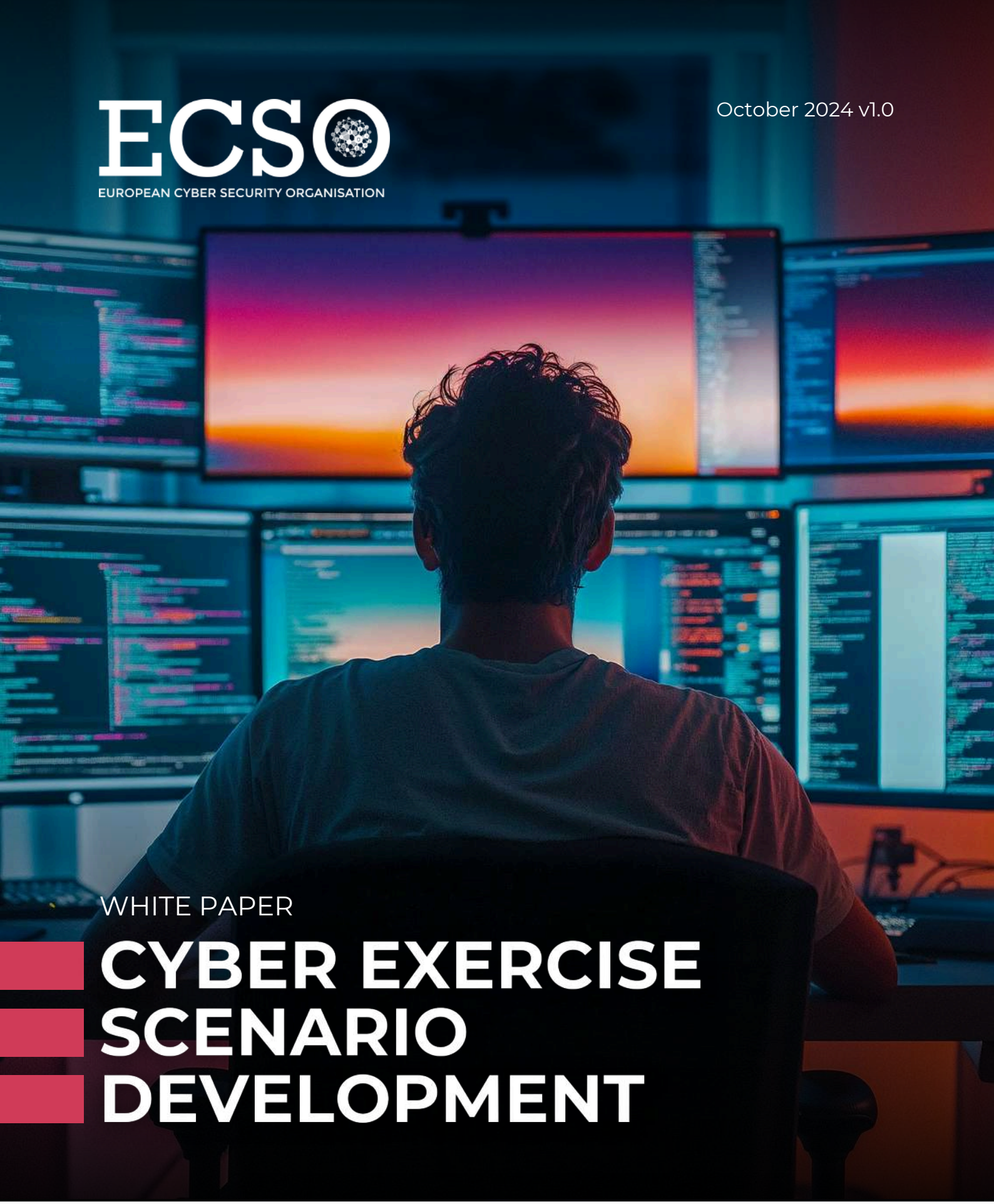
ECSO
EUROPEAN CYBER SECURITY ORGANISATION

October 2024 v1.0



WHITE PAPER

CYBER EXERCISE SCENARIO DEVELOPMENT

WORKING GROUP 5
Skills & Human Factors
Training & Cyber Ranges Workstream

ecs-org.eu

DISCLAIMER

The use of the information contained in this document is at your own risk, and no relationship is created between ECSO and any person accessing or otherwise using the document or any part of it. ECSO is not liable for actions of any nature arising from any use of the document or part of it. Neither ECSO nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Third-party sources are quoted as appropriate. ECSO is not responsible for the content of the external sources, including external websites referenced in this publication.

COPYRIGHT NOTICE

ACKNOWLEDGEMENTS

Main editors: Csaba Virág (CYBER RANGES), Donna O'Shea (MTU/Cyber Ireland), and Matteo Merialdo (Nexova Group).

