AIRPORTS COUNCIL INTERNATIONAL

Penetration Testing Guidelines for OT and ICS Environments in Airport Settings

ACI EUROPE GUIDANCE DOCUMENT

ACI EUROPE
Cybersecurity Committee

TLP: CLEAR

Document Control

Document Details

Document Title	Penetration Testing Guidelines for OT and ICS Environments in Airport Settings
Document Number	202501
Classification	TLP CLEAR
Version Number	2.0
Status	Active

Author & Owner Details

Author	ACI EUROPE Cyber Security Committee
Owner	ACI EUROPE
Approved For Release By	ACI EUROPE Aviation and Cyber Security Director

Next Review Date

Next Review Date	01/04/2026

Version History

Version	Date	Comments	Reviewed by
0.1	23/04/2025	Review	Pen Testing WG
0.2	24/04/2025	Content Approved	Cyber Security Committee
0.3	17/05/2025	Edits for release	Pen Testing WG
0.4	25/06/2025	Edits for release, version control	ACI EUROPE
0.5	26/06/2025	Shared for approval of the design	ACI EUROPE Aviation and Cyber Security Director
0.9	22/07/2025	Edited according to feedback provided -	ACI EUROPE
1.0	28/07/2025	Approved for Release	ACI EUROPE

Executive Summary

The Penetration Testing Guidelines for OT and ICS Environments in Airport Settings provide a comprehensive framework for conducting cybersecurity assessments tailored specifically to operational technology (OT) and industrial control systems (ICS) within airports. Developed by the ACI EUROPE Cyber Security Committee, this guidance recognizes the unique safety, operational, and regulatory challenges of performing penetration tests in uptime-critical aviation environments.

The document outlines the risks and requirements for safely and effectively testing systems, including baggage handling, lighting, fuel management, and access control technologies. It emphasizes the need for careful planning, stakeholder coordination, and a deep understanding of airport OT/ICS landscapes to avoid disruptions during testing. The guidance addresses various testing approaches, from vulnerability scanning to red teaming, and underscores the limitations of traditional IT methodologies in OT contexts.

Key components include a risk-based testing schedule, methodologies adapted to legacy and proprietary systems, and a strong focus on compliance with European and international cybersecurity standards (e.g., NIS2, EASA, ISA/IEC 62443, NIST). The guidance promotes white-box and hybrid testing, discourages the use of fully automated tools in sensitive environments, and recommends rigorous cleanup and reporting protocols.

By following this guidance, airport operators can improve the security maturity of their OT/ICS systems, ensure compliance, and strengthen resilience against cyber threats—while minimizing operational disruption and maintaining trust across stakeholders. The framework is scalable and modular, allowing for phased implementation based on an organization's risk tolerance and resource availability.

Acknowledgement

ACI EUROPE would like to express its sincere gratitude to the members of the Cyber Security Committee for their valuable input and contribution to this document. A special note of thanks goes to Attila Horváth, Director of IT and Cybersecurity at Budapest Airport, whose leadership, dedication, and significant time investment were instrumental in the development of this guidance. His efforts have been key in shaping a document that will support and enhance airports' cybersecurity posture.

The ACI EUROPE Cyber Security Committee serves as a strategic advisory body to the ACI EUROPE Board, both on its own initiative and at the Board's request. Acting as a think-tank within its area of expertise, the Committee identifies key strategies, stakeholders, priorities, regulatory initiatives, and policies related to cybersecurity in the airport industry. It helps members to comply with relevant regulatory requirements and to safeguard their ability to operate by promoting higher levels of cybersecurity maturity across the air transport sector. Additionally, the Committee monitors and analyses emerging cybersecurity challenges and trends affecting airports. A key part of its mission is to foster a "system of trust" among ACI EUROPE members, encouraging the open exchange of experiences, best practices, and information regarding cybersecurity incidents.

Table of Contents

1. Introduction

1.1 Purpose of the Guideline

The purpose of this guideline is to provide comprehensive and structured best practices for conducting penetration testing in Operational Technology (OT) and Industrial Control Systems (ICS) environments, within airport settings.

By adhering to these guidelines, airport operators and security professionals will gain further insights into penetration testing in these environments, and therefore, be better equipped to protect their critical infrastructure from cyber threats, thereby ensuring the safety and security of their operations by scoping such tests appropriately.

1.2 Scope

This document is designed to enhance security awareness and deepen understanding of Operational Technology (OT) and Industrial Control Systems (ICS) at airports, highlighting the potential security threats these critical systems may encounter. It provides a comprehensive overview of establishing a penetration testing program and introduces a tailored framework that meets the unique requirements of airport OT/ICS environments. This guideline not only explores key cybersecurity practices but also promotes stakeholder engagement, fostering collaboration among all parties involved to ensure thorough security assessments and the effective implementation of mitigation strategies addressing the risks associated with penetration testing.

Although this document primarily concentrates on penetration testing, the assessments and findings discussed provide valuable insights applicable across a broad spectrum of cybersecurity practices, from vulnerability scanning to red teaming.

It is imperative that the penetration test scope is undertaken by security professionals in conjunction with the Technical / Business Owner of the system to ensure the system is adequately and appropriately tested. Furthermore, the organisation undertaking the testing should be suitably experienced in OT/ICS systems.

1.3 Exploring Key Security Practices – From Vulnerability Scanning to Red Teaming

The table (*Table1)* below provides an example of the various testing types that can be undertaken. It should be noted that the *Relative Risk level will differ from one implementation to another and differ depending on an organisation's risk appetite.

WARNING
In OT/ICS environments, even "Vulnerability Scanning" marked at the lowest relative risk level can cause critical errors, indicating a significantly higher risk compared to traditional IT environments.

Security Practice	Short Definition and Scope	Goal / Intended Outcomes	Frequency	Expected Effort in Weeks	Tools and Techniques	Relative Risk
Vulnerability Scanning	Automated process to identify known vulnerabilities across numerous systems.	Identify known vulnerabilities to maintain compliance with security best practices.	Frequent (e.g., monthly, weekly)	1-2 weeks (mostly automated)	Primarily automated tools	Low (Automated, known vulnerabilities)
Vulnerability Assessment	Comprehensive evaluation and prioritization of vulnerabilities in systems.	Detailed understanding of vulnerabilities in context to prepare for deeper testing.	Periodic (e.g., quarterly, annually)	2-4 weeks	Automated tools with some manual analysis	Moderate (Detailed, risk-based prioritization)
Penetration Testing	Simulated attack to identify and exploit weaknesses in specific targets.	Identify, exploit, and patch security vulnerabilities.	Less frequent (e.g., annually, biannually)	4-8 weeks	Mixed, automated and extensive manual techniques	High (Targeted, potential operational disruption)
Red Teaming	Full-scale attack simulation testing overall organizational defences and response.	Test overall security posture and incident response effectiveness.	Infrequent (e.g., biannually, as needed)	8-12 weeks	Variety of tools and methods, extensive manual techniques	Very High (Comprehensive, potential operational disruption and data breach)

Table1

2. Proposed Considerations for an OT/ICS Penetration Testing Program

2.1 Common OT/ICS Systems in Airports

Airports are complex infrastructures where operational technology (OT) and industrial control systems (ICS) play a critical role in ensuring safety, security, efficiency, and reliability. In special cases, OT/ICS systems may process passenger-related data, at which point privacy becomes relevant as well. As we prepare to delve into the specifics of penetration testing within the OT/ICS environments at airports, we present a comprehensive list of the most commonly utilized OT/ICS systems. This overview will serve as a foundation for our discussions, helping participants understand the potential risks associated with different security practices, from vulnerability scanning to red teaming.

- ILS – Instrument Landing Systems
- AGL – Aerodrome Ground Lighting, Runway and Taxiway Lighting Systems
- Passenger Boarding Bridges
- DGS – Aircraft Docking Guidance System
- BHS – Baggage Handling Systems including the Sort Allocation
- BRS – Baggage Reconciliation Systems
- FDS – Fence Defense System, Perimeter Intrusion Detection Systems
- X-ray – Screening related system(s)
- CCTV, VSS – Security cameras related system(s), Video Surveillance System
- FMMS – Fuel Management and Monitoring Systems, most probably separate systems manage aircraft refuelling and monitor fuel for ground support vehicles, including those used in apron operations and other airport activities.
- BAS, BMS – Building Automation Systems or Building Management Systems, or related special systems e.g. Smoke Detection and Exhaust, Automatic Door and Emergency Exit Control System
- FAS – Fire Alarm Systems
- ATC – Air Traffic Control systems, with the comment that these systems are typically maintained and operated by Air Navigation Service Providers (ANSPs)
- TTS, Rail – Transit systems with the organisation
- Engineering Automation and Remote Telemetry – Control of utilities such as water, electricity, access signals

2.2 Navigating the Complexities of OT/ICS Penetration Testing – A Summary of Expert Perspectives

In OT/ICS environments, availability is often prioritized over confidentiality and integrity. This prioritization significantly influences the planning and execution of penetration tests, dictating which testing scenarios to avoid and emphasizing approaches that ensure uninterrupted operation of critical functions.

OT/ICS penetration testing demands a highly cautious, collaborative, and specialized approach that prioritizes the safety and continuity of operations. It requires a deep understanding of the unique challenges, risks, and protocols associated with industrial environments, along with significant adaptations to traditional IT penetration testing methodologies.

