INFOSECTRAIN

CYBER SECURITY ANALYST

LEVEL - 1

COURSE CONTENT

sales@infosectrain.com | www.infosectrain.com

Course Content

1. Security Fundamentals : Security+
2. CSA : EC-Council CSA
3. Wireshark : Customized
4. SIEM Solutions (Splunk + Allien Vault)
5. ISO 27001 Fundamental /PCI-DSS

Security Fundamentals : Security+

- Entry level course for understanding and performing security functions in IT security
- Understanding risk management terminologies
- Threat response and handling techniques
- **CompTIA Security+**

1.0 Threats, Attacks and Vulnerabilities

1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.

- Viruses
- Crypto-malware
- Ransomware
- Trojan
- Rootkit
- Keylogger
- Spyware
- Logic
- Backdoor

1.2 Compare and contrast types of attacks.

- Social engineering
  - Phishing
  - Spear phishing
  - Whaling
  - Vishing
  - Tailgating
  - Impersonation
  - Dumpster diving
  - Shoulder surfing
  - Hoax
  - Watering hole attack
  - Principles (reasons for effectiveness)
    - Authority
    - Intimidation
    - Consensus
    - Scarcity
    - Familiarity
    - Trust
    - Urgency
- Application/service attacks
  - DoS
  - DDoS
  - Man-in-the-middle
  - Buffer overflow
  - Injection
  - Cross-site scripting
  - Cross-site request forgery
  - Privilege escalation
  - ARP poisoning
  - Amplification
  - DNS poisoning
  - Domain hijacking
  - Man-in-the-browser
  - Zero day
  - Replay
  - Pass the hash
  - Hijacking and related attacks
    - Clickjacking
    - Session hijacking
    - URL hijacking
    - Typo squatting

- Driver manipulation
  - Shimming
  - Refactoring
- MAC spoofing
- IP spoofing

- Wireless attacks
  - Replay
  - IV
  - Evil twin
  - Rogue AP
  - Jamming
  - WPS
  - Bluejacking
  - Bluesnarfing
  - RFID
  - NFC
  - Disassociation

- Cryptographic attacks
  - Birthday
  - Known plain text/cipher text
  - Rainbow tables
  - Dictionary
  - Brute force
    - Online vs. offline
  - Collision
  - Downgrade
  - Replay
  - Weak implementations

1.3 Explain threat actor types and attributes.

- Types of actors
  - Script kiddies
  - Hacktivist
  - Organized crime
  - Nation states/APT
  - Insiders
  - Competitors

- Attributes of actors
  - Internal/external
  - Level of sophistication
  - Resources/funding
  - Intent/motivation
- Use of open-source intelligence

1.4 Explain penetration testing concepts.

- Active reconnaissance
- Passive reconnaissance
- Pivot
- Initial exploitation
- Persistence
- Escalation of privilege
- Black box
- White box
- Gray box
- Penetration testing vs. vulnerability scanning

1.5 Explain vulnerability scanning concepts.

- Passively test security controls
- Identify vulnerability
- Identify lack of security controls
- Identify common misconfigurations
- Intrusive vs. non-intrusive
- Credentialed vs. non-credentialed
- False positive

1.5 Explain vulnerability scanning concepts.

- Race conditions
- Vulnerabilities due to:
  - End-of-life systems
  - Embedded systems
  - Lack of vendor support
- Improper input handling
- Improper error handling
- Misconfiguration/weak configuration
- Default configuration
- Resource exhaustion
- Untrained users
- Improperly configured accounts
- Vulnerable business processes
- Weak cipher suites and implementations
- Memory/buffer vulnerability
  - Memory leak
  - Integer overflow
  - Buffer overflow
  - Pointer dereference
  - DLL injection
- System sprawl/undocumented assets
- Architecture/design weaknesses
- New threats/zero day
- Improper certificate and key management

2.0 Technologies and Tools

2.1 Install and configure network components, both hardware and software-based, to support organizational security.

- Firewall
  - ACL
  - Application-based vs. network-based
  - Stateful vs. stateless
  - Implicit deny
- VPN concentrator
  - Remote access vs. site-to-site
  - IPSec
  - Tunnel mode
  - Transport mode
  - AH
  - ESP
  - Split tunnel vs. full tunnel
  - TLS
  - Always-on VPN
- NIPS/NIDS
  - Signature-based
  - Heuristic/behavioral
  - Anomaly
  - Inline vs. passive
  - In-band vs. out-of-band
  - Rules
  - Analytics
    - False positive
    - False negative
- Router
  - ACLs
  - Antispoofing
- Switch
  - Port security
  - Layer 2 vs. Layer 3
  - Loop prevention
  - Flood guard