Contributors: Almerindo Graziano from CYBER RANGES and Dr Anila Mjeda, Mr Dean Brennan, and Dr George O'Mahony from Munster Technological University (Cyber Ireland).

Thanks to all WG5 members who provided feedback on the document.

ABOUT

The **European Cyber Security Organisation (ECSO)** is a not-for-profit membership-based organisation established in 2016. Uniting more than 320 stakeholders, ECSO develops a competitive European cybersecurity ecosystem that provides trusted cybersecurity solutions, advances Europe's technological independence, and unifies its cybersecurity posture. ECSO also leads the European project ECCO, supporting activities needed to develop, promote, coordinate and organise the European-level Cybersecurity Competence Community.

EMPOWERING EUROPEAN CYBERSECURITY COMMUNITIES

CONTENTS

INTRODUCTION & BACKGROUND

1.

1.1. Purpose of the White Paper

This White Paper aims to provide a comprehensive guide to the development process of cyber exercise technical scenarios, grounded in real-life use cases. It sets forth a joint understanding and approach to cyber exercise methodologies among European cyber exercise service providers. The document offers an in-depth guidance to cyber exercise types, scenario development processes, and customisation techniques to ensure the effectiveness and relevance of each exercise. Readers should also refer to other documents that also contribute to a shared understanding and practical guides on how to develop different types of cyber exercises such as Tabletops,[1] [2] [3] [4] national exercises, [5] and various other open source[6] and academic contributions[7] [8] etc.

1.2. Target Audience

The target audience for this White Paper includes cybersecurity professionals, organisations seeking to enhance their security posture, cyber exercise service providers, education, and training institutions, along with stakeholders responsible for designing, implementing, and evaluating cyber exercises. Additionally, this guide will be beneficial for decision-makers who seek to understand the value of conducting cyber exercises and the role they play in strengthening an organisation's cybersecurity defences.

1.3. The Role of Cyber Exercises

Cyber exercises play a crucial role in preparing organisations to face the dynamic threats in today's cybersecurity landscape. These exercises simulate real-world scenarios, allowing participants to test and refine their skills, processes, and technologies in a controlled environment. They enable organisations to assess their preparedness, identify weaknesses, and improve their overall cybersecurity posture. By conducting regular cyber exercises, organisations can better anticipate, detect, and respond to cyber threats and minimise the potential impact of an actual attack.

[1] https://thegfce.org/wp-content/uploads/Deliverable-1-Intro-to-TTX-Final-Version.pdf

[2] https://csrc.nist.gov/glossary/term/tabletop_exercise#:~:text=Definition(s)%3A,to%20a%20particular%20emergency%20situation

[3] https://www.pwc.com/gx/en/issues/crisis-solutions/tabletop-exercises.html

[4] https://pubs.naruc.org/pub/615A021F-155D-0A36-314F-0368978CC504

[5] https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide

[6] https://documentation.opencyberrange.ee/docs/

[7] Muhammad Mudassar Yamin, Basel Katt, Modeling and executing cyber security exercise scenarios in cyber ranges, Computers & Security, Volume 116, 2022, 102635, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2022.102635. (https://www.sciencedirect.com/science/article/pii/S0167404822000347)

[8] Vykopal J, Vizvary M, Oslejsek R, Celeda P, Tovarnak D. Lessons learned from complex hands-on defence exercises in a cyber range. In2017 IEEE Frontiers in education conference (FIE) 2017 Oct 18 (pp. 1-8). IEEE.

While this publication describes the importance of cyber exercises as an overall approach it is important to highlight that cyber exercises are a collection of multiple elements into one coherent activity. The different elements can provide value on their own, like a technical scenario for training purposes.

1.4. Benefits of Cyber Exercise Scenarios

Well-designed cyber exercise scenarios offer numerous benefits to participating organisations, which are further outlined below:

1. Improve Incident Response Plans (IRPs) by assessing the communication and collaboration among team members, and uncovering gaps in security policies, procedures, and infrastructure.

2. Provide insights into how an organisation's cybersecurity defences might fare against real-world threats, helping identify areas for improvement and prioritising remediation efforts.

3. Enhanced tool for cybersecurity training and practice enabling users to develop a comprehensive set of real-world applicable skills and the experience the real-world threats/scenarios needed to identify, analyse, and respond to cyber threats.

CYBER EXERCISE TYPES

2.

Cyber exercises assess specific aspects of an organisation's cybersecurity posture. Cyber exercises vary in complexity, scope, and objectives, allowing organisations to select the most appropriate type based on their needs, resources, and desired outcomes. Selecting the right type of exercise (or combination of them) ensures the organisation achieves its overall objectives for their needs.

