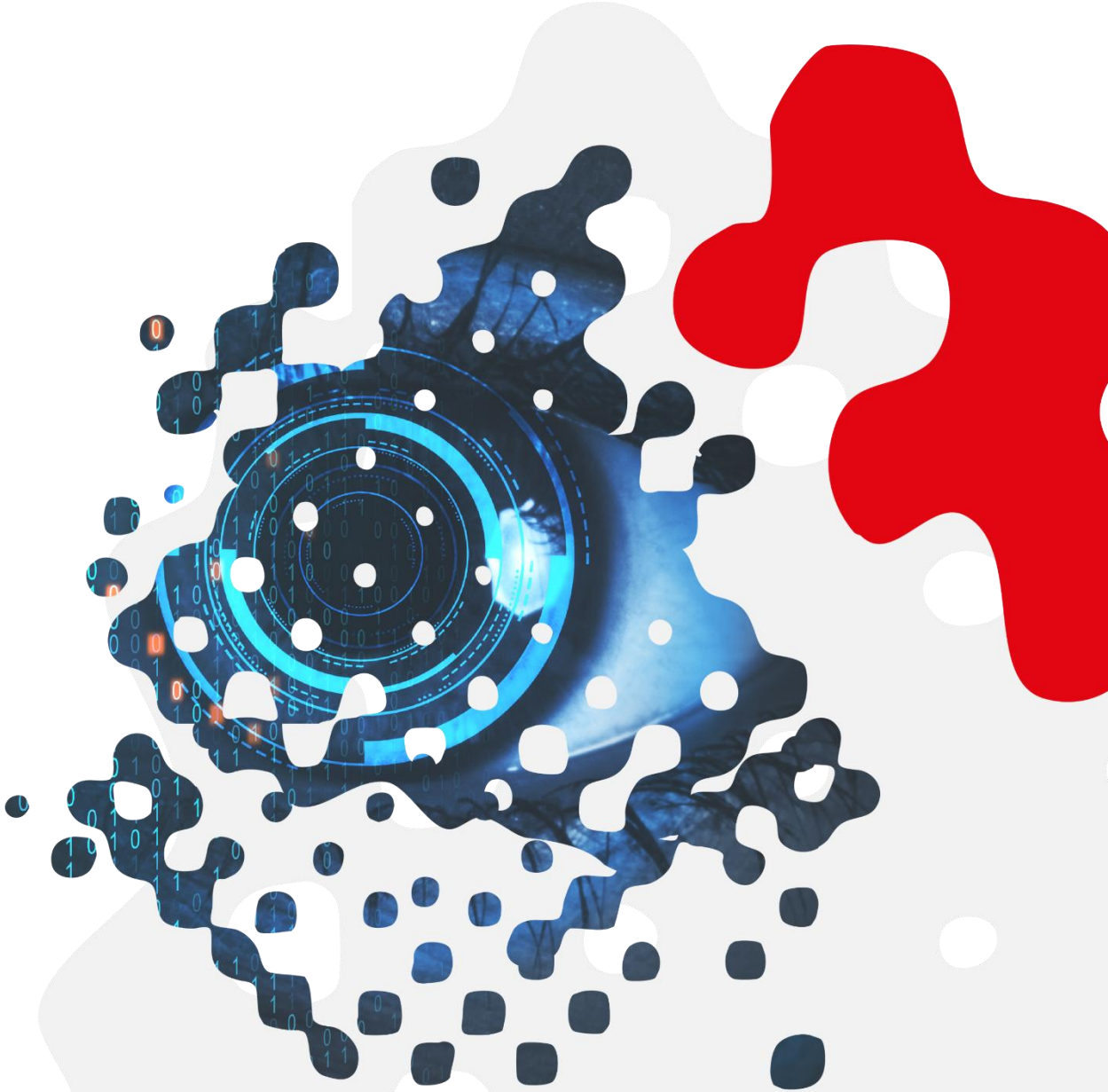
NetEye Conference DACH 2026



Die Zukunft der Cyber Defense

Mensch, KI und das SOC von Würth IT

Tobias Goller

WÜRTH | IT

GRAVITATE

Die aktuelle Bedrohungslage

Angriffe werden schneller, gezielter und automatisierter

- Ransomware, Phishing & Identitätsdiebstahl nehmen zu
- Lieferketten und hybride IT werden gezielt angegriffen
- KI professionalisiert Cybercrime
  - automatisierte Exploits und Echtzeit-Scans
  - personalisierte Phishing-Kampagnen

Angriffe erfolgen heute in Maschinengeschwindigkeit

Die aktuelle Bedrohungslage

Klassische Sicherheitsmechanismen reichen daher nicht mehr aus

DESHALB:

Gerade jetzt muss sich die Cyber Defense wesentlich weiterentwickeln

Was ist ein Security Operations Center?

