huddlex.at
IT . Consulting . Buchhaltung

Experts Group IT-Security

ERSETZT DIE **KI** DEINE SECURITY-EXPERT:INNEN?

mit Christoph Kofler,
Johannes Nöbauer und Elmar Jilka

AGENDA

Wo liegen die heutigen Grenzen von KI im Bereich Security?

Wie nutzen Expert:innen die KI in der Praxis?

Welche Fragen sollte ich mir als Unternehmen zu KI stellen?

3 Blickwinkel

- *Software-Entwicklung (Christoph, Gepardec)*
- *CyberRisiko Management & Compliance (Elmar Jilka, SEQiFY)*
- *Industrie & Strategie (Johannes, BytePeak Consulting)*

Takeaways

Fazit

Ersetzt die KI deine Security-Expert:innen?

gepardec
simplify your business

Christoph Kofler

Bergführer für deine Software Modernisierung
Chief Commercial Officer (CCO)

“In deiner Individualsoftware steckt der Kern deines Geschäftsmodells”

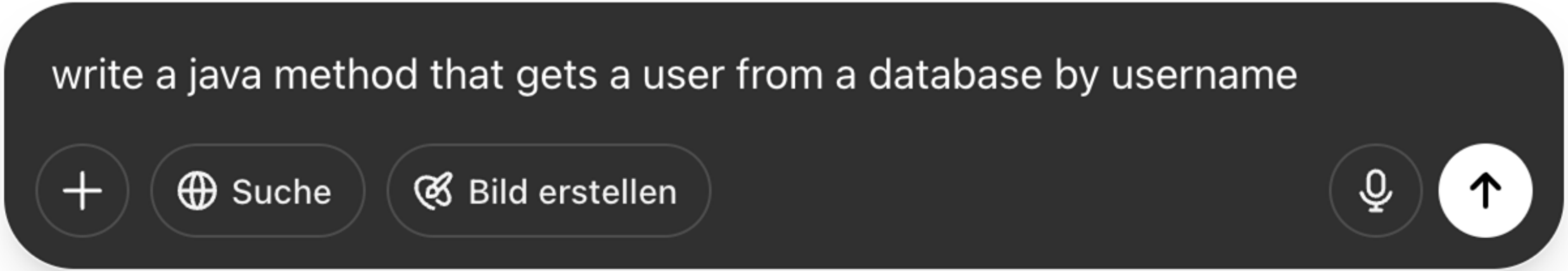
und das
Cyber Risiko

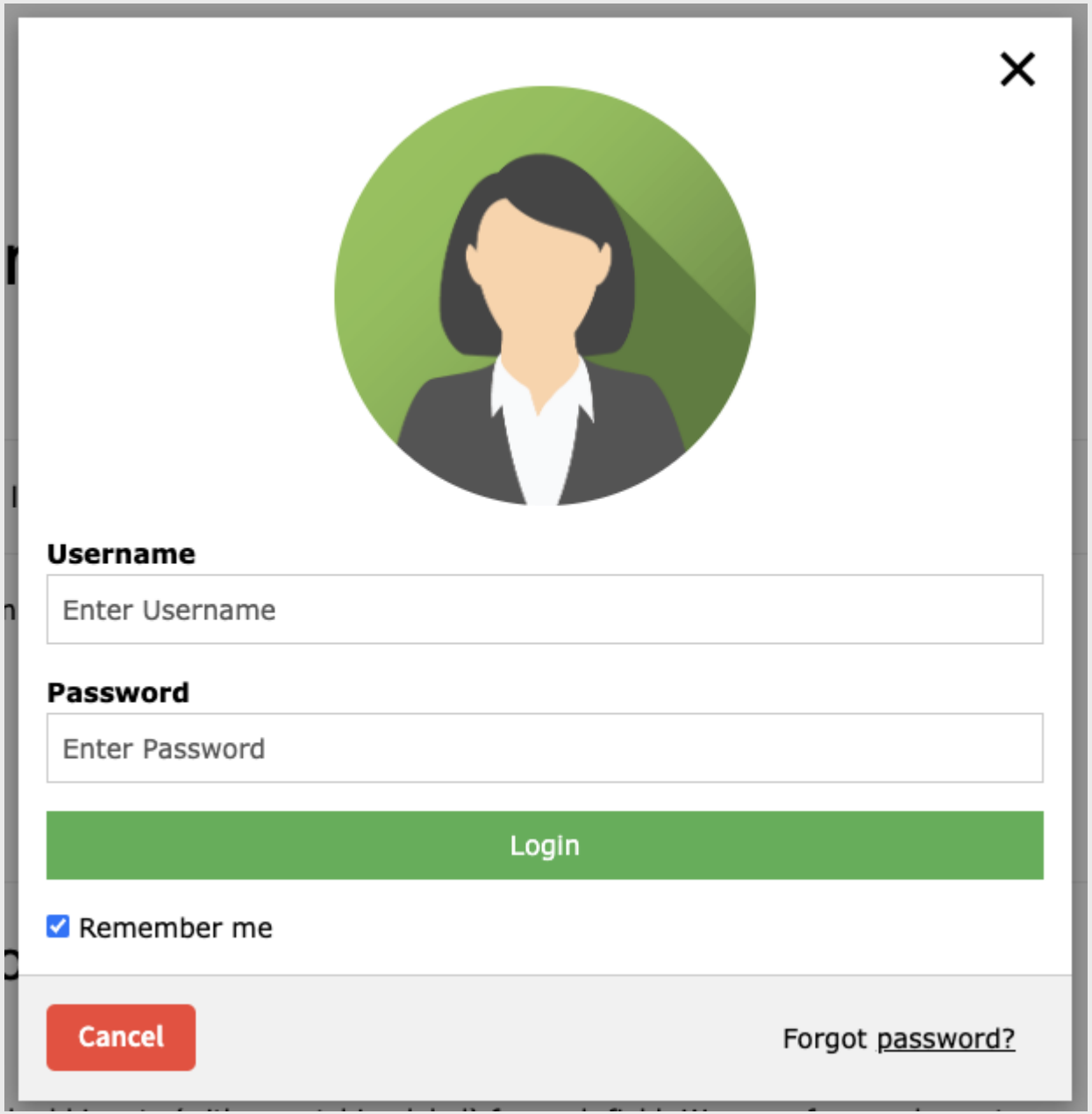
gepardec
simplify your business

Was sieht ein Secure Coding EXPERTE sofort, das ein Greenhorn übersieht?

gepardec
simplify your business

DAS GREENHORN MIT ChatGPT 4o (17.5.2025)





```java
public User getUser(String username) throws SQLException {
    Statement stmt = connection.createStatement();
    String query = "SELECT * FROM users WHERE username = '"
                                    + username + "'";
    ResultSet rs = stmt.executeQuery(query);

    if (rs.next()) {
        return new User(rs.getInt("id"),
                        rs.getString("username"));
    }
    return null;
}
```

