GENESIS Swiss Team AG

evolving your
digital future

Vortrag

Automatisiertes Pentesting – das nächste Level:

RansomwareAware to RansomwareReady™

We Make Security Measurable!

PENTERA

GENESIS
SWISS TEAM AG

Agenda & Ziele vom Vortrag “Next Level - RansomwareReady™”

1. Angreifer Perspektive – Häufigkeit von Angriffen und deren Folgen
2. Positionierung Pentera – Automatisierte Penetration Test & Validierung Platform – nächster Level «RansomwareReady™»
3. End-to-End 360° Grad Sicht Pentera
4. Q & A

GENESIS IT Security Management

Focused Topics & Solutions

Data Privacy & Protection

DDI - DNS Security

Penetration Test

Access Rights Management

Managed Security Services (MSS)

Consulting Training & Awareness

Security Monitoring & Log Management

Privileged Access & Account Management (PAM)

evolving your
digital future

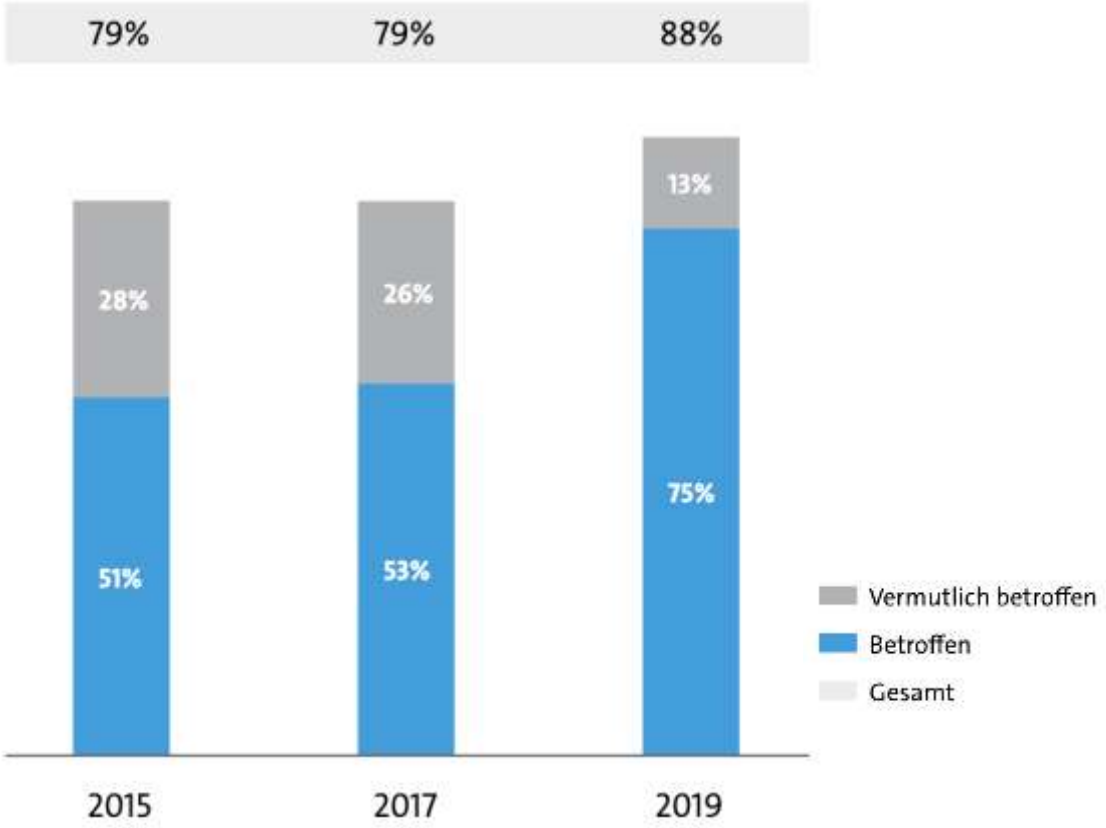
Angreifer Perspektive

Häufigkeit von Angriffen und

deren Folgen

Wir machen Security messbar!

