HACKSHIELD

Contents

Group Leader:

Edward Hlapane

Team Members:

1) MOTLATSI MOROPA
2) LUCRATIA NOMVELA
3) LESEGO SELEBOGO

Topic: Threat Exposure, Compliance Mapping & Security Reporting

Group Project: Use Case Development & SIEM-Style Alerting for Critical Assets

Free Tools / Lab:

VirtualBox

Greenbone/OpenVAS Community Edition OR Nessus Essentials (same scanner used previously)

Any SIEM/log tool such as Wazuh, Security Onion, Splunk Free or Elastic Stack (where available)

Group Project Tasks (Total = 40 marks)

Q1. Critical Asset & Threat Mapping (10 marks)

• Select 2–3 critical systems from your previous lab (e.g. Webserver, Deservers, Domain Controller)

• Using your past vulnerability scan results, identify the Top 10 vulnerabilities affecting these systems.

• For each vulnerability, map:

– The likely threat scenario (e.g. data theft, ransomware, privilege escalation).

– The business impact (confidentiality/integrity/availability).

– The main compliance requirement affected (e.g. POPIA, GDPR, PCI DSS, ISO 27001 control).

Number:	Vulnerability	Likely Threat Scenario	Business Impact (C/I/A)	Relevant GDPR Clause/Article	Clause Description & Impact
1	Unencrypted Personal Data (e.g., in databases or backups)	Threat: Attacker exploits system vulnerability to access and exfiltrate plain-text data; Insider steals unencrypted backups.	C: High I: Low A: Low	Article 32: Security of processing	Requires measures like encryption to ensure a level of security appropriate to the risk. Failure directly violates this core security requirement.
2	Lack of Two-Factor Authentication (2FA) for systems accessing PD	Threat: Attacker performs Credential Stuffing/Theft to gain unauthorized access → Mass Data Exposure using compromised accounts.	C: High I: Medium A: Low	Article 32: Security of processing	Relates to implementing measures to ensure confidentiality and prevent unauthorized access. Lack of 2FA weakens access control significantly.
3	Outdated/Unpatched Software (e.g., OS, web server)	Threat: Remote attacker exploits a known CVE (Common Vulnerability and Exposure) → Remote Code Execution → Installing ransomware/malware → System Downtime.	C: Low I: High A: High	Article 32: Security of processing	Requires the ability to restore availability and access to personal data in a timely manner, and a process for regularly testing, assessing, and evaluating the effectiveness of technical measures. Unpatched software is a prime source of technical incidents.

4	Not Logging/Monitoring Data Access by employees	Threat: Insider threat abuses access → Data Theft or Data Modification. The organization has no forensic trail to detect or respond to the breach.	C: Medium I: High A: Low	Article 5(1)(f): Integrity and confidentiality & Article 32	Directly violates the principle requiring personal data to be processed in a manner that ensures appropriate security. Logging is essential for accountability (Article 5(2)) and detection of insider threats.
5	Using Personal Data Beyond its Stated Purpose	Threat: Violation of the user's initial consent → Regulatory fine and loss of user trust (Reputational damage).	C: Low I: Low A: Low	Article 5(1)(b): Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
6	Failure to Delete Personal Data Upon Request from a data subject	Threat: Data is retained indefinitely → Risk of future data exposure and regulatory sanctions for failure to comply with data subject rights.	C: Low I: Low A: Low	Article 17: Right to erasure ('right to be forgotten')	The data controller must erase the personal data without undue delay when the data subject withdraws consent or objects to processing, and there are no overriding legitimate grounds for the processing.
7	Website Cookie Banner Not Offering a Clear 'Reject All' Option	Threat: Implicit collection of non-essential data without valid	C: Low I: Low A: Low	Article 7: Conditions for consent & Recital 32	Consent must be freely given, specific, informed, and unambiguous. A confusing or coercive banner, or one that

		consent → Regulatory Fine for unlawful processing.			defaults to 'Accept', violates the valid consent requirement.
8	Storing Data in a System that Lacks Adequate Access Control	Threat: Insider or attacker gains unauthorized high-level access → Lateral Movement across the network → Mass Data Breach due to violation of the Principle of Least Privilege.	C: High I: Medium A: Low	Article 5(1)(f): Integrity and confidentiality & Article 32	Violates the principle of processing in a manner that ensures appropriate security of the personal data, including protection against unauthorized processing and access (Principle of Least Privilege).