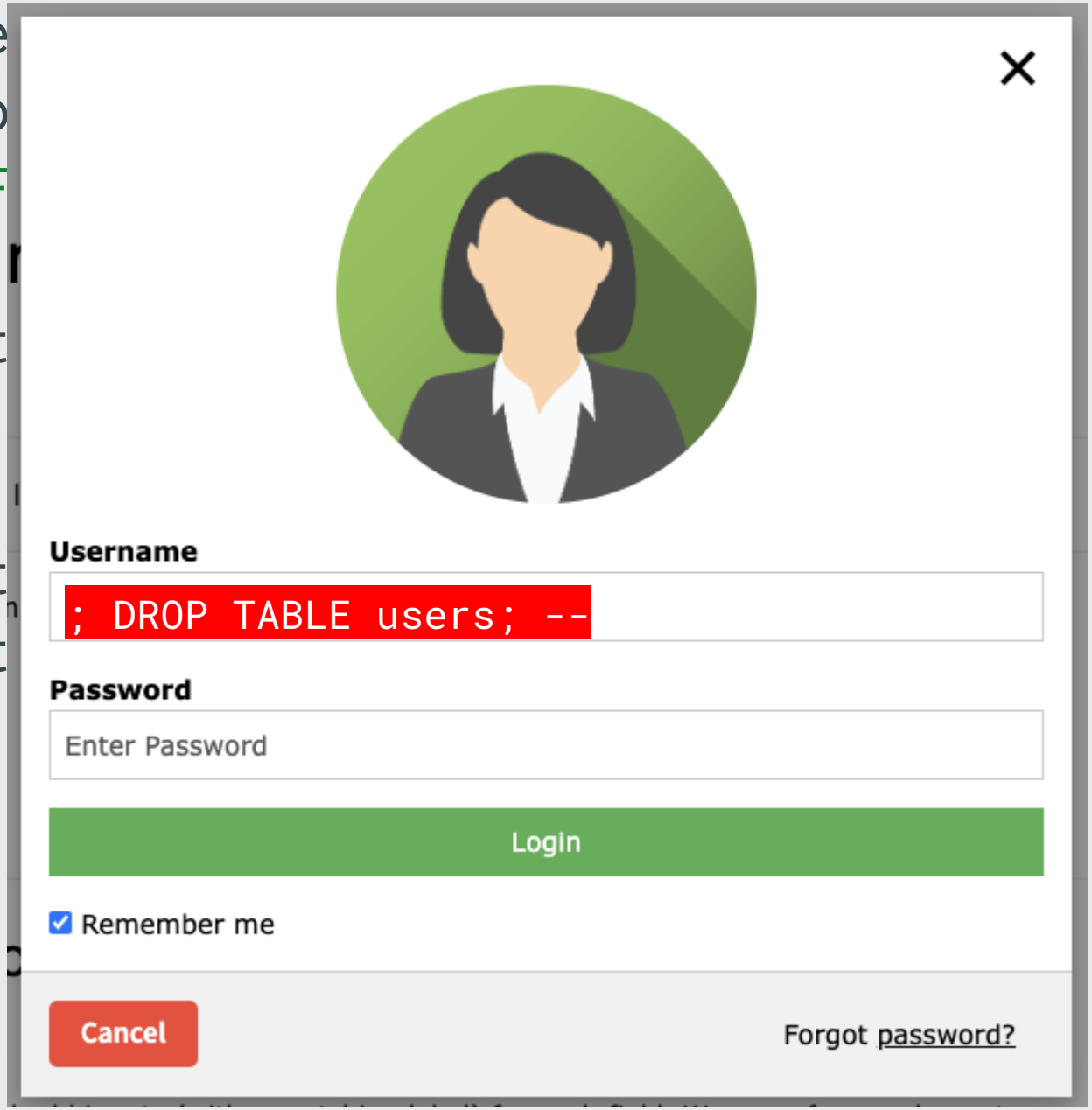
```
public User getUser(String username) throws SQLException {
    Statement stmt = connection.createStatement();
    String query = "SELECT * FROM users WHERE username = '"
                                    + username + "'";
    ResultSet rs = stmt.executeQuery(query);

    if (rs.next()) {
        return new User(rs.getInt("id"),
                        rs.getString("username"));
    }
    return null;
}
```

```
