NIS2 – Komplexe Herausforderungen und unsere konkreten Lösungen

Jürgen Reinhart, Solution Consultant

Stefan Linnig, Sales Engineer

Teil 1 - 30.01.2025

WITH secure

Unser Ziel ist es, digitales Vertrauen aufzubauen und aufrechtzuerhalten

150,000
Kunden

6,000
Partner

1000
Mitarbeiter

€143m
Umsatz 2023

Führendes europäisches
Cyber Security Unternehmen

70
Nationalitäten

35
Jahre erfolgreich am Markt

Notiert
an der NASDAQ OMX Helsinki Ltd

WITH secure

Cyber Security Technology – der europäische Weg.

Innovation, Privatsphäre, Schutz

WithSecure™ ist ein führender europäischer Anbieter für mittelständische Unternehmen und Managed Service Provider, die nach konformen und effektiven Cybersicherheitslösungen suchen – zugeschnitten auf europäische Standards und den Anforderungen der globalen Märkte insgesamt gerecht werdend.

CYBERSECURITY MADE IN EUROPE

Seit 1988 in Europa ansässig

NIS 2
Konform und Compliance Support Provider

ISO 27001
Zertifiziert und Compliance Support Provider

DORA
Compliance Support Provider

Vom ersten Tag an
Integration von europäischen Regulatorien

GDPR
Konform und Compliance Support Provider

WITH secure

NIS2: Betroffene Organisationen

- Betreiber kritischer Anlagen, bisher als kritische Infrastruktur bezeichnet
- Besonders wichtige Unternehmen (inklusive Betreiber kritischer Anlagen)
- Wichtige Unternehmen

Wer beaufsichtigt und überprüft die infolge von NIS-2 umgesetzten Maßnahmen?

- Oberste Aufsicht – Bundesinnenministerium
- Audits und Konformitätsbescheinigungen - private Institutionen
- VdS 10000 – Informationssicherheit für KMU

Verantwortlichkeit und – spiegelbildlich – Haftung

- **Persönliche Haftung**
  Geschäftsleiter haften persönlich für Fehler im Risikomanagement

- **Schulungen**
  Regelmäßige Schulungen zu Risikomanagementthemen sind Pflicht

- **Unabhängig von Rechtsform**
  Haftung gilt unabhängig von der Rechtsform des Unternehmens

Wie sind bei NIS-2 die Meldepflichten ausgestaltet?

- **Erstmeldung**
  Innerhalb von 24 Stunden nach Kenntniserlangung eines Vorfalls
- **Detailmeldung**
  Innerhalb von 72 Stunden mit erster Bewertung und Indikation
- **Zwischenmeldungen**
  Auf Ersuchen des Bundesamts mit Statusaktualisierung
- **Abschlussmeldung**
  Spätestens einen Monat nach Detailmeldung mit Beschreibung und Maßnahmen

BSI Ansatz sieht vor:
Schnelligkeit vor Vollständigkeit

Maßnahmen und ihre Priorität

Welche Maßnahmen sind von den betroffenen Organisationen mit jeweils welchem Gewicht bzw. welcher Priorität umzusetzen?

- Sicherheitsmaßnahmen treffen
- Systeme aktuell halten
- Meldepflichten beachten
- Risikomanagementsystem aufbauen

Die 10 Mindestanforderungen

Stefan Linnig, Sales Engineer

WITH secure

1

Konzepte zur Risikoanalyse und Sicherheit von IT-Systemen

NIS2 10 Mindestanforderungen: Artikel 21.2(a)

2

Fähigkeit zur Erkennung und Bewältigung von Cybersicherheits-vorfällen

NIS2 10 Mindestanforderungen: Artikel 21.2(b)

3

Möglichkeit die Geschäfts-kontinuität bei Cybersicherheits-vorfällen sicherzustellen

NIS2 10 Mindestanforderungen: Artikel 21.2(c)

WITH secure

4

Sicherheit der Lieferkette verbessern, inkl. Beziehung v. Zulieferern und Dienstanbietern

NIS2 10 Mindestanforderungen: Artikel 21.2(d)

