

**EXTRAHOP**

# Abdeckung der NIS2 Anforderungen: „Protokollierung-Detektion-Response“ durch eine NDR-Lösung

Prof. Dr. Dennis Kipker – IT Recht  
Fred Tavas – Area VP DACH  
Oktober 2024

# Agenda

NIS2: Betroffene Branchen und Massnahmen

NDR: Warum und was bringt es eigentlich?

NIS2: Vorgaben und die Umsetzung mit NDR

NDR für NIS2: Zusammenfassung

# NIS2: Betroffene Branchen und Massnahmen

# NIS 2 – neue EU-Richtlinie zu Netzwerk- und Informationssicherheit




**Ab 18. Oktober 2024**

- Registrierung bei nationaler Behörde
- Meldung Sicherheitsvorfälle
- Einhaltung Sicherheitsanforderungen
- Regelmäßiger Compliance-Nachweis (Zertifizierung/Audit)




**Geforderte Cybersicherheits-Maßnahmen**

- Policies/Richtlinien
- Incident Management
- Business Continuity
- Supply Chain Security
- Training
- Asset Management
- Reportingpflicht



**Strenge Meldepflichten**

- Bis 24 Stunden: Meldung Vorfall
- Bis 72 Stunden: Bericht Indicators of Compromise
- Bis 1 Monat: Abschlussbericht



**Strafen**

- Persönliche Haftung der Geschäftsführung
- Hohe Bußgelder bei Verstößen gegen Sicherungsmaßnahmen: bis 10 Mio. Euro oder 2 % des weltweiten Umsatzes

### Betroffene Branchen

**Seit NIS1 KRITIS**

  
Energie

  
Finanzmarktinfrastrukturen

  
Trinkwasser

  
Digitale Infrastruktur/Netze

  
Anbieter digitaler Dienste

  
Gesundheit

  
Verkehr

  
Ernährung

**Seit NIS2 zusätzlich**

  
Forschung

  
Bankwesen

  
Weltraum

  
Öffentliche Verwaltung

  
Abfall

  
Post- und Kurierdienste

  
Abwasser

  
Verwalter von IKT-Diensten

  
Chemie

  
Industrie/Produktion

Unternehmen	Mitarbeiter		Umsatz		Bilanz
Mittel	50–249	und	< 50 Mio. €	und/oder	< 43 Mio. €
Groß	≥ 250	und	≥ 50 Mio. €	und/oder	≥ 43 Mio. €

+ Unternehmen mit kritischer Tätigkeit & Auswirkungen auf öffentliche Ordnung, Systemrisiken oder grenzüberschreitenden Auswirkungen



NDR: Warum und was bringt es eigentlich?

# Full network visibility is essential

## Detect what others can't see !

Threat actors **exploit vulnerabilities** and constantly change TTPs to **evade detection** and magnify impact