public User getUser(String username) throws SQLException {
    Statement stmt = connection.createStatement();
    String query = "SELECT * FROM users WHERE username = '"
                                    + username + "'";
    ResultSet rs = stmt.executeQuery(query);

    if (rs.next()) {
        return new User(rs.
                        rs                    e"));
    }
    return null;
}
```

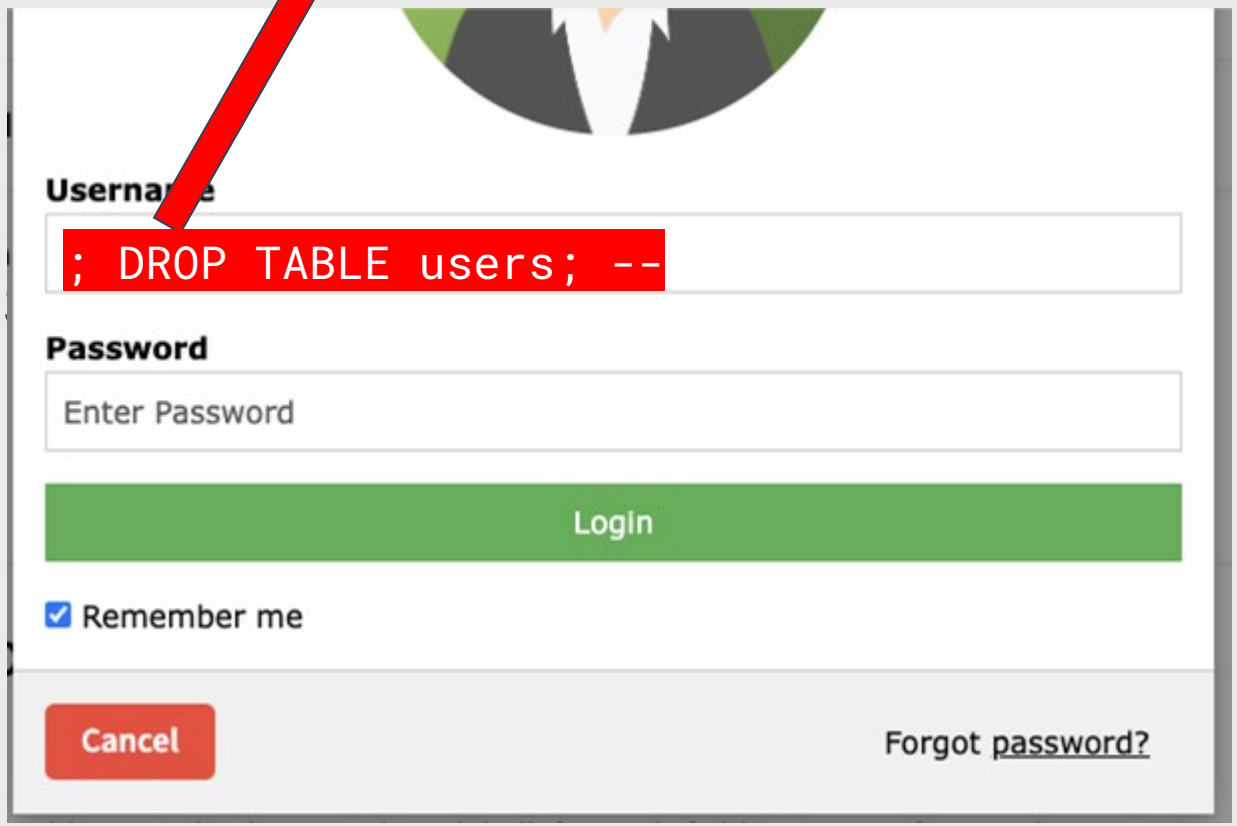
SQL Injection möglich!