5

kontinuierliche Offenlegung und Handhabung von Schwachstellen

NIS2 10 Mindestanforderungen: Artikel 21.2(e)

6

Konzepte und Verfahren zur Bewertung der Wirksamkeit von Cybersicherheitsmaßnahmen

NIS2 10 Mindestanforderungen: Artikel 21.2(f)

7

Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

NIS2 10 Mindestanforderungen: Artikel 21.2(g)

WITH secure

8

Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung

NIS2 10 Mindestanforderungen: Artikel 21.2(h)

WITH secure

9

Sicherheit des Personals, Konzepte für Asset Management und Access Control

NIS2 10 Mindestanforderungen: Artikel 21.2(i)

10

Verwendung von Lösungen zur Multi-Faktor-Authentifizierung, kontinuierlichen Authentifizierung, etc.

NIS2 10 Mindestanforderungen: Artikel 21.2(j)

Demo

WithSecure Elements Security Center - interaktive Demo

Cheat Sheet

NIS-2 (Mindest)Anforderung	WithSecure
1. Risikoanalyse & Sicherheit v. IT-Systemen	WithSecure Services & Elements Portfolio
2. Cybersicherheitsvorfälle bewältigen	Elements EPP, EDR, MDR, IR Services
3. Geschäftskontinuität sicherstellen	Incident Readiness & Response
4. Sicherheit der Lieferkette	Elements XM, Incident Readiness
5. Schwachstellenmanagement	Elements XM, EPP
6. Wirksamkeit der Maßnahmen	Elements Reports, API
7. Cyberhygiene	Produkte & Services getestet
8. Kryptographie & Verschlüsselung	Elements EPP
9. Asset und Access Management	Elements EPP, XM, Incident Readiness
10. Multi-Factor Authentication	Elements Plattform MFA enforced, XM

WithSecure™ Elements

Proactive and Modular. Made for Co-Security.

Exposure Management

- Attack Paths
- Exposure Score
- Remediation

Extended Detection and Response

- Endpoint Security
- Identity Security
- Collaboration Protection

Co-Security Services

- Elevate
- Co-Monitoring
- Managed Detection and Response
- Incident Response
- Exposure Management
- Countercept

WithSecure™ Support Services

Erweitern Sie Ihr Security Team durch den flexiblen Zugriff auf erfahrene Verteidiger

Bedarf an Detection und Response-Diensten und Risikoprofil

Extended Detection and Response

Elements Software

Elevate

Unterstützung, Untersuchung und Beratung auf Anfrage

Co-Monitoring

Ausgelagerte Überwachung, Untersuchung und Beratung

Managed Detection and Response

Managed Detection and Response

Countercept

„Premium MDR“ mit kontinuierlicher Verbesserung der Sicherheitslage.