2.2.1 Key Differences and Challenges

Visibility: Limited or no visibility into OT environments is a prevalent issue, significantly complicating the planning and execution phases of penetration testing. This lack of asset knowledge introduces technical challenges not typically encountered in more comprehensively visible IT environments.

Attack Methodology (ICS Cyber Kill Chain): Attacks unfold differently in OT/ICS. Penetration testing methodologies must adapt to the ICS Cyber Kill Chain, acknowledging the need for stringent limitations to avoid disrupting critical operational processes.

Use of Automated Tools: Traditional IT penetration testing often uses automated tools, especially starts with automated scanning. However, these tools can be disruptive and dangerous in sensitive OT systems. Alternative, non-intrusive reconnaissance, discovery and exploit approaches are crucial, potentially affecting the assessment timeline and thoroughness.

Legacy Systems and Protocols: The prevalence of legacy devices and unique protocols in OT systems introduces special challenges. Most OT protocols transmit unencrypted data (which shouldn't be reported as a vulnerability itself but understood as an inherent characteristic). Testers require specialized knowledge of these industrial protocols, and the potential for exploiting known vulnerabilities in older systems should not be underestimated.

Vendor-Specific Tools: While generally well-mitigated in IT, OT environments often contain vendor-installed specialized tools conducive to "living off the land" tactics. Testing for this becomes a critical focus in OT/ICS penetration testing and is often a testable risk within production environments. Identifying and potentially exploiting these requires a collaborative approach with the testing firm, OT operators, and manufacturers during planning and execution.

Building a Test Environment: Building a test environment for traditional IT systems is often unnecessary, or when required due to the system's criticality, can typically be accomplished with reasonable effort. In contrast, constructing an OT/ICS test environment for penetration testing presents extraordinary challenges due to specialized hardware requirements, proprietary protocols, and vendor-specific equipment that must be replicated to create a realistic simulation of production environments. The complex interdependencies between various industrial components make it difficult for test environments to accurately mirror the intricate operational nuances of live systems.

Risk Assessment: OT environments present a unique risk landscape where seemingly minor vulnerabilities can cascade into severe physical safety implications and significant operational disruptions. Conversely, vulnerabilities that might appear critical in isolation may be rendered unexploitable due to the presence of compensating security layers within the OT architecture. This necessitates a holistic and collaborative risk assessment methodology. Findings should be classified based on a joint analysis involving IT/cybersecurity experts, OT operations personnel, and the penetration testing team. This collective evaluation ensures a nuanced understanding of the true exploitability and potential impact within the specific OT context, which may lead to risk classifications that differ significantly from those in traditional IT environments.

2.2.2 Essential Methodological Adaptations and Considerations

Thorough Planning and Scope Definition: Significantly more detailed planning is required in OT/ICS testing compared to IT. Clear boundaries and limitations of the testing scope must be defined and understood by all involved, down to individual testers.

Verification of Tester Expertise: Rigorous vetting of the testing team's OT/ICS protocol knowledge and experience is critical during the tendering process. Demonstrations and knowledge testing are necessary.

Robust Change Management Processes: Mechanisms to strictly supervise the testing team's activities and ensure they remain within the defined scope are essential, including multi-level approvals before critical interventions. Adherence to strict change management processes is paramount. Every testing phase and tool deployment must be subject to approval. Change request processes require refinement to accommodate the intentional introduction of errors during testing.

Emphasis on White-Box and Hybrid Testing Approach: Black-box testing should likely be avoided in favor of white-box approaches, leveraging documentation and discussions about principles and techniques. Providing clear network and system architectural diagrams, as well as conducting detailed workshops with active participation from testers, is crucial for understanding the environment. Combining testing in simulated environments for individual components with strictly controlled testing of the network in the live production environment can be a viable strategy.

Defined Halt Conditions: Specific indicators for halting exploitation attempts before completion must be established, differing significantly from IT testing, where full exploitation is often the goal.

Collaboration and Communication: Close collaboration between the penetration testing team, OT operators, IT/cybersecurity departments, and even manufacturers is crucial throughout the entire process. Effective communication of findings between technical and management levels, taking into account the specifics of industrial processes, is essential.

2.3 Regulatory and Compliance Considerations

Penetration testing serves as a critical component of cybersecurity strategies, providing an essential method to identify, assess, and mitigate vulnerabilities within information systems and network infrastructures. It is particularly vital in environments where security breaches can lead to significant operational disruptions, data breaches, or compromise of safety. Penetration testing not only helps organizations understand their risk posture but also ensures compliance with various regulatory frameworks that mandate or recommend regular security assessments to protect sensitive data and critical infrastructure. The list below is not comprehensive and subject to change within different jurisdictions; however, the overall outcome and approach are very similar and applicable.

2.3.1 EU NIS and NIS2 Directive

Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS) and Directive (EU) 2022/2555 concerning measures for a high common level of cybersecurity across the Union (NIS2) - The NIS and NIS2 Directives mandate that Member States ensure operators of essential services and digital service providers take measures to secure network and information systems. While these directives implicitly require security assessments to manage risks effectively, they do not explicitly mandate vulnerability scanning, vulnerability assessments, penetration testing, or red teaming. However, the specific implementation of these directives can vary by member state, potentially including explicit requirements for such security practices. Airports are advised to investigate the specific cybersecurity obligations laid out by their respective national authorities to ensure compliance with local implementations of these directives.

2.3.2 EASA Part-IS

Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 laying down detailed measures for the implementation of the common basic standards on cybersecurity in the field of civil aviation and Acceptable Means of Compliance and Guidance Material to Annex II (Part-IS.I.OR) to Commission Implementing Regulation (EU) 2023/203 - The document focuses broadly on establishing a robust information security management system (ISMS) within aviation security, with several instances where activities like vulnerability assessments and risk management are implied or recommended. Mentions of “vulnerability” together with “information security incidents” and the need for “detecting, responding, and recovering” from such incidents suggest elements of vulnerability scanning and vulnerability assessment. Furthermore, the text discusses “vulnerability management”, which typically includes vulnerability scanning and assessments as critical components.

2.3.3 UK NCSC Cyber Assessment Framework (CAF)

In section B4.d. Vulnerability Management, it explicitly discusses management of known vulnerabilities, which typically includes vulnerability scanning and assessments as critical components.

2.3.4 ISO 27001/27002

ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements and ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls

2.3.5 ISA/IEC 62443-3

The ISA/IEC 62443 series of standards provides a critical framework for defining the requirements and processes necessary to implement and maintain electronically secure Industrial Automation and Control Systems (IACS). Notably, the section ISA/IEC 62443-3-3, which focuses on "Industrial communication networks - Network and system security", is particularly important for security practices such as penetration testing. However, it is essential that all sections are carefully reviewed to ensure comprehensive coverage and security.

2.3.6 NIST SP 800-53

In the NIST Security and Privacy Controls for Information Systems and Organizations (SP 800-53) the control “RA-5 VULNERABILITY MONITORING AND SCANNING” specifically mandates organizations to scan for vulnerabilities in the information system and hosted applications periodically. It also refers to “vulnerability monitoring” several times. The control “CA-8: Penetration Testing” explicitly recommends that organizations conduct penetration testing on an annual basis and when significant changes are made to the information system, the environment of operation, or other conditions that may impact the security of the system. In other controls, such as “SA-11 DEVELOPER TESTING AND EVALUATION” and the “SR-5 ACQUISITION STRATEGIES, TOOLS, AND METHODS” the penetration testing is also mentioned.

2.3.7 NIST SP 800-82

In the NIST Guide to Operational Technology (OT) Security (SP 800-82), Section 6.3.2.4 of Vulnerability Scanning (DE.CM-8) explicitly recommends conducting vulnerability scanning as part of the security monitoring and detection strategy in OT environments. It addresses the implementation of vulnerability scanning protocols to identify security weaknesses that require attention. Vulnerability Monitoring and Scanning (RA-5) - Section on Risk Assessment discusses the specific risks associated with vulnerability scanning in OT environments, highlighting the need for tailored approaches that consider the sensitive nature of operational technologies. Penetration Testing (CA-8) - Section on Security Assessment- similar to vulnerability scanning, this section discusses the inherent risks

associated with penetration testing in OT environments. It advises on the careful planning and execution of penetration tests to avoid disrupting operational systems. Penetration Testing Mentioned with Incident - Appendix C, C.3.4 - In the context of accidental events, this section discusses the implications of penetration testing, which, if not carefully managed, could potentially lead to incidents. This inclusion underscores the importance of penetration testing in identifying and mitigating unintended vulnerabilities and operational risks.

2.4 Penetration Testing and Red Teaming Frameworks and Best Practices

- Open Information Systems Security Group – Information Systems Security Assessment Framework 0.2.1 (ISSAF)
- Open Source Security Testing Methodology Manual ("OSSTMM") v3
- NIST Technical Guide to Information Security Testing and Assessment (SP 800-115)
- NIST Guideline on Network Security Testing (SP 800-42)
- NIST Guideline on Protecting Controlled Unclassified Information in Non-federal Systems and Organizations (SP 800-171).
- Open Web Application Security Project ("OWASP")
- Penetration Testing Execution Standard ("PTES")
- Payment Card Industry ("PCI") Data Security Standard ("DSS") Penetration Testing Guidance
- Federal Risk and Authorization Management Program ("FedRAMP"): FedRAMP Penetration Test Guidance 1.0.1.
- Threat Intelligence-based Ethical Red Teaming (TIBER-EU)
- MITRE ATT&CK

Most of these frameworks provide a high-level, comprehensive methodology to guide security testing and assessments but often lack the granular, context-specific guidance needed to address the unique challenges of critical systems. They tend to offer a broad approach which might not delve into the specifics required by different industries or technologies, such as real-time systems or those handling sensitive data under strict regulatory requirements.