gepardec
simplify your business

```
public User getUser(String use
    Statement stmt = connectio
    String query = "SELECT * F

    ResultSet rs = stmt.execut

    if (rs.next()) {
        return new User(rs.get
                        rs.get
    }
    return null;
}
```



```
public User getUser(String username) throws SQLException {
    Statement stmt = connection.createStatement();
 String query = "SELECT * FROM users WHERE username = '"
                                        + username + "'";
    ResultSet rs = stmt.executeQuery(query);

    if (rs.next()) {
        return new User(rs.get
                        rs.get
    }
    return null;
}
```



```
public User getUser(String username) throws SQLException {
    Statement stmt = connection.createStatement();
    String query = "SELECT * FROM users WHERE username = '"
                                        + '; DROP TABLE users;
--' + "'";
    ResultSet rs = stmt.executeQuery(query);

    if (rs.next()) {
        return new User(rs.getInt("id"),
                        rs.getString("name"));
    }
    return null;
}
```

Wieviel unsicherer Code steckt in Deiner Business Software?

gepardec
simplify your business

EXPERT:IN

write a java method that retrieves a user securely using a prepared statement to prevent sql injection

Suche Bild erstellen

DAS GREENHORN

write a java method that gets a user from a database by username

Suche Bild erstellen

```
public User getUser(String username) throws SQLException {
    String sql = "SELECT id, username FROM users WHERE
                                        username = ?";
    try (PreparedStatement stmt =
                connection.prepareStatement(sql)) {
        stmt.setString(1, username);
        ResultSet rs = stmt.executeQuery();
        if (rs.next()) {
          return new User(rs.getInt("id"),
                          rs.getString("username"));
        }
        return null;
    }
}
```

Wer macht bei Dir die Security Code Reviews?

gepardec
simplify your business

Christoph Kofler

Bergführer für deine Software Modernisierung
Chief Commercial Officer (CCO)

Secure Java Code Upgrade

gepardec
simplify your business

BYTEPEAK CONSULTING

Industrie & Strategie – KI als Sicherheitsakteur?

Johannes Nöbauer
CEO & Executive Advisor
johannes@bytepeak.at

Agenda

- Über uns
- Warum KI im Security Bereich eine riesen Chance bedeutet?
- Wo liegen die heutigen Grenzen von KI im Bereich Security?
- Wie nutzen Expert:innen KI in der Praxis?
- Welche Fragen sollte ich mir als Unternehmen stellen?
- Zukunftsausblick: Das KI-unterstützte Security Operations Center

Über uns

Die BytePeak Consulting GmbH begleitet Unternehmen ganzheitlich auf dem Weg in die digitale Zukunft, von der Strategie über die technologische Machbarkeit bis zur erfolgreichen Skalierung und Zertifizierung. Unser Ansatz verbindet Expertise, Umsetzungsstärke und nachhaltigen Mehrwert.

