CompTIA Sec+ SY0-401, Part 4 of 8: Operational Security [Deprecated/Replaced]

Meet the expert: Ryan Hendricks is an experienced instructor who teaches networking and security courses to IT professionals throughout the nation. He currently has the CompTIA Certified Technical Trainer (CTT+ Classroom) and the Cisco Certified Academy Instructor (CCAI) credentials. He holds certifications from (ISC)2, EC-Council, CompTIA, and Cisco. When not on the podium instructing, he delves into IT books, always looking to learn more and keep up with the latest security topics.

Prerequisites: This course assumes that the user has working knowledge of networks and networking. Ideally, the user should have their CompTIA Network+ certification, but can be replaced with networking experience.

Runtime: 01:20:32

Course description: In this course we will discuss security incidents and how to properly manage them. Adding to our understanding of incident response we will cover evidence gathering in depth by focusing on forensics to support an investigation. We will then cover dealings with third parties including different agreements and arrangements and the security issues to keep in mind with those. Finishing the course is the topic of security awareness and training which can either make or break the organization's security stance. This course will cover the CompTIA Security+ objectives 2.2, 2.4, 2.5, and 2.6.

Course outline:

Incident Response
- Introduction
- Preparation
- Incident Identification
- First Responder
- Escalation and Notification
- CIRT
- Mitigation Steps
- Incident Isolation
- Collecting Evidence
- Recovery Procedures
- Lessons Learned
- Data Breach
- Damage and Loss Control
- Reporting
- Summary

Incident Forensics
- Introduction
- Digital Forensics
- Identifying
- Order of Volatility
- Order of Volitility, Cont.
- Capture System Image
- Take Hashes
- Network Traffic and Logs
- Record Time Offsets
- Capture Video
- Screenshots
- Witnesses
- Track Man Hours and Expense
- Chain of Custody
- Summary

Third Parties
- Introduction
- On-Boarding/Off Boarding
- Interoperability Agreements
- Service Level Agreement
- Business Partner Agreement
- Memorandum of Understanding
- Unauthorized Data Sharing
- Data Ownership
- Data Backups
- Agreement Compliance
- Summary

Incident Training
- Introduction
- Security Policy Training
- Awareness
- Education
- Training
- Personally Identifiable Info
- Classification System
- Data Labeling
- Data Handling
- Data Disposal
- Compliance
- User Habits
- Password Behaviors
- Password Example
- Password Example, Cont.
- Clean Desk
- Tailgating and Piggybacking
- Personally Owned Devices
- New Threats and Trends
- Social Networking
- Peer to Peer Applications
- Statistics
- Summary