Wenn KI zum Angreifer wird

Vertraulichkeit: White

SECURE. DEFEND. EVOLVE.

bpn-group.com

ABOUT US

Reinhard Kucera
CTO BPN Group

MSc in IT-Security
(FH St. Pölten, San Diego State University, FH Technikum Wien)
~ 4 Jahre CISO-Unterstützung im Bankenbereich
~ 9 Jahre bei kritischer Infrastruktur, CISO ~ 7 Jahre
Seit 2023 bei BPN
Consultant (NIS2, DORA), Prozessoptimierer

ABOUT US

BP Networks

Mehr als 20 Jahre Erfahrung im Bereich Cybersicherheit

Wir bieten maßgeschneiderte Cybersicherheitsdienste und Red-Teaming-Services, die höchste Standards, innovative Lösungen und globale Erfahrung kombinieren.

Von der D-A-CH Region bis in den Nahen Osten stärken wir die digitale Resilienz unserer Kunden mit modernsten, angriffsorientierten Verteidigungsstrategien.

2B1

ABOUT US

BPN

- AUSTRIA
- GERMANY
- UAE

Folie 4

PB1 [@KRAINER Bernhard | [BPN/AT]] Bitte noch die logos von DOKA, MIBA, KNAPP,Spängler privatbank, Casinos Austria
BARDEL Patrick | [BPN]; 2025-05-14T15:58:10.838

2 [@BARDEL Patrick | [BPN]] bitte hier noch die logos, die du nicht drin haben willst, rausnehmen. Und für ein wietersdorfer entscheiden (hab w&p zement schon drin und die group oben, falls dir die lieber ist
KRAINER Bernhard | [BPN/AT]; 2025-05-21T14:50:52.454

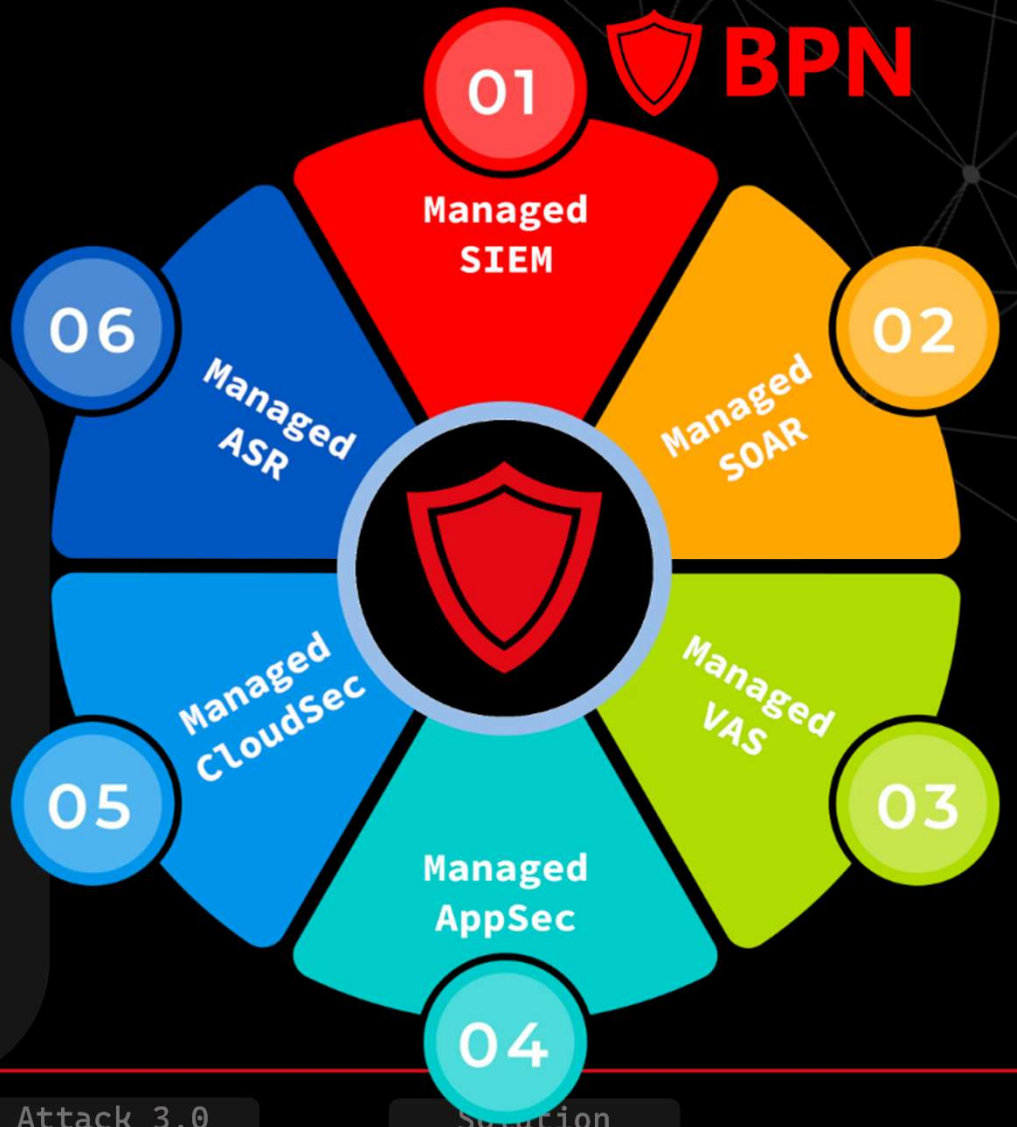
ABOUT US
MANAGED SERVICES

Immer aktiv. Immer besser. Immer für Sie da.

Unsere Managed Services decken alles ab, was für kontinuierlichen Schutz und die Verbesserung Ihrer Sicherheitsinfrastruktur erforderlich ist.

Wir agieren als Erweiterung Ihres internen Sicherheitsteams – überwachen, schützen und verbessern Ihre Systeme rund um die Uhr.

Unsere Grundlage: **Vertrauen, Resilienz und ganzheitliche Verteidigung.**



ABOUT US
MANAGED SERVICES

- SOC mit ausschließlich **in Österreich** ansässigen Analysten
- SIEM **ohne Kostenüberraschungen**
- Laufende **Schwachstellenscans** inkl. Expertenbewertungen
- Attack Surface Erkennung
- **Automatisierte Abwehr** von Angriffen auf Unternehmen

ABOUT US
MANAGED SERVICES

Kontinuierliche Verbesserung durch:

- Analyse **neuer Schwachstellen und Bedrohungslandschaften**
- Tuning und Weiterentwicklung von **Detection-Use-Cases**
- Proaktive **Threat Intelligence Integration**
- **Red-Teaming und Purple-Teaming**
- Erkennung und Verteidigung von **AI-gestützten Angriffen**

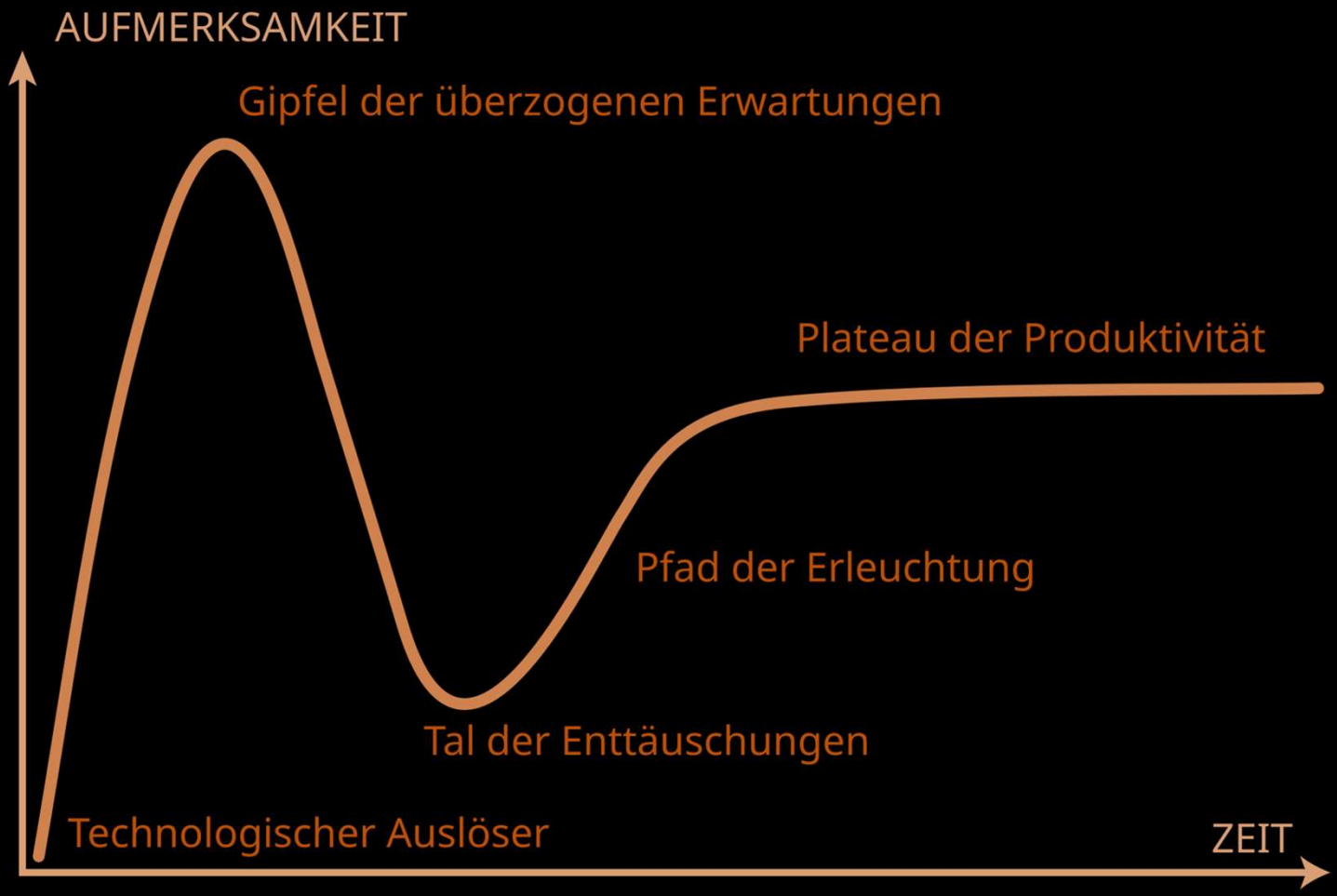
PB1

Folie 8

PB1 [@KRAINER Bernhard | [BPN/AT]] hier auch datum dazu bei jeder - wann ist veröffentlicht worden ?
BARDEL Patrick | [BPN]; 2025-05-14T14:22:32.462

PB2

AI – HYPE CYCLE



Folie 9

PB1 [@KRAINER Bernhard | [BPN/AT]] when ? (Version, datum ?)
BARDEL Patrick | [BPN]; 2025-05-14T14:21:13.751

PB2 [@KRAINER Bernhard | [BPN/AT]]wann wurde veröffentlicht ? Bitte dazuschreiben - wann ist die Lücke aufgetaucht ?
BARDEL Patrick | [BPN]; 2025-05-14T14:22:08.045

AI IN CYBERSE

BPN

Forbes

INNOVATION > C

Goog
Finds

By Davey Winde

Published Nov 05, 2

README

Digital Transformation » AI » The AI cybercrime wave has now reached 87% of global businesses

The AI cybercrime wave has now reached 87% of global businesses

Author
Marina Mouka

Date published
March 10, 2025

Categories
AI
CFO and Technology
Cyber Security
Fraud

A new arms race is unfolding in cybersecurity, and artificial intelligence is at its core. Attackers are using AI to supercharge deception, making fraud more convincing, more scalable, and harder to detect. The numbers are staggering: 87% of global organizations faced an AI-powered cyberattack in the past year, according to SoSafe's *Cybercrime Trends 2025* report. And the threat is only accelerating.

Quelle: the-cfo.io

Who We

tution

CYBER ANGRIFFE – GESTERN

- Von Menschen gesteuerte Angriffe
- Fokussierte Ziele, begrenzte Reichweite
- Langsam
- Nicht skalierbar

