# **RACI Chart: Incident Response Prozess**

## **Definition der RACI-Matrix**

Ein RACI Chart definiert Rollen und Verantwortlichkeiten innerhalb eines Prozesses. Jede Aufgabe wird einer oder mehreren Rollen zugeordnet, wobei folgende Verantwortlichkeiten gelten:

• **R** (Responsible): Verantwortlich für die Ausführung der Aufgabe.

* **A** (Accountable): Letztlich verantwortlich, genehmigt Entscheidungen und trägt die Rechenschaft.

• **C** (Consulted): Berät und liefert Input, bevor Entscheidungen getroffen werden.

• **I** (Informed): Wird über Fortschritte und Ergebnisse informiert.

## **RACI Chart für den Incident Response Prozess**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Phase -ID** | **SOC Analyst (Tier-1)** | **SOC Analyst (Tier-2)** | **Incident Response Manager** | **Systemadministrator** | **Compliance Officer** | **Geschäfts-führung** |
| Erkennung und Analyse | R | C | A | I | I | I |
| Überwachung von Logs | R | C | I | I | I | I |
| Alarmanalyse | R | C | A | I | I | I |
| Hypothesenbildung | R | C | A | I | I | I |
| Eindämmung | C | R | A | R | I | I |
| Isolierung betroffener Systeme | C | R | A | R | I | I |
| Sperrung kompromittierter Konten | C | R | A | I | I | I |
| Blockierung bösartiger IPs | C | R | A | I | I | I |
| Beseitigung | I | R | A | R | I | I |
| Malware-Entfernung | I | R | A | R | I | I |
| Wiederherstellung aus Backups | I | R | A | R | I | I |
| Schwachstellenbehebung | I | R | A | R | I | I |
| Nachbereitung | I | R | A | C | R | C |
| Erstellung des Post Mortem Reports | I | R | A | C | R | I |
| Lessons Learned | I | C | A | C | R | I |
| Optimierung von Playbooks | I | C | A | C | R | I |
| Kommunikation | I | I | A | I | C | R |
| Interne Kommunikation | I | I | A | I | C | R |
| Externe Kommunikation | I | I | A | I | C | R |

## **Erläuterungen:**

1. **SOC Analyst (Tier-1):**

* Primäre Verantwortung für die Überwachung und initiale Analyse von Sicherheitsvorfällen.

2. **SOC Analyst (Tier-2):**

* Validiert Vorfälle und führt weiterführende Analysen sowie Eindämmungsmaßnahmen durch.

3. **Incident Response Manager:**

* Übernimmt die strategische Verantwortung und koordiniert den gesamten Prozess.

4. **Systemadministrator:**

* Führt technische Maßnahmen wie Isolierung, Beseitigung und Wiederherstellung durch.

5. **Compliance Officer:**

* Berät bei regulatorischen Anforderungen und überwacht die Einhaltung von Vorschriften.

6. **Geschäftsführung:**

* Wird informiert und ist für strategische Entscheidungen sowie externe Kommunikation verantwortlich.