# **Security Incident Classification Matrix**

**Version:** 1.0

**Datum:** [Einfügedatum]

**Verantwortlich:** SOC Manager

**Genehmigt durch:** [Name des Sicherheitsbeauftragten]

## **1. Zweck der Matrix**

Die Security Incident Classification Matrix dient der standardisierten Bewertung und Klassifizierung von Sicherheitsvorfällen basierend auf ihrer Kritikalität, ihrem Umfang und ihrer Auswirkung. Diese Klassifizierung hilft dabei, die geeigneten Reaktionsmaßnahmen zu bestimmen, Ressourcen effizient zuzuweisen und die Eskalation zu steuern.

## **2. Geltungsbereich**

Die Matrix gilt für alle Sicherheitsvorfälle, die im SOC gemeldet werden, einschließlich:

• Technischer Vorfälle (z. B. Malware, DDoS-Angriffe).

• Physischer Vorfälle (z. B. unbefugter Zugang).

• Compliance-Vorfälle (z. B. Datenschutzverletzungen).

## **3. Kriterien für die Klassifizierung**

Die Matrix basiert auf folgenden Kriterien:

• **Kritikalität:** Wie schwerwiegend ist der Vorfall für die Organisation?

• **Umfang:** Wie viele Systeme, Benutzer oder Standorte sind betroffen?

* **Auswirkungen:** Welche Auswirkungen hat der Vorfall auf Verfügbarkeit, Vertraulichkeit und Integrität?

• **Wiederherstellungszeit:** Wie lange dauert es, den Vorfall zu beheben?

## **4. Klassifizierungsstufen**

|  |  |  |
| --- | --- | --- |
| **Stufe** | **Beschreibung** | **Beispiele** |
| Niedrig | Begrenzt auf einen einzelnen Benutzer oder ein System. Keine signifikante Auswirkung auf die Organisation. | Phishing-E-Mail, die keinen Schaden verursacht. |
| Mittel | Beeinträchtigt mehrere Benutzer oder Systeme. Mögliche Auswirkungen auf die Produktivität. | Malware auf einem Endpunkt ohne Ausbreitung. |
| Hoch | Beeinträchtigt kritische Systeme oder Daten. Potenziell große Auswirkungen auf die Organisation. | Ransomware-Angriff auf Produktionsserver. |
| Kritisch | Organisation weit betroffen. Schwerwiegende Auswirkungen auf Verfügbarkeit, Integrität oder Vertraulichkeit. | Datenexfiltration oder kompletter Netzwerkausfall. |

## **5. Klassifizierungsmatrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kriterium | Niedrig | Mittel | Hoch | Kritisch |
| Betroffene Systeme | Einzelner Endpunkt | Mehrere Endpunkte | Kritische Systeme | Gesamte Organisation |
| Betroffene Benutzer | 1–5 Benutzer | 6–50 Benutzer | >50 Benutzer | Alle Benutzer |
| Auswirkungen | Keine | Leichte Einschränkungen | Bedeutende Einschränkungen | Geschäfts-unterbrechung |
| Wiederherstellungs-zeit | <1 Stunde | 1–4 Stunden | 4–24 Stunden | >24 Stunden |

## **6. Eskalationspfad basierend auf Klassifizierung**

|  |  |  |  |
| --- | --- | --- | --- |
| **Stufe** | **Aktion** | **Verantwortliche Rollen** | **Stufe** |
| **Niedrig** | Lokale Untersuchung und Dokumentation. Keine Eskalation notwendig. | SOC Tier 1 Analyst | **Niedrig** |
| **Mittel** | Untersuchung und Eskalation an Tier 2. Benachrichtigung des betroffenen Teams. | SOC Tier 2 Analyst | **Mittel** |
| **Hoch** | Sofortige Eskalation an SOC Tier 3 und Sicherheitsbeauftragten. Eröffnung eines Major Incidents. | SOC Tier 3 Analyst, Sicherheitsbeauftragter | **Hoch** |
| **Kritisch** | Aktivierung des Incident Response Teams und Eskalation an das Management. | Incident Response Team, SOC Manager | **Kritisch** |

## **7. Monitoring und Reporting**

• **Dashboards:** SOC-Dashboards zeigen die Verteilung der Vorfälle nach Klassifizierung.

• **Berichte:** Monatliche Reports an das Management enthalten Statistiken über Vorfälle und ihre Klassifizierungen.

• **KPIs:**

• Anzahl der Vorfälle je Stufe.

• Mittlere Zeit zur Eskalation (MTTE).

• Mittlere Zeit zur Behebung (MTTR).

## **8. Überprüfung und Aktualisierung**

Diese Matrix wird mindestens einmal jährlich oder bei Bedarf überprüft und aktualisiert. Änderungen werden vom SOC Manager und dem Sicherheitsbeauftragten genehmigt.

## **9. Anhang: Beispiele für Vorfälle**

|  |  |
| --- | --- |
| **Stufe** | **Beispiele** |
| **Niedrig** | Spam-E-Mail, die blockiert wurde. |
| **Mittel** | Verdächtige Anmeldung von einem unbekannten Gerät. |
| **Hoch** | Angriff mit einem bekannten Exploit auf einen Webserver. |
| **Kritisch** | Datenleck mit sensiblen Kundendaten, Verschlüsselung des gesamten Netzwerks durch Ransomware. |