An Introduction to
CompTIA Cybersecurity Analyst (CSA+)

PATRICK LANE, COMPTIA PRODUCTS DIRECTOR
CSA+ Webinar Speaker

Patrick Lane, M.Ed., Security+, Network+, CISSP, MCSE

Director, Products, IT Skills Certification

Product Manager for:
CompTIA Security+
CompTIA Cybersecurity Analyst (CSA+)
CompTIA Advanced Security Practitioner (CASP)
CompTIA Server+
A Little Housekeeping

Sound & Picture
Please unmute your speakers. If you are still having sound issues, try refreshing your browser.

Recording
This webinar is being recorded, and you are muted by default.

Email
You will receive an email shortly after the webinar with a link to view this webinar (same link you used to attend today), along with additional CSA+ information.

On-Demand
Webinar presentation slides and recording link will be available tomorrow.

Q&A & Group Chat
Got a question? Use the Q&A widget. Also, you can chat with other event attendees in the Group Chat widget!

Survey & Feedback
We want your feedback! Please complete brief survey at the completion of the webinar.

PLEASE NOTE: This is an informational webinar, and it does not count for a Continuing Education Unit (CEU) toward renewal of CompTIA certifications.
Why did CompTIA develop CSA+?
- Recent attacks
- Analytics approach needed
- Job demand

Cybersecurity Career Pathway

CSA+ Exam Specifics
- Development process
- Technical aspects

Training Resources

Q&A
WHO WE ARE

CompTIA is a global, not-for-profit IT trade association and the voice of the industry

OUR MISSION

Advance the IT industry
Technology is infrastructure, just like roads and bridges. Our economic growth, national security and quality of life depend on it. When we help tech businesses grow and help build a skilled tech workforce, we make that infrastructure stronger.

WHO WE SERVE

Tech businesses, tech professionals, tech educators, and anyone interested in a tech career or a vibrant tech industry.

HOW WE DO IT

NETWORKING
Member-led communities, councils, and events that help thousands of tech executives and professionals learn and collaborate with peers.

EDUCATION
Vendor-neutral education, business standards, technical content and career advice to help drive business revenue and professional growth.

THOUGHT LEADERSHIP
Highly regarded research and subject-matter expertise on topics including technology trends, cybersecurity and workforce issues.

CERTIFICATION
Vendor-neutral certifications that help millions of IT pros around the world validate their skills and advance in their careers.

ADVOCACY
Advocacy at state, federal, and international levels for policies that build a skilled tech workforce and advance the digital economy.

PHILANTHROPY
Help for those who are under-represented in IT and those who lack economic opportunity to prepare for, secure and succeed in IT careers.
CompTIA Certifications: A Quick Overview

- Best Practices
  - IT Fundamentals
  - CyberSecure

- Professional-Level
  - A+
  - Project+
  - Cloud+
  - Security+
  - Linux+
  - Network+
  - Server+
  - CSA+ (NEW!)

- Mastery Level
  - CompTIA Advanced Security Practitioner (CASP)

- Specialty
  - Cloud Essentials
  - CTT+
  - CDIA
WHY DID WE DEVELOP CSA+?
Seminal Event: Target Hack of 2014

- Wake up call for the IT security world
- Brought widespread attention to the “Advanced Persistent Threat”
- Demonstrated that traditional security tools, such as firewalls and anti-virus, do not alone protect networks
- More recent high profile attacks at Yahoo! and Democratic National Committee (DNC)
The Advanced Persistent Threat (APT)

Characteristics:
- Never stop
- Often highly coordinated / state sponsored
- Bad actors lurk on systems and networks
- Hard to detect
Lessons Learned

We must apply behavioral analytics to the IT security market to improve the overall state of IT security.

- We must focus on network behavior in an organization’s interior network
- We must identify network anomalies that indicate bad behavior

We must train IT security professionals security analyst skills, which include:

- Threat management
- Vulnerability management
- Cyber incident response
- Security and architecture tool sets
TOTAL NUMBER OF JOB POSTINGS:
Security Analyst Job Role

175% increase from 2012 to 2015. Data for U.S. only, but reflects an international need.

Source: Burning Glass Technologies Labor Insights, January 2016
Additional Indicators

The U.S. Bureau of Labor Statistics predicts that information security analysts will be the *fastest growing job category*, with 37% overall growth between 2012 and 2022.*

* CompTIA, Trends in Information Security 2015

In an analysis of recent U.S. Bureau of Labor Statistics data, information security analysts saw an 8% bump in growth over the first three months of 2016. *That’s a new BLS record.* **

** U.S. Bureau of Labor Statistics data

8 in 10 managers indicate that IT security certifications are very valuable (38%) or valuable (42%) in terms of validating security-related knowledge/skills or evaluating job candidates.***

*** International Trends in Cybersecurity, CompTIA, 2016
The Result...

CompTIA Cybersecurity Analyst (CSA+)
Developed to address the need for IT Security Analysts.