Incident Response

Incident Response Service

Exposure Management

Elements Software

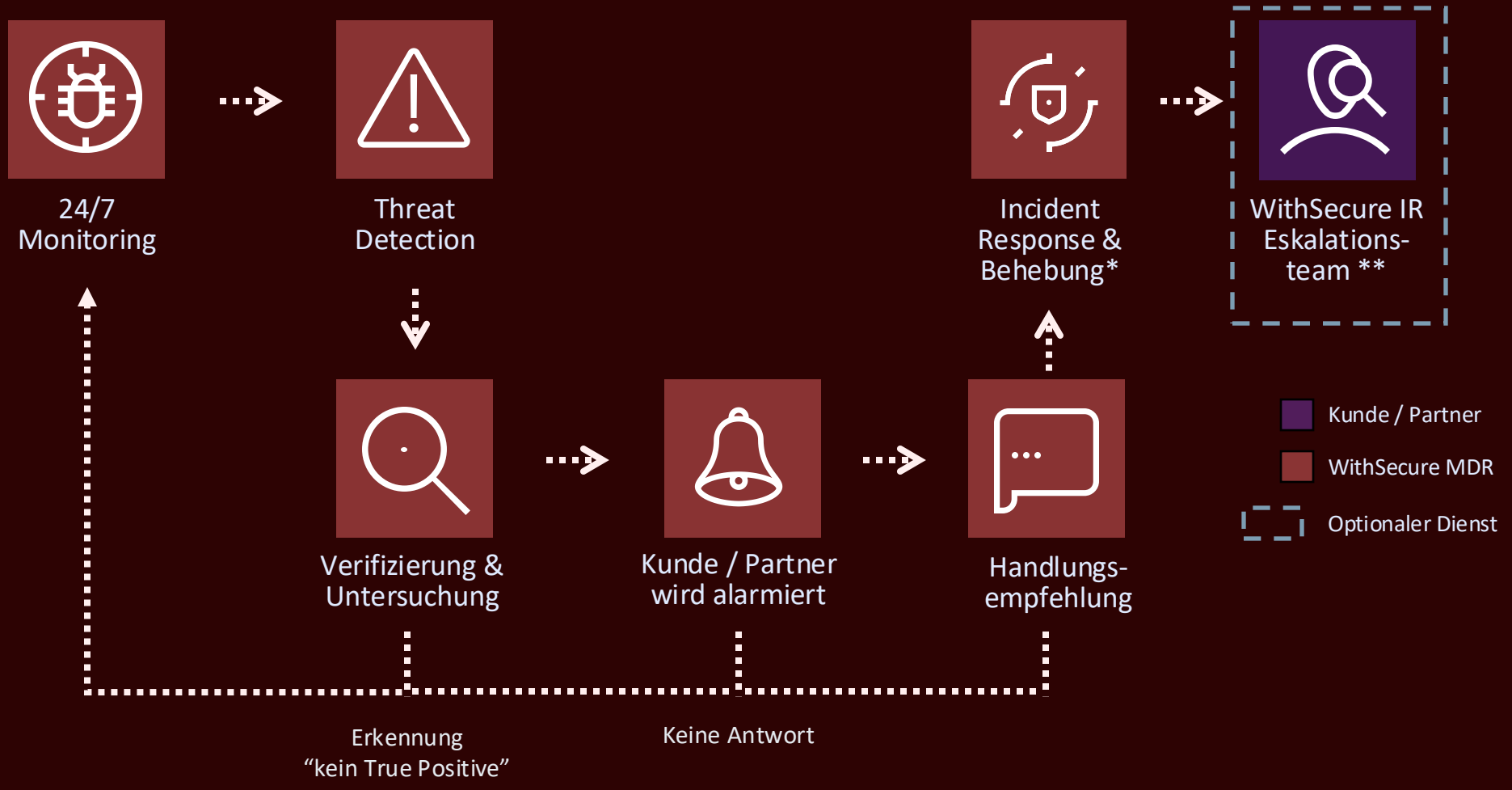
Exposure Management

Exposure Management Service

Menge der von Menschen erbrachten Dienstleistungen

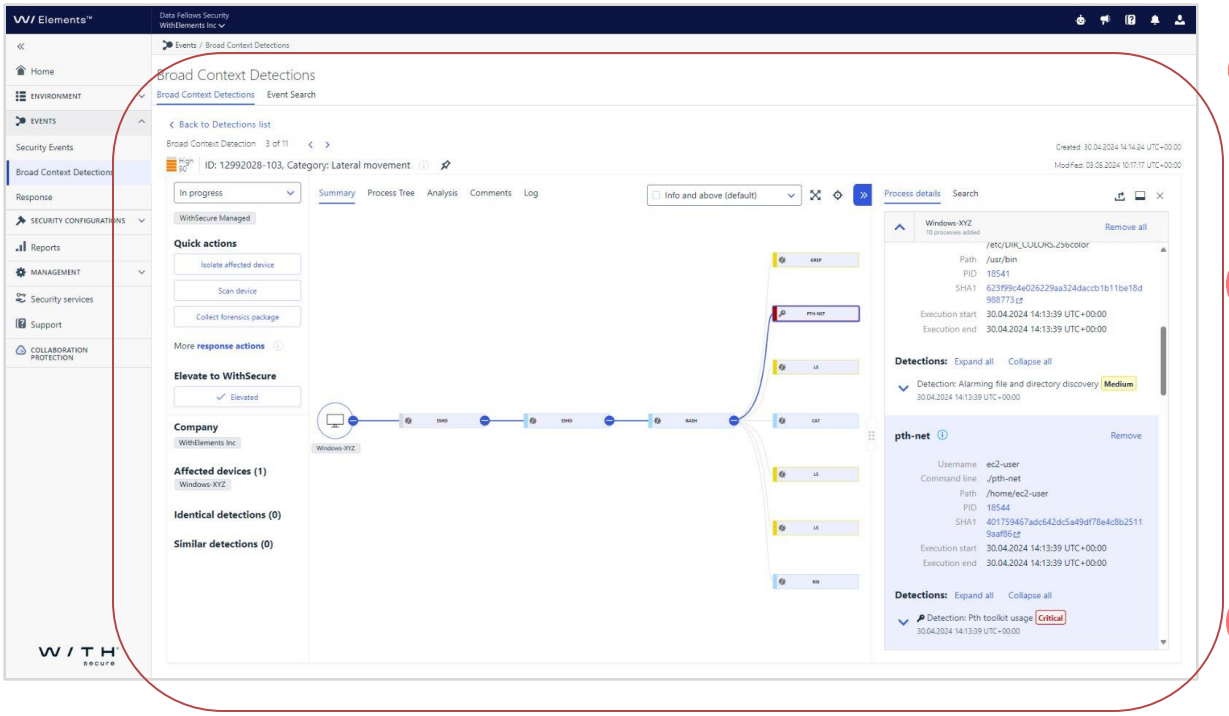
WITH secure

So funktioniert WithSecure MDR