CYBER ANGRIFFE – HEUTE

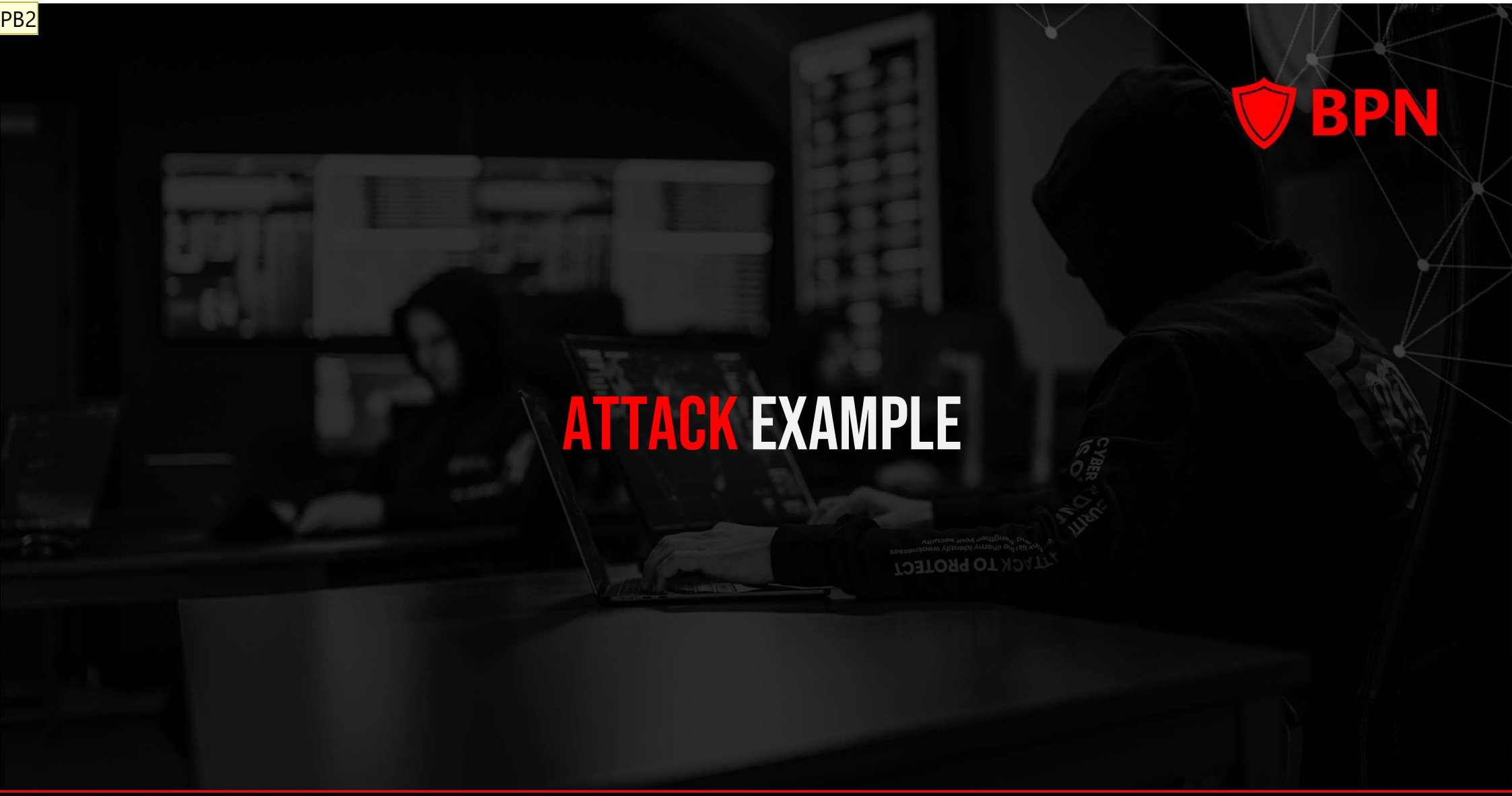
- KI-gestützte Automatisierung
- Massive Skalierung und Parallelität
- Schnell und adaptiv
- Personalisiert statt „Spray & Pray“

ABWEHR VON AI-DRIVEN ATTACKS

BPN

- Angriff ist die beste Verteidigung
- Ausführen und Lernen von AI gestützten Angriffen
- Anpassen von SOC-Detection Use-Cases
- Laufende Verbesserung

PB2



Folie 14

PB1 [@KRAINER Bernhard | [BPN/AT]] hier auch datum dazu bei jeder - wann ist veröffentlicht worden ?
BARDEL Patrick | [BPN]; 2025-05-14T14:22:32.462