As attackers have learned to evade traditional signature-based solutions, an analytics-based approach has become extremely important. CSA+ applies behavioral analytics to the IT security market to improve the overall state of security.
CSA+ EXAM SPECIFICS
Organizations that Assisted in CSA+ Development

So far, the CSA+ certification had been reviewed by nearly 2,200 security analysts and/or IT pros, including those who took the beta exam. It has received feedback from organizations and partners across the globe to reach its current status. Some of the biggest contributors are listed below.
Performance-Based Assessment

The CSA+ exam will include hands-on, performance-based simulations.

- To prepare for these performance-based assessments, trainers, educators and publishers should emphasize open-source analytics tools and teamwork.

<table>
<thead>
<tr>
<th>Recommended open source software for training purposes*</th>
<th>Description</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireshark</td>
<td>Network protocol analyzer / packet capture tool</td>
<td><a href="https://www.wireshark.org">https://www.wireshark.org</a></td>
</tr>
<tr>
<td>Bro and/or Snort</td>
<td>Network intrusion detection systems (NIDS)</td>
<td><a href="https://www.bro.org">https://www.bro.org</a></td>
</tr>
</tbody>
</table>

*This software may or may not appear on the exam. It is listed so that readers may better understand the job role.
# CSA+ Exam Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exam code</td>
<td>CS0-001</td>
</tr>
<tr>
<td>Launch Date</td>
<td>February 15, 2017</td>
</tr>
<tr>
<td>Availability</td>
<td>Worldwide</td>
</tr>
<tr>
<td>Pricing</td>
<td>$320 USD (same pricing tier as Security+)</td>
</tr>
<tr>
<td>Testing Provider</td>
<td>Pearson VUE Testing Centers</td>
</tr>
<tr>
<td>Question Types</td>
<td>Performance based and multiple choice</td>
</tr>
<tr>
<td>No. of Questions</td>
<td>Maximum of 85 questions</td>
</tr>
<tr>
<td>Length of Test</td>
<td>165 minutes</td>
</tr>
<tr>
<td>Passing Score</td>
<td>750 (on a scale of 100-900)</td>
</tr>
<tr>
<td>Languages</td>
<td>English (Feb 15), Japanese &amp; Simplified Chinese (late Q3)</td>
</tr>
<tr>
<td>Recommended Experience</td>
<td>3-4 years of hands-on information security or related experience. Network+, Security+, or equivalent knowledge.</td>
</tr>
<tr>
<td>CE Program</td>
<td>Yes</td>
</tr>
</tbody>
</table>
The CompTIA CSA+ examination is a vendor-neutral certification designed for IT security analysts, vulnerability analysts, or threat intelligence analysts.

The exam will certify that the successful candidate has the knowledge and skills required to:

- configure and use threat detection tools,
- perform data analysis,
- interpret the results to identify vulnerabilities, threats, and risks to an organization with the end goal of securing and protecting applications and systems within an organization.
Job Roles

Skills competence for key job roles:

– Security Analyst
– Security Operations Center (SOC) Analyst
– Vulnerability Analyst
– Cybersecurity Specialist
– Threat Intelligence Analyst
– Security Engineer
– Information Systems Security Engineer
CSA+ Domain Objectives

1.0 Threat Management

1.1 Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes.

1.2 Given a scenario, analyze the results of a network reconnaissance.

1.3 Given a network-based threat, implement or recommend the appropriate response and countermeasure.

1.4 Explain the purpose of practices used to secure a corporate environment.
CSA+ Domain Objectives

2.0 Vulnerability Management

2.1 Given a scenario, implement an information security vulnerability management process.

2.2 Given a scenario, analyze the output resulting from a vulnerability scan.

2.3 Compare and contrast common vulnerabilities found in the following targets within an organization.
CSA+ Domain Objectives

3.0 Cyber Incident Response

3.1 Given a scenario, distinguish threat data or behavior to determine the impact of an incident.

3.2 Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation.

3.3 Explain the importance of communication during the incident response process.

3.4 Given a scenario, analyze common symptoms to select the best course of action to support incident response.

3.5 Summarize the incident recovery and post-incident response process.
4.1 Explain the relationship between frameworks, common policies, controls, and procedures.

4.2 Given a scenario, use data to recommend remediation of security issues related to identity and access management.

4.3 Given a scenario, review security architecture and make recommendations to implement compensating controls.

4.4 Given a scenario, use application security best practices while participating in the Software Development Life Cycle (SDLC).

