INFOSECTRAIN

CompTIA AUTHORIZED PARTNER

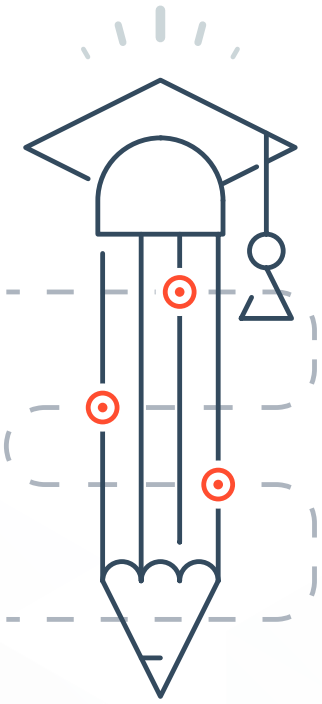
CompTIA Security+

SY0-701

CERTIFICATION TRAINING

INFOSECTRAIN

COURSE highlights



01 40 Hrs of Instructor-led Training

02 Certified & Experienced Trainers

03 Blended Learning Model

04 CompTIA Authorized Training Partner

www.infosectrain.com

COURSE DESCRIPTION

Overview

The CompTIA Security+ SY0-701 course from InfosecTrain, provides a comprehensive and expert-led training experience, covering five key domains that are essential for understanding and excelling in the field of information security. Participants will delve into general security concepts, threats, vulnerabilities, mitigations, security architecture, security operations, and security program management. The course features practical exercises and hands-on labs to develop participant's skills, ensuring that participants are well-prepared for the SY0-701 certification exam.

INFOSECTRAIN

TARGET-Audience

- System Administrators
- Security Engineers and Consultants
- Network Administrators
- IT Auditors/Penetration Testers

PRE-Requisites

- CompTIA A+ and CompTIA Network+
- It is recommended to have at least 2 years of experience in IT administration with a focus on security, hands-on experience with technical information security, and broad knowledge of security concepts.

INFOSECTRAIN

EXAM Information

Exam Code	SY0-601	SY0-701
Launch Date	12th, November 2020	7th, November 2023
Exam Description	The CompTIA Security+ certification exam ensures that candidates possess the expertise and proficiencies necessary to evaluate the security standing of enterprise environments, suggest and execute suitable security solutions, oversee and secure hybrid environments that encompass cloud, mobile, and IoT, and conduct operations in alignment with relevant laws and regulations, encompassing governance, risk management, and compliance principles. Furthermore, it attests to candidates' ability to effectively identify, assess, and manage security events and incidents.	
Recommended Experience	CompTIA Network+ and two years of experience in IT administration with a security focus	CompTIA Network+ and two years of experience working in a security/ systems administrator job role
Number of Questions	Maximum of 90 Questions	
Exam Format	Multiple Choice and Performance-Based	
Exam Duration	90 Minutes	
Passing Score	750 (on a scale of 100-900)	
Languages	English, Japanese, Portuguese, and Spanish	
Retirement	July 2024	TBD – Usually three years after launch

INFOSECTRAIN

COMPTIA SECURITY+ SY0-701
COURSE OBJECTIVES

- Develop a comprehensive understanding of foundational security concepts and principles that serve as the cornerstone of cybersecurity.
- Learn to identify, assess, and mitigate various threats, vulnerabilities, and risks that can compromise the security of digital environments.
- Master the principles and practices of designing, implementing, and managing a robust security architecture that can withstand diverse cyber threats.
- Gain expertise in day-to-day security operations, including incident response, monitoring, and safeguarding critical assets.
- Acquire the knowledge and skills required to oversee and manage a security program effectively, ensuring compliance, governance, and the protection of valuable data.

INFOSECTRAIN

COURSE CONTENT

- **Domain 1** General Security Concepts (12%)
- **Domain 2** Threats, Vulnerabilities, and Mitigations (22%)
- **Domain 3** Security Architecture (18%)
- **Domain 4** Security Operations (28%)
- **Domain 5** Security Program Management and Oversight (20%)

INFOSECTRAIN

Domain 01 General Security Concepts

1.1: Compare and Contrast Various Types of Security Controls

- Categories
  - Technical
  - Managerial
  - Operational
  - Physical
- Control
  - Preventive
  - Deterrent
  - Detective
  - Corrective
  - Compensating
  - Directive

1.2: Summarize Fundamental Security Concepts

- Confidentiality, Integrity, and Availability (CIA)
- Non-Repudiation
- Authentication, Authorization, and Accounting (AAA)
  - Authenticating People
  - Authenticating Systems
  - Authorization Models
- Gap Analysis
- Zero Trust

- **Control Plane**
  - Adaptive Identity
  - Threat Scope Reduction
  - Policy-Driven Access Control
  - Policy Administrator
  - Policy Engine
- **Data Plane**
  - Implicit Trust Zones
  - Subject/System
  - Policy Enforcement Point

- **Physical Security**
  - Bollards
  - Access Control Vestibule
  - Fencing
  - Video Surveillance
  - Security Guard
  - Access Badge
  - Lighting
  - Sensors
    - Infrared
    - Pressure
    - Microwave
    - Ultrasonic

Deception and Disruption Technology

- Honeypot
- Honeynet
- Honeyfile
- Honeytoken

1.3: Explain the Importance of Change Management Processes and the Impact to Security

Business Processes Impacting Security Operation

- Approval process
- Ownership
- Stakeholders
- Impact Analysis
- Test Results
- Backout Plan
- Maintenance Window
- Standard Operating Procedure

Technical Implications

- Allow Lists/Deny Lists
- Restricted Activities
- Downtime
- Service Restart
- Application Restart
- Legacy Applications
- Dependencies

- Documentation
  - Updating Diagrams
  - Updating Policies/Procedures
- Version Control

1.4: Explain the Importance of Using Appropriate Cryptographic Solutions

- Public Key Infrastructure (PKI)
  - Public Key
  - Private Key
  - Key Escrow
- Encryption
  - Level
    - Full-Disk
    - Partition
    - File
    - Volume
    - Database
    - Record
  - Transport/Communication
  - Asymmetric
  - Symmetric
  - Key Exchange
  - Algorithms
  - Key length

- **Tools**
  - Trusted Platform Module (TPM)
  - Hardware Security Module (HSM)
  - Key Management System
  - Secure Enclave
- **Obfuscation**
  - Steganography
  - Tokenization
  - Data Masking
- Hashing
- Salting
- Digital Signatures
- Key Stretching
- Blockchain
- Open Public Ledger
- Certificates
  - Certificate Authorities
  - Certificate Revocation Lists (CRLs)
  - Online Certificate Status Protocol (OCSP)
  - Self-Signed
  - Third-Party
  - Root of Trust
  - Certificate Signing Request (CSR) Generation
  - Wildcard

INFOSECTRAIN

Domain 02 Threats, Vulnerabilities, and Mitigations

2.1: Compare and Contrast Common Threat Actors and Motivations

Threat Actors

- Nation-State
- Unskilled Attacker
- Hacktivist
- Insider Threat
- Organized Crime
- Shadow IT

Attributes of Actors

- Internal/External
- Resources/Funding
- Level of Sophistication/Capability

Motivations

- Data Exfiltration
- Espionage
- Service Disruption
- Blackmail
- Financial Gain
- Philosophical/Political Beliefs
- Ethical
- Revenge
- Disruption/Chaos
- War

INFOSECTRAIN

2.2: Explain Common Threat Vectors and Attack Surfaces

- **Message-Based**
  - Email
  - Short Message Service (SMS)
  - Instant Messaging (IM)
- Image-Based
- File-Based
- Voice Call
- Removable Device
- Vulnerable Software
  - **Client-Based vs. Agentless**
- Unsupported Systems and Applications
- Unsecure Networks
  - Wireless
  - Wired
  - Bluetooth
- Open Service Ports
- Default Credentials
- Supply Chain
  - Managed Service Providers (MSPs)
  - Vendors
  - Suppliers

