HORIZONSHIELD

Securing Your Digital Future, Today.

BLUE TEAM SERIES · BOOK 07 OF 16

Threat Hunting & SOC Operations

Building World-Class Detection Capability

From SOC maturity models to advanced threat hunting using the MITRE ATT&CK framework. Covers SIEM architecture, detection engineering, hunt hypothesis development, and SOC KPIs — with 50+ hunt hypotheses and 100+ SIEM queries.

MITRE TACTICS	HUNT HYPOTHESES	SIEM QUERIES	LEVEL
14	50+	100+	Advanced

Contents

THREAT HUNTING & SOC OPERATIONS 2026

CHAPTER 01

SOC Maturity Model

Understanding where your SOC sits on the maturity curve determines the right investments to make next.

MATURITY PEOPLE PROCESS TECHNOLOGY

SOC Maturity Assessment

Level	Capability	Typical Profile	Key Gap to Next Level	Investment Priority
L1: Reactive	Alert triage, basic incident handling, AV response	SMBs with MSSP or basic SIEM. Security generalists.	Reduce MTTR. Improve triage quality. Document playbooks.	Playbook documentation, SIEM tuning, analyst training
L2: Proactive	Threat intel integration, custom detections, basic hunting	Mid-market with in-house security team. Dedicated analysts.	Detection engineering capability. Structured hunt programme.	SIEM engineering skills, threat intel platform, hunt workflow
L3: Predictive	SOAR automation, adversary emulation, purple teaming	Mature enterprise SOC. Dedicated detection engineers.	Full kill chain visibility. ML/AI integration. Red-blue integration.	SOAR platform, red team partnership, data science skills
L4: Adaptive	Continuous improvement feedback loops, supply chain risk	Mature enterprise or specialist MSSP. Full ATT&CK coverage.	Automated detection-to-remediation. Full supply chain visibility.	Automation pipeline, advanced analytics, threat sharing

Core SOC Capabilities by Level

L1-L2 FOUNDATION

Monitoring & Triage

24/7 alert monitoring from critical sources. Documented severity classification. Triage playbooks for top-10 alert types. Clear escalation path from L1 → L2 → IR team. Average triage decision < 15 minutes.

L2-L3 INTERMEDIATE

Detection Engineering

Custom detection rule development. SIEM correlation rules tuned to environment. False positive rate tracked and reduced. New rules validated in test environment before production. ATT&CK technique coverage mapped and gaps prioritised.

PEOPLE ARE THE CONSTRAINT, NOT TECHNOLOGY

The limiting factor in most SOC operations is not SIEM capability or log volume — it is analyst skill and analyst retention. A well-trained L2 analyst with a basic SIEM outperforms an untrained team with a $2M platform. Invest in analyst training before investing in more tools. ATT&CK training, SANS FOR508, and live threat hunting exercises provide the highest return.

CHAPTER 05

Threat Hunting Methodology

Hypothesis-driven proactive search for threats not caught by automated detections.

PEAK MODEL | HYPOTHESIS | DATA SOURCES | TTPs

The PEAK Threat Hunting Model

1

Prepare — Define Your Hunt

BEFORE YOU SEARCH

Identify hunt hypothesis (what specific attacker behaviour are you looking for?). Map to MITRE ATT&CK technique. Identify required data sources (are they available? Is quality sufficient?). Define success criteria: what would confirm or refute the hypothesis?

2

Execute — Run the Hunt

ACTIVE INVESTIGATION

Run queries across defined data sources. Analyse results: identify outliers, baseline deviations, unusual patterns. Pivot on anomalies: follow the thread, expand scope as new indicators emerge. Document all findings — positive AND negative.

3

Act — Apply Findings

AFTER THE HUNT

If threat confirmed: escalate to IR immediately, collect IOCs, document TTP. If negative: document as completed hunt with learnings — a negative hunt is valuable evidence. ALWAYS produce a detection rule from confirmed hypothesis to automate future detection of the same TTP.

Hunt Hypothesis Library — Sample Entries

ATT&CK Tactic	Technique	Hypothesis	Data Source	Key Query Element
Persistence	T1053.005	Attacker created scheduled task for persistence	Windows Security 4698	TaskName + CommandLine containing powershell/wscript/cmd
Credential Access	T1003.001	LSASS memory dump via procdump or comsvcs.dll	Process creation 4688, EDR	ParentProcess + CommandLine: -ma lsass / MiniDump / comsvcs
Defence Evasion	T1055	Process hollowing using legitimate binary	EDR process telemetry	Suspicious parent/child process combination + memory anomaly
Lateral Movement	T1550.002	Pass-the-hash via NTLM authentication	Auth logs 4624, 4648	LogonType=3 + NtLmSsp auth + admin share access from workstation
Exfiltration	T1048.003	DNS tunnelling for data exfiltration	DNS logs	TXT record responses > 255 bytes, high query frequency to single domain
Execution	T1059.001	PowerShell encoded command execution	PowerShell 4104 (script block logging)	EncodedCommand (-enc) flag + base64 string
Discovery	T1087.002	Domain user enumeration via LDAP	LDAP/AD logs, network	Bulk LDAP queries for samaccounttype=805306368 from non-DC host
Command & Control	T1071.001	HTTP C2 beaconing to non-corporate domains	Proxy/firewall logs	Regular interval HTTP/S requests to unknown domain, small consistent payload

```
// Splunk: Hunt for suspicious scheduled task creation
index=windows EventCode=4698
| eval cmd=lower(coalesce(TaskContent,""))
| where match(cmd, "powershell|cmd\.exe|wscript|cscript|mshta|regsvr32|rundll32")
| stats count by TaskName, SubjectUserName, ComputerName, TaskContent
| where count < 5  // Rare tasks more suspicious than common ones
| sort -count

// Splunk: Hunt for LSASS access (potential credential dumping)
index=windows EventCode=10  // Sysmon: ProcessAccess
TargetImage=*lsass.exe CallTrace=*
| where NOT match(SourceImage, "antivirus|csrss|winlogon|werfault")
```

```
| stats count by SourceImage, SourceProcessId, Computer
| where count < 3
```

HS

H O R I Z O N S H I E L D

Securing Your Digital Future, Today.

Threat Hunting & SOC Operations 2026

Part of the HorizonShield Security Series — 16 comprehensive professional cybersecurity manuals covering every domain of modern enterprise security.