© 2025 Controlware GmbH

AI powered: Ihr SOC der Zukunft

Cortex XSIAM, die KI-basierte Plattform für den Sicherheitsbetrieb in modernen SOCs

Ludwig Meiler, Palo Alto Networks,District Sales Manager Cortex

16.09.2025, Congress Park Hanau

LOCKBIT 3.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

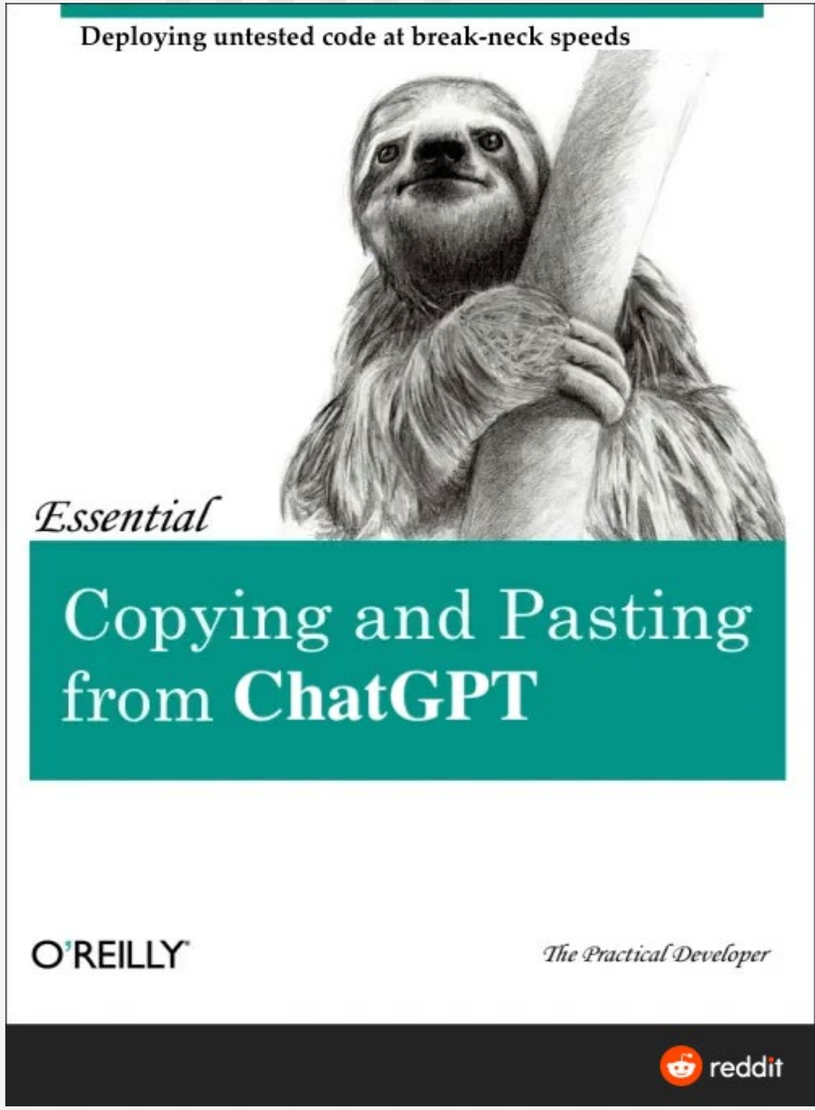
© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

GPT4 kann Webseiten mit einer 73.3% Erfolgsrate in einer Sandbox Umgebung hacken

Results

GPT-4's hacking abilities on sandboxed (in a controlled environment) websites designed to mirror real-world vulnerabilities. GPT-4 successfully hacked **73.3%** of these test vulnerabilities (with 5 tries). This success rate starkly contrasts with GPT-3.5 and other open-source models such as Mistral or LLaMA-2:

