



TEELONIC  
network ▪ security ▪ analytics



# // LOGPOINT & ■■■■■ TELONIC

Europäische Cybersecurity als Zeichen für digitale Souveränität



**Andreas Föhringer**

Strategic Sales Manager MSSP  
[afo@logpoint.com](mailto:afo@logpoint.com)



**Erich Heinemann**

Leiter T-CERT  
[e.heinemann@telonic.de](mailto:e.heinemann@telonic.de)

# SCHLÜSSELFAKTOREN FÜR DIE DIGITALE SOUVERÄNITÄT

Datensicherheit

DSGVO Risikominimierung

Kontrollierbare Sicherheitsrisiken

Wettbewerbsvorteile

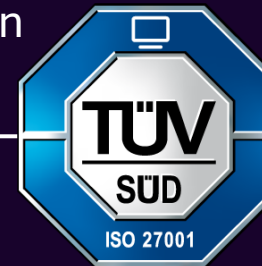
Vertrauen & Reputation



# UNSER VERSPRECHEN

Aus Europa für Europa

- **Technische Infrastruktur und Datenverarbeitung in der EU**
- **Rechtsverbindlich:** Strikte Einhaltung EU Datensicherheitsrichtlinien
- Unabhängig geprüft und zertifiziert
- **Vertraulichkeit:** KEIN Zugriff durch Dritte
- Unabhängige Wahl weiterer Quellen ( INTEL-Feeds )



Zertifizierte LogPoint-Spezialisten  
Service  
Zertifizierte Produkt-Spezialisten

