RSA® Education Services

RSA® Intelligence-Driven Event Analysis

Course Description

AT-A-GLANCE

The *RSA Intelligence-Driven Event Analysis* course discusses an intelligence-driven approach to event and incident management for a Tier 1 Security Analyst in a forward-thinking Security Operations Center (SOC).

Overview

Participants learn about intelligence-driven SOC processes, standard operating procedures (SOPs), and monitoring tools. They learn to recognize the formats associated with the various sources of information available in a network environment. The course follows the end-to-end workflow of a Tier 1 Security Analyst, including all appropriate steps that are needed to handle each type of identified security incident.

Audience

IT professionals with 2 to 3 years of experience in a troubleshooting role, such as a systems/network engineer, a system administrator, network operations analyst, or a newly-hired security analyst. Knowledge of security fundamentals is required.

Duration

2 days

Prerequisite Knowledge/Skills

Proven capabilities with networking fundamentals, operating systems, and security concepts such as confidentiality, integrity, availability, authentication, and identity.

Course Objectives

Upon successful completion of this course, participants should be able to:

- Identify the roles and responsibilities in a SOC.
- Interpret sources of information in a SOC.
- Describe how Security Analysts interact with information and data in the SOC environment.
- Monitor incoming event queues for potential security events and/or incidents using various security tools per operational procedures.
- Perform initial investigation and triage of potential incidents.
- Investigate/analyze an incident.
- Escalate an incident for further analysis aligned to SOPs.
- Document and communicate investigative results aligned to escalation and/or handoff SOPs.
- Walk through an incident from alert to escalation to closure.
- Apply concepts that are learned in the classroom setting to their specific working environment.

REGISTER FOR CLASSES:

For an up-to-date schedule of Instructor-led classes and other training options, visit the RSA Training and Certification web site:

www.emc.com/rsa-training

CONTACT US:

Email: trainingregistration@rsa.com

Phone: 800-995-5095

Int'l: 781-515-7700

Fax: 781- 515-6630

174 Middlesex Turnpike

Bedford, Massachusetts 01730

COURSE PART NUMBERS:

ED ACD IDEA 110 – Public class

ED ACD IDEA 210 - Onsite class

Course Outline

- Roles and Responsibilities in a Security Operations Center
  - Describe the purpose of a Security Operations Center (SOC) and its basic structure.
  - Define an event and an incident and describe the difference between the two terms.
  - Identify the roles and responsibilities in a SOC.
  - Name some of the tools that are commonly used to monitor events in the SOC.
  - Outline some of the key components in the incident processing workflow

- Interpreting Sources of Information
  - Diagram the components and tools of technical environment you are working in
  - Categorize sources of information available to a security analyst
  - Recognize information formats
  - Establish the context of the observed information/data
  - Assimilate external threat data and threat intelligence
  - Apply internal and external sources of intelligence to an incident

- Interacting with Information (Identifying Events)
  - Become the ‘eyes on glass’
  - Analyze logs from distributed system and network security devices
  - Monitor all alerting systems
  - Inspect network packet data
  - View information using a console

- Correlating Events
  - Define event correlation
  - Use several correlation engines
  - Assist in the identification of potential computer and communications security issues
  - Correlate events and incidents with knowledge base of historical events and incidents

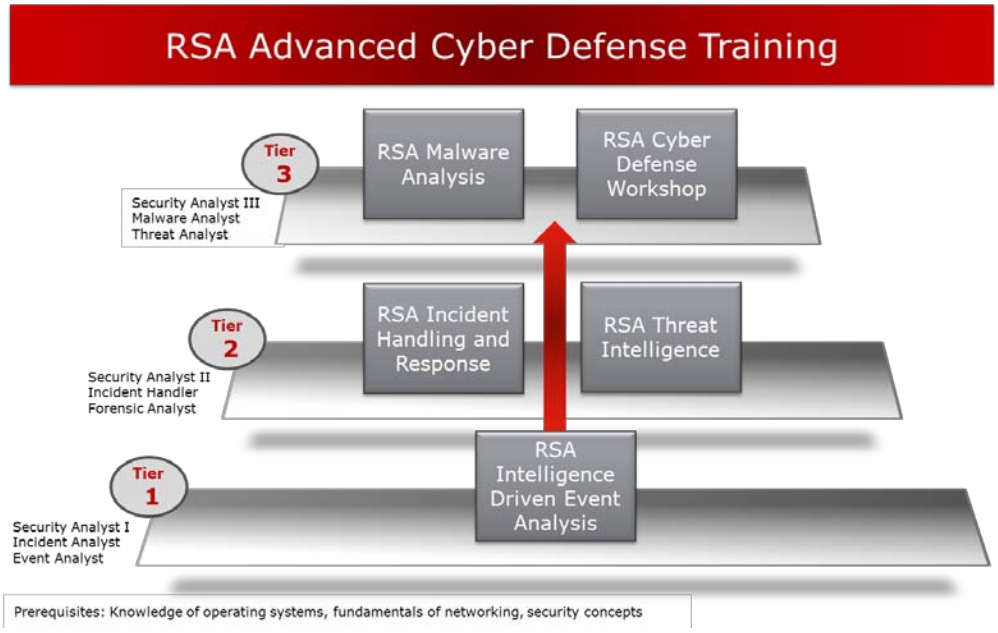
- Triaging Events
  - Follow the triage process
  - Prioritize incidents
  - Apply standard operating procedures

- Analyzing incidents using sources of information
  - Explain the incident – is your system infected?
  - Demonstrate fundamental understanding of all standard information sources
  - Determine whether an incident occurred and handle appropriately

- Escalation and Handoff
  - Escalate an event for further analysis to the incident handler
  - Follow the SLA to resolution or escalation
  - Standard operating procedures and analysis

- Documenting and Communicating Issues
  - Update the internal knowledge base and wiki
  - Perform maintenance activities on security related databases
  - Assimilate external threat data and threat intelligence

Learning Path



Prerequisites: Knowledge of operating systems, fundamentals of networking, security concepts