Häufigkeit von Angriffen - Fakten

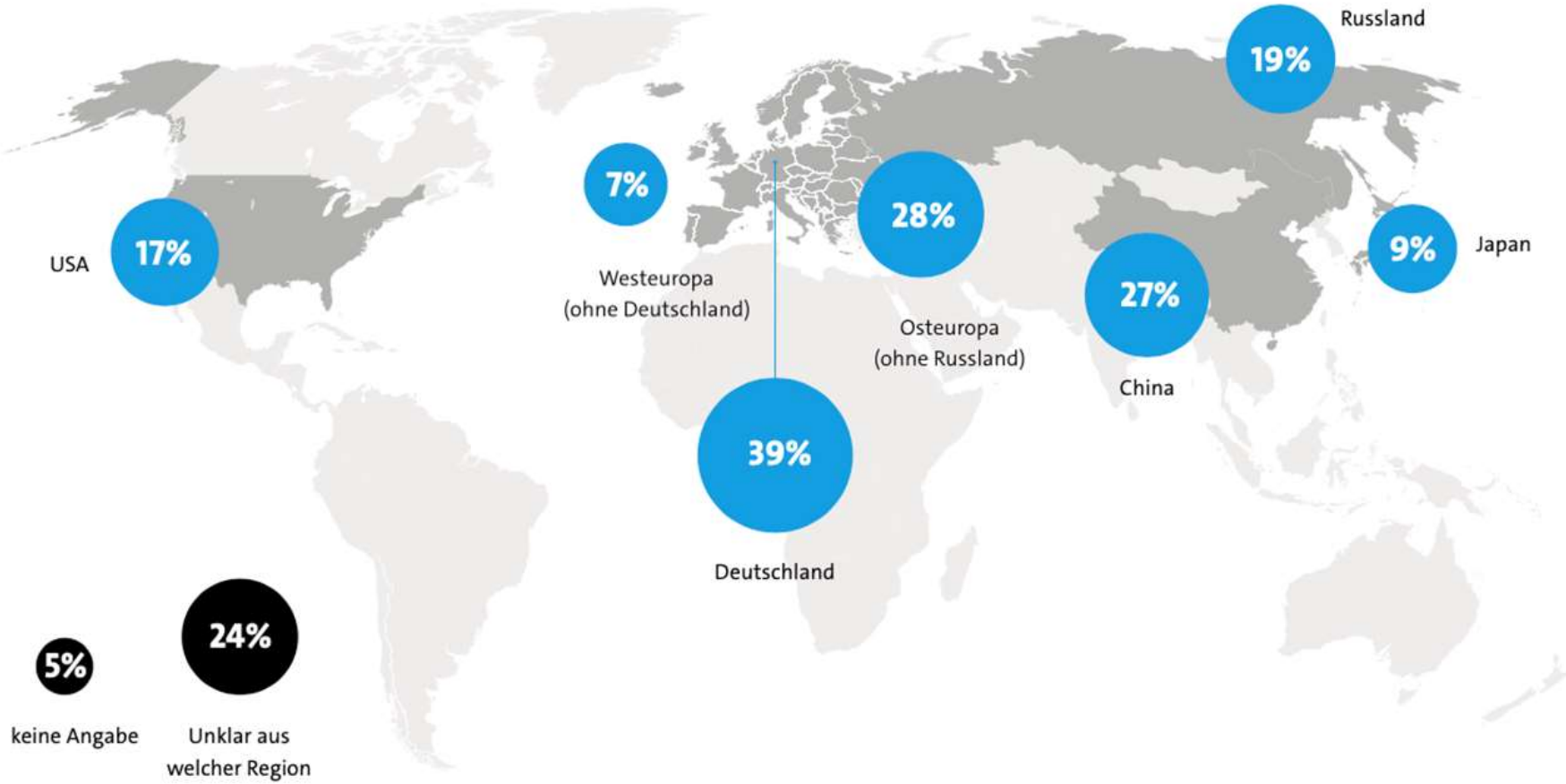


- Neun von zehn Unternehmen wurden laut einer aktuellen Studie in den Jahren 2020 und 2021 Opfer von Cyberkriminellen.
- „Die Wucht, mit der Ransomware-Angriffe unsere Wirtschaft erschüttern, ist besorgniserregend und trifft Unternehmen aller Branchen und Größen“, sagte Achim Berg (Präsident Bitkom).
- Die Angreifer habe es auf Kommunikationsdaten, Patente, Forschungsergebnisse abgesehen, auf Geld, manche Angriffe sind ausschließlich Sabotageakte.
- Neun Prozent der Unternehmen sehen ihre geschäftliche Existenz durch Cyberattacken bedroht
- 24 Prozent der Firmen haben ihre Investitionen in IT-Sicherheit als Reaktion auf die verschärfte Bedrohungslage deutlich erhöht (Zitate: Interview zur Bitkom Studie, 05.08.2021)

Schaden pro Jahr (Bitkom Studie 2019)

Delikttyp	Schadenssummen in Mrd. Euro (2019)
Kosten für Ermittlungen und Ersatzmaßnahmen	36,5
Kosten für Rechtsstreitigkeiten	31,2
Patentrechtsverletzungen (auch schon vor der Anmeldung)	28,6
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	27,0
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	22,2
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	22,2
Imageschaden bei Kunden oder Lieferanten/ Negative Medienberichterstattung	18,6
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	10,5
Datenschutzrechtliche Maßnahmen (z. B. Information von Kunden)	8,8
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	-
Sonstige Schäden	<0,1
Gesamtschaden innerhalb der letzten 2 Jahre	**205,7**