Ein *Security Operations Center* ist eine zentrale organisatorische Einheit in einem Unternehmen oder einer Behörde, die für die **kontinuierliche Überwachung, Erkennung, Analyse und Abwehr von Cybersicherheitsbedrohungen** zuständig ist.

Es werden unter anderem Netzwerke, Endgeräte, Server, Cloud-Dienste, Identitäten, usw. überwacht

Dabei ist der typischer Ablauf: **Detect – Analyze – Respond – Recover**

Der Mensch im SOC

Der Mensch gibt der Cyber Defense Kontext und Urteilskraft

Rolle	Kernaufgabe
Tier 1 – Triage	Alarme überwachen und bewerten
Tier 2 – Incident Response	Vorfälle untersuchen und eindämmen
Tier 3 – Thread Hunting	Versteckte Bedrohungen proaktiv aufspüren
SOC Leac	Betrieb, Prioritäten und Kommunikation steuern

Menschen erkennen Fehlalarme, bewerten Risiken und treffen strategische Entscheidungen.

Der Mensch im SOC

Herausforderungen im SOC

- **Alarm-Müdigkeit**
  Tausende Meldungen pro Tag – viele davon ohne Relevanz.

- **Entscheidungen unter Zeitdruck**
  Bei kritischen Vorfällen zählt jede Minute.

- **Mehr als IT-Know-how**
  Analytik, Angreiferdenken und klare Kommunikation sind entscheidend.

Technologie liefert Signale – Menschen schaffen Verständnis und Priorität.

Einsatz von KI in der Cyber Defense

KI erkennt Bedrohungen in Maschinengeschwindigkeit

- **Erkennt Anomalien**
  Analysiert große Datenmengen und auffälliges Verhalten.

- **Entlastet das SOC**
  Priorisiert Alarme und reduziert Routineaufgaben.

- **Erkennt Angriffspfade früher**
  Identifiziert Risiken, bevor Schaden entsteht.

- **Stärkt die Phishing-Abwehr**
  Erkennt verdächtige Absender, Inhalte und Muster.

Einsatz von KI in der Cyber Defense

Einige der wichtigsten Vorteile:

- Skalierbarkeit & Rund-um-die-Uhr-Schutz: KI arbeitet 24/7 ohne Ermüdung und verarbeitet Datenmengen, die für Menschen manuell unmöglich zu bewältigen wären.

- Geschwindigkeit: Angriffe verkürzen sich durch autonome Hackertools oft von Tagen auf wenige Minuten. KI-Verteidigungssysteme reagieren in Millisekunden.

- Erkennung komplexer Muster: Klassische, regelbasierte Firewalls scheitern oft an neuen Mustern. Maschinelles Lernen (ML) erkennt auch mutierte oder völlig neue Schadsoftware-Varianten.

Das SOC der Zukunft

Das sogenannte “AI-Driven SOC” in vier zentralen Säulen:

Agentic AI SOC

Autonome Triage, Vorabanalyse in Sekundenschnelle

Automatisierter Incident Response (blockieren,isolieren)

Mensch greift bei hochkomplexen Angriffen ein

Cyber Fusion Center

SOC überwacht nicht mehr nur klassische IT Endpunkte, sondern verknüpft Telemtriedaten, IoT Geräte und OT Daten

Das CFC fungiert als zentrale Validierungsinstanz für die Zero-Trust-Architektur

Threat Hunting & K-Resilienz

Auf Basis der Thread Intelligence Daten such das SOC nach unentdeckten, subtilen Mustern, die herkömmliche Filter umgehen

Zukünftige SOC agiert präventiv, und wartet nicht auf Alarm

Dezentralisierung und Kollaboration

SOC zentralisiert die Expertisen und stellt Tools bereit, während die Behebung an die jeweiligen IT-Produkt- und Systemverantwortlichen übertragen werden.

Eigenverantwortung und Wiederherstellungen werden gestärkt.

