# **Threat Intelligence Sharing Policy**

**Version:** 1.0

**Datum:** [Einfügedatum]

**Verantwortlich:** SOC Manager

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

## **1. Zweck der Policy**

Diese Threat Intelligence Sharing Policy definiert die Regeln und Verfahren für die Sammlung, Analyse, Nutzung und Weitergabe von Bedrohungsinformationen. Ziel ist es, die Sicherheit der Organisation zu verbessern, indem relevante Informationen über Bedrohungen innerhalb der Organisation und mit externen Partnern sicher und effizient geteilt werden.

## **2. Geltungsbereich**

Diese Policy gilt für:

• Alle SOC-Mitarbeiter, die Bedrohungsinformationen sammeln und nutzen.

• Externe Partner, die Threat Intelligence teilen oder empfangen.

• Tools und Plattformen wie MISP, openCTI und kommerzielle Threat Intelligence Feeds.

## **3. Ziele**

1. Verbesserung der Erkennung und Abwehr von Cyberbedrohungen durch den Austausch von Bedrohungsinformationen.
2. Förderung der Zusammenarbeit mit externen Partnern, z. B. CERTs, Branchenorganisationen und Sicherheitsanbietern.
3. Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Bedrohungsinformationen.
4. Unterstützung bei der Einhaltung regulatorischer Anforderungen (z. B. NIS2, ISO 27001, DORA).

## **4. Rollen und Verantwortlichkeiten**

|  |  |
| --- | --- |
| **Rolle** | **Verantwortlichkeiten** |
| Threat Intelligence Analyst | Analyse, Validierung und Priorisierung von Bedrohungsinformationen. |
| SOC Manager | Genehmigung und Überwachung des Austauschs von Bedrohungsinformationen. |
| Compliance Officer | Sicherstellung der Einhaltung von Datenschutz- und Sicherheitsvorgaben. |
| Externe Partner | Nutzung und Schutz der bereitgestellten Bedrohungsinformationen. |

## **5. Richtlinien für den Umgang mit Threat Intelligence**

**5.1 Sammlung von Bedrohungsinformationen**

• Informationen aus vertrauenswürdigen Quellen sammeln, z. B.:

• Open Source Plattformen (z. B. MISP, openCTI).

• Kommerzielle Threat Feeds.

• Branchenpartnerschaften und CERTs.

• Automatische Sammlung und Aggregation durch SIEM- und SOAR-Tools.

**5.2 Validierung und Analyse**

* Alle gesammelten Informationen müssen durch den Threat Intelligence Analyst überprüft und auf ihre Relevanz hin bewertet werden.

• Informationen werden nach ihrer Kritikalität eingestuft:

• **Hoch:** Sofortige Maßnahmen erforderlich.

• **Mittel:** Beobachtung und Vorbereitung.

• **Niedrig:** Dokumentation und regelmäßige Überprüfung.

**5.3 Verwendung von Threat Intelligence**

• Integration in bestehende Sicherheitsmaßnahmen, z. B.:

• SIEM-Regeln für Erkennung und Alarmierung.

• Erstellung von Playbooks für automatisierte SOAR-Prozesse.

• Incident Response Prozesse basierend auf neuen IoCs (Indicators of Compromise).

**5.4 Weitergabe von Bedrohungsinformationen**

* Bedrohungsinformationen dürfen nur mit genehmigten Partnern geteilt werden.
* Sensible Informationen müssen anonymisiert werden, bevor sie extern weitergegeben werden.
* Alle weitergegebenen Daten müssen dokumentiert und mit einem Vermerk zur Nutzung versehen sein.

## **6. Sicherheit bei der Weitergabe**

|  |  |
| --- | --- |
| **Risikofaktor** | **Maßnahmen zur Risikominderung** |
| **Unbefugter Zugriff** | Nutzung von verschlüsselten Übertragungswegen (z. B. TLS, VPN). |
| **Fehlinterpretation** | Bereitstellung von Metadaten zur Kontextualisierung der Bedrohungsinformationen. |
| **Datenlecks** | Anonymisierung sensibler Informationen vor der Weitergabe. |

## **7. Plattformen und Tools für Threat Intelligence Sharing**

|  |  |
| --- | --- |
| **Tool/Plattform** | **Funktion** |
| **MISP** | Open Source Threat Intelligence Plattform. |
| **openCTI** | Verwaltung und Analyse von Cyber Threat Intelligence. |
| **Threat Intelligence Feeds** | Kommerzielle Anbieter wie Recorded Future, Palo Alto AutoFocus. |
| **TheHive** | Case Management und IoC-Verwaltung. |

## **8. Reporting und Monitoring**

* **Berichte:** Regelmäßige Berichte an das Management über die genutzten und geteilten Bedrohungsinformationen.
* **Monitoring:** Überwachung der Effektivität von Threat Intelligence durch KPI-Metriken wie:

• Anzahl der validierten Threat Intelligence Reports.

• Anzahl der Vorfälle, die durch Threat Intelligence verhindert wurden.

• Durchschnittliche Zeit von Erkennung bis zur Reaktion.

## **9. Compliance**

Diese Policy stellt sicher, dass die Verarbeitung und Weitergabe von Bedrohungsinformationen mit den folgenden Standards und Vorschriften übereinstimmt:

• **ISO 27001:** Anforderungen an Informationssicherheits-Managementsysteme.

• **NIS2:** Sicherheitsanforderungen für Betreiber wesentlicher Dienste.

• **DORA:** Vorschriften zur digitalen Betriebsresilienz.

• **DSGVO:** Schutz personenbezogener Daten.

## **10. Eskalation und Überprüfung**

* Sicherheitsprobleme oder Vorfälle im Zusammenhang mit Threat Intelligence Sharing müssen sofort an den SOC Manager eskaliert werden.

• Diese Policy wird jährlich überprüft und bei Bedarf aktualisiert.