IR500 Incident Response

Course Overview

IR500 - Incident Response equips students with the needed tools to implement robust defense-in-depth practices within the workplace. IR provides detailed training on proper documentation and planning for computer network defense.

The course exposes students to a variety of real-world scenarios and provides hands-on experience in event detection and recovery in an enterprise environment.

Objectives

- Provide in-depth exposure to network and systems intrusion protection methods, what to do before, during and after an event, and how to recover from events and strengthen organizational security

Target Audience

- IT and Cyber Security professionals looking to acquire hands-on experience, in the identification of and recovery from security events, and to establish and maintain a robust computer network defense posture

Estimated Course Length: 24 hours

Day 1

Day 1 introduces students to sound IR concepts focusing on proper awareness of information systems and networks, clear and up-to-date documentation and effective use of risk management theory.

Topics List

- IR today
- Network mapping and awareness
- Standard documentation requirements and options
- System and network baselining practices
- Wisdom of security auditing
- Proactive vs. reactive action
- Risk management and defense

Day 2

Students use the tools learned on Day 1 to detect a possible incident and conduct a full-spectrum analysis on a selection of corporate network systems in order to judge impact and threat to business or company data.

Topics List

- Incident detection approaches
- Baselining saves the day
- Practices for analyzing an incident
- Approaches for confirming an incident
- Using all logs for impact analysis
- Techniques for analyzing files

Day 3

Students learn to formulate a fully-realized recovery plan based on data received on a confirmed cyber incident on their company network. They will contain and eradicate threats to the network and use security auditing tools to verify success . Recovery efforts will be completed by verifying no new vulnerabilities were introduced to the network. Day 3 ends with students reporting on details of the event identification, response and recovery to organizational management.

Topics List

- Incident Recovery Plans
- Testing recovery options before/after rollout
- Standard Operating Procedures and Recovery Plans
- Approaches for confirming an incident
- Using all logs for impact analysis
- Techniques for analyzing files
- Reporting to management

Day 4

Students apply forensically-sound principles to image a machine and recover useful information from additional imaged systems. Students participate in the recovery experience and are required to update a response plan.

Topics List

- Real world recoveries
- Forensic imaging and analysis
- Maintaining clear communications
- Post-incident actions and lessons learned
- Updating documentation to prep for the next cycle

Day 5

Day 5 comprises a full-spectrum IR scenario that requires students to recover from a series of attacks discovered on a corporate network. They must scope the impacted systems, create a mitigation plan, harden weak defenses and conduct recovery efforts. This final exercise replicates a variety of network services, hardware, and configurations. The capstone reinforces exposure to tools and techniques learned during the previous four days.

Capstone Exercise

All the material covered in the course will be put to use in the final exercise.

About CYBRScore®

Comtech Mission-Critical Technologies (Comtech MCT) provides cybersecurity solutions and services tailored to training and workforce development. The CYBRScore® product portfolio was created by a team of former National Intelligence Community members who all possess the necessary hands-on, practical cybersecurity experience and abilities required to meet the needs of our demanding customer base. Our experts share the intellectual curiosity to constantly ask the 'why' and 'how' as they develop and deliver truly unique products and services to help close the growing cybersecurity skills gap. The Comtech MCT CYBRScore® offerings include off-the-shelf and custom training, hands-on skills labs, and competency-based assessments mapped to cybersecurity job roles.

CYBRScore®
Comtech Mission-Critical Technologies
275 West Street, Annapolis, MD 21401

www.cybrscore.io
ComtechMCT-CYBRScore@comtechtel.com