112-DAY SOC ANALYST ELITE TRAINING REGIME

Consolidated Master Table (Multi-Source Aggregation)

Sources: Standard Curriculum, MITRE ATT&CK/D3FEND Guides, Elite Corpus, & Master Regime.

Day	Objective / Focus	Tactical Tasks & Hourly Ops	Framework Mappings
Day 1	Configure high-fidelity logging on the Windows target.	**09:00 10:30:*Host Hardening: Disable unnecessary services (LLMNR, NetBIOS) to reduce noise. **09:00:*Analyzing Firewall & Web Server logs for Nmap/Nikto signatures. **09:00:*Configure Advanced Audit Policies (`secpol.msc`). Focus: Process Creation, Account Logon, Object Access. **09:00:*Configure Advanced Audit Policies (`secpol.msc`). Focus: Process, Account, Object. **10:30 12:30:*Deploying Windows 10/11 Evaluation. **11:00:***Lab Exercise:*Launch an `nmap -sV -A` scan against your range. **11:00:*Deploy [Sysmon](https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon) with [SwiftOnSecurity Config](https://github.com/SwiftOnSecurity/sysmon-config). **13:30 15:00:*Configuring Advanced Audit Policies (`secpol.msc`). **13:30:*Detecting "User-Agent" anomalies (e.g., `Nmap Scripting Engine`). **13:30:*Enable PowerShell Script Block Logging (Event ID 4104). **15:00 17:00:*Deploying [Sysmon](https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon) with [SwiftOnSecurity Config](https://github.com/SwiftOnSecurity/sysmon-config). **15:00:*Technical Drill: Map scanning IPs to known "Good" vs "Bad" infrastructure using CTI. **15:00:*Verification Drill: Check `Event Viewer` for ID 4688 and Sysmon ID 1. **Hourly Ops:** **Master Command:*`sysmon64.exe -i sysmonconfig-export.xml -accepteula` **Practical Drill:*Run `sysmon.exe -i config.xml`. Verify Event ID 1 (Process Create) in Event Viewer. 1. Open PowerShell as Admin and run: `sysmon64.exe -i sysmonconfig-export.xml -accepteula`. 2. GPO Path: `Computer Config > Admin Templates > Windows Components > Windows PowerShell > Turn on PowerShell Script Block	ATT&CK: - T1059 (Command and Scripting Interpreter) D3FEND: - D3-BI (Boot Integrity) D3FEND: - D3-NSM (Network Surveillance) D3FEND: - [D3-BI] (Boot Integrity)

		Logging`. Screenshot: Event ID 4688 with "Command Line" enabled. Screenshot: Sysmon Operational log populated.	
Day 2	Identify, distinguish, and document authentication attacks.	**09:00:*Incident Analysis: Extracting headers from "Phishing Emails" (EML files). **09:00:*Study Event ID 4624 (Success) vs 4625 (Failure). **11:00:***Lab Exercise:*Launch `hydra` against the Windows user `operator`. **11:00:***Lab Exercise:*Simulate a malicious attachment download (ISO/LNK/ZIP). **11:00:***Lab Exercise:*Use `hydra` on Kali to brute-force a local Windows user via SMB. **11:00:***Lab Exercise:*Use a Bash script on Ubuntu or Hydra on Kali to brute-force a local Windows user. **13:30:*Analyze Logon Types (Type 2: Local, Type 3: Network, Type 10: RDP). **13:30:*Tracking "Mark-of-the-Web" (MotW) bypass techniques. **15:00:*Triage: Identify the "Attacker Hostname" and "Source IP" from the logs. **15:00:*Triage: Identify the `src_ip` and `download_url` from Sysmon Event ID 3/15. **Hourly Ops:** **Operator Logic:*If LogonType == 3 and IpAddress != 127.0.0.1, suspect external pivot. 1. [Ultimate Windows Security 4625](https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625) 2. [Microsoft: Monitoring for Brute Force](https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625) hydra -l operator -p P@ssword123 smb://[Target_IP]	ATT&CK: - T1110 (Brute Force) D3FEND: - D3-LAP (Logon Authentication Analysis) D3FEND: - D3-MSI (Message Segment Inspection) D3FEND: - [D3-LAP] (Logon Authentication Analysis)
Day 3	Detect unauthorized account creation and privilege assignment.	**09:00:*Mastering PowerShell Script Block Logging (Event ID 4104). **09:00:*Monitor ID 4720 (User Created) and 4732 (Group Assigned). **11:00:***Lab Exercise:*Create a "hidden" user via CMD and add to Administrators. **11:00:***Lab Exercise:*Execute an obfuscated IEX (Invoke-Expression) script. **13:30:*De-obfuscation: Use CyberChef to reveal the true intent of the script. **13:30:*Hunt for Event ID 4672 (Special Privileges Assigned). **15:00:*Identify the `SeDebugPrivilege` assignment. **15:00:*Verification Drill: Hunt for "Hidden Window" and "-EncodedCommand" flags in Sysmon ID 1. **Hourly Ops:** 1. [SANS: Windows Logging for Security](https://www.sans.org/posters/windows-logging-and-it-compliance-cheat-sheet/) 2. [SpecterOps: Detecting PrivEsc](https://posts.specterops.io/host-based-detection-of-privilege-escalation-eb79498d5c4b)	ATT&CK: - T1548 (Abuse Elevation Control Mechanism) D3FEND: - D3-PSA (Process Spawn Analysis) D3FEND: - D3-SFL (Script File Logging) D3FEND: - [D3-PSA] (Process Spawn Analysis)
Day 4	Detect suspicious tool usage	### **WEEK 2: PERSISTENCE & AUTOSTART (T1547, T1037)** ### **WEEK 2: THE LINUX PERSISTENCE CHALLENGE** **09:00:*Analyzing Log4j and ProxyLogon style exploit signatures.	ATT&CK: - T1218 (System Binary Proxy

