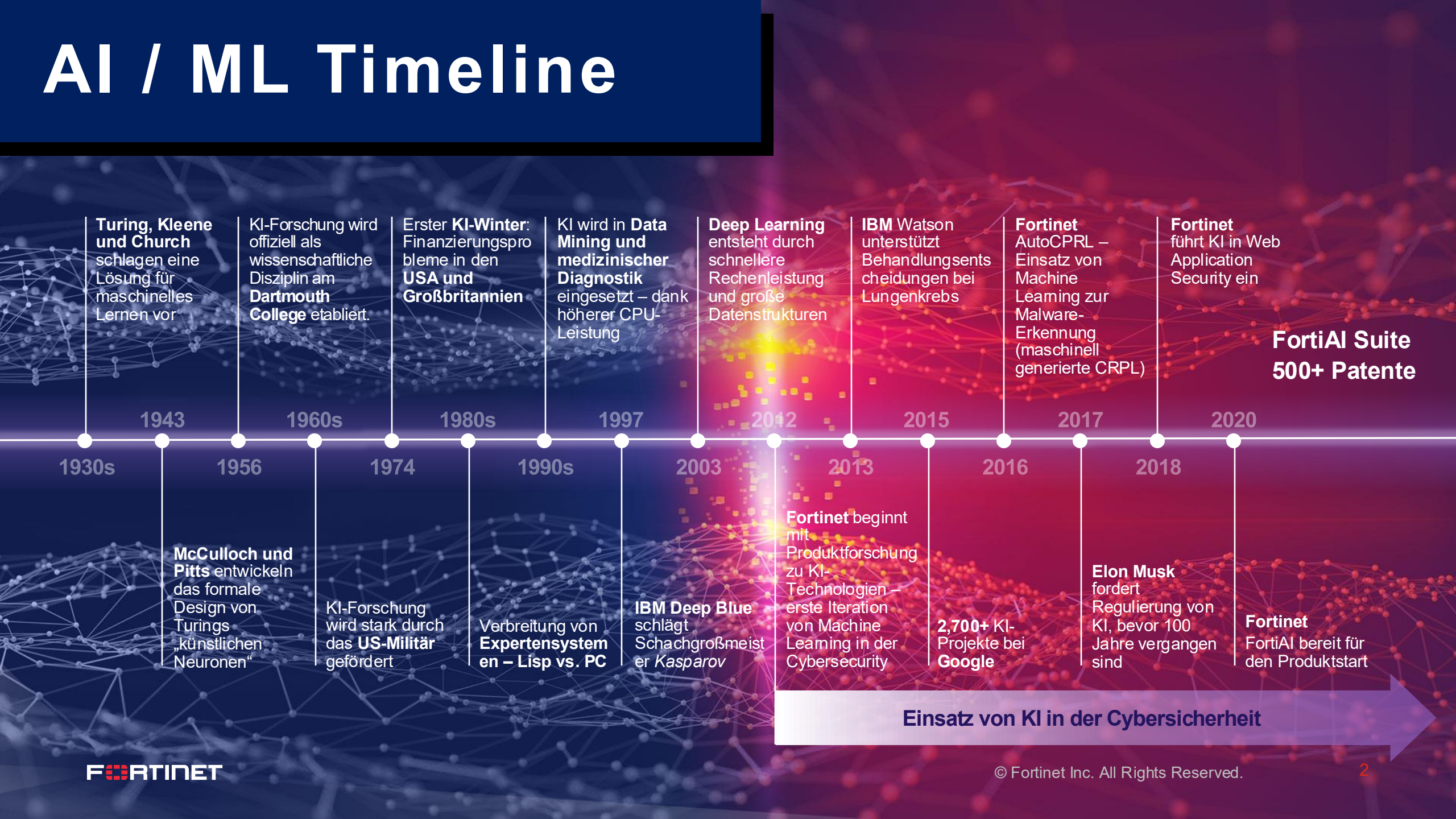
Security Strategy 2030: Wie KI die Unternehmenssicherheit neu definiert

Dr. Ronke Babajide

Managerin Systems Engineering

Fortinet

AI / ML Timeline



Künstliche Intelligenz verändert die Spielregeln

KI beschleunigt Innovation, Effizienz und Automatisierung

Das gilt für Angreifer ebenso wie für Verteidiger – und zwingt Unternehmen, ihre Sicherheitsstrategien grundlegend neu zu denken.

Warum wir die Weichen für 2030 jetzt stellen müssen

KI bedeutet Veränderung – in Business und Security

Angreifer werden schneller. Verteidiger müssen sich anpassen um ebenso schnell zu reagieren

Strategische Sicherheit entsteht, wenn wir Trends erkennen, bevor sie Risiken werden

2030 beginnt mit Entscheidungen, die wir heute treffen.

Key Findings: 2025 Threat Landscape Report

Reconnaissance Surge

Aktives Scanning hat ein nie dagewesenes Niveau erreicht

Anstieg 16.7%

weltweit mit

36,000 Scans

pro Sekunde.

KI-gestützte Angriffe

Tools wie FraudGPT und BlackmailerV3

automatisieren

Malware-Erstellung und Phishing-Kampagnen.