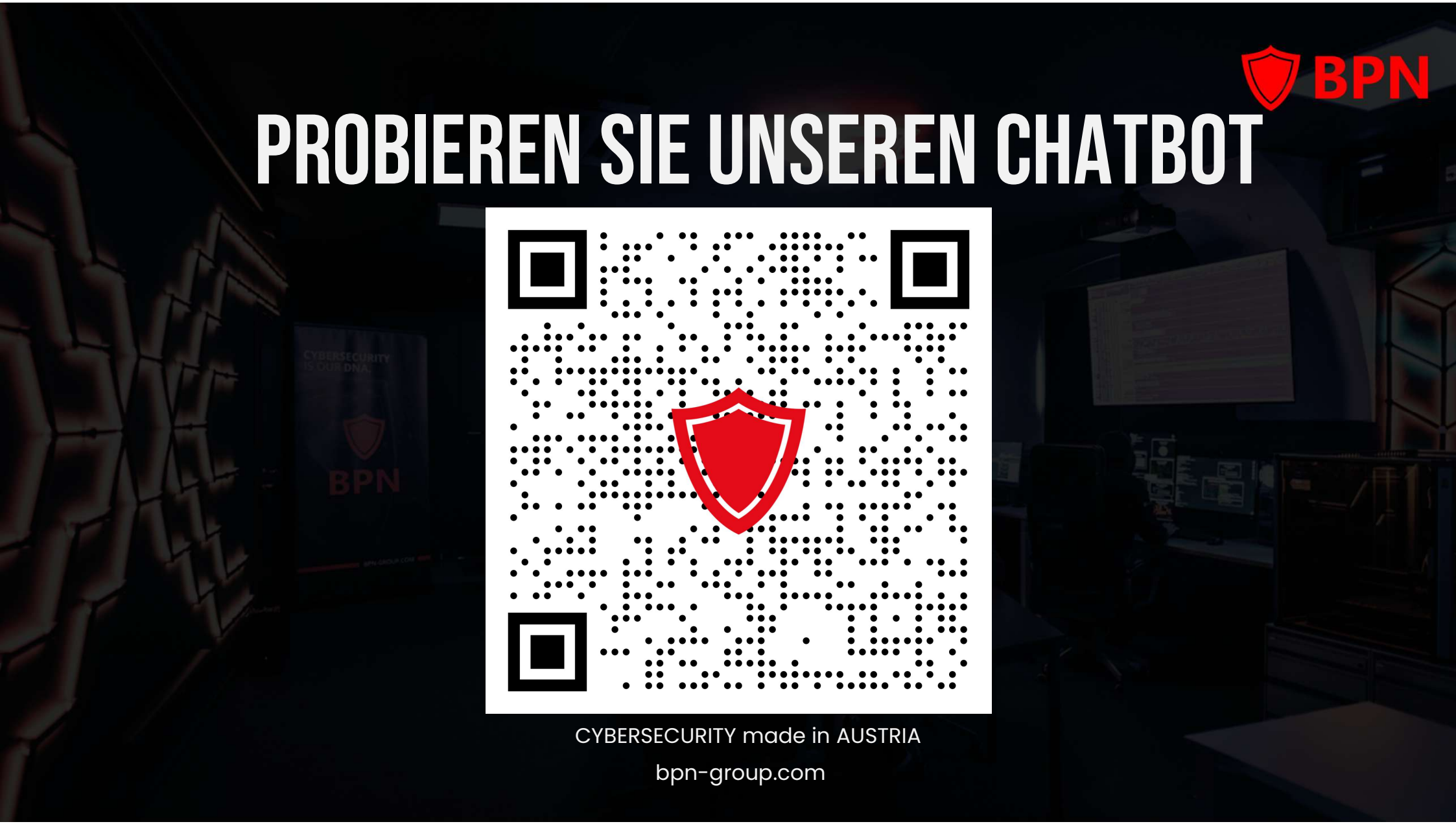
PB2 [@KRAINER Bernhard | [BPN/AT]] kannst da ein BPN attacker foto nehmen von unserem Shooting ?
BARDEL Patrick | [BPN]; 2025-05-14T17:02:37.264