DAS SOC DER ZUKUNFT: EVOLUTION & TRANSFORMATION

KRITERIUM	TRADITIONELLES SOC	SOC DER ZUKUNFT
ARBEITSWEISE	 REAKTIV 	 PROAKTIV (Continuous Threat Hunting & Vorhersage) 
FOKUS DER ANALYSTEN	 MANUELLE TRIAGE, SICHTEN VON LOGFILES 	 STRATEGIE, GOVERNANCE, KOMPLEXE FORENSIK 
TECHNOLOGIE	 STARRE SIEM-KORRELATIONSREGELN 	 AGENTIC AI, DEEP LEARNING, XDR 
REAKTIONSZEIT (MTTR)	 MINUTEN BIS STUNDEN 	 SEKUNDEN (AUTONOME EINDÄMMUNG) 
STRUKTUR	SILO (REINES IT-SICHERHEITSTEAM) 	INTEGRIERTES CYBER FUSION CENTER (IT, OT, CLOUD, BUSINESS) 

Mensch und KI als Team

- Mensch und KI bilden im modernen Security Operation Center (SOC) ein unschlagbares „Cyber-Tandem“.
- Künstliche Intelligenz analysiert gigantische Datenmengen in Echtzeit und automatisiert Routineaufgaben.
- Der Mensch bringt den Kontext, strategisches Denken und die finale Urteilskraft.

Mensch und KI als Team

Rollenverteilung im SOC : KI - Mensch

Funktionen	Die Rolle der KI (Der Datendetektiv)	Die Rolle des Menschen (Der Stratege)
Hauptfokus	Mustererkennung, Korrelation vieler Einzelereignisse, Skalierung & Speed	Kontext, Kreativität & Entscheidung
Geschwindigkeit	Analysiert Millionen von Events in Millisekunden.	Bewertet komplexe Vorfälle in Minuten bis Stunden.
Stärken	Erkennt Anomalien über Silos hinweg; schläft nie.	Kommunikation, versteht Business-Relevanz, Absichten und Nuancen. – Umgang mit neuen Situationen
Aufgaben	Filtert Fehlalarme (False Positives), korreliert Daten.	Leitet die Forensik, trifft die finale Eindämmungs-Entscheidung (Verantwortung)

Mensch und KI als Team

Das passende Zukunftsmodell ist daher nicht
„Mensch gegen KI“,
sondern:

Mensch entscheidet, KI unterstützt und automatisiert.

Bedeutung für Würth IT

Auch bei Würth IT setzen wir verstärkt auf KI im SOC.

Was bisher war:

Einsatz vom AI Assistent bei der Unterstützung von ausgelösten Alarmen.

Bedeutung für Würth IT

Neue Wege:

Erweiterter Einsatz der KI im SOC:

- Erkennung von offensichtlichen False Positives durch gezielte Abfragen im Hintergrund
- KI prüft die Serie von Alarmen und kann daraus den konkreten Vorfall automatisiert und in Sekundenschnelle erkennen.
- Rekonstruktion von Angriffsketten (z.B. durch Tools wie certutil.exe, powershell.exe)
- Angriffe werden automatisch den bekannten Mustern der MITRE ATT&CK-Matrix zugeordnet
- Automatisierte Erstellung von Dashboards
- Automatisierte Workflows

Bedeutung für Würth IT

Neue Wege:

Der Mensch im erweiterten Einsatz der KI im SOC:

- Analyse von komplexen Angriffen bleibt beim Menschen
- Definitionen der False Positive
- Erstellung von Playbooks, Workflows und deren Optimierung
- Integration neuer Datenquellen (Cloud, OT Welten, usw.)
- Kommunikation und Prozessverständnis

Erkenntnisse bei Würth IT : Neue Rollen und Kompetenzen

Die Arbeitsweise des SOC Analysten und die Rollen im SOC ändern sich:

- Security Analyst mit KI-Unterstützung
- Spezialist für Security Automationen (Erkennung von Ketten, Workflows, usw.)
- Experte für KI-Risiken und Überwachung der Modellüberwachung
- Es braucht verantwortliche für Governance und Datenschutz
- Prüfung automatischer Empfehlungen der KI
- Kommunikationsfähigkeit

