



DEFENSE

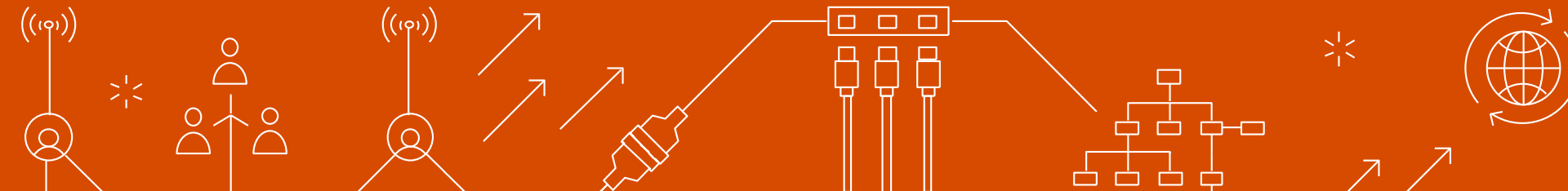




DEFENSE SERVICES

NTS EXPERT TALK

Isabel Wech | Product Manager | NTS
Mathias Spörr | Engineering Manager Defense | NTS

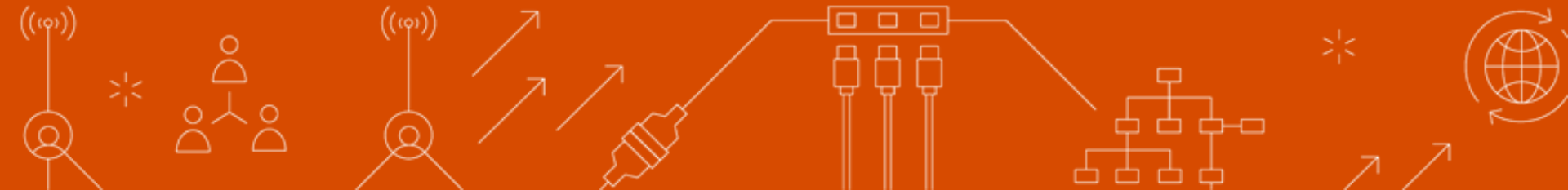


- **NTS DEFENSE TEAM** - Die NTS Security Spezialisten
- **VORSTELLUNG** - NTS THREAT DETECTION SERVICE | SIEM
- **VULNERABILITY MANAGEMENT** - Die Security Basis
- **AUSBLICK** – Wie geht es weiter?



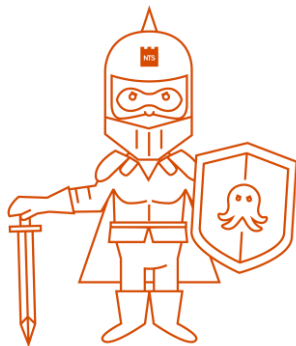
DEFENSE

*Noun /dɪ'fens/
Verteidigung, die*



HERAUSFORDERUNGEN FÜR UNSERE KUNDEN

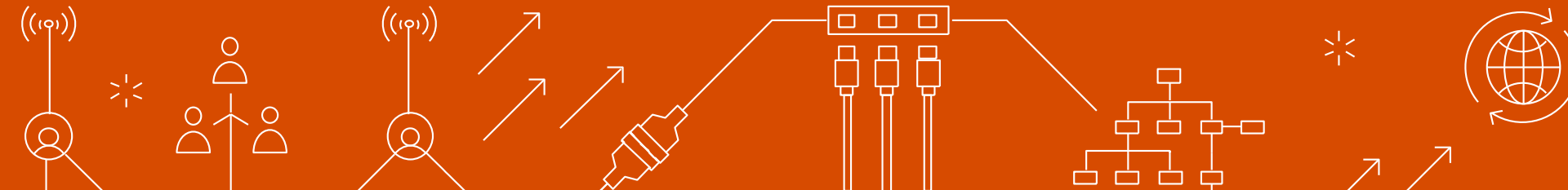
- IT Security ist sehr wichtig, aber auch aufwändig
- Komplexe Zusammenhänge
- Angriffsfläche wird größer und die Bedrohungen verändern sich laufend
- Schwer die richtigen Leute zu finden



NTS DEFENSE
ZU IHREN DIENSTEN

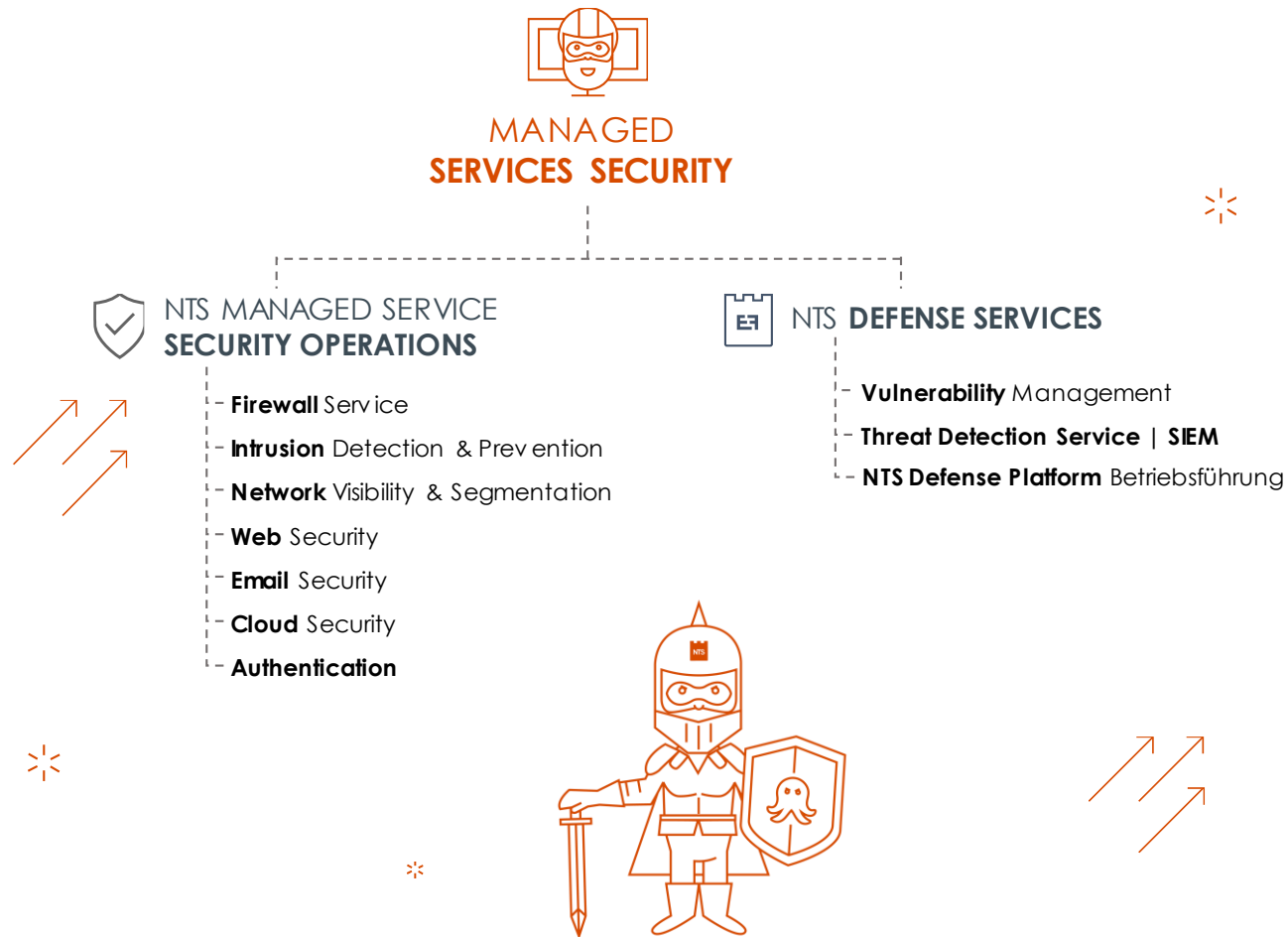


NTS DEFENSE SERVICE-ARCHITEKTUR

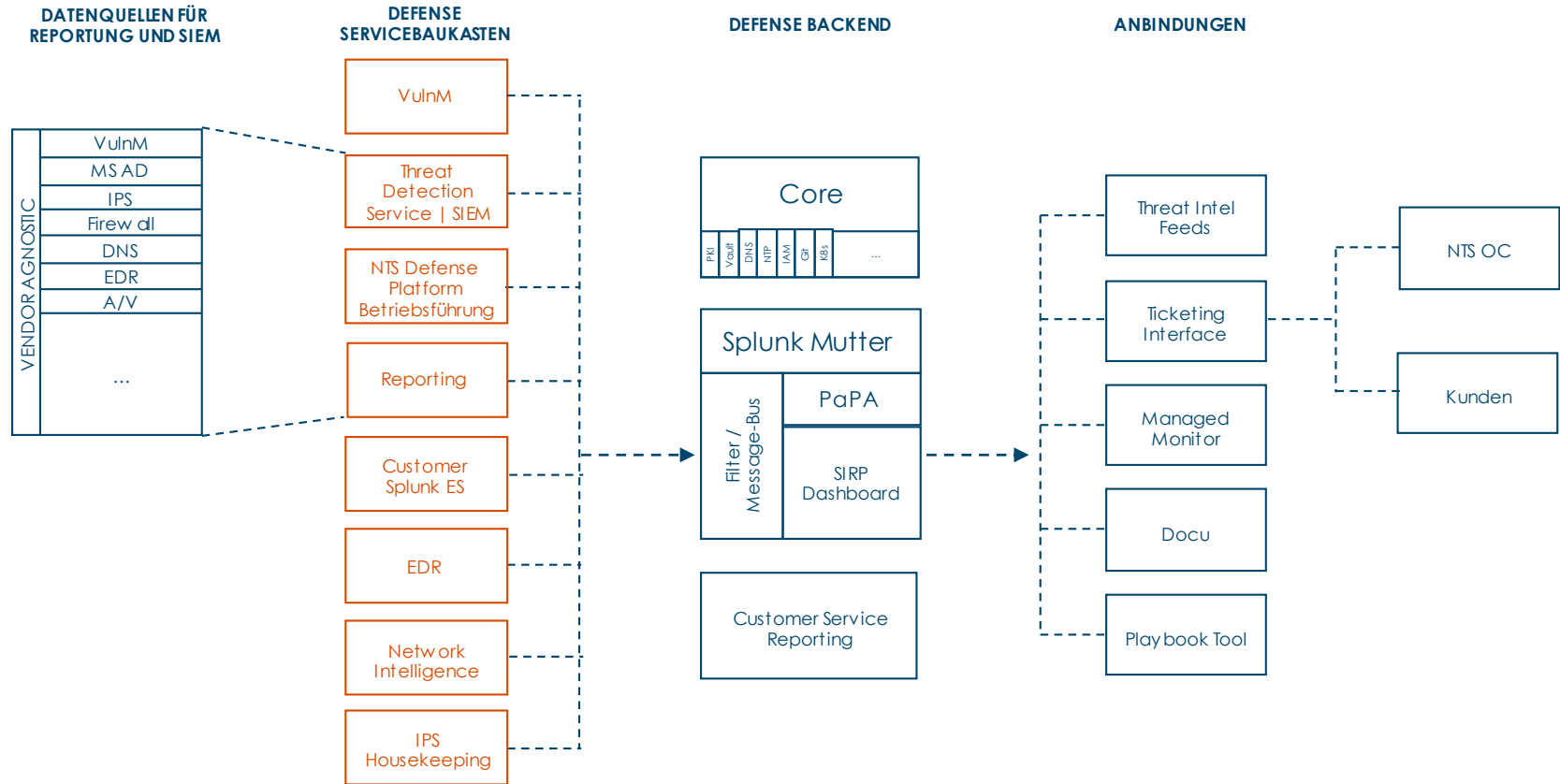




DEFENSE SERVICES



NTS DEFENSE ARCHITEKTUR





NTS DEFENSE ARCHITEKTUR

ECKPUNKTE

Offene Plattform

- Alle Funktionen können vom Kunden genutzt werden
- Die NTS Defense Platform ist erweiterbar (z.B. Splunk Use Cases)
- Die einzelnen Module sind von einander unabhängig, können aber kombiniert werden

INTEGRATION MIT
ANDEREN NTS SERVICES

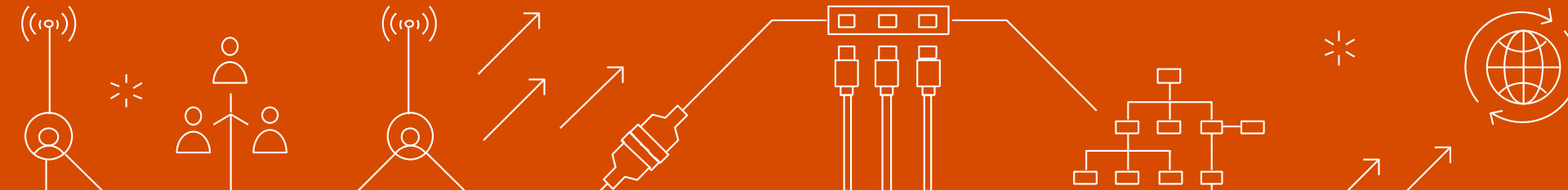


**RELAX,
WE CARE**



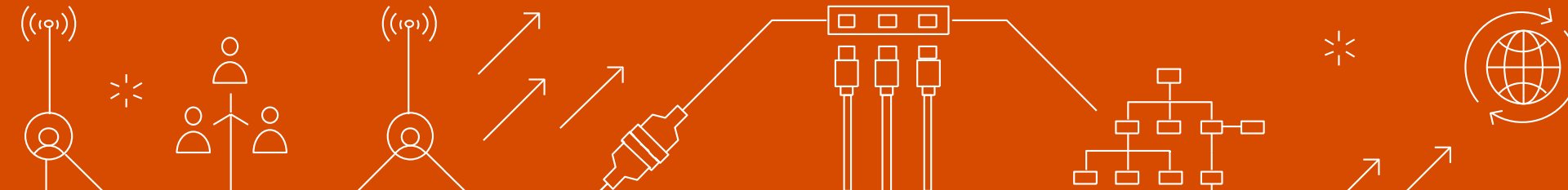
THREAT DETECTION SERVICE | SIEM

Kontinuierliche Analyse zur Entdeckung verdächtigen Verhaltens





SIEM?!



SECURITY INFORMATION AND EVENT MANAGEMENT

... ermöglicht einen **ganzheitlichen Blick** auf die **IT-Sicherheit**, indem **Events** und **Metriken** verschiedener **Systeme** gesammelt und **ausgewertet** werden. **Verdächtige** Ereignisse oder gefährliche Trends lassen sich in **Echtzeit** erkennen.

FOLGENDE PROZESSE WERDEN UNTERSTÜTZT



Log Management



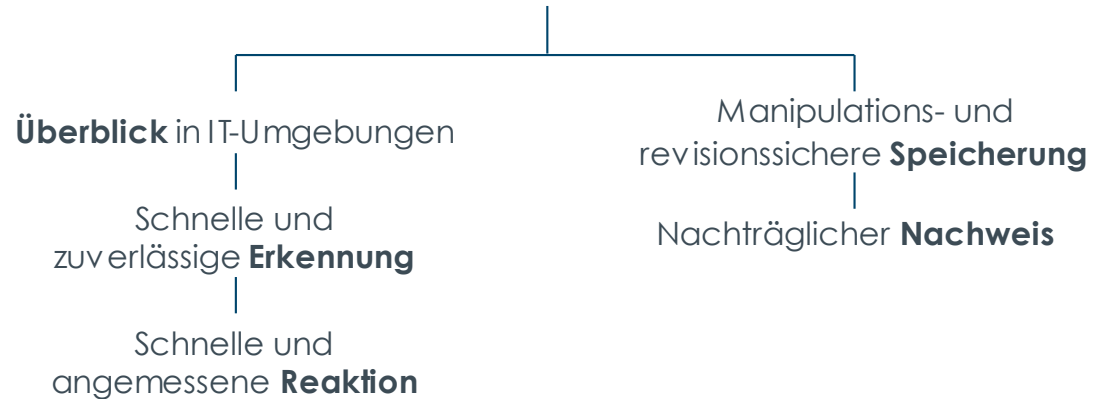
Threat Detection



Compliance

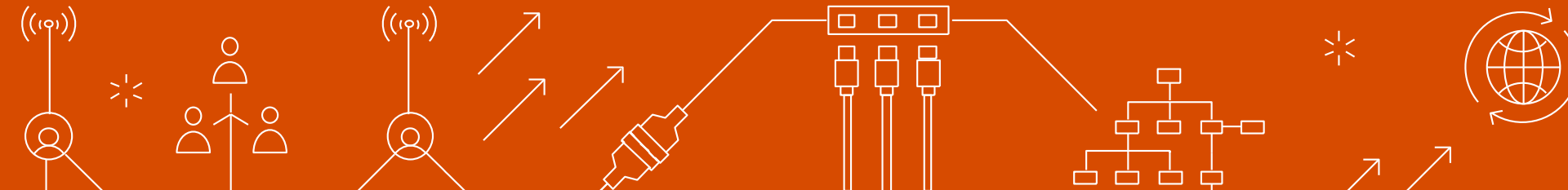


Sicherheitsrelevante Ereignisse





YET ANOTHER SIEM SERVICE?