These penetration testing standards and methodologies provide a benchmark to assess cybersecurity and offer recommendations adapted to a specific context to protect against bad actors; however:

- No framework discusses how to effectively negotiate or manage vendor constraints during penetration testing.
- Specific techniques for dealing with closed, proprietary systems are rarely covered.
- The specifics of handling sensitive data during penetration testing are often not detailed.
- Many frameworks advocate for comprehensive testing but do not always provide concrete methods to go beyond surface-level vulnerabilities, especially in specialized contexts.
- Broad guidelines exist, but detailed strategies for integrating penetration testing into change management processes or for conducting detailed risk analyses are less common.
- Risks associated with over-reliance on automated tools are acknowledged but not deeply explored in terms of mitigation strategies.
- While there's general advice on avoiding disruptive tests, specific guidelines on safe yet effective testing techniques are sparse.
- Guidelines for setting boundaries in attack simulations are usually generic.
- The specifics of avoiding or managing the impact of residual data and tools post-testing are rarely addressed in detail.

Overall, these frameworks serve well as foundational guides and can help standardize procedures, but they do not provide the depth of guidance needed for specific challenges in penetration testing uptime-critical systems. For more practical, nuanced guidance, organizations need to develop their own tailored approaches.

2.5 Penetration Testing Program – Schedule

Unless superseded by specific regulatory or legislative mandates, the organization shall adhere to the following schedule for penetration testing activities.

2.5.1 Initial Testing Requirements

- All new systems should undergo comprehensive penetration testing during the implementation phase as a mandatory component of the project work. Testing should be completed, and all critical/high findings should be remediated before production deployment.
- For systems not previously tested during implementation, a structured long-term testing calendar shall be established. The testing calendar shall prioritize systems based on:
  - Business criticality
  - External (or internal) visibility and accessibility
  - Regulatory compliance requirements
- The complete inventory of systems shall be tested on a rolling basis according to the established risk-based schedule. Resource constraints shall be addressed through proper capacity planning.

2.5.2 Retesting Requirements

- All systems with identified vulnerabilities should undergo structured retesting following remediation activities. Testing must verify that remediation efforts are successful and have not introduced new security vulnerabilities.
- Systems should undergo retesting following significant changes to their security posture, including:
  - Major version upgrades of critical components (operating systems, databases, application servers, OT components).
  - Architectural changes affecting data flow or processing.
  - Modifications to network segmentation or security boundaries.
- Retesting should be conducted promptly following the completion of remediation activities or significant environmental changes, within 90 days from the implementation date.

3. Comprehensive Analysis of OT/ICS Penetration Testing in Airport Environments

3.1 How to Read This Chapter

This chapter provides a structured framework for understanding and implementing OT/ICS system penetration testing concepts. Each topic follows a consistent format that progresses from identification of relevant attack techniques through definition, challenges, and practical solutions, concluding with a balanced assessment of potential impacts on testing relevance. This standardized approach enables security professionals to quickly navigate complex ICS testing considerations while ensuring comprehensive coverage of both technical and operational risk factors.

Title

Each section title identifies a specific OT/ICS risk area that presents substantially higher testing dangers compared to traditional IT environments, requiring specialized consideration and controls during penetration testing activities.

Related MITRE ATT&CK Technique(s)

This section (if applicable) lists the specific MITRE ATT&CK framework techniques relevant to the topic, providing standardized reference points for understanding the attack vectors being discussed.

Definition

This section provides a clear understanding of the penetration testing concept being addressed, explaining its significance within industrial control systems and why it is important from a security perspective.

Problems and Challenges

This section outlines the key difficulties and complications that organizations face when attempting to test against the described tactics, highlighting why special consideration is needed.

Proposed Solution

This section provides actionable recommendations and methodologies that organizations can implement to effectively test for the described vulnerabilities while minimizing operational risks.

Potential Impact on Relevance of the Penetration Test Result

This section assesses the impact of including or excluding these test elements on the overall value and accuracy of the penetration test findings.

Pros (under the Potential Impact)

These bullet points highlight the specific benefits and advantages that organizations gain by properly incorporating these testing elements and the proposed mitigations into their security assessment.

Cons (under the Potential Impact)

These bullet points present the potential drawbacks, limitations, or resource requirements that organizations should consider before implementing the recommended testing approaches.

3.2 PLANNING AND SCOPING

3.2.1 Understanding Proprietary OT/ICS Technologies and Balancing Comprehensive Testing with Vendor Constraints

Definition

Proprietary OT/ICS technologies often operate as black-box systems, with limited transparency and access to administrative controls. Vendor technical insights are crucial during penetration testing, particularly for evaluating the impact of potentially destructive outcomes. This lack of vendor-shared administrative credentials and insight into the system's inner workings necessitates a balanced approach to testing that ensures comprehensive coverage without violating vendor constraints or risking system integrity.

Problems and Challenges

- Limited Access to System Internals: The closed nature of proprietary systems means penetration testers often lack the necessary access to thoroughly test the systems, potentially leaving significant vulnerabilities undiscovered.
- Vendor Dependency: Reliance on vendor cooperation for access and information can lead to delays and limitations in testing scope, especially if the vendor is uncooperative or protective of their intellectual property.
- Risk of System Damage: Without complete understanding or access, testing can risk damaging the system or triggering fail-safe mechanisms that disrupt operations, particularly if testing extends beyond known safe parameters.
- OT/ICS systems may be composed of software and hardware components therefore compensating controls other than patches and upgrades may be required as a result of the pen testing results.

Proposed Solution

- Negotiated Access Agreements: Establish agreements with vendors and appropriate stakeholders i.e. Business and Technical Owners that allow for limited but sufficient access to critical system components for testing purposes, ensuring that both parties understand and agree on the scope and limits of the testing.
- Use of Simulated Environments: Where possible, use replicas or simulated environments that are representative of the proprietary systems for initial testing phases to identify potential vulnerabilities without risking the actual operational systems. System operational availability must be considered as an important factor as due to the criticality of OT / ICS systems, scheduling and penetrating testing duration may be challenging hence the need a representative test environment.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Increased Safety and Accuracy: Controlled access and vendor collaboration can lead to more accurate testing outcomes by ensuring that tests are conducted under informed conditions, reducing the risk of false positives and unintended disruptions.
  - Compliance and Trust: Vendor involvement and approved testing parameters can ensure compliance with industry standards and build trust between all stakeholders, enhancing the validity of the test results.

- Cons:
  - Potential for Incomplete Testing: Negotiated constraints and limited access might result in tests that do not fully explore the system's vulnerabilities, leaving gaps in security. Please be aware that local regulations may prohibit conducting penetration tests in simulated environments. For instance, the "GSA Conducting Penetration Test Exercises (CIO-IT Security-11-51 Rev 7)" mandates that penetration tests be conducted against the production environment unless the system is new and has been placed into a pre-production ("pre-prod") environment. This requirement stems from the understanding that replicating an identical production environment for testing purposes is nearly impossible. Although this example is not specific to the aviation industry, it underscores the importance of thoroughly reviewing local regulations related to penetration testing. The CISO and CIO of the airport should carefully examine the regulations to ensure compliance and avoid potential legal issues.
  - Potential for inappropriate scoping or system knowledge may affect the effectiveness of a penetration test.
  - Dependency on Vendor Transparency: The effectiveness of the penetration test is heavily dependent on the vendor's willingness to provide detailed insights and access, which may not always be forthcoming or sufficiently detailed.

3.2.2 White-box penetration testing on Proprietary Closed Systems (e.g. appliances, embedded devices)

Definition

White-box penetration testing on proprietary closed systems, such as appliances and embedded devices, involves an in-depth examination of the internal workings of systems. Despite the collaborative involvement of vendors, access may be significantly restricted compared to traditional IT systems. Unlike typical IT environments where white-box approaches are standard during post-exploitation phases, proprietary systems require alternative strategies and precise scoping to effectively navigate these constraints.

Problems and Challenges

- Access Restrictions: Even with vendor involvement, proprietary systems often come with strict access limitations, preventing testers from examining critical components of the system fully.
- Lack of Transparency: Vendors may be reluctant to disclose full details about their systems, fearing intellectual property theft or exposure of vulnerabilities that could be exploited by malicious actors.
- Complexity of Systems: Proprietary systems, particularly embedded devices, can be highly specialized and complex, making it difficult to apply standard testing tools and techniques effectively.

Proposed Solution

- Enhanced Vendor Agreements: Work towards more comprehensive agreements with vendors that specify the extent of access and information disclosure necessary for thorough testing.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Targeted Insight: Even limited white-box testing can provide deeper insights into the most critical components of the system, improving the relevance and accuracy of the test results.

- Cons:
  - Incomplete Coverage: Restricted access might result in significant portions of the system remaining untested, potentially leaving undetected vulnerabilities.
  - Dependence on Vendor Cooperation: The effectiveness of the testing is heavily reliant on the level of cooperation from the vendor, which can vary widely and affect the comprehensiveness of the testing outcomes.

3.2.3 Handling Sensitive Data and Systems

Definition

The partner responsible for conducting the penetration test will access sensitive systems and data within critical infrastructure. It is imperative to secure a robust non-disclosure agreement with the company, even on an individual basis, incorporating a thorough vetting process. Additionally, penetration testers should not use their standard devices and laptops; instead, a sanitized laptop provided by the airport must be used within the premises.

