HPE Digital Learner CompTIA - CySA + CASP Content Pack

Courses are independent of each other but combined provide proof of advanced capabilities

- CySA+ certification covers advanced persistent threats in a cybersecurity environment
- CASP+ certification is hands-on, performance-based certification for practitioners with advanced levels of cybersecurity skills – This is not for managers

Supplementing this program with additional material prior to sitting an exam is recommended

<table>
<thead>
<tr>
<th>Why HPE Education Services?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• IDC MarketScape leader 5 years running for IT education and training*</td>
</tr>
<tr>
<td>• Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*</td>
</tr>
<tr>
<td>• Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and SUSE</td>
</tr>
<tr>
<td>• Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training</td>
</tr>
<tr>
<td>• Simplified purchase option with HPE Training Credits</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>CySA+ security professionals looking to consolidate and extend existing security knowledge to incorporate cybersecurity into the design and implementation of software and software products</td>
</tr>
<tr>
<td>CASP+ security professionals looking to acquire the technical knowledge and skills to conceptualize, engineer, integrate and implement secure solutions across complex environments to support a resilient enterprise</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content Pack Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>• To provide confirmation of the capability and competency of an individual in the security and cyber security domains</td>
</tr>
<tr>
<td>• To demonstrate the practical and hands-on solutions-based capability of an individual, based on current technology, to support the integrity of the enterprise</td>
</tr>
</tbody>
</table>

*Realize Technology Value with Training. IDC Infographic 2017, Sponsored by HPE, October 2017
**CompTIA Cybersecurity Analyst+ CS0-001: Network Architecture and Reconnaissance**

- Map network hardware and software to the OSI model
- Identify when to use specific network hardware
- Understand IPv4 settings
- Understand IPv6 settings
- Understand transport protocols
- Understand which Windows tools to use when configuring and troubleshooting TCP/IP
- Understand which Linux tools to use when configuring and troubleshooting TCP/IP

- Identify various conditions that control access to resources
- Use logs to learn about the network environment
- Use packet capturing tools for network traffic analysis
- Configure network services securely
- Explain common wired and wireless network concepts
- Scan for wireless networks and understand the returned results
- Determine placement of network devices
- Explain the purpose of cloud computing
- Recognize the use of cloud service models
- Recognize the role of virtualization in cloud computing
- Identify cloud security options
- Explain how to discover network devices
- Apply patches properly to secure network hosts
- Reduce the attack surface of a network host
- Recognize the importance of keeping hardware and software up to date
- Set the correct access to file systems while adhering to the principle of least privilege
- Recognize the purpose of controlling network access with NAC
- Recognize the purpose of network segregation using VLANs
- Identify positive learned outcomes resulting from incidents
- Thoroughly remove data
- Identify physical security controls
- Identify logical security controls
- Configure router ACL rules to block ICMP traffic
- Identify administrative security controls
- Identify compensating security controls
- Recognize the importance of continuous monitoring
- Explain how firmware must be accredited before universal trust is established
- Identify factors related to conducting penetration tests
- List categories of security controls and threat mitigations

**CompTIA Cybersecurity Analyst+ CS0-001: Threat Identification**

- Identify assets and related threats
- Recognize known, unknown persistent, and zero-day threats
- Identify what constitutes PII
- Explain payment card data
- Identify intellectual property
- Control how valuable data is used
- Configure group policy to prevent data leakage
- Determine the effect of negative incidents
- Identify stakeholders related to incident response

- Recognize incident response roles
- Describe incident disclosure options
- Analyze host symptoms to determine the best response
- Analyze network symptoms to determine the best response
- Analyze application symptoms to determine the best response
- Contain negative incidents
- Thoroughly remove data
- Identify positive learned outcomes resulting from incidents
- Identify how OEM documentation can be used to reverse engineering products
- Recognize the relevance of up-to-date network documentation
- Recognize the ongoing maintenance of incident response plans
- Create proper incident forms
- Protect the integrity of collected evidence
- Implement changes to processes resulting from lessons learned
- Determine which type of report provides the best data for a specific situation
- Determine if SLA details are aligned with business needs
- Explain the purpose of a MOU
- Use existing inventory to drive decisions related to security
- Recognize threat impact and design an incident response plan