- Proxy
  - Forward and reverse proxy
  - Transparent
  - Application/multipurpose
- Load balancer
  - Scheduling
    - Affinity
    - Round-robin
  - Active-passive
  - Active-active
  - Virtual IPs
- Access point
  - SSID
  - MAC filtering
  - Signal strength
  - Band selection/width
  - Antenna types and placement
  - Fat vs. thin
  - Controller-based vs. standalone
- SIEM
  - Aggregation
  - Correlation
  - Automated alerting and triggers
  - Time synchronization
  - Event deduplication
  - Logs/WORM
- DLP
  - USB blocking
  - Cloud-based
  - Email
- NAC
  - Dissolvable vs. permanent
  - Host health checks
  - Agent vs. agentless
- Mail gateway
  - Spam filter
  - DLP
  - Encryption
- Bridge
- SSL/TLS accelerators
- SSL decryptors
- Media gateway
- Hardware security module

2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.

- Protocol analyzer
- Network scanners
  - Rogue system detection
  - Network mapping
- Wireless scanners/cracker
- Password cracker
- Vulnerability scanner
- Configuration compliance scanner
- Exploitation frameworks
- Data sanitization tools
- Steganography tools
- Honeypot
- Backup utilities
- Banner grabbing
- Passive vs. active
- Command line tools
  - ping
  - netstat

- tracert
- nslookup/dig
- arp
- ipconfig/ip/ifconfig
- tcpdump
- nmap
- netcat

2.3 Given a scenario, troubleshoot common security issues.

- Unencrypted credentials/clear text
- Logs and events anomalies
- Permission issues
- Access violations
- Certificate issues
- Data exfiltration
- Misconfigured devices
  - Firewall
  - Content filter
  - Access points
- Weak security configurations
- Personnel issues
  - Policy violation
  - Insider threat
  - Social engineering
  - Social media
  - Personal email
- Unauthorized software
- Baseline deviation
- License compliance violation (availability/integrity)
- Asset management
- Authentication issues

2.4 Given a scenario, analyze and interpret output from security technologies.

- HIDS/HIPS
- Antivirus
- File integrity check
- Host-based firewall
- Application whitelisting
- Removable media control
- Advanced malware tools
- Patch management tools
- UTM
- DLP
- Data execution prevention
- Web application firewall

2.5 Given a scenario, deploy mobile devices securely.

- Connection methods
  - Cellular
  - WiFi
  - SATCOM
  - Bluetooth
  - NFC
  - ANT
  - Infrared
  - USB
- Mobile device management concepts
  - Application management
  - Content management
  - Remote wipe
  - Geofencing
  - Geolocation
  - Screen locks
  - Push notification services
  - Passwords and pins
  - Biometrics
  - Context-aware authentication
  - Containerization
  - Storage segmentation
  - Full device encryption
- Enforcement and monitoring for:
  - Third-party app stores
  - Rooting/jailbreaking

- Sideloading
- Custom firmware
- Carrier unlocking
- Firmware OTA updates
- Camera use
- SMS/MMS
- External media
- USB OTG
- Recording microphone
- GPS tagging
- WiFi direct/ad hoc
- Tethering
- Payment methods

- Deployment models
  - BYOD
  - COPE
  - CYOD
  - Corporate-owned
  - VDI

2.4 Given a scenario, implement secure protocols.

- Protocols
  - DNSSEC
  - SSH
  - S/MIME
  - SRTP
  - LDAPS
  - FTPS
  - SFTP
  - SNMPv3
  - SSL/TLS
  - HTTPS
  - Secure POP/IMAP
- Use cases
  - Voice and video
  - Time synchronization
  - Email and web
  - File transfer
  - Directory services
  - Remote access
  - Domain name resolution
  - Routing and switching
  - Network address allocation
  - Subscription services

3.0 Architecture and Design

3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides.

