SecOps 2024

International Exercise & Conference on Security Operations

WAR GAME

OPERATION RESILIENT SHIELD
DEFENDING AGAINST THE KILLWARE THREAT

Powered by BLACK CELL

OVERVIEW

Welcome to Operation Resilient Shield, a comprehensive Tabletop Exercise (TTX) coupled with an OT-cyber range simulation designed to test the skills, collaboration, and response capabilities of five competing teams, consisting of CSIRTs (Computer Security Incident Response Teams) and CERTs (Computer Emergency Response Teams). In this dual-layered scenario, participants will not only confront the technical challenges of cyberattacks, but also engage their decision-making skills in a war game setting, as they will face a critical threat - the activation of a sophisticated malware known as "killware", within a plastic factory. This malware compromises the facility's operations, specifically targeting the Acrylonitrile production process, which, when released into the air, can transform into hydrogen cyanide under humid conditions, posing a threat to thousands of lives.

SCENARIO

A prominent plastic factory that specializes in Acrylonitrile production, a compound used in various industrial applications, has fallen victim to a targeted cyberattack. The assailants have unleashed a potent strain of malware referred to as "killware." This malicious software has infiltrated the factory's Operational Technology (OT) and Information Technology (IT) systems, resulting in a loss of control over critical processes.

The stakes are high, as the release of Acrylonitrile into the air, when combined with humidity, can lead to the formation of deadly hydrogen cyanide gas, putting more than 10,000 lives at immediate risk. The factory's safety systems have been compromised, and it's up to the participants to regain control over the OT and IT systems to avert this catastrophic outcome.

TABLETOP EXERCISE

In addition to the technical cyber range component, Operation Resilient Shield incorporates a vital Tabletop Exercise (TTX). This segment challenges participants to engage their strategic thinking and decision-making skills in a simulated war game environment. Teams will confront a range of physical threats, including potential sabotage, espionage, and operational disruptions. Through this TTX, participants must make critical choices related to resource allocation, crisis response, communication strategies, and risk assessment to safeguard both the facility and its personnel. This integrated approach ensures that participants not only excel in cybersecurity defense but also demonstrate their ability to manage complex, real-world emergencies in critical infrastructure settings, ultimately enhancing their preparedness and resilience.

WAR GAME | 2024

SecOps 2024 International Exercise & Conference on Security Operations

KEY OBJECTIVES

Containment and Control

Teams must work quickly to identify the entry point of the killware and isolate infected systems to prevent further spread.

System Restoration

Reassert control over the factory's PLCs DCSs, IEDs, HMIs, as well as the mixed environment of Windows and Linux systems.

Collaborative Response

Foster cooperation among CSIRT and CERT members within each team to leverage their specialized skills in IT and OT security.

Malware Analysis

Analyze the killware to understand its capabilities, communication channels, and potential backdoors.

Network Recovery

Identify compromised network devices, remove unauthorized access points, and restore network functionality.

Complex decision-making

Demonstrate sound decision-making in the war game, prioritizing the safety of personnel and the integrity of the facility.

TECHNOLOGY STACK

Participants will engage with a diverse range of industrial technologies, including:

- PLCs (Programmable Logic Controllers)
- DCSs (Distributed Control Systems)
- IEDs (Intelligent Electronic Devices)
- HMIs (Human-Machine Interfaces)
- Windows and Linux systems
- Network devices

SUCCESS CRITERIA

The team's performance will be evaluated based on their ability to:

- Identify and neutralize the killware threat effectively and swiftly.
- Prevent the release of Acrylonitrile and the subsequent formation of hydrogen cyanide.
- Collaborate seamlessly between CSIRTs and CERTs to leverage expertise.
- Restore control over the OT and IT systems while minimizing downtime.

CONCLUSION

Operation Resilient Shield challenges participants to combine their technical expertise, crisis management skills, and teamwork in a high-pressure environment.

By defending against the killware threat and saving thousands of lives, participants will demonstrate their readiness to respond to real-world cybersecurity emergencies in critical infrastructure settings.

THANK YOU

for your consideration, and we look forward to the possibility of working with you.

CONTACT

https://blackcell.io/secops-24

secops@blackcell.io