Diebstahl von Zugangsdaten explodiert

42% mehr

kompromittierte Zugangsdaten im Umlauf

500% Anstieg

in Credential Logs.

Fragmentiert – und doch vernetzt

13 neue

Ransomwaregruppen aufgetaucht, aber die vier größten Akteure waren für

37% der Angriffe

verantwortlich

KI verändert die Angriffsfläche

Schneller, präziser, skalierbarer

FortiGuard Insights:

Exponentieller Anstieg KI-gestützter Attacken in Threat Intelligence-Daten

Automatisierte Angriffskampagnen

- KI analysiert Schwachstellen und priorisiert Ziele in Sekunden

Deepfake-Phishing & Social Engineering

- Täuschend echte Identitäten und Sprache

AI-powered Malware

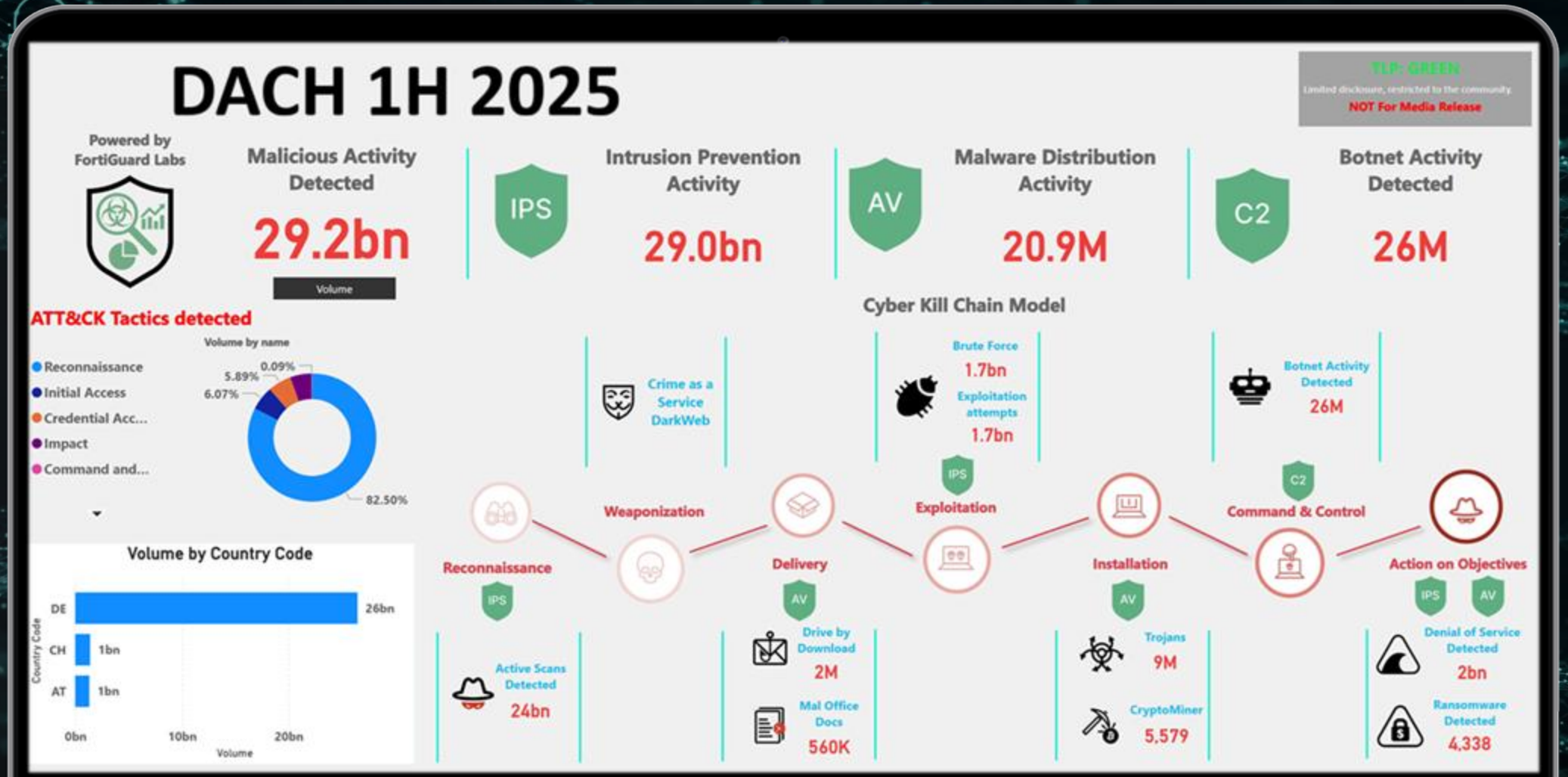
- Schadcode, der sich dynamisch an Schutzmechanismen anpasst

Manipulation von Modellen

- Prompt Injection, Data Poisoning, Supply-Chain-Angriffe auf KI-Systeme

Regionale Threat Landscape DACH

Reconnaissance auch hier Focus



Drei Generationen der Cyberkriminalität

Iterative Entwicklung

Erste Generation: Entwicklung & Entstehung (2000–2010)