Handling sensitive data and systems during penetration testing involves strict protocols to ensure the confidentiality and integrity of the information and systems accessed. The complexity increases within critical infrastructures, where security breaches can have severe implications. It is critical to establish robust non-disclosure agreements and involve a thorough vetting process for all personnel involved. The use of sanitized, designated devices that remain on-site further mitigates risks associated with data leakage or unauthorized access.

Problems and Challenges

- Data Breach Risks: Sensitive data exposure can lead to significant security and privacy breaches, impacting the organization's compliance with regulations and its public image.
- Integrity of Testing Devices: Standard devices used by penetration testers may carry risks of contamination or cross-contamination with data from other environments, compromising the test's integrity.
- Insider Threats: Even with NDAs, the risk of information leakage by insiders, whether intentional or accidental, remains a significant concern.

Proposed Solution

- Robust Non-Disclosure Agreements: Ensure comprehensive NDAs are in place, tailored to the sensitivity of the data and systems, and legally enforceable, covering all individuals involved in the testing process.
- Thorough Vetting Process: Implement a rigorous vetting process for all testing personnel, which may include background checks, previous employment verification, and security clearance status.
- Use of Sanitized, On-site Devices: Require penetration testers to use sanitized laptops provided by the host organization, which are configured to prevent data leakage and must remain within the testing premises at all times.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Enhanced Security Measures: The strict control measures ensure that the penetration test is conducted in a secure environment, minimizing the risk of data breaches and maintaining the integrity of the test results.

  - Compliance and Trust: These protocols help in maintaining compliance with legal and regulatory standards, building trust among stakeholders and protecting the organization's reputation.
- Cons:
  - Operational Complexity: The requirement for specialized procedures and equipment can complicate the logistics of the penetration test, potentially leading to delays and increased costs.

3.2.4 Dealing with Clear Text Communication in OT/ICS Networks

Definition

Clear text communication within OT/ICS networks involves the transmission of unencrypted data over the network, which is common in industrial control system protocols such as Modbus over TCP. This method of communication can expose critical systems to eavesdropping and tampering attacks. Effective penetration testing must go beyond simply identifying the use of clear text protocols to truly add value, emphasizing the need for a well-defined scope that targets meaningful security enhancements. Traditional penetration testing, which often reveals only well-known vulnerabilities of a clear-text protocol, may not be effective.

Problems and Challenges

- Limited Value of Surface-Level Testing: Traditional penetration tests that only confirm the well-known vulnerabilities associated with clear-text protocols provide little additional value. Such tests often fail to uncover deeper, more complex security issues.

Proposed Solution

- In-depth Protocol Analysis: Conduct thorough analyses of how clear text protocols are implemented and used within the specific OT/ICS context to identify unique vulnerabilities or misconfigurations.
- Enhanced Testing Techniques: Employ advanced penetration testing techniques that simulate real-world attack scenarios beyond mere protocol analysis, such as man-in-the-middle (MITM) attacks and data integrity attacks.
- Scope Refinement: Clearly define the scope of the penetration test to focus on actionable outcomes that genuinely enhance system security, such as identifying ways to encrypt communications or to implement compensating controls.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Actionable Insights: By focusing on comprehensive testing and analysis, penetration testing can provide actionable insights that lead to significant improvements in network security and data integrity.
  - Increased Awareness and Remediation: A well-defined scope helps ensure that the testing results in a deeper understanding of the risks associated with clear text communication and encourages the implementation of more robust security measures.
- Cons:
  - Resource Intensiveness: In-depth testing of clear text communication protocols and their implementations can be resource-intensive, requiring specialized knowledge and potentially more time and financial investment.

3.2.5 Change Management, Risk analysis, Communication Plan and Response Plan

Definition

The penetration test itself should be treated as a Change Request within the airport's operational and IT frameworks, necessitating the same level of oversight and management as any other changes, even if the test does not involve actual system modifications. This approach ensures that the testing is integrated with existing operational protocols, maintaining alignment with the airport's security, operational, and compliance standards. The change management process, along with comprehensive risk analysis, communication plans, and response strategies, are critical components of penetration testing preparation. This rigorous planning is essential not only to manage potential impacts of the test but also to ensure that the testing process itself is executed within a controlled and predictable framework. Close collaboration among the airport's IT Operations, Cybersecurity, and OT teams is crucial and extends beyond the capabilities of external penetration testing partners.

Problems and Challenges

- Potential Operational Disruption: Even absent actual configuration changes, the process of penetration testing could potentially disrupt systems if not meticulously planned and managed.
- Need for Comprehensive Stakeholder Engagement: Effective change management requires consensus and synchronized action across various departments, a challenging endeavor that requires careful planning and communication.

Proposed Solution

- Implement a Formal Change Management Process: Initiate the penetration testing process through a formal Change Request procedure, documenting the test's scope, objectives, and expected outcomes. This document should gain approval from all necessary stakeholders to ensure full alignment and understanding.
- Detailed Risk Assessment: Perform a detailed risk assessment tailored to the penetration testing scenario to foresee potential impacts and establish robust mitigation strategies.
- Develop a Structured Communication Plan: Establish a communication plan that ensures all relevant parties are informed and engaged throughout the testing process, from planning through to execution and post-testing review.
- Prepare a Proactive Response Plan: Design a response plan that specifies immediate actions and responsibilities, ready to be implemented swiftly in response to any findings or incidents that arise during the test.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Supports Operational Stability: Treating the penetration test as a formal change helps avoid operational issues, unexpected breakdowns, and potential disruptions, ensuring that the airport's operations continue smoothly.
  - Controlled and Predictable Testing Environment: Treating the penetration test as a formal change ensures that all aspects of the test are managed in a predictable and controlled manner, enhancing the reliability of the test results.
- Cons:
  - Resource and Time Intensive: The process requires significant resources and time, which can strain operational capacities and introduce delays in the testing schedule.
  - Administrative Complexity: The need for extensive documentation and approvals can complicate the testing process, potentially leading to bureaucratic inefficiencies.

3.3 MITRE ATTACK Enterprise – Reconnaissance

3.3.1 Harmful Scanning Methods and Tools

Related MITRE ATT&CK Technique(s)

- T1595 Active Scanning

Definition

It is vital to document the potential hazards of unregulated scanning activities. Providing guidance through illustrative examples may be the most effective method to convey this information. It's also crucial to emphasize that penetration testing partners may seek to streamline their efforts by resorting to rudimentary 'script-kiddie' tactics, such as unmonitored scripted scanning activities.

Harmful scanning methods and tools refer to scanning practices that lack oversight and regulation, potentially causing unintended disruptions or damage in operational technology and information systems environments. These methods often include unmonitored automated scans and rudimentary tactics such as 'script-kiddie' approaches, which involve using pre-made scripts or tools without a deep understanding of their workings or the potential impacts. It is crucial to document and communicate the risks associated with these practices clearly and effectively, using illustrative examples to highlight the potential hazards. Examples of risky scanning techniques are:

- Excessive Network Scanning: Involves high-volume port scanning, scanning with special scripts, and aggressive vulnerability scanning that can overwhelm network resources and disrupt normal operations. These techniques often aim to uncover as many vulnerabilities as possible, but can inadvertently impact network performance and stability.
- Fuzz Testing (Fuzzing): Involves automatically injecting invalid, unexpected, or random data into the system or communication channels to check for vulnerabilities such as buffer overflows or memory leaks. This includes protocol fuzzing and randomized excessive input which can destabilize systems by causing them to handle data they are not designed to process.
- Injecting Malicious Payloads: Includes techniques such as injecting malicious firmware updates, exploit payload injection, and malformed packet injection. These actions are intended to demonstrate how an attacker might compromise a system, but they carry the risk of harming the system if not carefully controlled.
- Stress Testing and Load Testing: Involves deliberately overloading systems, networks, or applications with excessive broadcast or multicast traffic or simulating high loads to observe how they handle stress or heavy loads. While this can be crucial for identifying capacity limits and data handling ability, it risks causing performance degradation or system crashes.
- DoS Type of Scanning: Techniques that can overload systems, networks, or applications with excessive data, requests, or malformed packets intended to exhaust resources and result in denial of service. These are sometimes employed in stress testing to determine capacity limits but can disable systems or make them unavailable to legitimate users if not properly managed.
- Aggressive Network Scanning: Uses comprehensive scanning tools to probe every port and protocol to uncover network services and vulnerabilities. This intensive approach is designed to be thorough but can generate a high volume of traffic that may lead to network saturation and disruption of normal operations.
- Recursive Crawling Techniques: This method involves systematically exploring every endpoint or service across various communication protocols such as FTP, SNMP, HTTP and more. While designed to uncover vulnerabilities by testing every possible path, it can overburden servers

or network devices, potentially causing performance issues or triggering defensive mechanisms, such as rate limiting.

Problems and Challenges

- System Disruptions: Unregulated scanning can inadvertently overload systems, cause network congestion, or trigger fail-safes that disrupt operations, particularly in sensitive environments.

