PROJECT SENTINEL THREAT LOGIC SPECIFICATION

Document: Sentinel_Threat_Logic_Specification_v3.4.pdf
Status: Approved | Version 3.4 | Effective Date: November 1, 2023
Owner: Threat Intelligence & Security Research
Audience: Threat Analysts, SOC Analysts, Security Engineers

1.0 INTRODUCTION

This document defines all detection logic, correlation rules, scoring algorithms, and response actions for the Sentinel Platform. It is the authoritative source for what we detect and why. All platform behavior must be traceable to rules defined herein.

2.0 THREAT TAXONOMY

2.1 Threat Severity Levels

Level	Description	Response SLA	Business Impact
Critical	Active compromise/data exfiltration	15 minutes	Severe financial/reputational loss
High	Likely compromise, lateral movement	1 hour	Significant operational impact
Medium	Suspicious activity, reconnaissance	4 hours	Potential future impact
Low	Anomalous behavior, informational	24 hours	Minimal immediate impact
Informational	Confirmed benign, baseline events	No SLA	For awareness only

2.2 MITRE ATT&CK Coverage

Tactics Covered (14/14):

Initial Access, Execution, Persistence, Privilege Escalation

Defense Evasion, Credential Access, Discovery, Lateral Movement

Collection, Command & Control, Exfiltration, Impact

Techniques Mapped: 120+ enterprise techniques with detection logic

3.0 CORRELATION RULES LIBRARY

3.1 Rule Format & Structure

Each rule follows this structure:

text

```
RULE_ID: TLP-001-2023
NAME: "Credential Dumping via LSASS Memory Access"
TACTIC: Credential Access (TA0006)
TECHNIQUE: OS Credential Dumping: LSASS Memory (T1003.001)
SEVERITY: Critical
CONFIDENCE: High
DATA SOURCES:
  - EDR: Process creation events
  - Windows Security Events: Event ID 4688
  - Sysmon: Event ID 10 (ProcessAccess)
TRIGGER LOGIC:
  IF process_name IN ("procdump.exe", "mimikatz.exe", "lsass.exe")
  AND target_process = "lsass.exe"
  AND access_mask INCLUDES "PROCESS_VM_READ"
THEN
  CREATE_ALERT with SCORE = 950
  EXECUTE_RESPONSE: "Isolate Host"
  APPLY_TAGS: ["credential-access", "lsass", "critical"]
```

3.2 High-Priority Rule Examples

Rule TLP-045-2023: "Cobalt Strike Beacon Detection"
Logic: HTTP beaconing pattern + JA3/S signature + Certificate anomalies
Data Sources: Proxy logs, SSL/TLS inspection, EDR
Confidence Score: 0.92
Auto-response: Block external C2 IP, Quarantine host

Rule TLP-128-2023: "Living-off-the-Land Binary (LOLBin)"
Logic: Sysmon detects rundll32.exe or regsvr32.exe loading DLL from user temp directory
Data Sources: Sysmon, EDR
Confidence Score: 0.78
Auto-response: Alert only, require analyst review

Rule TLP-212-2023: "Data Staging to Cloud Storage"
Logic: Large volume upload to unfamiliar S3/GCP bucket from corporate asset
Data Sources: CloudTrail, DLP, Proxy logs
Confidence Score: 0.85
Auto-response: Block upload, Disable IAM keys, Alert data owner

4.0 INDICATOR SCORING FRAMEWORK

4.1 Composite Threat Score Formula

text

```
Composite_Score =
  (Base_Reputation × 0.3) +
  (Internal_History × 0.4) +
  (Temporal_Freshness × 0.2) +
  (Source_Trust × 0.1)
```

4.2 Scoring Components

Base Reputation (0-100)

Source	Score	Reason
VirusTotal (>50 engines)	100	Broad community detection
Commercial Intel (Confirmed)	90	Vendor validation
Internal Sandbox (Malicious)	85	Internal confirmation
ISAC Feed	75	Peer organization reporting
Unstructured Intel	60	Requires corroboration

Internal History (0-100)

text

```
If seen_before = TRUE:
  Score = 100 - (days_since_last_seen × 2)
  Minimum score = 40
Else:
  Score = 20 (unknown entity)
```

Temporal Freshness (0-100)

text

```
Score = MAX(0, 100 - (hours_since_first_seen × 5))
```

Source Trust (0-100)

Trust Tier	Sources	Score
Tier 1	Internal EDR, Firewall logs	100
Tier 2	Commercial Feeds (Recorded Future)	90
Tier 3	ISAC/Community Feeds	80
Tier 4	Unstructured/OSINT	60
Tier 5	Anonymous/Unverified	30