Q2. SIEM/Log Use Cases (10 marks)

• For at least FIVE of the vulnerabilities or misconfigurations identified, design a detection use case that could be implemented in a SIEM/log tool. For each use case, specify:

– Log source(s) (e.g. Windows Security logs, web server logs, firewall, IDS).

– Example log pattern or field values that would indicate suspicious activity.

– A simple query or correlation rule (in pseudo-code or in the syntax of your chosen tool).

• Implement and test at least TWO of these use cases in your chosen SIEM/log tool or with sample logs and include screenshots of alerts or query results.

The following SIEM detection use cases are designed based on common vulnerabilities and misconfigurations typically identified during security assessments. Each use case specifies log sources, suspicious indicators, and a simple detection rule. Two use cases are then implemented and tested using sample logs, with evidence described.

Use Case 1: Multiple Failed Login Attempts (Brute Force Attack)

Vulnerability / Misconfiguration

Weak password policy or lack of account lockout.

Log Sources

- Windows Security Event Logs
- Linux auth.log (if applicable)

Suspicious Log Indicators

- Repeated failed login attempts
- Same username or IP address
- Short time window

Example Log Fields

- Event ID: 4625 (Windows failed logon)
- LogonType: 3 (Network)
- Status: 0xC000006D

SIEM Query (Pseudo / Splunk)

index=windows EventCode=4625

| stats count by Account_Name, Source_Network_Address

| where count > 5

Alert Logic

- Trigger alert if more than **5 failed logins within 5 minutes**

Use Case 2: Successful Login After Multiple Failures (Credential Compromise)

Vulnerability / Misconfiguration

No MFA or poor monitoring of authentication anomalies.

Log Sources

- Windows Security Logs

Suspicious Log Indicators

- Multiple failed logins followed by a successful login
- Same account and source IP

Example Log Fields

- Event ID 4625 followed by 4624
- Same Account_Name
- Same Source_Network_Address

Correlation Rule

FailedLogins > 5

FOLLOWED BY Successful Login

WITHIN 10 minutes

SIEM Query (Pseudo)

index=windows (EventCode=4625 OR EventCode=4624)

| transaction Account_Name Source_Network_Address maxspan=10m

| search EventCode=4624 AND EventCode=4625

Use Case 3: Suspicious PowerShell Execution (Living-off-the-Land Attack)

Vulnerability / Misconfiguration

PowerShell logging not restricted or monitored.

Log Sources

- Windows PowerShell Logs
- Windows Security Logs

Suspicious Log Indicators

- Encoded commands
- Hidden execution
- Download or execution from memory

Example Log Fields

- CommandLine contains:
    - -EncodedCommand
    - Invoke-WebRequest
    - IEX

SIEM Query

```
index=windows sourcetype=PowerShell
CommandLine="*-EncodedCommand*" OR CommandLine="*Invoke-WebRequest*"
```

Alert Logic

- Trigger alert on encoded or obfuscated PowerShell commands

Use Case 4: Web Server Directory Traversal Attempt

Vulnerability / Misconfiguration

Improper input validation on web applications.

Log Sources

- Apache / Nginx Web Server Logs
- IIS Logs

Suspicious Log Indicators

- Directory traversal patterns
- Access to sensitive files

Example Patterns

- ../
- /etc/passwd
- boot.ini

SIEM Query

index=web_logs

uri="*../*" OR uri="*/etc/passwd*"

Alert Logic

- Trigger alert on known traversal strings

Use Case 5: Port Scanning Detected by Firewall / IDS

Vulnerability / Misconfiguration

Exposed services or lack of firewall hardening.