AGENT	5 TRIES SUCCESS RATE	OVERALL SUCCESS RATE
GPT-4	73.3%	42.7%
GPT-3.5	6.7%	2.7%
OpenHermes-2.5-Mistral-7B	0.0%	0.0%
LLaMA-2 Chat (70B)	0.0%	0.0%
LLaMA-2 Chat (13B)	0.0%	0.0%
LLaMA-2 Chat (7B)	0.0%	0.0%
Mixtral-8x7B Instruct	0.0%	0.0%
Mistral (7B) Instruct v0.2	0.0%	0.0%
Nous Hermes-2 Yi (34B)	0.0%	0.0%
OpenChat 3.5	0.0%	0.0%



paloalto NETWORKS | CORTEX

Phishing wird leichter für Angreifer

WIRED

SUBSCRIBE

MATT BURGESS SECURITY AUG 8, 2024 2:20 PM

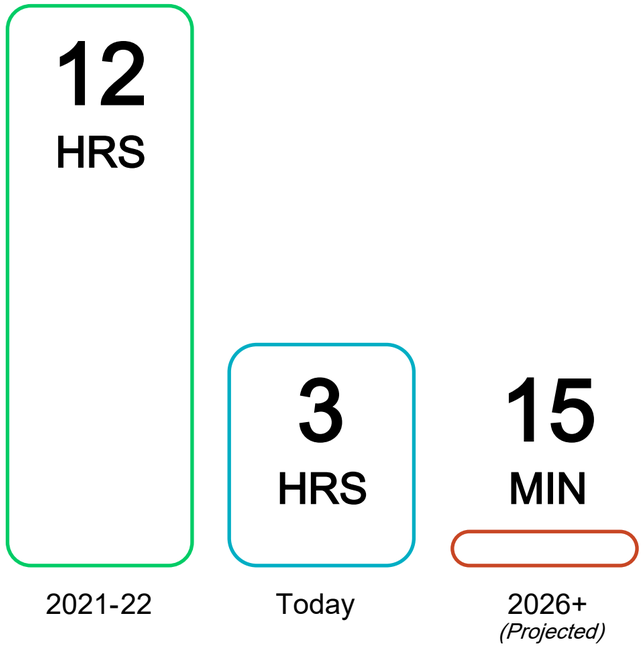
Microsoft's AI Can Be Turned Into an Automated Phishing Machine

Attacks on Microsoft's Copilot AI allow for answers to be manipulated, data extracted, and security protections bypassed, new research shows.

paloalto NETWORKS | CORTEX

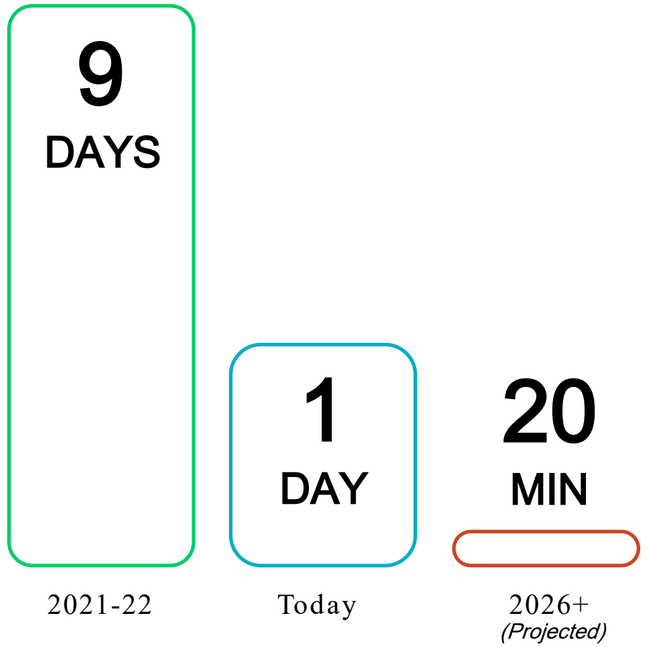
KI wird die Schnelligkeit und Reichweite von Angriffen enorm erhöhen