5.0 ENRICHMENT LOGIC SPECIFICATIONS

5.1 IP Address Enrichment

text

```
IP → [
  Geolocation (Country, City, ASN),
  Reputation: (VPN/Proxy/Tor check),
  Internal History: (Previous alerts, blocks),
  Related Domains: (Reverse DNS, PassiveDNS),
  Threat Feeds: (AbuseIPDB, AlienVault OTX)
]
```

5.2 File Hash Enrichment

text

```
Hash → [
  AV Detection: (VirusTotal count, engines),
  Sandbox Analysis: (Behavior, network, drops),
  Prevalence: (VT first_seen, last_seen),
  Signatures: (YARA, ClamAV),
  Internal Sightings: (Other hosts, count)
]
```

5.3 Domain Enrichment

text

```
Domain → [
  WHOIS: (Creation date, registrar),
  Reputation: (Web of Trust, Google Safe Browsing),
  Certificates: (Issuer, expiration, anomalies),
  Related Infrastructure: (IPs, subdomains),
  Historical Changes: (PassiveDNS history)
]
```

6.0 CORRELATION SCENARIOS

6.1 Multi-Stage Attack Detection

Scenario: "Phishing → C2 Beacon → Lateral Movement"

text

```
PHASE 1: Initial Access
  - Rule: TLP-301 (Suspicious Email Attachment)
  - Indicators: Malicious macro document
  - Score: 650

PHASE 2: Execution & C2
  - Rule: TLP-045 (Cobalt Strike Beacon)
  - Correlation: Same host as Phase 1
  - Score Increase: +300 (now 950)

PHASE 3: Lateral Movement
  - Rule: TLP-189 (PsExec to Multiple Hosts)
  - Correlation: Same user, time proximity
  - Final Score: 990 → CRITICAL ALERT
```

6.2 Insider Threat Detection

Scenario: "Data Exfiltration by Departing Employee"

text

```
INDICATOR 1: Unusual access patterns (after hours, weekends)
INDICATOR 2: Large volume downloads to personal cloud
INDICATOR 3: Access to unrelated business units
INDICATOR 4: HR flag (resignation submitted)
CORRELATION: All within 30-day window
SEVERITY: High (880)
RESPONSE: Manager notification, temporary access restriction
```

7.0 RESPONSE ACTION MATRIX

7.1 Automated Actions by Severity

Severity	Automated Actions	Required Approvals
Critical	Block IP, Quarantine Host, Kill Session	None (Post-action report)
High	Block IP, Alert SOC, Create Ticket	SOC Lead (1-click)
Medium	Alert SOC, Create Ticket	None
Low	Log only, Add to watchlist	None
Informational	Store in intelligence database	None

7.2 Action Specifications

Auto-Block IP (CRITICAL)

text

```
ACTION_ID: ACT-001
CONDITIONS:
  - Composite_Score >= 900
  - Severity = Critical
  - Indicator_Type = IP
  - NOT in whitelist (Business justification required)
IMPLEMENTATION:
  - API Call: Palo Alto Panorama
  - Duration: 24 hours (auto-expire)
  - Notification: SOC, Network Team
  - Rollback: Manual only (via ticket)
```

Host Quarantine (HIGH+)

text

```
ACTION_ID: ACT-002
CONDITIONS:
  - Host involved in Critical/High alert
  - Evidence of compromise
  - No critical business service impact
IMPLEMENTATION:
  - EDR API: Isolate from network
  - Duration: Until investigated
  - Notification: System Owner, SOC
```

8.0 MAINTENANCE & TUNING

8.1 Rule Lifecycle Management

Draft: Researcher creates rule (testing phase)

Staging: Rule deployed in monitor-only mode (7 days)

Production: After validation, rule active (alerting)

Tuning: Adjust based on false positive rate

Deprecation: Replace with improved rule or retire

8.2 Performance Metrics per Rule

Metric	Target	Review Threshold
Precision	> 85%	< 70%
Recall	> 80%	< 60%
False Positive Rate	< 5%	> 15%
Alert Volume	< 50/day	> 100/day
Mean Time to Triage	< 10 minutes	> 30 minutes

8.3 Quarterly Review Process

Metrics Review: All rules evaluated against targets

Threat Landscape Update: New techniques added

Rule Optimization: Tune thresholds, logic

Documentation Update: This specification revised

Stakeholder Sign-off: SOC, Engineering, Compliance

9.0 APPENDICES

Appendix A: Rule ID Nomenclature

TLP-XXX-YYYY where:

TLP: Threat Logic Project

XXX: Sequential rule number

YYYY: Creation year

Appendix B: Data Source Mappings

Detailed mapping of log sources to MITRE techniques

Appendix C: External Feed Specifications

Configuration for each commercial/open source feed

Appendix D: Change History

Version history of detection logic and scoring changes

APPROVAL SIGNATURES

Head of Threat Intelligence: ___________ Date: _________

SOC Manager: ___________ Date: _________

Chief Information Security Officer: ___________ Date: _________