Erkenntnisse bei Würth IT
Ausblick und Handlungsempfehlungen

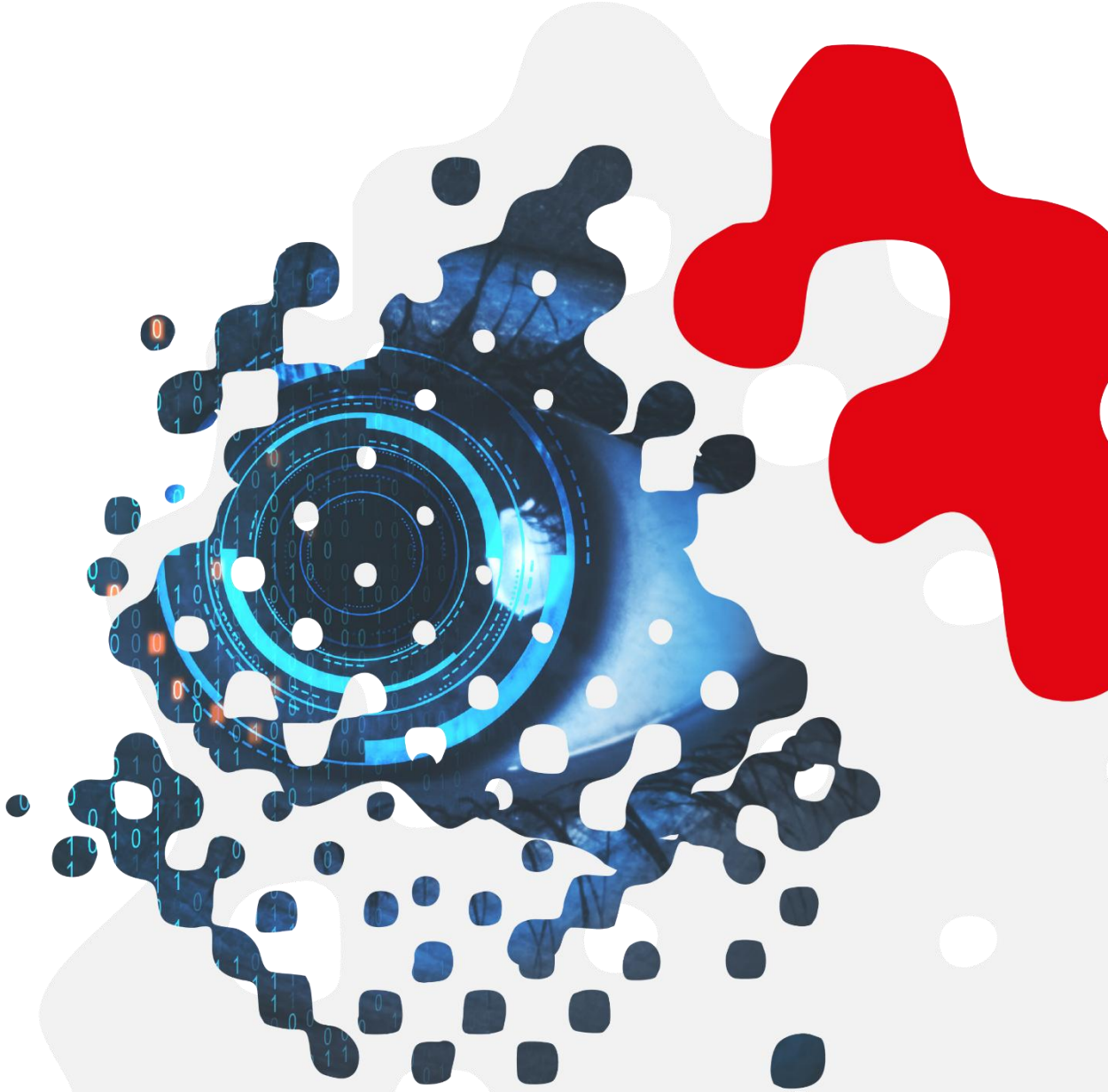
- Start des KI Einsatzes bei risikoarmen Routineaufgaben
- Menschliche Freigaben für kritische Aktionen beibehalten
- Modelle regelmäßig testen und überwachen
- Datenqualität und zentrale Sicherheitsdaten verbessern
- SOC-Mitarbeitende kontinuierlich weiterbilden
- Automatisierung mit klaren Verantwortlichkeiten verbinden
- Erfolgskennzahlen definieren, zum Beispiel:

Zeit bis zur Erkennung > > Zeit bis zur Reaktion > > Anzahl der Fehlalarme > > Qualität der Vorfallbewertung

NetEye Conference DACH 2026

Vielen Dank

… und jetzt freue ich mich auf Ihre Fragen und den Austausch



WÜRTH | IT

GRAVITATE