**CompTIA Cybersecurity Analyst+ CS0-001: Threat Mitigation**

- Identify SDLC phases
- Apply secure coding practices
- Properly test technology solutions for security
- Reduce the attack surface of a network host
- Recognize the importance of keeping hardware and software up to date
- Apply patches properly to secure network hosts
- Set the correct access to file systems while adhering to the principle of least privilege
- Recognize the purpose of controlling network access with NAC
- Recognize the purpose of network segregation using VLANs
- Identify various conditions that control access to resources

- Recognize the purpose of intentionally creating vulnerable hosts to monitor malicious use
- Recognize the purpose of a jump box
- Explain how proper IT governance results in secured IT resources
- Recognize how regulatory compliance can influence security controls
- Apply NIST’s Cybersecurity Framework to your digital assets
- Apply ISO security standards to harden your environment
- Recognize how the TOGAF enterprise IT architecture can increase efficiency of security controls
- Recognize how to assess risk and apply effective security controls to mitigate that risk
- Recognize how to apply ITIL to increase the efficiency of IT service delivery
- Identify physical security controls
- Identify logical security controls
- Configure router ACL rules to block ICMP traffic
- Identify administrative security controls
- Identify compensating security controls
- Recognize the importance of continuous monitoring
- Explain how firmware must be accredited before universal trust is established
- Identify factors related to conducting penetration tests
- List categories of security controls and threat mitigations
### CompTIA Cybersecurity Analyst+ CS0-001: Reducing Vulnerabilities
- Recognize how crypto is used to secure data in the enterprise
- Differentiate symmetric from asymmetric encryption
- Differentiate asymmetric from symmetric encryption
- Identify the PKI hierarchy
- Request a security certificate from a CA
- Encrypt files on a Windows system using EFS
- Explain how file integrity can be maintained
- Enable file integrity using Linux
- Enable file integrity using Windows
- Recognize authentication methods used to prove one’s identity
- Require VPN connections to use MFA
- Recognize how resource access gets authorized
- Configure centralized authentication using RADIUS
- Describe what user provisioning entails
- Describe how identity federation differs from traditional authentication
- Identify security weaknesses in server OSs
- Identify security weaknesses on endpoint devices
- Identify security weaknesses at the network level
- Identify security weaknesses on mobile devices
- Recognize the overall process of scanning for vulnerabilities
- Configure appropriate vulnerability scanning settings
- Explain how the SCAP standard is used to measure vulnerability issues and compliance
- Conduct a vulnerability scan using Nessus
- Distinguish various vulnerability scanning tools from one another
- Conduct a vulnerability scan using MBSA
- Understand vulnerability scan results
- Put controls in place to mitigate threats
- Reduce vulnerabilities that can be exploited

### CompTIA Cybersecurity Analyst+ CS0-001: Investigate Security Incidents
- Recognize the purpose of various firewall types
- Recognize how firewall rules are created based on what type of traffic should or should not be allowed
- Recognize how packet filters work
- Configure a packet filtering firewall
- Explain the purpose of a proxy server
- Explain the purpose of a security appliance
- Recognize the unique capabilities of web application firewalls
- Explain the importance of intrusion detection and prevention
- Recognize when to use NIDS
- Recognize when to use NIPS
- Identify different types of malware
- Identify viruses
- Identify worms
- Identity spyware and adware
- Explain how ransomware works
- Mitigate malware using antimalware solutions
- Explain why user training and awareness is one of the most important security defenses
- Describe digital forensics
- Determine which forensic hardware is best suited for a specific situation
- Determine which forensic software is best suited for a specific situation
- Explain how forensic tools can be used against data stored on media
- Distinguish common forensic tools from one another
- Explain the sequence of steps that should be followed when conducting mobile device forensics
- Create a memory dump
- Retrieve and view deleted files
- Prevent threat materialization and follow proper forensic procedures

