**Cybersecurity Templates**

**Major Issue Report Model**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Major Issue Report Model** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document ID:** | SEC‑MIR‑[####] | **Owner (Service/Process):** | [Name, Role] |
| **Reviewed By:** | [CIRT Lead / Problem Manager / Legal Counsel] | **Approved By:** | [CISO or Delegate] |

Contents

[Major Issue Report Model 4](#_Toc207145144)

[1. Executive Summary 4](#_Toc207145145)

[2. Issue Overview 4](#_Toc207145146)

[3. Business & Security Impact 5](#_Toc207145147)

[4. Timeline of Events 5](#_Toc207145148)

[5. Technical Context & Evidence 5](#_Toc207145149)

[6. Root Cause Analysis (RCA) 6](#_Toc207145150)

[7. Risk Assessment 6](#_Toc207145151)

[8. Communications, Legal & Compliance 6](#_Toc207145152)

[9. Actions & Outcomes 6](#_Toc207145153)

[9.1 Actions Executed (Containment/Eradication/Recovery) 6](#_Toc207145154)

[9.2 Workarounds (Temporary) 7](#_Toc207145155)

[9.3 Corrective & Preventive Actions (CAPA) 7](#_Toc207145156)

[10. Metrics & Post‑Incident Review 8](#_Toc207145157)

[11. Approvals 8](#_Toc207145158)

[Appendices 8](#_Toc207145159)

[Appendix A — Attachments & Evidence Index 8](#_Toc207145160)

[Appendix B — Affected Assets List 8](#_Toc207145161)

[Appendix C — Major Issue Register (Extract) 9](#_Toc207145162)

[Appendix D — Communications Log 9](#_Toc207145163)

[Appendix E — Glossary & Acronyms (excerpt) 9](#_Toc207145164)

[Appendix F — References & Cross‑Links 9](#_Toc207145165)

# Major Issue Report Model

# 1. Executive Summary

* **What happened:** [1–3 sentences stating the precipitating event and immediate impact.]
* **Current status:** [Stable/Degraded/Recovering].
* **Security impact:** [Data class affected, confidentiality/integrity/availability impact.]
* **Business impact:** [Services/customers affected, downtime (hh: mm), financial estimate (range).]
* **Cause (current view):** [Suspected root cause or unknown pending RCA.]
* **Key actions taken:** [Containment highlights; comms sent.]
* **Next steps & owners (24–72h):** [Top 3 prioritized items with owners/D‑dates.]
* **Ask/Decision needed:** [Budget, exception, approval, media/notification, etc.]

# 2. Issue Overview

* **Issue ID/Title:** [MIR‑2025‑0001 — e.g., “Unauthorized access to payment database”]
* **Category:** ☐ Major Incident ☐ Vulnerability Exposure ☐ Compliance Breach ☐ Degradation ☐ Other: […]
* **Detection Source:** [EDR/SIEM alert, user report, audit, third-party notice, regulator]
* **First Seen:** [YYYY‑MM‑DD HH: MM]
* **Last Seen/Ended:** [YYYY‑MM‑DD HH: MM]
* **Affected Services/Assets:** [Service names, Asset IDs, versions, regions]
* **Customer/Regulatory Touchpoints:** [Y/N] (details in Section H)

**Severity & Priority**

* **Impact:** [Critical/Major/Moderate/Minor] — describe user/business effect (e.g., % outage, data scope).
* **Urgency:** [Immediate / High / Normal] — time sensitivity.
* **Priority (derived):** [P1/P2/P3] — **SLA:** response [x]h, closure target [y]h.

**Key Metrics**

* **Dwell Time:** [first compromise → detection]
* **MTTD / MTTR:** [hh:mm]
* **Records/Data at Risk:** [# est.]
* **Attack Surface Notes:** [exposed port/cert/credential, etc.]

# 3. Business & Security Impact

* **Customers/Users affected:** [counts, cohorts]
* **Data exposure:** [classification, types of PII/PHI/PCI; encryption state; exfiltration evidence]
* **Operational impact:** [SLO breach, orders delayed, transactions failed]
* **Financial estimate:** [range and assumptions]
* **Regulatory/Contractual implications:** [breach notification windows; contract clauses]
* **Public/Media posture:** [low/medium/high interest; social mentions if relevant]

Attach supporting exhibits in **Appendix A**. Use quantitative measures where possible.

# 4. Timeline of Events

| **Date/Time (TZ)** | **Actor** | **Event** | **Evidence Ref** |
| --- | --- | --- | --- |
| 2025‑08‑24 03:42 | SIEM | Alert: anomalous admin login from geo X | A‑03 |
| 2025‑08‑24 03:45 | CIRT | Triage began; isolated host **srv‑db‑12** | A‑05 |
| … | … | … | … |

Reference attachments by **ID** in Appendix A; keep this factual and time‑ordered.

# 5. Technical Context & Evidence

* **Environment Summary:** [Architecture diagram ref; versions; dependencies.]
* **Impacted Components:** [hosts, containers, DBs, queues, external APIs; build/version; region.]
* **Indicators of Compromise (IoCs):** [hashes, IPs, domains, file paths]
* **MITRE ATT&CK Mapping:** [e.g., Initial Access T1190 → Execution T1059 → Exfiltration T1041]
* **Evidence Handling:** Collected by [name] using [tool]; **chain‑of‑custody** recorded; **hashes** stored in case file.

# 6. Root Cause Analysis (RCA)

* **Method:** ☐ 5‑Whys ☐ Fault Tree ☐ Fishbone ☐ Post‑Incident Review (PIR)
* **Proximate Cause:** [describe]
* **Contributing Factors:** [patch backlog, misconfig, monitoring gap, vendor failure, process lapse]
* **Why detection didn’t stop it sooner:** [coverage limits, noisy alerts, no rule, etc.]
* **Escaped Defect Analysis:** [what testing/controls failed to catch this]

If the root cause is not yet confirmed, note **assumptions**, evidence gaps, and ETA for final RCA.