Proposed Solution

- Establish Scanning Guidelines: Develop and enforce comprehensive guidelines for scanning practices that include risk assessments, method selection, and post-scan analysis. These guidelines should discourage the use of harmful scanning tools and promote techniques that are informed and context-sensitive. Make these guidelines mandatory for both internal teams and external partners to ensure consistency in scanning practices across the board.
- Use of Controlled Environments: Where possible, conduct initial scans within controlled environments to assess the impact and adjust methods before deployment in live settings. This step should be standard practice for any scans, whether conducted by internal staff or external partners, to mitigate potential risks.
- Education and Training for All Testers: Provide regular training for all penetration testers, including external partners, on the appropriate use of scanning tools and the potential consequences of unregulated scanning. Ensure that external partners are required to participate in orientation sessions that cover your organization's specific security protocols and expected standards before they begin any penetration testing activities.
- Contractual Obligations and Audits: Include specific clauses in contracts with external partners that mandate adherence to your scanning guidelines and allow for regular audits of their practices to ensure compliance. This may include stipulations for training verification, method approval, and detailed reporting on scanning activities.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Enhanced Accuracy and Safety: By enforcing strict guidelines and ensuring that all testers, including external partners, are well-trained, the accuracy of penetration testing is improved, reducing the risk of false positives and minimizing disruptions.
- Cons:
  - Increased Overhead and Complexity: Managing training and compliance for external partners adds complexity and potential overhead to the penetration testing process.
  - Possible Resistance from Partners: External partners may resist strict guidelines if they feel these limit their methodology or increase their operational costs. Managing these relationships carefully will be key to ensuring compliance without straining partnerships.

3.3.2 Risk of Fully Automated Vulnerability Assessment or Penetration testing

Related MITRE ATT&CK Technique(s):

- T1595 Active Scanning

Definition

Fully automated vulnerability assessments and penetration testing utilise software tools that conduct scans and tests without requiring ongoing human oversight. These tools can execute extensive testing sequences across network and system infrastructures but lack the ability to dynamically adjust or halt in response to unfolding risks or adverse effects. This lack of control can pose significant challenges when trying to align such tests with a structured Change Management process.

Problems and Challenges

- Lack of Real-Time Control: Fully automated tools run predefined scripts and cannot make real-time adjustments or stop automatically in response to critical system impacts, potentially leading to operational disruptions.
- Alignment with Change Management: Integrating automated scans within a change management framework is difficult because these scans may not conform to procedural checks and balances typically required in sensitive environments.
- Risk of Unintended Consequences: Automated tests might trigger system failures, security lockdowns, or other disruptive responses that go unnoticed until significant damage occurs.

Proposed Solution

- Semi-Automated Scanning Approaches: Implement semi-automated testing where human operators can intervene in real-time. This approach combines the efficiency of automation with the control of manual oversight.
- Fully Manual Testing Option: Where feasible, consider fully manual testing methodologies, especially in highly sensitive or critical areas where automated tools might pose too great a risk. Manual testing ensures maximum control and allows testers to use their judgment and experience to navigate complex environments and avoid triggering unintended system responses.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Increased Control and Precision: Both semi-automated and fully manual testing methods provide greater control over the testing process, allowing for real-time adjustments and immediate responses to unexpected findings or disruptions. This control helps to minimize operational disruptions and avoid triggering unintended system responses.
  - Tailored Testing: Manual and semi-automated methods allow testers to apply their expertise and situational awareness, tailoring the testing process to the specific context and complexities of the environment. This can lead to more accurate identification of relevant vulnerabilities that automated tools might overlook.
- Cons:
  - Time and Resource Intensive: Both semi-automated and fully manual testing methods are more resource-intensive than fully automated scans. They require more time and skilled personnel, which can increase the cost and duration of the testing process.
  - Potential for Human Error: While manual testing allows for nuanced judgment, it also introduces the possibility of human error. Testers may miss vulnerabilities that automated systems can catch due to fatigue, oversight, or a lack of expertise in specific areas.

3.4 MITRE ATTACK ICS tactics – Initial Access, Execution

3.4.1 Risks of Disruptive and Destructive Testing Techniques

Related MITRE ATT&CK Technique(s)

- 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
- T0848 Rogue Master
- T0895 Autorun Image
- T0858 Change Operating Mode
- T0807 Command-Line Interface
- T0871 Execution through API
- T0823 Graphical User Interface
- T0874 Hooking
- T0821 Modify Controller Tasking
- T0834 Native API
- T0853 Scripting

Definition

The exploitation phase of penetration testing involves attempting to exploit identified vulnerabilities to gain unauthorized access or escalate privileges within a system. While this phase is crucial for demonstrating the potential impact of vulnerabilities, it carries significant risks, especially when conducted without meticulous planning and assessment. The use of 'script-kiddie' tactics - employing poorly coded or generic exploits without considering their reliability or the specific context of the target system - can lead to unintended disruptions or even permanent damage.

Problems and Challenges

- System Instability and Damage: Poorly coded exploits may cause systems to crash, corrupt data, or trigger unintended behaviours in critical systems, particularly in complex OT/ICS environments where systems are often finely tuned to specific operational parameters.

Proposed Solution

- Rigorous Exploit Review and Testing Protocol: Develop and adhere to a strict protocol for reviewing and testing exploits before their use in the operational environment. This protocol should ensure that all exploits are specifically tailored to the target system and thoroughly tested in controlled conditions to assess their impact and effectiveness.
- Use of Professional and Customized Exploits: Avoid the use of generic, publicly available exploits that are often used by 'script-kiddie'. Instead, invest in professional-grade tools or develop custom exploits that are carefully crafted to interact safely and effectively with the target environment.
- Stakeholder Communication and Approval: Ensure that all planned exploitation activities are communicated to and approved by relevant stakeholders. This includes detailed briefings on the expected actions, potential impacts, and mitigation strategies to manage any adverse outcomes.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Targeted and Effective Testing: By using well-crafted and tested exploits, the testing can accurately demonstrate real-world attack vectors and the actual exposure of the system to security threats, providing valuable insights into critical vulnerabilities.
  - Minimized Negative Consequences: Controlled and thoughtful exploitation reduces the risk of unintended system disruptions or damage, ensuring the stability and availability of critical systems throughout the testing process.
- Cons:
  - Resource Intensity: Developing custom exploits and conducting thorough testing require significant resources, including skilled personnel and time, potentially increasing the cost and duration of the testing process.
  - Complexity in Execution: The need for detailed planning, stakeholder communication, and compliance with strict testing protocols can add complexity to the penetration testing process, requiring meticulous organization and coordination.

3.4.2 Accidental Triggering of Safety Systems or Alarms

Related MITRE ATT&CK Technique(s)

- 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
- T0848 Rogue Master
- T0895 Autorun Image
- T0858 Change Operating Mode
- T0807 Command-Line Interface
- T0871 Execution through API
- T0823 Graphical User Interface
- T0874 Hooking
- T0821 Modify Controller Tasking
- T0834 Native API
- T0853 Scripting

Definition

Accidental triggering of safety systems or alarms refers to the unintended activation of emergency response mechanisms during penetration testing activities. In OT/ICS environments, these safety systems are designed to prevent damage, protect personnel, and maintain operational integrity. When penetration testing activities inadvertently trigger these mechanisms, they can cause operational disruptions, unnecessary emergency responses, and potential damage to equipment.

Problems and Challenges

- Operational Disruption: Accidental triggering of safety systems can lead to production halts, emergency shutdowns, or other operational disruptions that may have significant financial and safety implications.

- False Emergency Response: Triggered alarms may initiate emergency protocols, potentially leading to unnecessary evacuation, emergency service calls, or activation of automated safety responses.
- Damage to Equipment: Some safety protocols, when activated, may cause physical changes to equipment states that could lead to wear, stress, or damage to sensitive industrial components.
- Difficult Risk Assessment: It is challenging to accurately predict which penetration testing activities might trigger safety systems without detailed knowledge of all safety mechanism thresholds and configurations.

Proposed Solution

- Gradual Approach Methodology: Implement a phased testing approach that begins with passive reconnaissance and gradually increases in potential impact, with constant monitoring for early warning signs of safety system activation.
- Use of Isolated Testing Environments: Where possible, create isolated test environments that replicate critical systems but are disconnected from actual safety mechanisms or employ safety simulators.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Increased Safety: A carefully planned approach minimizes the risk of unexpected safety system activations while still identifying vulnerabilities.
- Cons:
  - Potentially Incomplete Testing: Safety boundaries may prevent comprehensive testing of certain attack vectors, potentially leaving some vulnerabilities undiscovered.
  - Additional Resource Requirements: The need for extensive pre-planning and specialized personnel increases the cost and complexity of the penetration testing process.
  - Extended Timeline: A more cautious, phased approach typically requires more time to complete than traditional penetration testing methodologies.

3.5 MITRE ATTACK ICS tactics – Persistence, Privilege Escalation, Evasion

3.5.1 Unauthorized Firmware Updates and Infecting Project Files

Related MITRE ATT&CK Technique(s)

- T0839 Module Firmware
- T0857 System Firmware
- T0873 Project File Infection

Definition

Unauthorized firmware updates could cause system failures or introduce vulnerabilities. Infecting project files could inadvertently spread malware to operational systems, potentially compromising the integrity and reliability of industrial control systems.

Problems and Challenges

- Excessive Scope Requirements: The scope of a penetration test attempting to fully verify these vulnerabilities would be overly ambitious and resource-intensive.
- Resource Limitations: It is unlikely that sufficient time would be allocated for such testing or that the penetration testing firm would possess the specialized capabilities required to safely execute these tests in operational environments.

- Risk of Operational Disruption: Testing actual firmware modification or file infection could lead to unintended operational impacts on critical systems.