Angriffsursprung



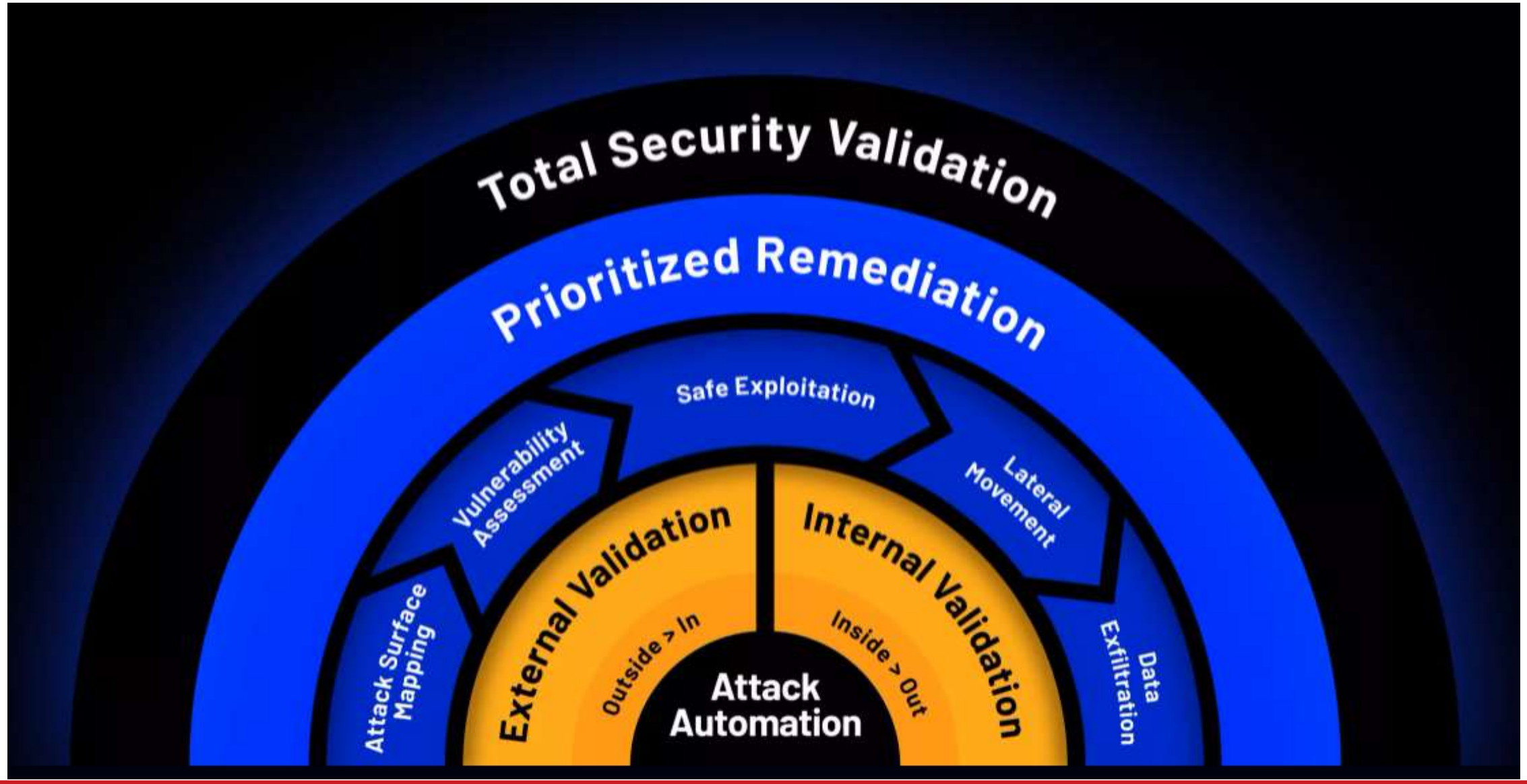
evolving your
digital future

Automated Security Validation™

PENTERA

Wir machen Security messbar!

Automated Security Validation Platform



Die Zunkunft von Pentetrationtest und Risiko Validierung

Pentera: +1000 Pen Tester zu Ihrer Verfügung – nicht auf Ihrer Gehaltsliste

> I think we can risk saying that Pentesting, as it is today, will cease to exist.