- Human Vectors/Social Engineering
  - Phishing
  - Vishing
  - Smishing
  - Misinformation/Disinformation
  - Impersonation
  - Business Email Compromise
  - Pretexting
  - Watering Hole
  - Brand Impersonation
  - Typosquatting

2.3: Explain Various Types of Vulnerabilities

Application

- Memory Injection
- Buffer Overflow
- Race Conditions
  - Time-of-Check (TOC)
  - Time-of-Use (TOU)
- Malicious Update

- Operating System (OS)-Based
- Web-Based

- Structured Query Language (SQL) Injection
- Cross-Site Scripting (XSS)

- Hardware
  - Firmware
  - End-of-Life
  - Legacy
- Virtualization
  - Virtual Machine (VM) Escape
  - Resource Reuse
- Cloud-Specific
- Supply Chain
  - Service Provider
  - Hardware Provider
  - Software Provider
- Cryptographic
- Misconfiguration
- Mobile Device
  - Side Loading
  - Jailbreaking
- Zero-Day

INFOSECTRAIN

2.4: Given a Scenario, Analyze Indicators of Malicious Activity

Malware Attacks

- Ransomware
- Trojan
- Worm
- Spyware
- Bloatware
- Virus
- Keylogger
- Logic Bomb
- Rootkit

Physical Attacks

- Brute Force
- Radio Frequency Identification (RFID) Cloning
- Environmental

Network Attacks

- Distributed Denial-of-Service (DDoS)
  - Amplified
  - Reflected
- Domain Name System (DNS) Attacks
- Wireless
- On-Path
- Credential Replay
- Malicious Code

INFOSECTRAIN

Application Attacks

- Injection
- Buffer Overflow
- Replay
- Privilege Escalation
- Forgery
- Directory Traversal

Cryptographic Attacks

- Downgrade
- Collision
- Birthday

Password Attacks

- Spraying
- Brute Force

Indicators

- Account Lockout
- Concurrent Session Usage
- Blocked Content
- Impossible Travel
- Resource Consumption
- Resource Inaccessibility
- Out-of-Cycle Logging
- Published/Documented
- Missing Logs

INFOSECTRAIN

2.5: Explain the Purpose of Mitigation Techniques Used to Secure the Enterprise

- **Segmentation**
- **Access Control**
  - Access Control List (ACL)
  - Permissions
- Application Allow List
- Isolation
- Patching
- Encryption
- Monitoring
- Least Privilege
- Configuration Enforcement
- Decommissioning
- Hardening Techniques
  - Encryption
  - Installation of Endpoint Protection
  - Host-Based Firewall
  - Host-Based Intrusion Prevention System (HIPS)
  - Disabling Ports/Protocols
  - Default Password Changes
  - Removal of Unnecessary Software

INFOSECTRAIN

Domain 03 Security Architecture

3.1: Compare and Contrast Security Implications of Different Architecture Models

- Architecture and Infrastructure Concepts
  - Cloud
    - Responsibility Matrix
    - Hybrid Considerations
    - Third-Party Vendors
  - Infrastructure as Code (IaC)
  - Serverless
  - Microservices
  - Network Infrastructure
    - On-Premises
    - Centralized vs. Decentralized
    - Containerization
    - Virtualization
    - IoT
    - Industrial Control Systems (ICS)/
    - Supervisory Control and Data Acquisition (SCADA)
    - Real-Time Operating System (RTOS)
    - Embedded Systems
    - High availability

- **Considerations**
  - Availability
  - Resilience
  - Cost
  - Responsiveness
  - Scalability
  - Ease of Deployment
  - Risk Transference
  - Ease of Recovery
  - Patch Availability
  - Inability to Patch
  - Power
  - Compute

3.2: Given a Scenario, Apply Security Principles to Secure Enterprise

- **Infrastructure Considerations**
  - Device Placement
  - Security Zones
  - Attack Surface
  - Connectivity
  - Failure Modes
    - Fail-Open
    - Fail-Closed
- **Device Attribute**
  - Active vs. Passive
  - Inline vs. Tap/Monitor