- Industry-standard frameworks and reference architectures
  - Regulatory
  - Non-regulatory
  - National vs. international
  - Industry-specific frameworks
- Benchmarks/secure configuration guides
  - Platform/vendor-specific guides
  - Web server
  - Operating system
  - Application server
  - Network infrastructure devices
  - General purpose guides
- Defense-in-depth/layered security
  - Vendor diversity
  - Control diversity
    - Administrative
    - Technical
  - User training

3.2 Given a scenario, implement secure network architecture concepts.

- Zones/topologies
  - DMZ
  - Extranet
  - Intranet
  - Wireless
  - Guest
  - Honeynets
  - NAT
  - Ad hoc
- Segregation/segmentation/isolation
  - Physical
  - Logical (VLAN)
  - Virtualization
  - Air gaps
- Tunneling/VPN
  - Site-to-site
  - Remote access
- Security device/technology placement
  - Sensors
  - Collectors
  - Correlation engines
  - Filters
  - Proxies
  - Firewalls
  - VPN concentrators
  - SSL accelerators
  - Load balancers
  - DDoS mitigator
  - Aggregation switches
  - Taps and port mirror
- SDN

3.3 Given a scenario, implement secure systems design.

- Hardware/firmware security
  - FDE/SED
  - TPM
  - HSM
  - UEFI/BIOS
  - Secure boot and attestation
  - Supply chain
  - Hardware root of trust
  - EMI/EMP
- Operating systems
  - Types
    - Network
    - Server
    - Workstation
    - Appliance
    - Kiosk
    - Mobile OS
  - Patch management
  - Disabling unnecessary ports and services
  - Least functionality
  - Secure configurations
  - Trusted operating system
  - Application whitelisting/blacklisting
  - Disable default accounts/passwords
- Peripherals
  - Wireless keyboards
  - Wireless mice
  - Displays
  - WiFi-enabled MicroSD cards

- Printers/MFDs
- External storage devices

3.4 Explain the importance of secure staging deployment concepts.

- Sandboxing
- Environment
  - Development
  - Test
  - Staging
  - Production
- Secure baseline
- Integrity measurement

3.5 Explain the security implications of embedded systems.

- SCADA/ICS
- Smart devices/IoT
  - Wearable technology
  - Home automation
- HVAC
- SoC
- RTOS
- Printers/MFDs
- Camera systems
- Special purpose
  - Medical devices
  - Vehicles
  - Aircraft/UAV

3.6 Summarize secure application development and deployment concepts.

- Development life-cycle models
  - Waterfall vs. Agile
- Secure DevOps
  - Security automation
  - Continuous integration
  - Baselining
  - Immutable systems
  - Infrastructure as code
- Version control and change management
- Provisioning and deprovisioning
- Secure coding techniques
  - Proper error handling
  - Proper input validation
  - Normalization
  - Stored procedures
  - Code signing
  - Encryption
  - Obfuscation/camouflage
  - Code reuse/dead code
  - Server-side vs. client-side execution and validation
  - Memory management
  - Use of third-party libraries and SDKs
  - Data exposure
- Code quality and testing
  - Static code analyzers
  - Dynamic analysis (e.g., fuzzing)
  - Stress testing
  - Sandboxing
  - Model verification

- Compiled vs. runtime code

3.7 Summarize cloud and virtualization concepts.

- Hypervisor
  - Type I
  - Type II
  - Application cells/containers
- VM sprawl avoidance
- VM escape protection
- Cloud storage
- Cloud deployment models
  - SaaS
  - PaaS
  - IaaS
  - Private
  - Public
  - Hybrid
  - Community
- Secure baseline
- Integrity measurement
- On-premise vs. hosted vs. cloud
- VDI/VDE
- Cloud access security broker
- Security as a Service

3.8 Explain how resiliency and automation strategies reduce risk.

- Automation/scripting
  - Automated courses of action
  - Continuous monitoring
  - Configuration validation
- Templates
- Master image
- Non-persistence
  - Snapshots
  - Revert to known state
  - Rollback to known configuration
  - Live boot media
- Elasticity
- Scalability
- Distributive allocation
- Redundancy
- Fault tolerance
- High availability
- RAID

3.9 Explain the importance of physical security controls.

- Lighting
- Signs
- Fencing/gate/cage
- Security guards
- Alarms
- Safe
- Secure cabinets/enclosures
- Protected distribution/Protected cabling
- Airgap
- Mantrap
- Faraday cage
- Lock types
- Biometrics
- Barricades/bollards
- Tokens/cards