VORTEILE DEFENSE SERVICE



NTS **Defense Platform**



Offene Plattform und
kein Security Silo



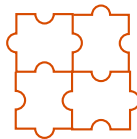
Die **Daten verlassen das Unternehmen nicht**



Umfangreicher **NTS Security Use Case Katalog**



Persönliche Betreuung durch
Defense Analysten



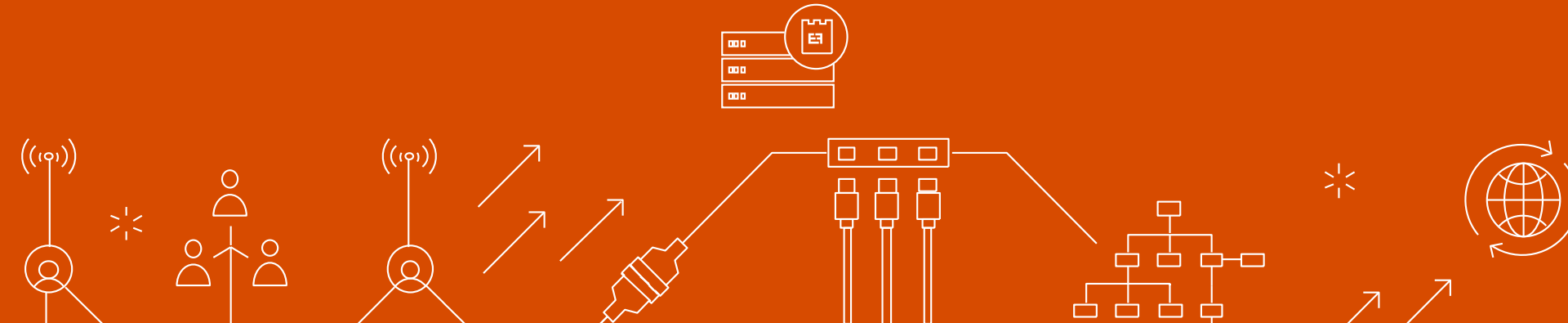
Ein **monatlicher Preis**
über die Laufzeit



Privacy by Design



NTS DEFENSE PLATFORM



SERVICE FIRST!

- Die Infrastruktur muss initial gut durchdacht und aufgesetzt sein
- So viel Automatisierung wie möglich
- Flexibilität und Skalierbarkeit

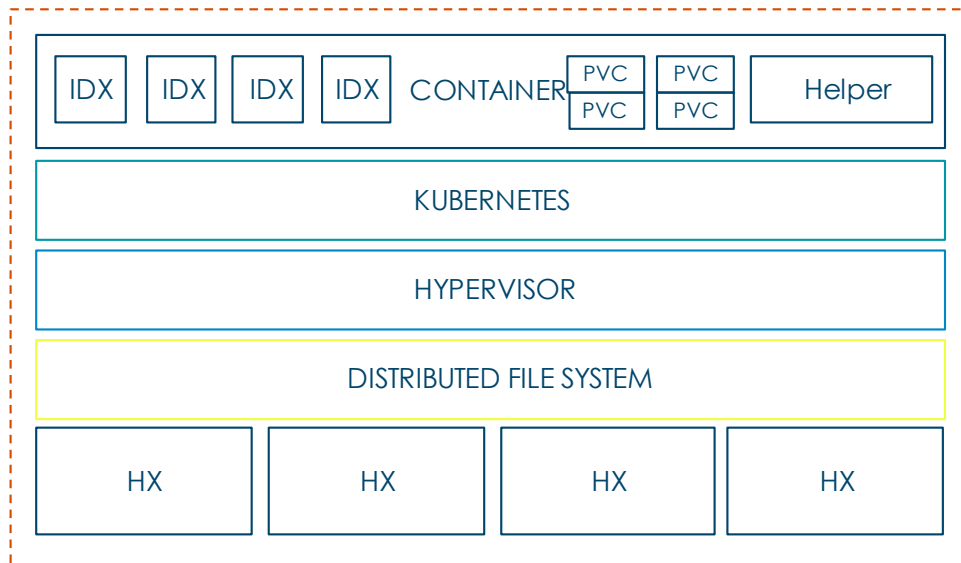


MEHR ZEIT FÜR DAS INCIDENT HANDLING

NTS DEFENSE PLATFORM



CUSTOMER DATA CENTER



**STANDARDISIERUNG DER INFRASTRUKTUR
VON DER HARDWARE BIS ZUR ANWENDUNG**

PLATTFORM - GRÖßEN



Small

Datenvolumen GB/Tag	CPU (Cores / vCPUs)	RAM (GB)	STORAGE (TB)
20-200	80 / 160	160	13,95

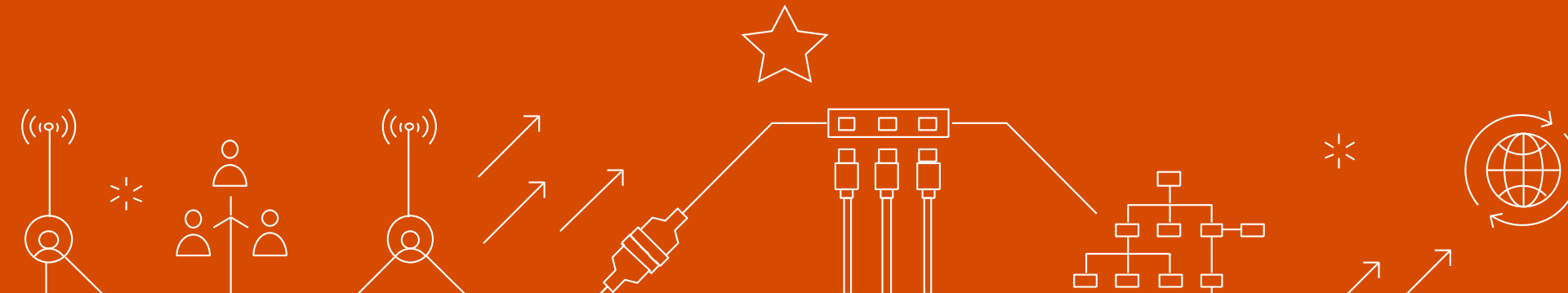


Medium

Datenvolumen GB/Tag	CPU (Cores / vCPUs)	RAM (GB)	STORAGE (TB)
200-500	160 / 320	1344	83,90



OFFENE PLATTFORM UND KEIN SECURITY SILO



WARUM SPLUNK?