Unsere Philosophie:

- Unabhängige, objektive, Ende-zu-Ende Beratung
- T-M-S-S Prinzip: Technologie, Mensch, Strategie, Storytelling
- Tiefes Branchen- und Technologieverständnis
- Strategische Exzellenz mit Umsetzungsfokus

Johannes Nöbauer

CEO & Executive Advisor

Unsere fachlichen Schwerpunkte

BYTEPEAK CONSULTING

Digitalstrategie Beratung

Business Development

Technologiestrategie Beratung

Zertifizierungs Beratung

Ende-zu-Ende Beratung mit dem Fokus auf digitaler Exzellenz

Warum KI im Security Bereich eine riesen Chance bedeutet?

- **Security ist datengetrieben und KI versteht Daten.**
- **Die 4 großen Chancen:**
  - **Früherkennung statt Schadensbegrenzung**
    → KI erkennt Muster und Anomalien, bevor der Mensch sie sieht.
  - **Entlastung überlasteter Security-Teams**
    → Automatisierung repetitiver Aufgaben (z. B. Log-Analyse, Alert-Triage)
  - **Reaktion in Echtzeit**
    → KI kann in Millisekunden auf Bedrohungen reagieren – Menschen nicht.
  - **Lernen aus jedem Vorfall**
    → KI-gestützte Systeme werden besser mit jedem Angriff (adaptive Security).

Wo liegen die heutigen Grenzen von KI im Bereich Security?

- **Technologische und regulatorische Grenzen:**
  - **"Road to KI":** Ohne qualitativ hochwertige Daten, klare Zieldefinition und systematische Umsetzung bleibt KI eine Spielerei.
  - **Safety-Systeme:** Autonome Systeme dürfen nicht ohne Redundanz oder Kontrolle arbeiten, besonders in sicherheitskritischen Umgebungen (verpflichtende Anforderungen).
  - **Safety-Zertifizierungen:** Normen wie ISO 26262, IEC 61508, ... schließen autonome KI-Systeme (noch) weitgehend aus.
  - **Human-in-the-Loop (HitL):** Pflicht in vielen sicherheitsrelevanten Bereichen – KI darf unterstützen, nicht entscheiden.
- **Fallbeispiel Bosch:**
  - **Bosch als Vorreiter in Europa:** Kombination aus starker Datenstrategie, AI-Governance, Sicherheitsstandards.
  - Nutzung von KI im Predictive Maintenance, Threat Detection und Anomalieerkennung, immer mit HitL-Ansatz.

Der Gap als Innovationschance

„Warum KI eine riesen Chance ist.“

- ✚ Hier ist KI nicht Bedrohung, sondern Enabler!
- ✚ Die 5 Evolutionsstufen einhalten!

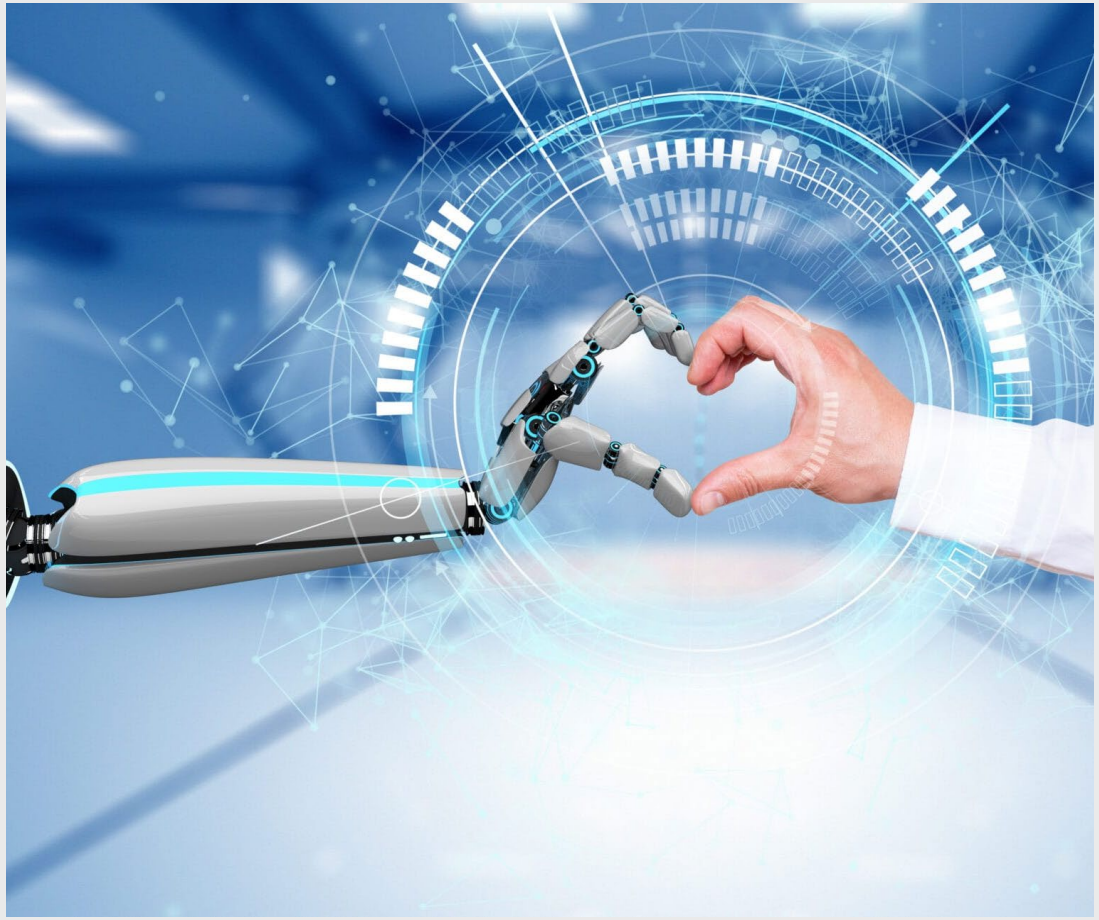
Wie nutzen Expert:innen KI in der Praxis?