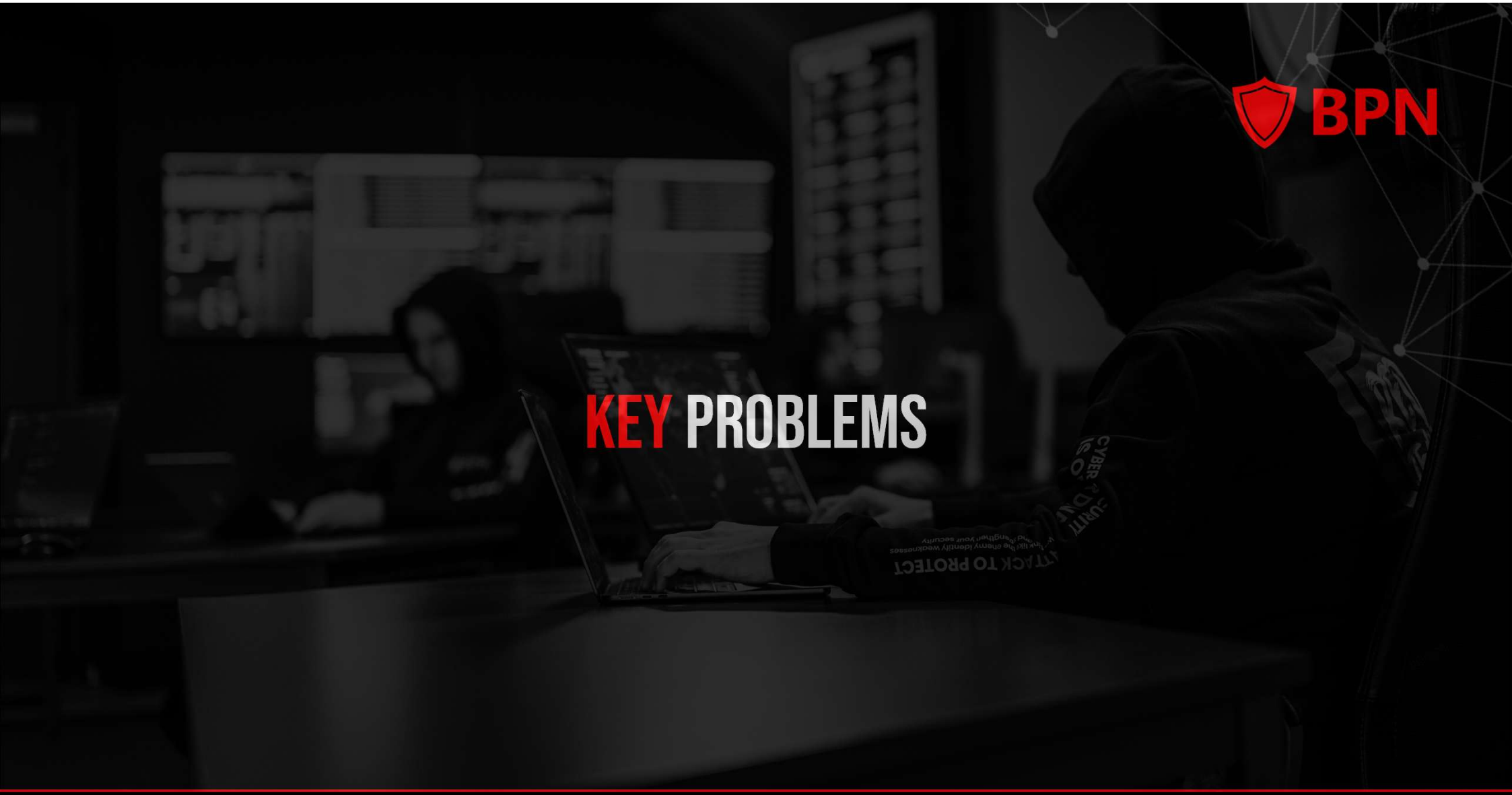
BPN

Who We Are | Actual News | Attack 3.0 | Solution

BPN

Who We Are | Actual News | Attack 3.0 | Solution


BPN
PROBIEREN SIE UNSEREN CHATBOT
CYBERSECURITY made in AUSTRIA
bpn-group.com


BPN
KEY PROBLEMS

KI-GESTÜTZTE ANGRIFFE

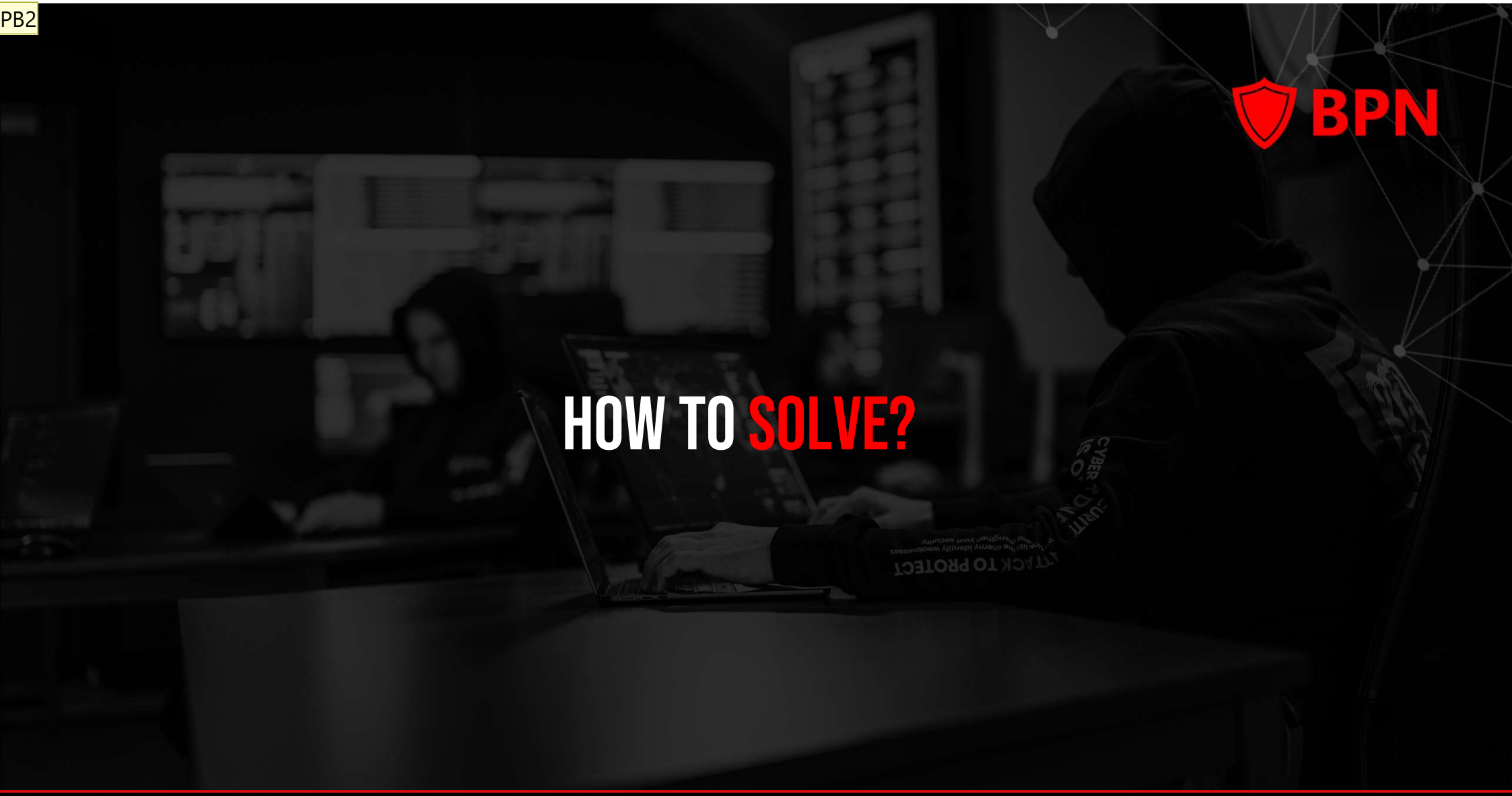
- Autonome & gezielte Phishing-Kampagnen
- Deepfake & Targeted Social Engineering
- KI-gestütztes Ausnutzen von Schwachstellen

ZUNEHMENDE KOMPLEXITÄT DER INFRASTRUKTUR

BPN

- Hybride und Multi-Cloud-Infrastrukturen
- Shadow IT & unbekannte Systeme
- Permanente Sichtbarkeitslücken bei IT/OT Assets

PB2



Folie 21

PB1 [@KRAINER Bernhard | [BPN/AT]] hier auch datum dazu bei jeder - wann ist veröffentlicht worden ?
BARDEL Patrick | [BPN]; 2025-05-14T14:22:32.462

PB2 [@KRAINER Bernhard | [BPN/AT]] kannst da ein BPN attacker foto nehmen von unserem Shooting ?
BARDEL Patrick | [BPN]; 2025-05-14T17:02:37.264

STRATEGISCHER ANSATZ FÜR MODERNE VERTEIDIGUNG

BPN

- Kontinuierliche 24/7-Bedrohungsüberwachung & Asset Discovery
- KI-gestützte Bedrohungserkennung & Alarmierung
- Vollständige (!) Sichtbarkeit über die gesamte Angriffsfläche

BPN SOC KEY FACTS

BPN

20 YEARS
Providing Reliable Security Solutions

70+
Countries

1.135 B+
Events per Year

250.000
Protected Assets

1.600 TB
Annual Analyzed Logs
(~2.2 B DIN A4 pages per Day)

100+
Satisfied Customers

MAßNAHMEN

- Aktive Reduzierung der Angriffsfläche (ASR)
- Situationsbewusstsein auf Management-Level
- Ständige Erkennung und Behebung v. Lücken 24/7
- Sofortiges Handeln

DER BPN ANSATZ

- Umfassende Sichtbarkeit der Angriffsfläche
- Risikobasierte Priorisierung von Schwachstellen
- Automatisierte Workflows
- Überwachung der techn. Verbesserung (KVP)
- Sensibilisierung des Top-Managements