Proposed Solution

- Shift Testing Focus: Avoid spending unnecessary time and resources attempting to reproduce actual unauthorized firmware updates and project file infections. Rather than demonstrating the vulnerabilities themselves, focus on testing the surrounding environment.
- Target Supporting Infrastructure: Concentrate testing efforts on the environments through which these processes occur - typically engineering workstations - and attempt to identify vulnerabilities that could lead to unauthorized modifications of the file system.
- Test Integrity Monitoring: If available, test the capabilities and potential vulnerabilities of systems responsible for monitoring the integrity of the relevant file systems.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Feasibility: Makes this test case executable at some level while managing resource constraints.
  - Risk Reduction: Minimizes the potential for operational disruptions during testing activities.
- Cons:
  - Indirect Assessment: Will not provide a direct evaluation of the actual vulnerabilities, but rather an indirect picture of the defensive capabilities.
  - Limited Scope: May not identify all potential attack vectors or vulnerabilities related to firmware and project files.

3.5.2 Risks of Disruptive and Destructive Testing Techniques

Related MITRE ATT&CK Technique(s)

- T0890 Exploitation for Privilege Escalation
- T0874 Hooking
- T0858 Change Operating Mode
- T0820 Exploitation for Evasion

The risk-related challenges of the test and proposed mitigation strategies mirror those previously detailed in the Initial Access and Execution phase section of this document.

3.5.3 Accidental Triggering of Safety Systems or Alarms

Related MITRE ATT&CK Technique(s)

- T0890 Exploitation for Privilege Escalation
- T0874 Hooking
- T0858 Change Operating Mode
- T0820 Exploitation for Evasion

The risk-related challenges of the test and proposed mitigation strategies mirror those previously detailed in the Initial Access and Execution phase section of this document.

3.5.4 Auditing and Recovery Challenges After Evasion Testing

Related MITRE ATT&CK Technique(s)

- T0872 Indicator Removal on Host
- T0849 Masquerading
- T0851 Rootkit

Definition

Evasion testing in OT/ICS environments involves evaluating how effectively an organization can detect and respond to adversaries attempting to hide their presence within industrial systems. These techniques include removing indicators of compromise, disguising malicious software as legitimate components, and implementing rootkits that fundamentally alter system behaviour while concealing these changes. Testing these evasion capabilities presents unique challenges for both auditing the test activities and ensuring complete recovery of systems to their pre-test state. Unlike IT environments where system rebuilds are routine, OT/ICS systems often contain proprietary software, custom configurations, and safety-critical settings that must be preserved and accurately restored after testing.

Problems and Challenges

- Uncertain Recovery State: Testing evasion techniques can make it difficult to verify that all test artefacts have been completely removed, potentially leaving systems in an uncertain operational state after testing concludes.
- Limited Logging Capabilities: Many legacy OT/ICS systems have minimal or easily subverted logging capabilities, making it challenging to maintain comprehensive audit trails of testing activities.
- Persistence Mechanisms: Advanced evasion techniques may implement persistence mechanisms that survive standard cleanup procedures, potentially leaving dormant test tools in production environments.
- Verification Complexity: Confirming complete system recovery often requires specialized knowledge of normal OT/ICS baseline operations that may exceed the expertise of security testing teams.
- Safety System Integrity: Evasion testing that modifies system behaviour may inadvertently alter safety-critical parameters or monitoring capabilities that are difficult to fully validate after testing.

Proposed Solution

- Pre-Test System Baselining: Create comprehensive baselines of system configurations, network traffic patterns, process behaviours, and control parameters before initiating any evasion testing.
- Testing Containment Boundaries: Establish strict scope limitations that clearly define which systems can be subject to which types of evasion techniques, with increasing restrictions for safety-critical components.
- Phased Recovery Procedures: Implement a multi-stage recovery validation process that includes both automated verification and manual expert review of systems to confirm complete removal of test artefacts.
- Dedicated Testing Infrastructure: When possible, conduct more aggressive evasion testing on isolated test systems that accurately reflect production environments rather than on operational equipment.

- Detailed Activity Logging: Maintain comprehensive external logging of all testing activities, captured on systems not subject to the evasion techniques being tested, to ensure a reliable audit trail.
- Vendor Involvement: Engage OT/ICS system vendors in the planning and recovery phases of evasion testing to leverage their specialized knowledge of system behaviour and restoration requirements.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Realistic Threat Simulation: Well-designed evasion testing reveals blind spots in detection capabilities that might otherwise remain undiscovered until exploited by actual adversaries.
  - Enhanced Monitoring Improvements: Organizations typically strengthen their monitoring infrastructure as a direct result of evasion testing, benefiting their overall security posture.
  - Recovery Process Validation: Testing inadvertently validates and improves system recovery procedures, which strengthens operational resilience beyond just security considerations.
- Cons:
  - Resource Intensiveness: Complete validation of system recovery after evasion testing requires significant time and expertise, potentially extending testing windows.
  - Residual Uncertainty: Even with rigorous recovery procedures, subtle system changes may go undetected, potentially affecting operational reliability over time.
  - Limited Scope Coverage: Safety concerns often necessitate restricting the most aggressive evasion techniques to non-critical systems, potentially leaving gaps in the assessment of critical infrastructure.

3.5.5 Living off the Land in ICS/OT

Related MITRE ATT&CK Technique(s)

- T0894 System Binary Proxy Execution

Definition

"Living off the land" in the context of ICS/OT penetration testing refers to the use of built-in system tools and processes to conduct attack simulations. This approach minimizes the detection footprint but presents unique risks, such as the unintentional retention of penetration testing tools or data extraction remnants on the system. These artefacts can potentially be exploited by malicious actors if not properly managed and removed.

Problems and Challenges

- Residual Data and Tools: Tools and scripts used during the testing, as well as extracted or manipulated data, can inadvertently remain on the system. These artefacts might provide backdoors or leverage points for malicious actors.
- System Integrity and Security Risks: Residual penetration testing artefacts can compromise the integrity and security of the ICS/OT environment, making it vulnerable to future attacks.

Proposed Solution

- Strict Cleanup Protocols: Implement rigorous cleanup protocols to ensure that all tools, scripts, and data used during penetration testing are completely removed from the system post-test. This includes automated scripts that perform a cleanup after the test, as well as manual checks to confirm their effectiveness.

- Use of Non-Persistent Tools: Where possible, use non-persistent tools and techniques that automatically expire or delete themselves after use, reducing the risk of leaving behind artefacts.
- Regular Audits and Inspections: Conduct regular post-test audits and system inspections to ensure no residual data or tools are left behind. This could involve third-party verifications to add an extra layer of assurance.
- Training and Awareness: Train all penetration testers on the importance of leaving no trace on the system. Emphasize the security implications and compliance requirements related to residual artefacts. Require external partners to participate in detailed orientation sessions that cover your organization's security protocols, the expected standards for "Living off the Land" strategies, and the consequences of non-compliance. These sessions should also include best practices for ensuring that all digital footprints are erased after testing.
- Contractual Obligations and Audits: Embed specific clauses in contracts with external partners that mandate strict adherence to cleanup protocols and the removal of all test-related artefacts. Contracts should also stipulate the use of approved tools and methods that align with your organization's security policies.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Cleaner Security Posture: Ensuring that no artefacts are left behind maintains the cleanliness and integrity of the ICS/OT environment, preventing future vulnerabilities.
- Cons:
  - Increased Testing Complexity and Duration: Implementing thorough cleanup processes and ensuring all artefacts are removed can add complexity and extend the duration of the testing process.
  - Resource Intensive: The need for additional checks, tool management, and potential third-party audits to ensure cleanliness increases the resource requirements for the penetration test.

3.6 MITRE ATTACK ICS tactics – Discovery, Lateral Movement, Collection

3.6.1 Harmful Scanning Methods and Tools

Related MITRE ATT&CK Technique(s)

- T0840 Network Connection Enumeration
- T0842 Network Sniffing
- T0846 Remote System Discovery
- T0887 Wireless Sniffing
- T0861 Point & Tag Identification

The risk-related challenges of the test and proposed mitigation strategies mirror those previously detailed in the Reconnaissance phase section of this document.

3.6.2 Risks of Disruptive and Destructive Testing Techniques

Related MITRE ATT&CK Technique(s)

- T0866 Exploitation of Remote Services
- T0867 Lateral Tool Transfer
- T0886 Remote Services
- T0830 Adversary-in-the-Middle

The risk-related challenges of the test and proposed mitigation strategies mirror those previously detailed in the Initial Access and Execution phase section of this document.

3.6.3 Defining Safe Boundaries for Real-World Attack Simulations

Related MITRE ATT&CK Technique(s)

- T0812 Default Credentials
- T0866 Exploitation of Remote Services
- T0891 Hardcoded Credentials
- T0867 Lateral Tool Transfer
- T0843 Program Download
- T0886 Remote Services
- T0859 Valid Accounts
- T0861 Point & Tag Identification

Definition

The post-exploitation phase in penetration testing and red team exercises involves actions taken after gaining initial access, typically including privilege escalation, the exploitation of additional systems, and lateral movements within the network. While this phase is crucial for assessing the depth of security defences and the potential for data exfiltration or further compromise, it carries significant risks. Without strict boundaries and control, activities such as privilege escalation using known CVEs and lateral movements can lead to system damage, data loss, or unintended service disruptions.