- **Network Appliances**
  - Jump Server
  - Proxy Server
  - Intrusion Prevention System (IPS)/Intrusion Detection System (IDS)
  - Load Balancer
  - Sensor
- **Port Security**
  - 802.1X
  - Extensible Authentication
- **Firewall Types**
  - Web Application Firewall (WAF)
  - Unified Threat Management (UTM)
  - Next-Generation Firewall (NGFW)
  - Layer 4/Layer 7
- **Secure Communication/Access**
  - Virtual Private Network (VPN)
  - Remote Access
  - Tunneling
    - Transport Layer Security (TLS)
    - Internet Protocol Security (IPSec)
  - Software-Defined Wide Area Network (SD-WAN)
  - Secure Access Service Edge (SASE)
- **Selection of Effective Controls**

INFOSECTRAIN

3.3: Compare and Contrast Concepts and Strategies to Protect Data

Data Types

- Regulated
- Trade Secret
- Intellectual Property
- Legal Information
- Financial Information
- Human and Non-Human-Readable

Data Classifications

- Sensitive
- Confidential
- Public
- Restricted
- Private
- Critica

General Data Considerations

- Data States
  - Data at Rest
  - Data in Transit
  - Data in Use
- Data Sovereignty
- Geolocation

Methods to Secure Data

- Geographic Restrictions
- Encryption
- Hashing
- Masking
- Tokenization
- Obfuscation
- Segmentation
- Permission Restrictions

3.4: Explain the Importance of Resilience and Recovery in Security Architecture

High Availability

- Load Balancing vs. Clustering
- Site Considerations
  - Hot
  - Cold
  - Warm
  - Geographic Dispersion
- Platform Diversity
- Multi-Cloud Systems
- Continuity of Operations
- Capacity Planning

- People
- Technology
- Infrastructure

Testing

- Tabletop Exercises
- Fail over
- Simulation
- Parallel Processing

Backups

- Onsite/Offsite
- Frequency
- Encryption
- Snapshots
- Recovery
- Replication
- Journaling

Power

- Generators
- Uninterruptible Power Supply (UPS)

INFOSECTRAIN

Domain 04 Security Operations

4.1: Given a Scenario, Apply Common Security Techniques to Computing

- **Secure Baselines**
  - Establish
  - Deploy
  - Maintain
- **Hardening Targets**
  - Mobile Devices
  - Workstations
  - Switches
  - Routers
  - Cloud Infrastructure
  - Servers
  - ICS/SCADA
  - Embedded Systems
  - RTOS
  - IoT devices
- **Wireless Devices**
  - Installation Considerations
    - Site Surveys
    - Heat Maps

- **Mobile Solutions**
  - Mobile Device Management (MDM)
  - Deployment Models
    - Bring your Own Device (BYOD)
    - Corporate-Owned, Personally Enabled (COPE)
    - Choose Your Own Device (CYOD)
  - **Connection Methods**
    - Cellular
    - Wi-Fi
    - Bluetooth
- **Wireless Security Settings**
  - Wi-Fi Protected Access 3 (WPA3)
  - AAA/Remote Authentication
  - Dial-In User Service (RADIUS)
  - Cryptographic Protocols
  - Authentication Protocols
- **Application Security**
  - Input Validation
  - Secure Cookies
  - Static Code Analysis
  - Code Signing
- Sandboxing
- Monitoring

INFOSECTRAIN

4.2: Explain the Security Implications of Proper Hardware, Software, and Data Asset Management

- Acquisition/Procurement Process
- Assignment/Accounting
    - Ownership
    - Classification
- Monitoring/Asset Tracking
    - Inventory
    - Enumeration
- Disposal/Decommissioning
    - Sanitization
    - Destruction
    - Certification
    - Data retention

4.3: Explain Various Activities Associated with Vulnerability Management

- Identification Methods
    - Vulnerability Scan
    - Application Security
        - Static Analysis
        - Dynamic Analysis
        - Package Monitoring