### CompTIA Cybersecurity Analyst+ CS0-001: Monitoring for Security Issues
- Recognize proper hiring practices
- Provision new user accounts in accordance with organizational security policies
- Apply personnel management best practices
- Distinguish the difference between threats, vulnerabilities, and exploits
- Explain the concept of spoofing
- Craft forged packets using free tools
- Recognize how impersonation can be used to gain unauthorized access
- Recognize CSS attacks
- Recognize root kits
- Explain the concept of privilege escalation
- Distinguish the difference between common exploit tools
- Use Metasploit tools to further understand the attacker toolset
- Use Kali Linux tools to further understand the attacker toolset
- Crack passwords
- Recognize the importance of continuous monitoring of various systems
- Distinguish the difference between common monitoring tools
- Monitor the Linux OS
- Monitor the Windows OS
- Configure Windows event log forwarding
- Identify where SIEM is used
- Identify where SCADA and ICS are used in different industries
- View network utilization
- Analyze timestamped data from various sources
- Identify trends in network usage
- Identify events from specific types of logs
- Describe the difference between vulnerabilities and exploits as well as use various reporting tools
| CompTIA CASP CAS-003: Business and Industry Influences and Risks | • Manage risks of new initiatives | • Define security concerns of diverse industries | • Describe external influences |
| | • Describe new or changing business models and strategies | • Recognize and apply business and industry policies | • Specify the impacts of deperimeterization |
| | | • Describe internal influences | • Describe industry influences and risks |

| CompTIA CASP CAS-003: Organizational Security and Privacy Policies | • Describe process and policy life cycle management | • Define common business documentation | • Develop standard policies and procedures |
| | • Work closely with human resources, legal, and executives | • Describe security requirements for contracts | • Describe security and privacy policies |
| | | • Specify general principles for sensitive information | |

| CompTIA CASP CAS-003: Risk Mitigation Strategies and Controls | • Determine risk | • Define business continuity planning | |
| | • Translate risk into business terms | • Describe IT governance and frameworks | |
| | • Treating risk | • Specify enterprise resilience and continual improvement | |
| | • Describe risk management processes | • Describe risk mitigation strategies and controls | |

| CompTIA CASP CAS-003: Risk Metric Scenarios for Enterprise Security | • Prototype and test multiple solutions | • Analyze solution metrics for business needs | |
| | • Create benchmarks and compare to baselines | • Use judgment to solve problems | |
| | • Analyze cyber defense trends | • Describe risk metrics for enterprise security | |

| CompTIA CASP CAS-003: Integrating Network and Security Components, Concepts, and Architectures | • Define application and protocol-aware technologies | • Define advanced device configuration | |
| | • Design advanced networking | • Define additional advanced device configuration | |
| | • Design additional advanced networking | • Describe advanced device configurations, port filtering with CEF, and IoT/IoE security | |
| | • Specify complex solutions for data flow | • Describe network and security architectures | |
| | • Describe secure configuration and software-defined networking | |
| | • Compare network management and monitoring tools | |

| CompTIA CASP CAS-003: Integrating Security Controls for Host Devices | • Harden host systems | • Protect the boot loader programs | |
| | • Define scripting and replication | • Describe terminal services and application delivery services | |
| | • Harden wireless peripherals | • Describe integrating controls for host devices | |
| | • Secure physical host peripherals | |

| CompTIA CASP CAS-003: Integrating Controls for Mobile and Small Form Factor Devices | • List types and characteristics of wearable technology | • Describe mobility security and privacy issues | |
| | • Integrate controls for mobile devices | • Describe mobility security and privacy concerns | |
| | • Manage enterprise mobility | • Describe rooting, jailbreaking, and sideloading | |
| | • Describe application, content, and data management | |
### CompTIA CASP CAS-003: Selecting Software Security Controls
- Describe application security design considerations
- Define specific application attacks
- Describe application vulnerabilities and issues
- Define additional application security concerns
- Describe application data issues
- Define sandboxing and enclaves
- Compare client-side processing to server-side processing
- Compare server-side processing to client-side processing
- Describe OS and firmware vulnerabilities
- Select software security controls

### CompTIA CASP CAS-003: Conducting Security Assessments
- Describe security assessment methods
- Describe reconnaissance, fingerprinting, and social engineering
- Describe open-source intelligence
- Define additional security assessment tools
- Describe types of host tools
- Specify physical security tools
- Describe how to conduct security assessments