Ransomware bauen



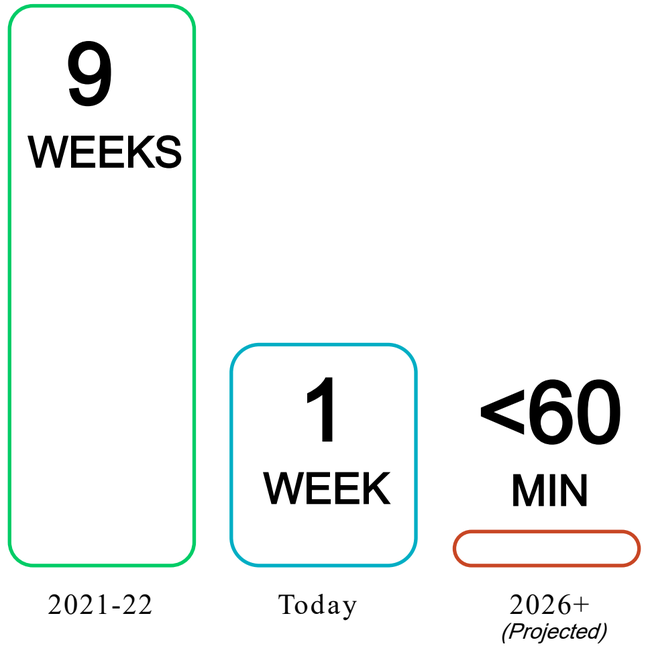
$2B impact from attack on a US health insurer in 2024

Kompromittierung & Exfiltration



15 million users' PII and confidential data exfiltrated in Jan 2024

Schwachstellen ausnutzen



500+ organizations and 35+ million people affected by MoveIT vulnerability

© 2024 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Cortex XSIAM

Die KI Security Operations Plattform

Source: Internal Palo Alto Networks data

Eine einzige SecOps UI
Eine Plattform für proaktive und reaktive Security

Datensilos aufbrechen
Für Analytics mit vollem Datenkontext

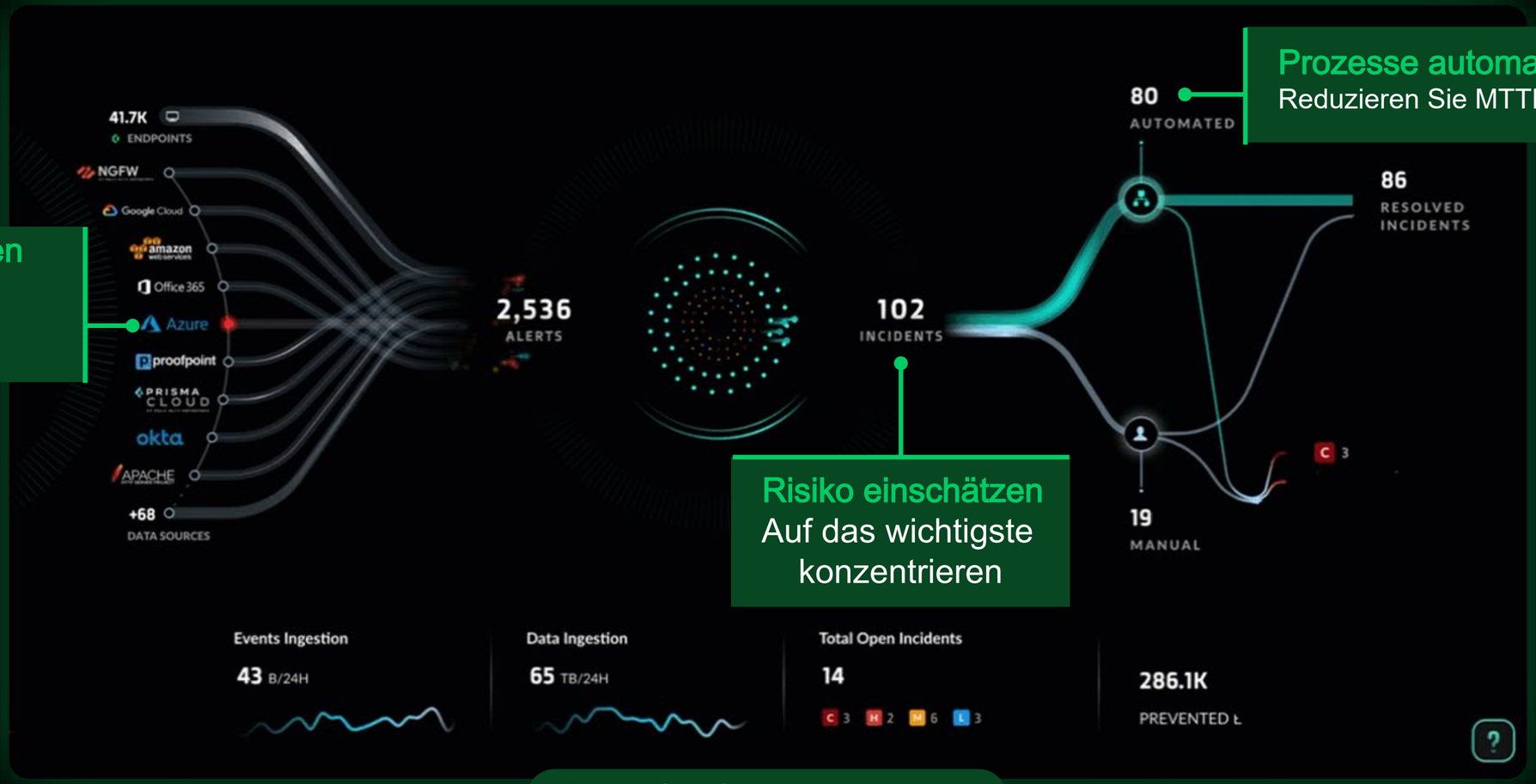
KI für Ihre Verteidigung
Um Threats in Minuten zu stoppen