- **Threat Feed**
  - Open-Source Intelligence (OSINT)
  - Proprietary/Third-Party
  - Information-Sharing Organization
  - Dark Web
- **Penetration Testing**
- **Responsible Disclosure Program**
  - Bug Bounty Program
- System/Process Audit

- Analysis
  - Confirmation
    - **False Positive**
    - **False Negative**
  - Prioritize
  - Common Vulnerability Scoring System (CVSS)
  - Common Vulnerability Enumeration (CVE)
  - Vulnerability Classification
  - Exposure Factor
  - Environmental Variables
  - Industry/Organizational Impact
  - Risk Tolerance

- Vulnerability Response and Remediation
  - Patching
  - Insurance
  - Segmentation
  - Compensating Controls
  - Exceptions and Exemptions
- Validation of Remediation
  - Rescanning
  - Audit
  - Verification
- Reporting

4.4: Explain Security Alerting and Monitoring Concepts and Tools

- Monitoring Computing Resources
  - Systems
  - Applications
  - Infrastructure
- Activities
  - Log Aggregation
  - Alerting
  - Scanning
  - Reporting

- Archiving
- Alert Response and Remediation/ Validation
    - Quarantine
    - Alert Tuning
    - Tools
- Security Content Automation Protocol (SCAP)
- Benchmarks
- Agents/Agentless
- Security Information and Event Management (SIEM)
- Antivirus
- Data Loss Prevention (DLP)
- Simple Network Management Protocol (SNMP) Traps
- NetFlow
- Vulnerability Scanners

4.5: Given a Scenario, Modify Enterprise Capabilities to Enhance Security

- Firewall
    - Rules
    - Access Lists
    - Ports/Protocols
    - Screened Subnets

INFOSECTRAIN

- **IDS/IPS**
  - Trends
  - Signatures
- **Web Filter**
  - Agent-Based
  - Centralized Proxy
  - Universal Resource Locator (URL) Scanning
  - Content Categorization
  - Block Rules
  - Reputation
- **Operating System Security**
  - Group Policy
  - SELinux
- **Implementation of Secure Protocols**
  - Protocol Selection
  - Port Selection
  - Transport Method
- **DNS Filtering**
- **Email Security**
  - Domain-based Message
  - Authentication Reporting and Conformance (DMARC)
  - Domain Keys Identified Mail (DKIM)
  - Sender Policy Framework (SPF)
  - Gateway

- File Integrity Monitoring
- DLP
- Network Access Control (NAC)
- Endpoint Detection and Response (EDR)/Extended Detection and Response (XDR)
- User Behavior Analytics

4.6: Given a Scenario, Implement and Maintain Identity and Access Management

- Provisioning/De-provisioning user Accounts
- Permission Assignments and Implications
- Identity Proofing
- Federation
- Single Sign-On (SSO)
    - Lightweight Directory Access Protocol (LDAP)
    - Open Authorization (OAuth)
    - Security Assertions Markup Language (SAML)
- Interoperability
- Attestation
- Access Controls

- Mandatory
- Discretionary
- Role-Based
- Rule-Based
- Attribute-Based
- Time-of-Day Restrictions
- Least Privilege

Multi Factor Authentication

- **Implementations**
  - Biometrics
  - Hard/Soft Authentication Tokens
  - Security Keys
- **Factors**
  - Something You Know
  - Something You Have
  - Something You Are
  - Somewhere You Are

Password Concepts

- **Password Best Practices**
  - Length
  - Complexity
  - Reuse
  - Expiration
  - Age

- Password Managers
- Passwordless

- **Privileged Access Management Tools**
  - Just-in-Time Permissions
  - Password Vaulting
  - Ephemeral Credentials

4.7: Explain the Importance of Automation and Orchestration Related to Secure Operations

- **Use Cases of Automation and Scripting**
  - User Provisioning
  - Resource Provisioning
  - Guard Rails
  - Security Groups
  - Ticket Creation
  - Escalation
  - Enabling/Disabling Services and Access
  - Continuous Integration and Testing
  - Integrations and Application Programming Interfaces (APIs)
- **Benefits**
  - Efficiency/Time Saving
  - Enforcing Baselines
  - Standard Infrastructure Configurations
  - Scaling in a Secure Manner