- Environmental controls
  - HVAC
  - Hot and cold aisles
  - Fire suppression
- Cable locks
- Screen filters
- Cameras
- Motion detection
- Logs
- Infrared detection
- Key management

4.0 Identity and Access Management

4.1 Compare and contrast identity and access management concepts

- Identification, authentication, authorization and accounting (AAA)
- Multifactor authentication
  - Something you are
  - Something you have
  - Something you know
  - Somewhere you are
  - Something you do
- Federation
- Single sign-on
- Transitive trust

4.2 Given a scenario, install and configure identity and access services.

- LDAP
- Kerberos
- TACACS+
- CHAP
- PAP
- MSCHAP
- RADIUS
- SAML
- OpenID Connect
- OAUTH
- Shibboleth
- Secure token
- NTLM

4.3 Given a scenario, implement identity and access management controls.

- Access control models
  - MAC
  - DAC
  - ABAC
  - Role-based access control
  - Rule-based access control
- Physical access control
  - Proximity cards
  - Smart cards
- Biometric factors
  - Fingerprint scanner
  - Retinal scanner
  - Iris scanner
  - Voice recognition
  - Facial recognition
  - False acceptance rate
  - False rejection rate
  - Crossover error rate

- Tokens
  - Hardware
  - Software
  - HOTP/TOTP
- Certificate-based authentication
  - PIV/CAC/smart card
  - IEEE 802.1x
- File system security
- Database security

4.4 Given a scenario, differentiate common account management practices.

- Account types
  - User account
  - Shared and generic accounts/credentials
  - Guest accounts
  - Service accounts
  - Privileged accounts
- General Concepts
  - Least privilege
  - Onboarding/offboarding
  - Permission auditing and review
  - Usage auditing and review
  - Time-of-day restrictions
  - Recertification
  - Standard naming convention
  - Account maintenance
  - Group-based access control
  - Location-based policies
- Account policy enforcement
  - Credential management
  - Group policy
  - Password complexity
  - Expiration
  - Recovery
  - Disablement
  - Lockout
  - Password history
  - Password reuse
  - Password length

5.0 Risk Management

5.1 Explain the importance of policies, plans and procedures related to organizational security.

- Standard operating procedure
- Agreement types
  - BPA
  - SLA
  - ISA
  - MOU/MOA
- Personnel management
  - Mandatory vacations
  - Job rotation
  - Separation of duties
  - Clean desk
  - Background checks
  - Exit interviews
  - Role-based awareness training
  - Data owner
  - System administrator
  - System owner
  - User
  - Privileged user

- Executive user
- NDA
- Onboarding
- Continuing education
- Acceptable use policy/rules of behavior
- Adverse actions

- General security policies
  - Social media networks/applications
  - Personal email

5.2 Summarize business impact analysis concepts.

- RTO/RPO
- MTBF
- MTTR
- Mission-essential functions
- Identification of critical systems
- Single point of failure
- Impact
  - Life
  - Property
  - Safety
  - Finance
  - Reputation
- Privacy impact assessment
- Privacy threshold assessment

5.3 Explain risk management processes and concepts.

- Threat assessment
  - Environmental
  - Manmade
  - Internal vs. external
- Risk assessment
  - SLE
  - ALE
  - ARO
  - Asset value
  - Risk register
  - Likelihood of occurrence
  - Supply chain assessment
  - Impact
  - Quantitative
  - Qualitative
  - Testing
    - Penetration testing authorization
    - Vulnerability testing authorization
  - Risk response techniques
    - Accept
    - Transfer
    - Avoid
    - Mitigate
- Change management

5.4 Given a scenario, follow incident response procedures.

- Incident response plan
  - Documented incident types/category definitions
  - Roles and responsibilities
  - Reporting requirements/escalation
  - Cyber-incident response teams
  - Exercise

- Incident response process
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons learned

5.5 Summarize basic concepts of forensics.

- Order of volatility
- Chain of custody
- Legal hold
- Data acquisition
  - Capture system image
  - Network traffic and logs
  - Capture video
  - Record time offset
  - Take hashes
  - Screenshots
  - Witness interviews
- Preservation
- Recovery
- Strategic intelligence/ counterintelligence gathering
  - Active logging
- Track man-hours