2.1. Tabletop Exercises

Tabletop exercises are discussion-based simulations (scenario modelling) that focus on evaluating an organisation's strategic and tactical decision-making capabilities. Participants engage in a facilitated discussion of a hypothetical cyber incident, reviewing existing policies, procedures, and resources to determine the most effective response. Tabletop exercises are cost-effective and provide a low-pressure environment for participants to identify areas of improvement and share best practices.

2.2. Walkthrough Exercises

Walkthrough exercises involve a step-by-step review of an organisation's incident response procedures in the context of a simulated cyber incident. Participants follow their documented plans and procedures, identifying any gaps, inconsistencies, or areas for improvement. This type of exercise enables organisations to assess the effectiveness of their incident response plans and ensure that all team members understand their roles and responsibilities during an actual event.

2.3. Full-Scale Exercises

Full-scale exercises are the most complex and resource-intensive type of cyber exercise. They simulate a realistic, multi-faceted cyber incident, requiring participants to execute their incident response plans and utilise their technical skills, tools, and resources. Full-scale exercises test an organisation's ability to detect, analyse, and mitigate cyber threats in a high-pressure environment, providing valuable insights into the effectiveness of their cybersecurity defences and capabilities.

2.4. Cyber Drills

Cyber drills are practical, hands-on exercises designed to test specific cybersecurity skills, processes, or technical capabilities within an organisation. They are typically designed to address a narrow aspect of an organisation's cyber defence, such as a particular security control, incident response procedure, or malware analysis. Cyber drills provide targeted training and assessment, facilitating real time monitoring of exercise progress metrics, thereby allowing organisations to identify gaps and improve the preparedness of their security personnel in a controlled environment.

CYBER EXERCISE SCENARIO DEVELOPMENT PROCESS

3.

To simplify how to develop a cyber exercise scenario, we have defined five steps which are further explained below and in the section 'Example Scenarios' we have provided three examples on how these steps are implemented.

Before commencing the development process, it's essential to establish clear scenario constraints, including budget, time, and resource limitations, and communicate these to all involved. The scenarios must also be crafted to challenge participants effectively. They should require the application of knowledge, skills, and expertise in a realistic setting, thereby providing a practical, hands-on experience. It's important to strike the right balance in terms of difficulty – the scenarios should be neither too easy nor excessively hard. Maintaining a positive level of stress is key to keeping participants engaged and focused. Whether it's for simple tabletop exercises or comprehensive full-scale simulations, the scenarios should be designed to test and refine the participants' abilities in a realistic and engaging manner, reflecting the actual challenges they may face in their professional environment.

After the exercise is conducted it is also important to debrief participants and gather feedback on their experience. Analyse the exercise results based on the predefined evaluation criteria, and identify strengths, weaknesses, and areas for improvement in the organisation's ability to detect and respond to supply chain attacks. Use the insights gained from the exercise to enhance the organisation's cybersecurity posture. This may involve updating security policies and processes, investing in new security technologies, or implementing additional training and awareness programmes.

STEP 1
DEFINE EXERCISE OBJECTIVES

Clearly defining the goals and objectives of a cyber exercise is crucial for its success. Goals should reflect the higher-level purpose of the exercises, aligning with the organisation's cybersecurity strategy and risk profile. Objectives should focus on the most relevant and critical areas that are exercised, like technical capabilities and methodologies. Examples of exercise objectives can include testing incident response capabilities, evaluating communication processes, and identifying gaps in security policies. One should ensure that the objectives are specific, measurable, achievable, relevant, and time-bound (SMART) to facilitate effective assessment and evaluation. At the end of this step you should have defined SMART goals for the exercise objectives.

STEP 2
IDENTIFY PARTICIPANTS & STAKEHOLDERS

Defining the participants and stakeholders involved in the cyber exercise is part of the objective of the exercise and essential for effective planning and execution. Participants may include internal teams such as IT, security, legal, and management, as well as external entities like vendors, partners, regulators, and law enforcement agencies. Consider the roles and responsibilities of each participant, their level of expertise, and how they will contribute to the exercise's success. In this step, it may also be beneficial to detail how these stakeholders receive threat intelligence information at

the operational, tactical, and strategic levels. Providing this detail may assist in defining the relevant injects in the scenario in step 4 and how information flows between the different stakeholders at different levels of the organisation, i.e. with different decision-making responsibilities.

Based on the above, at the end of this step you should have clearly identified the participants and stakeholders, their role in the exercise, their role/responsibilities with level of threat intelligence information available to them (listed as bullet points or in a table).

