CompTIA

Partner Summit

July 26 – 28, 2016 | Caribe Royale, Orlando

#Partnersummit16

Cybersecurity Analyst+: The Next Security Certification from CompTIA

- Where does this certification fit into CompTIA’s certification roadmap?
- Why CSA+?
- What topics will be covered in the CSA+?
- In which jobs will this certification be helpful?

Cybersecurity Analyst+

Coming Q1 2017

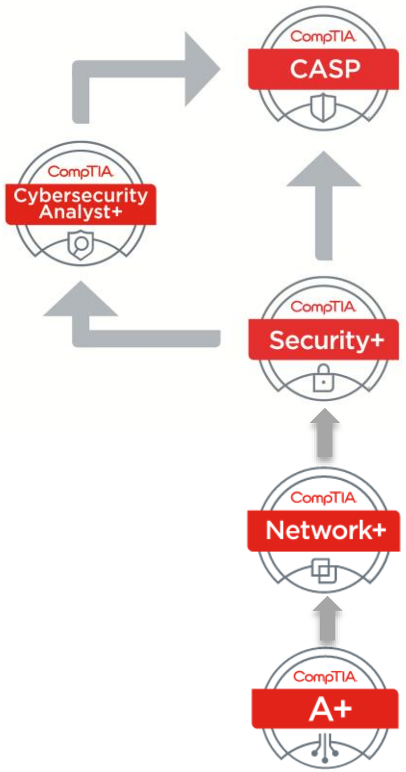
Exam purpose

“This exam will certify that the successful candidate has the knowledge and skills required to configure and use threat detection tools, perform data analysis, interpreting the results to identify vulnerabilities, threats and risk to an organization with the end goal of securing and protecting applications and systems within an organization.”

Key concept

The CompTIA Cybersecurity Analyst+ certification applies behavioral analytics to the IT security market to improve the overall state of IT security. Analytics have been successfully integrated in the business intelligence, retail and financial services industries for decades. Analytics are now applied to IT security.

Where does CSA+ fit into CompTIA's certification roadmap?



Note: This certification path is based on years of recommended experience: Security+, 2 years; Cybersecurity Analyst+, 2-3 years; and CASP, 5-10 years.

Why CSA+?

- As attackers have learned to evade traditional signature-based solutions, an analytics-based approach has become extremely important.

- IT security has expanded from traditional signature-based security of firewalls and antivirus software to an analytics-based approach.

What topics will be covered in the CSA+?

- Threat Management
- Vulnerability Management
- Incident Response
- Security Architecture
- Tool Sets

Threat Management Topics

- Environmental reconnaissance
- Network reconnaissance
- Response and countermeasures
- Secure practices

Threat Management Tasks and Tools

- NMAP
- Host scanning
- Network mapping
- NETSTAT
- Packet analyzer
- IDS/IPS
- HIDS/NIDS
- Firewall rule-based and logs
- Syslog
- Vulnerability scanner
- SIEM
- Resource monitoring tool
- Netflow analyzer
- Network Access Control (NAC)
- Penetration Testing
- Reverse Engineering
- Red, Blue, and White Team Training Exercises
- Risk Evaluation

Vulnerability Management Topics

- Understand information security vulnerability management process
- Analyze output from a vulnerability scan
- Understand common vulnerabilities and their targets

Vulnerability Management Tasks and Tools

- Scanning frequency
- Scanning criteria
- Report generation
- Remediation
- Continuous monitoring

Incident Response Topics

- Analyze threat behavior to determine impact
- Assemble a forensic toolkit, including forensic applications
- Understand incident response communication process
- Understand symptoms to select best response
- Understand incident recovery process

Incident Response Tasks and Tools

- Incident classification, threat, and severity
- Forensic kit contents
- Forensic kit applications
- Network, host, and application symptoms

Security Architecture Topics

- Frameworks, policies, controls, procedures
- Identity and access management issue remediation
- Security architecture and compensating controls
- Application security best practices in Software Development Life Cycle (SDLC)

Tool Sets

- General purpose of preventive tools
- General purpose of collective tools
- General purpose of analytical tools
- General purpose of exploitation tools
- General purpose of forensic tools

In which jobs will this certification be helpful?

The Cybersecurity Analyst+ exam will demonstrate skills competence for key job roles. Related job roles are included.