### CompTIA CASP CAS-003: Implementing Incident Response and Recovery
- Describe e-discovery
- Specify data breach detection, collection, and analytics
- Specify data breach isolation, recovery, and response
- Facilitate incident detection and response
- Describe incident and emergency response
- Describe disaster recovery and order of volatility
- Define incident response support tools
- Specify incident or breach severity
- Describe post-incident response
- Describe incident response and recovery

### CompTIA CASP CAS-003: Integrating Hosts, Storage, and Applications in the Enterprise
- Adapt data flow security
- Describe data flow security standards
- Define interoperability issues
- Specify resilience issues
- Describe data security considerations
- Define resource provisioning and de-provisioning
- Consider merger and acquisition design
- Diagram and segment the logical network
- Describe security issues with application integration
- Describe enterprise integration

### CompTIA CASP CAS-003: Integrating Cloud and Virtualization Technologies in the Enterprise
- Describe technical models for cloud and virtualization
- Describe cloud service models
- Compare the pros and cons of virtualization
- Compare the pros and cons of virtualization
- Specify cloud augmented security services
- Specify CASB and sec-as-a-service offerings
- Define host comingling vulnerabilities
- Define resource provisioning and de-provisioning
- Describe enterprise cloud and virtualization technologies

### CompTIA CASP CAS-003: Integrating and Troubleshooting Advanced AAA Technologies
- Recognize the different components of advanced authentication
- Specify various types of access management
- Identify the different types of advanced authorization
- Compare attestation, proofing, and propagation
- List characteristics of SAML and OpenID federation
- Describe Shibboleth and WAYF and how they work
- List the features of several types of trust models
- Integrate advanced AAA technologies

### CompTIA CASP CAS-003: Implementing Cryptographic Techniques
- Implement cryptographic techniques
- Implement cryptographic mechanisms
- Describe cryptographic data processing
- Use the OpenPuff steganography tool
- Implement cryptographic modules and processors
- Recognize various types of cryptographic implementations
- Implement SSH, S/MIME, and SSL/TLS
- Implement cryptographic applications
- Implement key components of PKI
- Describe Blockchain and mobile cryptography
- Select cryptographic techniques based on requirements
CompTIA CASP CAS-003: Secure Communication and Collaboration Solutions

- Specify remote access resources and services
- Describe desktop and application sharing
- Describe remote assistance
- Specify conferencing and web services
- Specify video and audio services
- Specify storage and document collaboration tools
- Specify IM and presence
- Specify e-mail and telephony
- Specify social media and cloud services
- Describe secure collaboration

CompTIA CASP CAS-003: Applying Research Methods for Trend and Impact Analysis

- Recall best practices for ongoing research
- Research new technologies, security systems, and services in order to stay up to date
- Avoid threats and attacks
- Describe the features and benefits of zero-day mitigation controls
- Recognize the important of researching social media and methods of integration
- List the features and benefits of big data, machine learning, and artificial intelligence
- Define the global IA industry and who is involved
- List typical groups included in the global IA community
- Apply research methods to determine industry trends and their impact on the enterprise

CompTIA CASP CAS-003: Implementing Security Activities across the Technology Life Cycle

- Describe the system DLC requirements, acquisition, testing, and evaluation
- Describe the system DLC operations, monitoring, and maintenance
- Describe the system DLC configuration and change management
- Define the software DLC applications and software assurance
- Define the software DLC NX/XN bit, ASLR, and code quality
- Define the software DLC testing and DevOps
- Define agile, waterfall, and spiral software development
- Define the security requirements traceability matrix
- Define testing and validation in the software DLC
- Adapt adequate solutions
- Describe asset management and inventory control
- Describe life cycle activities

CompTIA CASP CAS-003: Interacting across Diverse Business Units

- Interact with sales and HR stakeholders
- Interpret goals with programmers and administrators
- Communicate goals with stakeholders
- Express goals with disaster recovery stakeholders
- Provide objective guidance and recommendations
- Establish effective collaboration
- Describe the importance of the governance, risk, and compliance committee
- Interact professionally with various business units

Learn more at
www.hpe.com/ww/digitallearner
www.hpe.com/ww/digitallearner-contentpack

Follow us: