# CompTIA Sec+ SY0-501, Part 7 of 9: Risk Assessment and Monitoring



**Meet the expert:** Jason Dion, CISSP No. 349867, is a professor at University of Maryland University College with multiple information technology professional certifications, including Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Network Defense Architect (CNDA), Digital Forensic Examiner (DFE), Digital Media Collector (DMC), CySA+, Security+, Network+, A+, PRINCE2 Practitioner, and ITIL. He holds a Masters of Science degree in Information Technology with a specialization in Information Assurance

**Prerequisites:** • Basic familiarity with computer networks, administration, and security is helpful (But, all required information will be covered during the course)
• Completion of the CompTIA A+ and Network+ certifications (Helpful, but not required)

**Runtime:** 01:53:02

**Course description:** This course talks about qualitative quantitative risk assessments as well as penetration testing and vulnerability assessments. Next it will discuss network scanning as well as how to monitor networks, protocol analyzers and finally finish up with auditing and logging for the SY0-501 Exam.

**Course outline:**

**Risk Assessments**
• Introduction
• Risk Assessments
• Qualitative Risk
• Quantitative Risk
• Methodologies
• Security Controls
• Summary

**Vulnerability Management**
• Introduction
• Vulnerability Management
• Penetration Testing
• OVAL
• Vulnerability Assessment
• Summary

**Nmap Scanning**
• Introduction
• Nmap Scanning
• Demo: Vulnerability Scanning
• Password Analysis
• Demo: Password Cracking
• Summary

**Monitoring**
• Introduction
• Monitoring Types
• Performance Baselining
• Protocol Analyzers
• SNMP
• Demo: Analytical Tools
• Summary

**Auditing**
• Introduction
• Auditing
• Demo: Auditing Files
• Logging
• Log Files
• SIEM
• Summary