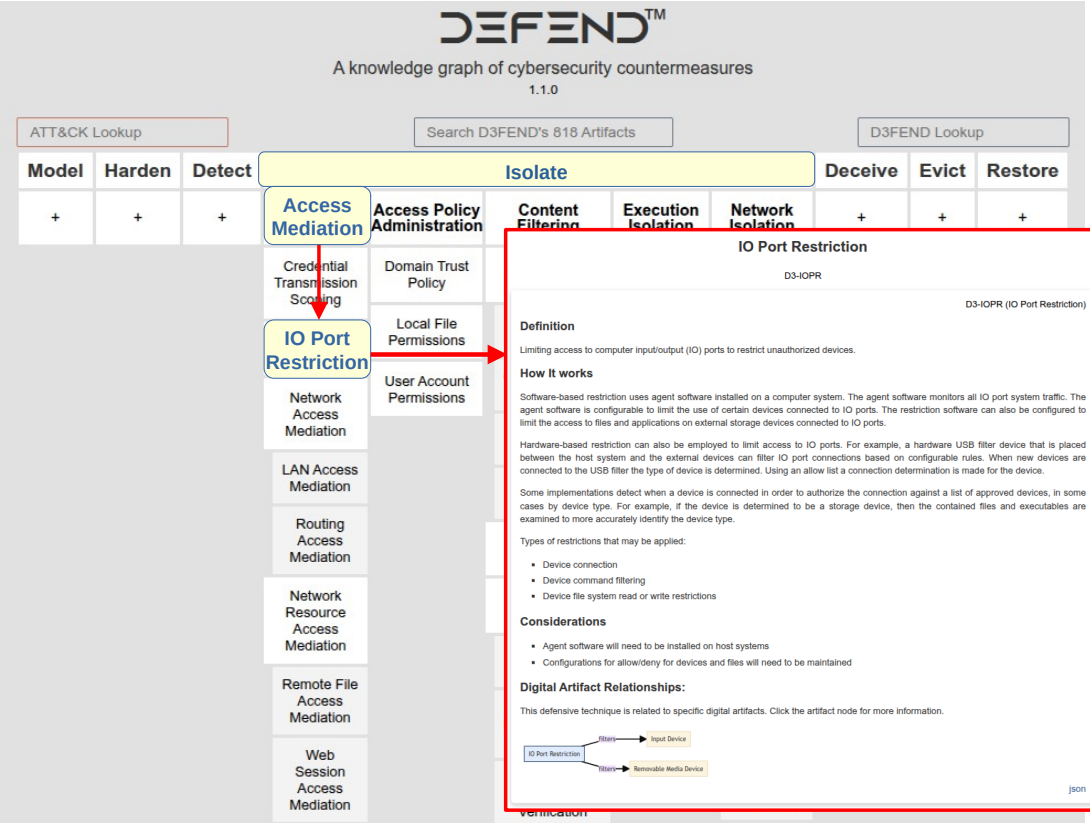


Figure 7: Platform Hardening D3FEND Technique

The **IO Port Restriction (D3-IOPR)** technique is found under the **Isolate** tactic's **Access Mediation** countermeasure. It limits unauthorised device connectivity and data transfer by controlling system input/output ports to contain adversarial activity. Breaking this down by **Tactic** > **Countermeasure** > **Technique** within the D3FEND framework.

- **Tactic: Isolate**
  - Techniques aimed at containing or limiting the impact of adversarial activity by segmenting or restricting access within a system or network.
- **Countermeasure: Access Mediation**
  - These are a set of techniques that enforce control over how subjects (users, processes) interact with objects (resources, data) at runtime, preventing unauthorised or malicious access.
- **Technique: IO Port Restriction (D3-IOPR)**
  - Preventing or controlling the use of specific input/output ports (e.g., USB, FireWire, optical drives) on a system to limit unauthorised device connectivity and data transfer.

9 Threat Models

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.

A threat model can be used for a variety of purposes, including:

- **Identifying and prioritising risks**: Threat models can help organisations to identify the most serious risks they face and to prioritise their security efforts accordingly.
- **Developing security controls**: Threat models can be used to develop specific security controls to mitigate the identified risks.
- **Communicating security risks**: Threat models can be used to communicate security risks to stakeholders, such as senior management and board members.
- **Preparing for incidents**: Threat models can be used to develop incident response plans to respond to security incidents.