- Employee Retention
- Reaction Time
- Workforce Multiplier

Other Considerations

- Complexity
- Cost
- Single Point of Failure
- Technical Debt
- Ongoing Supportability

4.8: Explain Appropriate Incident Response Activities

Process

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Lessons learned

Training

Testing

- Tabletop Exercise
- Simulation

- Root Cause Analysis
- Threat Hunting
- Digital Forensics
  - Legal Hold
  - Chain of Custody
  - Acquisition
  - Reporting
  - Preservation
  - E-Discovery

4.9: Given a Scenario, Use Data Sources to Support an Investigation

- Log Data
  - Firewall Logs
  - Application Logs
  - Endpoint Logs
  - OS-Specific Security Logs
  - IPS/IDS Logs
  - Network Logs
  - Metadata
- Data Sources
  - Vulnerability Scans
  - Automated Reports
  - Dashboards
  - Packet Captures

INFOSECTRAIN

Domain 05 Security Program Management and Oversight

5.1: Summarize Elements of Effective Security Governance

- Guidelines
- Policies
  - Acceptable Use Policy (AUP)
  - Information Security Policies
  - Business Continuity
  - Disaster Recovery
  - Incident Response
  - Software Development Lifecycle (SDLC)
  - Change Management
- Standards
  - Password
  - Access Control
  - Physical Security
  - Encryption
- Procedures
  - Change Management
  - Onboarding/Offboarding
  - Playbooks

- **External Considerations**
  - Regulatory
  - Legal
  - Industry
  - Local/Regional
  - National
  - Global
- **Monitoring and Revision**
- **Types of Governance Structures**
  - Boards
  - Committees
  - Government Entities
  - Centralized/Decentralized
- **Roles and Responsibilities for Systems and Data**
  - Owners
  - Controllers
  - Processors
  - Custodians/Stewards

INFOSECTRAIN

5.2: Explain Elements of the Risk Management Process

- **Risk Identification**
- **Risk Assessment**
  - Ad hoc
  - Recurring
  - One-Time
  - Continuous
- **Risk Analysis**
  - Qualitative
  - Quantitative
  - Single Loss Expectancy (SLE)
  - Annualized Loss Expectancy (ALE)
  - Annualized Rate of Occurrence (ARO)
  - Probability
  - Likelihood
  - Exposure Factor
- **Risk Register**
  - Key Risk Indicators
  - Risk Owners
  - Risk Threshold
- **Risk Tolerance**
- **Risk Appetite**

- Expansionary
- Conservative
- Neutral

- **Risk Management Strategies**
  - Transfer
  - Accept
    - Exemption
    - Exception
  - Avoid
  - Mitigate
- **Risk Reporting**
- **Business Impact Analysis**
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)
  - Mean Time to Repair (MTTR)
  - Mean Time Between Failures (MTBF)

INFOSECTRAIN

5.3: Explain the Processes Associated with Third-Party Risk Assessment and Management

- **Vendor Assessment**
  - Penetration Testing
  - Right-to-Audit Clause
  - Evidence of Internal Audits
  - Independent Assessments
  - Supply Chain Analysis
- **Vendor Selection**
  - Due Diligence
  - Conflict of Interest
- **Agreement Types**
  - Service-Level Agreement (SLA)
  - Memorandum of Agreement (MOA)
  - Memorandum of Understanding (MOU)
  - Master Service Agreement (MSA)
  - Work Order (WO)/Statement of Work (SOW)
  - Non-Disclosure Agreement (NDA)
  - Business Partners Agreement (BPA)
- **Vendor Monitoring**
- **Questionnaires**
- **Rules of Engagement**

