Hewlett Packard Enterprise

HPE Digital Learner CompTIA - CySA + CASP Content Pack

HPE Content Pack number	CP032
Content Pack length	28 Hours
Content Pack category	Category 2
Learn more	**View now**

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

Why HPE Education Services?

- IDC MarketScape leader 5 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and SUSE
- 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
- Simplified purchase option with HPE Training Credits

Audience

CySA+ security professionals looking to consolidate and extend existing security knowledge to incorporate cyber security into the design and implementation of software and software products

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.

Content Pack Objectives

- To provide confirmation of the capability and competency of an individual in the security and cyber security domains
- To demonstrate the practical and hands-on solutions-based capability of an individual, based on current technology, to support the integrity of the enterprise

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, October 2017

Detailed Content Pack outline

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
- 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
- Use logs to learn about the network environment
- Use packet capturing tools for network traffic analysis
- Capture and interpret FTP and HTTP traffic
- Discover network configurations
- Explain harvesting techniques
- Recognize social engineering techniques
- Identify details within acceptable use policies
- Identify details within data ownership and retention policies
- Identify details within data classification policies
- Identify details within a password policy
- Recognize various network configurations and perform network reconnaissance

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 HIDS
- 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
- Describe new or changing business models and strategies
- Define security concerns of diverse industries
- Recognize and apply business and industry policies
- Describe internal influences
- Describe external influences
- Specify the impacts of deperimeterization
- Describe industry influences and risks

CompTIA CASP CAS-003: Organizational Security and Privacy Policies

- Describe process and policy life cycle management
- Work closely with human resources, legal, and executives
- Define common business documentation
- Describe security requirements for contracts
- Specify general principles for sensitive information
- Develop standard policies and procedures
- Describe security and privacy policies

CompTIA CASP CAS-003: Risk Mitigation Strategies and Controls

- Describe confidentiality, integrity, and availability decisions
- Determine minimum required security controls
- Define system-specific worst-case analysis
- Determine risk
- Translate risk into business terms
- Treating risk
- Describe risk management processes
- Define business continuity planning
- Describe IT governance and frameworks
- Specify enterprise resilience and continual improvement
- Describe risk mitigation strategies and controls

CompTIA CASP CAS-003: Risk Metric Scenarios for Enterprise Security

- Review control effectiveness
- Reverse engineer and deconstruct
- Collect and analyze metrics
- Prototype and test multiple solutions
- Create benchmarks and compare to baselines
- Analyze cyber defense trends
- Analyze solution metrics for business needs
- Use judgment to solve problems
- Describe risk metrics for enterprise security

CompTIA CASP CAS-003: Integrating Network and Security Components, Concepts, and Architectures

- Describe physical and virtual network and security devices including security switches, routers, and firewalls
- Describe physical and virtual network and security devices including WAPs, WLCs, NIDS, NIPS, and NAC
- Define application and protocol-aware technologies
- Design advanced networking
- Design additional advanced networking
- Specify complex solutions for data flow
- Describe secure configuration and software-defined networking
- Compare network management and monitoring tools
- Define advanced device configuration
- Define additional advanced device configuration
- Describe advanced device configurations, port filtering with CEF, and IoT/IoE security
- Describe network and security architectures

CompTIA CASP CAS-003: Integrating Security Controls for Host Devices

- Implement trusted operating systems
- Define least functionality
- Describe endpoint security software
- Describe host-based IDS and IPS
- Harden host systems
- Define scripting and replication
- Harden wireless peripherals
- Secure physical host peripherals
- Protect the boot loader programs
- Describe terminal services and application delivery services
- Describe integrating controls for host devices

CompTIA CASP CAS-003: Integrating Controls for Mobile and Small Form Factor Devices

- Describe tokenization and TPM
- Describe tethering, Bluetooth, and gestures
- Describe mobility biometrics
- List types and characteristics of wearable technology
- Integrate controls for mobile devices
- Manage enterprise mobility
- Describe application, content, and data management
- Describe mobility security and privacy issues
- Describe mobility security and privacy concerns
- Describe rooting, jailbreaking, and sideloading

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
- Describe routing tables, DNS records, and search engines
- Describe security assessment types
- Describe penetration testing and assessments
- Define exercises and audits
- Describe scanners
- 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 hypervisors
- 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:

CP032, May 2019

Hewlett Packard Enterprise