TABLETOP EXERCISE INDUSTRIAL CONTROL SYSTEMS

Based on CISA Tabletop Exercise Packages

WISEFROG
‘s-Hertogenbosch, The Netherlands
Document date: 08/10/2024

CONTENTS

EXERCISE OVERVIEW

<table>
<tr><th>Exercise Name</th><th colspan="2">Tabletop Industrial Control Systems Incident Simulation</th></tr>
<tr><td>Exercise Date, Time, and Location</td><td colspan="2">TBD</td></tr>
<tr><td rowspan="6">Exercise Activities</td><th>Time</th><th>Activity</th></tr>
<tr><td>30 Minutes</td><td>Threat Briefing and Opening Remarks</td></tr>
<tr><td>90 Minutes</td><td>Module 1</td></tr>
<tr><td>20 Minutes</td><td>Break</td></tr>
<tr><td>90 Minutes</td><td>Module 2</td></tr>
<tr><td>30 Minutes</td><td>Hotwash</td></tr>
<tr><td>Purpose</td><td colspan="2">Assess the cyber resilience of the client and their ability to secure their industrial control systems (ICS) against cyber threats.</td></tr>
<tr><td>National Institute of Standards and Technology Cybersecurity Framework</td><td colspan="2">Govern, Identify, Protect, Detect, Respond, Recover</td></tr>
<tr><td>Objectives</td><td colspan="2">Assess the resilience of the client during and following a cyber incident impacting ICS.
Improve IT and OT cybersecurity coordination to enhance organizational cybersecurity posture.
Evaluate the ability to restore operations after disruptions from cyber intrusions.</td></tr>
<tr><td>Threat or Hazard</td><td colspan="2">Cyber Incident</td></tr>
<tr><td>Scenario</td><td colspan="2">During a transition of systems to the cloud, employees receive a possibly fraudulent email, encounter odd vendor activity, and detect suspicious network traffic. After receiving reports of service disruptions, ICS failures occur, and malware encrypts systems.</td></tr>
<tr><td>Sponsor</td><td colspan="2"></td></tr>
<tr><td>Participating Organizations</td><td colspan="2">Incident response team</td></tr>
<tr><td>Points of Contact</td><td colspan="2">Insert Organization POC(s)
Contact Information</td></tr>
</table>

GENERAL INFORMATION

Building Resilience

The purpose of the National Cyber Exercise Program's CISA Tabletop Exercise Packages (CTEPs) that will executed by WiseFrog Security are to increase your organization's resilience by assessing and validating capabilities and identifying areas for improvement. The National Institute of Standards and Technology (NIST) defines cyber resilience as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources

Participant Roles and Responsibilities

Players have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario.

Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.

Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.

Note-takers are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

Exercise Structure

This exercise is intended to be a multimedia, facilitated exercise. Players will participate in the following:

- Cyber threat briefing
- Scenario modules:
    - **Module 1**: This module introduces a modernization of technology to the cloud, a possible phishing attempt, and odd vendor activity.
    - **Module 2**: This module includes reports of service disruptions, industrial control systems (ICS) failures, and malware.
- Hotwash

Structure Note: Modules, timeline dates, and discussion questions included in each module may be modified as desired

Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions.

MODULE 1 – CLOUD MIGRATION AND PHISHING RISKS

Scenario 1 – Phishing bypasses MFA, targets ICS systems

The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) release a joint alert regarding a cyber campaign targeting organizations in your sector over the past several months. Malicious actors are using sophisticated phishing schemes combined with social engineering tactics to circumvent multi-factor authentication (MFA) security measures. These malicious actors seek to compromise ICS with the intent to disrupt operations and extort victims.

Scenario 2 – Cloud Modernization for ICS

Your organization's IT and OT teams are working on a technology modernization project at your facility. This project involves multiple IT/OT vendors to assist with the development of cloud infrastructure to support ICS. This project also involves implementation of a remote access solution for technicians to monitor and control OT systems.

Scenario 3 – Phishing Attempt Targets IT/OT Staff

Several employees in the IT and OT departments receive an email that appears to be from the CEO. The email asks these employees to log in to a website to complete a questionnaire related to the ongoing modernization project. Some employees report the email as suspicious while others follow the link for the questionnaire.

Scenario 4 – MFA Fatigue Attack

Several employees receive repeated notifications from the MFA app on their phones to approve attempted log-ons. Some employees approve the requests.

Scenario 5 – OT Vendor No-Show

An OT vendor is scheduled to install equipment at one of your organization's remote facilities. A technician from your OT department calls from the remote facility to report the vendor did not show up at the scheduled time, but it appears that the equipment was already installed.

ICS monitoring tools do not report anything outside the baseline for your network.

Discussion Questions

Discussion questions included in each module are designed to explore different aspects of your operational resilience. The questions may be modified as desired.

1. Discuss your organization’s cyber resilience planning.
    a. How are IT and OT business continuity functions coordinated?
    b. What IT and OT infrastructure supports your essential functions, as documented in continuity of operations and incident response plans?
    c. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?
2. What cybersecurity threat information does your organization receive?
    a. What threat information is most useful?
    b. How is information disseminated to the relevant parties within your organization?
    c. What actions would your organization take in response to an alert like the one presented in the scenario?
3. Describe your organization’s asset management plan and how you prioritize critical assets.
    a. How does your organization maintain availability of critical or key assets (e.g., network connectivity)?
4. How does your organization baseline network activity?
    a. How do you distinguish between normal and abnormal traffic?
    b. What are your next steps when abnormal activity is detected/reported?
5. Describe the risks/advantages to maintaining legacy equipment/systems.
    a. How do you manage technology that is no longer supported by the manufacturer?
    b. What supply chain concerns do you have regarding legacy equipment/systems?
    c. Describe your organization’s equipment commissioning and decommissioning processes.
6. What level of access do your third-party vendors have to your organization’s network?
    a. How often are third-party access rights and data logs reviewed?
    b. What mechanisms or processes are in place to prevent malicious activity originating from vendors?
7. Describe your organization’s cybersecurity training program for employees.
    a. How often are employees required to complete this training?
    b. Describe the cross-training or the coordination between the IT and OT departments.
    c. What additional training is required for employees who have system administrator-level privileges?
    d. What type of training methods or approaches have you found most beneficial?
8. How do employees report suspected phishing attempts or other possible cybersecurity incidents?
    a. What actions does the IT department take when suspicious emails are reported?
    b. What feedback do employees receive after reporting a suspicious email or event?

    c. Does your organization employ phishing tests? If so, describe the conduct of the tests and how employees receive feedback/training following the tests.

9. What policies and procedures does your organization have to maintain the security of facilities, networks, and systems?
    a. What are your access control measures for both OT and IT assets and associated facilities?
    b. Where are these policies and procedures documented?

MODULE 2 – SERVICE DISRUPTIONS AND ICS FAILURES

Scenario 1 – Service Disruptions Reported

Your organization's customer support center receives an influx of calls reporting service disruptions.

Later that day, technicians monitoring your organization's various IT/OT systems notice lagging and distorted data inputs that impact their ability to monitor the equipment and processes.

Scenario 2 – System Failure Alarm

A system alarm alerts facility operators, causing a shutdown of operations due to automatic emergency fail safes. Technicians cannot access ICS controls, data is encrypted, and several employees from your IT and OT departments report being locked out of their user accounts. During physical inspection of the failed components, technicians discover there is no physical reason for the failure.

Scenario 3 – Red Screen Threat

Computers throughout your organization display a red screen with a message taking credit for the malfunctioning industrial processes and threatens to continue the IT/OT system lockout.

Scenario 4 – Vulnerability Disclosure

Security researchers disclose details of a critical vulnerability in the remote access solution shared on a hacker email list. Their report also includes information found on the dark web about Known Exploited Vulnerabilities used to compromise your organization's various IT and OT components along with sensitive information offered for sale to the highest bidder.

Discussion Questions

1. What policies and procedures does your organization have to maintain the security of facilities, networks, and systems?
    a. What are your access control measures for both OT and IT assets and associated facilities?
    b. Where are these policies and procedures documented?
2. Using your organization's cyber incident response plan (CIRP), describe the actions your organization would take to minimize impact on current operations.
    a. What guidance does the plan include on assessing the severity of the incident?
    b. How does incident severity level dictate response?
    c. How are critical systems and processes incorporated within your CIRP?
3. How does your CIRP/IT response plan incorporate OT incident response?
    a. Is your CIRP aligned with any OT incident response plans?
4. What redundant systems exist when primary systems are compromised?
    a. What alternative systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period?
    b. Does your CIRP include procedures to operate in manual mode if a cyber incident compromises OT systems?
    c. Who authorizes the use of alternate systems or procedures?
    d. How long can you perform manual or alternate processes?
5. Does your organization have backups of control files and other important files stored in a location separate from your primary working files/copies? ,
    a. How long would it take to restore primary files from backups?
    b. How frequently do you test restoration from backups?
    c. How long do you keep copies of archived files backed up?
6. What are the roles of your security operations center during a response?
7. Who is responsible for coordinating information across different organizational-level incidents?
8. How sufficient are your organization's current internal resources for responding to the cyber incidents in this scenario?
    a. What additional resources outside of your organization would be necessary for responding to the cyber incident?
    b. What are the processes or procedures for requesting additional resources?
    c. What external partners (e.g., CISA, FBI, etc.) would you contact for assistance?
9. What legal and regulatory notifications are required based on the scenario?
    a. When are notifications made and who is responsible for making the notifications?
10. Based on discussion, what changes will you implement to increase the resilience of your organization?