5.6 Explain disaster recovery and continuity of operation concepts.

- Recovery sites
  - Hot site
  - Warm site
  - Cold site
- Order of restoration
- Backup concepts
  - Differential
  - Incremental
  - Snapshots
  - Full
- Geographic considerations
  - Off-site backups
  - Distance
  - Location selection
  - Legal implications
  - Data sovereignty
- Continuity of operation planning
  - Exercises/tabletop
  - After-action reports
  - Failover
  - Alternate processing sites
  - Alternate business practices

5.7 Compare and contrast various types of controls.

- Deterrent
- Preventive
- Detective
- Corrective
- Compensating
- Technical
- Administrative
- Physical

5.8 Given a scenario, carry out data security and privacy practices.

- Data destruction and media sanitization
  - Burning
  - Shredding
  - Pulping
  - Pulverizing
  - Degaussing
  - Purging
  - Wiping
- Data sensitivity labeling and handling
  - Confidential
  - Private
  - Public
  - Proprietary
  - PII
  - PHI
- Data roles
  - Owner
  - Steward/custodian
  - Privacy officer
- Data retention
- Legal and compliance

6.0 Cryptography and PKI

6.1 Compare and contrast basic concepts of cryptography.

- Symmetric algorithms
- Modes of operation
- Asymmetric algorithms
- Hashing
- Salt, IV, nonce
- Elliptic curve
- Weak/deprecated algorithms
- Key exchange
- Digital signatures
- Diffusion
- Confusion
- Collision
- Steganography
- Obfuscation
- Stream vs. block
- Key strength
- Session keys
- Ephemeral key
- Secret algorithm
- Data-in-transit
- Data-at-rest
- Data-in-use
- Random/pseudo-random number generation
- Key stretching
- Implementation vs. algorithm selection
  - Crypto service provider
  - Crypto modules
- Perfect forward secrecy
- Security through obscurity
- Common use cases
  - Low power devices
  - Low latency
  - High resiliency
  - Supporting confidentiality
  - Supporting integrity
  - Supporting obfuscation
  - Supporting authentication
  - Supporting non-repudiation
  - Resource vs. security constraints

6.2 Explain cryptography algorithms and their basic characteristics.

- Symmetric algorithms
  - AES
  - DES
  - 3DES
  - RC4
  - Blowfish/Twofish
- Cipher modes
  - CBC
  - GCM
  - ECB
  - CTR
  - Stream vs. block
- Asymmetric algorithms
  - RSA
  - DSA
  - Diffie-Hellman
    - Groups
  - DHE
  - ECDHE
  - Elliptic curve
  - PGP/GPG
- Hashing algorithms
  - MD5
  - SHA
  - HMAC
  - RIPEMD
- Key stretching algorithms
  - BCRYPT
  - PBKDF2
- Obfuscation
  - XOR
  - ROT13
  - Substitution ciphers

6.3 Given a scenario, install and configure wireless security settings.

- Cryptographic protocols
  - WPA
  - WPA2
  - CCMP
  - TKIP
- Authentication protocols
  - EAP
  - PEAP
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS
  - IEEE 802.1x
  - RADIUS Federation
- Methods
  - PSK vs. Enterprise vs. Open
  - WPS
  - Captive portals

6.4 Given a scenario, implement public key infrastructure.

- Components
  - CA
  - Intermediate CA
  - CRL
  - OCSP
  - CSR
  - Certificate
  - Public key
  - Private key
  - Object identifiers (OID)
- Concepts
  - Online vs. offline CA
  - Stapling
  - Pinning
  - Trust model
  - Key escrow
  - Certificate chaining
- Types of certificates
  - Wildcard
  - SAN
  - Code signing
  - Self-signed
  - Machine/computer
  - Email
  - User
  - Root
  - Domain validation
  - Extended validation
- Certificate formats
  - DER
  - PEM
  - PFX
  - CER
  - P12
  - P7B

CSA : EC-Council CSA

- Beginner course for performing entry-level, intermediate-level SOC operations
- Security Operation Management fundamentals
- Understanding of incident detection, incident response and logging concepts
- In-depth understanding of Security Information and Event Management (SIEM)
- Concepts of threat intelligence
- **Certified SOC Analyst**