	(`certutil`, `bitsadmin`, `powershell -enc`).	**09:00:*Introduction to [LOLBAS Project](https://lolbas-project.github.io/). **11:00:***Lab Exercise:*Attack a local vulnerable web app (DVWA) via SQLi. **11:00:***Lab Exercise:*Execute a base64 encoded PowerShell script. **13:30:*Tracking "Web Shell" creation (Writing `.jsp`/`.php` to disk). **13:30:*Use Sysmon ID 1 to find the decoded command line. **15:00:*Hunt for `certutil -urlcache -f` network connection logs (Sysmon ID 3). **15:00:*Triage: Mapping the "Post-Exploitation" command to the Web Server process. **Hourly Ops:** Decoded PowerShell command captured in Sysmon logs.	Execution) D3FEND: - D3-SFL (Script File Logging) D3FEND: - D3-WAF (Web Application Filtering) D3FEND: - [D3-SFL] (Script File Logging)
Day 5	Detect log clearing and service interference.	**09:00:*Study Event ID 1102 (The Log was Cleared). **11:00:***Lab Exercise:*Use `wevtutil` to wipe the Security, System, and Sysmon logs. **13:30:*Identify the user/process that executed the log clear. **15:00:*Define a detection rule hypothesis for "Rapid Log Clearing". 1. [MITRE ATT&CK: Indicator Removal (T1070)](https://attack.mitre.org/techniques/T1070/) 2. [Elastic: Detecting Windows Log Clearing](https://www.elastic.co/blog/detecting-windows-log-clearing-with-suricata)	
Day 6	Reconstruct a multi-stage attack from raw logs.		
Day 7	WEEK 1 PRACTICAL ASSESSMENT	### **WEEK 2: THE LINUX PERSISTENCE CHALLENGE** A technical IR report including screenshots of every Event ID triggered in Day 6. Analysis of the "Attacker IP" and "Malicious URLs" found.	
Day 8	Establish granular file and process monitoring on Linux.	**09:00:*Deep dive into `ASEPs` (Auto-Start Extension Points). **09:00:*Overview of the Linux Audit Framework (`auditd`). **11:00:***Lab Exercise:*Configure rules to monitor `/etc/shadow` and `/etc/passwd`. **11:00:***Lab Exercise:*Configure rules to monitor `/etc/shadow` and `/etc/sudoers`. **11:00:***Lab Exercise:*Configure rules to monitor `/etc/shadow`, `/etc/passwd`, and `/etc/sudoers`. **11:00:***Lab Exercise:*Create a "Run Key" and a "New Service" for a reverse shell. **13:30:*Monitoring Registry changes with Sysmon ID 12/13. **13:30:*Real-time Log Streaming: Use `tail -f /var/log/auth.log` and `ausearch`. **13:30:*Real-time Log Streaming: Use `tail -f /var/log/auth.log`. **15:00:*Design a rule to detect "Execution of suspicious shells" (e.g., `nc`, `nmap`). **15:00:*Design a rule to detect "Execution of suspicious shells". **15:00:*Hunt: Find unauthorized services using the `sc query` and `Get-Service` commands. **Hourly Ops:** **Master Rule:*`-w /etc/sudoers -p wa -k sudoers_mod`	ATT&CK: - T1053 (Scheduled Task/Job) D3FEND: - D3-MPA (Model Process Activity) D3FEND: - D3-RIA (Registry Ingestion Analysis) D3FEND: - [D3-MPA] (Model Process Activity)

		1. [DigitalOcean: Linux Auditd Implementation](https://www.digitalocean.com/community/tutorials/how-to-write-custom-system-audit-rules-on-centos-7) 2. [RedHat: Configuring System Auditing](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/configuring-and-managing-networking-auditing_security-hardening)	
Day 9	Detect and analyze high-volume authentication failures.	## 📅 MONTH 2: THE FOOTHOLD & ESCALATION PHASE ### **WEEK 5: PRIVILEGE ESCALATION COMBAT (T1548, T1068)** **09:00:*Deep dive into `auth.log` format. Identify "Failed password" vs "Accepted password". **09:00:*Understanding `Winlogon` and `UserInit` registry values. **11:00:***Lab Exercise:*Inject a script into the `userinit.exe` sequence. **11:00:***Lab Exercise:*Launch a parallel SSH brute force from Kali using Hydra. **13:30:*Detecting abnormal "Process Parent" for shell executions. **13:30:*Scripting for SOC: Write a Python script to extract unique IPs from `auth.log`. **15:00:*Analysis: Distinguish between "Normal User Mistake" vs "Attack Pattern". **15:00:*Verification Drill: Hunt for modifications in `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`. CSV list of Top 10 Attacking IPs from the lab.	D3FEND: - D3-PSA (Process Spawn Analysis)
Day 10	Detect privilege escalation through binary abuse.	## 📅 MONTH 2: PRACTICAL SIEM OPERATIONS & ALERT ENGINEERING (Days 29-56) ### **WEEK 3: NETWORK TRAFFIC SURVEILLANCE** ### **WEEK 5: THE SPLUNK POWER USER MASTERCLASS** **09:00:*Understanding `sudo` logging and `visudo` auditing. **11:00:***Lab Exercise:*Execute a command from [GTFOBins](https://gtfobins.github.io/) (e.g., `sudo find . -exec /bin/sh \; -quit`). **13:30:*Identifying the "Audit ID" in `auth.log` to track the user pivot. **15:00:*Hunt for `sudoers` file tampering via Auditd. **Detection:*Analyze `auth.log` for the elevation token and the subsequent command execution as root. **Lab:*Execute `sudo find . -exec /bin/sh \; -quit`. **Lab:*`sudo find . -exec /bin/sh \; -quit`. **Triage:*Find the `AUDIT_USER` and `CMD` fields in `/var/log/audit/audit.log`. 1. [GTFOBins: Sudo Category](https://gtfobins.github.io/#+sudo) 2. [Sudo Security Documentation](https://www.sudo.ws/docs/security/)	ATT&CK: - T1548.003 (Sudo and Sudo Caching) D3FEND: - [D3-LAP] (Logon Authentication Analysis)
Day 11	Detect backdoors in system scheduling and services.	**09:00:*Auditing user crontabs (`/var/spool/cron/crontabs`). **11:00:***Lab Exercise:*Create a malicious Systemd service that spawns a reverse shell. **13:30:*Detect the service creation in `syslog` and `journalctl`. **15:00:*Hunting for "Hidden" cron files in `/etc/cron.d/`. 1. [Elastic: Linux Persistence Mechanisms](https://www.elastic.co/blog/linux-persistence-mechanisms) 2. [MITRE ATT&CK: Cron	

		(T1053.003)](https://attack.mitre.org/techniques/T1053/003/) for user in $(cut -f1 -d: /etc/passwd); do crontab -l -u $user; done	
Day 12	Analyze binary system logs for session metadata.	**09:00:*Understanding `wtmp` (logins) and `btmp` (failures). **11:00:***Lab Exercise:*Use `utmpdump` to convert binary logs to readable format. **13:30:*Map a specific "Time of Entry" to a "Time of Persistence Creation". **15:00:*Documenting the "Terminal (pts)" associated with suspicious root activity.	
Day 13	Perform a forensic reconstructio n of a complex Linux breach.		
Day 14	WEEK 2 PRACTICAL ASSESSMENT	### **WEEK 3: NETWORK INTRUSION DISCOVERY** A 5-page report documenting the "Dark-Root" scenario. Must include the `auditctl` rules used to detect the breach. Root Cause Analysis (RCA) and Mitigation steps.	
Day 15	Master `tcpdump` for efficient head-less packet capture.	**09:00:*Difference between Capture Filters (`-f`) and Display Filters. **11:00:***Lab Exercise:*Capture traffic on the target network while simulating a large file transfer. **13:30:*Analyzing Protocol Hierarchy in Wireshark. Identify "High Entropy" flows. **15:00:*Verification Drill: Extract "Cleartext Password" from a Telnet/FTP pcap. **Command:*`tcpdump -i eth0 -n -s 0 -w traffic.pcap` **Field Manual:*Use `tshark -r traffic.pcap -q -z conv,ip` to find the most active talkers. 1. [Wireshark: Analysis of Common Protocols](https://www.wireshark.org/docs/wsug_html_chunked/ChAnalyseMenuSection.html) 2. [SANS: TCPDUMP Cheat Sheet](https://www.sans.org/posters/tcpdump-cheat-sheet/)	ATT&CK: - T1041 (Exfiltration Over C2 Channel) D3FEND: - [D3-NSM] (Network Surveillance)
Day 16	Detect data exfiltration over the Domain Name System.	## 🗓️ MONTH 2: PRACTICAL SIEM OPERATIONS (Days 29-56) ### **WEEK 5: THE SPLUNK POWER USER** **09:00:*Understanding "Large TXT Records" and "Domain Entropy". **11:00:***Lab Exercise:*Use `dnscat2` or `iodine` to create a DNS tunnel. **13:30:*Analyze PCAPs for NXDOMAIN spikes and "Long Subdomains". **15:00:*Triage: Identify the "Tunneling Subdomain" used by the attacker. **Lab:*Run `dnscat2`. Detect via "High entropy subdomains" and "Unusual record types" in Zeek `dns.log`. 1. [Active Countermeasures: Hunting DNS Tunneling](https://www.activecountermeasures.com/blog/dns-analysis/) 2. [Cisco: DNS Security Best Practices](https://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html)	ATT&CK: - T1132 (Data Encoding) D3FEND: - [D3-DT] (DNS Tunneling Detection)
Day 17	Detect SQLi and XSS in raw HTTP	**09:00:*Analyzing HTTP GET/POST parameters for attack strings. **11:00:***Lab Exercise:*Attack a local "Juice Shop" or "DVWA" instance.	

	traffic.	**13:30:*Identifying "User-Agent" anomalies (e.g., `sqlmap`, `nmap`, `dirb`). **15:00:*Mapping 404/403 status codes to a "Directory Brute Force" attack.	
Day 18	Convert bulk PCAPs into high-level metadata logs.	**09:00:*Installing and processing traffic with Zeek. **11:00:***Lab Exercise:*Identify the "Top 5 Talkers" using `conn.log`. **13:30:*Analyzing `dns.log` for anomalous query frequencies. **15:00:*Lab: Track a single file download through `http.log` and `files.log`. 1. [Zeek: Getting Started Guide](https://docs.zeek.org/en/master/getting-started.html) 2. [Corelight: Zeek Training Resources](https://www.corelight.com/resources/zeek-training)	
Day 19	Write and tune IDS signatures for specific threats.	**09:00:*Understanding Suricata Header and Options syntax. **11:00:***Lab Exercise:*Write a rule to detect a specific C2 User-Agent. **13:30:*Testing the rule against a PCAP using `suricata -r`. **15:00:*Tuning: Decrease "False Positive" noise from a vulnerability scanner.	
Day 20	Use statistical analysis to find interval-based traffic.	**09:00:*Intro to "Beaconing" and "Jitter". **11:00:***Lab Exercise:*Run RITA against the Month 1 Week 3 traffic logs. **13:30:*Analyzing the "Score" based on frequency and size delta. **15:00:*Visualizing beacons using the RITA HTML report.	
Day 21	WEEK 3 PRACTICAL ASSESSMENT	### **WEEK 4: EDR & LIVE RESPONSE** A report documenting the discovery of a DNS Tunnel and a C2 beacon. Must include the `Zeek` log snippets as evidence.	
Day 22	Deploy a centralized detection engine and manage endpoints.	**09:00:*Wazuh Architecture: Manager, Indexer, and Dashboard. **11:00:***Lab Exercise:*Install the Wazuh Manager on the SIEM server VM. **13:30:*Fleet Deployment: Deploy agents to your Windows and Linux VMs. **15:00:*Verification Drill: Confirm agents are "Active" in the Wazuh UI. 1. [Wazuh Quickstart Guide](https://documentation.wazuh.com/current/quickstart.html) 2. [Wazuh: Managing Agents](https://documentation.wazuh.com/current/user-manual/agents/index.html)	
Day 23	Customizing detection logic for your environment.	**09:00:*Understanding Decoders and Rules (`/var/ossec/etc/rules`). **11:00:***Lab Exercise:*Write a rule to alert when a new user is added to the "Remote Desktop Users" group. **13:30:*Implementing Alert Throttling and Email/Slack notifications. **15:00:*Triage: Investigating a "High Severity" alert in the Wazuh Dashboard.	
Day 24	Perform live, host-based forensics at scale.	**09:00:*Deploying the Velociraptor Server and Client. **11:00:***Lab Exercise:*Run the `Windows.System.Pslist` artifact to find hidden processes. **13:30:*Forensic Hunt: Identify all systems containing a specific malicious file hash. **15:00:*Verification Drill: Use VQL (Velociraptor Query Language) to find persistence in the Registry. 1. [Velociraptor: VQL Reference](https://docs.velociraptor.app/vql/reference/)	

		2. [Velociraptor Artifact Exchange](https://docs.velociraptor.app/exchange/)	
Day 25	Detect PowerShell script execution and memory-only threats.	**09:00:*Tracking PowerShell parent-child relationships in Wazuh. **11:00:***Lab Exercise:*Simulate a Beacon or Reverse Shell using "PowerShell IEX". **13:30:*Searching for "EncodedCommand" in the EDR telemetry. **15:00:*Lab: Hunt for Living off the Land (LOLBAS) execution via Velociraptor.	
Day 26	Track unauthorized changes to critical system files.	**09:00:*Configuring Wazuh Syscheck for `/etc/` and `C:\Windows\System32`. **11:00:***Lab Exercise:*Modify a sensitive config file and analyze the "Who-What-When" log. **13:30:*Tuning FIM to ignore authorized system updates (Noise reduction). **15:00:*Audit: Reviewing the FIM summary for the past 24 hours.	
Day 27	Neutralize threats through tactical host isolation.	**09:00:*Intro to "Active Response" in Wazuh. **11:00:***Lab Exercise:*Configure an automatic "IP Block" when an SSH brute force is detected. **13:30:*Manual Isolation: Isolating a compromised Windows host from the network via EDR. **15:00:*Verification Drill: Confirming no traffic reaches the isolated host except to the SIEM.	
Day 28	MONTH 1 FINAL PRACTICAL ASSESSMENT	## 🗓️ MONTH 2: PRACTICAL SIEM OPS (Days 29-56) ### **WEEK 5: SPLUNK POWER SEARCH & DASHBOARDS** A comprehensive document outlining how you integrated Windows/Linux logs, Network traffic (Zeek/Suricata), and EDR (Wazuh) into a single SOC visibility strategy. Must include a flowchart of an alert's lifecycle from detection to remediation.	
Day 29	Detect techniques used to bypass User Account Control.	**09:00:*Splunk Architecture: UFs, Indexers, and Search Heads. **09:00:*The architecture of UAC and "Auto-Elevate" binaries. **11:00:***Lab Exercise:*Install Splunk Free on the SIEM Server VM. **11:00:***Lab Exercise:*Use `Fodhelper` to gain an Admin token. **13:30:*Data Onboarding: Config an "Upload" for the Windows/Linux logs collected in Month 1. **13:30:*Detecting abnormal process integrity levels in Sysmon. **15:00:*Basic Search: Using `index=*`, `sourcetype`, and `host`. **15:00:*Verification Drill: Hunt for registry modifications in `ms-settings`. **Tasks:*Install Splunk Distributed environment. Configure the UF on Windows to send logs via port 9997. **Tasks:*Install Splunk. Configure Universal Forwarder (UF) on Windows. **Verification:*`index=win_sysmon | stats count by host` 1. [Splunk: Getting Data In (GDI)](https://docs.splunk.com/Documentation/Splunk/latest/Data/WhatSplunkcanmonitor) 2. [Splunk Free Infrastructure Guide](https://www.splunk.com/en_us/resources/splunk-architecture.html)	D3FEND: - D3-PSA (Process Spawn Analysis) D3FEND: - [D3-AAM] (Asset Inventory)
Day 30	Detect kernel exploits and	## 🗓️ MONTH 3: INCIDENT RESPONSE & THREAT HUNTING (Days 57-84)	

	service vulnerabilities.	### **WEEK 7: CREDENTIAL ACCESS MASTERCLASS (T1003, T1555)** ### **WEEK 9: INCIDENT RESPONSE DYNAMICS (PICERL)** ### **WEEK 9: THE IR LIFE CYCLE (PICERL)** **09:00:*Analyzing Event ID 4673 (Sensitive Privilege Use). **09:00:*Mastering `stats`: `count`, `distinct_count (dc)`, `values`, `list`. **11:00:***Lab Exercise:*Calculate the "Peak Login Hour" for the Windows VM. **11:00:***Lab Exercise:*Run a "PrintNightmare" simulation. **13:30:*Tracking "Service Creation" with SYSTEM accounts. **13:30:*Using `chart`, `timechart`, and `top/rare`. **15:00:*Triage: Identify the "Vulnerable Binary" that was abused. **15:00:*Verification Drill: Sort the Top 5 processes by Sysmon Event Count. **Commands:*`stats`, `chart`, `timechart`, `top`, `rare`. **Commands:*`stats`, `chart`, `timechart`, `top`. **Lab:*Calculate the "Peak Login Hour" and "Top 5 Attacked Users". **SPL:*`index=windows EventCode=4625 | bin _time span=1h | stats count by _time | sort count`	
Day 31	Extracting and manipulating fields on-the-fly.	**09:00:*Introduction to `eval` functions: `if`, `case`, `match`, `lower`. **11:00:***Lab Exercise:*Use `rex` to extract a custom "Source IP" from a semi-structured log. **13:30:*Formatting timestamps with `strftime`. **15:00:*Triage: Creating a "Risk Score" field based on event severity.	
Day 32	Normalizing data for enterprise search.	**09:00:*What is CIM and why do we need it? **11:00:***Lab Exercise:*Install the "Splunk InfoSec App" or "CIM Validator". **13:30:*Normalizing the Month 1 Linux `auth.log` to the "Authentication" model. **15:00:*Triage: Search across both Windows and Linux data using a single CIM field (e.g., `user`). 1. [Splunk CIM Documentation](https://docs.splunk.com/Documentation/CIM/latest/User/Overview) 2. [Splunkbase: CIM Validator](https://splunkbase.splunk.com/app/2968/)	
Day 33	Build high-fidelity alerts that don't cause fatigue.	**09:00:*Alert Triggers: "Greater than X", "Relative to Average". **11:00:***Lab Exercise:*Build a "Brute Force" alert: 10 failed logins followed by 1 success within 5 mins. **13:30:*Configuring "Suppression/Throttling" to prevent alert storms. **15:00:*Verification Drill: Trigger the alert and check the "Triggered Alerts" dashboard.	
Day 34	Visualizing complex threats at a glance.	**09:00:*Intro to "Dashboard Studio" (Classic vs Studio). **11:00:***Lab Exercise:*Create a "Global Attack Map" using the `iplocation` command. **13:30:*Adding Dropdowns and Time Range Pickers for interactivity. **15:00:*Design: Build a "Malware Overview" panel showing Sysmon ID 1 outbreaks. 1. [Splunk: Dashboard Studio Examples](https://docs.splunk.com/Documentation/Splunk/latest/Dash Studio/StudioExamples) 2. [Splunk: Using iplocation](https://docs.splunk.com/Documentation/Splunk/latest/Sea	

		rchReference/Iplocation)	
Day 35	WEEK 5 PRACTICAL ASSESSMENT	### **WEEK 6: ADVANCED SIEM ENGINEERING & ES** A shared link or export of a dashboard containing: Account Lockout trends. Suspicious parent-child process tree. Top 10 blocked IPs.	
Day 36	Correlate disparate events across different data sources.	**09:00:*Mastering `join`, `map`, and `transaction`. **11:00:***Lab Exercise:*Correlate a Firewall "Accept" event with a Windows "Successful Login" (ID 4624). **13:30:*Performance Audit: Why `transaction` is expensive and how to use `stats` instead. **15:00:*Verification Drill: Build a flow showing "File Created" (Sysmon 11) -> "Network Connect" (Sysmon 3).	
Day 37	Optimize SIEM performance for high-volume logs.	**09:00:*Reusable Logic: Creating and calling `macros`. **11:00:***Lab Exercise:*Accelerate the "Authentication" Data Model. **13:30:*Using `tstats` to query accelerated data in milliseconds. **15:00:*Triage: Investigating a search that takes > 60 seconds and optimizing it.	
Day 38	Introduction to Splunk Enterprise Security (ES)	**09:00:*Navigating the "Incident Review" dashboard. **11:00:***Lab Exercise:*Triage a "Notable Event" and assign it to an "Owner". **13:30:*Understanding Risk-Based Alerting (RBA). **15:00:*Lab: Increase a user's "Risk Score" based on a detected PowerShell exploit. 1. [Splunk ES User Manual](https://docs.splunk.com/Documentation/ES/7.1.0/User/Overview) 2. [Splunk: Risk-Based Alerting Guide](https://www.splunk.com/en_us/blog/security/risk-based-alerting-a-new-era-of-detection.html)	
Day 39-41	Search Optimization & ES Dashboards		
Day 42	WEEK 6 PRACTICAL ASSESSMENT	### **WEEK 7: THE ELK STACK (Elasticsearch, Logstash, Kibana)** A step-by-step documentation of resolving 3 "Notable Events" in a simulated ES environment.	
Day 43	Detect the extraction of passwords from memory.	**09:00:*Elasticsearch Nodes, Shards, and Replicas. **09:00:*Understanding LSASS memory and `comsvcs.dll` dumps. **11:00:***Lab Exercise:*Install Elasticsearch and Kibana (8.x) using Docker or APT. **11:00:***Lab Exercise:*Simulate an LSASS dump using `rundll32`. **13:30:*Configuring `elasticsearch.yml` for TLS/SSL security. **13:30:*Detecting Process Access to LSASS: Sysmon ID 10. **15:00:*Verification Drill: Analyze "GrantedAccess" masks in your SIEM. **15:00:*Verification Drill: Ping the Elasticsearch API and check for "Green" status.	D3FEND: - D3-LPA (Lsass Process Analysis)
Day 44	Transforming raw logs into JSON-structured	## 🗓️ MONTH 3: THE MOVEMENT & COMMAND PHASE ### **WEEK 9: INTERNAL RECONNAISSANCE & DISCOVERY (T1087, T1082)** **09:00:*Analyzing file access to SQLite `Login Data` files.	

	events.	**09:00:*Input, Filter (Grok/Mutate), and Output stages. **11:00:***Lab Exercise:*Create a Logstash pipeline for custom CSV malware logs. **11:00:***Lab Exercise:*Use a Python script to extract passwords from the local profile. **13:30:*Detecting "Unusual Process Access" to AppData. **13:30:*Using GeoIP filters to map attacking IPs. **15:00:*Triage: Debugging a Logstash pipeline using `stdout { codec => rubydebug }`. **15:00:*Triage: Mapping the "Data Access" event to an signature-less execution. 1. [Elastic: Grok Filter Reference](https://www.elastic.co/guide/en/logstash/current/plugins-filters-grok.html) 2. [Elastic: Logstash Configuration Examples](https://www.elastic.co/guide/en/logstash/current/config-examples.html)	
Day 45	Building drag-and-drop analytics.	**09:00:*Mastering Kibana Query Language (KQL). **11:00:***Lab Exercise:*Build a "Network Throughput" chart using Kibana Lens. **13:30:*Creating TSVB (Time Series) charts for anomaly detection. **15:00:*Dashboard: Build an "Elastic Security Overview" page.	
Day 46	Proactive detection using the Elastic Security framework.	**09:00:*Navigating the "Hosts" and "Network" tabs. **11:00:***Lab Exercise:*Enable pre-built MITRE ATT&CK rules. **13:30:*Creating a custom detection rule for "Suspicious Cron Modification". **15:00:*Lab: Perform a "Timeline Investigation" for a malware event.	
Day 47-48	Fleet, Elastic Agent & Final ELK Polish		
Day 49	WEEK 7 PRACTICAL ASSESSMENT	### **WEEK 8: ALERT TUNING & THE SOC WORKFLOW** A PDF export of a Kibana Dashboard showing real-time host and network telemetry.	
Day 50	Effectively tune out authorized activity from high-fidelity alerts.	**09:00:*The "Signal-to-Noise" ratio concept. **11:00:***Lab Exercise:*Analyze a noisy "Suspicious PowerShell" alert and identify "Authorized Admin Tasks". **13:30:*Implementing "Exclusion Macros" in Splunk or "Suppression Filters" in Elastic. **15:00:*Verification Drill: Confirm the alert only triggers on non-whitelisted activity. 1. [SANS: Successful SIEM Tuning](https://www.sans.org/blog/successful-siem-and-log-management-strategies/) 2. [Splunk: Best practices for alert tuning](https://docs.splunk.com/Documentation/Splunk/latest/Alert/Bestpracticesforalerting)	
Day 51	Detect anomalies based on statistical deviations.	**09:00:*Calculating baselines using `stats avg` and `stdev`. **11:00:***Lab Exercise:*Build a search to find users who download > 3 standard deviations above their 7-day average. **13:30:*Understanding "High Cardinality" fields and their impact on performance.	

		**15:00:*Triage: Investigating a "Volume Anomaly" in network egress traffic.	
Day 52	Professionally documenting the "Why" and "How" of a detection.	**09:00:*Overview of the SANS Use Case Documentation framework. **11:00:***Lab Exercise:*Write a formal Use Case for "Ransomware-linked Domain Discovery". **13:30:*Mapping the Use Case to MITRE ATT&CK Tactic and Technique IDs. **15:00:*Verification Drill: Peer-review your Use Case against the "Field Manual". 1. [SANS: SIEM Use Case Guide](https://www.sans.org/white-papers/37735/)	
Day 53-54	Playbook Engineering & Intel Enrichment		
Day 55	Evaluate Splunk vs ELK for specific SOC mission profiles.	**09:00:*Feature-by-feature comparison (Search, Alerting, Visualization, Cost). **11:00:***Lab Exercise:*Deploy the SAME detection in both Splunk and ELK. **13:30:*Measuring "Time-to-Insight" for both platforms. **15:00:*Reflection: Choosing the right tool for a specific budget/team size.	
Day 56	MONTH 2 FINAL PRACTICAL ASSESSMENT	## 🗓️ MONTH 3: INCIDENT RESPONSE & THREAT HUNTING (Days 57-84) ### **WEEK 9: THE IR LIFE CYCLE & TRIAGE** 1 High-Fidelity Use Case Document. 1 Tuned Dashboard. A collection of 5 Custom SPL/KQL alerts.	
Day 57	Apply high-level frameworks to granular technical incidents.	## 🗓️ MONTH 4: CLOUD, AUTOMATION & CTI (Days 85-112) ### **WEEK 13: CLOUD SECURITY OPERATIONS (AWS/AZURE)** **09:00:*Comparing NIST SP 800-61 vs SANS PICERL. **09:00:*Distinguishing between Admin `net user` calls vs Malicious Discovery. **11:00:***Lab Exercise:*Take a raw incident (e.g., "Suspicious Admin Login") and map it to each phase of PICERL. **11:00:***Lab Exercise:*Use `AdFind` or `BloodHound` to map AD relationships. **13:30:*Detecting unauthorized LDAP queries in the Domain Controller logs. **13:30:*Understanding the "Criticality Matrix": Determining P1 (Critical) vs P4 (Low). **15:00:*Triage: Tracking the "Source Account" used for mass enumeration. **15:00:*Verification Drill: Fill out an "Incident Intake Form" based on a mock alert. **Lab:*Identification Scope a breach using "Pivot Analysis". **SANS PICERL:*Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned. **SPL:*`index=endpoint [search index=endpoint hash="BAD_HASH" | fields hostname] | stats count by dest_ip` 1. [NIST: Incident Handling Guide](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.	D3FEND: - D3-LAA (Local Account Analysis)

		800-61r2.pdf) 2. [SANS: Incident Handler's Handbook](https://www.sans.org/white-papers/33901/)	
Day 57-63	Scoping & Containment	## 🗓️ MONTH 4: CLOUD, AUTOMATION & CTI (Days 85-112) ### **WEEK 15: CTI & SIGMA ENGINEERING** **Containment:*Use Wazuh "Active Response" to block an IP. **Framework:*SANS PICERL. **Lab:*Given one bad process hash, find all systems in the SIEM that executed it.	
Day 58	Identifying "What else is broken?" during an active breach.	### **WEEK 10: LATERAL MOVEMENT COMBAT (T1021, T1570)** **09:00:*Monitoring for `systeminfo`, `hostname`, and `net config` usage. **09:00:*Pivot Analysis: Using common fields (IP, User, Host) to scope an attack. **11:00:***Lab Exercise:*Given a single bad process hash, find all other hosts in the SIEM that have seen that hash. **11:00:***Lab Exercise:*Launch a discovery script that collects OS, CPU, and Disk info. **13:30:*Detecting "Process Environment" enumeration. **13:30:*Identifying "Shared Infrastructure" (e.g., same C2 domain used across multiple hosts). **15:00:*Triage: Calculate the "Impacted User Count" and "Data Volume Leaked". **15:00:*Verification Drill: Hunt for the `whoami` command in Sysmon ID 1.	
Day 59	Execution of emergency host and user isolation.	**09:00:*Isolation types: Physical (Pulling cable) vs Logical (VLAN/EDR). **11:00:***Lab Exercise:*Disable a compromised user account via PowerShell and verify they are kicked from active sessions. **13:30:*Host Isolation: Applying a "Quarantine Policy" in your Wazuh or EDR lab. **15:00:*Verification Drill: Confirm the isolated host can only talk to the SIEM manager.	
Day 60-61	Eradication & Recovery Tactics		
Day 62	Transforming failure into defensive resilience.	**09:00:*Structure of a professional Post-Mortem. **11:00:***Lab Exercise:*Conduct a mock AAR for the "Echo Case" from Month 1. **13:30:*Identifying "Control Gaps" (Why didn't the SIEM catch this earlier?). **15:00:*Deliverable: Create a "Defensive Improvement Roadmap".	
Day 63	WEEK 9 PRACTICAL ASSESSMENT	### **WEEK 10: DIGITAL FORENSICS (DFIR) FOR SOC** Complete documentation of a P1 incident from "Intake" to "Containment". Must include the specific commands used for isolation.	
Day 64	Securely collect evidence without contaminating the "Crime Scene".	**09:00:*Analyzing Event ID 4624 (Logon Type 3 vs 10). **09:00:*The "Order of Volatility": Why Memory (RAM) comes first. **11:00:***Lab Exercise:*Move from System A to System B using `PsExec`. **11:00:***Lab Exercise:*Use `DumpIt` or `Magnet RAM Capture` to take a memory dump of your Windows VM. **13:30:*Calculating Hashes (SHA-256) for the image to ensure	D3FEND: - D3-LAP (Logon Authentication Analysis)

		integrity. **13:30:*Detecting "Service Installation" with remote source paths. **15:00:*Triage: Mapping the "Lateral Hop" across multiple hosts in the SIEM. **15:00:*Verification Drill: Verify the hash of your dump before and after moving it to the SIEM. 1. [SANS: Forensic Acquisition Cheat Sheet](https://www.sans.org/posters/forensic-acquisition-cheat-sheet/)	
Day 65	Identifying malicious injections and network connections in RAM.	### **WEEK 11: COMMAND & CONTROL (C2) INFRASTRUCTURES (T1071, T1090)** **09:00:*Auditing SMB `IPC$` share access and administrative shares (`C$`). **09:00:*Volatility 3 Architecture and Plugin system. **11:00:***Lab Exercise:*Transfer a binary from workstation to server via SMB. **11:00:***Lab Exercise:*Use `windows.pslist` and `windows.pstree` to find hidden processes. **13:30:*Detecting "Bitsadmin" and "Certutil" for internal downloads. **13:30:*Detecting Hollowed Processes: Using `windows.malfind` to find injected code. **15:00:*Verification Drill: Extract the "Command Line" of a suspicious process from memory. **15:00:*Verification Drill: Identify the "Originating Host" of the binary. 1. [Volatility Foundation: Plugin Guide](https://github.com/volatilityfoundation/volatility/wiki) 2. [SANS: Volatility Cheat Sheet](https://www.sans.org/posters/volatility-3-cheat-sheet/)	D3FEND: - D3-FMA (File Modification Analysis)
Day 66	Finding "Evidence of Execution" after a process has closed.	**09:00:*Deep dive into Prefetch (`.pf`) and Shimcache. **11:00:***Lab Exercise:*Use [Eric Zimmerman's PECmd](https://ericzimmerman.github.io/#!index.md) to parse Prefetch files. **13:30:*Mapping "First Run" and "Last Run" times for a malicious tool. **15:00:*Triage: Tracking `certutil.exe` usage through Prefetch forensics.	
Day 67	Recovering configuration, persistence, and recent file activity.	**09:00:*Understanding User Hives (`NTUSER.DAT`) vs System Hives. **11:00:***Lab Exercise:*Use `Registry Explorer` to find "RunKeys" and "UserAssist" artifacts. **13:30:*Tracking "Recent Docs" and "ShellBags" to find exfiltrated folder names. **15:00:*Verification Drill: Document the exact Registry Key used by a common piece of malware for persistence.	
Day 68	Analyzing the "Footprints" left on a Linux server.	**09:00:*Analyzing `.bash_history` (and detecting its deletion). **11:00:***Lab Exercise:*Recover deleted files from a Linux partition using `extundelete` or `fls`. **13:30:*Auditing Log File gaps: Identify missing entries in `syslog` or `journald`. **15:00:*Triage: Mapping a "Cron Job" creation to a "SSH Session" start time.	
Day 69	Unified forensic analysis using	**09:00:*Creating a "Case" in Autopsy. **11:00:***Lab Exercise:*Import a `.vmdk` or `.raw` image of your target machine.	

	an open-source GUI.	**13:30:*Running ingest modules: Keyword Search, Email Analysis, and Web History. **15:00:*Verification Drill: Generate a "Case Summary PDF" from Autopsy.	
Day 70	WEEK 10 PRACTICAL ASSESSMENT	### **WEEK 11: THREAT INTELLIGENCE & MITRE ATT&CK** A report containing evidence found in RAM (Volatility) and Disk (Autopsy) for a specific attack. Must include the "Chain of Custody" for the handled images.	
Day 71	Operationalize raw intelligence for the SOC floor.	## 🗓️ MONTH 4: THE IMPACT & INTELLIGENCE PHASE ### **WEEK 13: EXFILTRATION DYNAMICS (T1048, T1041)** **09:00:*Direction, Collection, Processing, Analysis, and Dissemination. **09:00:*Identifying "Fixed Interval" beacons through statistical analysis. **11:00:***Lab Exercise:*Setup a `Sliver` or `Empire` C2 beacon. **11:00:***Lab Exercise:*Use [AlienVault OTX](https://otx.alienvault.com/) to find indicators for a known ransomware group (e.g., LockBit). **13:30:*Analyzing "Jitter" and packet size deltas in Wireshark. **13:30:*Creating "Watchlists" in the SIEM based on downloaded IOCs (IPs/Hashes). **15:00:*Triage: Mapping reaching out to "New Domains" with high entropy. **15:00:*Verification Drill: Trigger an alert by simulating a connection to a "Known Bad" IP. 1. [CrowdStrike: What is Threat Intelligence?](https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/) 2. [SANS: Cyber Threat Intelligence Cheat Sheet](https://www.sans.org/posters/cyber-threat-intelligence-cheat-sheet/)	D3FEND: - D3-HBA (HTTP Beacon Analysis)
Day 72	Visualize your detection coverage against attacker techniques.	**09:00:*Navigating the [ATT&CK Navigator](https://mitre-attack.github.io/attack-navigator/). **11:00:***Lab Exercise:*Create a Layer that highlights all techniques covered by your Month 1 & 2 SIEM rules. **13:30:*Identifying "Blind Spots": Which tactics (e.g., Exfiltration) are you not monitoring? **15:00:*Deliverable: An exported JSON layer showing current SOC visibility.	
Day 73	Centralizing and sharing intelligence data.	**09:00:*Introduction to MISP (Malware Information Sharing Platform). **11:00:***Lab Exercise:*Import a "Threat Bulletin" into your lab environment. **13:30:*Scripting: Use a Python script to pull IOCs from a MISP API into a SIEM lookup table. **15:00:*Triage: Compare recent `syslog` entries against the MISP "Technical Indicators".	
Day 74-76	Actor Dossiers & Rule Mapping		
Day 77	WEEK 11 PRACTICAL ASSESSMENT	### **WEEK 12: PROACTIVE THREAT HUNTING LABS** A report containing a MITRE Navigator layer and a dossier for one active threat group.	
Day	Search for	**09:00:*Hypothesis Generation (e.g., "Attackers use WMI for	

78	threats that bypass automated alerts.	persistence"). **11:00:***Lab Exercise:*Search your environment for anomalous WMI subscriptions or Scheduled Tasks. **13:30:*Filtering "Known Good" system tasks to find the outlier. **15:00:*Verification Drill: Document the SPL/KQL query used for the hunt. 1. [Microsoft: Threat Hunting in the SOC](https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/threat-hunting-scenarios) 2. [SANS: Threat Hunting Cheat Sheet](https://www.sans.org/posters/threat-hunting-cheat-sheet/)	
Day 79	Detect attackers moving across your network using native tools.	**09:00:*Analyzing Event ID 4624 (Type 3) and `PsExec` activity. **11:00:***Lab Exercise:*Use `PsExec` to move from System A to System B in your lab. **13:30:*Hunt for "Service Installation" events (ID 7045) on the destination host. **15:00:*Triage: Mapping the "Source Workstation" to the "Target User".	
Day 80	Exfiltration & C2 Hunting		
Day 84	MONTH 3 FINAL PRACTICAL ASSESSMENT	## 🗓️ MONTH 4: CLOUD SOC, AUTOMATION & CAREER (Days 85-112) ### **WEEK 13: CLOUD SOC (AWS & AZURE)** A detailed log of 3 successfully executed hunts, including the hypothesis, data searched, and findings.	
Day 85	- Detect public access and data theft in cloud storage.	## 🗓️ PHASE 6: MITRE D3FEND ENGINEERING REGIME (Days 141-160) ### **WEEK 15: CTI ENGINEERING WITH MITRE (STIX/JSON)** ### **WEEK 21: ONTOLOGY & SEMANTIC MAPPING** **09:00:*AWS CloudTrail log structure. **09:00:*Understanding "Large Outbound Spikes" in flow data. **09:00:*Understanding "Management" vs "Data" events. **11:00:***Lab Exercise:*Use `DNSCat2` to exfiltrate a 1MB file. **11:00:***Lab Exercise:*Use the AWS CLI or Console to create a Trail and store logs in S3. **11:00:***Lab:*Simulate an S3 bucket leakage via configuration mistake. **13:30:*Detect `PutBucketPublicAccessBlock` deletion in logs. **13:30:*Detecting "High Byte Count" in ICMP Echo requests. **13:30:*Search for "IAM Policy Modifications" in CloudTrail using `athena` or SIEM. **15:00:*Triage: Identifying the "Destination IP" and "Data Volume". **15:00:*Verification Drill: Identify which API call caused a specific "S3 Bucket Public" event. **Hourly Ops:** 1. [AWS: CloudTrail User Guide](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html) 2. [SANS: AWS Security Persistence](https://www.sans.org/blog/how-to-hunt-for-persistence-in-aws/)	D3FEND: - D3-NSM (Network Surveillance) D3FEND: - [D3-AAM] (Asset Inventory)
Day 86	Establishing visibility in the Microsoft	**09:00:*Navigating "Monitor", "Log Analytics", and "Microsoft Sentinel". **11:00:***Lab Exercise:*Configure the "Activity Log" to stream events	

	Cloud.	to a workspace. **13:30:*Hunt for "Virtual Machine Creation" and "Admin Role Assignment" events. **15:00:*Triage: Investigating a suspicious login to the Azure Portal from a new Geo-Location.	
Day 87	Identifying "Privilege Escalation" in the cloud.	**09:00:*Understanding "Cross-Account" access and "Role Assumption". **11:00:***Lab Exercise:*Simulate an attacker creating a new Access Key for a compromised user. **13:30:*Detecting "Credential Stuffing" attempts against Azure AD (Entra ID). **15:00:*Verification Drill: Map an IAM abuse event to the MITRE ATT&CK Cloud Matrix.	
Day 88-90	Storage Exposure & Container Logs		
Day 91	WEEK 13 PRACTICAL ASSESSMENT	### **WEEK 14: SOC AUTOMATION (PYTHON & SOAR)** A technical doc showing an AWS/Azure monitoring plan, including 3 high-fidelity cloud alerts.	
Day 92	Writing scripts to parse and filter security data.	**09:00:*Python for String manipulation and Log parsing. **11:00:***Lab Exercise:*Write a Python script to extract all URLs from a suspicious `.json` log file. **13:30:*Using the `requests` library to talk to external APIs. **15:00:*Verification Drill: Generate a "Summary Report" of failed logins using Python.	
Day 93	Saving analyst time through auto-lookup of bad IPs/Hashes.	**09:00:*Understanding API Keys and Rate Limits. **11:00:***Lab Exercise:*Build a script that takes a list of IPs and checks them against [VirusTotal API](https://developers.virustotal.com/). **13:30:*Outputting the results to a structured CSV file. **15:00:*Verification Drill: Auto-flag "High Confidence" malicious IPs in your SIEM. 1. [Python: Official Requests Library](https://requests.readthedocs.io/en/latest/) 2. [VirusTotal: Python SDK](https://github.com/VirusTotal/vt-py)	
Day 94	Automating the "Incident Response" workflow.	**09:00:*What is SOAR (Security Orchestration, Automation, and Response)? **11:00:***Lab Exercise:*Design a "Visual Playbook" for an "Account Lockout" event. **13:30:*Steps: Enrichment -> Triage -> User Confirmation -> Auto-Unlock (or Reset). **15:00:*Triage: When to NOT automate a response (The "Human-in-the-loop").	
Day 95-97	API Integration & ChatOps		
Day 98	WEEK 14 PRACTICAL ASSESSMENT	### **WEEK 15: MALWARE ANALYSIS FOR THE SOC** A GitHub repo (or local folder) containing 3 functioning Python scripts: Enrichment, Reporting, and Isolation.	
Day 99	Identifying malware characteristics without	**09:00:*Safe handling of malware in a disconnected "Sandbox". **09:00:*Understanding STIX 2.1 JSON structure. **11:00:***Lab Exercise:*Use [Pestudio](https://www.winitor.com/) to find suspicious strings and imports in a sample.	

	executing the code.	**11:00:***Lab Exercise:*Write a Python script to extract all IPs associated with **APT29*from the `cti` folder. **13:30:*Calculating Hashes and checking against Malware Repositories. **13:30:*Mapping the extracted IOCs to your SIEM lookup tables. **15:00:*Verification Drill: Identify if the sample is "Packed" or "Obfuscated". **15:00:*Verification Drill: Trigger an alert based on an IOC from a real-world APT report. **Tasks:*Build a script to convert MITRE CTI JSON (STIX) into SIEM lookups. **Tool:*`MITRE_CTI_Scraper.py`. 1. [Practical Malware Analysis: Essentials](https://nostarch.com/malware) 2. [SANS: Malware Analysis Cheat Sheet](https://www.sans.org/posters/malware-analysis-cheat-sheet/)	
Day 100	Building internal documentation from the `attack-website` repo.	### **LAB 16: DNS TUNNELING DISCOVERY** ### **LAB 1: THE WINDOWS TELEMETRY GRID** ### **WEEK 16: THE GRAND CAPSTONE FULL CHAIN APT EMULATION** **09:00:*Navigating the local `attack-website` structure. **09:00:*Setting up `Procmon` and `Wireshark` for behavioral capture. **11:00:***Lab Exercise:*Create a "Technique Cheat Sheet" for your SOC team. **11:00:***Lab Exercise:*Execute the malware and track its File, Registry, and Network changes. **13:30:*Identifying the "C2 Callback" IP and port. **13:30:*Mapping "Mitigations" to "Detection Capabilities". **15:00:*Final Reflection: Scoring your SOC visibility using the [ATT&CK Navigator](https://mitre-attack.github.io/attack-navigator/). **15:00:*Triage: Mapping the observed behavior to the MITRE ATT&CK techniques. **Lab:*Write a Sigma rule to detect `whoami /priv` and compile for Splunk. **Master Rule:** 2. **Steps:*Install Sysmon, Configure Event Log rotation to 512MB, Deploy SwiftOnSecurity XML. 2. **Steps:*Launch `dnscat2`. Capture traffic. Analyze `TXT` record frequency. 3. **Verification:*Generate a 'calc.exe' launch; confirm in Sysmon ID 1.	
Day 101-103	Automated Analysis & Extraction		
Day 105	WEEK 15 PRACTICAL ASSESSMENT	### **WEEK 16: CAPSTONE & CAREER READINESS** A 2-page report detailing the Static and Dynamic findings for a provided malware sample.	
Day 106-110	THE FINAL CAPSTONE SIMULATION		
Day 106-112	Scenario: "The Lazarus Shadow"	## 🗓️ PHASE 6: MITRE D3FEND ENGINEERING REGIME (Days 141-160) ### **WEEK 21: ONTOLOGY & SEMANTIC MAPPING** **D3FEND Challenge:*Map every detection to a D3FEND	

		countermeasure. **Deliverable:***"The MITRE Master Portfolio"*(PDF technical showcase). **Success Criteria:*Zero false negatives on critical tactic transitions. A full 7-day emulation of an APT kill-chain. Complete 7-day emulation of a full APT kill-chain. Final Deliverable: **"The MITRE Master Portfolio"**. Must Detect: Phish -> Persistence -> PrivEsc -> Lateral Movement -> Exfil.	
Day 111	Practical, high-pressure interview preparation.	**09:00:*Answering "The Technical Trio": 3-way handshake, OSI model, and the Incident IR steps. **11:00:*The "Scenario Question": How would you handle a Ransomware alert at 4 AM? **13:30:*Reviewing "Red Flags" in your personal portfolio. **15:00:*Mock Interview session with a peer or mentor.	
Day 112	CURRICULUM GRADUATION & PORTFOLIO EXPORT	**CELEBRATE:*You have completed 112 days of intensive, hands-on training. A unified PDF/DOCX of your **"SOC Analyst Practical Portfolio"**, containing all 16 weekly assessments.	
Day 141	- Navigate the D3FEND ontology using SPARQL and Python.	### **LAB 16: DNS TUNNELING DISCOVERY** ### **LAB 1: THE WINDOWS TELEMETRY SENSORY GRID** **09:00:*Deep dive into `d3fend-protege.ttl`. Understanding Classes vs Restrictions. **11:00:***Lab Exercise:*Run a SPARQL query to find all countermeasures for "Process Execution". **13:30:*Semantic Linkage: How `D3-PSA` links to `T1053` via the `executes` property. **15:00:*Engineering Drill: Build a local JSON map of DIDs to TIDs. **Lab:*Querying `d3fend-protege.ttl` for all countermeasures related to "Process Execution". 2. **Steps:** 3. **Detection Rule:*`if count(dns_qry_name > 100) > 20 in 1min: TRIGGER ALERT`. 3. **Verification:*Generate a 'calc.exe' launch and confirm it appears in Sysmon ID 1. Capture traffic on the bridge. Configure Event Log rotation to 512MB. Deploy "SwiftOnSecurity" XML. Install Sysmon. Launch `dnscat2` on the victim. Use `tshark` to analyze the frequency of `TXT` records.	
Day 142	Map offensive artifacts to defensive functions.	### **WEEK 22: DECEPTIVE ENGINEERING & TACTICAL LABS** **09:00:*Analyzing Digital Artifacts: File, Process, Hive, Network. **11:00:***Lab Exercise:*Correlate "Sysmon ID 1" fields to D3FEND `ProcessSpawnAnalysis` attributes. **13:30:*Identifying Gaps: Which ATT&CK techniques in your lab have NO D3FEND countermeasure? **15:00:*Reporting: Create a "Defensive Coverage Gap Analysis" for your range.	
Day 148	Engineer "Canary" tokens and	**09:00:*Architecture of Decoy Files and Honey-Users. **11:00:***Lab Exercise:*Create a "Honey-Registry-Key" that alerts when accessed (Sysmon ID 13).	

	Honeypots.	**13:30:*Honey-Credentials: Injecting "Fake" tokens into LSASS for retrieval detection. **15:00:*Triage: Designing a "P0" High-Fidelity alert for Deceptive Artifact access.	
Day 149	Operationalizing D3FEND "Harden" and "Isolate" tactics.	**09:00:*Application Path Hardening (**D3-APH**) and Boot Integrity (**D3-BI**). **11:00:***Lab Exercise:*Configure "Process Execution Restrictions" using AppLocker (D3-PER). **13:30:*Host-Based Isolation: Implementing micro-segmentation for high-risk workstations. **15:00:*Final Reflection: Scaling D3FEND across an Enterprise SOC.	