Gartner

Gartner COOL VENDOR 2020

Pentera – Disruptive Technologie

- **Keine Simulation** - keine statistischen Modelle, um Schlussfolgerungen von einem Lab zu einer Produktionsumgebung zu ziehen
- **Keine einfache CVSS-Scorecard** - Tausende von Ergebnissen, von denen nur ein Bruchteil ausnutzbar ist
- **Pentera verwendet ethische, "gutartige" Angriffe** - selbst entwickelt, um jede Art von Schaden zu vermeiden
- **Pentera Wiki** - erklärt die Schwachstellen, wie man sie behebt und wie man überprüft, ob die Abhilfemaßnahmen im Laufe der Zeit funktionieren
- **Validierung, dass Schwachstellenbehebungen funktionieren** - Wiederholung von PT mit identischen Einstellungen
- **Erhöhung der Häufigkeit** von Penetrationstests
- **Verringerung der Risiken** durch Berücksichtigung kundenspezifischer Anlagen, Schwachstellen und Bedrohungen
- **Executive Reporting:** Sicherheitslage im Zeitverlauf, Rechtfertigung, Fokus für weitere Investitionen
- **Intelligente Priorisierung von Aufgaben** - situationsbezogene Entscheidungsfindung auf der Grundlage der verfügbaren InformationenÜbersetzt mit www.DeepL.com/Translator (kostenlose Version)

Auszug Referenzen

Stand December 2021: Über 420 Kunden weltweit in unterschiedlichen Verticals

Finance

Blackstone, City National Bank (An RBC Company), FIS, BNP Paribas, Pharmaceutical Performance Network, BTIG, newamerican funding, B. Riley Financial

Healthcare

teva, Stevanato Group, NHS, GenesisCare, Apria Healthcare, Precision Medicine Group, beurer, Dechra

Manu

CATERPILLAR, CARRARO, ELECTRA, Israel Electric, DIODES, BUCHER, Leica Geosystems, CAMOZZI

Energy &Utilities

CRODA, agsm ENERGIA, A-GAS, eog resources, ICL, EAAGEZZ

E-commerce Retail

WILLIAMS SONOMA, PUIG, Grupo Damm, MANGO, SEPHORA, YOOX NET A PORTER GROUP, GAP, Herc Rentals

Insurance

AA, Alliant, Phoenix, Monuta, LOMBARD INTERNATIONAL ASSURANCE, HAREL, CLAL INSURANCE & FINANCE, AYALON

Agriculture & Food

CKE RESTAURANTS, LAKESIDE FOODS, Big Y, BREWDOG, NETAFIM, CHIPOTLE

Education

University of South Wales, DEAN COLLEGE, GWINNETT COUNTY PUBLIC SCHOOLS, South Staffordshire College, MOUNT ST. MARY'S UNIVERSITY, Ravensbourne

Construction

zehnder, EMAAR, SHAPIR, SKANSKA, INTERNATIONAL MARKET CENTERS, JANSEN, Anticipa

Cybersecurity/MSSP

towerwall, GUIDEPOINT SECURITY, exabeam, CYBERARK, BlueVoyant, Redpoint, Netswitch Technology Management

Aerospace & Defense

ADDSECURE, John Cockerill, TBG SECURITY

Government & Municipality

City of Vienna

Business & Consulting

SCHELLENBERG, YIGAL ARNON & CO., PAUL HASTINGS, DRAWBRIDGE, Taylor Vinters, Insight

Telecommunications

dish, NTT, etisalat, altice, IP TELECOM, NineStar

Transportation & Navigation

LA THE PORT, TOYOTA, CAR-O-LINER, ermewa, ISRAEL RAILWAYS, RHENUS LOGISTICS

Nonprofits

British RedCross, Christian Care MINISTRY, Seventh-day Adventist Church, TCI Fund Management Limited, liveBetter

Pentera - Vorteile

- Agentenlos
  - Network «Plug & Play»
- On-prem Lösung
- Umfassend
  - 7x24; nie müde
- Wählen Sie ihre Pen-Testing Boxfarbe:
  - Blackbox Pentest (PT), Graybox (geführt) PT & Single Action PT
  - Schwachstellen Analyse
  - Password Analse Assessment
  - RansomwareReady Analyse

