SOC ANALYST L1

THE DEFENDER'S PLAYBOOK

OPERATIONS // SIMULATION // PROTOCOL

USER ROLE: ANALYST_L1
CLEARANCE: RESTRICTED
SESSION ID: ACT-492-22

SYSTEM STATUS: ONLINE

THE PRIME DIRECTIVE:
MINIMIZE DWELL TIME

SCENARIO A: WITHOUT SOC

287 DAYS

Attackers remain hidden. Breaches discovered by external parties (FBI, Customers).

Result: Catastrophic financial & reputation loss.

SCENARIO B: WITH SOC

7 DAYS

Rapid detection and containment. Threat neutralized before critical damage occurs.

The SOC exists to close the gap between infiltration and detection.

OPERATIONAL LANES: KNOW YOUR SCOPE

SOC
Security Operations Center

The Shield
Inter Regular

- Monitor Security Events
- Detect Threats
- Analyze Alerts

NOC
Network Operations Center

The Flow
Inter Regular

- Monitor Network Performance
- Track Uptime
- Bandwidth Issues

IR
Incident Response

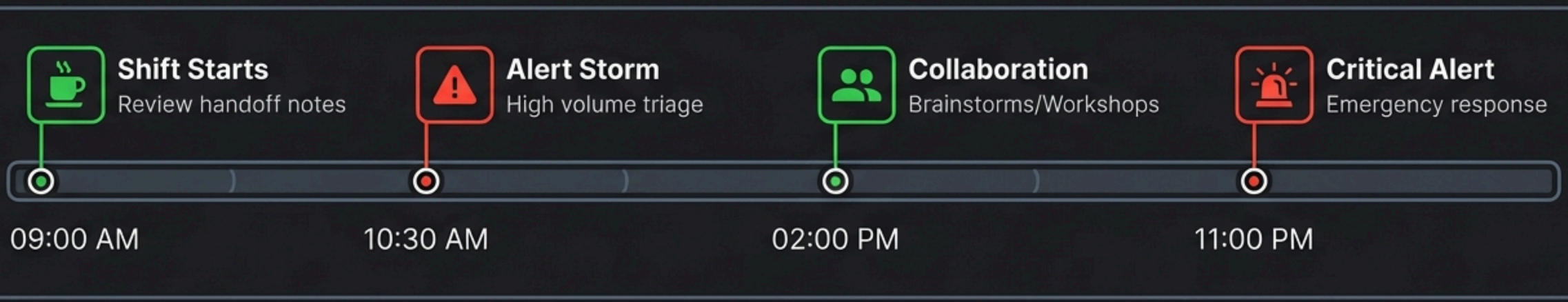
The Firefighters
Inter Regular

- Respond to Confirmed Incidents
- Perform Forensics
- Containment Actions

CONSEQUENCES OF FAILURE → Reputation Loss → Financial Loss → Legal Issues → Compliance Violations

THE OPERATOR'S LOOP & SHIFT PROTOCOLS

SOC Analyst Workflow



TRIAGE PROTOCOL: THE DECISION ENGINE

01 INITIAL ASSESSMENT

Read alert description.
Check severity rating.

Context check: Critical server or workstation? Business hours or 3 AM?

Severity Level

Critical

Affected Asset

Workstation

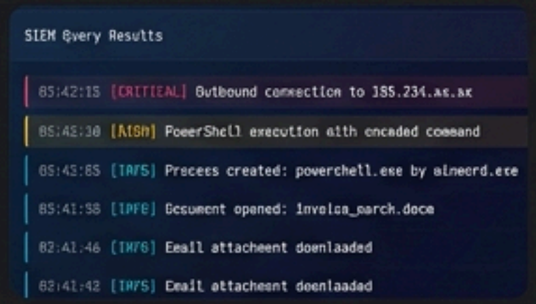
Time of Event

03:42 AM (Off-hours)

02 LOG ANALYSIS

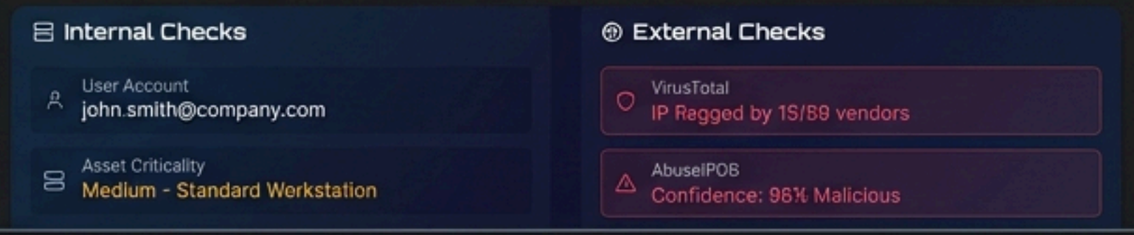
Query SIEM (30 mins +/- alert time).

Look for: Source IP, User account, Process details.



03 CONTEXT GATHERING

Internal vs. External validation.
Check Threat Intel (VirusTotal). Is the IP known malicious? Is the user legitimate?



04 DECISION

TRUE POSITIVE
Escalate with documentation.

FALSE POSITIVE
Close with justification.

UNSURE
Escalate.

GOLDEN RULE: WHEN IN DOUBT, ESCALATE.

SIGNAL VS. NOISE

RED FLAGS (True Positive Indicators)	**BENIGN TRIGGERS** (Common False Positives)
Connection to known malicious IP/Domain	Automated vulnerability scans triggering port scan alerts
Unusual timing (e.g., 3 AM access to finance data)	Legitimate admin activity (verify with change tickets)
Privilege escalation patterns	Poorly tuned detection rules (low thresholds)
Multiple failed logins followed by success	Scheduled backup tasks appearing as unusual processes
Data exfiltration patterns (large uploads)	Security researchers using TOR (verify user context)

THREAT PROFILE 01: PHISHING & C2 CALLBACK

ALERT FEED (WHAT SOC SEES)

CRITICAL ALERT: Outbound Connection to Known C2

Process:	`outlook.exe -> powershell.exe -> rundll32.exe`
Destination:	`185.234.xx.xx (Malicious)`
Pattern:	`Beaconing detected (60s interval)`

INVESTIGATION & ACTION

Evidence

1. **Check Headers:** Sender spoofed (security@micr0soft-verify.com)
2. **Threat Intel:** IP flagged as Cobalt Strike C2
3. **Process Tree:** Confirmed malicious spawning.

Required Actions

- Isolate Endpoint
- Block C2 IP at Firewall
- Reset Credentials

THREAT PROFILE 02: BRUTE FORCE ATTACK

Log Viewer

ACTIVE DIRECTORY LOGS

```
23:45:13 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:14 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:15 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:16 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:17 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:18 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:19 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:20 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:21 [4625] Failed login: admin@company.com from 192.168.1.100
23:45:20 [4624] Successful login: admin@company.com from 192.168.1.100
```

PATTERN DETECTED:
100+ Failed Attempts followed by Success

ANALYSIS

This is not a forgotten password. This is a compromise.

IMMEDIATE ACTION: ACCOUNT LOCKOUT + ESCALATE

THREAT PROFILE 03: RANSOMWARE DETONATION

EDR ALERT - CRITICAL

Process: `vssadmin.exe`

Command Executed: `'vssadmin delete shadows'`

Risk: `RANSOMWARE BEHAVIOR`

FILE SYSTEM MONITOR

```
C:\Users\victim\Documents\budget_2024.xlsx.encrypted
C:\Users\victim\Documents\contracts.pdf.encrypted
C:\Users\victim\Photos\team_photo.jpg.encrypted
C:\Users\victim\Projects\roadmap.docx.encrypted
C:\Users\victim\Database\customers.db.encrypted
C:\Users\victim\Backups\full_backup.zip.encrypted
```

TRIAGE PROTOCOL

Shadow copy deletion is the smoking gun.

IMMEDIATE ACTION: ISOLATE ENDPOINT (Network Cut).

⚠ DO NOT REBOOT (Preserve RAM Evidence).

THREAT PROFILE 04: MALWARE & CRYPTOMINING

SYSTEM PROCESSES

Process	PID	CPU	Path
svchost.exe	4928	0%	C:\Users\Public\svchost.exe
svchost.exe	4921	95%	C:\Users\Public\svchost.exe
svchost.exe	4921	1%	C:\Users\Public\svchost.exe
svchost.exe	3606	0%	C:\Users\Public\svchost.exe
svchost.exe	4926	0%	C:\Users\Public\svchost.exe
svchost.exe	3377	0%	C:\Users\Public\svchost.exe
svchost.exe	688	0%	C:\Users\Public\svchost.exe
svchost.exe	4921	0%	C:\Users\Public\svchost.exe

Entry Point:
Vulnerable Jenkins Plugin
Inter Regular

ANOMALY: Real svchost lives in System32.

NETWORK CONNECTIONS

Destination: xmr.pool.minergate.com

Protocol: TCP/Stratum

Entry Point:
Vulnerable Jenkins Plugin

Actions:
- Kill Process
- Quarantine
- Patch Jenkins

THREAT PROFILE 05: DATA EXFILTRATION (INSIDER)

USER ACTIVITY ALERT

Unusual Data Transfer Volume

User: john.smith@company.com

Activity: Upload 2.3GB / 15 mins

Destination: mega.nz (Cloud Storage)

Tags Detected: [CONFIDENTIAL] [INTERNAL_ONLY]

CONTEXTUAL ANALYSIS

HR STATUS CHECK

Status: RESIGNATION SUBMITTED (Notice Period).

Timing: 19:42 PM (After Hours).

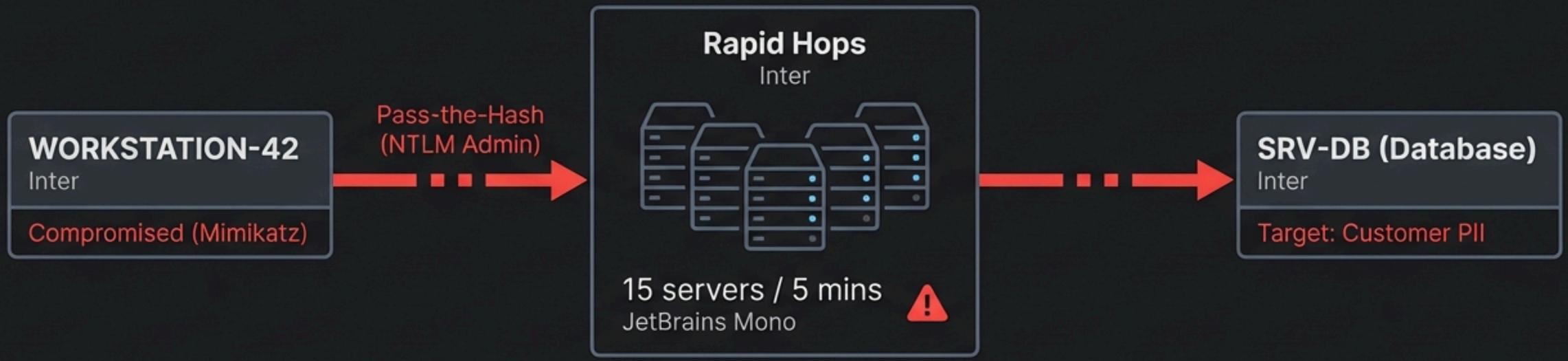
The Clincher: High volume upload + Notice period = Data Theft.

Bottom Action Bar

Actions: Block Storage Access | Preserve Mailbox | Contact Legal

THREAT PROFILE 06: LATERAL MOVEMENT

Network Map



ANALYSIS & ACTION

Attack is spreading from workstation to infrastructure.

- `PROTOCOL: ❌ Disable Account → ❌ Force Password Reset → ❌ Isolate All Systems → ✅ Activate IR.`

THE ARMORY: CORE TOOLSETS

THE BRAIN (SIEM)

Logs & Correlation

Splunk, Microsoft Sentinel, IBM QRadar

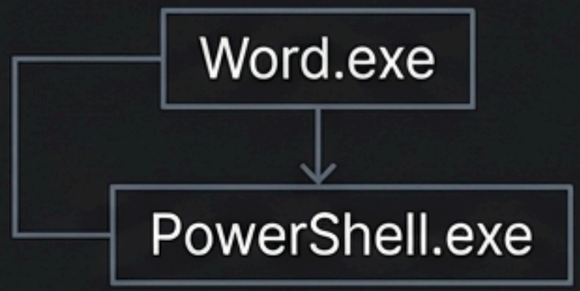
```
index=security action=failure
| stats count by src_ip
```

Function: Aggregates logs, runs queries, builds dashboards.

THE EYES (EDR/XDR)

Endpoint Telemetry

CrowdStrike Falcon, Microsoft Defender, Carbon Black



Function: Real-time protection, process trees, isolation.

INTELLIGENCE & OPERATIONS

THREAT INTELLIGENCE (CONTEXT)

Is this IP bad?

Tools: VirusTotal (Reputation), AbuseIPDB, MITRE ATT&CK

Threat Intel

VirusTotal

File and URL analysis service

15/89 Malicious ⚠

Key Use Cases

- Hash lookup
- URL scanning
- Malware analysis
- IOC enrichment

TICKETING (THE AUDIT TRAIL)

If it isn't documented, it didn't happen.

Tools: ServiceNow, Jira

Function: Legal proof of action, SLA tracking, investigation notes.

Ticketing

ServiceNow

IT service management and security operations

Key Use Cases

- Incident management
- SLA tracking
- Workflow automation

DEBRIEF: THE L1 ANALYST MINDSET

✅ Don’t just memorize theory; learn to analyze logs.
✅ Understand attack patterns, not just tool names.
✅ Think like a defender.

NEXT STEPS

HOME LAB

Build it. Break it.
Document it.

CERTIFICATIONS

BTL1 (Blue Team L1) / CCD (Certified Cyber Defender).

CAREER

Move from Alert Triage to Threat Hunting.