Learning Objectives

- Gain Knowledge of SOC processes, procedures, technologies, and workflows.
- Gain basic understanding and in-depth knowledge of security threats, attacks, vulnerabilities, attacker's behaviors, cyber kill chain, etc.
- Able to recognize attacker tools, tactics, and procedures to identify indicators of compromise (IOCs) that can be utilized during active and future investigations.
- Able to monitor and analyze logs and alerts from a variety of different technologies across multiple platforms (IDS/IPS, end-point protection, servers and workstations).
- Gain knowledge of Centralized Log Management (CLM) process.
- Able to perform Security events and log collection, monitoring, and analysis.
- Gain experience and extensive knowledge of Security Information and Event Management.
- Gain knowledge on administering SIEM solutions (Splunk/AlienVault/OSSIM/ELK).
- Understand the architecture, implementation and fine tuning of SIEM solutions (Splunk/AlienVault/OSSIM/ELK).
- Gain hands-on experience on SIEM use case development process.
- Able to develop threat cases (correlation rules), create reports, etc.
- Learn use cases that are widely used across the SIEM deployment.
- Plan, organize, and perform threat monitoring and analysis in the enterprise.
- Able to monitor emerging threat patterns and perform security threat analysis.
- Gain hands-on experience in alert triaging process.
- Able to escalate incidents to appropriate teams for additional assistance.
- Able to use a Service Desk ticketing system.
- Able to prepare briefings and reports of analysis methodology and results.
- Gain knowledge of integrating threat intelligence into SIEM for enhanced incident detection and response.

- Able to make use of varied, disparate, constantly changing threat information.
- Gain knowledge of Incident Response Process.
- Gain understating of SOC and IRT collaboration for better incident response

Course Outline

Module 01: Security Operations and Management

Module 02: Understanding Cyber Threats, IoCs, and Attack Methodology

Module 03: Incidents, Events, and Logging

Module 04: Incident Detection with Security Information and Event Management (SIEM)

Module 05: Enhanced Incident Detection with Threat Intelligence

Module 06: Incident Response

Wireshark : Customized

- Establishing fundamental concepts through use-cases
- Traffic capturing and analysis techniques
- Configurational understanding

1. Introduction to Network Analysis and Wireshark

» TCP/IP Analysis Checklist
» Top Causes of Performance Problems
» Get the Latest Version of Wireshark
» Capturing Traffic
» Opening Trace Files
» Processing Packets
» The Qt Interface Overview
» Using Linked Panes
» The Icon Toolbar
» Master the Intelligent Scrollbar
» The Changing Status Bar
» Right-Click Functionality
» General Analyst Resources
» Your First Task When You Leave Class

2. Learn Capture Methods and Use Capture Filters

» Analyze Switched Networks
» Walk-Through a Sample
» Analyze Full-Duplex Links with a Network TAP
» Analyze Wireless Networks
» USB Capture
» Initial Analyzing Placement
» Remote Capture Techniques
» Available Capture Interfaces
» Save Directly to Disk
» Capture File Configurations
» Limit Your Capture with Capture Filters
» Examine Key Capture Filters

3. Customize for Efficiency: Configure Your Global Preferences

» First Step: Create a Troubleshooting Profile
» Customize the User Interface
» Add Custom Columns for the Packet List Pane

» Set Your Global Capture Pr
» Define Name Resolution Preferences
» Configure Individual Protocol Preferences

4. Navigate Quickly and Focus Faster with Coloring Techniques

» Move Around Quickly: Navigation Techniques
» Find a Packet Based on Various Characteristics
» Build Permanent Coloring Rules
» Identify a Coloring Source
» Use the Intelligent Scrollbar with Custom Coloring Rules
» Apply Temporary Coloring
» Mark Packets of Interest

5. Spot Network and Application Issues with Time Values and Summaries

» Examine the Delta Time (End-of-Packet to End-of-Packet)
» Set a Time Reference
» Compare Timestamp Values
» Compare Timestamps of Filtered Traffic
» Enable and Use TCP Conversation Timestamps
» Compare TCP Conversation Timestamp Values
» Determine the Initial Round Trip Time (iRTT)
» Troubleshooting Example Using Time
» Analyze Delay Types

6. Create and Interpret Basic Trace File Statistics

» Examine Trace File Summary Information
» View Active Protocols
» Graph Throughput to Spot Performance Problems Quickly
» Locate the Most Active Conversations and Endpoints
» Other Conversation Options
» Graph the Traffic Flows for a More Complete View
» Burst Statistics
» Numerous Other Statistics are Available
» Quick Overview of VoIP Traffic Analysis
» SIP and RTP Analysis Overview
» SIP Call Setup
» Analyzing Call Setup with SIP
» Session Bandwidth and RTP Port Definition