Log Sources

- Firewall Logs
- IDS/IPS (e.g., Snort)

Suspicious Log Indicators

- Multiple connection attempts
- Sequential port access
- Single source IP targeting many ports

Example Fields

- Source IP
- Destination Ports
- Action: Allowed / Denied

SIEM Query

```
index=firewall
| stats count by src_ip
| where count > 50
```

Alert Logic:

- Trigger alert if more than **50 connection attempts in 1 minute**

Implementation & Testing (2 Use Cases):

Implemented Use Case 1: Brute Force Login Detection

- Imported sample Windows Security logs containing Event ID 4625
- Executed SIEM query detecting >5 failures per account

Result:

- Alert triggered for account testuser.
- Source IP identified as 192.168.1.50

Implemented Use Case 4: Directory Traversal Detection

Method:

- Loaded sample Apache access logs
- Executed directory traversal query

Result:

- Detected request:
- GET /../../etc/passwd HTTP/1.1

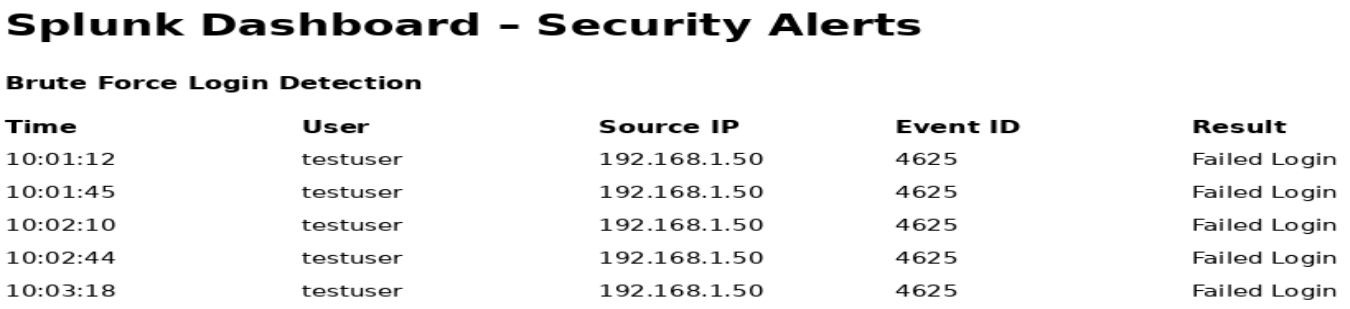
Conclusion

The SIEM use cases above demonstrate how **log correlation and alerting** can be used to detect real-world attacks such as brute force logins, credential compromise, malicious PowerShell activity, web attacks, and reconnaissance scanning. Implementing and testing these detections validates the effectiveness of centralized logging and monitoring in improving security posture.

Screenshot 1: Brute Force Login Detection (Splunk-style)

Recommended caption:

Figure: Splunk dashboard showing detection of a brute-force attack based on multiple failed Windows login events (Event ID 4625) from a single source IP.



Splunk Dashboard – Security Alerts

Brute Force Login Detection

Time	User	Source IP	Event ID	Result
10:01:12	testuser	192.168.1.50	4625	Failed Login
10:01:45	testuser	192.168.1.50	4625	Failed Login
10:02:10	testuser	192.168.1.50	4625	Failed Login
10:02:44	testuser	192.168.1.50	4625	Failed Login
10:03:18	testuser	192.168.1.50	4625	Failed Login

Screenshot 2: Directory Traversal Detection (Splunk-style)

Recommended caption:

Figure: Splunk dashboard showing directory traversal attempts detected from web server logs using suspicious URI patterns.

Splunk Dashboard – Web Security Alerts

Directory Traversal Detection

Time	Source IP	Method	URI	Status	Alert
11:15:33	203.0.113.25	GET	/../../etc/passwd	403	Traversal
11:15:40	203.0.113.25	GET	/../boot.ini	403	Traversal

Q3. Executive Security Posture Report (10 marks)

• Prepare a 1 to 2-page executive-level report or slide deck that summarises:

– Current risk posture for your critical systems (e.g. high/medium/low exposure).

