JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Intro to Cyber Incident Response

CYBER INCIDENT RESPONSE

What does this section cover?

- Phases of an incident response
- Creating an incident response team
- How to classify an incident
- Analyzing network events
- Detecting network probes and attacks

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

What does this section cover?

- Investigating issues on a host/server
- Investigating service and applications
- Building a basic forensic toolkit
- Capabilities of different forensic tools
- How to conduct a forensic investigation

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

What is Cyber Incident Response?

- Actions taken in response to a security incident or event

- An organized approach to understanding the incident, mitigating its negative effects, planning the recovery, and investigating the root cause

Bottom Line…

- We will discuss the high-level concepts of how to develop a cyber incident response program and how the incident response team should operate during a cyber incident, including the basics of digital forensics and its associated toolsets

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE