🛡️ THE SOC ELITE: 112-DAY TACTICAL TRAINING CORPUS

Version 4.0 - Full Master Integration The Definitive Guide for SOC Analysts, Engineers, and Hunters

---

📋 PREFACE: THE ARCHITECTURE OF DEFENSE

In the modern landscape, defensive capability is no longer measured by the tools you buy, but by the logic you engineer. This corpus provides the technical blueprints to transition from a passive observer to a tactical defender.

The Dual-Framework Philosophy

This program is unique in its dual-alignment:

1. **MITRE ATT&CK® (The Offense):** We map every day to specific adversary techniques to understand the "Why" and "How" of the breach.
2. **MITRE D3FEND™ (The Defense):** We map every day to a specific defensive countermeasure to understand the "What" of the response.

🔧 THE SOC RANGE: CORE LAB INFRASTRUCTURE

Deploying the lab is the first test of an engineer's capability.

Infrastructure Map:

Node	OS	Primary Function
Sentinel-01	Windows 10/11	Target Host, Sysmon Telemetry Generator.
Nexus-Primary	Ubuntu 22.04 LTS	Log Aggregator, SIEM (Splunk/ELK), EDR Manager (Wazuh).
Bridge-Router	vyos/pfsense	Network Monitoring (Zeek/Suricata), Traffic Capture.
Attacker-Box	Kali Linux	Attack Simulation (Metasploit, Hydra, BloodHound).

🗓️ MONTH 1: PRACTICAL LOG MASTERY & FORENSICS (Days 1-28)

Objective: Mastering the Source of Truth - Telemetry.

WEEK 1: THE WINDOWS DEFENSIVE FRONT

Focus: Internalizing Windows Host-Based Telemetry.

Day 1: Telemetry Sensor Deployment (T1595/T1059)

- **ATT&CK Mapping:** T1059 (Command and Scripting Interpreter)
- **D3FEND Mapping: [D3-BI]** (Boot Integrity)
- **Hourly Ops:**
  - **09:00:** Configure Advanced Audit Policies (`secpol.msc`). Focus: Process Creation, Account Logon, Object Access.
  - **11:00:** Deploy Sysmon with SwiftOnSecurity Config.

    - **13:30:** Enable PowerShell Script Block Logging (Event ID 4104).
    - **15:00:** Verification Drill: Check `Event Viewer` for ID 4688 and Sysmon ID 1.
- **Master Command:** `sysmon64.exe -i sysmonconfig-export.xml -accepteula`

Day 2: The Brute Force Challenge (T1110)

- **ATT&CK Mapping:** T1110 (Brute Force)
- **D3FEND Mapping: [D3-LAP]** (Logon Authentication Analysis)
- **Hourly Ops:**
    - **09:00:** Study Event ID 4624 (Success) vs 4625 (Failure).
    - **11:00: Lab Exercise:** Launch `hydra` against the Windows user `operator`.
    - **13:30:** Analyze Logon Types (Type 2: Local, Type 3: Network, Type 10: RDP).
    - **15:00:** Triage: Identify the "Attacker Hostname" and "Source IP" from the logs.
- **Operator Logic:** If LogonType == 3 and IpAddress != 127.0.0.1, suspect external pivot.

Day 3: Privilege Escalation Lab (T1548/T1068)

- **ATT&CK Mapping:** T1548 (Abuse Elevation Control Mechanism)
- **D3FEND Mapping: [D3-PSA]** (Process Spawn Analysis)
- **Hourly Ops:**
    - **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.
    - **13:30:** Hunt for Event ID 4672 (Special Privileges Assigned).
    - **15:00:** Identify the `SeDebugPrivilege` assignment.

Day 4: Living Off The Land (LOLBAS) Hunt (T1218)

- **ATT&CK Mapping:** T1218 (System Binary Proxy Execution)
- **D3FEND Mapping: [D3-SFL]** (Script File Logging)
- **Hourly Ops:**
    - **09:00:** Introduction to LOLBAS Project.
    - **11:00: Lab Exercise:** Execute a base64 encoded PowerShell script.
    - **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).

WEEK 2: THE LINUX PERSISTENCE CHALLENGE

Day 8: Auditd & The Rules of Strategic Monitoring (T1053)

- **ATT&CK:** T1053 (Scheduled Task/Job)
- **D3FEND: [D3-MPA]** (Model Process Activity)
- **Hourly Ops:**
    - **09:00:** Overview of the Linux Audit Framework (`auditd`).
    - **11:00: Lab Exercise:** Configure rules to monitor `/etc/shadow` and `/etc/sudoers`.
    - **13:30:** Real-time Log Streaming: Use `tail -f /var/log/auth.log` .
    - **15:00:** Design a rule to detect "Execution of suspicious shells".
- **Master Rule:** `-w /etc/sudoers -p wa -k sudoers_mod`

Day 10: The Sudo Ninja Lab (T1548.003)

- **ATT&CK:** T1548.003 (Sudo and Sudo Caching)
- **D3FEND: [D3-LAP]** (Logon Authentication Analysis)
- **Lab:** Execute `sudo find . -exec /bin/sh \; -quit` .
- **Triage:** Find the `AUDIT_USER` and `CMD` fields in `/var/log/audit/audit.log` .

WEEK 3: NETWORK TRAFFIC SURVEILLANCE

Day 15: Deep Packet Capture (T1041)

- **ATT&CK:** T1041 (Exfiltration Over C2 Channel)
- **D3FEND: [D3-NSM]** (Network Surveillance)
- **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.

Day 16: DNS Tunneling Discovery (T1132)

- **ATT&CK:** T1132 (Data Encoding)
- **D3FEND: [D3-DT]** (DNS Tunneling Detection)
- **Lab:** Run `dnscat2`. Detect via "High entropy subdomains" and "Unusual record types" in Zeek `dns.log`.

🗓️ MONTH 2: PRACTICAL SIEM OPERATIONS (Days 29-56)

Objective: Mastering the Central Nervous System of the SOC.

WEEK 5: THE SPLUNK POWER USER

Day 29: Splunk Ingestion (T1059)

- **Tasks:** Install Splunk. Configure Universal Forwarder (UF) on Windows.
- **Verification:** `index=win_sysmon | stats count by host`

Day 30: SPL Mastery - Transformation

- **Objective:** Summarizing telemetry for high-level triage.
- **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`

🗓️ MONTH 3: INCIDENT RESPONSE & THREAT HUNTING (Days 57-84)

Objective: Winning the War on the Network.

WEEK 9: THE IR LIFE CYCLE (PICERL)

Day 57-63: Scoping & Containment

- **Framework:** SANS PICERL.
- **Lab:** Given one bad process hash, find all systems in the SIEM that executed it.
- **Containment:** Use Wazuh "Active Response" to block an IP.

🗓️ MONTH 4: CLOUD, AUTOMATION & CTI (Days 85-112)

Objective: Engineering for the Future.

WEEK 15: CTI & SIGMA ENGINEERING

Day 99: Python for Threat Intel

- **Tasks:** Build a script to convert MITRE CTI JSON (STIX) into SIEM lookups.

- **Tool:** `MITRE_CTI_Scraper.py`.

Day 100: Sigma Rule Mastery

- **Lab:** Write a Sigma rule to detect `whoami /priv` and compile for Splunk.
- **Master Rule:**

```
title: Suspicious Privilege Discovery
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 4688
        CommandLine|contains: '/priv'
    condition: selection
```

📖 THE ANALYST'S BIBLE: COMPLETE COMMAND MASTER REFERENCE

1. WINDOWS EXECUTION & TRIAGE

Task	Command
List Process Owners	`Get-WmiObject -Query "Select * from Win32_Process"
Check Active Connections	`netstat -ano
Parse Prefetch Files	`.\PECmd.exe -d "C:\Windows\Prefetch" --csv "C:\Triage\Prefetch"`
Search Event Logs (PS)	`Get-WinEvent -FilterHashtable @{LogName='Security';ID=4624} -MaxEvents 50`

2. LINUX HARDENING & INVESTIGATION

Task	Command
Check Active Connections	`ss -atpu`
Monitor Audit Logs	`ausearch -m USER_LOGIN -sv no`
Find SUID Binaries	`find / -perm -4000 -type f 2>/dev/null`

🧪 FULL LAB MANUAL: 112+ TACTICAL DRILLS

LAB 1: THE WINDOWS TELEMETRY GRID

1. **Objective:** Deploy a hardened sensor grid.
2. **Steps:** Install Sysmon, Configure Event Log rotation to 512MB, Deploy SwiftOnSecurity XML.
3. **Verification:** Generate a 'calc.exe' launch; confirm in Sysmon ID 1.

LAB 16: DNS TUNNELING DISCOVERY

1. **Objective:** Detect data leaving via Port 53.
2. **Steps:** Launch `dnscat2`. Capture traffic. Analyze `TXT` record frequency.

🛡️ D3FEND DEFENSIVE MATRIX

D3FEND Tactic	Key Countermeasure (DID)	Description
Model	**D3-AAM**	Asset Inventory and Model Process Activity.
Harden	**D3-APH**	Application Path Hardening (AppLocker).
Detect	**D3-PSA**	Process Spawn Analysis (Sysmon 1).
Isolate	**D3-HBI**	Host-based Isolation (EDR).
Deceive	**D3-DA**	Deceptive Artifact (Honey-tokens).

📜 GRADUATION: THE GRAND CAPSTONE

Day 106-112: Scenario: "The Lazarus Shadow" A full 7-day emulation of an APT kill-chain. Reveal Phish -> Persistence -> Lateral -> Exfil.

End of Corpus - (c) 2025 SOC Elite