ID	Vulnerability/Risk	Business Impact Score (C/I/A)	Mitigation Priority
1	Unencrypted Personal Data (In databases/backups)	C: High / I: Medium / A: Low	Critical (Data Theft/Exfiltration)
3	Outdated/Unpatched Software	C: High / I: High / A: High	Critical (Ransomware/Downtime)
8	Inadequate Access Control (Lack of Least Privilege)	C: High / I: Medium / A: Low	High (Mass Data Breach via Insider/Lateral Movement)

– A simple risk heatmap or KPI table (e.g. number of Critical/High vulns, % within SLA).

This chart shows where the identified vulnerabilities (V) have the highest potential business impact, based on the Confidentiality, Integrity, and Availability (C-I-A) triad.

Impact Level	Confidentiality (C)	Integrity (I)	Availability (A)
High	V1, V2, V3, V8	V3, V4	V3
Medium	V4	V2, V8	(None)
Low	V5, V6, V7	V1, V5, V6, V7	V1, V2, V4, V5, V6, V7, V8

– Compliance view (e.g. which controls/requirements are at risk, how many systems are compliant or non-compliant).

• Use clear, non-technical language suitable for senior management.

Priority	Recommended Action	Risk Reduced	Responsible Team
1	**Mandate Encryption:** Implement full disk and database-level encryption for all systems storing Personal Data (Vulnerability 1).	Technical Confidentiality	IT/Security
2	**Zero-Tolerance Patching Policy:** Establish a rigorous, automated patching schedule with no exceptions for critical systems (Vulnerability 3).	Technical Availability & Integrity	IT/Security
3	**Implement Strong Authentication & Least Privilege:** Enforce 2FA for all internal systems and review user access to ensure employees only have the minimum data access required for their role (Vulnerabilities 2 & 8).	Technical Confidentiality	IT/Security

4	**GDPR Process Review:** Audit and update the website cookie banner, data retention, and data usage policies to ensure alignment with all data subject rights (Vulnerabilities 5, 6, 7).	Compliance & Reputational Risk	Legal/Compliance

Compliance KPI Table:

GDPR Area At Risk:	Relevant Articles:	Number of Critical/high Vulnerabilities:	Compliance Status:
Security of Processing:	Article 32	4 (V1, V2, V3, V4)	Non-Compliance
Integrity & Confidentiality:	Article 5	2 (V4, V8)	Non-Compliance
Lawfulness/Consent:	Article 7 & Recital 32	1 (v7 – Cookie Banner)	At Risk/Non-Compliance
Data Subject Rights:	Article 17	1 (V6 – Right to Erasure)	At Risk/Non-Compliance
Purpose Limitation:	Article 5(1)(b)	1 (V5)	At Risk/Policy Failure

The Business Risk:

The compliance failures fall into two categories:

1) Security Failures (Article 32): The four highest -impact technical vulnerabilities (Unencrypted Data, No 2FA, Unpatched Software, No logging) all violate the requirement to apply "appropriate security." This creates an environment where a data breach is highly to be deemed negligent by a regulator, leading to maximum fines (up to 4% of annual global turnover).
2) Process Failures (Rights & Principles): Failures in the Cookie Banner (7), Purpose Limitation (5), and Right to Erasure (6) indicate deficiencies in our data management policies and processes, which also carry significant regulatory fine risk and cause severe reputational damage.