By implementing mitigation strategies, such as those identified in Figure 5 for *Conficker*, organisations can significantly reduce their risk of being compromised by this computer worm and other similar attacks.

9.1 Sample threat model

Threat model

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

Threat Actor

- **Type**: 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

ATT&CK Attack Path

- **Reconnaissance** (TA0043):
  - The attacker gathers information about the target system, such as its network configuration and vulnerabilities (e.g., identifying open SMB ports, unpatched systems).
  - ATT&CK Technique: T1595 - Active Scanning (e.g., Network Scanning for open SMB ports).
- **Initial Access** (TA0001):
  - The attacker gains initial access to the target system by exploiting the MS08-067 vulnerability via exposed Windows drive shares.
  - ATT&CK Technique: T1210 - Exploitation of Remote Services (specifically targeting the SMB vulnerability).
- **Execution** (TA0002):
  - Upon successful exploitation, the Conficker worm is executed, allowing the attacker to gain control of the system.
  - ATT&CK Technique: T1569.002 - System Services: Service Execution (Conficker often creates and starts a service to execute its payload).
- **Installation** (TA0003) & **Persistence** (TA0003):
  - The worm installs itself on the system and creates persistence mechanisms to ensure it remains active even after reboots. It then spreads to other systems through shared drives.
  - ATT&CK Technique (Installation/Persistence): T1543.003 - Create or Modify System Process: Windows Service (creating a new service for persistence).

    - ATT&CK Technique (Persistence): T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (modifying registry keys to launch on startup).
- **Lateral Movement** (TA0008):
    - The worm moves laterally through the network, infecting other systems by exploiting the same SMB vulnerability on shared drives.
    - ATT&CK Technique: T1021.002 - Remote Services: SMB/Windows Admin Shares (using the compromised system to access and infect other machines via SMB).
- **Collection** (TA0009):
    - The worm gathers sensitive data from the infected systems, such as personal information, financial data, and intellectual property.
    - ATT&CK Technique: T1005 - Data from Local System (collecting files and information directly from the compromised host).
- **Command and Control** (TA0011):
    - The worm establishes communication with the attacker's command and control (C2) server.
    - ATT&CK Technique: T1071.001 - Application Layer Protocol: Web Protocols (using HTTP/HTTPS for C2 communication).
- **Exfiltration** (TA0010):
    - The worm exfiltrates the stolen data to the attacker's command and control server.
    - ATT&CK Technique: T1041 - Exfiltration Over C2 Channel (sending collected data over the established C2 channel).

D3FEND Mitigation Strategies

Defensive strategies to D3FEND Tactics, Countermeasures, and Techniques, directly addressing the ATT&CK TTPs identified in the previous section.

- **Countering Initial Access / Execution / Persistence / Lateral Movement** (via MS08-067 / SMB)
    - D3FEND Tactic: **Harden**
    - Countermeasure: **Platform Hardening**
        - **Software Update (D3-SU)**: Promptly apply the MS08-067 patch and all other critical security updates to all Windows systems. This directly removes the vulnerability exploited by Conficker.
        - **System Configuration Permissions (D3-SCP)**: Implement strong permissions on shared drives and critical system configurations to restrict unauthorised access and prevent the worm from writing or modifying files in sensitive locations.
        - **OS Hardening (D3-OSH)**: Configure operating systems to disable unnecessary services and features, reducing the overall attack surface.

- Countermeasure: **Network Hardening**
  - Technique: **Network Segmentation (D3-NS)**: Segment networks to isolate critical systems and limit the lateral spread of the worm via SMB shares. Disable unnecessary network shares to reduce the attack surface.

- **Detecting and Preventing Worm Activity**
  - D3FEND Tactic: **Detect**
  - Countermeasure: **Network Anomaly Detection**
    - **Protocol Metadata Anomaly Detection (D3-PMAD)**: Monitor SMB traffic for unusual patterns, such as unexpected connection attempts from non-standard ports or high volumes of failed SMB connection attempts, which could indicate Conficker's scanning or exploitation.
    - **Traffic Filtering (D3-TF)**: Use firewalls and IPS to block known malicious SMB traffic patterns associated with MS08-067 exploitation.

