# **Threat Hunting Guideline**

*Leitfaden für die proaktive Suche nach Bedrohungen im Security Operations Center (SOC)*

## **1. Ziel der Guideline**

Die Threat Hunting Guideline bietet eine strukturierte Vorgehensweise zur Identifikation und Untersuchung potenzieller Bedrohungen in der IT-Umgebung. Ziel ist es, proaktiv Anomalien und Indikatoren für Kompromittierungen (Indicators of Compromise, IoCs) zu erkennen, bevor diese größeren Schaden verursachen können.

## **2. Anwendungsbereich**

Diese Guideline gilt für alle Mitarbeiter des SOC-Teams, die für Threat Hunting, Incident Response und Sicherheitsüberwachung verantwortlich sind. Sie umfasst alle Systeme, Netzwerke und Anwendungen der Organisation.

## **3. Voraussetzungen**

Bevor mit dem Threat Hunting begonnen wird, müssen folgende Voraussetzungen erfüllt sein:

1. **Technische Voraussetzungen:**

• Ein funktionsfähiges SIEM-System (z. B. Elastic Security, Splunk).

• EDR/XDR-Lösungen (z. B. CrowdStrike, SentinelOne).

• Threat Intelligence Plattformen (z. B. MISP, openCTI).

• Zugriff auf Logs und Systemdaten.

2. **Wissen und Schulung:**

• SOC-Mitarbeiter müssen regelmäßig in Threat Hunting Techniken geschult werden.

* Kenntnis gängiger Angriffsmuster, wie TTPs (Tactics, Techniques, and Procedures) nach MITRE ATT&CK.

3. **Dokumentation:**

• Vorhandensein von Playbooks und Incident Response Prozessen.

* Verfügbarkeit von eskalationsbereiten Kontaktlisten (Tier 2, Tier 3, Incident Response Manager).

## **4. Threat Hunting Prozess**

**4.1 Vorbereitung**

• Definieren des Ziels:

* Welche Bedrohungen sollen untersucht werden? (z. B. Ransomware, Insider Threats, Phishing-Angriffe).
* Sammeln von Threat Intelligence:
* Aktualisieren der IoC-Datenbank mit den neuesten Informationen aus MISP, openCTI oder anderen Plattformen.
* Tools bereitstellen:
* Sicherstellen, dass alle benötigten Werkzeuge (SIEM, Forensik-Tools, Netzwerk-Monitoring) verfügbar und einsatzbereit sind.

**4.2 Hypothesenbildung**

• Formulieren einer Hypothese, z. B.:

• “Angreifer nutzen gängige RDP-Port-Scans, um ungeschützte Systeme zu finden.”

• “Es könnte Anzeichen für lateral movement nach einem Konto-Diebstahl geben.”

**4.3 Datenanalyse**

• **Logs analysieren:**

* Durchsuchen von Log-Daten nach Anomalien (z. B. verdächtige Login-Versuche, ungewöhnliche Datenübertragungen).

• Einsatz von SIEM- und EDR-Filtern, um verdächtige Aktivitäten zu erkennen.

• **Netzwerkanalyse:**

* Überprüfen von Netzwerkverkehr auf ungewöhnliche Muster oder Verbindungen zu bekannten bösartigen IPs/Domains.

• **Endpoint-Untersuchung:**

• Analyse von Endpunkten auf verdächtige Prozesse, Dateien oder Registry-Einträge.

**4.4 Validierung der Hypothese**

• Überprüfung, ob die gefundenen Anomalien tatsächlich Indikatoren für einen Angriff sind.

* Cross-Referencing mit Threat Intelligence Datenbanken, um bösartige Aktivitäten zu bestätigen.

• Falsche Positivmeldungen ausschließen.

**4.5 Reaktion**

• Falls Bedrohungen identifiziert werden:

• Einleiten des Incident Response Prozesses.

• Eskalation an Tier-2/3 Analysten oder Incident Response Manager.

• Maßnahmen zur Eindämmung:

• Isolieren kompromittierter Systeme.

• Blockieren von bösartigen IPs/Domains.

## **5. Tools und Technologien**

1. **SIEM:**

• Elastic Security, Splunk, Wazuh.

2. **EDR/XDR:**

• CrowdStrike, SentinelOne.

3. **Threat Intelligence:**

• MISP, openCTI.

4. **Netzwerkanalyse:**

• Wireshark, Zeek.

5. **Forensik-Tools:**

• Volatility, Autopsy.

## **6. Berichterstellung**

Nach Abschluss einer Threat Hunting Session wird ein Bericht erstellt, der folgende Punkte enthält:

1. Ziel und Hypothese der Untersuchung.

2. Beschreibung der durchgeführten Analysen und Ergebnisse.

3. Identifizierte Bedrohungen und empfohlene Maßnahmen.

4. Lessons Learned für zukünftige Analysen.

## **7. Best Practices**

1. **Regelmäßige Durchführung:**

• Threat Hunting sollte ein fester Bestandteil der SOC-Strategie sein.

2. **Automatisierung nutzen:**

• Automatisierte Tools zur Unterstützung manueller Analysen einsetzen.

3. **Proaktive Haltung:**

• Anomalien frühzeitig erkennen und untersuchen, bevor sie zu Vorfällen eskalieren.

4. **Zusammenarbeit fördern:**

* SOC-Teams sollten eng mit Incident Response und Threat Intelligence Teams zusammenarbeiten.

## **8. KPI zur Erfolgsmessung**

• Anzahl der durchgeführten Threat Hunting Sessions.

• Zeit bis zur Identifikation einer Bedrohung.

• Anzahl der gefundenen IoCs.

• Reduzierung der False Positives durch optimierte Prozesse.

## **9. Fazit**

Threat Hunting ist ein essenzieller Bestandteil eines proaktiven SOC-Betriebs. Durch strukturierte Analysen und den Einsatz moderner Technologien können Bedrohungen frühzeitig erkannt und Risiken minimiert werden.

Dieser Leitfaden dient als Grundlage für alle SOC-Mitarbeiter, um systematisch und effektiv nach Bedrohungen zu suchen und die Sicherheitslage des Unternehmens zu verbessern.