TRAINERS

Nariman Aga-Tagiyev is an Application Security Architect with more than 20 year experience in software development. Have been working as full stack web application developer, backend developer, DevOps engineer, cloud developer and since 2016 fully involved in Application Security related activities.

https://www.linkedin.com/in/aganariman/

Serhat Altın has a strong focus on security by design and secure configuration by default. He excels at creating user experiences that prioritize security without compromising usability, ensuring that systems are both intuitive and inherently secure from the outset. With his deep understanding of secure design principles, Serhat integrates security best practices into every stage of product development, making it easier for users to adopt secure configurations effortlessly.

https://www.linkedin.com/in/serhataltin/

TRAINING LOCATION FACILITIES

The Table Top Exercise will take place at a location selected by the hiring company within the European Union. For locations outside the EU, special quotes can be provided upon request. The following facilities are required:

- A projector and power outlet for the trainer
- Adequate space to allow participants to form working groups of 3-4 people for independent hands-on exercises

CONTACT INFORMATION

We would be happy to have a short call with you to discuss your needs and answer your questions. We do not have aggressive marketing strategy and won’t spam you if you get in touch with us.

Contact by email: security@wisefrog.nl

Contact by phone or WhatsApp: +31613732993

Schedule a 30 minutes call: https://calendly.com/aganariman/nariman-30-minutes

SUPPLIER INFORMATION

Company name	WiseFrog
Country of establishment	Netherlands
Address	Willemspoort 102, 5223WV, 's-Hertogenbosch, Netherlands
Email (Invoices)	Invoice@wisefrog.nl
Email (administrative)	info@wisefrog.nl
EU VAT-ID	NL003278436B94
KVK - Dutch Chamber of Commerce number	78029260
IBAN	NL92 ABNA 0876 9924 91
BANK SWIFT (BIC)	ABNANL2A
Contact person	Nariman Aga-Tagiyev
Contact person email	nariman@wisefrog.nl
Phone:	+31613732993

ABOUT WISEFROG

Our Story

Founded with a passion for innovation and a commitment to excellence, WiseFrog has been at the forefront of the digital landscape for over a decade. What started as a small team of visionaries has grown into a powerhouse of creative minds, dedicated to pushing boundaries and delivering cutting-edge solutions.

Our Approach

At the core of WiseFrog's philosophy lies a commitment to collaboration and innovation. We work closely with our clients, understanding their unique needs and goals, to deliver tailored solutions that drive tangible results. Our team of experts combines creativity with technical expertise, ensuring every project is executed with precision and attention to detail.

Our Mission

At WiseFrog, we bring together the dynamic worlds of creative media production, innovative product development, and robust cybersecurity. Our mission is to transform ideas into secure, impactful realities. Whether you're looking to create compelling content, develop cutting-edge products, or ensure the highest level of digital security, we're here to make it happen.

Our team consists of passionate creatives, product developers, and cybersecurity experts who are dedicated to excellence in every project we undertake. We believe that every story, product, and system deserves a meticulous and innovative approach. That's why we foster a culture of collaboration and ingenuity, ensuring that your vision is brought to life safely and effectively.

TERMS AND CONDITIONS

1. **Confidentiality**

All information shared by clients during the collaboration will be treated as confidential. Our trainers are committed to maintaining the privacy and security of any sensitive information provided. This data will not be disclosed, shared, or distributed to any third party outside of the training, except as required by law.

2. **Offer Validity**

The offer for this workshop is valid for a duration of 30 days from the date of issuance. After this period, the offer may be subject to change or withdrawal.

3. **Payment Terms**

Invoices for the training must be paid within 30 days following the completion of the workshop. Travel costs related to the workshop are not included in the quoted price and will be invoiced separately after the event. Late payments may incur additional charges or penalties as per WiseFrog's billing policy.

4. **Travel Costs**

Travel and accommodation costs incurred by trainers for on-site workshops will be billed separately after the workshop. These costs will be outlined in a detailed invoice sent to the client.

5. **Cancellation Policy**

Cancellations made up to 7 days before the scheduled training date will be eligible for a full refund. Cancellations made within 7 days of the training will not be eligible for a refund. However, substitutions or rescheduling may be allowed with prior notice.

6. **Liability**

While every effort is made to ensure the accuracy and relevance of the information provided during the training, we are not responsible for any consequences resulting from the use or misuse of the information provided. Clients are responsible for applying threat modeling practices in accordance with their own organizational policies and legal requirements.

7. **Intellectual Property**

All training materials, including presentations, handouts, and digital resources, remain the intellectual property of WiseFrog. Clients are not permitted to reproduce, distribute, or share these materials outside their organization without prior written consent.