NTS

- Einer der Marktführer bei Security Analytics Plattformen
- NTS hat viel Know-How und große Erfahrung mit Splunk



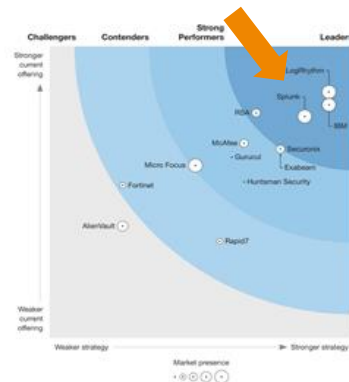
SOLUTIONS REVIEW

Source: 2020 | Solutions Review 509 West Cummings Park | Woburn, MA 01801 | USA



GARTNER MQ

Source: Gartner (February 2020)



FORRESTER WAVE

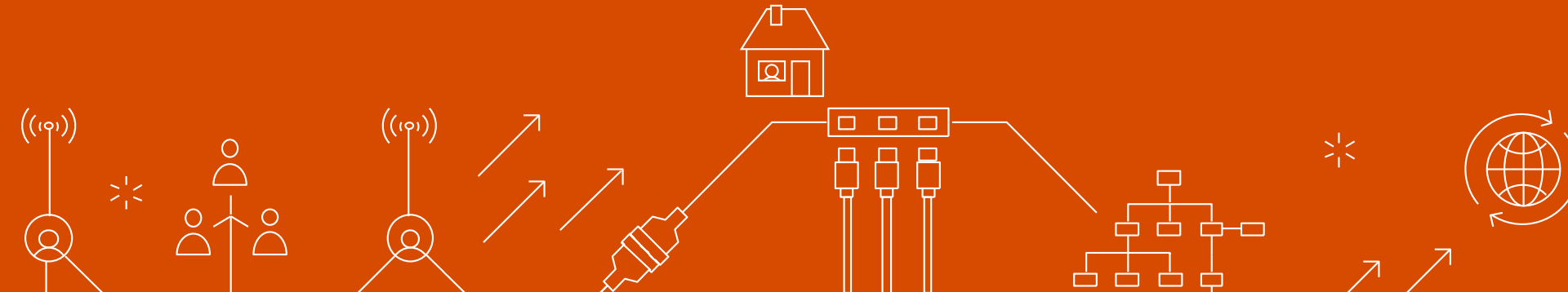
Source: THE FORRESTER WAVE | Security Analytics Platforms | Q3 2018

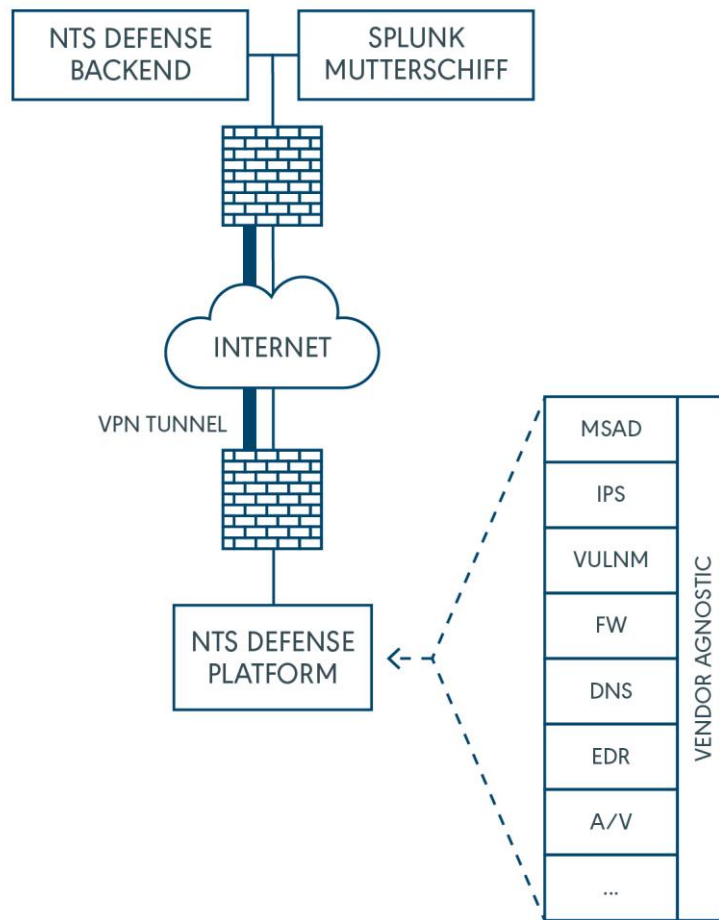
KEIN SECURITY SILO

- Kunde erhält vollen Zugriff auf seine Daten
- Kunde kann die Plattform für eigene Zwecke nutzen
 - IT Operations
 - Business Analytics
 - Predictive Maintenance
 - Compliance
 - ...



