Blue Team or Cyber Defense Package Level 1 Syllabus

SEC450,SEC503,SEC505

SEC450: Blue Team Fundamentals: Security Operations and Analysis

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
  - 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
    - 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
    - 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
    - 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
    - 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
    - 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
    - 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
    - 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
  - 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
  - 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
  - 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 : Continious Improvements , 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

SEC503: Intrusion Detection In-Depth

SEC503.1 : Fundamentals of Traffic Analysis : Part I

- Concepts of TCP/IP
- Why is it necessary to understand packet headers and data?
- TCP/IP communications model
- Data encapsulation/de-encapsulation
- Discussion of bits, bytes, binary, and hex
- Introduction to Wireshark
- Navigating around Wireshark
- Examination of Wireshark statistics
- Stream reassembly
- Finding content in packets
- Network Access/Link Layer: Layer 2
- Introduction to 802.x link layer
- Address resolution protocol
- ARP spoofing
- IP Layer: Layer 3
- IPv4
    - Examination of fields in theory and practice
    - Checksums and their importance, especially for an IDS/IPS
    - Fragmentation: IP header fields involved in fragmentation, composition of the fragments, fragmentation attacks
- IPv6
    - Comparison with IPv4
    - IPv6 addresses
    - Neighbor discovery protocol
    - Extension headers
    - IPv6 in transition

SEC503.2 : Fundamentals of Traffic Analysis : Part II

- Wireshark Display Filters
- Examination of some of the many ways that Wireshark facilitates creating display filters
- Composition of display filters
- Writing BPF Filters
- The ubiquity of BPF and utility of filters

- Format of BPF filters
- Use of bit masking
- TCP
- Examination of fields in theory and practice
- Packet dissection
- Checksums
- Normal and abnormal TCP stimulus and response
- Importance of TCP reassembly for IDS/IPS
- UDP
- Examination of fields in theory and practice
- UDP stimulus and response
- ICMP
- Examination of fields in theory and practice
- When ICMP messages should not be sent
- Use in mapping and reconnaissance
- Normal ICMP
- Malicious ICMP
- Real-World Analysis -- Command Line Tools
- Regular Expressions fundamentals
- Rapid processing using command line tools
- Rapid identification of events of interest

SEC503.3 : Signature Base Detection

- Scapy
- Packet crafting and analysis using Scapy
- Writing a packet(s) to the network or a pcap file
- Reading a packet(s) from the network or from a pcap file
- Practical Scapy uses for network analysis and network defenders
- Advanced Wireshark
- Exporting web objects
- Extracting arbitrary application content
- Wireshark investigation of an incident
- Practical Wireshark uses for analyzing SMB protocol activity
- Tshark
- Detection Methods for Application Protocols
- Pattern matching, protocol decode, and anomaly detection challenges
- DNS
- DNS architecture and function
- Caching
- DNSSEC
- Malicious DNS, including cache poisoning
- Microsoft Protocols
- SMB/CIFS

- MSRPC
- Detection challenges
- Practical Wireshark application
- Modern HTTP and TLS
- Protocol format
- Why and how this protocol is evolving
- Detection challenges
- SMTP
- Protocol format
- STARTTLS
- Sample of attacks
- Detection challenges
- IDS/IPS Evasion Theory
- Theory and implications of evasions at different protocol layers
- Sampling of evasions
- Necessity for target-based detection
- Identifying Traffic of Interest
- Finding anomalous application data within large packet repositories
- Extraction of relevant records
- Application research and analysis
- Hands-on exercises after each major topic that offer students the opportunity to reinforce what they just learned.

SEC503.4 : Anomalies and Behaviors

- Network Architecture
- Instrumenting the network for traffic collection
- IDS/IPS deployment strategies
- Hardware to capture traffic
- Introduction to IDS/IPS Analysis
- Function of an IDS
- The analyst's role in detection
- Flow process for Snort and Bro
- Similarities and differences between Snort and Bro
- Snort
- Introduction to Snort
- Running Snort
- Writing Snort rules
- Solutions for dealing with false negatives and positives
- Tips for writing efficient rules
- Zeek
- Introduction to Zeek
- Zeek Operational modes
- Zeek output logs and how to use them
- Practical threat analysis
- Zeek scripting

- Using Zeek to monitor and correlate related behaviors
- Hands-on exercises, one after each major topic, offer students the opportunity to reinforce what they just learned.

