

The logo consists of the letters 'NTS' in a bold, sans-serif font, centered within a white square with rounded corners.

**NTS**

**RELAX,  
WE CARE**



# NTS DEFENSE SERVICES 360° SECURITY

Dominik Mocher | Security Architect  
Dejan Rajkovic | Product Manager

# AGENDA

- Herausforderungen
- NTS Threat Detection Service | MDR
- NTS Incident Response Service
- Zusammenfassung
- Q&A



**WER HAT NOCH NIE EINE PHISHING  
MAIL BEKOMMEN?**

# PHISHING „FRÜHER“

Betreff: Ihr Konto hat ein Problem

Helo [Vorname],

Ihr Konto hat ein große problem. Wir brauchen Ihre Sofortig Antwort. Klicken Sie auf diese hier Link [\[https://example-phishing-site.com\]](https://example-phishing-site.com) und geben Sie Ihre Login Daten ein. Wenn Sie das nicht tun, wird Ihr Konto wird gesperrt.

Wir warten auf Sie Antwort.

Beste Grüße,  
[Dubioser Absender]

# PHISHING „HEUTE“

Hallo [Vorname],

Aufgrund einer kürzlich entdeckten Sicherheitslücke in unserem System führen wir dringend erforderliche Sicherheitsupdates durch, um die Integrität Ihrer Kontodaten zu gewährleisten.

Um sicherzustellen, dass Ihr Konto nicht gefährdet ist, bitten wir Sie, Ihr Passwort zu aktualisieren. Klicken Sie dazu einfach auf den folgenden Link:

[\[https://example-secure-update.com\]](https://example-secure-update.com)

Wir verstehen, dass dies vielleicht unerwartet kommt, aber die Sicherheit unserer Benutzer hat oberste Priorität.

Vielen Dank für Ihr Verständnis und Ihre sofortige Zusammenarbeit.

Freundliche Grüße,  
[Name von IT-Mitarbeiter]

# PHISHING „MORGEN“

ChatGPT 3.5 ▾



You

Kannst du diesen Text so umformulieren, als hätte ihn Jan Böhmermann geschrieben?

**Betreff:** Wichtige Meldung von deinem liebsten Konto-Bodyguard

Moin, moin lieber Fan!

Ich hoffe, du hast deinen Kaffee mit einer extra Portion Ironie getrunken, denn ich hab schlechte Neuigkeiten. Unser Super-Geheim-Konto-Melder hat verdächtige Aktivitäten entdeckt. Klar, da denkt man gleich an Geheimagenten, aber wahrscheinlich sind es nur Langeweile und schlechte Witze.

Klick auf den Mega-Wichtig-Dringend-Update-Link hier: [\[https://www.boehmi-secure-update.de\]](https://www.boehmi-secure-update.de)

Ich weiß, du liebst Sicherheits-Updates genauso wie ich meine fabelhafte Frisur. Also, sei ein Held und rette dein Konto vor den bösen Buben.

Bussi,

Jan Böhmermann



**UND DANACH?**

# RANSOMWARE



# WIE KOMMT ES ZUR RANSOMWARE INFEKTION?

Zugang erlangen

Phishing

Ausnutzen von Schwachstellen

Malware versenden

Erraten der Zugangsdaten

Kontrolle übernehmen

Weitere Geräte infizieren



Zugang ausweiten

Auswirkung am Ziel

Daten abgreifen

Verschlüsseln von Daten

Vernichten von Backups

# WIE KOMMT ES ZUR RANSOMWARE INFEKTION?

Zugang erlangen

Phishing

**NTS VulnM**

Malware versenden

Erraten der Zugangsdaten

Kontrolle übernehmen

**TDS | SIEM**  
**TDS | MDR**

Auswirkung am Ziel

Daten abgreifen

Verschlüsseln von Daten

Vernichten von Backups



**TDS | MDR**

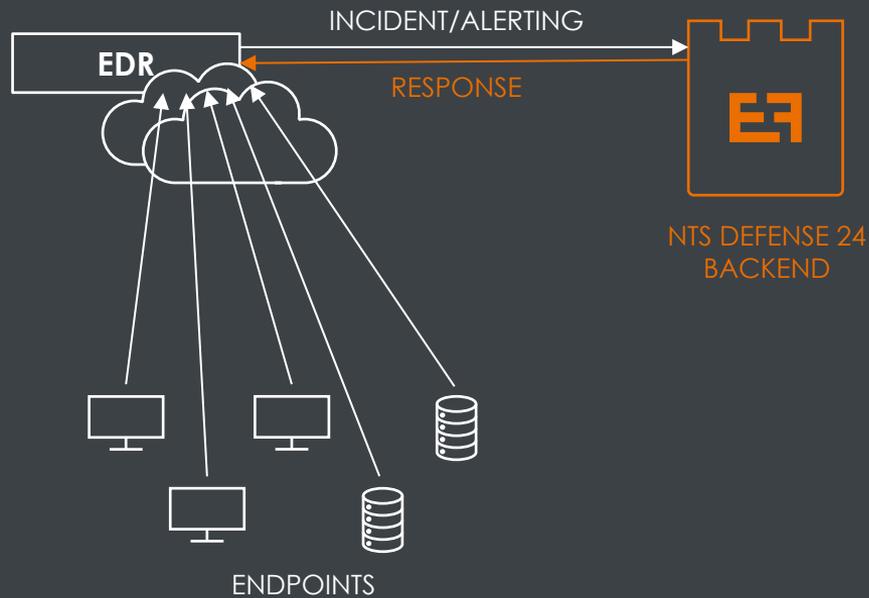
# WAS IST TDS | MDR?