STEP 3
DETERMINE SCENARIO SYSTEM ENVIRONMENT

Scenarios can vary greatly, ranging from simple, targeted attacks on a single system to complex, large-scale assaults that affect the entire infrastructure. Given the variation involved, it is important when designing the scenario to determine the scenarios' technical configuration including the components, systems and actors involved. As part of this technical configuration, it is important to identify the variety and quantity of unique resources required to execute the scenario. This could involve a detailed arrangement of virtual machines (VMs), containers, user lists, Active Directory (AD) integration, network segments, devices, and OS builds, all tailored to the scenario use case.

The technical configuration can be highly complex, but when designing it, it is important to remember not to over- or under-complicate the configuration. For instance, in a scenario focused on spotting malicious traffic, the complexity and scale can be minimal while still effectively meeting the exercise's objectives. In such a case, only a traffic generator and a machine with a traffic monitor might be necessary. This contrasts with other scenarios that may require a full-scale model of the organisation's entire system and procedures.

The introduction of attack elements and Tactics, Techniques, and Procedures (TTPs), along with the use of open-source intelligence (OSINT), should be calibrated based on the designed complexity. Moreover, the integration of vulnerabilities and the configuration of security appliances should be aligned based on the scale of the scenario. This scale can vary greatly, ranging from simple, targeted attacks on a single system to complex, large-scale assaults that affect the entire infrastructure. This flexibility allows for tailored exercises that accurately test the required aspects under various conditions, ensuring a realistic and practical training experience.

At the end of this step, it is recommended that a clearly defined architecture including a diagram, if possible, of the elements required to enable the reproduction and execution of the scenario.

STEP 4
DESIGN REALISTIC SCENARIOS BASED ON RELEVANT CYBER THREATS

The scenario when designed should be divided into clear phases, such as preparation, detection, response, and recovery, to help participants focus on specific aspects of the incident lifecycle and evaluate their performance at each stage.

During the preparation phase, it's essential to balance realism and relevance, which are key to maintaining engagement and ensuring the practical applicability of the exercise – along with managing costs. This involves crafting scenarios that are based on relevant cyber threats and vulnerabilities, either fully tailored to the specific environment, infrastructure, and threat landscape of the organisation, or using generic environment when the focus is on skills like firewall development or malware analysis where customisation has low added value.

Digital assets and artifacts like simulated networks and mock data files are crucial for creating realistic settings. However, their use and inclusiveness depend on the exercise's format; some scenarios may not rely heavily on these components. Assets, like developed virtual machines or containers that represent the exercise security devices, desktops, servers, routers, etc., need to be developed and configured in accordance with the scenario overview and the selected attack vectors and TTPs.

The VMs or containers also act as the injection and trigger points. Injects are pre-planned events or pieces of information introduced into the scenario to prompt specific actions, decisions, or responses from participants, whereas triggers are conditions or events that initiate or escalate the scenario, such as a security alert or a suspicious email. When designing the scenario, it is recommended to design injects and triggers to test participants' ability to detect, respond to, and mitigate threats effectively. Additionally, media injects, such as simulated news reports or social media updates; network traffic or user simulations, etc can also be incorporated to add depth and realism to exercises, providing participants with a diverse range of challenges and learning opportunities.

Using the output from the previous step, in this step it is expected that the Tactics, Techniques and Procedures (TTPs) are defined that enables the end user to implement the scenario using the designed architecture.

STEP 5
SCENARIO VALIDATION & EVALUATION

Once the scenario is designed and environment setup established, the exercise should be validated to ensure the scenario aligns with participant's infrastructure and meets all objectives, with a focus on verifying the functionality of injects, triggers, and monitoring systems.

Once validated, monitoring requirements should be identified and configured within the exercise environment. These monitoring requirements may include evaluation criteria and metrics to measure the success of the exercise and participants' performance. For example, time taken to detect and respond to incidents, the accuracy and completeness of incident reports, the effectiveness of communication and collaboration, or the number of identified vulnerabilities and gaps. It is important to establish a process for collecting, analysing, and reporting on this data to inform improvements and future exercises. If automated monitoring capabilities are available, many of these aspects can be integrated into real-time progress where both the participant and exercise controllers can see when certain tasks or objectives have been completed.

At the end of this step, evaluation metrics and KPIs to assess the quality and outcome of the scenario should be defined which results against the KPIs included.

EXAMPLE SCENARIOS

4.

The following section provides examples of the expected outcome of each step defined in the previous section. The examples are not meant to be prescriptive and the outcome and format will vary depending on the scenario and level of detail required by the organisation.

4.1. A Passive Reconnaissance Informed Spear Phishing Campaign Using Malicious Files and Third-Party Executables

STEP 1
DEFINE EXERCISE OBJECTIVES

This training scenario aims to enhance the IT security teams ability against a real-world attack where the objective of the attacker is to remain hidden as long as possible (advanced persistent threat).

