# **SOC Training Plan**

**Version:** 1.0

**Datum:** [Einfügedatum]

**Verantwortlich:** SOC Manager

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

## **1. Zweck des Training Plans**

Dieser Training Plan dient dazu, die Fähigkeiten und das Wissen der SOC-Mitarbeiter kontinuierlich zu erweitern. Ziel ist es, die Effektivität des SOCs zu steigern, Bedrohungen schneller zu erkennen und darauf zu reagieren sowie regulatorische Anforderungen zu erfüllen.

## **2. Geltungsbereich**

Der Plan gilt für:

• Alle SOC-Mitarbeiter (Tier 1 bis Tier 3).

• Neue SOC-Mitarbeiter während der Einarbeitungsphase.

• Externe Partner, die regelmäßig mit dem SOC zusammenarbeiten.

## **3. Trainingsziele**

1. Vermittlung grundlegender und fortgeschrittener Fähigkeiten in Bedrohungserkennung, Incident Response und Threat Hunting.
2. Regelmäßige Aktualisierung des Wissens über neue Angriffsvektoren und Bedrohungen.
3. Verbesserung der Nutzung und Verwaltung von SOC-Tools wie SIEM, SOAR und Threat Intelligence Plattformen.
4. Erfüllung von Compliance-Anforderungen wie NIS2, ISO 27001 und DORA durch dokumentierte Schulungen.

## **4. Trainingsmodule**

|  |  |  |  |
| --- | --- | --- | --- |
| **Modul** | **Inhalt** | **Zielgruppe** | **Dauer** |
| Einführung in das SOC | Grundlagen des SOC-Betriebs, Rollen und Verantwortlichkeiten. | Neue Mitarbeiter | 1 Tag |
| SIEM-Schulung | Nutzung von Tools wie Elastic SIEM, Splunk, Wazuh für Log-Analyse und Bedrohungserkennung. | Alle SOC-Mitarbeiter | 2 Tage |
| Incident Response Basics | Incident Management Prozesse, Eskalation, Phasen der Incident Response. | Tier 1 & Tier 2 | 2 Tage |
| Threat Hunting | Identifikation von Bedrohungen in Log-Daten und Netzwerken. | Tier 2 & Tier 3 | 3 Tage |
| Advanced Threat Intelligence | Nutzung von Plattformen wie MISP, openCTI und IoC-Management. | Tier 3 | 2 Tage |
| Red Teaming und Forensik | Grundlagen des Red Teamings und IT-Forensik mit Tools wie Autopsy und Volatility. | Tier 3 | 3 Tage |
| Compliance und Reporting | Schulung zu Compliance-Frameworks wie ISO 27001, NIS2, DORA, Erstellung von Berichten. | Alle SOC-Mitarbeiter | 1 Tag |

## **5. Methodik und Tools**

**5.1 Schulungsmethodik**

• **Theorie:** Vermittlung grundlegender Konzepte und Prozesse.

• **Praxis:** Hands-on-Übungen in einer simulierten Umgebung.

• **Workshops:** Interaktive Sessions zur Vertiefung spezifischer Themen.

**5.2 Tools für die Schulung**

• **SIEM-Tools:** Elastic Stack, Splunk, Wazuh.

• **SOAR-Tools:** Shuffle, Cortex XSOAR.

• **Threat Intelligence:** MISP, openCTI.

• **Forensik-Tools:** Autopsy, Volatility, Wireshark.

## **6. Trainingskalender**

|  |  |
| --- | --- |
| **Monat** | **Trainings** |
| Januar | Einführung in das SOC, SIEM-Schulung. |
| März | Incident Response Basics, Threat Hunting. |
| Juni | Advanced Threat Intelligence, Red Teaming und Forensik. |
| September | Compliance und Reporting, Refresher zu Incident Response. |
| Dezember | Jahresabschluss-Übung: Tabletop Exercise & Simulation eines kritischen Sicherheitsvorfalls. |

## **7. Tabletop-Übungen und Simulationen**

• **Thema:** Ransomware-Angriff auf kritische Systeme.

• **Ziel:** Test der Reaktionszeit und des Wissens der Mitarbeiter.

* **Durchführung:** Simulierte Angriffe in einer kontrollierten Umgebung mit anschließender Auswertung.

## **8. Zertifizierungen und Weiterbildungen**

|  |  |
| --- | --- |
| **Zertifizierung** | **Beschreibung** |
| **Certified SOC Analyst (CSA)** | Grundkenntnisse im SOC-Betrieb. |
| **Certified Incident Responder (eCIR)** | Fähigkeiten in Incident Response und Forensik. |
| **Blue Team Level 2 (BTL2)** | Erweiterte Fähigkeiten in Threat Hunting und Forensik. |
| **Certified Threat Hunter (eCTHP)** | Spezialisierung auf Threat Hunting in komplexen Umgebungen. |

## **9. Erfolgsmessung**

• **KPIs:**

• Anzahl erfolgreich abgeschlossener Trainings.

• Verbesserte Mean Time to Detect (MTTD) und Mean Time to Respond (MTTR).

• Mitarbeiterzufriedenheit nach Schulungen.

• **Evaluierung:**

* Regelmäßige Tests und praktische Übungen, um den Fortschritt der Mitarbeiter zu messen.

• Feedback-Umfragen nach jedem Training.

## **10. Überprüfung und Aktualisierung**

Dieser Trainingsplan wird jährlich überprüft und bei Bedarf aktualisiert, um den neuesten Entwicklungen und Bedrohungen gerecht zu werden.