# **SOC Charter**

## **1. Einführung**

**Zweck der SOC Charter:**

Die SOC Charter definiert die Mission, Ziele, Verantwortlichkeiten und den organisatorischen Rahmen des Security Operations Centers (SOC). Sie dient als Leitfaden für alle SOC-Aktivitäten und stellt sicher, dass das SOC seine Rolle effektiv und effizient erfüllt.

## **2. Mission und Vision**

**Mission:**

Das Security Operations Center (SOC) ist dafür verantwortlich, die Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme und Daten des Unternehmens zu schützen. Dies wird durch kontinuierliche Überwachung, proaktive Bedrohungserkennung, effektive Reaktion auf Vorfälle und Zusammenarbeit mit anderen Teams erreicht.

**Vision:**

Das SOC strebt danach, ein hochmodernes und proaktives Zentrum für Cybersicherheitsoperationen zu sein, das in der Lage ist, Bedrohungen frühzeitig zu erkennen, schnell darauf zu reagieren und die Sicherheitslage des Unternehmens kontinuierlich zu verbessern.

## **3. Geltungsbereich**

Die SOC Charter gilt für:

1. Alle IT-Systeme, Netzwerke, Anwendungen und Daten des Unternehmens.
2. Alle internen und externen Mitarbeiter, Auftragnehmer und Partner, die mit dem SOC interagieren.
3. Alle Sicherheitsvorfälle, die Vertraulichkeit, Integrität oder Verfügbarkeit beeinträchtigen können.

## **4. Ziele**

* **Überwachung:** Kontinuierliche Überwachung der IT-Infrastruktur, um Bedrohungen in Echtzeit zu erkennen.
* **Bedrohungserkennung:** Einsatz modernster Technologien und Threat Intelligence, um bekannte und unbekannte Bedrohungen zu identifizieren.
* **Vorfallsmanagement:** Effektive Reaktion auf Sicherheitsvorfälle, um Schäden zu minimieren und den Betrieb schnell wiederherzustellen.
* **Schwachstellenmanagement:** Identifizierung und Behebung von Schwachstellen in der IT-Infrastruktur.
* **Compliance:** Unterstützung bei der Einhaltung regulatorischer Anforderungen wie ISO 27001, NIS2, DORA und GDPR.
* **Zusammenarbeit:** Enge Zusammenarbeit mit IT-, Compliance- und Geschäftsführungsteams.

## **5. Verantwortlichkeiten**

Das SOC ist verantwortlich für:

1. **Bedrohungsüberwachung:**

• Nutzung von SIEM, EDR und SOAR-Tools zur kontinuierlichen Überwachung.

• Analysieren von Protokollen, Alarmen und Anomalien.

2. **Vorfallsmanagement:**

• Erkennen, Analysieren, Eindämmen und Beheben von Sicherheitsvorfällen.

• Koordinieren der Incident Response mit internen und externen Stakeholdern.

3. **Schwachstellenmanagement:**

• Regelmäßige Schwachstellenscans und Priorisierung von Maßnahmen.

• Zusammenarbeit mit IT-Teams zur Implementierung von Sicherheits-Patches.

4. **Reporting:**

• Erstellung regelmäßiger Berichte zur Sicherheitslage und Vorfällen.

• Bereitstellung von Compliance-Berichten an die Geschäftsführung.

5. **Awareness und Training:**

• Schulung der Mitarbeiter zu sicherheitsrelevanten Themen.

• Durchführung von Phishing-Simulationen und Tabletop-Übungen.

## **6. Governance**

**Organisatorische Struktur:**

Das SOC ist Teil der IT-Sicherheitsabteilung und berichtet direkt an den CISO.

**Hierarchie im SOC:**

1. **SOC Manager:** Verantwortlich für die strategische Leitung und Berichterstattung.

2. **Tier-1 Analysten:** Überwachung und erste Analyse von Sicherheitsvorfällen.

3. **Tier-2 Analysten:** Vertiefte Analyse, Eindämmung und Behebung von Vorfällen.

4. **Tier-3 Analysten:** Spezialisten für komplexe Vorfälle und Forensik.

**Zusammenarbeit:**

Das SOC arbeitet eng mit folgenden Abteilungen zusammen:

• IT-Abteilung: Für technische Maßnahmen wie Patching oder Konfigurationsänderungen.

• Compliance-Abteilung: Für regulatorische Berichterstattung und Audits.

• Geschäftsführung: Für strategische Entscheidungen und Eskalationen.

## **7. Prozesse und Workflows**

Das SOC orientiert sich an standardisierten Prozessen, um konsistente Ergebnisse sicherzustellen. Dazu gehören:

1. **Incident Response Prozess:**

• Standardisierte Playbooks für verschiedene Vorfallsarten.

2. **Threat Hunting:**

• Proaktive Suche nach versteckten Bedrohungen in der IT-Infrastruktur.

3. **Schwachstellenmanagement:**

• Identifikation, Bewertung und Behebung von Schwachstellen.

4. **Reporting:**

• Regelmäßige Erstellung von Berichten für interne und externe Stakeholder.

## **8. Tools und Technologien**

Das SOC nutzt folgende Technologien, um seine Aufgaben effektiv zu erfüllen:

• **SIEM:** Elastic Security, Splunk, Wazuh.

• **EDR/XDR:** CrowdStrike, SentinelOne.

• **SOAR:** Automatisierung und Orchestrierung von Sicherheitsprozessen.

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

• **Case Management Tools:** TheHive, DFIR-IRIS.

## **9. Metriken und KPIs**

Das SOC misst seine Leistung anhand folgender Kennzahlen:

* **Mean Time to Detect (MTTD):** Durchschnittliche Zeit bis zur Erkennung eines Vorfalls.
* **Mean Time to Respond (MTTR):** Durchschnittliche Zeit bis zur Eindämmung eines Vorfalls.
* **Anzahl erkannter Vorfälle:** Monatlich identifizierte Sicherheitsvorfälle.
* **Anzahl geschlossener Schwachstellen:** Pro Monat behobene Schwachstellen.
* **Awareness-Level:** Ergebnisse regelmäßiger Phishing-Tests und Schulungen.

## **10. Weiterentwicklung**

Das SOC verpflichtet sich zur kontinuierlichen Verbesserung durch:

1. Regelmäßige Audits und Überprüfungen der Prozesse.

2. Fortbildung und Zertifizierung der SOC-Mitarbeiter.

3. Integration neuer Technologien und Tools zur Steigerung der Effektivität.

4. Anpassung der Playbooks und Richtlinien basierend auf Lessons Learned.

## **11. Genehmigung**

Diese SOC Charter wurde von der Geschäftsführung genehmigt und ist ab dem [Datum] gültig.

**Genehmigt durch:**

[Name der Führungskraft]

[Position]

[Datum]

[Unterschrift]