Wie sie die NIS2 Direktive mit Palo Alto Networks umsetzen können

Christian Kurta Systems Engineer - Austria

Eine Flut von vernetzten Geräten wird die Möglichkeiten für Angriffe erhöhen

WACHSENDE ANGRIFFSFLÄCHE

2.6Mrd

vernetzte IT/OT-Geräte bis 2030, eine Steigerung um 400 % gegenüber 2020

paloalto NETWORKS

Sind somit auch große Risiken für den Betrieb

Ukrainian Electric Grid Attack

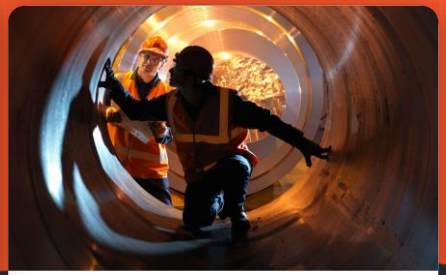
Angriffe auf das Stromnetz, die zu Stromausfällen führen

Oiltanking Tanklager Deutschland

Gezielt Öl und Gas, Nuklearindustrie und verarbeitendes Gewerbe

Norsk Hydro Ransomware Attack

Betroffen ist die Aluminiumproduktion in 170 Werken



Colonial Pipeline Hack

Verursachte Kraftstoff- und Benzinknappheit

10 erfolgreiche Ransomware-Angriffe auf das verarbeitende Gewerbe jeden Monat in 2022! FBI Internet Crime report 2021

*HIPAA Journal 2021

NIS2 in Österreich - Wen betrifft es?

- + Vor-Ort Kontrollen +Stichproben
- +AD-Hoc Prüfungen
- Regelmäßige Security Audits
- Cybersecurity Konzepte
- Anforderung des Zugangs

WESENTLICHE EINRICHTUNGEN

- Security Scans
- Cybersecurity Konzepte
- Anforderung des Zugangs

WICHTIGE EINRICHTUNGEN

paloalto NETWORKS

Wie kann ich mich auf NIS2 vorbereiten?

Angriffsfläche verstehen mit einer umfangreichen Beurteilung der Schwachstellen

Organisatorische Maßnahmen

- Sicherheitsüberprüfung durch NIS2 akkreditierte Stelle
- Cybersecurity Konzepte
- Verpflichtung zur Übermittlung von Informationen
- Anforderung des Zugangs
- Backup-, Notfall- und Krisenmanagement
- Schulungen

Technische Maßnahmen

- Advanced Threat Prevention
- Risikomanagement
- Attack Surface & Vulnerability Management
- Koordinierte Offenlegung von Schwachstellen & Automatisierung
- Multifaktor-Authentifizierung & UEBA
- Gesicherte Kommunikation

- Aktive Prevention, Detection und Mitigation von Angriffen
- Komplette Sicht aller Assets in der Cloud, On Premise und deren Schwachstellen
- End-to-End Kontrolle über alle Applikationen und gesicherte Kommunikation

Ein Unternehmen benötigt 10+ Punktlösungen für die NIS2 Umsetzung

paloalto NETWORKS

Konsolidierung durch eine AI-Unterstützte, modulare Plattform

Unternehmen konsolidieren ihre Punktlösungen

Versteckte Kosten der Punktlösungen

96%
organizations attacked in the last year *

33%
Security experts experienced operational disruption as a negative consequence of a breach*

$2.4M
average cost to recover from a breach **

Unser Plattformansatz

77%

security executives believe it is critical to **reduce the number of security solutions and services** *

Der Outcome für den Kunden

- **Security Posture**
- **Operational Efficiency**
- **Simplicity**
- **Cybersecurity Unit Cost**

Source: * Palo Alto Networks "What's Next in Cyber" survey;
** Forrester; Palo Alto Networks; Business Value Consulting analysis

Unsere modulare AI/ML Plattform seit über 10+ Jahren

Network Security

Industry leading Zero Trust network architecture

2019

- First ML powered NGFW
- Acquired CloudGenix SD-WAN*
- NFGW IoT*, DLP, DNS, SD-WAN subs
- CN-series for 5G infrastructure
- Autonomous Digital Experience Mngt*
- Next-Gen CASB*
- AIOPs & Advanced Wildfire
- Next-Gen Remote Browser Isolation*
- PAN OS 11.0
- Medical IoT Security
- Deep Learning NGFW
- Zero Trust OT Security

2023

Cloud Security

Comprehensive code-to-cloud platform

2019

- Acquired Redlock*
- Prisma Cloud 1.0
- Container Cloud Security*
- Serverless Cloud Security*
- IAM Security
- Data Protection
- Microsegmentation*
- Web App & API Security
- Shift-Left CI/CD Security*
- SW Supply Chain Security*
- AI-Powered ADEM

2023

SOC Security

Game changing SecOps underpinned by AI

2019

- Cortex XDR 1.0
- Acquired Demisto for XSOAR*
- Cortex XSOAR with Threat Intel Mngt
- XDR Host Insights
- Acquired Xpanse for ASM*
- Cortex XSOAR Marketplace
- XDR 3.5 with cloud / ID analytics
- XSIAM
- Identity Threat Detection & Response

2023

Advisory & IR

Trusted cybersecurity partner of choice

2019

- Acquired Crypsis Group*
- Ransomware readiness
- Cloud incident response services
- Expert threat briefings
- Expert malware analysis
- Forward Deployed Analyst
- New Proactive Services

2023

*14 Acquisitions

NIS2 mit 3 Produkten und einem Partner

SUB-CATEGORY	NETWORK SECURITY
Firewall	Network Security
Intrusion Detection	
URL Filtering	
Sandbox Detection	
DNS Security	
IoT Security	
Data Loss Prevention	
Cloud Access Security Broker	
Posture and Health Management	
Remote Access for Users	
SWG	
SD-WAN	

SUB-CATEGORY	CLOUD SECURITY
Cloud Security Posture Management	Prisma Cloud
Cloud Workload Protection	
Identity & Access Management	
Code Security	
Web Application / API Security	

SUB-CATEGORY	AUTONOMOUS SOC
Security Information & Event Management (SIEM)	Cortex XSIAM
Endpoint + EDR	
NTA / UEBA	
SOAR	
Attack Surface Management	

Unsere Cybersecurity Formel - mit LLM & AI

Integrierte Telemetriedaten

Networks Cloud Endpoints

+

ML / AI Automatisierung

Strata NGFW

Cortex XSIAM

Cortex XSOAR

=

Improved Cyber Resilience

Mean Time to Respond
(High priority alerts)

Vielen Dank

Christian Kurta | Systems Engineer | Austria