SEC503.5 : Modern and Future Monitoring : Forensics , Analytics , and Machine Learning

- Introduction to Network Forensics Analysis
- Theory of network forensics analysis
- Phases of exploitation
- Data-driven analysis vs. Alert-driven analysis
- Hypothesis-driven visualization
- Using Network Flow Records
- NetFlow and IPFIX metadata analysis
- Using SiLK to find events of interest
- Identification of lateral movement via NetFlow data
- Examining Command and Control Traffic
- Introduction to command and control traffic
- TLS interception and analysis
- TLS profiling
- Covert DNS C2 channels: dnscat2 and Ionic
- Other covert tunneling, including The Onion Router (TOR)
- Analysis of Large pcaps
- The challenge of analyzing large pcaps
- Students analyze three separate incident scenarios.

SEC505: Securing Windows and PowerShell Automation

SEC505.1 : Learn Poweshell Scripting for Security

- **PowerShell Is Dangerous (and Fun)**
- PowerShell is like simplified C#
- Piping .NET and COM objects, not text
- The backbone of Windows and Azure automation
- Graphical admin tools wrapped around PowerShell
- Built-in remote script execution
- **Writing Your Own Scripts, Functions, and Modules**
- Passing arguments into your scripts
- Cmdlets, functions, and aliases in your profile script
- Flow control: if-then, do-while, foreach, switch
- The .NET Framework class library: a vast playground
- How to pipe data in/out of your scripts
- How to create your own module script
- **Up and Running Quickly with PowerShell**
- Capturing the output of commands
- Parsing text files and logs with regex patterns
- Mounting the registry as a drive

- Importing third-party modules and functions
- https://www.PowerShellGallery.com
- **Piping Objects Instead of Text**
- Classes, objects, properties, and methods
- An array of objects is like a table of SQL records
- Extracting just the properties you want
- Exporting objects to CSV, HTML, XML, and JSON files
- Filtering, sorting, and grouping objects (not text)

SEC505.2 : You Don't Know THE POWER

- **PowerShell Remoting**
- Remote command shells with PowerShell
- Smart card and YubiKey authentication
- Using SSL/TLS, SSH or IPsec to encrypt traffic
- Remote command execution in scheduled tasks
- File upload and download using the PowerShell Remoting protocol
- Graphical apps can use PowerShell remoting too
- **OpenSSH on Windows**
- Windows can be an SSH server? Yes!
- OpenSSH support is now built into Windows
- PowerShell Core integration with SSH
- Hardening SSH for Internet use
- Kerberos and public key authentication for SSH
- **PowerShell Just Enough Admin (JEA)**
- JEA is like *setuid root* on Linux
- Restricting PowerShell commands and arguments
- Verbose transcription logging of commands
- How to set up and configure JEA
- JEA for Privileged Access Workstations (PAWs)
- **PowerShell, Group Policy, and the Task Scheduler**
- Deploying PowerShell startup and logon scripts
- Group Policy scheduled tasks to run PowerShell scripts
- The Task Scheduler service and admin credentials
- WMI item-level targeting of PowerShell scripts

SEC505.3 : WMI and Active Directory Scripting

- **PowerShell Baselines with WMI**
- What is WMI and why do hackers abuse it so much?
- Remote command execution through WMI
- Using PowerShell to query WMI namespaces and classes
- WMI service authentication and traffic encryption
- Baseline auditing of remote systems
- Microsoft Windows Admin Center (WAC) web application
- WMI logging for hacker and malware visibility