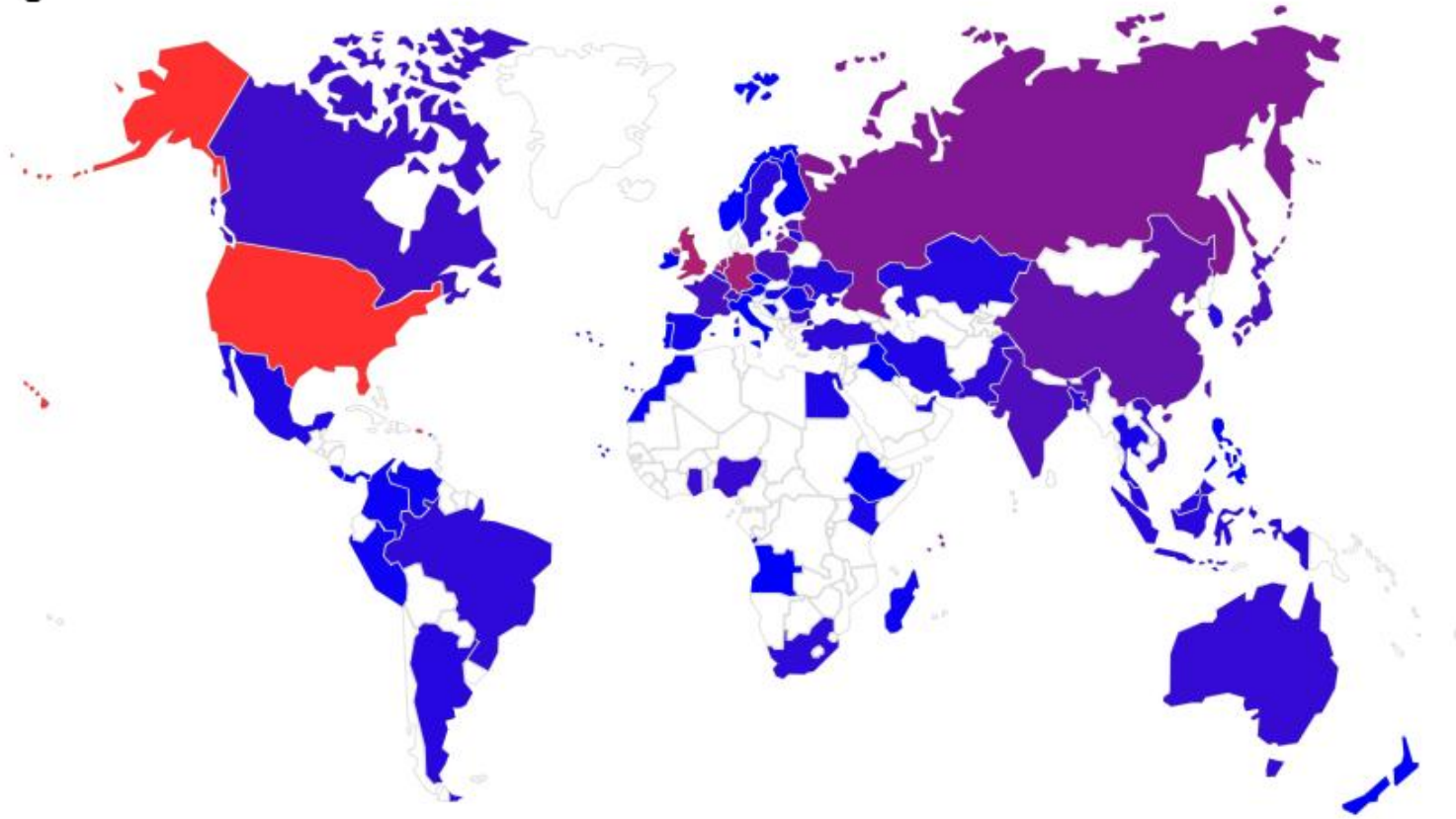
# ANFORDERUNGEN an den Service

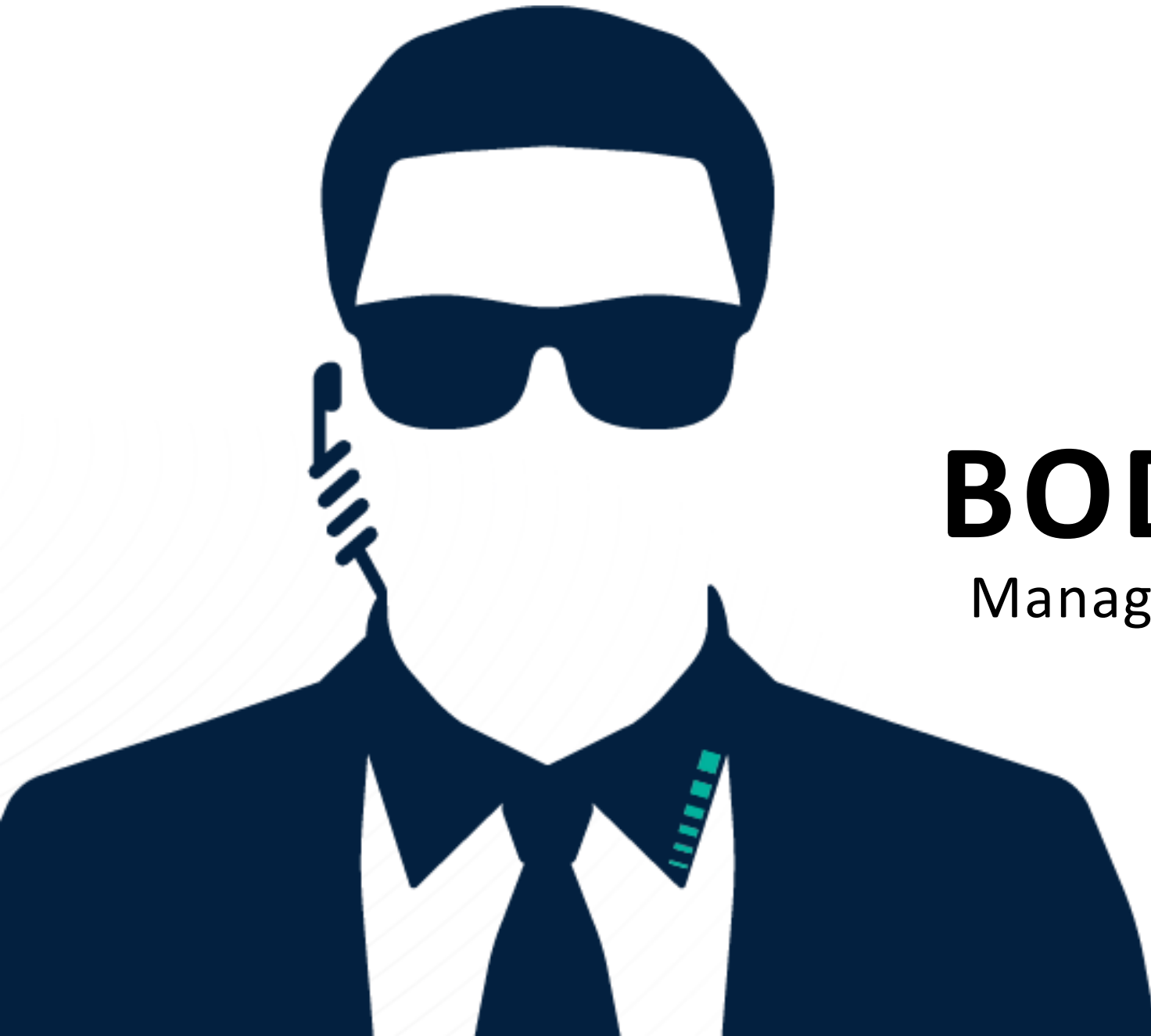
- Incident Detection and Response
- Klassifikation von Events > **Humboldt**
- Ableitung von Maßnahmen
- Forensische Analyse
- 24/7/365
- Eine Plattform zur Analyse und Response **LOGPOINT**