Problems and Challenges

- Potential for Excessive Damage: Uncontrolled privilege escalation and lateral movements can lead to more extensive system compromise than necessary for testing purposes, potentially disrupting operations or causing irreversible damage.
- Loss of Trust: If penetration testers do not adhere to predefined boundaries and rules, it can lead to a loss of trust between the testing team and the organization, compromising future security efforts.

Proposed Solution

- Clear Definition of Boundaries and Rules: Establish explicit boundaries for post-exploitation activities, including which systems can be accessed, what level of data interaction is allowed, and how far lateral movements can extend. These boundaries should be aligned with the criticality and sensitivity of systems.
- Use of Pre-Approved Tools: Specify and approve the tools and methods that can be used during the post-exploitation phase to ensure they are suitable for the target environment and do not exceed necessary force or impact.
- Continuous Monitoring and Oversight: Implement real-time monitoring of the penetration testing activities to ensure compliance with the established boundaries. This should include mechanisms to immediately halt activities if they threaten to go beyond safe limits.
- Stakeholder Involvement and Communication: Keep stakeholders continuously informed during the testing process, especially during critical phases like post-exploitation. Regular updates and immediate reporting on rule deviations are essential for maintaining trust and control.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Enhanced Realism and Relevance: By simulating real-world attacks within controlled boundaries, the test can provide deep insights into potential security lapses and the effectiveness of existing controls, enhancing the relevance of the findings.
  - Minimized Risk of Damage: Careful control and monitoring help to minimize the risk of unintentional damage or disruptions, ensuring the organization's operations can continue unaffected.
- Cons:
  - Resource Intensity: Maintaining strict oversight and using only pre-approved tools require significant resources, both in terms of technology and manpower.
  - Potential Underestimation of Threats: By limiting the scope of actions during the post-exploitation phase, there is a risk that not all security vulnerabilities will be discovered, potentially leaving some areas untested.

3.6.4 Handling Sensitive Data and Systems

Related MITRE ATT&CK Technique(s)

- T0811 Data from Information Repositories
- T0893 Data from Local System
- T0868 Detect Operating Mode
- T0801 Monitor Process State
- T0861 Point & Tag Identification
- T0852 Screen Capture

The risk-related challenges of the test and proposed mitigation strategies mirror those previously detailed in the PLANNING AND SCOPING section of this document.

3.7 MITRE ATTACK ICS tactics – Command and Control

3.7.1 Risks of Disruptive and Destructive Testing Techniques

Related MITRE ATT&CK Technique(s)

- T0885 Commonly Used Port
- T0884 Connection Proxy
- T0869 Standard Application Layer Protocol

Definition

Command and Control (C2) in industrial control systems involves the mechanisms adversaries use to communicate with compromised systems within an OT/ICS environment after gaining initial access. Unlike traditional IT environments, C2 in OT/ICS environments often requires specialized protocols and communication channels designed to interact with industrial equipment. Adversaries typically establish C2 infrastructure using commonly used ports, connection proxies, or standard application layer protocols to blend in with legitimate industrial traffic, making detection challenging. This phase is critical for adversaries as it enables remote manipulation of industrial processes, potentially leading to physical consequences in critical infrastructure.

WARNING
Testing these tactics represents an extraordinarily dangerous testing scope that should be approached with extreme caution, as improper methodologies could trigger the very catastrophic impacts the assessment aims to evaluate; the editors of this guideline strongly recommend excluding these tactics from standard penetration testing scopes unless there is absolute confidence in the testing team's expertise and comprehensive safeguards are in place.

Problems and Challenges

- Operational Sensitivity: Testing C2 channels may introduce network traffic patterns or system interactions that could trigger unexpected responses in sensitive industrial equipment or disrupt critical processes.
- Testing Limitations: Many traditional C2 testing tools are designed for IT environments and may contain aggressive features that are unsafe for use in operational technology environments.
- Realistic Testing vs. Safety: Finding the balance between realistic testing (to identify actual vulnerabilities) and maintaining operational safety presents significant challenges unique to OT/ICS environments, especially in the Command and Control phase.
- Limited Test Windows: Many OT/ICS system at airport require continuous operation, severely restricting available testing windows and forcing rushed or incomplete C2 assessments.

Proposed Solution

- Simulation-First Approach: Begin with testing in isolated lab environments that simulate the production OT/ICS infrastructure before introducing any testing tools to operational environments.
- Graduated Testing Methodology: Implement a phased approach that begins with passive monitoring for C2 indicators before progressing to more active testing techniques only after safety reviews.
- OT-Specific Test Tools: Develop or select C2 testing tools specifically designed for OT environments that include safety limiters and automatic rollback capabilities to prevent unintended consequences.
- Collaborative Testing Teams: Ensure penetration testing teams include both security experts and OT engineers who understand the industrial processes and can immediately identify potentially dangerous testing actions.
- Pre-Approved Command Sets: Establish explicitly defined sets of commands that can be safely executed during C2 testing, with strict prohibitions against actions that could alter control parameters or operational states.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Identification of Real-World Vulnerabilities: Well-designed C2 testing in OT/ICS environments can reveal critical security gaps that might otherwise remain undiscovered until exploited by actual adversaries.
  - Improved Detection Capabilities: Testing helps organizations tune their monitoring systems to recognize suspicious command patterns without disrupting legitimate industrial communications.
  - Enhanced Response Procedures: Organizations can develop and validate response procedures specific to C2 persistence in industrial environments without experiencing actual incidents.

- Cons:
  - Incomplete Testing Coverage: Safety limitations often prevent comprehensive testing of all potential C2 scenarios, potentially leaving blind spots in the assessment.
  - Resource Intensity: Properly conducted OT/ICS C2 testing requires specialized expertise, equipment, and extended preparation time compared to conventional IT penetration testing.
  - Risk-Benefit Calculation: Organizations must carefully weigh whether the security insights gained justify even the minimal operational risks introduced by testing activities.

3.8 MITRE ATTACK ICS tactics – Inhibit Response Function, Impair Process Control, Impact

3.8.1 Risks of Disruptive and Destructive Testing Techniques

Related MITRE ATT&CK Technique(s)

- T0800 Activate Firmware Update Mode
- T0878 Alarm Suppression
- T0803 Block Command Message
- T0804 Block Reporting Message
- T0805 Block Serial COM
- T0892 Change Credential
- T0809 Data Destruction
- T0814 Denial of Service
- T0816 Device Restart/Shutdown
- T0835 Manipulate I/O Image
- T0838 Modify Alarm Settings
- T0851 Rootkit
- T0881 Service Stop
- T0857 System Firmware
- T0806 Brute Force I/O
- T0836 Modify Parameter
- T0839 Module Firmware
- T0856 Spoof Reporting Message
- T0855 Unauthorized Command Message
- T0879 Damage to Property
- T0813 Denial of Control
- T0815 Denial of View
- T0826 Loss of Availability
- T0827 Loss of Control
- T0828 Loss of Productivity and Revenue
- T0837 Loss of Protection
- T0880 Loss of Safety
- T0829 Loss of View
- T0831 Manipulation of Control
- T0832 Manipulation of View
- T0882 Theft of Operational Information

Definition

Penetration testing that addresses the Inhibit Response Function, Impair Process Control, and Impact tactics involves evaluating the vulnerability of an industrial control system to attacks that could prevent safety mechanisms from functioning, interfere with control processes, or cause physical consequences. These represent the most critical and dangerous areas of OT/ICS security testing, as they directly relate to an adversary's ability to cause operational disruption, equipment damage, or safety incidents.

WARNING
Testing these tactics represents an extraordinarily dangerous testing scope that should be approached with extreme caution, as improper methodologies could trigger the very catastrophic impacts the assessment aims to evaluate; the editors of this guideline strongly recommend excluding these tactics from standard penetration testing scopes unless there is absolute confidence in the testing team's expertise and comprehensive safeguards are in place.

Problems and Challenges

- Safety-Critical Testing: Many of these techniques directly involve manipulating safety systems or critical operational parameters, creating significant risk of actual harm if testing proceeds without proper safeguards.
- Prohibition of Live Testing: Complete testing of many Impact techniques is fundamentally incompatible with operational environments, as they would require actually causing disruption to verify effectiveness.
- Regulatory Compliance Concerns: Testing activities that manipulate safety systems may violate regulatory requirements or safety certifications, particularly in highly regulated industries such as the aviation.
- Difficult Risk Quantification: Organizations struggle to weigh the uncertain benefits of comprehensive testing against the known risks of disrupting production or safety systems.

Proposed Solution

- Tiered Testing Approach: Implement a multi-stage testing methodology that begins with documentation review and passive analysis before proceeding to increasingly invasive testing only under strict controls.
- "Point of No Return" Identification: For each test case, clearly identify specific actions or system states that must not be crossed to prevent unintended consequences, with automated safeguards where possible.
- Simulation and Tabletop Exercises: Supplement technical testing with human-focused exercises that simulate response to successful exploitation without requiring actual system manipulation.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Critical Vulnerability Identification: Testing these high-impact tactics, even in limited form, can reveal critical vulnerabilities that might otherwise remain unaddressed until exploited by an actual adversary.
  - Safety System Validation: Well-designed testing can validate whether safety systems function as intended when faced with cyber threats, potentially preventing catastrophic failures.
  - Regulatory Preparedness: Organizations can demonstrate due diligence in security testing to regulators without compromising operational safety.