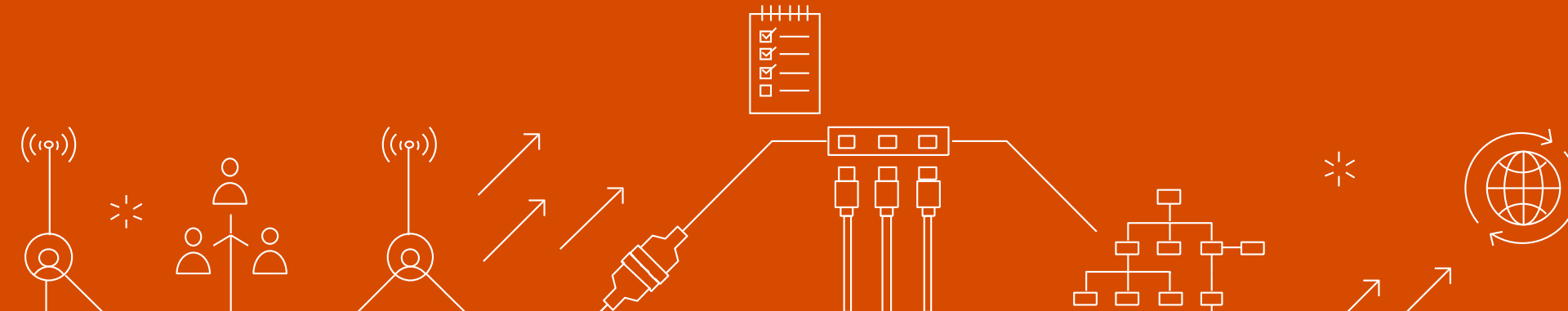
DATEN VERLASSEN DAS UNTERNEHMEN NICHT







UMFANGREICHER NTS SIEM USE CASE KATALOG



USE CASE

“... **Methodology** used by the SOC team **to identify** and **organize technical** and **organizational requirements** for **detection** and response to specific **threats**.”

CYBER KILL CHAIN



Intruder selects target, researches it, and attempts to identify vulnerabilities in the target network.

Intruder creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.

Intruder transmits weapon to target (e.g., via e-mail attachments, websites or USB drives)

Malware weapon's program code triggers, which takes action on target network to exploit vulnerability.

Malware weapon installs access point (e.g., "backdoor") usable by intruder.

Malware enables intruder to have "hands on the keyboard" persistent access to target network.

Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom.

USE CASE BEISPIELE



Externe Firewall Logs können auf Port Scans und andere Reconnaissance Taktiken überwacht werden.

Schwachstellen können mit unserem VulnM Service reduziert werden.

Alarmierung bei unbekannten USB-Sticks oder Aufruf von Phishing Seiten. Erkennung von homographischen Angriffen.

Überwachung von neuen Prozessen und verdächtigen Powershell Befehlen/Scripts.

Erkennung von unbekannten privilegierten Usern oder unerwünschter Software bzw. Registry Modifikationen.

Aufzeigen von P2P Aktivität, Tunneling oder Nutzung von firmenfremden Proxies/VPNs

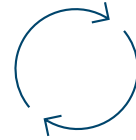
Analyse von seltenen oder unüblichen Prozessen auf Hosts.

VON ANFANG AN GESCHÜTZT



Bis zu 15 Use Cases werden
beim Servicestart
implementiert

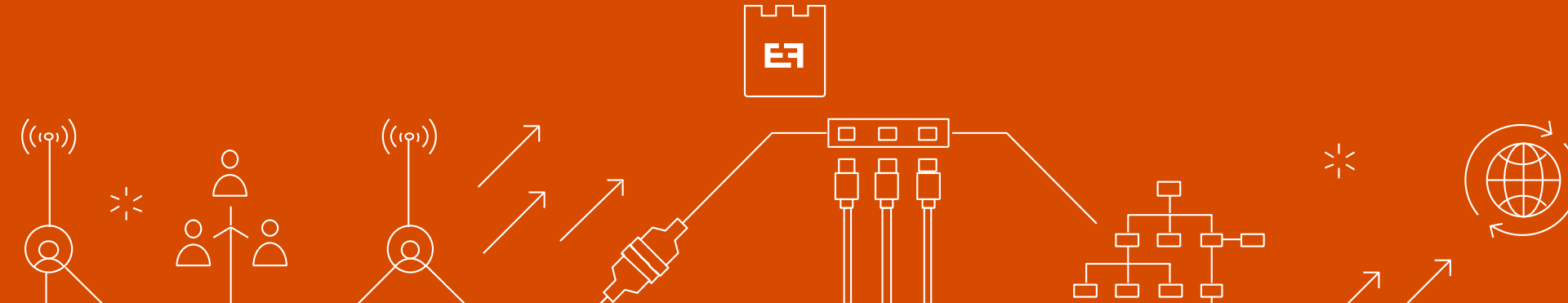
LAUFENDE SERVICEERWEITERUNG



2 weitere Use Cases
werden regelmäßig
hinzugefügt



PERSÖNLICHE BETREUUNG DURCH DEFENSE ANALYSTEN



BETREUUNG DURCH DEDIZIERTE ANALYSTEN

- Kennt die Kundenumgebung
- Tut sich leichter Notable Events richtig einzuschätzen
- Hat langjährige Erfahrung und großes Know How im IT Security Umfeld
- Hat die Stärke vom gesamten Defense Team im Rücken



DEFENSE TEAM



Mathias Spörr



Frederik Ahrens



Daniel Buchberger



Daniel Deuschl



Thomas Fellingner



Julian Kaufmann



Stefan Lembach



Daniel Pauler



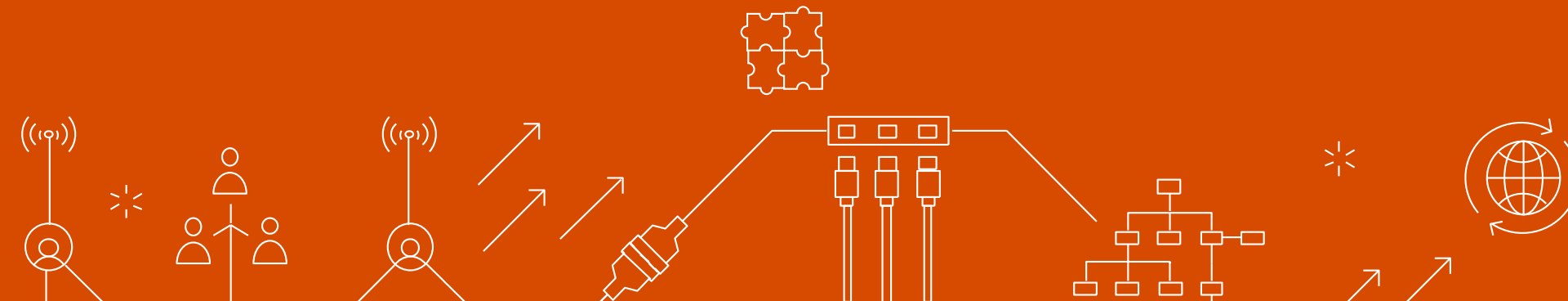
Sebastian Schejbal



Isabel Wech (PT)



