SEC450.1: Blue Team Tools and Operations

- Introduction to the Blue Team Mission
 - What is a SOC? What is the mission?
 - Why are we being attacked?
 - Modern defense mindset
 - The challenges of SOC work
- SOC Overview
 - The people, process, and technology of a SOC
 - Aligning the SOC with your organization
 - SOC functional component overview
 - Tiered vs. tierless SOCs
 - Important operational documents
- Defensible Network Concepts
 - Understanding what it takes to be defensible
 - Network security monitoring (NSM) concepts
 - NSM event collection
 - NSM by network layer
 - Continuous security monitoring (CSM) concepts
 - CSM event collection
 - Monitoring sources overview
 - Data centralization
- Events, Alerts, Anomalies, and Incidents
 - Event collection
 - Event log flow
 - Alert collection
 - Alert triage and log flow
 - Signatures vs. anomalies
 - Alert triage workflow and incident creation
- Incident Management Systems
 - SOC data organization tools
 - o Incident management systems options and features
 - Data flow in incident management systems
 - Case creation, alerts, observables, playbooks, and workflow
 - Case and alert naming convention
 - Incident categorization framework
- Threat Intelligence Platforms
 - What is cyber threat intelligence?
 - Threat data vs. information vs. intelligence
 - Threat intel platform options, features, and workflow
 - Event creation, attributes, correlation, and sharing
- SIEM
 - Benefits of data centralization
 - SIEM options and features
 - o SIEM searching, visualizations, and dashboards

- Use cases and use case databases
- Automation and Orchestration
 - How SOAR works and benefits the SOC
 - Options and features
 - SOAR value-adds and API interaction
 - Data flow between SOAR and the SIEM, incident management system, and threat intelligence platform
- Who Are Your Enemies?
 - Who's attacking us and what do they want?
 - Opportunistic vs. targeted attackers
 - o Hacktivists, insiders, organized crime, governments
 - Motivation by attacker group
 - Case studies of different attack groups
 - Attacker group naming conventions

SEC450.2: Understanding Your Network

- Corporate Network Architecture
 - Routers and security
 - Zones and traffic flow
 - Switches and security
 - o VLANs
 - Home firewall vs. corporate next-gen firewall capabilities
 - The logical vs. physical network
 - Points of visibility
 - Traffic capture
 - Network architecture design ideals
 - Zero-trust architecture and least-privilege ideals
- Traffic Capture and Analysis
 - Network traffic capture formats
 - NetFlow
 - Layer 7 metadata collection
 - PCAP collection
 - Wireshark and Moloch
- Understanding DNS
 - Name to IP mapping structure
 - DNS server and client types (stub resolvers, forwarding, caching, and authoritative servers)
 - Walkthrough of a recursive DNS resolution
 - Request types
 - Setting records via registrars and on your own server
 - A and AAAA records
 - PTR records and when they might fail
 - TXT records and their uses
 - CNAME records and their uses
 - MX records for mail
 - SRV records

• NS records and glue records

• DNS analysis and attacks

- Detecting requests for malicious sites
- Checking domain reputation, age, randomness, length, subdomains
- Whois
- Reverse DNS lookups and passive DNS
- Shared hosting
- Detecting DNS recon
- Unauthorized DNS server use
- Domain shadowing
- DNS tunneling
- DNS traffic flow and analysis
- IDNs, punycode, and lookalike domains
- New DNS standards (DNS over TLS, DNS over HTTPS, DNSSEC)

• Understanding HTTP and HTTPS

- Decoding URLs
- \circ $\;$ HTTP communication between client and server $\;$
- Browser interpretation of HTTP and REST APIs
- GET, POST, and other methods
- Request header analysis
- Response header analysis
- Response codes
- \circ The path to the Internet
- REST APIs
- WebSockets
- HTTP/2 & HTTP/3
- Analyzing HTTP for Suspicious Activity
 - HTTP attack and analysis approaches
 - Credential phishing
 - Reputation checking
 - \circ Sandboxing
 - URL and domain OSINT
 - Header and content analysis
 - User-agent deconstruction
 - Cookies
 - Base64 encoding works and conversion
 - File extraction and analysis
 - High frequency GET/POST activity
 - Host headers and naked IP addresses
 - Exploit kits and malicious redirection
 - HTTPS and certificate inspection
 - SSL decryption what you can do with/without it
 - TLS 1.3
- How SMTP and Email Attacks Work
 - Email delivery infrastructure
 - SMTP Protocol
 - Reading email headers and source

- Identifying spoofed email
- Decoding attachments
- How email spoofing works
- How SPF works
- How DKIM works
- How DMARC works
- Additional Important Protocols
 - SMB versions and typical attacks
 - DHCP for defenders
 - ICMP and how it is abused
 - FTP and attacks
 - SSH and attacks
 - PowerShell remoting

SEC450.3: Understanding Endpoints, Logs, and Files

• Endpoint Attack Tactics

- Endpoint attack centricity
- Initial exploitation
- Service-side vs client-side exploits
- Post-exploitation tactics, tools, and explanations execution, persistence, discovery, privilege escalation, credential access, lateral movement, collection, exfiltration
- Endpoint Defense In-Depth
 - Network scanning and software inventory
 - Vulnerability scanning and patching
 - Anti-exploitation
 - Whitelisting
 - Host intrusion prevention and detection systems
 - Host firewalls
 - File integrity monitoring
 - Privileged access workstations
 - Windows privileges and permissions
 - Endpoint detection and response tools (EDR)
 - File and drive encryption
 - Data loss prevention
 - User and entity behavior analytics (UEBA)

How Windows Logging Works

- Channels, event IDs, and sources
- XML format and event templates
- Log collection path
- Channels of interest for tactical data collection
- How Linux Logging Works
 - Syslog log format
 - Syslog daemons
 - Syslog network protocol
 - Log collection path