* Für das betroffene Endgerät werden Reaktionsmaßnahmen gemäß der vereinbarten Autorisierung für Server und Clients ergriffen (Vorautorisierung / Explizit / Keine).
* * Erfordert die Zustimmung des Kunden oder einen bestehenden IR-Dienst wie Incident Response Retainer.

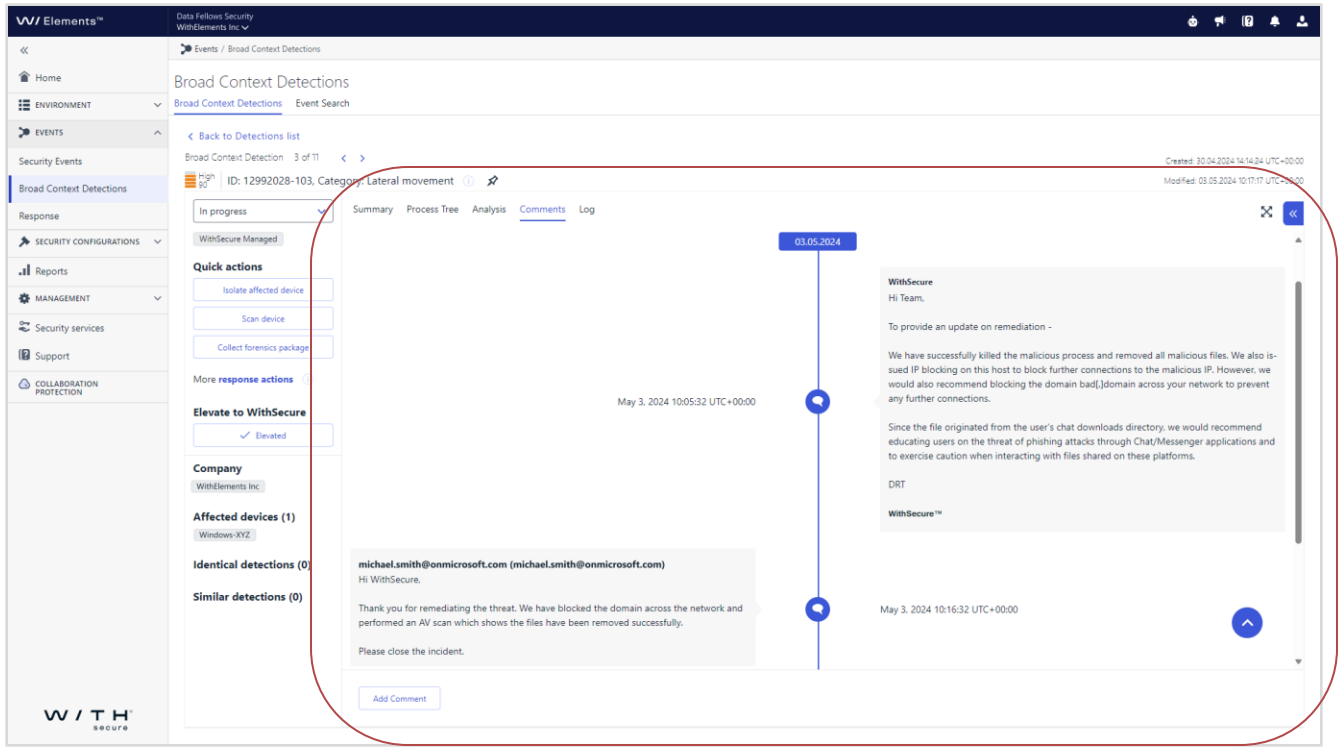
Bleiben Sie über Elements EDR auf dem Laufenden, während wir uns um Ihre Erkennung und Reaktion kümmern



