

## 1. Phishing-E-Mail-Erkennung

**Ziel:** Klassifikation einer E-Mail als „Phishing“ oder „Legitim“.

**Prompt:**

Du bist ein KI-Modell zur Erkennung von Phishing-E-Mails. Analysiere die folgende E-Mail und gib an, ob sie als Phishing einzustufen ist. Gib eine kurze Begründung.

E-Mail:  
""

Sehr geehrter Kunde, Ihr Konto wurde gesperrt. Bitte loggen Sie sich unter folgendem Link ein: <http://sicherheits-check.example.com>  
""

**Ergebnis:**

- Kategorie: Phishing
- Begründung: Enthält dringende Aufforderung und verdächtigen Link.

## 2. Analyse von verdächtigen Login-Logs

**Ziel:** Einschätzung des Risikos eines Login-Ereignisses.

**Beispieldaten:**

```
{  
  "event": "login",  
  "user": "admin",  
  "ip": "185.14.98.2",  
  "location": "Russland",  
  "result": "mehrere fehlgeschlagene Versuche"  
}
```

**Prompt:**

Bewerten Sie das folgende Login-Ereignis in Bezug auf sein Sicherheitsrisiko: niedrig, mittel, hoch. Begründen Sie die Einschätzung.

**Antwort (Beispiel):**

- Risiko: Hoch
- Begründung: Mehrere fehlgeschlagene Versuche aus ungewöhnlichem Herkunftsland.

### 3. Analyse von Firewall-Logs

**Ziel:** Erkennung potenziell gefährlicher Verbindungen.

**Beispiel-Logzeile:**

DROP TCP 203.0.113.45:443 → 192.168.1.10:445 Flags: SYN

**Prompt:**

Ist diese Verbindung verdächtig oder unkritisch? Analysiere die Zielportnummer und gib eine Begründung.

**Antwort (Beispiel):**

- Klassifikation: Verdächtig
- Begründung: Zielport 445 (SMB) wird häufig für Angriffe wie EternalBlue verwendet.

### 4. Erkennung von Datenexfiltration

**Ziel:** Analyse von Datenmengen im ausgehenden Verkehr.

**Prompt:**

Eine interne IP-Adresse hat innerhalb von 30 Minuten 8 GB an Daten an eine unbekannte IP außerhalb des Unternehmensnetzwerks gesendet. Handelt es sich hierbei möglicherweise um Datenexfiltration? Begründen Sie Ihre Antwort.

**Antwort:**

- Einschätzung: Mögliche Exfiltration
- Begründung: Ungewöhnlich hohes Datenvolumen an unbekannte externe Adresse.

### 5. Triage von SOC-Tickets

**Ziel:** Automatische Risikoeinschätzung eingehender Tickets.

**Beispiel-Ticket:**

Betreff: Verdächtige Datei in E-Mail-Anhang

Text: Mitarbeiter berichtet über eine Excel-Datei mit Makros, die automatisch heruntergeladen wurde.

**Prompt:**

Ordne diesem Vorfall eine Risikokategorie zu (Niedrig, Mittel, Hoch). Gib eine Begründung.

**Antwort:**

- Risiko: Mittel
- Begründung: Makros in unbekannten Dateien sind potenziell gefährlich, aber keine Ausführung nachgewiesen.

## 6. Kategorisierung von Schwachstellenmeldungen (CVEs)

**Ziel:** Automatische Priorisierung von CVEs.

**Input:**

CVE-2024-12345: Heap Overflow in OpenSSL vor Version 3.1.0 ermöglicht Remote Code Execution über TLS.

**Prompt:**

Analysiere die Schwere dieser Schwachstelle (Niedrig, Mittel, Hoch). Begründe die Einschätzung.

**Antwort:**

- Schweregrad: Hoch
- Begründung: RCE über TLS erlaubt Angriffe ohne Benutzerinteraktion.