# Analyse, wer ist der Angreifer?

00



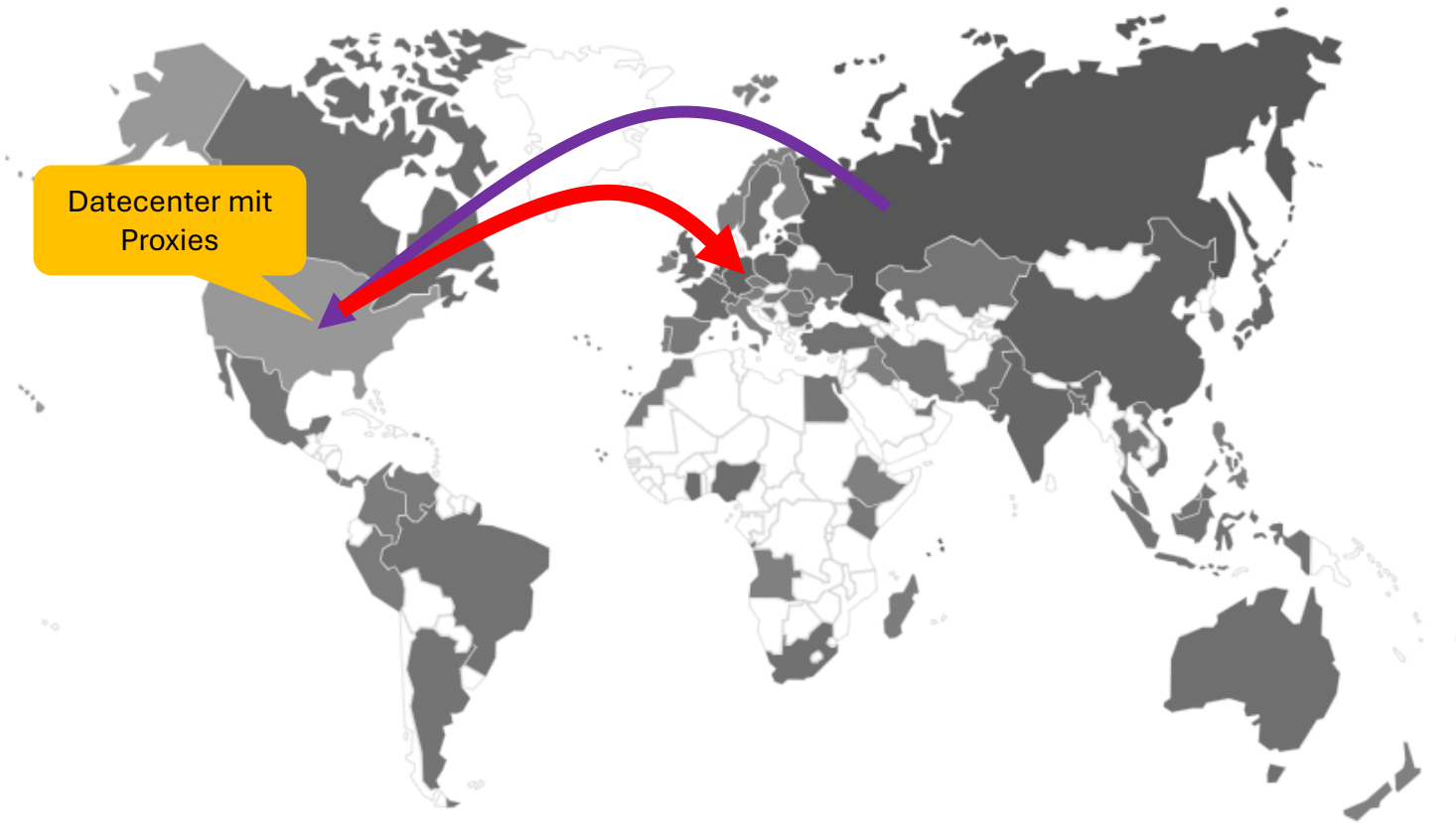


# BODYGUARD

Managed Security Services

Jeder Humboldt-Kunde kennt schon seinen „Bodyguard“ – der Techniker in den Detection-Reviews

# Analyse, wer ist der Angreifer? Wo ist der Angreifer?



Unsere Korrelation, warum wird dieser Kunde angegriffen? Situativ? Kundenspezifisch?



# SNOC



## Security Network Operation Center

- Ansprechpartner innerhalb Deutschlands
- Über 20 Jahre Branchenexpertise
- 24x7 Erreichbarkeit an 365 Tagen im Jahr
- Eskalationsmatrix gewährleistet Verfügbarkeit des passenden Spezialisten



# T-CERT



## Telonic - Computer Emergency Response Team

- Security Researcher
- Tuning der Analyseplattform
- Durchführung der Detection Reviews
- Erstellung von Playbooks und Reportings



TELONIC



# Unsere Plattform



## LOGPOINT

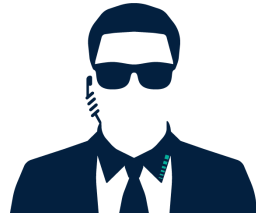
- Highend Security Information Event Management
  - Log Collection and Correlation, Integrations-Plattform für die Log-Analyse
  - SOAR  
( Security Orchestration Automation and Response )

## Humboldt – Vorsätze von 2017

- Schnellste Analyse und Klassifizierung von Threats
- Automatisierung mit den Ergebnissen der letzten Analysen, - eine Plattform mit Handlungsanweisungen
- Ein Maßanzug für ihre IT-Security, keine generische Ware von der Stange!