**70%**

of network traffic is **encrypted**

**37%**

of organizations' critical **devices are unmanaged**

**47%**

of critical **devices** are **exposed to public internet**

**98%**

of organizations run one or more **insecure network protocols**

## Existing tools are insufficient

### EDR

**doesn't cover all endpoints** and can be evaded

### SIEM

is **not a reliable data source** for detecting attacks and logs can be disabled

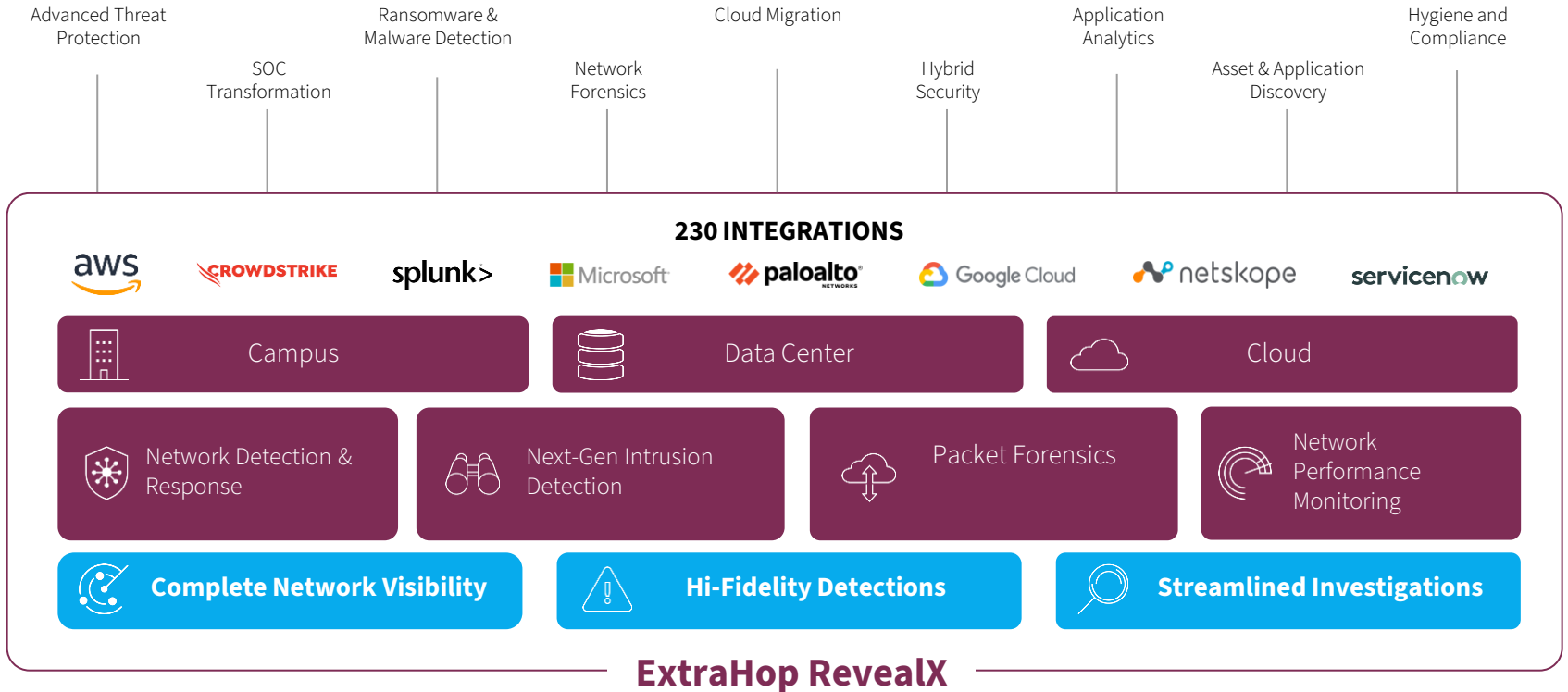
### IDS

**only catches known threats**

### NGFW

**lacks E-W traffic visibility;** data cumbersome to bring into investigation workflows

# Cloud-Native, Network Security & Performance Platform



# NIS2: Vorgaben und die Umsetzung mit NDR

# Risiko-Management

Automatische Erfassung aller Devices, Assets und Kommunikationsbeziehungen (Agenten/Protokolle???)

Dynamische Bewertung der Angriffsfläche

Out of Box Integration der CrowdStrike Threat Intelligence

Überwachung des Risikos aus der Supply-Chain

Grundlage zur Einführung von Zero-Trust

# Protokolierung (Meldepflicht)

Automatische Speicherung jeglicher Netzwerkdaten bis zu 180 Tage

Schneller Zugriff mit Filterung und Triage

Forensik: Wer hat wann/was/mit wem „gesprochen“

Grundlage für proaktive „Threat Hunts“

# Automatische Detektion

Anomalieerkennung mittels KI und ML

Volle Transparenz L2-L7 auch in verschlüsseltem Traffic

Korrelation von Events aus EDR, SIEM und NDR

Detektion von "Living-on-the Land" Attacken

Schnelle Erkennung von „Lateral Movements“

# Automatischer Response

Automatisierte Playbooks (Kill-Chain/Isolierung)

SOC Automatisierung durch SOAR

Reduzierung der Reaktionszeit (MTTR)

Schneller Response mit CrowdStrike Threat Intelligence

# NDR für NIS2: Zusammenfassung



**Risiko-Management**



**Auto-Detektion**



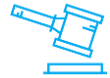
**Auto-Response**



**Protokollierung**



**Dashboard für  
Security-  
Compliance-  
Netzwerk**



**Starker Schutz vor  
Ransomware**

**Vielen Dank!**

**Weitere Infos: H7-347**