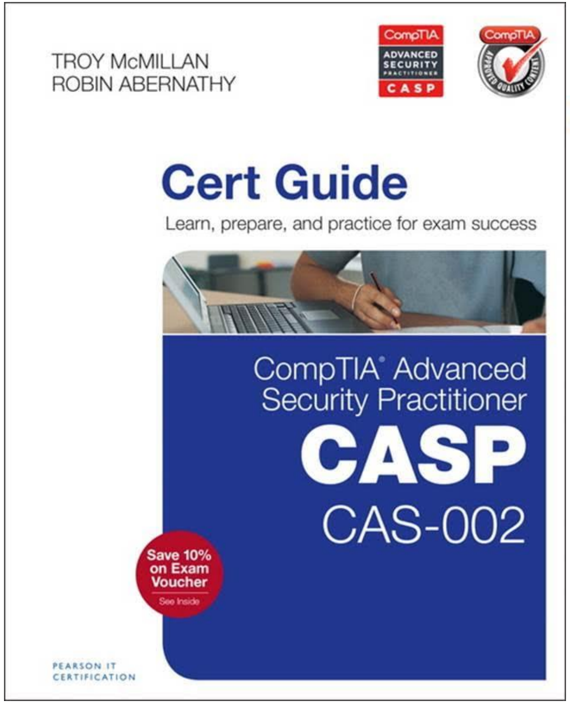
Key Job Roles	Related Job Roles
IT Security Analyst	Intrusion Detection System Analyst
Security Operations Center (SOC) Analyst	Risk Analyst
IT Vulnerability Analyst	Information Assurance Officer
Cybersecurity Specialist	Information Systems Security Officer
IT Threat Intelligence Analyst	Compliance Analyst
Security Engineer	Information Assurance Specialist
Information Systems Security Engineer	Threat Hunter

General Exam Information

- Expected release: Q1 2017
- Exam CS0-001 (*not* CAS-00x, which is CASP)
- 100 questions (estimated)
- 90 minutes (estimated)

Robin Abernathy

robin.abernathy@kaplan.com



TROY McMILLAN
ROBIN ABERNATHY

CompTIA ADVANCED SECURITY PRACTITIONER CASP

Cert Guide

Learn, prepare, and practice for exam success

CompTIA® Advanced Security Practitioner

CASP

CAS-002

Save 10% on Exam Voucher See Inside

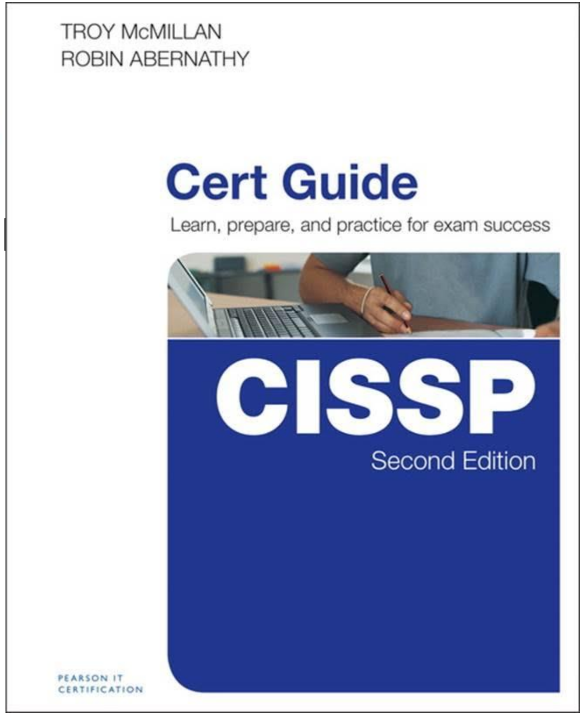
PEARSON IT CERTIFICATION

Transcender®

IT CERTIFICATION SUCCESS

For pricing information, contact:

Delvin Benjamin
delvin.benjamin@kaplan.com
(608) 779-2905 (Office)
(410) 463-3219 (Cell)
(608) 779-2984 (Fax)



TROY McMILLAN
ROBIN ABERNATHY

Cert Guide

Learn, prepare, and practice for exam success

CISSP

Second Edition

PEARSON IT CERTIFICATION

Ricky Doyle

ricky.doyle@practice-labs.com