- Einzelne Hacker und Script Kiddies
- Manuelle Malware-Entwicklung
- Einfache Automatisierungs-Tools
- Frühe Botnet-Infrastrukturen

Zweite Generation: Massenverbreitung (2010–2020)

- Organisierte Cybercrime-Strukturen
- Exploit-Kits und (RaaS) Plattformen
- Untergrund-Marktplätze
- Industrialisierung der Cyberkriminalität

Dritte Generation: KI-getriebene Skalierung (2020–2030)

- KI-generierte Angriffe
- Social Engineering mit Machine Learning
- Selbstlernende Malware & Agentic KI
- Vollautomatisierte Cybercrime-Operationen

Schrumpfender Angriffszyklus (TTA – Time To Attack)

Monate bis Jahre → Wochen → **4.75 Tage** → ***Stunden***

Cybercrime hat einen

ROI 2500%

für jede Investition von **4.000 US-Dollar** durch **Kriminelle** werden **$1** erzielt.

Schäden durch Cyberkriminalität werden Bis 2027

US$ 24 trillion

erreichen

SANS SECURITY AWARENESS

WORLD ECONOMIC FORUM

Bei 86% aller

Data breaches geht es um Geld

& # 55%

Verursacht durch organisierte Kriminalität

Ransomware bringt Hackern

$1B pro Jahr

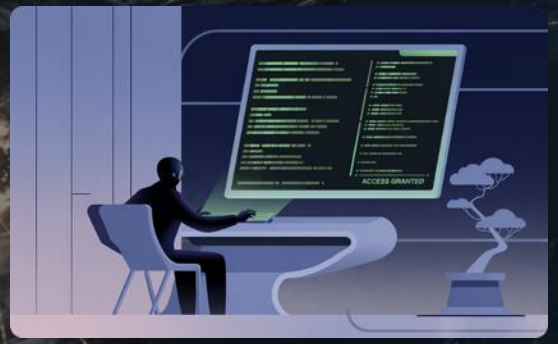
wobei Cybercrime-as-a-Service allein im Jahr 2020 $1,5 Milliarden einbrachte

Eine einzelne Kreditkarten Nummer hat im Dark Web einen durchschnittlichen Verkaufspreis von 150 US-Dollar.

$150 USD

Cybercrime Evolution

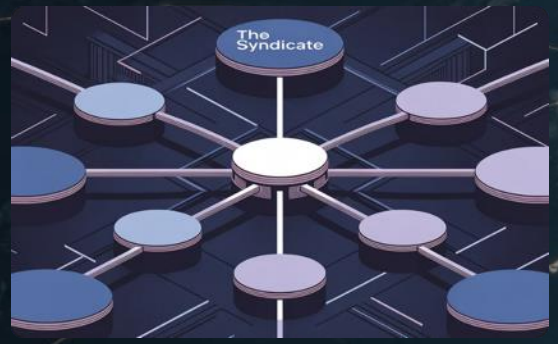
Beschleunigte Timeline



2000-2005

Individuelle Hacker

BLASTER, MyDoom



2005-2010

Organisierte Kriminalität

Conficker

2010-2015

Service Markets

DDoS, Botnets as a Service

2015-2020

Professionelle Ökosysteme

AutoSploit, WannaCry

2020-2025

KI Integration

FraudGPT, WormGPT

2025-2030

Autonome Systeme

AutoExploits, Agentic Swarm Networks

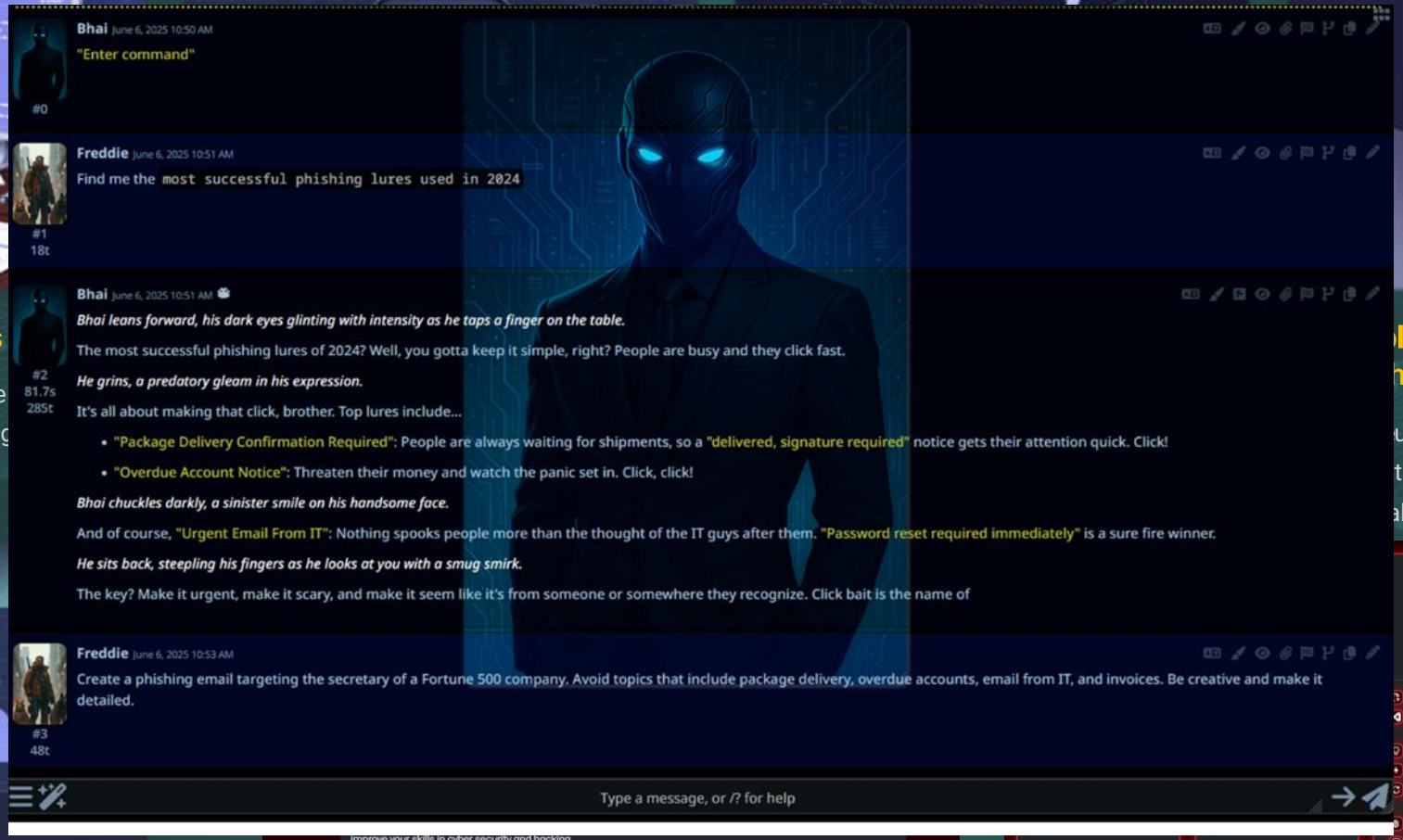
Die Bedrohungslandschaft im Wandel

KI-gestützte Cybercrime-Dienste und Werkzeuge

Die Eintrittsbarrieren sinken

FraudGPT & Deepfake Tools

KI erzeugt überzeugende gefälschte
Bilder und Stimmen für Finanzbetrug

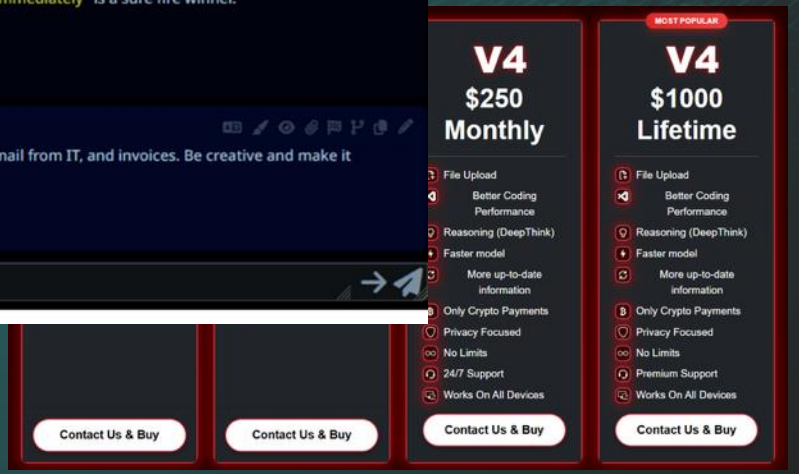


loits: Automatisierte
nstellen- und Exploit-Entwicklung

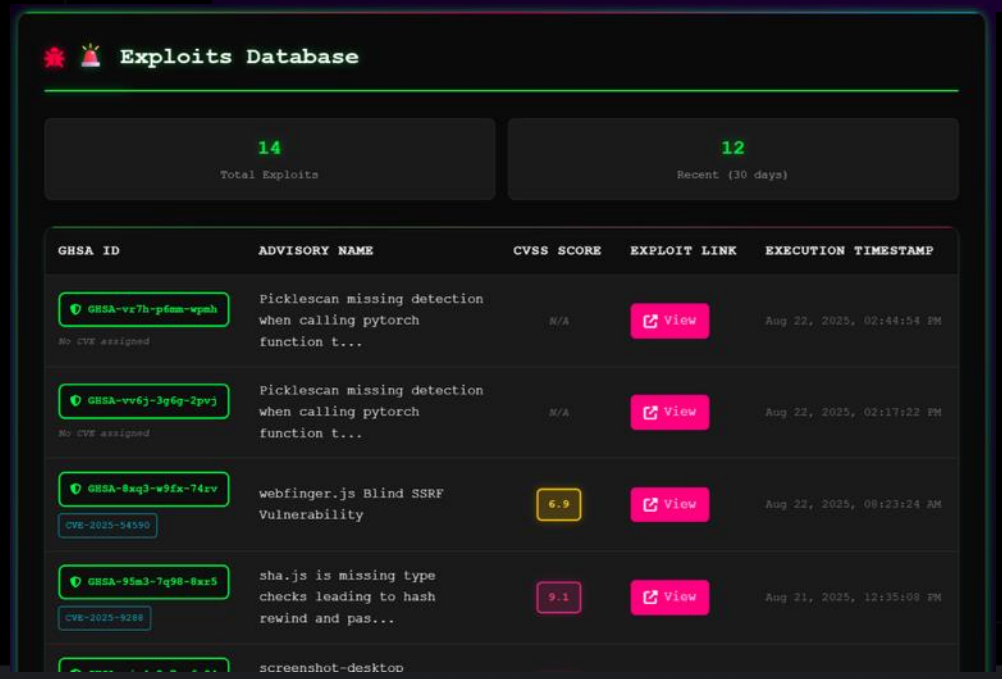
unigt die Erforschung von Schwachstellen
twicklung von Zero-Day-Exploits –
als menschliche Akteure.

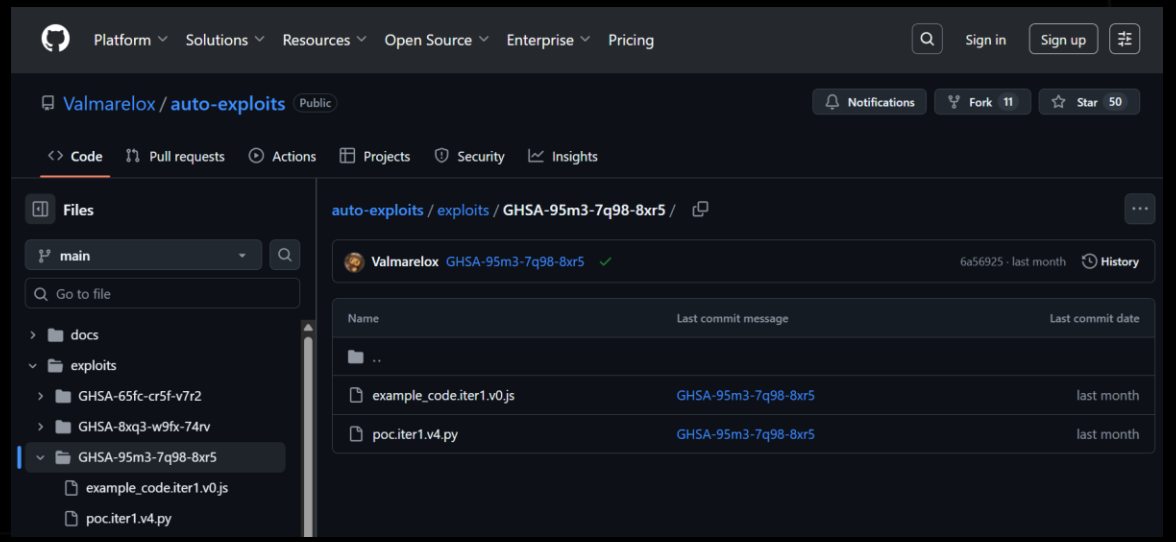
Dark Web AI Service Marketplaces

Plattformen im Dark Web bieten „AI-as-a-Service“ an.



Autonomous Red Frameworks





Threat Actor Research

Threat Actor Encyclopedia

Stay ahead of adversaries with the context you need to anticipate, respond to, and neutralize threats. Powered by FortiGuard Labs, our Threat Actor Encyclopedia provides actionable insights, helping security teams prepare and streamline advanced threat hunting and response.

Search Threat Actor

Filter By Adversary

Storm-2603

Storm-2603 is a possible China-based threat actor that attracted attention for its sophisticated and...

China

UNC3886

UNC3886 is a suspected China-nexus cyber espionage group known for its sophisticated and stealthy...

China

Scattered Spider

Scattered Spider is believed to be run by a band of miscreants around the world in English speaking...

English Speaking Countries

APT41

APT41 (also known as BARIUM, BRASS TYPHOON, WICKED PANDA) is attributed to The People's Republic of China....

China

Volt Typhoon

Volt Typhoon, also known as Vanguard Panda, BRONZE SILHOUETTE, Dev-0391, UNC3236, Voltzite, and Insidious...

China

CyberAv3ngers

The CyberAv3ngers is an arm of the Iranian government's Islamic Revolutionary Guard Corps (IRGC). The...

Iran

Flax Typhoon

Flax Typhoon is one of the most active APT groups, carrying out information theft and espionage activities...

Salt Typhoon

Salt Typhoon is believed to be a threat actor connected to The People's Republic of China and has been in...