- Systemd journal
- Additional command line auditing options
- Application logging
- Service vs. system logs

• Interpreting Important Events

- Windows and Linux login events
- Process creation logs for Windows and Linux
- Additional activity monitoring
- Firewall events
- Object and file auditing
- Service creation and operation logging
- o New scheduled tasks
- USB events
- User creation and modification
- Windows Defender events
- PowerShell logging
- Kerberos and Active Directory Events
- Authentication and the ticket-granting service
- Kerberos authentication steps
- Kerberos log events in detail

• Log Collection, Parsing, and Normalization

- Logging pipeline and collection methods
- Windows vs. Linux log agent collection options
- Parsing unstructured vs. structured logs
- SIEM-centric formats
- Efficient searching in your SIEM
- The role of parsing and log enrichment
- Log normalization and categorization
- Log storage and retention lifecycle
- Files Contents and Identification
 - File contents at the byte level
 - How to identify a file by the bytes
 - Magic bytes
 - Nested files
 - Strings uses, encoding options, and viewing

Identifying and Handling Suspicious Files

- Safely handling suspicious files
- Dangerous files types
- Exploits vs. program "features"
- Exploits vs. Payloads
- Executables, scripts, office docs, RTFs, PDFs, and miscellaneous exploits
- Hashing and signature verification
- Signature inspection and safety of verified files
- o Inspection methods, detecting malicious scripts and other files

SEC450.4: Triage and Analysis

• Alert Triage and Prioritization

- Priority for triage
- Spotting late-stage attacks
- Attack lifecycle models
- Spotting exfiltration and destruction attempts
- Attempts to access sensitive users, hosts, and data
- Targeted attack identification
- Lower-priority alerts
- Alert validation
- Perception, Memory, and Investigation
 - The role of perception and memory in observation and analysis
 - Working within the limitations of short-term memory
 - Efficiently committing info to long-term memory
 - Decomposition and externalization techniques
 - The effects of experience on speed and creativity

• Mental Models for Information Security

- Network and file encapsulation
- Cyber kill chain
- Defense-in-depth
- NIST cybersecurity framework
- Incident response cycle
- Threat intelligence levels, models, and uses
- F3EAD
- o Diamond model
- The OODA loop
- Attack modeling, graph/list thinking, attack trees
- Pyramid of pain
- MITRE ATT&CK

• Structured Analysis Techniques

- Compensating for memory and perception issues via structured analysis
- System 1 vs. System 2 thinking and battling tacit knowledge
- Data-driven vs. concept-driven analysis
- Structured analytic techniques
- o Idea generation and creativity, hypothesis development
- Confirmation bias avoidance
- Analysis of competing hypotheses
- Diagnostic reasoning
- Link analysis, event matrices

• Analysis Questions and Tactics

- Where to start breaking down an investigation
- Alert validation techniques
- Sources of network and host information
- Data extraction
- OSINT sources
- Data interpretation
- Assessing strings, files, malware artifacts, email, links
- Analysis OPSEC

- OPSEC vs. your threat model
- Traffic light protocol and intel sharing
- Permissible action protocol
- Common OPSEC failures and how to avoid them
- Intrusion Discovery
 - Dwell time and intrusion type
 - Determining attacker motivation
 - Assessing business risk
 - Choosing an appropriate response
 - Reacting to opportunistic/targeted attacks
 - Common missteps in incident response
- Incident Closing and Quality Review
 - Steps for closing incidents
 - Quality review and peer feedback
 - Analytical completeness checks
 - Closed case classification
 - Attribution
 - Maintaining quality over time
 - Premortem and challenge analysis
 - Peer review, red team, team A/B analysis, and structured self-critique

SEC450.5: Continuous Improvement, Analytics, and Automation

- Improving Life in the SOC
 - Expectations vs. common reality
 - Burnout and stress avoidance
 - Improvement through SOC human capital theory
 - The role of automation, operational efficiency, and metrics in burnout
 - Other common SOC issues
- Analytic Features and Enrichment
 - Goals of analytic creation
 - Log features and parsing
 - High-feature vs. low-feature logs
 - Improvement through SIEM enrichment
 - External tools and other enrichment sources

New Analytic Design, Testing, and Sharing

- Tolerance to false positives/negatives
- The false positive paradox
- Types of analytics
- Feature selection for analytics
- Matching with threat intel
- Regular expressions
- Common matching and rule logic options
- Analytic generalization and sharing with Sigma
- Tuning and False Positive Reduction
 - Dealing with alerts and runaway alert queues
 - How many analysts should you have?

- Types of poor alerts
- Tuning strategy for poor alert types
- Tuning via log field analysis
- Using policy to raise fidelity
- Sensitivity vs. specificity
- Automation and fast lanes

Automation and Orchestration

- The definition of automation vs. orchestration
- What is SOAR?
- SOAR product considerations
- Common SOAR use cases
- Enumeration and enrichment
- Response actions
- Alert and case management
- The paradox of automation
- DIY scripting

Improving Operational Efficiency and Workflow

- Micro-automation
- Form filling
- Text expanders
- Email templates
- Smart keywords
- Browser plugins
- Text caching
- JavaScript page modification
- OS Scripting

• Containing Identified Intrusions

- Containment and analyst empowerment
- Isolation options across network layers physical, link, network, transport, application
- DNS firewalls, HTTP blocking and containment, SMTP, Web Application Firewalls
- Host-based containment tools
- Skill and Career Development
 - Learning through conferences, capture-the-flag challenges, and podcasts
 - Home labs
 - Writing and public speaking
 - Techniques for mastery and continual progress

SEC450.6: Capstone: Defend the Flag