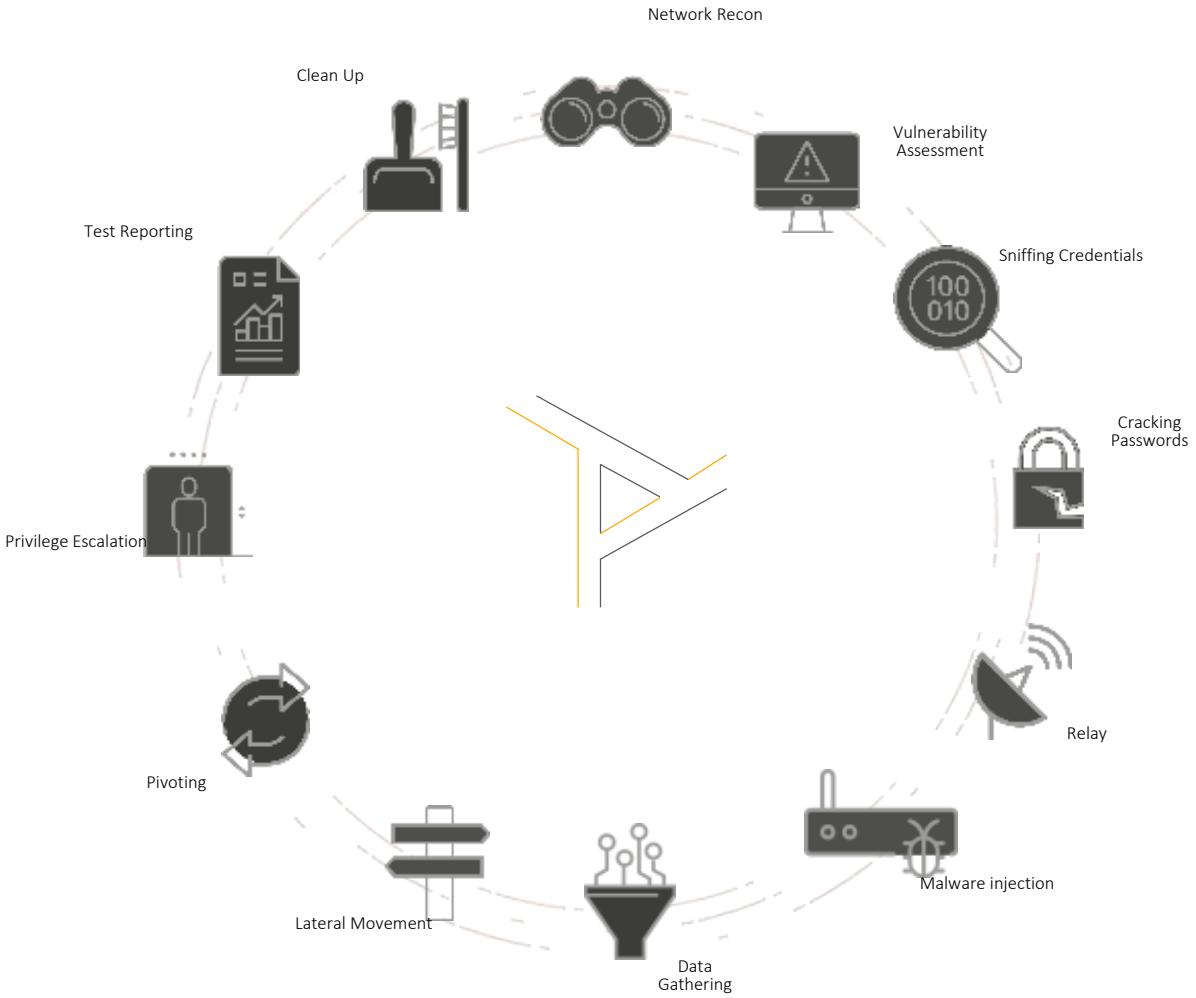
- Sicher & kontrollierter PT
  - Regel #1: Keinen Schaden anrichten!
- Einstellbarer PT - Tarnungslevel
  - Fordern Sie sowohl ihre Detektions- als auch ihre Präventionsysteme heraus!
- Keine Simulation – echte «ethical exploits»
  - Prüfung der «Verletzbarkeit» mit einem Minimum an «false positives»

A CISOs best friend:

QUICK SETUP	SAME DAY RESULTS	NO LEARNING PHASE	NO LENGTHY CONFIGURATION

Pentera Attack Orchestrator™

The power of 1’000 pen-testers in a click of a button



AGENTLESS

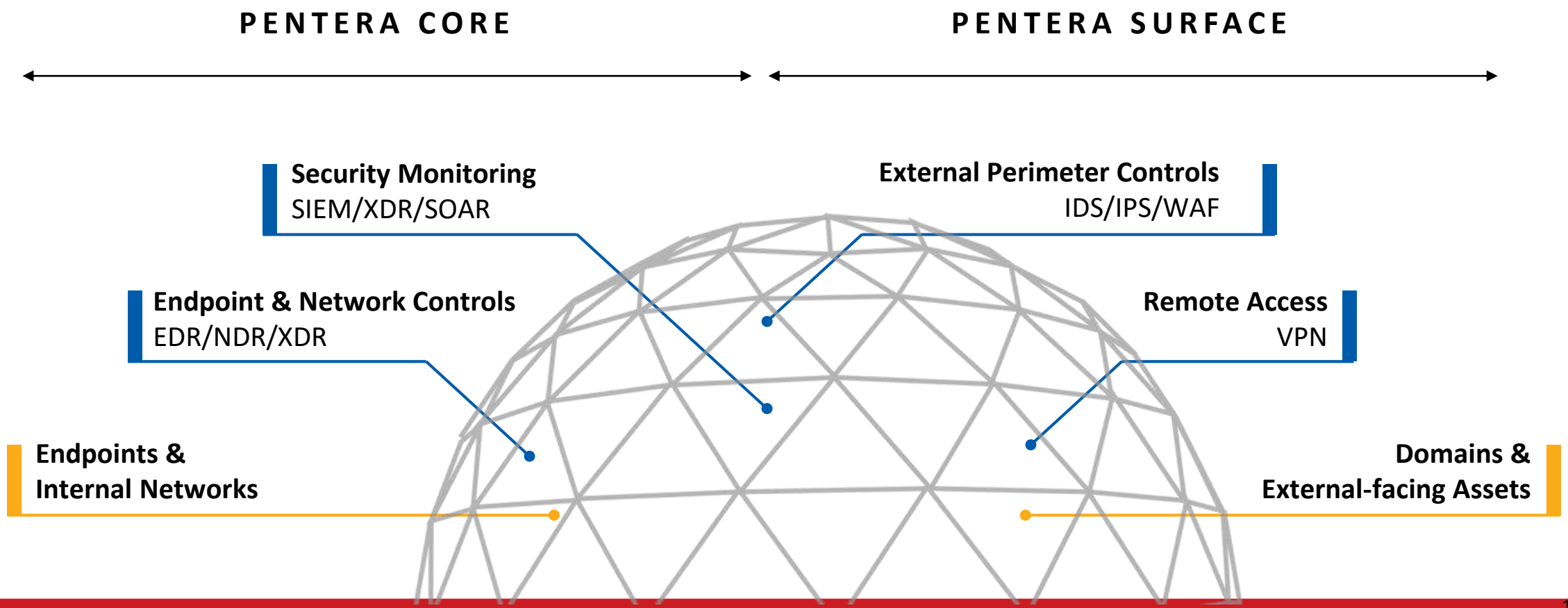
REAL

SAFE

AUTONOMOUS

COMPREHENSIVE

Sind Sie von der Leistungsfähigkeit Ihrer Organisation überzeugt? **Cyber Bedrohung & Risiken?**

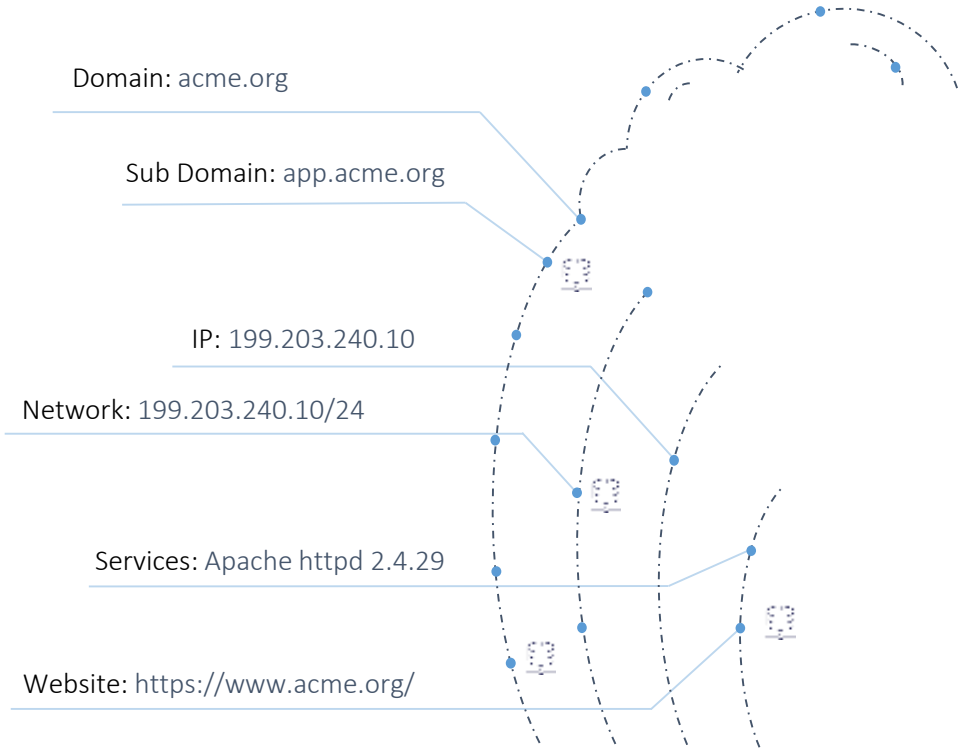


Was ist eine externe Angriffsfläche

Die Angriffsfläche eines Unternehmens besteht aus allen über das Internet zugänglichen

- Hardware-, Software-, SaaS- und Cloud-Ressourcen, die Daten verarbeiten oder speichern

und von einem Angreifer entdeckt werden können, um in die Umgebung einzudringen, eine Auswirkung darauf zu haben oder Daten daraus zu extrahieren.