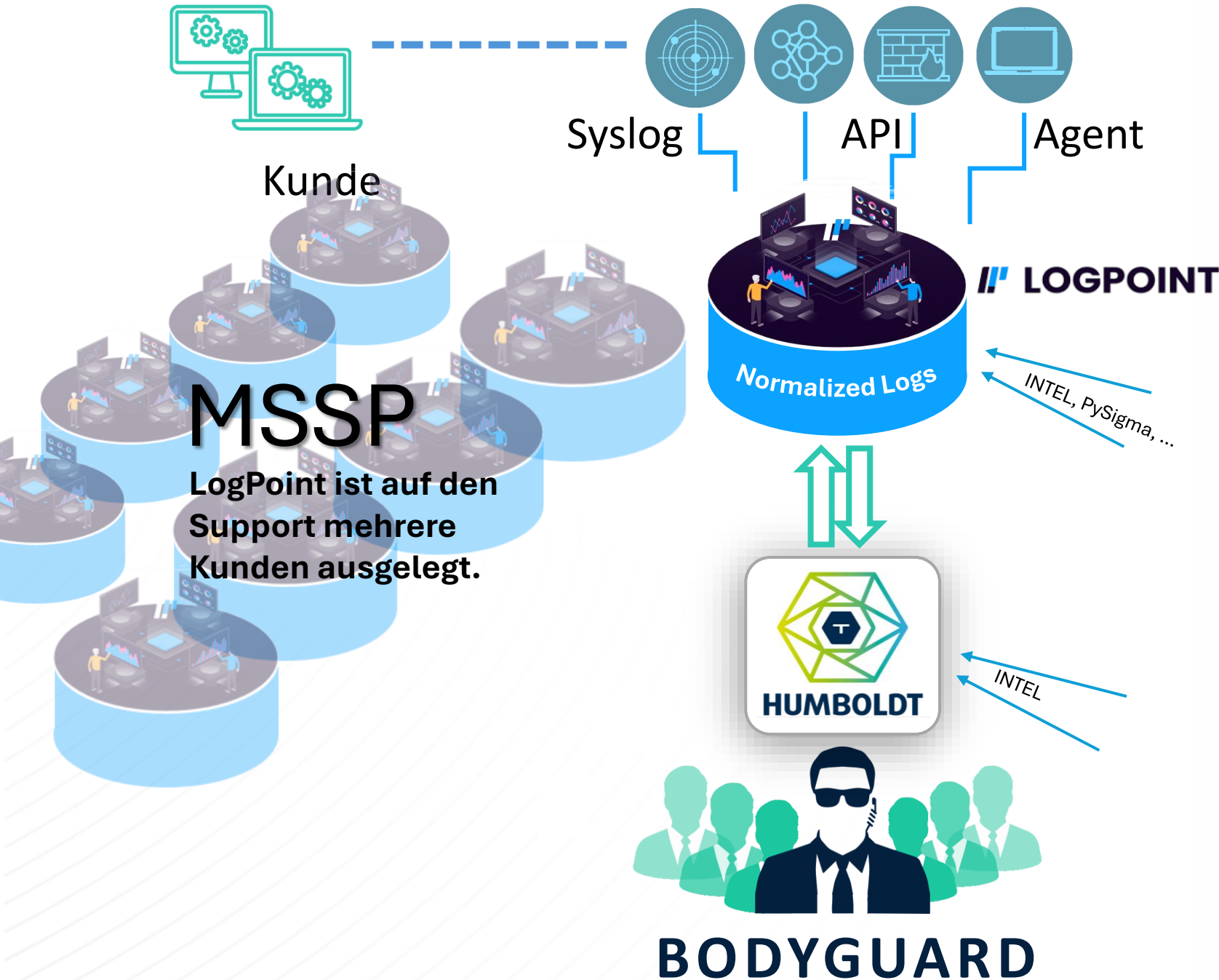
# DER BODYGUARD



## Ihr zentraler Ansprechpartner mit Zugriff auf die Events:

- Ihr Moderator der Detection-Reviews
- Im T-CERT Team
- Threat Hunter, Forensiker
- Infrastruktur Spezialist





Kunde

Syslog

API

Agent

LOGPOINT

Normalized Logs

INTEL, PySigma, ...