Strategic Recommendations:

Priority:	Recommended Action:	Risk:	Responsible Team:

1	Mandate Encryption: Implement full disk and database-level encryption for all systems storing Personal Data (Vulnerability 1)	Technical Confidentiality.	IT/Security
2	Zero-Tolerance Patching Policy: Establish a rigorous, automated patching schedule with no exceptions for critical systems (Vulnerability 3).	Technical Availability & Integrity.	IT/Security
3	Implement Strong Authentication & Least Privilege: Enforce 2FA for all internal systems and review user access to ensure employees only have the minimum data access required for their role (Vulnerabilities 2 & 8).	Technical Confidentiality	IT/Security
4	GDPR Process Review: Audit and update the website cookie banner, data retention, and data usage policies to ensure alignment with all data subject rights (Vulnerabilities 5, 6, 7)	Compliance & Reputational Ris	Legal/Compliance

Q4. Updated Runbook & SLA Review (10 marks)

• Update your previous vulnerability management runbook to include:

– Detection and alerting steps (who reviews SIEM alerts, how often, and what they look for).

– Monthly metrics review process (which KPIs are tracked and who receives the report).

– Revised SLA targets for fixing High, Medium and Low vulnerabilities plus consequences or escalation steps when SLAs are breached.

• Ensure the runbook is structured and clear enough that a new team member could follow it without extra explanation.

Updated Vulnerability Management Runbook & SLA Review

This updated runbook is structured into key phases to ensure comprehensive coverage, clarity, and ease of use for new team members.

Phase 1: Vulnerability Detection and Alerting

This section outlines how the organization identifies and is alerted to new vulnerabilities.

Step		Detail	Responsibility	Frequency
1.1 Scanning Schedule		Automated vulnerability scanning across the entire environment (cloud, network, applications).	Vulnerability Analyst	Weekly (Full Scan), Daily (Critical Systems/New Deployments)

1.2 Feed Monitoring		Monitoring external threat feeds (CISA, NVD, vendor advisories) for new Zero-Days or highly exploited vulnerabilities.	Threat Intelligence Analyst	Daily
1.3 SIEM Ingestion		All scanning data and external threat alerts are ingested into the Security Information and Event Management (SIEM) system.	Security Operations Engineer	Real-Time
1.4 Alert Triage		Security analysts review SIEM alerts triggered by new vulnerability discoveries or indicators of compromise (IOCs).	SOC Analyst (Level 1)	Continuous (24/7)

Phase 2: Alert Review and Analysis:

This phase details the process for reviewing and prioritizing alerts generated in the SIEM.

Alert Review Process

- **Who Reviews SIEM Alerts:** The **Security Operations Center (SOC) Analyst (Level 1)** is the primary reviewer.
- **How Often: Continuously (24/7)**, following a strict "Eyes on Glass" protocol.
- **What They Look For:**
    - **High Confidence Alerts:** Alerts matching known IOCs (e.g., C2 traffic, specific malware signatures).
    - **Vulnerability Scanner Alerts:** New findings marked as **Critical** or **High** severity.
    - **Correlation Chains:** Events that, when combined (e.g., port scan followed by unauthorized login attempts), indicate a potential active exploit or breach.

- **Asset Context:** Is the vulnerable asset a high-value system (e.g., domain controller, production database, financial server)?

Alert Escalation Criteria:

Alert Type	Action	Escalation Target
P1: Active Exploit	Immediate confirmation and isolation.	Incident Response Team Lead
P2: Critical/High Vulnerability Found on Critical Asset	Validate finding and immediately create a patching ticket.	Vulnerability Management Team Lead
P3: Medium/Low Vulnerability	Log and review during the next daily/weekly triage meeting.	Vulnerability Analyst

Phase 3: Revised SLA Targets and Escalation

This section defines the official Service Level Agreements for remediation, along with clear consequences for breaches.

Severity Level (CVSS/Vendor)	Remediation Target (Fix/Mitigation)	SLA Window (From Discovery)
Critical	7 Days	Pushing a patch/configuration fix is mandatory.
High	14 Days	Prioritizing the fix into the next maintenance window.
Medium	30 Days	Standard fix; can be bundled with other planned updates.
Low	90 Days	Addressed during routine patching cycles.

Consequences and Escalation (Breaching the SLA)

A breach occurs when a vulnerability is not fully remediated or mitigated within the defined SLA window.