Zusammenfassung der umfassenden Kontexterkennung auf unserer WithSecure Elements Cloud-Plattform, mit Optionen für schnelles Handeln.

- WithSecure™ MDR ist ein betrieblich effizienter und kostengünstiger Dienst für kontinuierliche Überwachung, Erkennung und Reaktion.
- Die Bearbeitung von Vorfällen erfolgt durch die erfahrenen Mitglieder unseres Detection and Response Teams (DRT), die das vereinte Wissen unserer branchenweit anerkannten Forscher, Entwickler, Operator und Incident Responder nutzen.
- Verwendet die Broad Context Detections™ (BCD), Telemetrie- und Reaktionsfunktionen von WithSecure™ Elements EDR.
  - Mit Elements EDR erhalten Sie umfassende Einblicke in Ihre digitale Infrastruktur, ohne sich Sorgen machen zu müssen, dass Sie Warnmeldungen zu Sicherheitsvorfällen verpassen.

Beinhaltet Incident Response



Ein Kunde wird über einen Sicherheitsvorfall informiert und unser Detection and Response Team (DRT) behebt das Problem und gibt weitere Hinweise zu den nächsten Schritten.

- In unserem 24/7 verfügbaren Managed Detection and Response-Dienst dämmen die WithSecure™-Experten vom DRT die Vorfälle auf Ihrem Endgerät* ein und beheben sie, bevor diese sich auf Ihr Geschäft auswirken können.
- Incident Response ist über die automatische Isolierung hinaus automatisch in Ihrem WithSecure™ MDR-Abonnement* enthalten.
- Wenn es zu einem groß angelegten Vorfall kommt, der mehrere Endgeräte betrifft, werden Kunden über zusätzliche Incident Response (IR)-Dienste informiert.**

* Kunden von WithSecure™ Managed Detection and Response haben bedingten Zugriff auf qualifizierte Incident-Response-Ressourcen. Vorfälle werden von unseren erfahrenen und offensiv denkenden Bedrohungsanalysten im Detection and Response Team (DRT) bearbeitet. Größere Vorfälle, bei denen mehrere Geräte betroffen sind, erfordern zusätzliche Incident-Response-Dienste.
** Die zusätzlichen IR-Dienste von WithSecure durch unser Incident Response-Team sind seit 2013 vom britischen National Cyber Security Centre zertifiziert, als eine von nur 9 IR-Organisationen, die für die Bewältigung der komplexesten Vorfälle kompetent sind. Sie sind auch vom deutschen Bundesamt für Sicherheit in der Informationstechnik zertifiziert.

Weitere Informationen

NIS-2 Infoseite

https://www.withsecure.com/nis2-infoseite

Webinar-Serie:

- ❑ Teil 1 am 30.01.25
  NIS2 – Komplexe Herausforderungen und unsere konkreten Lösungen
- ❑ Teil 2 am 19.02.25
  NIS2 & Compliance - Rechtliche Vorgaben umsetzen und Bußgelder vermeiden
- ❑ Teil 3 am 26.03.25
  Von der Theorie in die Praxis – So setzen unsere Partner NIS2 um

WITH secure

Q & A

WITH secure

WITH®

secure