HUMBOLDT

INTEL

BODYGUARD

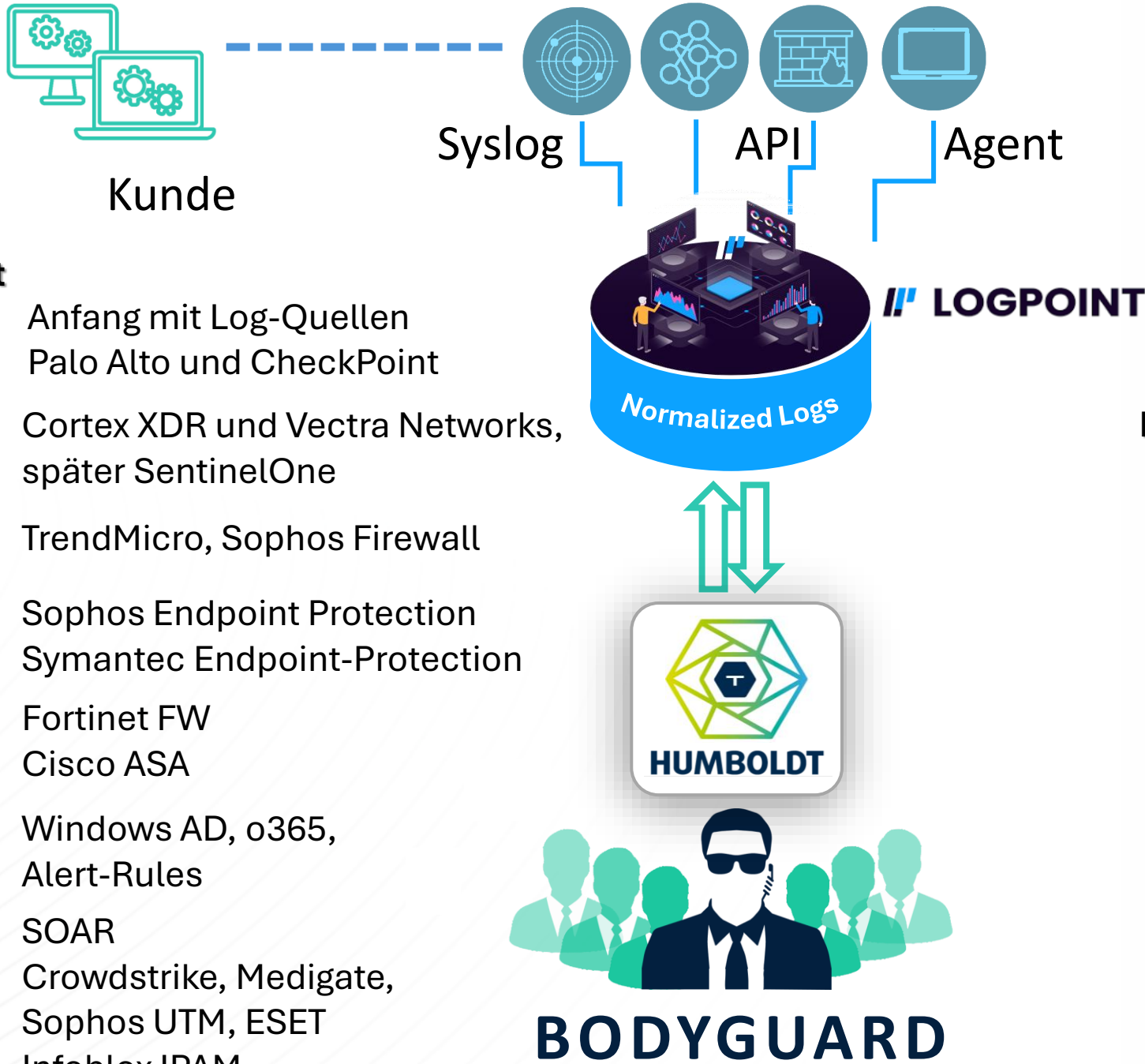
# MSSP

LogPoint ist auf den Support mehrere Kunden ausgelegt.

Die Plattform von Logpoint kombiniert als **SIEM** die Logs der **NDR** und **EDR** und ist somit detektorunabhängig.

Stattdessen haben wir die Freiheit, die Tools auszuwählen, die zu unseren Anwendungsfällen in der Cybersicherheit passen, ohne uns Gedanken über deren Integration machen zu müssen.

**Vorhandene Security-Systeme können integriert werden!**



Die Plattform von Logpoint kombiniert Erkennungen von SIEM, NDR und EDR und ist somit detektorunabhängig, sodass Sie sich nicht auf einen einzigen Anbieter binden müssen.  
 Stattdessen haben wir die Freiheit, die Tools auszuwählen, die zu unseren Anwendungsfällen in der Cybersicherheit passen, ohne uns Gedanken über deren Integration machen zu müssen.  
 ... komplette Transparenz