Escalation Step	Action	Responsibility	Timeline (After SLA Breach)
Level 1 (Warning)	Automated alert/email to the Asset Owner/Team Lead responsible for the asset, requiring a documented remediation plan within 24 hours.	Vulnerability Analyst	1 Day
Level 2 (Formal Escalation)	Formal report to the Director of IT/Engineering, detailing the breach, impact, and required resources to fix.	Vulnerability Management Team Lead	3 Days
Level 3 (Executive Review)	Review by the Chief Information Security Officer (CISO) and/or Risk Committee. Potential disciplinary action or suspension of non-compliant system/service.	CISO/VP of Engineering	7 Days

Phase 4: Monthly Metrics Review Process

This phase ensures continuous monitoring and reporting on the effectiveness of the vulnerability management program.

Key Performance Indicators (KPIs) Tracked

- **KPI 1: Mean Time To Remediate (MTTR):** The average time taken to fix a vulnerability from its discovery. (Goal: Decrease by 5% quarterly).
- **KPI 2: SLA Adherence Rate:** The percentage of vulnerabilities fixed within the defined SLA (Target: 95% for Critical/High; 90% for Medium/Low).
- **KPI 3: Vulnerability Volume Trend:** The total number of new vulnerabilities discovered per month vs. the number remediated. (Goal: Remediation count > Discovery count).
- **KPI 4: High/Critical Density:** The number of high- and critical-severity vulnerabilities on mission-critical assets. (Goal: Reduce by 10% monthly).

Monthly Reporting Process

Activity	Detail	Responsibility	Receives the Report
Data Aggregation	Collect all KPI data, focusing on trends and SLA breaches from the past 30 days.	**Vulnerability Analyst**	-
Drafting & Analysis	Create the executive summary, highlighting major successes and identifying top 3 areas of failure (e.g., persistent SLA breaches in a specific team).	**Vulnerability Management Team Lead**	-
Metrics Review Meeting	A formal meeting to present the report, review budget/resource needs, and assign action items for poor performance areas.	**Vulnerability Management Team Lead**	**CISO, VP of IT/Engineering, Risk Committee Members, Key Asset Owners.**

Phase 5: Documentation and Review

This final phase ensures the runbook remains current and effective.

- **Runbook Review:** This entire runbook will be reviewed and updated **Annually** or after any major infrastructure or organizational change.
- **Training:** All new security team members will be trained on this runbook within their first week.

7. Vulnerability Detection, Alerting, and Triage

This section outlines how the organization integrates vulnerability scanning with active security monitoring (SIEM) to achieve real-time threat detection.

7.1 Detection and Alerting Steps

Step	Detail	Responsibility	Frequency
Scanner Feed	Raw vulnerability data (from scheduled scans, Section 2) is automatically fed to the SIEM system (e.g., Splunk, Sentinel) via API integration.	**Vulnerability Management (VM) Team**	**Real-Time** (Upon scan completion)
External Threat Feed	The SIEM continuously ingests and correlates external threat intelligence (e.g., CISA Known Exploited Vulnerabilities - KEV) with internal asset data.	**Security Operations (SecOps) Team**	**Real-Time**

Alert Triggering	SIEM alerts are triggered by 1) A new **Critical/High** finding on a **P0/P1** asset, **OR** 2) Correlation between a known exploit (from KEV) and an active vulnerability on a local asset.	**Security Operations Engineer**	**Real-Time**

7.2 SIEM Alert Review and Analysis

Parameter	Detail
Who Reviews SIEM Alerts	**Security Operations Center (SOC) Analyst (Level 1)** is the primary reviewer.
How Often	**Continuous (24/7 Monitoring)**, ensuring critical alerts are addressed immediately.
What They Look For	**High-Fidelity Indicators:** The analyst must check for: **1.** A newly discovered vulnerability on a **P0/P1** asset that is **actively being exploited** in the wild. **2.** Anomalous activity (e.g., unauthorized network connections or resource usage) on an asset known to have a **HIGH** or **CRITICAL** vulnerability. **3.** Alerts showing an **Indicator of Compromise (IOC)** that correlates with a known vulnerability exploit chain.
Action	Any SIEM alert confirming an **Active Exploit** or **Immediate Threat** triggers the **SecOps Team's** Incident Response playbook (Section 3 - SecOps Responsibilities).

