CORTEX
BY PALO ALTO NETWORKS

Das autonome Security Operations Center

powered by Cortex

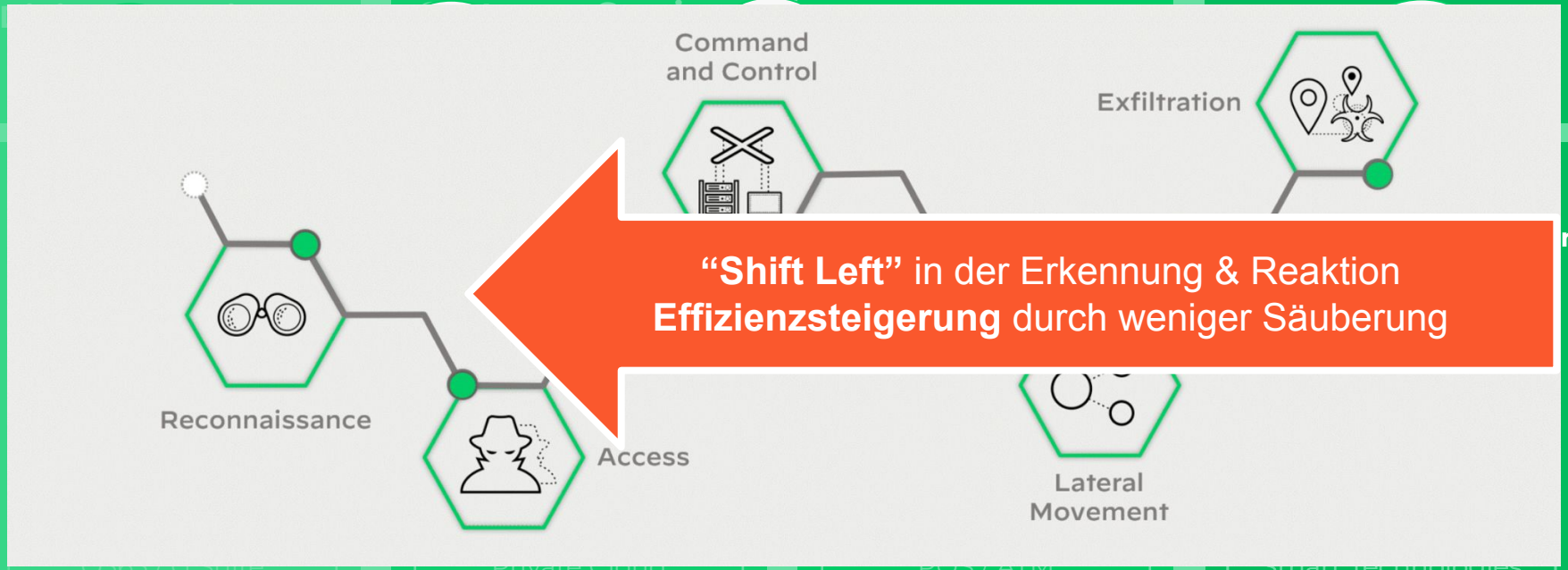
Bastian Schwittay
Cortex Systems Engineer Specialist

paloalto NETWORKS

Die digitale Transformation schafft Angriffsfläche und Risiken

Digitaler Arbeitsplatz Mobiles Arbeiten Cloud	Customer Services CI/CD DevOps	Konvergenz von IT und OT	F&E Innovation
Windows 10 / 11	Cloud (SaaS, IaaS)	Kritische Infrastruktur	Kollaboration
Mobile	Shadow IT	SCADA	Container
MAC OS / Linux	SDN	Produktion	Infrastruktur aus M&A
Legacy OS	Cloud Storage	Medizingeräte	Intellectual Property
O365 / G Suite	Private Cloud	POS / ATM	Smart Technologies

Angreifer suchen das schwächste Glied in der Kette



Verschlüsselung
(Telnet, SMTP, FTP)