The IT security team must SPECIFICALLY learn the danger of spear-phishing as an initial access and pathway to compromise, and the Tactics and Techniques used by attackers to gain access and escalate privileges. The IT Security team will also learn how to implement Intrusion Detection System (IDS), Security Information and Event Management (SIEMs) and other defensive tools to detect and respond to such attacks and how to bypass them from an attacking perspective. The IT security team performance will be MEASURED by their ability to perform passive reconnaissance, develop a spear phishing email with a malicious attachment and escalate privileges to access data to an internal data server.

The cyber-exercise is RELEVANT as security reports such as the IBM X-Force Threat Intelligence Index 2023, state that 41% of incidents involve phishing for initial access and phishing operations continue to be the top pathway to compromise. It is also RELEVANT as 62% of phishing attacks use spear phishing attachments as attackers prefer weaponized attachments, deployed by themselves or in a combination with links. This exercise is TIME-BOUND with the duration of 6hrs and will take place on DATE.

STEP 2
IDENTIFY PARTICIPANTS & STAKEHOLDERS

The scenario is focused on internal stakeholders within the organisation and includes:

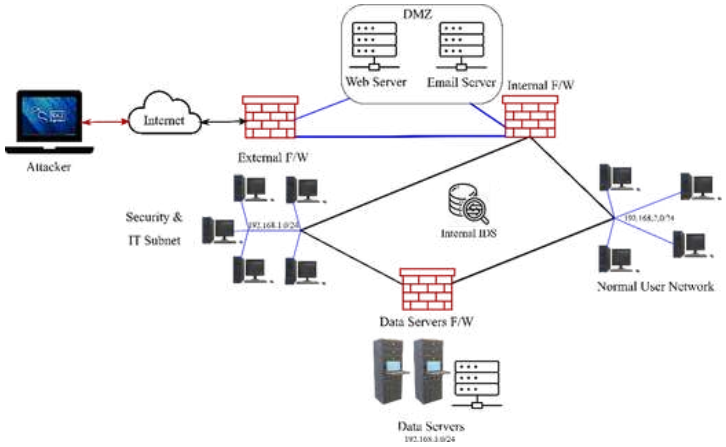
- IT Team with security responsibility – this team includes the CISO (10 years experience), senior IT engineer (7 years experience) with responsibility including the management and maintenance of data servers and firewalls, and junior security engineer who has recently graduated with an IT Management Degree (<1 year experience).
- Board of organisation – the board and in particular its IT steering committee who are interested in the evaluation of the scenario.

STEP 3
DETERMINE SCENARIO SYSTEM ENVIRONMENT

Deploy the architecture as per the example scenario environment. Develop an example organisation, design an associated website, and run a web server and email server in a DMZ. This website should have a variety of typical public information available and include a sensitive information disclosure which can be used in conjunction with the publicly available information to develop a spear phishing campaign.

Setup external, internal and data server firewalls as per the network exercise environment where the web server is publicly accessible. Allow access from one or multiple users in the security & IT subnet to the data servers where the required attack end goal resides. The sensitive data disclosure on the website should identify the target for the spear-phishing campaign inside the security subnet.

If Active Directory is required, then it can be implemented with multiple users and one domain admin.



STEP 4
DESIGN THE SCENARIO

The scenario "A Passive Reconnaissance Informed Spear Phishing Campaign using Malicious Files and Third-Party Executables" is designed based on a real-world social engineering attack using both a spear-phishing email with a malicious attachment and a spear-phishing attack using LNK files. This scenario is also linked to the stages of the cyber kill chain model.

The TTPs include:

- Tactics include TA0001 Initial Access, TA0002 Execution, TA0003 Persistence, TA0004 Privilege Escalation. The Techniques.
- Techniques include T1566 Phishing – T1566.001 Spearphishing Attachment, T1059 Command and Scripting Interpreter, T1204.002 User Execution – Malicious File, T1543.003 Create or Modify System Process – Windows Service, T1574 Hijack Execution Flow.
- Procedure
    - Conduct Passive Reconnaissance on the available webserver and develop a spear-phishing email based on an urgent Security Patch or similar. This email can also be sent from a variation of the example organisation domain.
    - If a more elaborate scenario is required, the email can be sent to the "Normal user network" and an attack path developed to gain access to the Security & IT subnet.
    - Prepare a library file and embed it in a .zip file to be attached to the email.
    - The library file will connect to an Attacker controlled "wsgidav" server which contains two malicious files. An "auto-config" shortcut and a PDF. Both will connect back to listeners on the attacker machine and provide initial shell access.
    - The attacker will need to have three listeners and serve a web server hosting Powercat, mimikatz and others.
    - The other malicious method would be a malicious link to a recognised third party .exe which has been altered to contain malicious code which will provide a reverse shell on execution and a way to bypass certain anti-virus software.
        - Example Tool: Shellter