INFOSECTRAIN

5.4: Explain Types and Purposes of Audits and Assessments

- **Attestation**
- **Internal**
  - Compliance
  - Audit Committee
  - Self-Assessments
- **External**
  - Regulatory
  - Examinations
  - Assessment
  - Independent Third-Party Audit
- **Penetration Testing**
  - Physical
  - Offensive
  - Defensive
  - Integrated
  - Known Environment
  - Partially Known Environment
  - Unknown Environment
  - Reconnaissance
    - Active
    - Passive

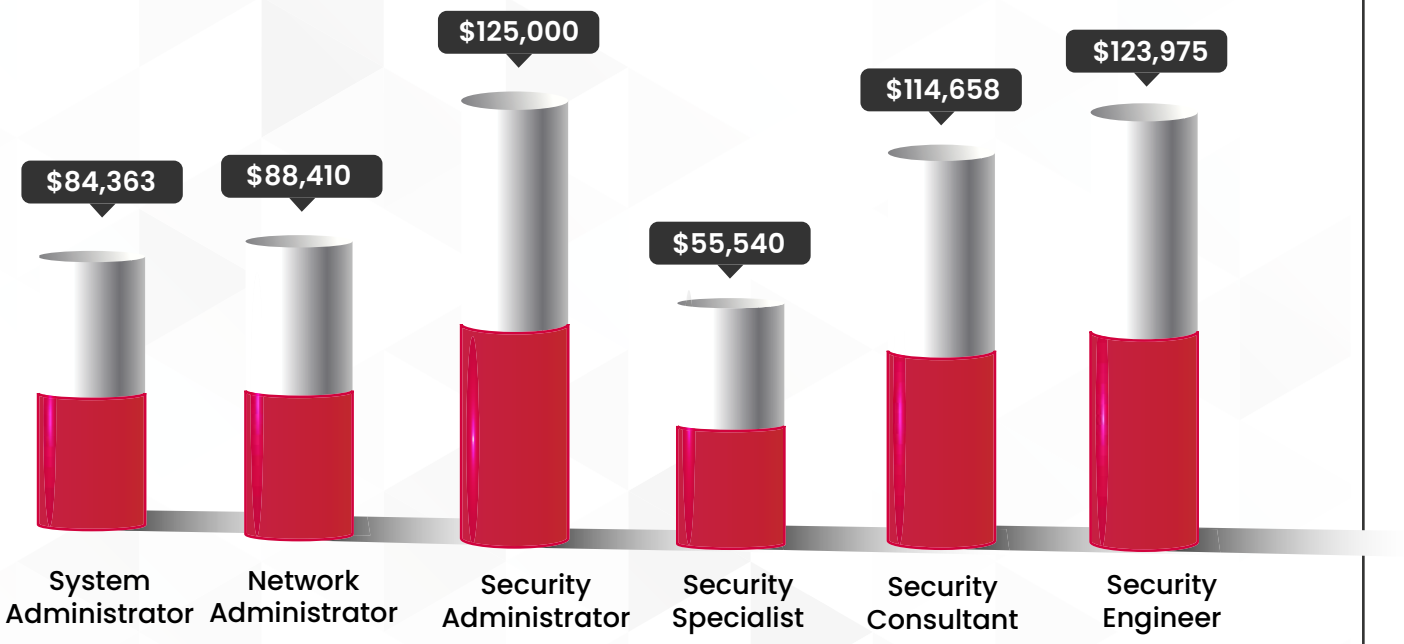
INFOSECTRAIN

5.5: Given a Scenario, Implement Security Awareness Practices

- **Phishing**
  - Campaigns
  - Recognizing a Phishing Attempt
  - Responding to Reported Suspicious Messages
- **Anomalous Behavior Recognition**
  - Risky
  - Unexpected
  - Unintentional
- **User Guidance and Training**
  - Policy/Handbooks
  - Situational Awareness
  - Insider Threat
  - Password Management
  - Removable Media and Cables
  - Social Engineering
  - Operational Security
  - Hybrid/Remote Work Environments
- **Reporting and Monitoring**
  - Initial
  - Recurring
- **Development**
- **Execution**

INFOSECTRAIN

COURSE benefits



Source: Indeed, Glassdoor

www.infosectrain.com I sales@infosectrain.com