Incident Response Fundamentals

Speaker - Eric Winterton

Summary - To introduce the student to the basic definitions, concepts, and procedures of or relating to incident response.

To answer the following questions:

Who can help me respond to an incident?
What are the main elements of an incident response team?
How do I REACT to a perceived incident (anomaly)?
How does the Incident Response Team RESPOND to a reported anomaly?
How do I RECOVER in the wake of an incident?

ERIC WINTERTON

Mr. Winterton has over five years of direct experience in automated information systems, security engineering, programming and operations. Mr. Winterton's expertise includes secure operations and maintenance of various UNIX Computer Networks, Windows NT security, security risk assessment, technical training, and computer forensic analysis.

Exodus Security Services supports training and onsite technical support for the National Security Agency (NSA) to their Network Intrusion Analysis Cell. Mr. Winterton supports the NIAC by training NSA personnel on forensic analysis of electronic data and devices. Mr. Winterton has provided training to a large number of students on Windows NT Security configurations, Risk Analysis, Security Policy, and Intrusion detection and response. In addition to teaching, Mr. Winterton developed material to be presented to a large number of students nationwide.