Discover

- Aufklärung Ihrer Angriffsfläche
- Aufzählung und Beschaffung aller erforderlichen Informationen

Assets, services, protocols, networks, domains, IPs, ports, DBs, VPN, …

Scan

- Statisches und dynamisches Scannen von Sicherheitslücken
- Konzentration auf ausnutzbare Sicherheitslücken und Schwachstellen

Expose

- Ziele mit hoher Konfidenz
- Top-verwertbare “attractions”

evolving your
digital future

RandsomWare Ready

PENTERA

We Make Security Measurable!
Wir machen Security mess- und kommunizierbar

Ransomware – Ein universelles Geschäftsmodell

- Einfache Lösegeld Forderung um Firmendaten zurück zu erhalten

- Bei der **«Double Extortion»** genannten doppelten Erpressung verschlüsseln die Angreifer die Daten ihrer Opfer und drohen zusätzlich damit, brisante Informationen zu veröffentlichen, wenn kein Lösegeld bezahlt wird.

- Relativ neu ist die Problematik der **«Triple Extortion»**. Hier versuchen die Angreifer nicht nur die Opfer zu erpressen, sondern auch deren Kunden und Partner. Die Angreifer kontaktieren also auch (vermutlich) ahnungslose Kontakte ihrer Opfer, um zusätzlichen Druck auszuüben.

Prioritized achievements based on true-risk

MITRE ATT&CK Tactics & Techniques successfully executed

Info & context to better understand risk and impact

Guided remediation steps

Hosts compromised

Resilience Score including
Encryption
Data Exfil
Achievements
EDR bypass

Endpoint Security bypass results

evolving your
digital future

Weitere Details

We Make Security Measurable!

