



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

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

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**

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

NIS2 THEMA

CISO THEMENGEBIET

CYBERSECURITY TOOLS

Übermittlung von Informationen	Data Security	Application Security	Identity & Access Management	Data Loss Prevention, Endpoint Encryption, Data Classification, Cloud Access Security Broker, Single Sign-On, Privileged Access Management, Dynamic Application Scanning, Container Security, Static Code Analysis, Web Application Firewall, Identity Management, Multi-Factor Authentication
Cybersecurity Konzepte	Governance, Risk & Compliance	Security Operations	Security Services	Risk Monitoring, Supplier / Partner Risk Management, Regulatory / Industry Mandate Compliance, Risk Statistics, Session Replay / Packet Capture, Security Monitoring, Digital Forensics, Log Correlation & Analysis, Event Ticketing, User Behavioural Analysis, Malware Analysis
Aktive Mitigation	Cloud Security	Security Operations	Endpoint Security	Threat Intelligence Management, Threat Investigation, SOAR, Container Security, System Hardening & Intrusion Detection, Serverless Computing, Malware Scanning for Storage, Cloud System Hardening & Workload Protection, Endpoint Protection
Asset & Vulnerability Management	Cloud Security	Application Security	Identity & Access Management	Dynamic Application Scanning, Container Security, Static Code Analysis, Web Application Firewall, Single Sign-On, Privileged Access Management, Identity Management, Multi-Factor Authentication
Multifaktor & UEBA	Data Security	Application Security	Identity & Access Management	Data Loss Prevention, Endpoint Encryption, Data Classification, Security Broker, Scanning, Security, Static Code Analysis, Web Application Firewall, Single Sign-On, Privileged Access Management, Identity Management, Multi-Factor Authentication
Advanced Threat Prevention	Network Security	Security Services	Endpoint Security	Endpoint Device Management, Endpoint Encryption, System Hardening, Local Sandboxing, Mobile Threat Protection, Endpoint Protection, Next Gen Firewalls, Incident Response Services, Attack Surface Management, Threat Research, Managed Threat Hunting, Phishing Readiness
Anforderung des Zugangs	Network Security	Cloud Security	Endpoint Security	Secure Web Gateway, DNS Security, Malware Analysis, Encrypted Traffic Management, Email Security, Network Analytics, Intrusion Prevention, Container Security, System Hardening & Intrusion Detection, Serverless Computing, Endpoint Protection, Endpoint Device Management, Endpoint Encryption
Offenlegung von Schwachstellen	Data Security	Application Security	Endpoint Security	Data Loss Prevention, Endpoint Encryption, Data Classification, Cloud Access Security Broker, Endpoint Protection, System Hardening, Dynamic Application Scanning, Container Security, Static Code Analysis, Content Inspection, Content Sandboxing, Local Sandboxing, Mobile Threat Protection
Sichere Kommunikation	Content & Collaboration	Cloud Security	Endpoint Security	Encryption in Transit, Content Filtering, Email Protection & Response, Browser Isolation, Container Security, System Hardening & Intrusion Detection, Serverless Computing, Malware Scanning for Storage, Container Security, Data Loss Prevention for Cloud, Cloud System Hardening & Workload Protection

Ein Unternehmen benötigt

10+ Punktlösungen für die NIS2 Umsetzung



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

Industry leading Zero Trust network architecture



Network Security

2019

- First ML powered NGFW
- Acquired CloudGenix SD-WAN*
- NFWG 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

Comprehensive code-to-cloud platform



Cloud Security

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

Game changing SecOps underpinned by AI



SOC Security

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

Trusted cybersecurity partner of choice



Advisory & IR

2019


- Acquired Cypsis 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	 <p>Network Security</p>
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	 <p>Prisma Cloud</p>
Cloud Workload Protection	
Identity & Access Management	
Code Security	
Web Application / API Security	

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

Unsere Cybersecurity Formel - mit LLM & AI

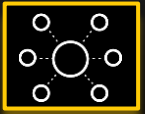
Integrierte
Telemetriedaten

+

ML / AI
Automatisierung

=

Improved Cyber
Resilience



Networks



Cloud



Endpoints



Strata
NGFW



Cortex
XSIAM



Cortex
XSOAR

10

SEKUNDEN

Risk Efficiency
Mean Time to Detect

TCO Simplicity

1

MINUTE

Mean Time to Respond
(High priority alerts)

Vielen Dank

Christian Kurta | Systems Engineer | Austria