EIN MONATLICHER PREIS ÜBER DIE LAUFZEIT



NTS THREAT DETECTION SERVICE | SIEM

- Die **NTS Defense Platform**
- Einrichtung und Betrieb der **NTS Defense Platform**
- **Threat Detection Service**

THREAT DETECTION

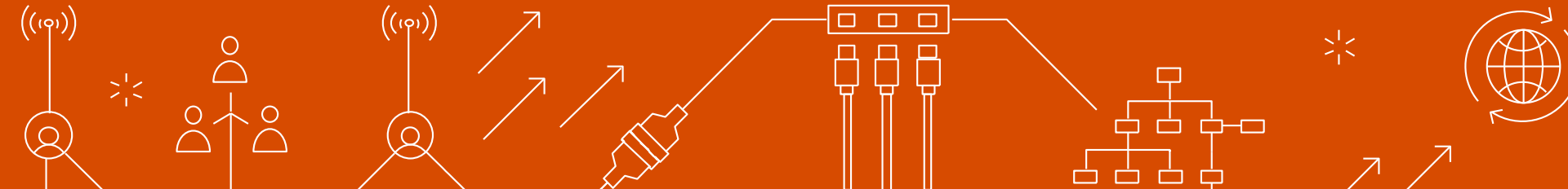
- Incident Handling und Benachrichtigung des Kunden im Falle eines relevanten Alarms
- Dedizierter Defense Kunden Analyst
- Regelmäßiges Reporting und regelmäßige Kundenmeetings
- Use Cases
 - Bis zu 15 beim Start des Service
 - Bis zu 2 Use Cases monatlich oder quartalsweise

NTS DEFENSE PLATFORM

- Design, Aufbau und Implementierung
- Betriebsführung und -verantwortung



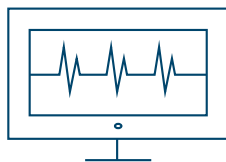
PRIVACY BY DESIGN



PRIVACY BY DESIGN



Privacy Datasheet



Datenminimierung

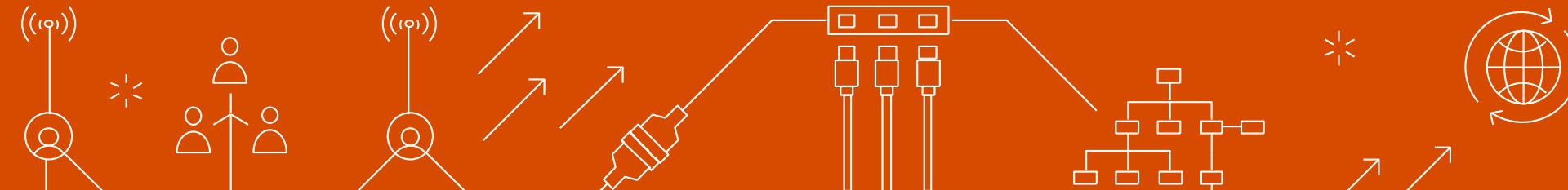


Auftragsverarbeitung
innerhalb der
deutschsprachigen EU



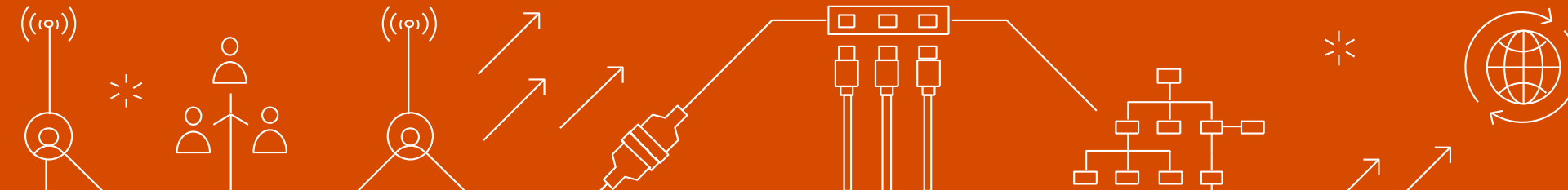
THREAT DETECTION SERVICE | SIEM

Kontinuierliche Analyse zur Entdeckung verdächtigen Verhaltens





VULNERABILITY MANAGEMENT





CIS CONTROLS

BASIC

1. Inventory and Control of Hardware Assets

2. Inventory and Control of Software Assets

3. Continuous Vulnerability Management

4. Controlled Use of Administrative Privileges

5. Secure Configuration for HW and SW on Mobile Devices, Laptops, Workstations and Servers

6. Maintenance, Monitoring and Analysis of Audit Logs

FOUNDATIONAL

7. Email and Web Browser Protections

8. Malware Defenses

9. Limitations and control of Network Ports, Protocols and Services

10. Data Recovery Capabilities

11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12. Boundary Defense

13. Data Protection

14. Controlled Access Based on the Need to Know

15. Wireless Access Control

16. Account Monitoring and Control

ORGANIZATIONAL

17. Implement a Security Awareness and Training Program

18. Application Software Security

19. Incident Response and Management

20. Penetration Tests and Red Team Exercises

WAS IST VULNERABILITY MANAGEMENT?

- Tool-unterstützter Prozess zur kontinuierlichen Erkennung, Bewertung und Behebung von Schwachstellen
 - Software
 - Konfiguration
- Verschafft Überblick über die Umgebung und den Schwachstellen im zeitlichen Verlauf
- Unterstützt Governance-, Risk- und Compliance-Prozesse (ISO27000, PCI,...)