BYTEPEAK CONSULTING

- **Security-relevante Anwendungsfelder:**
  - **Compliance & Audits:** KI-gestützte Analyse von Logdaten und Dokumentationen z. B. für ISO/IEC 27001 oder NIS-2. Automatisierte Erstellung von Audit-Reports.
  - **Chatbots zur ISO-/NIS-Schulung: "**AI Security Assistant“ für IT-Mitarbeiter und Management, Automatische Generierung von Awareness-Inhalten (in allen Sprachen)
  - **Supply Chain Risk Management:** KI erkennt Anomalien, z. B. durch ungewöhnliche Datenflüsse oder Abweichungen von normalen Mustern.
  - **Business Continuity & Resilience:** Unterstützung in Szenario-Simulationen und dynamischen Risikobewertungen.
  - **Datenmanagement:** KI als Enabler für Datenklassifizierung, Verschlüsselungskontrolle und Zugriffsmusteranalysen.

Welche Fragen sollte ich mir als Unternehmen stellen?

- **Strategisch:**
  - Wo kann KI meine Sicherheitsstrategie sinnvoll ergänzen und wo nicht? (Tipp: Nicht mit der Technik sondern mit dem Problem starten)
  - Wie sieht mein Zielbild für KI-gestützte Security aus und habe ich eine Roadmap?
- **Entlang der primären Wertschöpfungskette denken:**
  - **Entwicklung:** Wie sicher sind meine Software Builds?
  - **Produktion:** Wie erkenne ich Anomalien in Echtzeit?
  - **IT & Service:** Wie reagiere ich automatisiert auf Security Incidents?
- **Organisatorisch:**
  - Bin ich auf Regelwerke wie **ISO/IEC 42001** oder **EU AI Act** vorbereitet?
  - Ist meine Organisation in der Lage, KI verlässlich zu betreiben oder bin ich noch im "Jugend forscht“ Modus?



Zukunftsausblick:
Das KI-unterstützte Security Operations Center

- **Vision: Das SoC der Zukunft**
  - Klassische SoCs sind heute reaktiv, manuell geprägt, oft überlastet und teuer im Betrieb.
  - **Zukunft:** KI-gesteuerte SoCs arbeiten rund um die Uhr, priorisieren automatisch, erkennen Bedrohungen in Echtzeit – proaktiv statt reaktiv.
  - Mensch und Maschine arbeiten symbiotisch: KI identifiziert, klassifiziert, schlägt Maßnahmen vor, Security-Expert:innen entscheiden und eskalieren.

BYTEPEAK
CONSULTING

Vielen Dank!

Vorsprung durch digitale Exzellenz.

SCAN ME

bytepeak.at

Takeaways & Fazit

3 Blickwinkel

- *Software-Entwicklung (Christoph, Gepardec)*
- *CyberRisiko Management & Compliance (Elmar Jilka, SEQiFY)*
- *Industrie & Strategie (Johannes, BytePeak Consulting)*