- Set up the pivot point using the initial target and proxychains.
- Conduct enumeration and develop a lateral movement plan.
  - If AD is present, the goal is to get domain admin access through AD enumeration and mimikatz.
- Execute persistence and privilege escalation:
  - Service Binary Hijacking
  - Service DLL Hijacking
  - Unquoted Service Paths
  - Scheduled Tasks
  - Gain access to the Data Servers

STEP 5 EVALUATE THE SCENARIO

The scenario needs to be validated to ensure it works as expected and meets the defined objectives. This requires a full run-through and peer review of the developed scenario and all associated elements, including evaluation points, before deployment. Scenario validation is a critical quality control step that ensures the cyber range scenario meets its intended objectives, is technically sound and realistic, engages participants effectively, and avoids any unintended negative impacts.

For evaluation criteria, specific files or "flags" can be included in the environment and used as proof of privilege escalation, lateral movement and access to internal servers. The developed phishing campaign can be entered into a report style "Scenario Quiz" where the campaign can be evaluated for real-world effectiveness as part of the post-exercise debriefing. Other criteria can include process monitoring checks to identify the malicious connections and using IDS logs and SIEMs to identify malicious services and network connections. Additional evaluation checks can be included as part of an incident report which details the IT Security team's passive recon, malicious attachment development and implementation of IDS, SIEMs and other defensive tools to detect and respond to such attacks and how to bypass them from an attacking perspective. This report along with the phishing campaign would be essential elements of the post-scenario debriefing.

If the cyber range includes automatic grading or monitoring capabilities, many of these evaluations can be built into the exercise for real-time and post exercise analysis using, for example, file access, file content, process monitor, registry monitor, network connections, network listeners or remote port monitoring agents.

Once the exercise is completed or time limit reached, debrief participants and gather feedback on their experience. Analyse the exercise results based on the predefined evaluation criteria and submitted scenario reports, and identify strengths, weaknesses, and areas for improvement in the organisation's ability to detect and respond to a passive reconnaissance informed spear phishing campaign using malicious files and third-party executables. Any feedback collected from participants should be incorporated back into the scenario design where appropriate.

4.2. Supply Chain Attack

STEP 1
DEFINE EXERCISE OBJECTIVES

This training scenario goal is to understand supply chain attacks through a specific use case i.e. the SolarWinds attack. In the SolarWinds attack the threat actor compromised the software update mechanism of SolarWinds' Orion platform. The attackers inserted a backdoor, called "SUNBURST," into the software, which was then distributed to thousands of customers through legitimate software updates. Once the compromised updates were installed, the attackers gained unauthorised access to the networks of the affected organisations, allowing them to conduct espionage and potentially disrupt operations.

In this scenario, the organisation must SPECIFICALLY understand the Techniques, Tactics, and Procedures (TTPs) employed by Advanced Persistent Threat (APT) actors in supply chain attacks. The team’s performance will be MEASURED by their ability to detect, respond and recover to the attack. This cyber exercise is RELEVANT due the increased dependency on third party software and risks associated with software supply chain attacks and the importance of implementing robust security controls to mitigate this risk. This exercise is TIME-BOUND with the duration of 6hrs and will take place on DATE.

STEP 2
IDENTIFY PARTICIPANTS & STAKEHOLDERS

The SolarWinds attack use case can be relevant to various target audiences, including:

- IT and security teams: To help them understand the TTPs employed by APT actors and learn how to detect, respond to, and remediate supply chain attacks.
- Executives and decision-makers: To emphasise the potential impact of supply chain attacks on business operations, reputation, and regulatory compliance, and encourage them to invest in appropriate security measures.
- Third-party software vendors: To highlight the importance of secure software development practices and the need to maintain a secure software supply chain.

STEP 3
DETERMINE SCENARIO SYSTEM ENVIRONMENT

Design the cyber range environment either using an existing vendors' platform or using open-source tools and platforms, such as network simulators (e.g., GNS3), virtualization platforms (e.g., VirtualBox), and testing tools (e.g., Kibana, Wireshark, Metasploit, etc). This will enable participants to focus on the skills and techniques required to detect and respond to supply chain attacks, rather than on specific vendor products.

STEP 4
DESIGN THE SCENARIO

- Reconnaissance: The attacker identifies the target organisation and researches its third-party software dependencies.
- Weaponization: The attacker creates a backdoor and embeds it in the third-party software.
- Delivery: The attacker compromises the software vendor's update mechanism and distributes the malicious update to the target organisation.
- Exploitation: The target organisation installs the compromised update, allowing the attacker to exploit the backdoor.
- Installation: The backdoor is installed on the organisation's systems, providing the attacker with persistent access.

