SIEM Monitoring and Alert Triage

Splunk, Wazuh, and ELK

IronGrid Security | Period covered: January 2023 to March 2023

Prepared by Mahdi Ghaznawy

Executive summary

This report summarizes alert monitoring and triage activity conducted in a simulated SOC environment using Splunk, Wazuh, and ELK. The objective is to demonstrate practical detection engineering, enrichment, and response workflows. KPIs include alert volume, triage outcomes, mean time to acknowledge, and mean time to respond.

Key metrics

Metric	Value
Total alerts processed	2,357
Critical	142
High	611
Medium	987
Low	617
Escalated to incident handling	65
True positive rate	18 percent
Mean time to acknowledge	6 minutes
Mean time to respond	41 minutes
Use cases enabled	23 correlation rules

Detection sources include Splunk correlation searches, Wazuh rules, and ELK Kibana alerts that query file integrity events, authentication anomalies, suspicious process creation, and network beaconing patterns.

Notable triage cases

Suspicious PowerShell execution on Windows host

- Source: Wazuh rule 18107 and Splunk WinEventLog Security events.
- Indicator: Encoded command with powershell.exe spawning cmd.exe.
- Host: WIN10-LAB-04 and user lab\a.miller.
- Action: Isolated host and collected memory image. Searched for hash matches in Splunk.
- Outcome: Benign administrator script and rule tuned to exclude signed maintenance task.

Multiple failed RDP attempts then success from a new country

- Source: Splunk correlation for impossible travel followed by authentication success.
- Indicator: 27 failed logon attempts from 185.243.56.71 followed by success on lab\svc-backup.
- Action: Forced password reset, reviewed MFA logs, and checked VPN usage.
- Outcome: True positive. Credentials were exposed during a prior phishing simulation.

ELK 404 anomaly indicating potential scanning

- Source: Kibana Lens dashboard watch.
- Indicator: Spike in 404 responses on nginx-lab01 by 4.2 times baseline.
- Action: Blocked offending subnet in security group and reviewed WAF logs.
- Outcome: External scan. Added rate limit and updated WAF rules.

Sample queries and rules

Splunk SPL example for suspicious PowerShell

```
index=win* sourcetype="WinEventLog:Security" (Process_Name="*powershell.exe*" OR
New_Process_Name="*powershell.exe*") CommandLine="*-enc*" OR
CommandLine="*FromBase64String*" | stats count by host, user, CommandLine | where count > 0
```

Wazuh rule snippet reference

```
<rule id='18107' level='10'><if_group>windows</if_group><field
name='win.eventdata.Image'>.*powershell.exe</field><description>Suspicious PowerShell
execution</description></rule>
```

Kibana query for nginx 404 anomaly

```
event.dataset:"nginx.access" AND response:404 | stats count by client.ip, url.original |
sort -count
```

Recommendations

- Enable enrichment for GeoIP and threat intel on all authentication events to improve context during triage.
- Expand MFA coverage to service accounts where feasible and rotate credentials every 90 days.
- Tune PowerShell detection to trust approved signed scripts and alert on unsigned or obfuscated executions.
- Implement watchlists for privileged accounts and notify on first time source IP and first time device.
- Create a containment runbook that pairs SIEM alerts with EDR isolation steps to reduce response time.