PenTera in Zahlen: Maschinenbasierte Skalierbarkeit

500x schneller als ein manueller Pentester

Angriffsvektoren - Kombinationen

Protokolle X Zugriffs Typen X Payload Typen X Umgebungs Techniken X C2 Techniken

~4

Attack Vectors / day

PENTERA

~2000

Attack Vectors / day

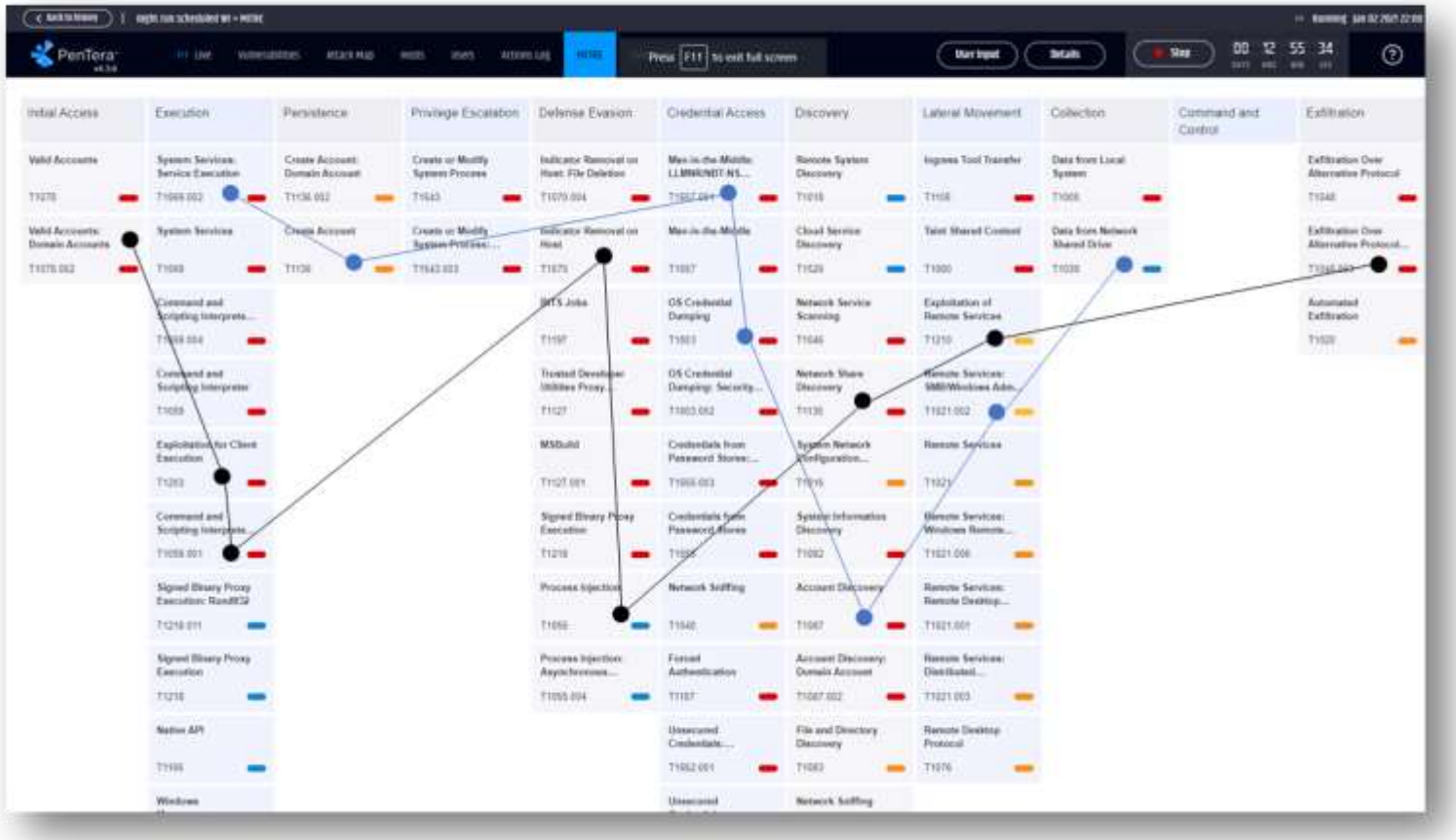
Pentera – Report Möglichkeiten

- Schwachstellen: Auflistung aller Schwachstellen sortiert nach CVSS, inklusive Schwachstellen Priorisierung basierend auf dem Kunden spezifischen Pentest Ergebnissen sowie Bereinigungs Anweisungen
- Angriffs Karte – Alle Angreifer Erfolge mit Detailinformationen sowie einer Visualisierung des gesamten Angriff Vektors. Beinhaltet auch eine Simulation um die hauptsächliche Schwachstelle des Angriff Vektors zu definieren
- Host Informationen – Darstellung aller gefundenen Informationen wie IP, OS, MAC Adresse, offene Péorts, Anzahl der Schwachstellen und deren bewertete Gewichtung
- Benutzer Informationen – Auflistung aller Benutzer im Pentest inkludierten Benutzer
- Action Log – Vollständiger Bericht, alle Log Informationen mit sämtlichen durchgeführten Aktionen mit entsprechenden Parametern und Status Informationen (erfolgreich bzw. nicht-erfolgreich)
- MITRE Framework – Regelwerk Abbildung basierend auf den Angreifer „Taktiken und Techniken“
- Footprint Report – Angabe aller heruntergeladenen Files sowie generierter User sowie deren Bereinigung Status
- Report – Zusammenfassungen für das (Exekutiv-) Management sowie Detail Reports für technische Mitarbeiter

PenTera Performs a Complete Attack Operation

Complete Attack Operation

Sniffing > Relay > Code-Execution



Pentera - Teststellung

Ablauf PoV (Proof of Value)

PoV Prinzipien:

- Sicher und kontrolliert
- Keine Lernphase; keine KI, kein cloudbbasiertes Interface voraussetzt
- On-prem – alle Informationen bleiben beim Kunden – keine VAR oder Pentera Zugriffsmöglichkeiten

Leistungsmerkmal POV:

- Blackbox-Test /Greybox-Test
- Bereich von **50/100** IP Adressen
- Auszug vom möglichen Services (Inhalt wird vorbesprochen)
  - Prüfen von Malware-Erkennung, Antivirenlösungen
  - Validieren von Passwortstärken
  - Darstellen von kritischen Schwachstellen und potentiellen Risiken
  - Validieren von internen wie externen Security Services
  - Objektive Bewertung inklusive Handlungsempfehlung
  - Dokumentation

DEMO TIME

Halle 7 – Stand 7-231

Was kann da schon schiefgehen…?

Thank you - Danke

GENESIS Swiss Team AG
Gerhard Bartsch
Bernstrasse 34
3072 Ostermundigen
Tel: +41 31 560 35 35
Mob: +41 79 208 91 29

gerhard.bartsch@genesis.swiss
www.genesis.swiss