- Command and Control (C2): The attacker establishes communication with the compromised systems to remotely control them.
- Actions on Objectives: The attacker conducts espionage or other malicious activities within the target organisation's network.

Create injects, or simulated events, that represent various stages of the cyber kill chain. These injects should be designed to challenge participants' ability to detect, respond to, and remediate the simulated attack. Develop evaluation criteria to measure the performance of participants in the exercise, such as the time taken to detect the attack, the effectiveness of incident response actions, and the ability to collaborate across teams.

STEP 5
EVALUATE
THE SCENARIO

The scenario needs to be tested to ensure it works as expected and meets the defined objectives. This could involve a small-scale run-through or a peer review. Scenario validation is a critical quality control step that ensures the cyber exercise meets its intended objectives, is technically sound and realistic, engages participants effectively, and avoids any unintended negative impacts.

4.3. Ransomware Attack – DarkSide Use Case

STEP 1
DEFINE EXERCISE OBJECTIVES

This scenario aims to offer an immersive learning for applying theoretical knowledge and refining practical skills essential for combating sophisticated ransomware attacks, taking cues from the DarkSide ransomware incident that targeted critical infrastructure in 2021.

The 2021 DarkSide ransomware attack notably affected a regional energy company, Colonial Pipeline, responsible for nearly half of the US East Coast's fuel supply. This attack disrupted crucial operations overseeing oil and gas distribution while also exfiltrating 100 GB of corporate data, underscoring widespread concerns regarding the susceptibility of essential services to ransomware threats.

The IT security team must SPECIFICALLY acquire specific skills in malware analysis, enabling the identification of Indicators of Compromise (IOCs), analysing malware behaviour through black box and white box approaches (malware reverse engineering), and devising effective response strategies to mitigate the attack's impact. The IT security team performance will be MEASURED on their proficiency in identifying and analysing IOCs associated with a malware attack, along with their competence in conducting static and dynamic analyses using precise metrics (e.g., identifying file system changes, registry modifications, networking activities, and malware defences).

This cyber-exercise is RELEVANT due to the escalating frequency of ransomware attacks, as reported in the 2023 State of Ransomware report. The evolving ransomware-as-a-service (RAAS) business model adopted by contemporary criminal groups is expected to contribute to this rising trend, emphasizing the urgent necessity for robust cybersecurity measures, rapid incident response strategies, and collaborative defence mechanisms to safeguard critical infrastructure against future threats. This exercise is TIME-BOUND with the duration of 6hrs and will take place on DATE.

STEP 2
IDENTIFY PARTICIPANTS & STAKEHOLDERS

The DarkSide attack use case can be relevant to various target audiences, including:

- IT and security teams: This case aids in comprehending the Tactics, Techniques, and Procedures (TTPs) utilised by Advanced Persistent Threat (APT) actors. It serves as a learning opportunity to detect, respond to, and mitigate ransomware attacks effectively.
- Executives and decision-makers: It underscores the potential consequences of ransomware attacks on business operations, reputation, and regulatory adherence. Encouragement is provided to invest in suitable security measures to counter such threats.
- Lawmakers and Politicians: This case serves to emphasise the criticality of securing essential infrastructure, highlighting the imperative need for stringent measures to safeguard critical systems.

STEP 3
DETERMINE SCENARIO SYSTEM ENVIRONMENT

Design the cyber range environment by employing either an established vendor's platform or utilising open-source tools and platforms. These may involve network simulators like FakeNet-NG, virtualization platforms such as VirtualBox, and diverse testing tools like Strings, PEStudio, ProcMon, Wireshark, and Metasploit. By leveraging these resources, participants can focus on mastering the skills and methodologies essential for malware analysis, rather than relying on specific vendor-based products.

A potential design utilising non-vendor specific and open-source tools could encompass several Virtual Machines (VMs) featuring different operating systems and patch levels akin to those used within the organisation. This setup could operate on virtualization platforms equipped with snapshot restoration capabilities, such as VirtualBox and incorporate open-source tools for malware analysis, such as the prepackaged tools available in FLARE VM designed for Windows systems. Additionally, integrating Mail, DNS, Web servers, or utilising tools like FakeNet-NG to replicate network behaviours within the environment can simulate realistic scenarios for comprehensive training.

STEP 4
DESIGN THE SCENARIO

Within the Cyber Range Environment:

- Establish Initial Attack Vector & Context: Replicate the initial attack vector, possibly through a simulated phishing email, or provide access to simulated logs, network traffic captures, ransom notes, or malware samples. Tailor the complexity of the scenario to align with the participants' diverse expertise profiles.

