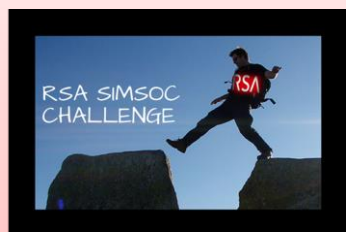


RSA® SOC Simulation Challenge ("SOCSim")

Offering Description



AT-A-GLANCE

Experience the challenge of competition while responding to questions based on a real-world breach scenario.

REGISTER:

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 NUMBER:

Public: ED ACD TRAIN UNIT
(9 units)

Onsite: ED ACD SOCSIM 210

Overview

RSA SOCSim, a forensic analysis experience, exposes participants to network and forensic analysis within a real-world breach scenario using simulated SOC dynamics. Participants are presented with a use case that requires them to analyze data flowing over the network. They are guided through the analysis by challenge questions using a "Jeopardy!" style interface based on the Cyber Kill Chain methodology. Answers are derived through data exploration and investigation of sophisticated "puzzles within puzzles" such as protocol and application analysis, steganography, reverse engineering, encryption/decryption, open source intelligence and much more...

Industry tools used in this course include:

- RSA Security Analytics
- Other open source tools

At the end of the challenge, the RSA facilitator will provide an overview of the breach scenario, including key analytical discoveries for each phase of the Cyber Kill Chain and respond to outstanding questions that participants may have.

Audience

Security analysts, computer forensic investigators, incident responders who have had exposure to network, log and host forensic analysis, and want to challenge themselves with simulated breach scenarios.

Duration

Approximately 6 hours.

Prerequisite Knowledge/Skills

Exposure to network and host forensic analysis is beneficial. Some security operations experience would be helpful. Working knowledge of RSA Security Analytics is required.

Course Objectives

At the end of the challenge, participants will walk away with hands on experience and exposure to:

- Network forensics through network protocol and application analysis
- Malware forensics through static and dynamic analysis
- Use of open source threat intelligence
- Common breach scenarios/tactics
- Cyber Kill Chain methodology
- Common tools used by network analysts/incident handlers

Experience of RSA's Experts

RSA and EMC have a 30-year legacy of working with clients worldwide to deliver security solutions. RSA has leveraged its relationships with industry leaders to give you deep insight into the most current threats and the intelligence-driven techniques and tools to mitigate the risk of disclosure of information.