- **PowerShell for Active Directory**
- Querying and managing Active Directory with PowerShell
- Enforcing desired Domain Admins group membership
- Disabling abandoned user accounts and resetting passwords
- Detecting password brute-force attacks
- Searching organizational units using filter criteria
- ADSI Edit and other helper tools for PowerShell
- Active Directory Administrative Center (ADAC)
- **Active Directory Permissions and Auditing**
- Active Directory objects have permissions
- Active Directory objects have auditing
- Limit what PowerShell scripts can do in Active Directory
- Log what PowerShell scripts are doing in Active Directory
- Delegate authority at the OU level instead
- Designing Active Directory for the inevitable breach

SEC505.4 : Hardening Network Services With Powershell

- **Server Hardening Automation for DevOps**
- Replacing Server Manager with PowerShell
- Adding and removing roles and features
- Remotely gathering an inventory of roles and features
- Why use Server Nano or Server Core?
- Running PowerShell automatically after service failure
- Service account identities, passwords, and risks
- Tools to reset service account passwords securely
- **Windows Firewall Scripting**
- PowerShell management of Windows Firewall rules
- Blocking malware outbound connections
- Role-based access control for listening ports
- Deep IPsec integration for user authentication
- Firewall logging to the event logs, not to text logs
- **Zero Trust with IPsec Port Authentication**
- PowerShell management of IPsec rules
- IPsec for blocking post-exploitation lateral movement
- Limiting access to ports based on global group membership
- IPsec-based encrypted VLANs
- IPsec is not just for VPNs!
- **PowerShell Visibility And Detection**
- PowerShell transcription logging
- WMI namespace auditing
- Windows Event Log audit policies
- Querying Windows Event Logs with PowerShell

SEC505.5 : Certificates and Multifactor Authentication

- **Certificate Authentication and TLS Encryption for PowerShell**
- Certificates for smart card authentication of PowerShell remoting
- Certificates for TLS encryption of PowerShell remoting
- Certificates to sign PowerShell scripts for AppLocker
- Certificates for TLS encryption of WMI queries with PowerShell
- Certificates to encrypt admin passwords (instead of LAPS)
- Certificates for web servers, domain controllers, and everything else
- **Install a Windows Certificate Server with PowerShell**
- PowerShell installation script for Public Key Infrastructure (PKI)
- Managing digital certificates with PowerShell
- Custom certificate templates in Active Directory
- Controlling certificate auto-enrollment
- Setting up an Online Certificate Status Protocol (OCSP) responder web farm
- Configuring Certificate Revocation List publication
- **Deploying Smart Cards, Smart Tokens, and TPM Virtual Smart Cards**
- The gold standard for multi-factor authentication is a smart card/token
- YubiKey smart tokens for logon, PowerShell remoting, and much more
- Trusted Platform Module (TPM) virtual smart cards
- Windows 11 requires a TPM
- Safely enroll tokens and cards on behalf of other users
- How to revoke compromised certificates
- PowerShell script to audit trusted root CAs
- PowerShell script to delete hacker certificates
- **Security Best Practices**
- Protect the private keys of your certificates from malware
- How to use PKI smart cards and smart tokens
- How to encrypt private keys on the hard drive
- Hardware Security Module (HSM) for CAs
- How to digitally sign PowerShell scripts
- SSL is dead, long live TLS
- TLS cipher suite optimization

SEC505.6 : PowerShell Security , Ransomware , and DevOps

- **PowerShell Ransomware**
- We will write a PowerShell ransomware script in a lab
- What can be done to combat ransomware?
- Just having backups is not enough
- **Anti-Exploitation Defenses for PowerShell**
- AppLocker for PowerShell
- Scripting AppLocker with PowerShell
- PowerShell execution policy
- PowerShell constrained language mode
- Anti-Malware Scan Interface (AMSI)
- Restricting network access to block pivoting
- Hashing scripts for change detection

- How to digitally sign our PowerShell scripts
- The Principle of (Endpoint) Least Privilege
- Prevent Domain Admin credential theft at all costs!
- Windows 10/11 Credential Guard
- User Account Control (UAC) instead of RUNAS.EXE
- **Capstone: DevOps PowerShell Orchestration Engine**
- Putting it all together with PowerShell
- How to write an all-in-one build script with OS hardening
- PowerShell for roles, features, networking, policies, etc.
- Security DevOps requires cross-platform automation
- We will all need to be "full stack engineers" soon