# **Tabletop Exercise Playbook**

**Version:** 1.0

**Datum:** [Einfügedatum]

**Verantwortlich:** SOC Manager

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

## **1. Zweck des Playbooks**

Dieses Playbook dient als Leitfaden zur Durchführung von Tabletop-Übungen (TTX), um die Reaktionsfähigkeit des Security Operations Centers (SOC) und anderer beteiligter Teams zu testen und zu verbessern. Ziel ist es, Bedrohungsszenarien in einer kontrollierten Umgebung durchzuspielen, Schwachstellen aufzudecken und die Zusammenarbeit zu fördern.

## **2. Geltungsbereich**

Dieses Playbook gilt für:

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

• Incident Response Teams.

• Externe Partner und Drittanbieter, sofern sie in den Übungen involviert sind.

## **3. Ziele der Tabletop-Übung**

1. Test der Incident Response Pläne und Prozesse.

2. Verbesserung der Kommunikation zwischen beteiligten Teams.

3. Identifikation von Lücken in der Reaktionsstrategie.

4. Förderung eines proaktiven Ansatzes zur Sicherheitsabwehr.

5. Stärkung der organisatorischen Resilienz.

## **4. Übungsszenarien**

|  |  |
| --- | --- |
| **Szenario** | **Beschreibung** |
| Ransomware-Angriff | Simuliert die Verschlüsselung kritischer Systeme durch eine Malware. |
| Phishing-Angriff | Szenario eines erfolgreichen Phishing-Angriffs mit gestohlenen Zugangsdaten. |
| Datenexfiltration | Angreifer laden sensible Daten aus einem internen System herunter. |
| Insider Threat | Ein Mitarbeiter mit privilegierten Rechten missbraucht seine Zugriffsrechte. |
| Distributed Denial of Service (DDoS) | Ein großangelegter Angriff, der kritische Systeme und Services lahmlegt. |

## **5. Übungsstruktur**

**5.1 Vorbereitung**

• Auswahl des Szenarios durch den SOC Manager.

• Erstellung eines detaillierten Übungsplans, einschließlich:

• Ziel der Übung.

• Beteiligte Teams und Rollen.

• Tools und Ressourcen.

• Briefing der Teilnehmer über das Szenario und die Regeln der Übung.

**5.2 Durchführung**

1. **Einleitung:**

• Der Übungsleiter beschreibt das Szenario und startet die Übung.

2. **Simulierte Ereignisse:**

• Das Übungsteam erhält schrittweise neue Informationen (z. B. Logs, Alerts).

3. **Reaktion:**

* Die Teilnehmer diskutieren und dokumentieren ihre Reaktionen basierend auf den Incident Response Plänen.

4. **Entscheidungsfindung:**

• Teams treffen Entscheidungen zur Eindämmung, Analyse und Wiederherstellung.

**5.3 Nachbesprechung (Debriefing)**

• Diskussion der Ergebnisse mit allen Teilnehmern.

• Identifikation von Stärken und Schwächen.

• Erstellung eines Abschlussberichts mit Lessons Learned und Handlungsempfehlungen.

## **6. Rollen und Verantwortlichkeiten**

|  |  |
| --- | --- |
| **Rolle** | **Verantwortlichkeiten** |
| **Übungsleiter** | Planung, Durchführung und Moderation der Übung. |
| **SOC Analysten** | Simulation der Echtzeitreaktion auf die Bedrohung. |
| **Incident Response Team** | Umsetzung der Reaktionsmaßnahmen und Koordination mit anderen Teams. |
| **Beobachter** | Dokumentation der Diskussionen und Identifikation von Verbesserungspotenzialen. |
| **Management** | Bewertung der strategischen Entscheidungen und Eskalationsprozesse. |

## **7. Tools und Ressourcen**

• **SIEM:** Wazuh, Elastic, Splunk für simulierte Logs.

• **Threat Intelligence:** MISP, openCTI zur Integration von IoCs (Indicators of Compromise).

• **Kommunikationstools:** Microsoft Teams, Slack.

• **Dokumentation:** Playbooks, Incident Response Pläne.

## **8. Erfolgsmessung**

**8.1 Bewertungskriterien**

* **Reaktionszeit:** Zeit vom Erkennen des Vorfalls bis zur ersten Maßnahme.
* **Eskalationsprozess:** Effizienz und Genauigkeit der Eskalation.
* **Kommunikation:** Klarheit und Effektivität der internen und externen Kommunikation.
* **Wiederherstellungszeit:** Zeit bis zur vollständigen Wiederherstellung der betroffenen Systeme.

**8.2 KPIs**

* Anzahl der erfolgreich umgesetzten Maßnahmen.
* Mittlere Zeit zur Eskalation (MTTE).
* Mittlere Zeit zur Wiederherstellung (MTTR).

## **9. Abschlussbericht**

Nach jeder Übung wird ein detaillierter Bericht erstellt, der Folgendes enthält:

1. **Übersicht:** Szenario, Beteiligte, Ziele.

2. **Ergebnisse:** Bewertung der Reaktion und Entscheidungen.

3. **Stärken:** Aspekte, die gut funktioniert haben.

4. **Schwächen:** Identifizierte Lücken oder Probleme.

5. **Empfehlungen:** Konkrete Maßnahmen zur Verbesserung der Prozesse und Fähigkeiten.

## **10. Überprüfung und Aktualisierung**

Dieses Playbook wird regelmäßig überprüft und bei Bedarf aktualisiert, um die neuesten Bedrohungen und Best Practices zu berücksichtigen.