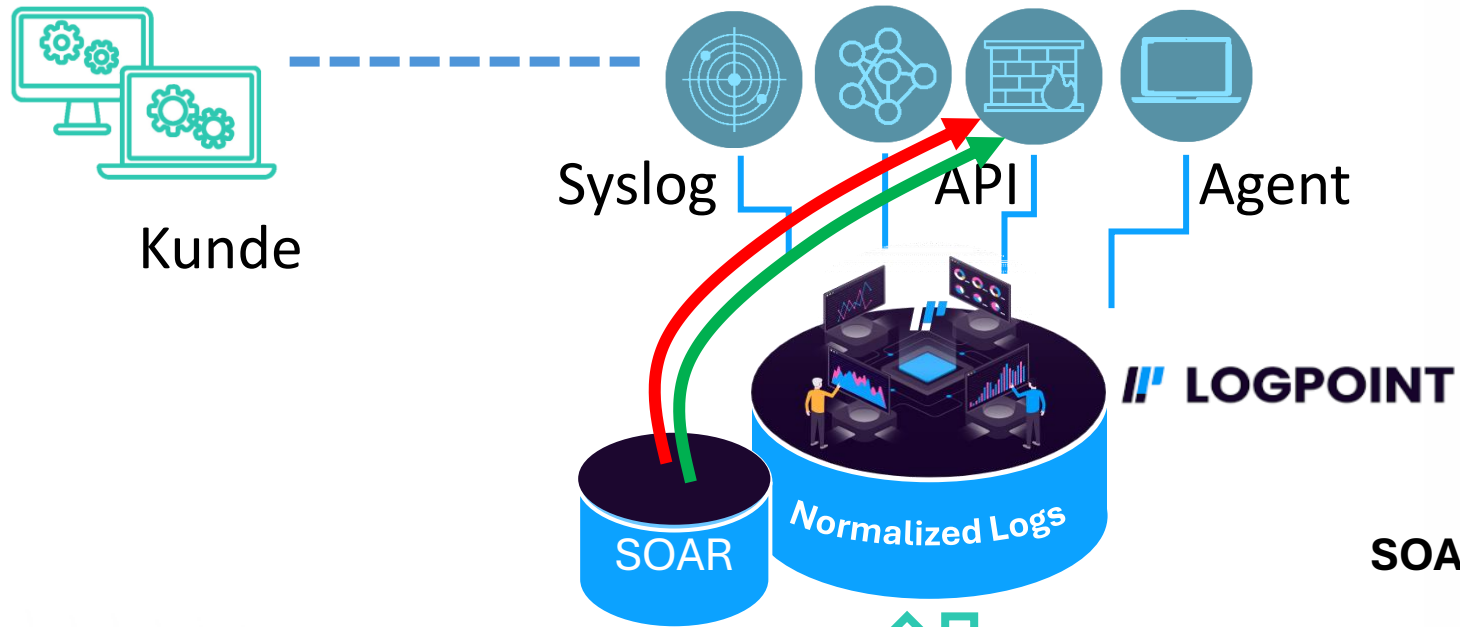
**LogPoint**

- 2020 Unabhängige INTEL-Feed-Integration
- 2022 Unabhängiges Research-Lab
- 2023 SOAR
- 2024 Universal REST-API Fetcher Templating  
 PySigma-Backend for TD  
 Response nativ mit MS  
 MUNINN NDR Integration

**Humboldt**  
2017

- Anfang mit Log-Quellen Palo Alto und CheckPoint
- Cortex XDR und Vectra Networks, später SentinelOne
- TrendMicro, Sophos Firewall
- Sophos Endpoint Protection  
 Symantec Endpoint-Protection
- Fortinet FW  
 Cisco ASA
- Windows AD, o365,  
 Alert-Rules
- SOAR  
 Crowdstrike, Medigate,  
 Sophos UTM, ESET  
 Infoblox IPAM





**SOAR – Reaktion in Sekunden – Lokal**

**Playbooks**, die zusammen mit den individuellen Zugangsdaten dann standardisierte Aktionen ausführen können, die einen SOC-Analysten ergänzen.

- Netzwerk-Quarantäne steuern
- Automatisierte Validation
- Enrichment

SOAR-Playbooks werden individuell mit den Kunden erstellt.

Wir haben einen Katalog mit sehr vielen vorgefertigten Playbooks, die wir nur minimal anpassen müssen, um unsere gewünschten Ergebnisse zu erhalten.

**BODYGUARD**



# Neu 2024 Bodyguards & Experts



**Wiese, Samuel**

Security Analytics (Giants)



**Enders, Daniel**

Security Analytics (Giants)



**Heuer, Sebastian**

Security Analytics (Giants)



**Wu, Lin**

Firewall & Security NOC (Sharks)



**Schmidt, Frank**

Senior Consultant • Security Monitoring (Eagles)



**Lueneburg, Hendrik**

Security Monitoring (Eagles)



**Weber, Joshua Daniel**

Security Monitoring (Eagles)



Chris Stroh  
Technical Director  
Managed Service

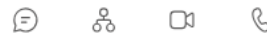


Erich Heinemann  
Leiter T-Cert



**Gruenewald, Philipp**

Firewall & Security NOC (Sharks)



**Geiger, Julia**

Firewall & Security NOC (Sharks)



# BODYGUARD SERVICE

managed detection & response

## // LOGPOINT

Datensammlung ▶ Normalisierung ▶ Usecases & Alerts ▶ SOAR

Humboldt 



▶ **Klassifizierung**

Deduplizierung und Klassifizierung aufgetretener Events in **Humboldt**.

# BODYGUARD SERVICE

managed detection & response

// LOGPOINT

Datensammlung ▶ Normalisierung ▶ Usecases & Alerts ▶ SOAR

Humboldt 



▶ Klassifizierung ▶ Handlungsanweisung & Alerting ▶ **Detection-Review & Reporting**