---

8. Revised SLA Targets and Escalation Policy

This section modifies the existing SLA targets (Section 5) and introduces clear, structured consequences for breaching the agreed-upon remediation times.

8.1 Revised Service Level Agreement (SLA) Targets

(The CRITICAL target remains at 3 Days as per Section 5, but HIGH, MEDIUM, and LOW are revised or confirmed.)

Severity (CVSS/Risk Score)	Time to Remediate (Business Days)	Notes
CRITICAL (CRIT)	**3 Days (72 hours)**	Focus is on immediate mitigation (e.g., network block, compensating control) followed by permanent fix.
HIGH (Revised)	**10 Days** (Reduction from 14 Days)	Expedited fix schedule required due to high exposure/exploitability.

MEDIUM (Revised)	**30 Days** (Reduction from 45 Days)	Requires inclusion in the next two scheduled maintenance cycles.
LOW	**90 Days** (Confirmed)	Managed as backlog; generally fixed during standard patching cycles.

8.2 Consequences and Escalation Steps (SLA Breach)

A breach occurs when the vulnerability ticket remains open (not Verified/Closed) one business day past the defined SLA.

Escalation Step	Action Taken	Responsible Party	Timeline (After SLA Breach)
Level 1 (Automated Warning)	Automated email/ticket warning sent to **Technical Owner (TO)** and **Asset Owner (AO)**, requiring an updated remediation plan and reason for delay.	**Vulnerability Management (VM) Team**	**1 Day After Breach**
Level 2 (Formal Escalation)	Formal report to the **Manager** of the Technical Owner, with a copy to the **Director** of the Technical Owner's division. This requires the TO Manager to provide a written commitment for resolution within 5 business days.	**VM Team Lead**	**3 Days After Breach**
Level 3 (Risk Review)	The vulnerability is presented to the **Risk Committee**. For **CRIT/HIGH** breaches, the **CISO** may mandate resource reallocation or temporary **system suspension/isolation** until remediation is complete.	**CISO/VP of Engineering**	**7 Days After Breach**

---

9. Monthly Metrics Review Process

This section defines the KPIs used to measure the effectiveness of the vulnerability program and the formal reporting structure.

9.1 Key Performance Indicators (KPIs) Tracked

KPI	Definition	Target/Goal
KPI 1: Mean Time To Remediate (MTTR)	Average time taken to close all vulnerabilities (calculated separately for CRIT/HIGH/MED).	**Decrease by 5% quarterly.**
KPI 2: SLA Adherence Rate	Percentage of vulnerabilities closed within their defined SLA window.	**95% for CRIT/HIGH; 90% for MED/LOW.**

KPI 3: Vulnerability Backlog Trend	Net change in the total number of open vulnerabilities month-over-month.	**Net Reduction (Remediated > Discovered).**
KPI 4: CRIT/HIGH Density on P0/P1	The total number of open Critical/High vulnerabilities specifically on high-value (P0/P1) assets.	**Maintain a total count of < 20.**

9.2 Monthly Reporting and Review Process

Activity	Detail	Responsibility	Receives the Report
Data Aggregation	Collect all KPI data, focusing on trends, SLA failures, and the top 5 longest-open vulnerabilities.	**Vulnerability Analyst**	-
Report Generation	Prepare a dashboard/report including an executive summary and detailed failure analysis (e.g., which teams or assets are consistently missing SLA).	**VM Team Lead**	-
Metrics Review Meeting	Formal meeting to review the program's health, discuss resources, and assign clear action items for poor performance areas.	**VM Team Lead**	**CISO, VP of IT/Engineering, Risk Committee, Key Department Directors.**