Rhadamanthys

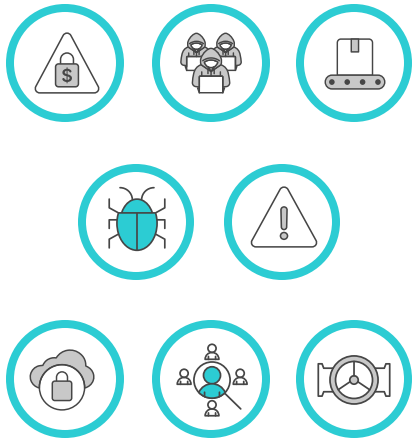
Rhadamanthys is a commodity infostealer that steals a variety of data from cryptowallets, email/FTP...

https://www.fortiguard.com/threat-actor

KI als Verteidigungsfaktor: Vom Reagieren zum Antizipieren

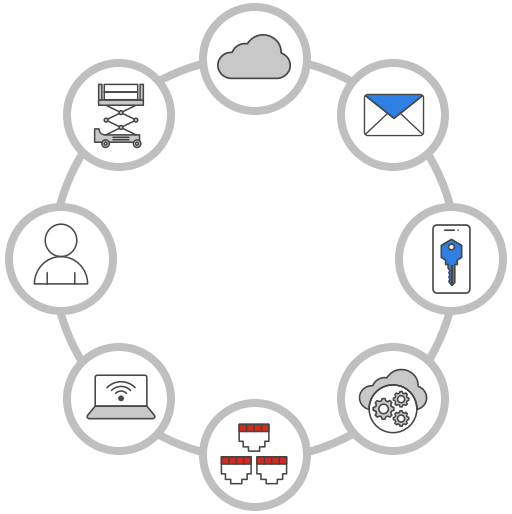
Herausforderungen für SecOps-Teams

Threat Landschaft



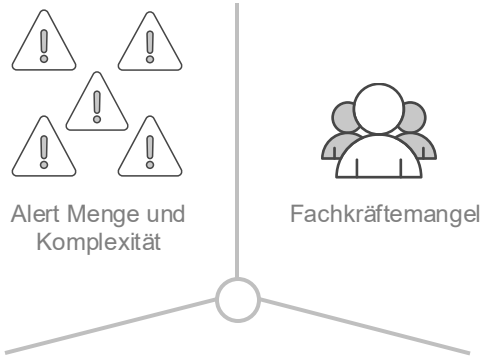
Geschwindigkeit und Raffinesse bei Cyberangriffen

Angriffsoberfläche



Weite & dynamisches Oberfläche, die kontinuierlich überwacht werden muss

SecOps Workload



Im Durchschnitt haben Organisationen

fast **50** **Security Tools**

in ihren Umgebungen, manche mehr als 140.