- Conduct Static Analysis: Employ tools like HashmyFiles, Detect It Easy, Strings, CAPA, and PEStudio to scrutinize Indicators of Compromise (IOCs) such as file hashes, suspicious domains, IP addresses, email headers and other strings of interest, and any indicators associated with the DarkSide ransomware.

- Conduct Dynamic Analysis: Utilise malware analysis tools (e.g. Regshot, ProcMon, Wireshark, etc) within the cyber range to delve into the dynamic behaviour, communication patterns, and encryption techniques used by DarkSide.

- Malware Reverse Engineering: Dissect ransomware samples in a controlled environment through malware reverse engineering. Explore the malware's code, decryption methods, Command and Control (C2) communication, and any obfuscation or anti-analysis mechanisms employed by DarkSide.

Post-mortem team-exercise follow-up:

- Incident Response Planning and Mitigation: Task teams to create mitigation plans to contain the analysed attack. Detail the steps to restore affected systems, and prevent further damage. Emphasise the importance of isolating infected systems, applying patches, strengthening security measures, and developing strategies to recover encrypted data without yielding to ransom demands.

- Reporting and Recommendations: Each team compiles a detailed report outlining their findings. This includes an overview of analysed IOCs, attack methodologies, mitigation strategies, and recommendations to bolster the company's cybersecurity defences against future threats.

STEP 5
EVALUATE
THE SCENARIO

The scenario needs to be tested to ensure it works as expected and meets the defined objectives. This could involve a small-scale run-through or a peer review. Scenario validation is a critical quality control step that ensures the cyber exercise meets its intended objectives, is technically sound and realistic, engages participants effectively, and avoids any unintended negative impacts.

For evaluation criteria, an approach akin to a Malware Analysis report style can be adopted. This involves documenting specific information such as file system changes, registry modifications, networking activities, malware defence mechanisms, and proposed recovery and cleanup strategies. This documentation can be evaluated for real-world effectiveness of these elements as part of the post-mortem phase of the exercise.

SCENARIO CUSTOMISATION & ADAPTATION

5.

5.1. Organisation-Specific Considerations

Customise scenarios to reflect the unique aspects of each organisation, such as its size, industry, infrastructure, and threat landscape. Adjust the scenario's complexity, scale, or objectives to align with the organisation's specific needs, capabilities, and risk tolerance. Consider the organisation's existing cybersecurity policies, procedures, and technologies, as well as any unique vulnerabilities or requirements. Additionally, ensure the inclusion of an appropriate number of devices and resources to accurately represent the organisation’s environment required to meet the exercise objective. The scale and diversity of resources should be sufficient to provide a comprehensive and realistic simulation, supporting the effectiveness of the cyber range and exercise.

5.2. Industry-Specific Considerations

Tailor scenarios to address the unique risks and challenges faced by specific industries. This may involve incorporating industry-specific regulations, standards, or best practices, as well as simulating threats that are particularly relevant or prevalent within the industry. Consider the potential impact of an attack on the industry's critical infrastructure, operations, or reputation.

5.3. Geographic and Regulatory Considerations

Adapt scenarios to account for geographic and regulatory factors, such as regional threat actors, legal requirements, and cultural considerations. This may involve adjusting the scenario to comply with local laws, such as data protection regulations, or incorporating region-specific threats or vulnerabilities. Consider the organisation's global footprint, including any regional offices or operations, as well as the potential impact of an attack on international relations or trade.

POST-EXERCISE ACTIVITIES

6.

6.1. Debriefing and Feedback

Conduct a debriefing session following the exercise to discuss the outcomes, challenges, and lessons learned. Encourage open and honest feedback from participants, focusing on both successes and areas for improvement. Use this feedback to refine the organisation's incident response plans, policies, and procedures, and to inform the design of future exercises.

6.2. Evaluating Exercise Outcomes

Evaluate the outcomes of the exercise against the predefined objectives and metrics. This may involve analysing the time taken to detect and respond to incidents, the effectiveness of communication and collaboration, or the number of identified vulnerabilities and gaps. Assess the organisation's overall performance and determine whether the exercise objectives were met.

6.3. Identifying Lessons Learned

Identify key lessons learned from the exercise, focusing on both strengths and weaknesses. This may include insights into the organisation's incident response capabilities, gaps in security policies, or areas where additional training or resources are needed. Document these lessons learned and share them with relevant stakeholders to ensure that improvements are implemented and knowledge is disseminated throughout the organisation.

6.4. Implementing Improvements

Develop an action plan to address the identified weaknesses and implement improvements based on the lessons learned from the exercise. This may involve updating incident response plans, revising security policies, conducting additional training, or investing in new technologies. Monitor the progress of these improvements and evaluate their effectiveness over time, adjusting the plan as needed.

Avenue des Arts 46, 1000, Brussels (Belgium)
nina.olesen@ecs-org.eu
www.ecs-org.eu