- Managed Detection and Response
- Verwendet Endpoint Detection and Response (EDR) Tools
- EDR analysiert Logdateien am Endgerät

# WAS IST TDS | MDR?

- Alarme werden im Cloud Dashboard angezeigt
- Mit vorgeschlagenen Reaktionsmaßnahmen kann eingegriffen werden
- Reaktionsmaßnahmen müssen für NTS Defense vorab autorisiert werden

# MDR AUFBAU



# EDR LÖSUNGEN

 **paloalto**<sup>®</sup> Cortex XDR Pro  
NETWORKS

 **CISCO** Secure Endpoint

# EDR LÖSUNGEN

- Erkennung von verdächtigen Ereignissen am Endpoint
- Machine Learning-gestützte Bedrohungserkennung
- Berücksichtigt Typisches Verhalten von Benutzer:innen
- Große Anzahl an Reaktionsmaßnahmen



# REAKTIONSMASSNAHMEN

# MÖGLICHE REAKTIONSMASSNAHMEN

- Endpoint Isolation
- Live Terminal Sessions
- Änderungen durch Malware zurückrollen
- Dateien vom Endpunkt abrufen
- Dateien in Quarantäne verschieben

# MÖGLICHE REAKTIONSMASSNAHMEN

- Dateiausführung einschränken
- Löschen verdächtiger Dateien
- Forensische Datenanalyse
- Analyse des Programmspeichers



**UNSER SERVICE**

# UNSER SERVICE



Investigation durch  
Defense Analysten



24/7 Abdeckung



Ergreifen von  
Reaktionsmaßnahmen



Monitoring kritischer  
Assets



Regelmäßige Reports

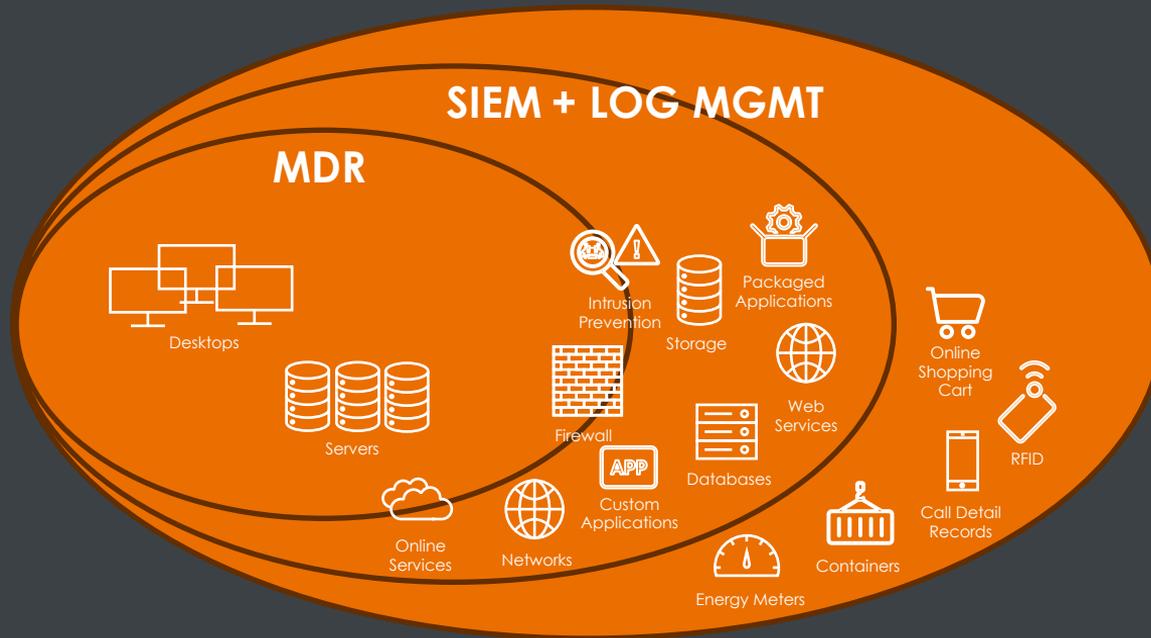


**TDS | MDR UND TDS | SIEM**

# TDS | MDR UND TDS | SIEM

	TDS   MDR	TDS   SIEM
Scope	Schutz der wichtigsten Assets	Vollumfänglicher Schutz
Individualität	Standardisiert	Kundenindividuell
Bedrohungserkennung	Standardisiert	An Kunde angepasst
Datenquellen	Endpoint (optional Next Gen Firewall)	Unlimitiert
Data Retention	30 Tage (Upgrade möglich)	Limitiert durch Disks
Zusatzhardware benötigt	Nein	Ja
Betreuung	NTS Defense Team	Dedizierter Kundenanalyst