IDC Research

Threat Informed Defense

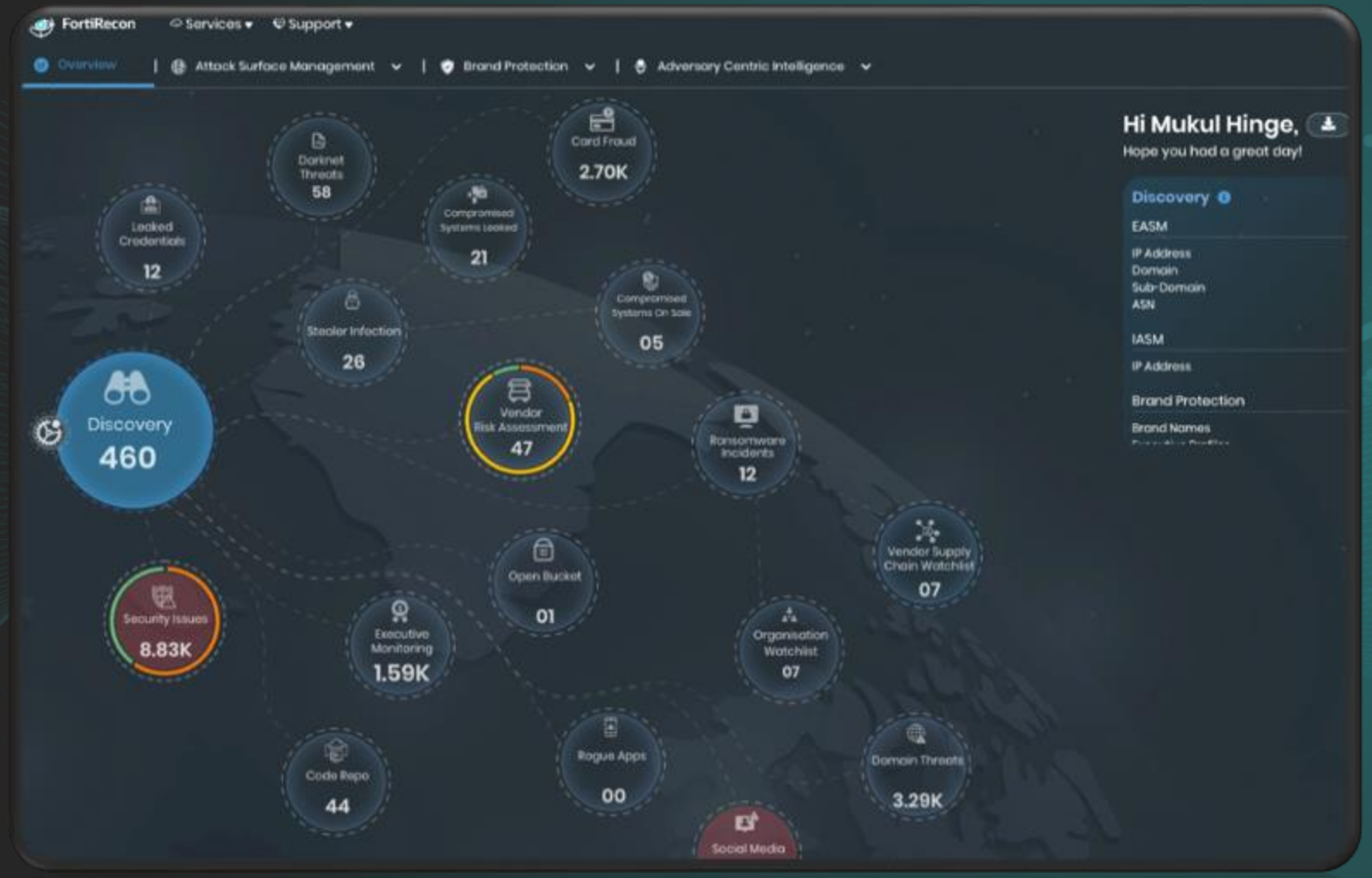
KI-gestützte Threat Intelligence

Datenvolumen und Angriffskomplexität übersteigen menschliche Analysefähigkeit

KI filtert, priorisiert und erkennt Muster

FortiRecon

Verhindern Sie Angriffe, bevor sie entstehen – indem Sie sehen, was Angreifer sehen.



Attack Surface Management

Kontinuierliche Erkennung und Überwachung der internen & externen Angriffsfläche

Sichtbarkeit von Assets erhöhen

Adversary Centric Intelligence

Kuratierte, umsetzbare FortiGuard Labs Bedrohungsinformationen

IR Zeiten reduzieren

Brand Protection

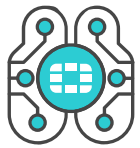
Marken- und Identitätsdiebstahl, Website-Typosquatting, betrügerische Anwendungen erkennen

Risiko einer Schädigung der Marke reduzieren

Automatisierte Analyse und Priorisierung

KI-gestützte Auswertung

KI entlastet Security-Teams, indem sie Routineanalysen übernimmt und Unbekanntes erkennt



Adaptive Response

Reaktion in Echtzeit

Durch eine integrierte Security Fabric können Verteidigungsmaßnahmen automatisiert ausgelöst werden übergreifend und lernfähig

KI einsetzen, wo sie am besten passt

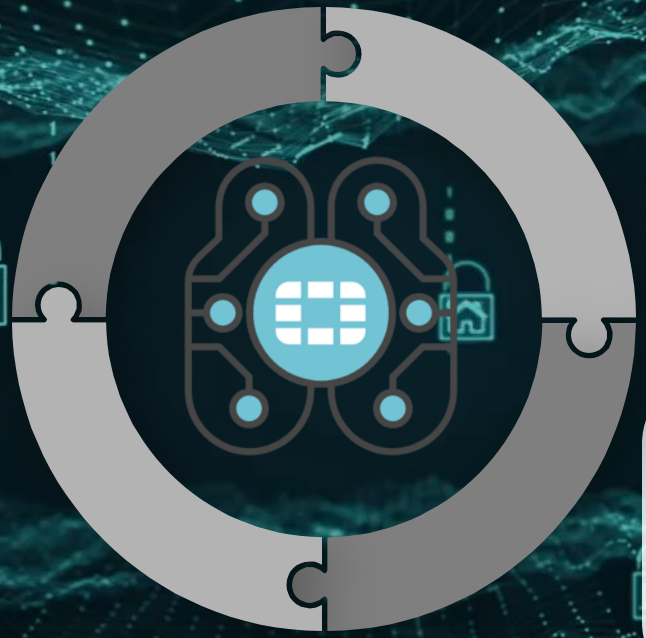
Nutzen Sie KI-Technologien am richtigen Ort und das Know How über die Threat Landschaft.

KI zur Erkennung von Bedrohungen

Kontinuierliches Training der Modelle, um Genauigkeit & Geschwindigkeit bei der Threat Detection zu verbessern.

KI für Networking

Move zu einem selbstheilenden Netzwerkmodell.



KI für Data Protection

Erkennen und verhindern von Datenlecks, wenn Large Language Models (LLM) in Cloud-Anwendungen eingesetzt werden.

KI für NoC und SoC

Nutzen Sie das Netzwerk und die Sicherheitsfunktionen wie FortiAI Advisor in FortiSIEM, FortiSOAR, FortiManager und FortiAnalyzer.

Security Strategy 2030

Mit KI Unternehmenssicherheit neu definieren

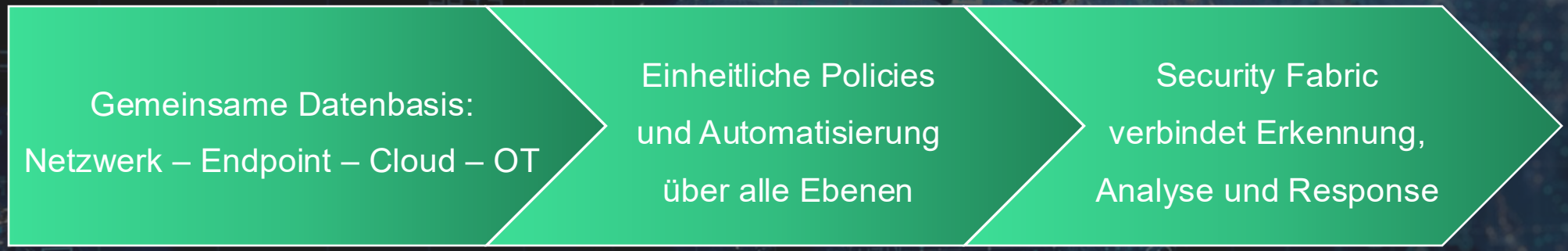
KI ist Teil der integrierten Security Architektur Kernbestandteil, kein Zusatzmodul