7. Focus on Traffic Using Display Filters

» Display Filters
» Filter on Conversations/Endpoints
» Build Filters Based on Packets
» Display Filter Syntax
» Use Comparison Operators and Advanced Filters
» Filter on Text Strings
» Build Filters Based on Expressions
» Watch for Common Display Filter Mistakes
» Share Your Display Filters

8. TCP/IP Communications and Resolutions Overview

» TCP/IP Functionality
» When Everything Goes Right
» The Multi-Step Resolution Process
» Resolution Helped Build the Packet
» Where Faults Can Occur
» Typical Causes of Slow Performance

9. Analyze DNS Traffic

» DNS Overview
» DNS Packet Structure
» DNS Queries
» Filter on DNS Traffic
» Analyze Normal/Problem DNS Traffic

10. Analyze ARP Traffic

» ARP Overview
» ARP Packet Structure
» Filter on ARP Traffic
» Analyze Normal/Problem ARP Traffic

11. Analyze IPv4 Traffic

» IPv4 Overview
» IPv4 Packet Structure
» Analyze Broadcast/Multicast Traffic
» Filter on IPv4 Traffic
» IP Protocol Preferences
» Analyze Normal/Problem IP Traffic

12. Analyze ICMP Traffic

» ICMP Overview
» ICMP Packet Structure
» Filter on ICMP Traffic
» Analyze Normal/Problem ICMP Traffic

13. Analyze UDP Traffic

» UDP Overview
» Watch for Service Refusals
» UDP Packet Structure
» Filter on UDP Traffic
» Follow UDP Streams to Reassemble Data
» Analyze Normal/Problem UDP Traffic

14. Analyze TCP Protocol

» TCP Overview
» The TCP Connection Process
» TCP Handshake Problem
» Watch Service Refusals
» TCP Packet Structure
» The TCP Sequencing/Acknowledgment Process

» Packet Loss Detection in Wireshark
» Fast Recovery/Fast Retransmission Detection in Wireshark
» Retransmission Detection in Wireshark
» Out-of-Order Segment Detection in Wireshark
» Selective Acknowledgement (SACK)
» Window Scaling
» Window Size Issue: Receive Buffer Problem
» Window Size Issue: Unequal Window Size Beliefs
» TCP Sliding Window Overview
» Troubleshoot TCP Quickly with Expert Info
» Filter on TCP Traffic and TCP Problems
» Properly Set TCP Preferences
» Follow TCP Streams to Reassemble Data 16. Examine Advanced Trace File Statistics
» Build Advanced IO Graphs
» Graph Round Trip Times
» Graph TCP Throughput
» Find Problems Using TCP Time-Sequence Graphs

15. Graph Traffic Characteristics

» Advanced I/O Graphing
» Graph Round Trip Times
» Graph TCP Throughput
» Find Problems Using TCP Time Sequence Graphs

16. Analyze HTTP Traffic

» HTTP Overview
» HTTP Packet Structure
» Filter on HTTP Traffic
» Reassembling HTTP Objects
» HTTP Statistics
» HTTP Response Time
» Overview of HTTP/2
» HTTP/2 Analysis Fundamentals
» HTTP /2 Frame Format
» Analyze Normal/Problem HTTP Traffic

17. Analyze TLS-Encrypted Traffic (HTTPS)

» Analyze HTTPS Traffic
» Encrypted Alerts
» Decryption Steps
» Filter on SSL

18. Review Your 10 Key Troubleshooting Steps

» Baseline "NormalTraffic
» Use Color
» Look Who's Talking: Examine Conversations and Endpoints
» Focus by Filtering
» Create Basic IO Graphs

» Examine Delta Time Values
» Examine the Expert System
» Follow the Streams
» Graph Bandwidth Use, Round Trip Time, and TCP Time/Sequence Information
» Watch Refusals and Redirections

SIEM Solutions (Splunk + Allien Vault)

- Understanding requirement and fundamentals of SIEM
- Administration and management of SIEM
- Traffic monitoring, searching, capturing, inspection, analysis and reporting
- Analysis using scenarios and use-cases

SIEM Solutions (Splunk + Allien Vault)

- Understanding the essentials of information security management system (ISMS)
- Implementation and management
- Introduction of ISO/IEC 27000 family of standards
- PCI- DSS

INFOSECTRAIN

sales@infosectrain.com | www.infosectrain.com