- Cons:
  - Limited Testing Depth: Safety considerations will inevitably restrict how thoroughly these tactics can be tested, potentially leaving vulnerabilities undiscovered.
  - False Confidence: Successful limited testing or excluding from the scope may create false confidence that systems are secure against all variations of these attack techniques.
  - Expertise Requirements: These test scenarios require rare combinations of OT/ICS security expertise, process knowledge, and safety engineering skills, making proper execution challenging and expensive.

3.9 REPORTING

3.9.1 Prioritization of Findings and Recommendations

Definition

Effective reporting and prioritization of findings in penetration testing are crucial for ensuring that critical vulnerabilities are addressed promptly and appropriately, especially in environments as sensitive as airport OT/ICS systems. Penetration testing partners often lack the necessary familiarity with the specific operational processes of airports, which can lead to incorrect prioritization of findings. This can be detrimental, as it may lead to inadequate mitigation measures that do not align with the airport's operational priorities and risk exposure.

Problems and Challenges

- Insufficient Contextual Understanding: Penetration testers without in-depth knowledge of airport operations might not fully understand the implications of certain vulnerabilities within the context of airport security, safety, and operational continuity.
- Inappropriate Risk Categorization: Relying solely on generic methods to prioritize findings does not take into account the unique aspects of airport operations and the interconnected nature of OT/ICS systems.
- Misalignment with Operational Priorities: Incorrect prioritization can lead to security resources being allocated inefficiently, potentially leaving critical vulnerabilities unaddressed while less critical issues are overemphasized.

Proposed Solution

- Custom Risk Assessment Framework: Develop and implement a custom risk assessment framework that considers the specific needs and operational contexts of the airport's OT/ICS environments. This framework should guide the prioritization of findings based on actual impact rather than generic vulnerability scores.
- Stakeholder Involvement in Reporting Process: Involve key airport stakeholders, including OT/ICS operations, security, and safety personnel, in the review and prioritization process of penetration testing findings. Their input is essential for accurately assessing the potential impact of each finding.
- Requirement for Contextual Risk Assessment Methodology: Specify that simplistic risk categorization methods, such as directly adopting published CVE scores or generic frameworks from consulting firms and penetration test companies, are not acceptable. Require proposals to include a methodology for context-based risk evaluation tailored to the specific needs of airport environments.

Potential Impact on Relevance of the Penetration Test Result

- Pros:
  - Enhanced Operational Security: By prioritizing findings based on informed assessments of operational impact, the airport can more effectively mitigate risks that pose a real threat to its operations and safety.
  - Resource Optimization: Accurate prioritization ensures that security resources are allocated efficiently, focusing on mitigating risks that could have the most severe consequences.
- Cons:
  - Complexity in Implementation: Developing a custom risk assessment framework and training external partners can be complex and resource intensive.
  - Potential Resistance from Vendors: External partners may resist adopting specialized risk assessment methods due to the increased effort and specific knowledge required.

4. Mitigation Strategy Framework for OT/ICS Penetration Testing in Airport Environments

The mitigation strategies presented form a comprehensive framework designed to integrate change management into airport environments. This framework is structured into two preparation phases: one for stakeholders and another for the penetration test team, leading to a detailed execution phase. Each phase ensures thorough coverage of security, operational integrity, and compliance during penetration testing of uptime-critical systems.

In the stakeholder preparation phase, the strategic definition of the testing scope sets the groundwork for all activities. Developing a custom risk assessment framework is crucial for understanding and mitigating threats tailored to the airport environment. Impact analyses and regulatory compliance checks align the testing process with legal and safety standards. Scheduling tests during low-activity periods reduces operational disruption, enhancing airport efficiency. Strong communication protocols and cybersecurity training for operational staff foster a security-aware culture and ensure clear role definitions. Reviewing test outcomes and securing vendor cooperation refine strategies and strengthen essential partnerships.

In the preparation phase for the penetration test team, efforts focus on the technical specifics necessary for successful testing. This includes reviewing system dependencies to mitigate indirect impacts, setting clear testing boundaries, and establishing abort criteria to manage risks. The team selects testing techniques that minimize disruption and uses sanitized, non-persistent tools with strict cleanup protocols to maintain system integrity. Rigorous checks, negotiated access, and robust non-disclosure agreements prepare and secure the team, while thorough vetting and mandatory training ensure professionalism and security expertise. Contractual obligations with audits enforce accountability.

During the execution phase, a continuous feedback loop adapts testing strategies based on real-time findings. Physical safety and segmentation checks maintain system integrity, while simulated DRP executions and backup validations ensure quick and effective system restoration. Incremental and failover testing within simulated environments allows for controlled observation of potential failures. Real-time monitoring and rapid incident response are crucial for maintaining operational continuity and system integrity, enabling the quick resolution of disruptions to keep the airport's critical systems secure and operational.

A. Preparation Phase – Stakeholders

1. Establishing testing scope
2. Custom risk assessment framework
3. Impact Analysis
4. Enhanced vendor agreements
5. Regulatory compliance check
6. Test window agreements to coincide with low-traffic or no-traffic periods
7. Communication protocols
8. Cybersecurity awareness for Operational staff
9. Post-Test review

B. Preparation Phase – Penetration Test Team

1. Test window agreements to coincide with low-traffic or no-traffic periods
2. Technical review of system dependencies
3. Establishing clear testing boundaries
4. Pre-defined abort criteria
5. Review automated and semi-automated techniques
6. Fully manual testing option
7. Review testing tools and techniques
8. Ban disruptive testing techniques
9. Use of sanitized, on-site testing tools and devices
10. Use of non-persistent tools
11. Strict cleanup protocols
12. Communication protocols
13. Penetration test team readiness assessment
14. Negotiated access agreements
15. Robust Non-Disclosure Agreements
16. Thorough vetting process
17. Education and training for all testers
18. Contractual obligations and audits
19. Requirement for contextual risk assessment methodology

C. Execution Phase

1. Continuous feedback loop
2. Physical safety checks
3. Segmentation checks
4. Pre-test full system image backup
5. Simulated Disaster Recovery Plan (DRP) execution to validate backup
6. Incremental testing
7. Failover or cold-backup testing
8. Simulated environment testing
9. Continuous real-time monitoring and oversight
10. Incident Response

The elements of the proposed framework for penetration testing on uptime-critical systems are designed to be flexible and optional. Implementing even a subset of these strategies can significantly mitigate the risks associated with penetration testing, reducing potential disruptions and enhancing system security. While each component adds a layer of protection and preparedness, it's understood that implementing the entire framework might be too complex and potentially excessive for some environments. Organizations can therefore assess their specific needs and operational contexts to select the most relevant and impactful measures. This approach allows for a tailored implementation that balances thorough risk management with practical constraints, making it adaptable to a variety of operational scales and security requirements.

5. Glossary

ACI (Airport Council International)	Global trade association representing the world's airports and their collective interests.
ACI-E (Airport Council International - Europe)	European division of ACI that represents over 500 airports in 45 European countries.
Black-Box Testing	Security testing methodology where the tester has no prior knowledge of the system's internal workings.
CAF (UK NCSC Cyber Assessment Framework)	Framework developed by the UK's National Cyber Security Centre to assess organizations' cybersecurity posture.
Change Management	Structured approach for controlling modifications to IT systems and infrastructure to minimize disruption.
EASA (European Union Aviation Safety Agency)	EU agency responsible for civil aviation safety regulations and certifications.
ICS (Industrial Control System)	Systems used to monitor and control industrial processes, including SCADA, DCS, and PLCs.
ICS Cyber Kill Chain	Framework that describes the stages of a cyber-attack specifically tailored to industrial control systems.
ISA/IEC 62443-3	International standard specifying security requirements for industrial automation and control systems.
ISO 27001/27002	International standards for information security management systems and security controls.
IT (Information Technology)	Systems used for storing, retrieving, and sending information, typically in enterprise settings. In this document the enterprise or traditional IT environments.
MITRE	Non-profit organization that operates research and development centers sponsored by the US federal government.
MITRE ATT&CK	Knowledge base of adversary tactics and techniques based on real-world observations.
MITRE ATT&CK Enterprise	Framework focused on adversary tactics and techniques used against enterprise IT environments.
MITRE ATT&CK ICS	Extension of the ATT&CK framework specifically addressing industrial control system environments.
MITRE ATT&CK Tactics	Categories representing the "why" of an ATT&CK technique or sub-technique.
MITRE ATT&CK Techniques	Specific methods used by adversaries to achieve tactical goals.
NIS (Network and Information Systems) Directive	EU legislation aimed at improving cybersecurity across the European Union.
NIS2	Updated version of the NIS Directive expanding scope and strengthening security requirements.
NIST (National Institute of Standards and Technology)	US federal agency that develops technology standards and guidelines.
NIST SP 800-53	Publication providing security and privacy controls for federal information systems and organizations.
NIST SP 800-82	Guide to industrial control systems security published by NIST.

OT (Operational Technology)	Hardware and software that monitors and controls physical devices and processes.
Part-IS	Aviation-specific information security program requirements for airports and air navigation service providers developed by EASA.
Penetration Testing	Authorized simulated attack against a computer system to evaluate its security.
Red Teaming	Advanced form of penetration testing that simulates a full-scale, targeted attack from multiple vectors.
Vulnerability Assessment	Process of identifying, classifying and prioritizing vulnerabilities in computer systems and networks.
Vulnerability Scanning	Manual, or automated process of proactively identifying security vulnerabilities in systems, networks, and applications.
White-Box Testing	Security testing methodology where the tester has complete knowledge of the system's internal workings.