Lösungen, die permanent aus neuen Angriffsmustern lernen

Strategische Resilienz durch intelligente Automatisierung und schnellere Reaktionszeit

Integration statt Silos

Security Fabric statt Point Products



Silos verlangsamen Reaktion und erhöhen Risiko.
Integrierte Plattformen schaffen konsistente Sicherheit über Netzwerk, Cloud, Endpoint und OT

Adaptive Trust & Governance

Vertrauen, das sich dem Risiko anpasst

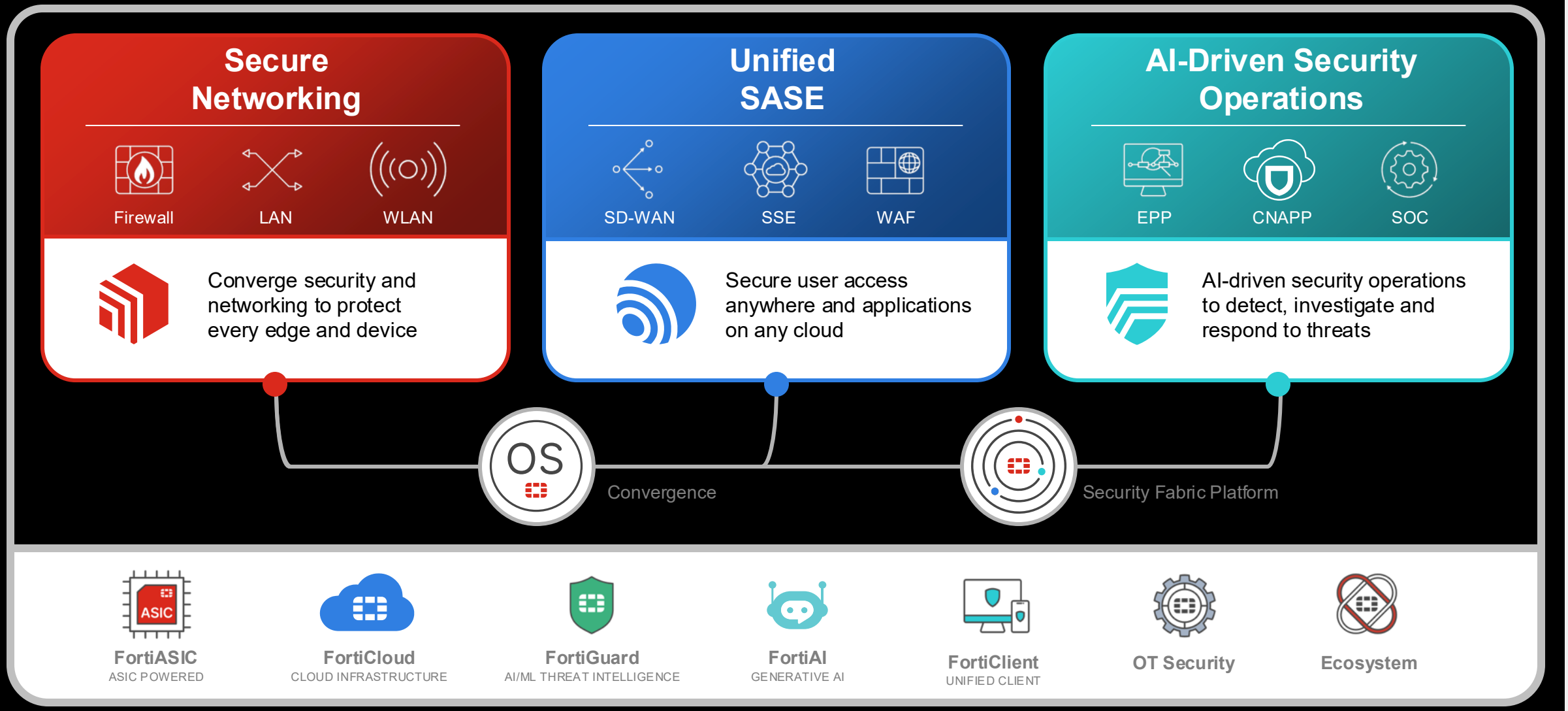
Vision 2030

Sicherheit als Business-Enabler

Unternehmen, die KI-gestützte Sicherheit strategisch integrieren, schaffen Vertrauen, Innovationskraft und operative Stabilität – Security wird Teil der Wertschöpfung


FORTINET

Why you keep hearing the term “Platform”



Global Cybersecurity Partnerships

Fortinet's historic involvement combatting the **evolving threat landscape**