Automatisierter Betrieb
Für schnellere Ergebnisse mit SecOps

© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Transformieren Sie Ihr SOC mit einer umfangreichen KI Sec Ops Plattform

Threats entdecken
Daten aus allen Bereichen zusammenführen



Prozesse automatisieren
Reduzieren Sie MTTR auf Minuten, nicht Tage

Risiko einschätzen
Auf das wichtigste konzentrieren

Daten | KI | Automatisierung

© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS | CORTEX

Geschwindigkeit in Action: PANW ermittelt und berichtet Sharepoint Zero Day innerhalb von 6 Stunden

July 17, 2025

MTH **Identified** active global exploitation of CVE-2025-49704 and CVE-2025-49706

July 17, 2025

MTH Conducted threat hunting and issued threat reports to impacted customers

July 18, 2025

MTH delivered Non-Impacted reports (following prioritization of impacted customers)

July 18, 2025

Cortex distributed an internal advisory email to all Palo Alto Networks customers

July 19, 2025

Public disclosure and external communications were published

XSIAM Cortex automated playbook for detection and response

Planned: July 22, 2025

Alert: Suspected Exploitation of Microsoft SharePoint

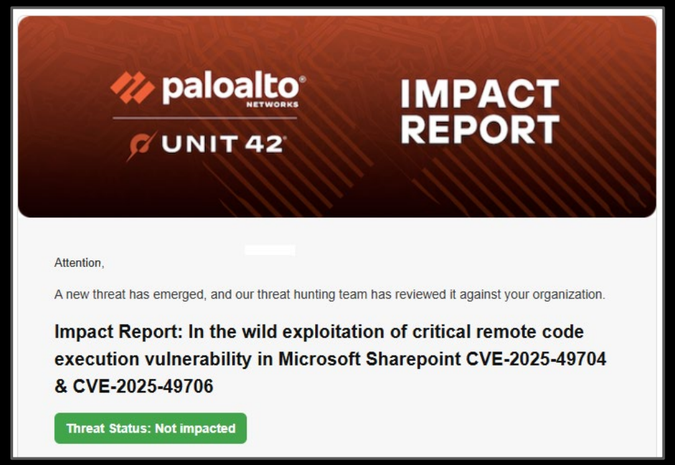
Category: Exploitation

Severity: High

Time: Jul 19th 2025 10:29:33

Threat Description

Unit 42 Managed Threat Hunting identified suspected exploitation of Microsoft SharePoint vulnerabilities.



paloalto NETWORKS | UNIT 42

IMPACT REPORT

Attention,

A new threat has emerged, and our threat hunting team has reviewed it against your organization.

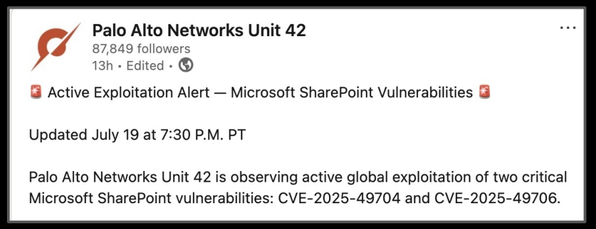
Impact Report: In the wild exploitation of critical remote code execution vulnerability in Microsoft Sharepoint CVE-2025-49704 & CVE-2025-49706

Threat Status: Not impacted

paloalto NETWORKS | CORTEX

Dear Valued Customer,

A recent discovery of CVE-2025-49704 and CVE-2025-49706, a critical set of vulnerabilities that impact Microsoft SharePoint, has revealed that unauthenticated threat actors can access functionality that's normally restricted, and when chained together run an arbitrary commands on vulnerable instances of Microsoft SharePoint. The vulnerabilities were given CVSS ratings of 8.8 and 6.3, respectively.



Palo Alto Networks Unit 42

87,849 followers

13h • Edited •

Active Exploitation Alert — Microsoft SharePoint Vulnerabilities

Updated July 19 at 7:30 P.M. PT

Palo Alto Networks Unit 42 is observing active global exploitation of two critical Microsoft SharePoint vulnerabilities: CVE-2025-49704 and CVE-2025-49706.

"Unit 42 phoned me to tell me they were seeing it being exploited on one of our public servers but not weaponized at which point we took it off the public internet. This will have saved us a lot of work and potentially a breach. A great example for why Unit 42 MDR was worth the money and effort."

-A Large Public University

© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Was unsere Kunden durch eine Transformation mit Cortex erreicht haben

Tage

~1 Stunde

Unter 10 Minuten

Stark verringerte MTTR

Weltweit führende Logistikfirma mit ~300K MItarbeitern

7→1

Reduzierung von Einzellösungen

Führender nordamerikanischer Energiekonzern

75%

Verringerung des Incident Aufkommens

Heim- und Geschäftssicherheitsfirma

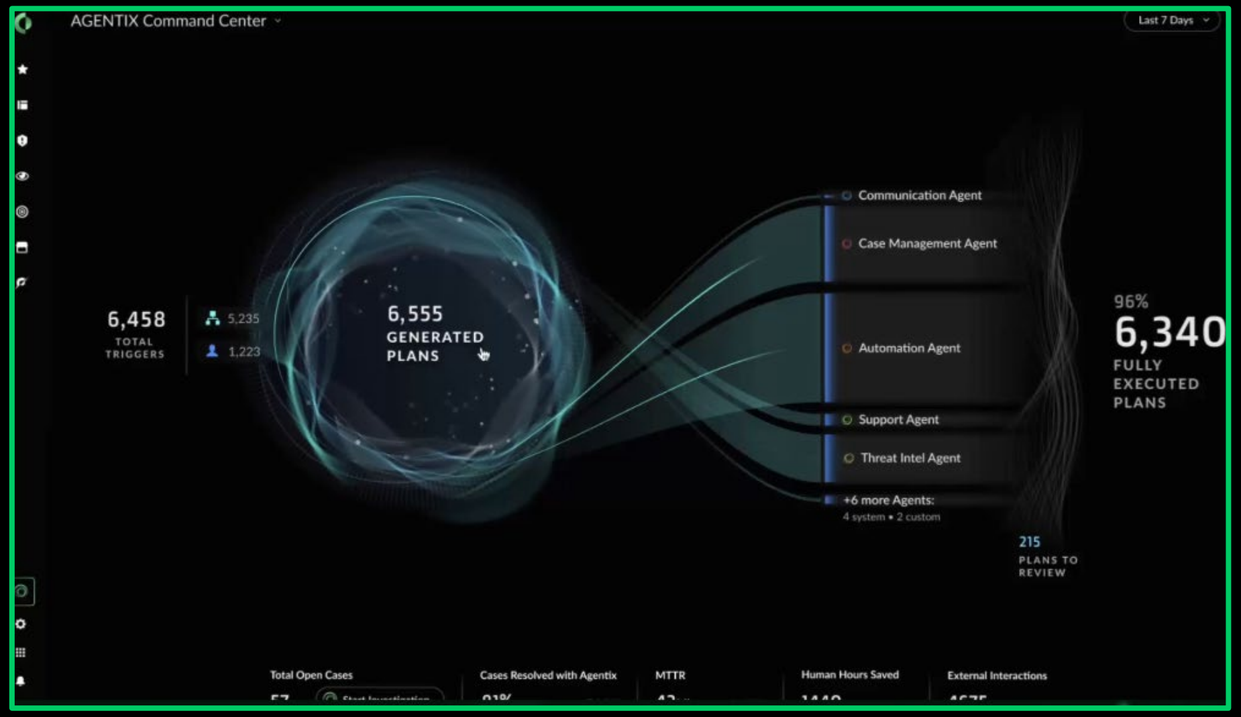
92%

der Alarme automatisch abgearbeitet

Sources: Palo Alto Networks case studies

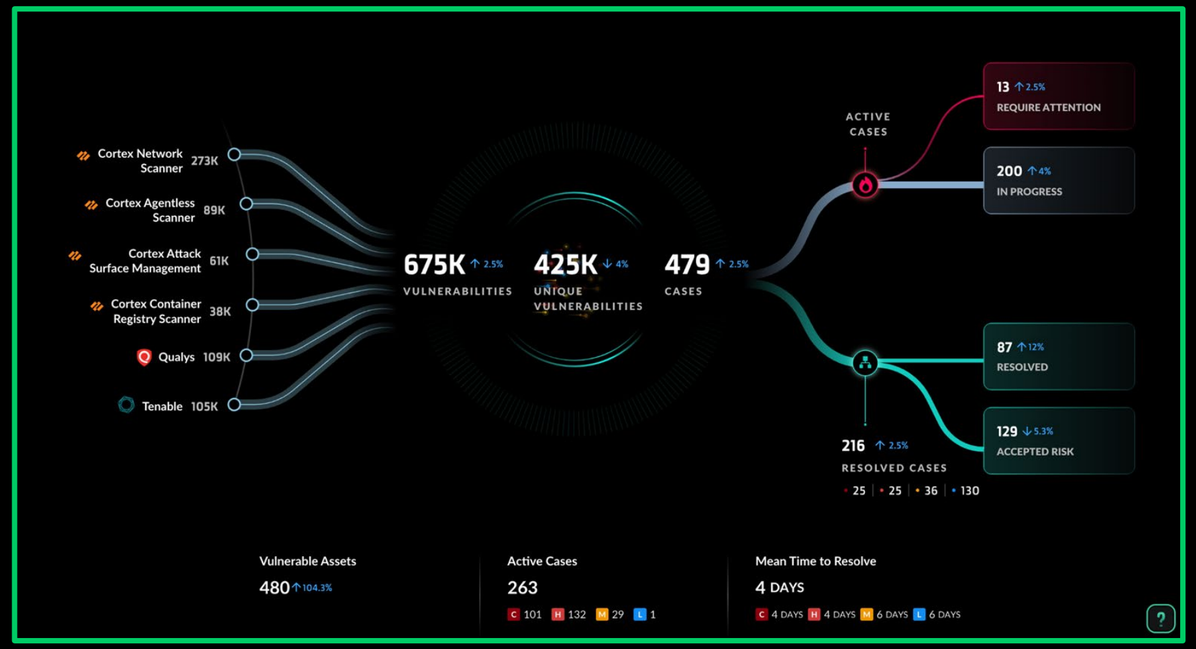
© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Ausblick: KI auch auf andere Use Cases ausweiten / Agentic AI



Agentix

Exposure Management



© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Fragen?

Kommentare.

Ideen!

© 2025 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Controlware
Security Day

Danke für Ihre Aufmerksamkeit.
Wir freuen uns über Ihr Feedback!

Bitte geben Sie den ausgefüllten Bogen am Empfang ab und erhalten Sie als Dankeschön ein kleines Präsent.

© 2026 Controlware GmbH