# ABDECKUNG





# VORTEILE

# VORTEILE

- Minderung des Risikopotenzials durch Endpoint-Überwachung
- Sicherstellung der Erkennung und Bearbeitung von kritischen Bedrohungen
- Rascher Servicestart – keine zusätzliche Hardware erforderlich
- 24/7 verfügbare hochqualifizierte Security Analyst:innen
- Ergreifen von Reaktionsmaßnahmen auf Kundenwunsch

# VORTEILE

- Transparenz durch Reporting
- Co-Working mit dem NTS Defense Team möglich
- Kann zu TDS | SIEM erweitert werden



**IST MDR DAS RICHTIGE FÜR MICH?**

# IST MDR DAS RICHTIGE FÜR MICH?

Unternehmen ...

... mit limitierten internen Ressourcen

... die Bedarf an zusätzlichem Security Know-how haben

... die Compliance Anforderungen erfüllen müssen

... die einen raschen Schutz benötigen

... die mit einem günstigeren Service einsteigen und skalieren wollen



**UND WENN DOCH ETWAS  
PASSIERT?**



# INCIDENT RESPONSE SERVICE

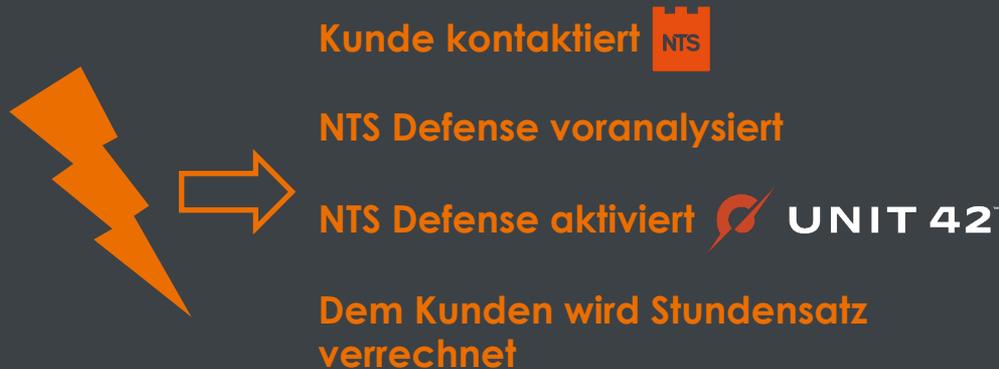
# INCIDENT RESPONSE

- Eindämmung einer Bedrohung
- Bewältigung des Incidents
- Wiederaufnahme des Betriebs
- Hochspezialisiert
- NTS arbeitet mit externen Teams zusammen



# NEU – NTS INCIDENT RESPONSE SERVICE

- Zusammenarbeit mit  paloalto® NETWORKS  UNIT 42™
- Servicekunden zahlen monatliche Bereitstellungsgebühr
- NTS stellt Stundenkontingent im Anlassfall zur Verfügung





**UNSER SERVICE**

# SERVICELLEISTUNG



24/7 Erreichbarkeit



Koordination und  
Unterstützung bei der  
Bewältigung des  
Sicherheitsvorfalls



Unterstützung bei Eindämmung  
und Beseitigung des  
Sicherheitsvorfalls



Unterstützung bei  
der  
Wiederherstellung  
des Betriebs



Verhandlungsführung  
durch Unit42 bei  
Ransomware



# VORTEILE

# VORTEILE

- Absicherung im Falle eines Cyberangriffs
- Übergabe der Führung an ein renommiertes Team von Expert:innen
- Großes Know-how und Erfahrung bei Security Incidents
- Ein Ansprechpartner für Defense Services und Incident Response
- Rasche Unterstützung innerhalb weniger Stunden dank 24x7 Bereitschaft
- Vorteilhaftes Finanzierungskonzept



**IST IR DAS RICHTIGE FÜR SIE?**

# IST IR DAS RICHTIGE FÜR SIE?

Unternehmen ...

... die zu KMUs oder Großunternehmen zuordenbar sind

... mit wenig internen Know-how zu Incident Response

... die Compliance Anforderungen erfüllen müssen (NIS 2)



# ZUSAMMENFASSUNG

# TDS | MDR

MS zur Bedrohungserkennung auf Endpoints

Standardisiert und rascher Servicestart

Einstiegsservice mit Upgrademöglichkeit auf TDS | SIEM

# INCIDENT RESPONSE SERVICE

Support Service zur Absicherung im Falle eines Angriffs

Großes Know-How und Erfahrung

Vorteilhaftes Finanzierungskonzept



**FRAGEN?**



# NTS DEFENSE SERVICES 360° SECURITY