  - Countermeasure: **Endpoint Anomaly Detection**
    - **Process Analysis (D3-PA)**: Monitor for suspicious process creation, particularly services being created or started by unusual parent processes or in unusual locations.
    - **File Analysis (D3-FA)**: Continuously scan files on endpoints for known Conficker signatures and behaviors.
    - **User Behaviour Analysis (D3-UBA)**: While less direct for automated worm spread, unusual access patterns to shared drives or system configurations by user accounts could indicate compromise.

- **Containing and Removing the Worm**
  - D3FEND Tactic: **Isolate**
  - Countermeasure: **Access Mediation**
    - **Network Access Control (D3-NAC)**: Implement NAC to quarantine or isolate infected systems from the rest of the network upon detection, preventing further lateral movement.
    - **Process Isolation (D3-PI)**: Use endpoint security solutions to isolate or sandbox suspicious processes created by the worm.

  - D3FEND Tactic: **Evict**
  - Countermeasure: **Malware Quarantine**
  - **Malware Quarantine (D3-MQ)**: Automatically quarantine or delete detected Conficker files.

  - Countermeasure: **Process Eviction**
    - **Process Termination (D3-PT)**: Terminate Conficker-related processes and services.

        - **Credential Eviction (D3-CE)**: If Conficker compromises credentials, force password resets and invalidate session tokens for affected accounts.

- **Recovering from Compromise**
    - D3FEND Tactic: **Restore**
    - Countermeasure: **Object Restoration**
        - **Restore File (D3-RF)**: Restore critical system files or data that may have been corrupted or exfiltrated by Conficker from clean backups.
        - **Restore Configuration (D3-RC)**: Restore system configurations to a known good state.

10 Exercise

Objective: To familiarise students with the MITRE ICS ATT&CK and D3FEND matrices and their application in understanding and defending against cyberattacks on ICS.

- Assign each student one of the ICS ATT&CK tactics.
- Research and summarise the key techniques and procedures associated with their assigned tactic.
- Present their findings to the class.
- Facilitate a discussion among the groups to compare and contrast the different tactics and their associated techniques.

Additional Activities:

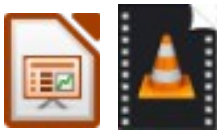
- Develop a threat model for a specific ICS system, identifying and mapping the potential attack paths that could be used by adversaries.
- Research and evaluate ICS security controls that can be implemented to mitigate the risks associated with the different ICS ATT&CK tactics.
- Researching real-world cyberattacks on ICS systems and analysing how the attackers employed the tactics and techniques described in the matrix.
- Developing a deeper understanding of the specific vulnerabilities and attack vectors that are relevant to ICS systems.
- Keeping up-to-date with the latest updates to the MITRE ICS ATT&CK matrix and its application in the ever-evolving cybersecurity landscape.

Assessment:

Assessment on your ability to:

- Identify and explain the key concepts of the MITRE ICS ATT&CK matrix.
- Summarise the key techniques and procedures associated with their assigned tactic.
- Compare and contrast the different tactics and their associated techniques.
- Develop a threat model for an ICS system and identify potential attack paths.
- Evaluate ICS security controls and their effectiveness in mitigating risks.
- Apply knowledge of the ICS ATT&CK matrix to pass the knowledge gained to others.

Create a presentation as part of the assessment, and using it as a tool, create a video to explain what you found that meets the given objective.



11 Bibliography

[1] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, ‘Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains’, *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, p. 80, 2011.

[2] M. J. Assante and R. M. Lee, ‘The industrial control system cyber kill chain’. SANS Institute, 2015. Accessed: Jan. 22, 2024. [Online]. Available: https://sansorg.egnyte.com/dl/HHa9fCekmc

[3] A. Di Pinto, ‘Your Guide to the MITRE ATT&CK Framework for ICS’. Nozomi Networks, Aug. 11, 2023. Accessed: Aug. 08, 2023. [Online]. Available: https://www.nozominetworks.com/blog/your-guide-to-the-mitre-attack-framework-for-ics/

[4] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, ‘Mitre att&ck: Design and philosophy’, in *Technical report*, The MITRE Corporation, 2018.

[5] O. Alexander, M. Belisle, and J. Steele, ‘MITRE ATT&CK for industrial control systems: Design and philosophy’, *The MITRE Corporation: Bedford, MA, USA*, vol. 29, 2020.

[6] D. K. Zafra, ‘Hello From the OT Side!’, 2020.