# 7. Risk Assessment

|  |  |  |  |
| --- | --- | --- | --- |
| **Dimension** | **Before Containment** | **After Containment** | **Notes** |
| Likelihood | High/Med/Low | High/Med/Low | Basis (telemetry, exposure) |
| Impact | High/Med/Low | High/Med/Low | Basis (data scope, downtime) |
| Residual Risk | — | High/Med/Low | Acceptance needed? (Y/N) |

**Decision:** ☐ Accept (temporary) ☐ Mitigate ☐ Transfer ☐ Avoid  
**Approver:** [Name/Role] — **Expiry:** [date] (record in Exception Register)

# 8. Communications, Legal & Compliance

* **Internal Comms:** [exec brief schedule; channel; recipients]
* **External Comms:** [customer notice, status page, PR; approval steps]
* **Regulatory:** [e.g., GDPR 72‑hour notice; sector regulators; AG offices] —
* **Deadline(s):** [date/time]
* **Legal Hold:** ☐ Applied ☐ Not required — **Case ID:** [if any]
* **Third Parties:** [vendors notified; ticket/bridge refs]

# 9. Actions & Outcomes

## 9.1 Actions Executed (Containment/Eradication/Recovery)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Action** | **Owner** | **Start** | **End** | **Result/Evidence** |
| Disable compromised account; rotate keys | IAM Lead | … | … | A‑07 |
| Patch CVE‑XXXX‑YYYY | Platform Eng | … | … | A‑11 |
| Restore from snapshot (srv‑db‑12) | Ops | … | … | A‑15 |

## 9.2 Workarounds (Temporary)

* **Description:** [e.g., rate‑limit API endpoint / disable non-essential feature]
* **Risks/Side effects:** [degraded UX, backlog growth]
* **Removal Criteria:** [metric threshold/date]

## 9.3 Corrective & Preventive Actions (CAPA)

| **#** | **Action** | **Type** | **Success Metric** | **Owner** | **Status** |
| --- | --- | --- | --- | --- | --- |
| 1 | Enforce MFA on admin VPN | Preventive |  |  |  |
| ≥ 99% MFA on admin accounts | Sec Eng | 2025‑09‑15 | Open |  |  |
| 2 | Add SIEM rule for anomalous geo/login | Corrective |  |  |  |
| False‑positive rate < 2% | SOC | 2025‑09‑05 | In progress |  |  |
| 3 | Patch pipeline for critical CVEs ≤ 7d | Preventive |  |  |  |
| SLA compliance ≥ 95% | Platform | 2025‑10‑01 | Planned |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Ensure each action is **SMART** (specific, measurable, achievable, relevant, time-bound).

# 10. Metrics & Post‑Incident Review

* **MTTD:** [hh: mm]; **MTTR:** [hh: mm]; **Containment Time:** [hh: mm].
* **Service impact:** [uptime %, error rate delta, SLO breach]
* **Data impact:** [records confirmed, suspected]
* **Lessons Learned:** [top 3; actionable]
* **Follow-up Reviews:** PIR date: [YYYY‑MM‑DD]; CAB review: [YYYY‑MM‑DD]

# 11. Approvals

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Name | Date | Signature/Consent |

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Name** | **Date** | **Signature/Consent** |
| Prepared By |  |  |  |
| Reviewed By (CIRT Lead) |  |  |  |
| Reviewed By (Legal) |  |  |  |
| Approved By (CISO) |  |  |  |

# Appendices

## Appendix A — Attachments & Evidence Index

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **File/Artifact** | **Hash (SHA‑256)** | **Description** | **Source/Path** |
| A‑03 | siem‑alert‑geo‑anomaly.json | [hash] | Initial alert payload | /cases/MIR‑2025‑0001/… |
| A‑05 | console‑session‑video.mp4 | [hash] | Isolation session recording | … |
| A‑11 | patch‑report‑srv‑db‑12.pdf | [hash] | Patch evidence | … |

**Evidence Handling Notes:** Tools used, collector(s), chain‑of‑custody steps.

## Appendix B — Affected Assets List

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset ID** | **Hostname** | **Service** | **Location/Zone** | **Owner** | **Data Classification** |
| srv‑db‑12 | … | Payments DB | Prod‑EU‑1 | DBA Team | Restricted |

## Appendix C — Major Issue Register (Extract)

Maintain a rolling log of open/closed **Major Issues** to support governance and trend analysis.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Category** | **Title** | **Description** | **Status** | **Action Details** | | **Urgency** | **Impact** | **Size/Scope** | **Target Date** | **Issue Owner** |
| MIR‑2025‑0001 | Security | Unauthorized DB access | … | Open | CAPA #1‑#3 | High | | High | 1 svc / EU‑1 | 2025‑09‑15 | CIRT Lead |

## Appendix D — Communications Log

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date/Time** | **Channel** | **Audience** | **Summary** | **Owner** |
|  |  |  |  |  |

## Appendix E — Glossary & Acronyms (excerpt)

* **CIRT:** Cyber Incident Response Team
* **CAPA:** Corrective & Preventive Actions
* **CAB:** Change Advisory Board
* **DLP:** Data Loss Prevention
* **PIR:** Post‑Implementation Review
* **SoR:** System of Record

## Appendix F — References & Cross‑Links

* Incident #[…]
* Change #[…]
* Problem #[…]
* Risk #[…]
* Policy/Standard references: [Incident Management], [Vulnerability Mgmt], [Records/Retention]