4.5 Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies.
Security Information and Event Management (SIEM) Example
Security Information and Event Management (SIEM) Example

- Top User (Impacted): steven.jacobs (9.030)
- Temporary User: us-finsvr001
- Top Host (Origin): us-finsvr001 (9.030)
- Top URL: http://www.drop...
### Alarm Details List

**Security Information and Event Management (SIEM) Example**

#### Search and Filter

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>System Compromise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitation &amp; Installation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delivery &amp; Attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reconnaissance &amp; Probing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental Awareness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Security Information and Event Management (SIEM) Example

#### Alarm Details List

<table>
<thead>
<tr>
<th>DATE</th>
<th>STATUS</th>
<th>INTENT &amp; STRATEGY</th>
<th>METHOD</th>
<th>RISK</th>
<th>ATTACK PATTERN</th>
<th>SOURCE</th>
<th>DESTINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 mins</td>
<td></td>
<td>Portscan</td>
<td>Nmap</td>
<td>1</td>
<td></td>
<td>189.54.233.116:21188</td>
<td>Cronus:https</td>
</tr>
<tr>
<td>54 mins</td>
<td></td>
<td>Portscan</td>
<td>Nmap</td>
<td>1</td>
<td></td>
<td>61.240.144.67:60000</td>
<td>Cronus:60010</td>
</tr>
<tr>
<td>11:40:18</td>
<td>open</td>
<td>Portscan</td>
<td>Nmap</td>
<td>1</td>
<td></td>
<td>61.240.144.65:60000</td>
<td>Cronus:ldapssl</td>
</tr>
<tr>
<td>11:38:27</td>
<td>open</td>
<td>Portscan</td>
<td>Nmap</td>
<td>1</td>
<td></td>
<td>63.142.244.130:44133</td>
<td>Cronus:3391</td>
</tr>
<tr>
<td>11:25:14</td>
<td>open</td>
<td>Portscan</td>
<td>Nmap</td>
<td>1</td>
<td></td>
<td>169.54.233.120:21188</td>
<td>Cronus:ups</td>
</tr>
</tbody>
</table>

| 11:00:42   | open   | Bruteforce Authentication | Windows Login | 1 |                | 192.169.55.249:54072 | Zeus |

**DELIVERY & ATTACK: BRUTEFORCE AUTHENTICATION**

**ATTACK PATTERN:** EXTERNAL TO INTERNAL ONE-TO-ONE

**IP ACTIVITY:** Malicious Host

**OPEN & CLOSED ALARMS**

- **TOTAL EVENTS**: 7
- **DURATION**: 4 SECS
- **ELAPSED TIME**: 2 HOURS

**VIEW DETAILS**

**CLOSE**

**DELETE**

**APPLY LABEL**
CYBERSECURITY CAREER PATHWAY
CompTIA Cybersecurity Pathway Recommendation

Enter where it makes sense for you. Consider your experience and existing certifications or course of study.
The creation of the CompTIA Multi-Cert Recognition program provides formal recognition of a course of achievement often used in establishing an IT career.

The designations offer unique benefits to individuals interested in establishing and advancing their careers as well as to the organizations that seek to train and employ those individuals.

<table>
<thead>
<tr>
<th>Certifications</th>
<th>Recognition</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+, Network+ and Security+</td>
<td>CompTIA IT Infrastructure Pro</td>
</tr>
<tr>
<td>Security+, CSA+ and CASP</td>
<td>CompTIA Cybersecurity Expert</td>
</tr>
</tbody>
</table>

Milestones of recognition while pursuing the pathway:
Multi-Cert Recognition – Why?

For CompTIA certified professionals, earning multi-cert designation demonstrates:

**Achievement of the CompTIA certifications that employers rely on when staffing their IT infrastructure teams.**

For years, employers have used combinations of CompTIA certifications when looking for IT professionals. It’s not uncommon to see a job posting that lists a qualification for a combination of CompTIA A+, Network+ and/or Security+.

**Commitment to sound career progression and professional development.**

Earning the CompTIA multi-cert designation validates an individual’s well-rounded knowledge of IT environments. The skills validated by the A+, Network+ and Security+ exams demonstrate IT professionals can evaluate and master new technologies.
TRAINING RESOURCES
E-Learning Content / Self-Study

Available at or Near February 15, 2017 Launch

Available After Launch (TBD)
Instructor-Led Training

Available at or Near
February 15, 2017 Launch

These training providers will offer instructor-led training classes for CSA+.

It may take several weeks for the courses to appear on their training calendars. If you need immediate training, consider the e-Learning offerings available at launch. Call your local training provider and ask to be informed when the class is available.

For more information, visit https://certification.comptia.org/training/instructor-led-training
Additional Resources

Find the following CSA+ Resources at Certification.CompTIA.org!

CSA+ Product Page
CSA+ Exam Objectives
CSA+ Training Info
Link to purchase voucher @ CompTIAStore.com
CompTIA IT Careers Blog
Link to CompTIA Cybersecurity Hub w/ Check Your Cybersecurity Status Quiz!
Everybody in technology should have this. It should be mandatory if you’re going to stay in IT over the coming decade.

-Jim Lucari, Senior Manager, Certification Solutions Development, HP Enterprise
Thank you.

IT Professionals, visit:
certification.comptia.org/certifications/cybersecurity-analyst

Employers
Contact your CompTIA Sales Representative
QUESTIONS?

Please type your questions in the Q&A widget.

We will try to address as many questions as possible, but may not be able to answer them all within the allotted timeframe.