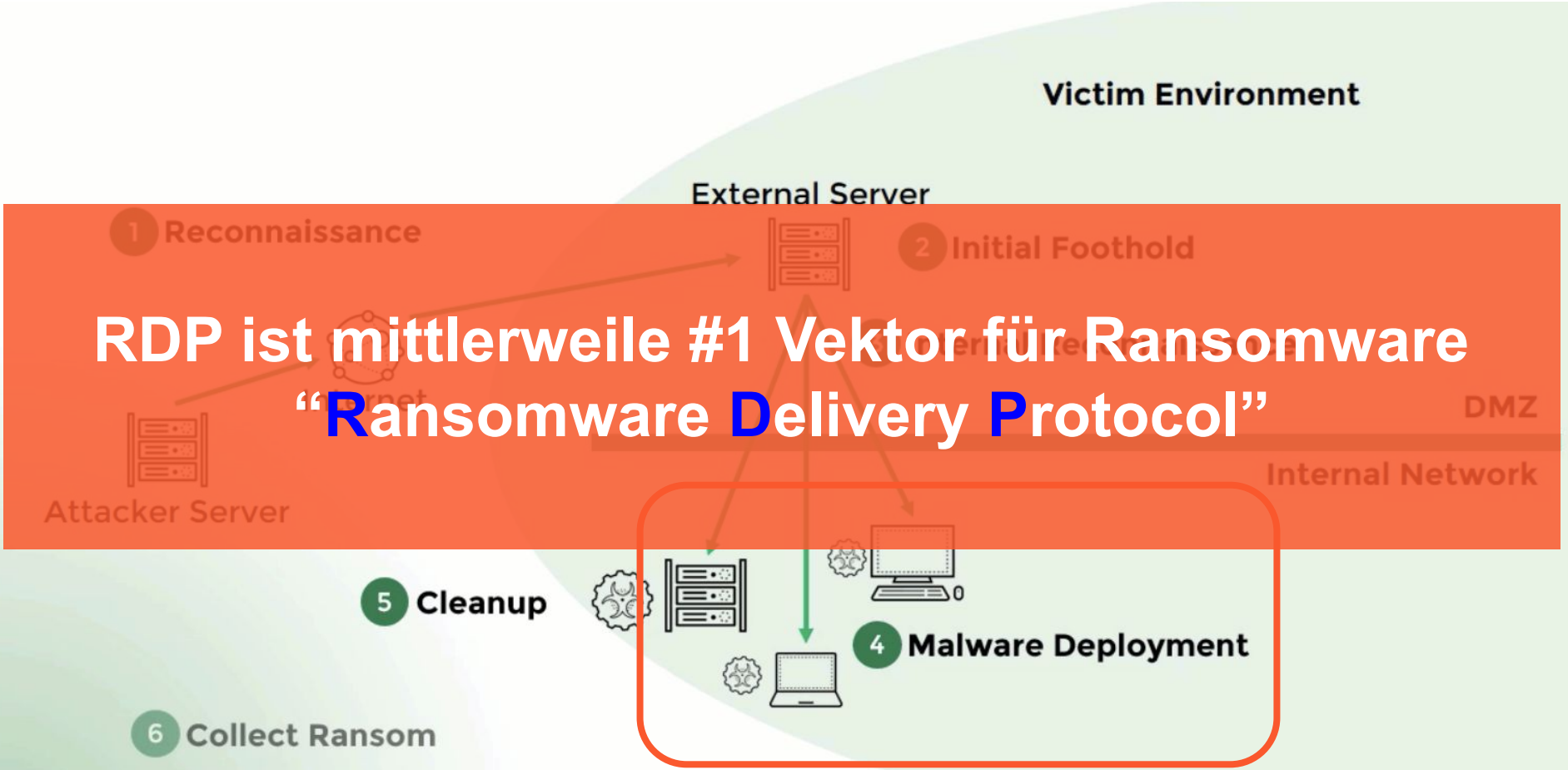
Geräte

Kryptographie

Entwicklungs-systeme

vergessene Marketing-Portale

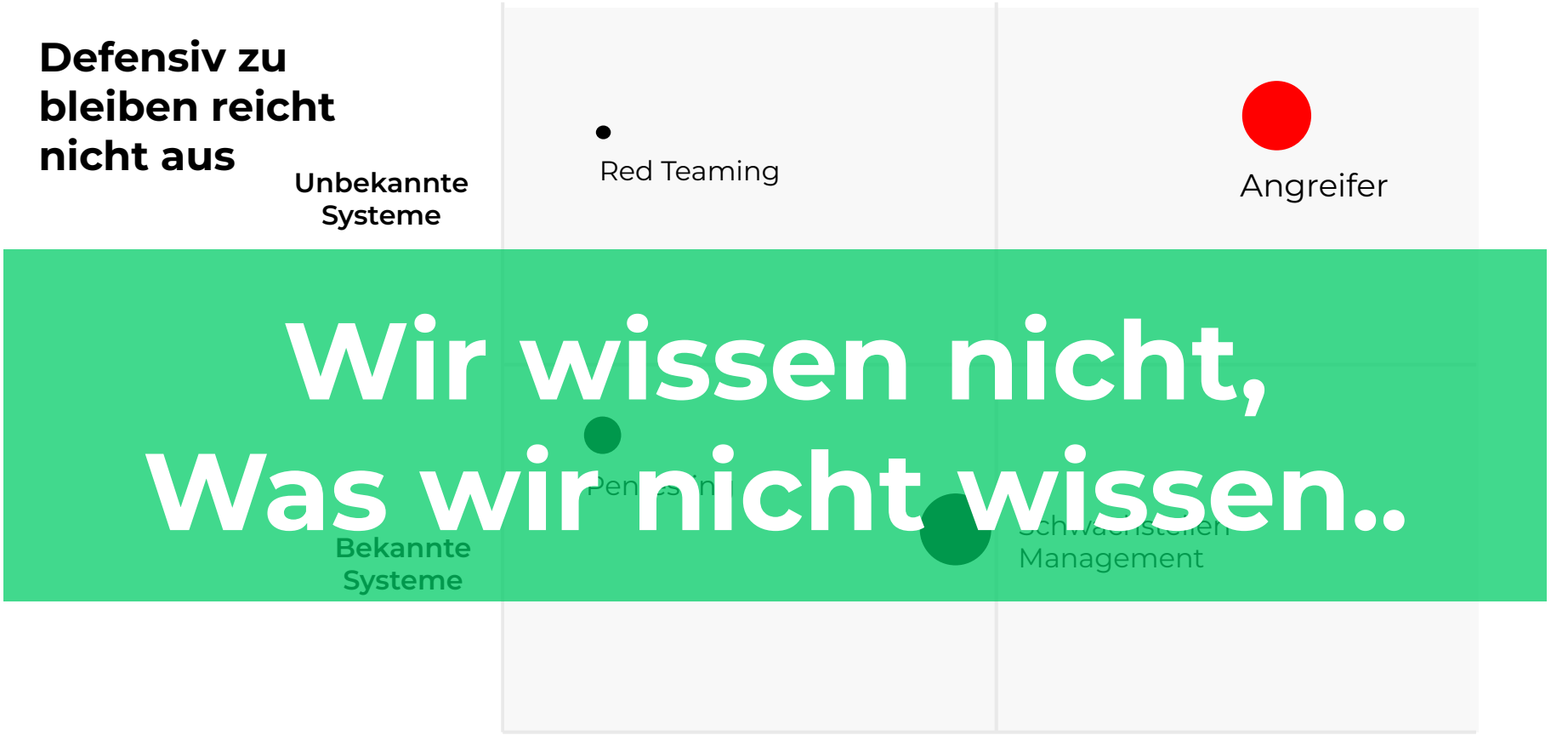
Ransomware Angriffe beginnen nicht am Endpunkt



RDP ist mittlerweile #1 Vektor für Ransomware

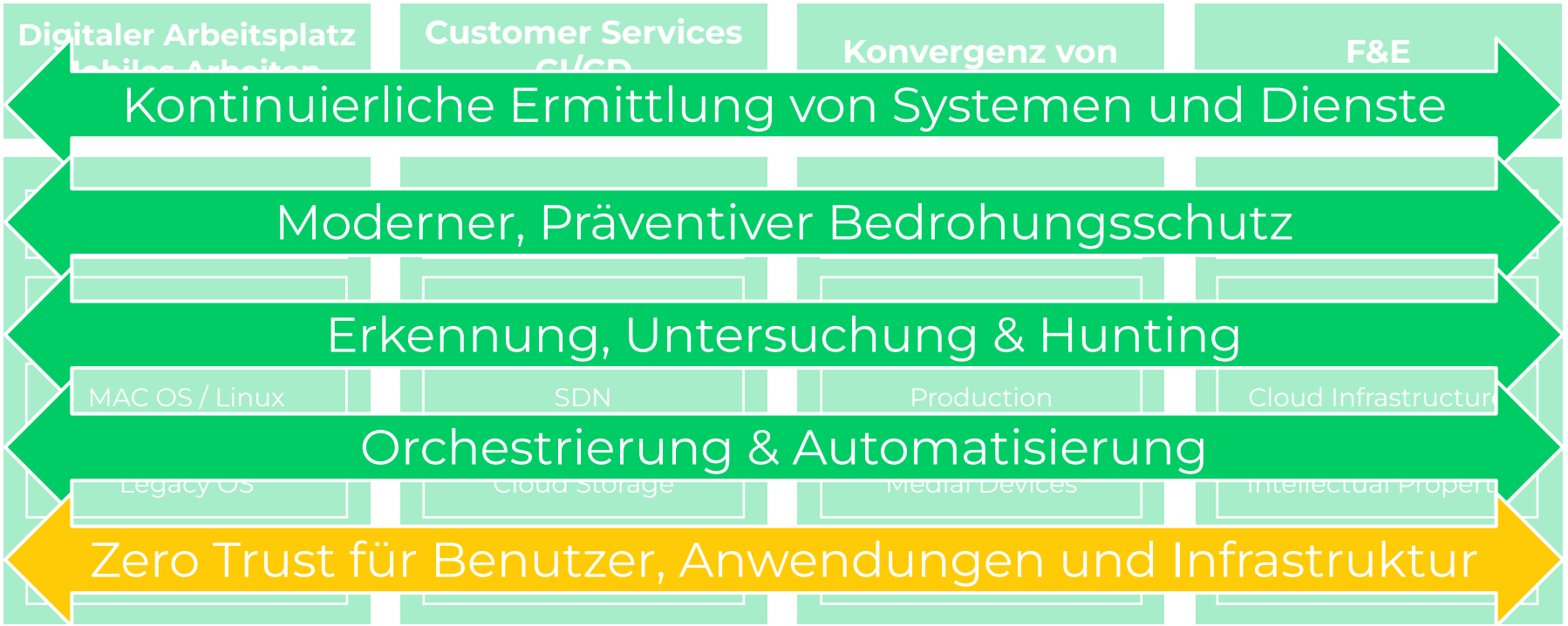
“Ransomware Delivery Protocol”

Defensiv zu bleiben reicht nicht aus



Wir wissen nicht, Was wir nicht wissen..

Wie kann man Risiken reduzieren und Effizienz steigern?



Technologische Durchsetzungspunkte - Da sein, wo es zählt

Endpunkt

Netzwerk

Cloud

Cortex Security Operations Platform

- Attack Surface Management (Cortex Xpanse)
- Vollständige Threat Detection & Response (Cortex XDR)
- Unternehmensweite Orchestrierung & Automatisierung (Cortex XSOAR)

Der X-Faktor für einen modernen IT Leitstand

paloalto NETWORKS

EDR- und SIEM-Produkte lösen das Problem nicht angemessen

EPP / EDR

Tiefgreifende Analysen & Bedrohungserkennung

Fehlende Abdeckung und Kontext für die gesamte Umgebung

EDR

Endpunkt

Fehlende Analytics

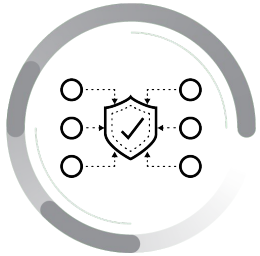
Fehlende Daten und Kontext

SIEM

Kein Endpunkt Sensor

Fehlende Analytics

SIEM



SIEM

Mangelnde Analytik und Erkennung

Fehlende Arbeitsabläufe

Fehlende Kontrollpunkte zur Behebung

Cortex XDR: Entwickelt, SOC-Effizienz zu erhöhen

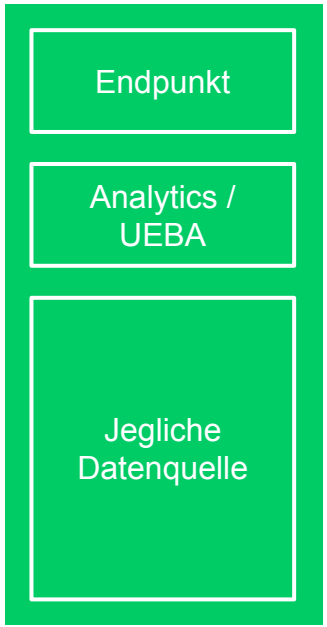
Schutz
- Moderne EPP Plattform

Erkennung
- Data Stitching, um die Story automatisch zu erzählen
- Stitching bedeutet ein einziges Ereignis und nicht mehrere Protokolldateien (ML-optimiert)

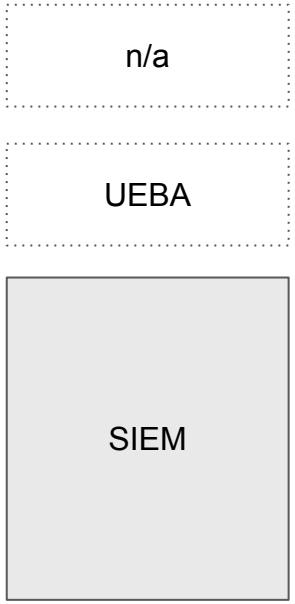
Untersuchung
- Eingebaute Analyse, die Anomalien über mehrere Tage hinweg zusammenfügt
- Workflows, die darauf ausgelegt sind, das Gesamtlagebild leicht zu verstehen

Reaktion
- Native Aktionen (Endpunkte, Firewalls, Cloud, OT)
- Live Terminal

XDR



SIEM



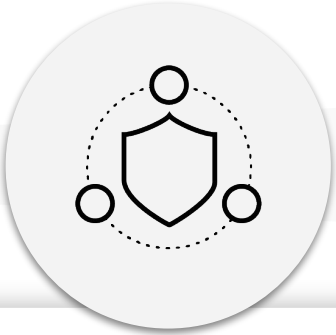
Schutz
- Nicht verfügbar

Erkennung
- Statische Korrelationsregeln - „als schlecht bekannt“
- Wird nur ausgelöst, wenn alle Kriterien erfüllt sind (wenn, dann, sonst Bedingungen)
- Historische Daten, nicht in Echtzeit

Untersuchung
- Untersuchungen erfolgen manuell
- Mangel an Kontext (z.B. Warnung, dass Personen an PII-Daten arbeiten, die im Kundenservice sind)

Reaktion
- API-basierte Integrationen mit Endpoint-Anbietern
- Begrenzte Aktionen

Cortex XSOAR: Alles Automatisieren

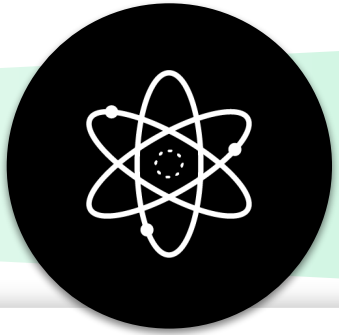


SOC Automatisierung

- Threat Intel Enrichment
- Phishing Response
- SIEM Enrichment
- Automated Threat Hunting

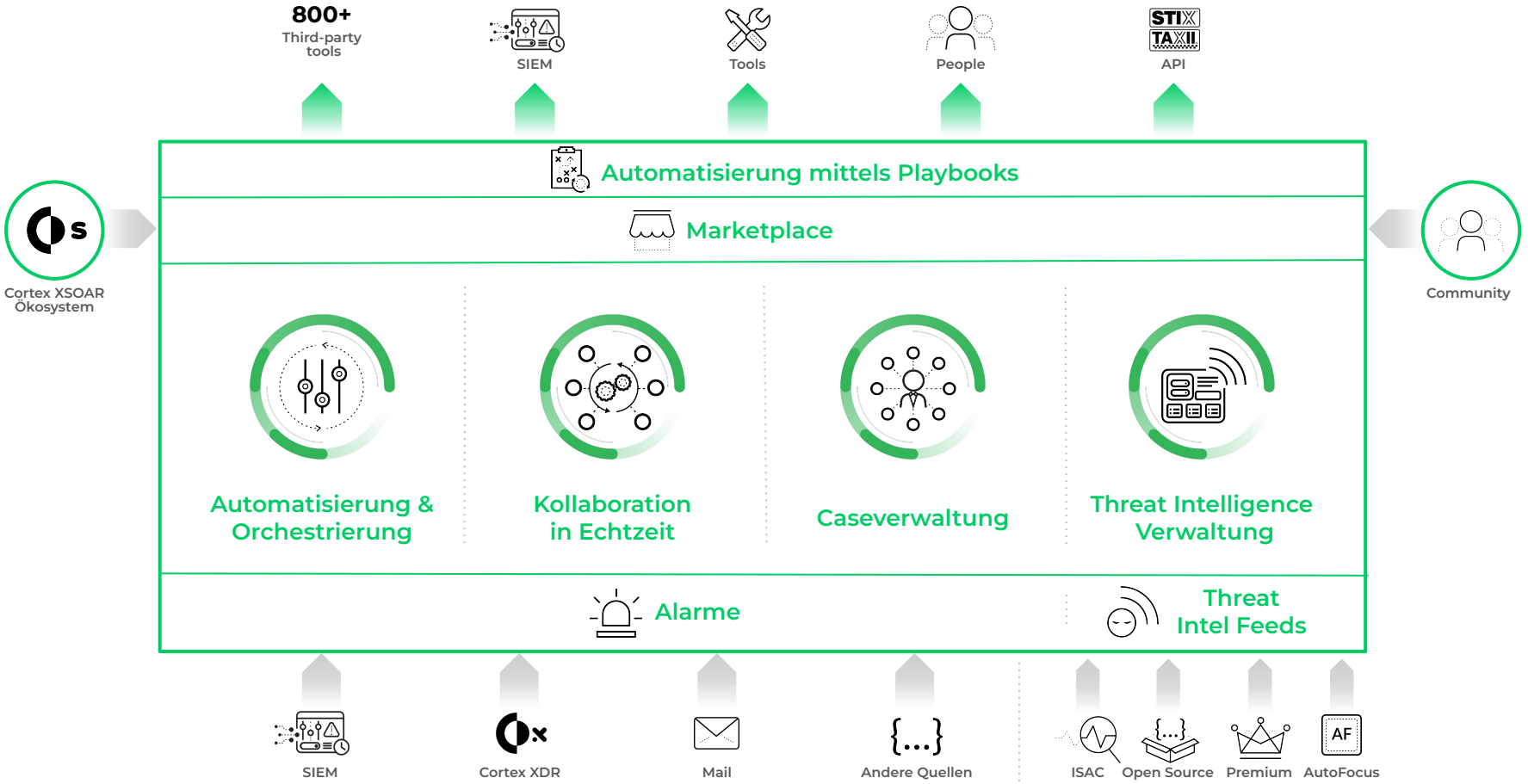
Erweiterte Security Automatisierung

- Schwachstellen-Management
- Cloud Security
- Threat Intelligence Verwaltung
- IoT Security

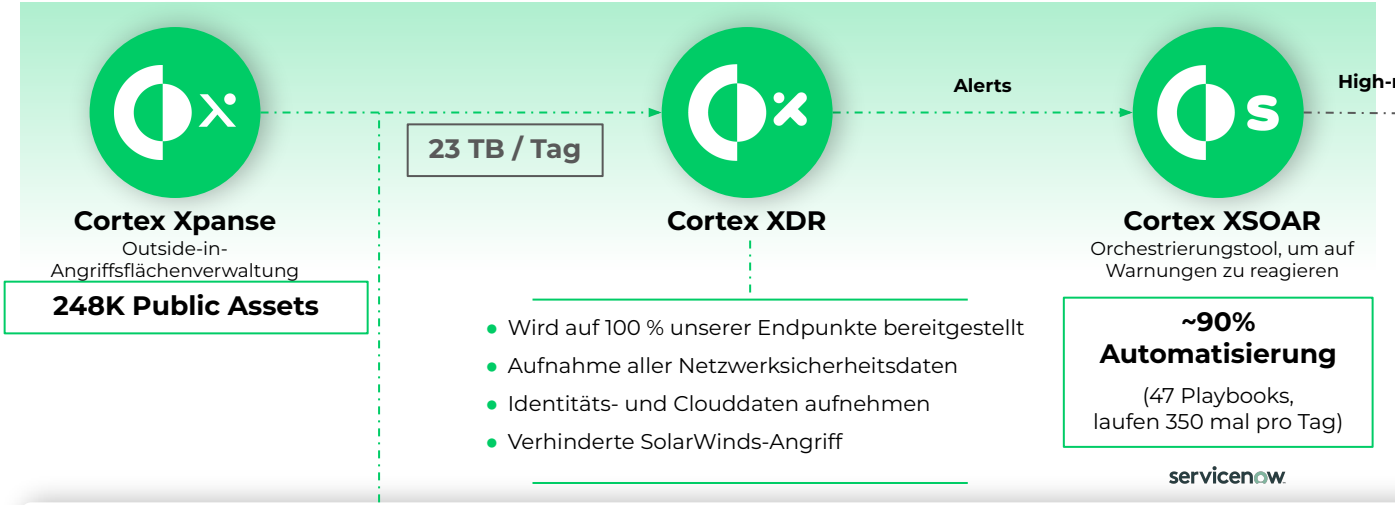


Enterprise Security Automatisierung

- Netzwerksicherheit
- Security Compliance
- Andere Security und IT Use Cases
- Identity & Password Verwaltung



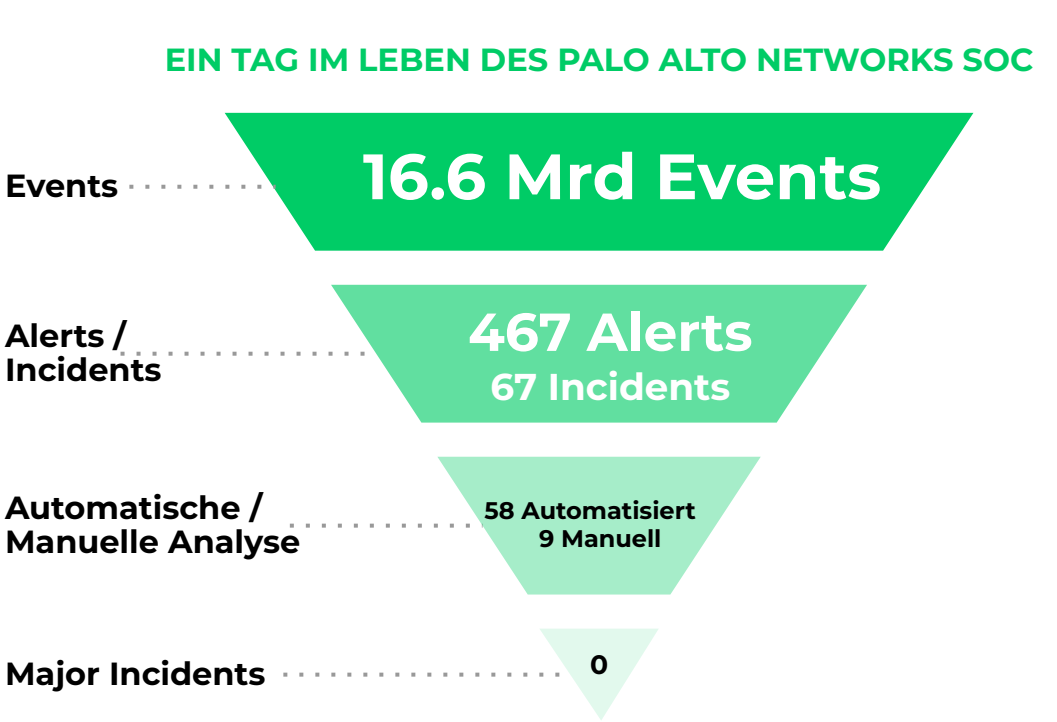
Palo Alto Networks SOC



Umfassende Sicherheit

Netzwerk	Endpunkt	Cloud
Prisma Access; NGFWs, VMs	Cortex XDR	Prisma SaaS; Prisma Cloud; Data Security
10K Mitarbeiter	50K Endpunkte	4.3 Millionen Cloud Assets

Palo Alto Networks SOC: Reaktionszeit von 1 Minute



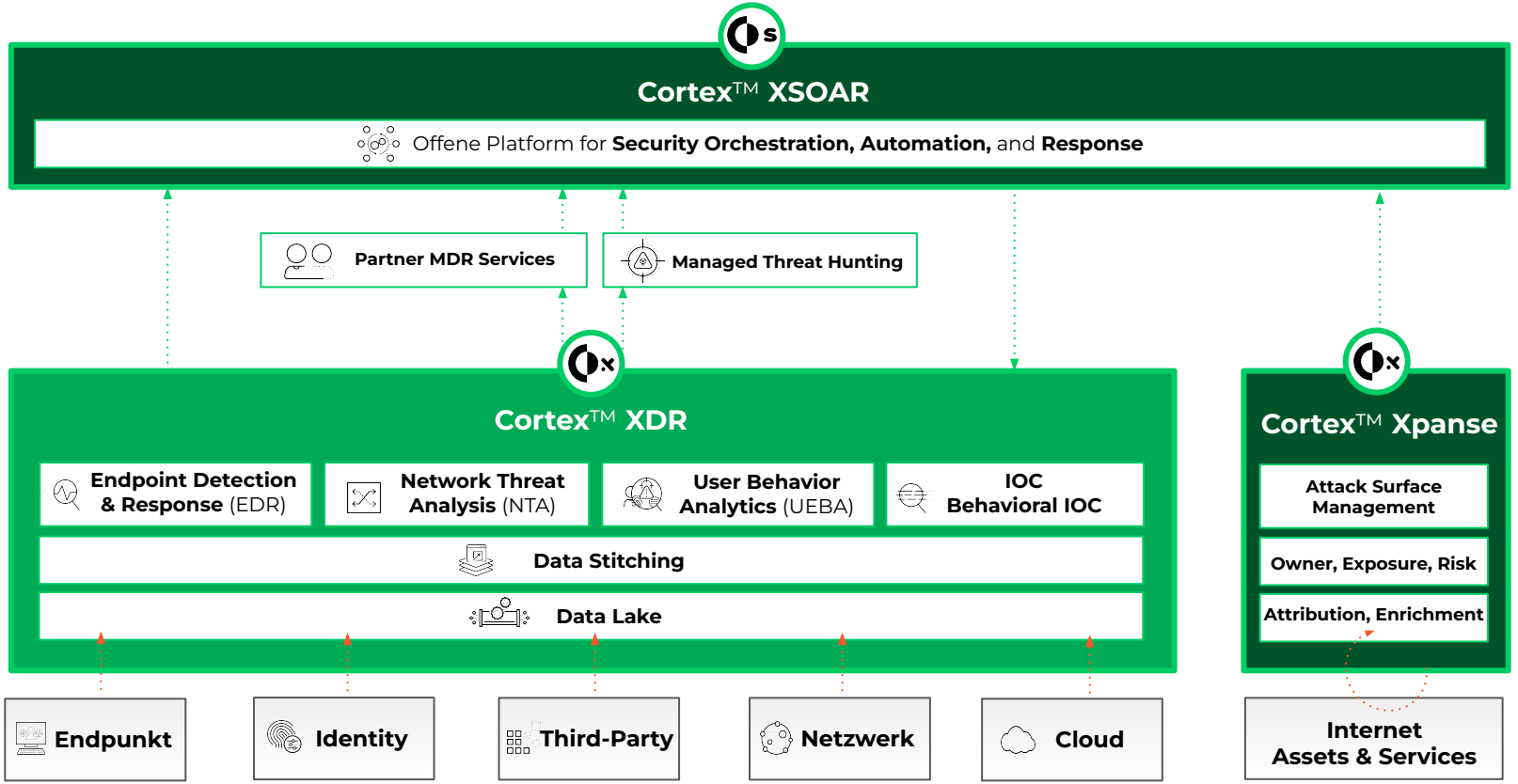
10
Sekunden

Mean Time to Detect

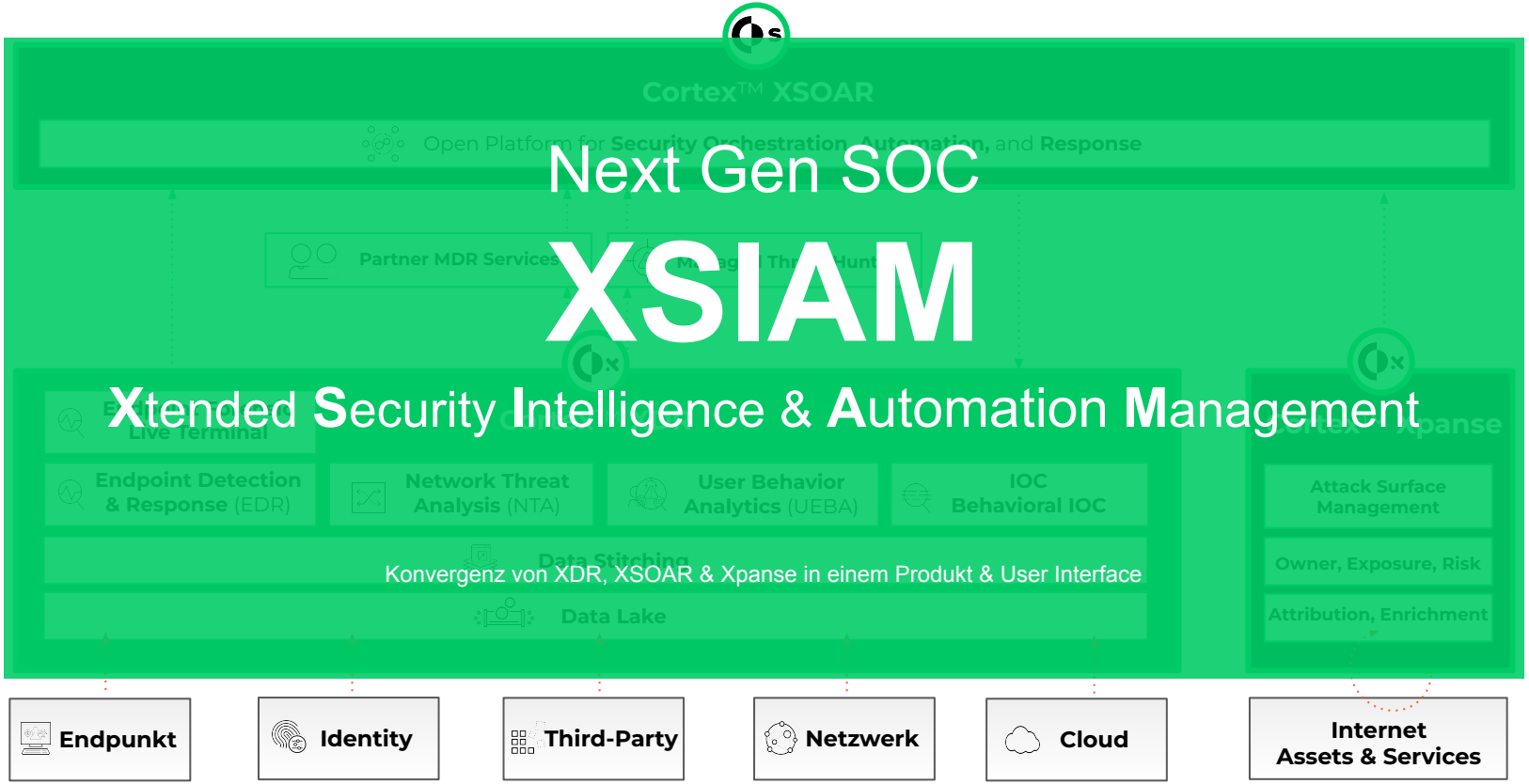
1
MINUTE

Mean Time to Respond
(High Prio Alarme)

Cortex: Eine ganzheitliche Plattform für integrierte SOC-Dienste



Cortex XSIAM: Die “Next Generation” SOC Platfform



CORTEX
BY PALO ALTO NETWORKS

Thank you

paloaltonetworks.com

paloalto NETWORKS