WAS LEISTET NTS?

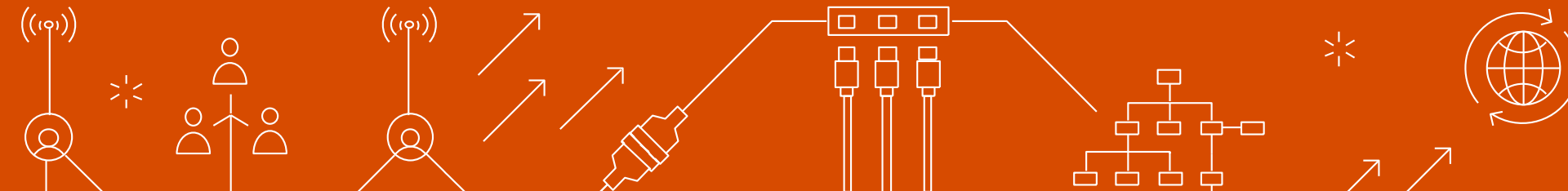
- Design, Aufbau und Implementierung
- Betriebsführung und -verantwortung
- Regelmäßiges Reporting – abgestimmt auf die Zielgruppe
- Kategorisierung und Risiko-Abschätzung der entdeckten Schwachstellen
- Regelmäßige Kundenmeetings
- Dedizierter Vulnerability Manager

VORTEILE IM UNTERNEHMEN

- Unabhängige Sicht von außen – Vermeidung von Interessenskonflikten
- Offenes Security System – Kunde kann selbst Dashboards und Reports erstellen
- Ist mehr als Patch Management

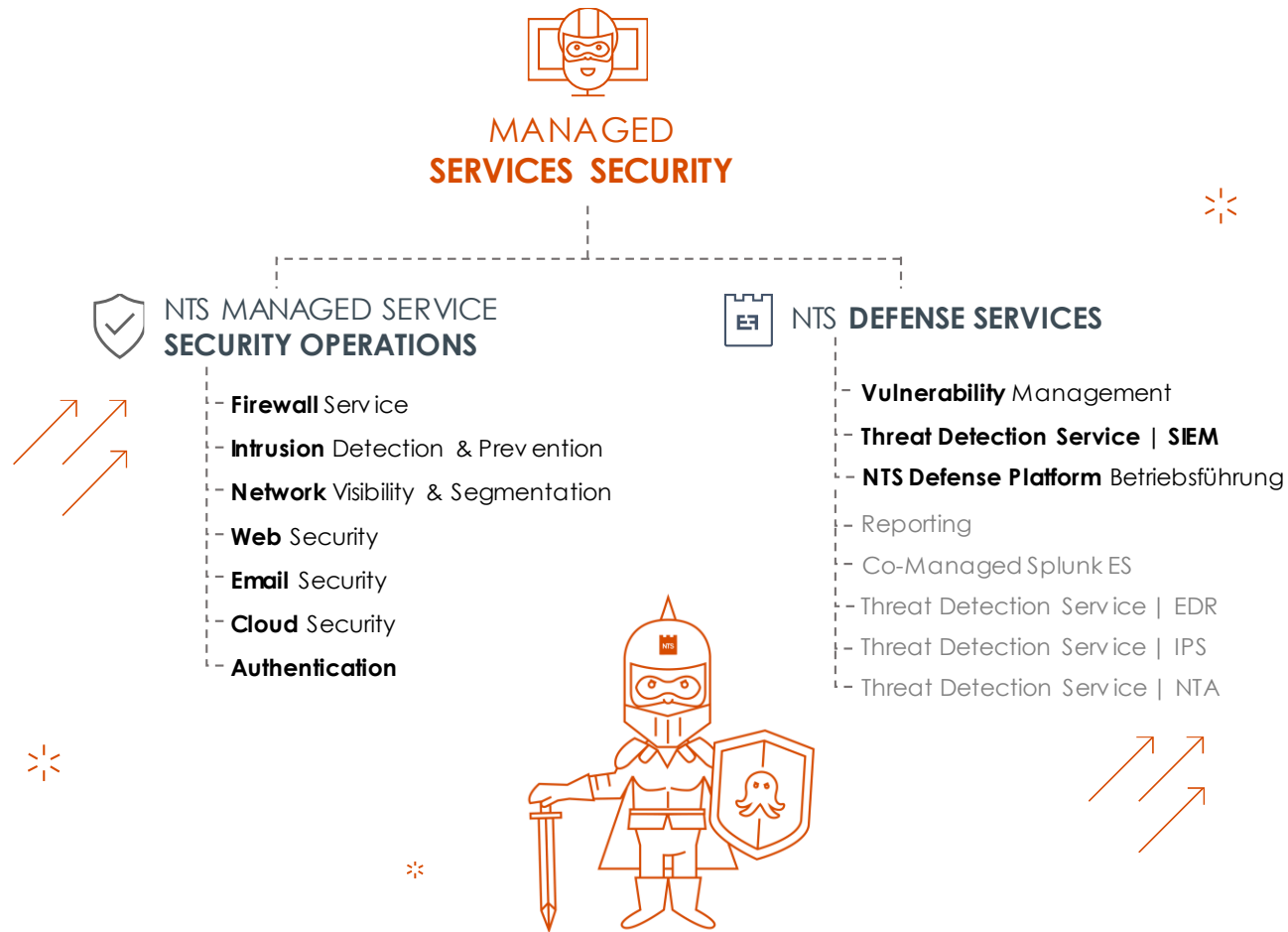


DEFENSE ROADMAP





DEFENSE SERVICES



The NTS logo consists of the letters "NTS" in a bold, sans-serif font, colored orange, centered within a white square.

NTS

FRAGEN?

ISABEL.WECH@NTS.EU
MATHIAS.SPOERR@NTS.EU