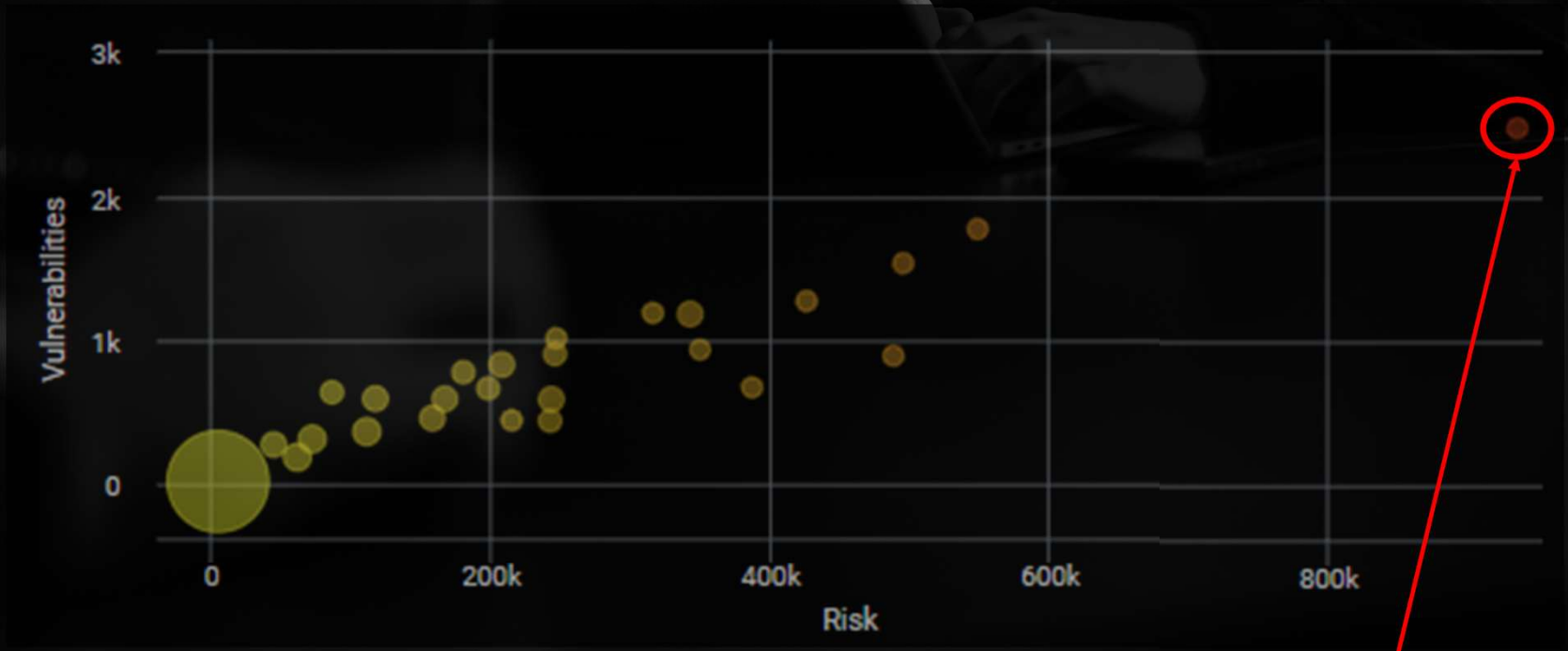
Full protection **Unlimited automation** **Unlimited auditing**

DER BPN ANSATZ

KONTINUITÄT

DER BPN ANSATZ

PRIORISIERUNG



Address	Name	Operating System	Malware	Exploits	Vulnerabilities	Risk
144.76.149.156	srv02	Microsoft Windows Server 2012 ...	0	30	2451	929.64k

DER BPN ANSATZ

REPORTING ANS RISKMANAGEMENT

BPN

Attack Surface ›

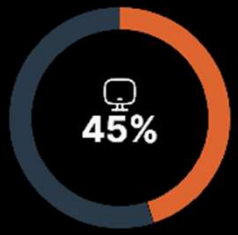
101,511 Assets ›

68,662 Identities ›

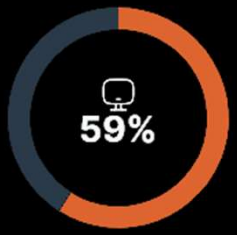
19,439 External Discoveries ›

10,231 Cloud Assets ›

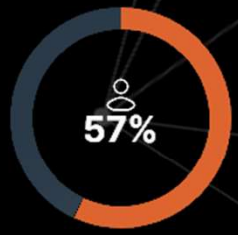
Assets with Endpoint Security ›



Assets with Vulnerabilities Assessed ›



Identities with MFA Enabled ›



Top Remediations

2025-05 Cumulative Update for Microsoft Windows 10, version 1607 (KB5058383)

2021-02 Cumulative Update for Windows 10 Version 1607 for x86-based Systems (KB4601318)

Upgrade to the latest version of Google Chrome

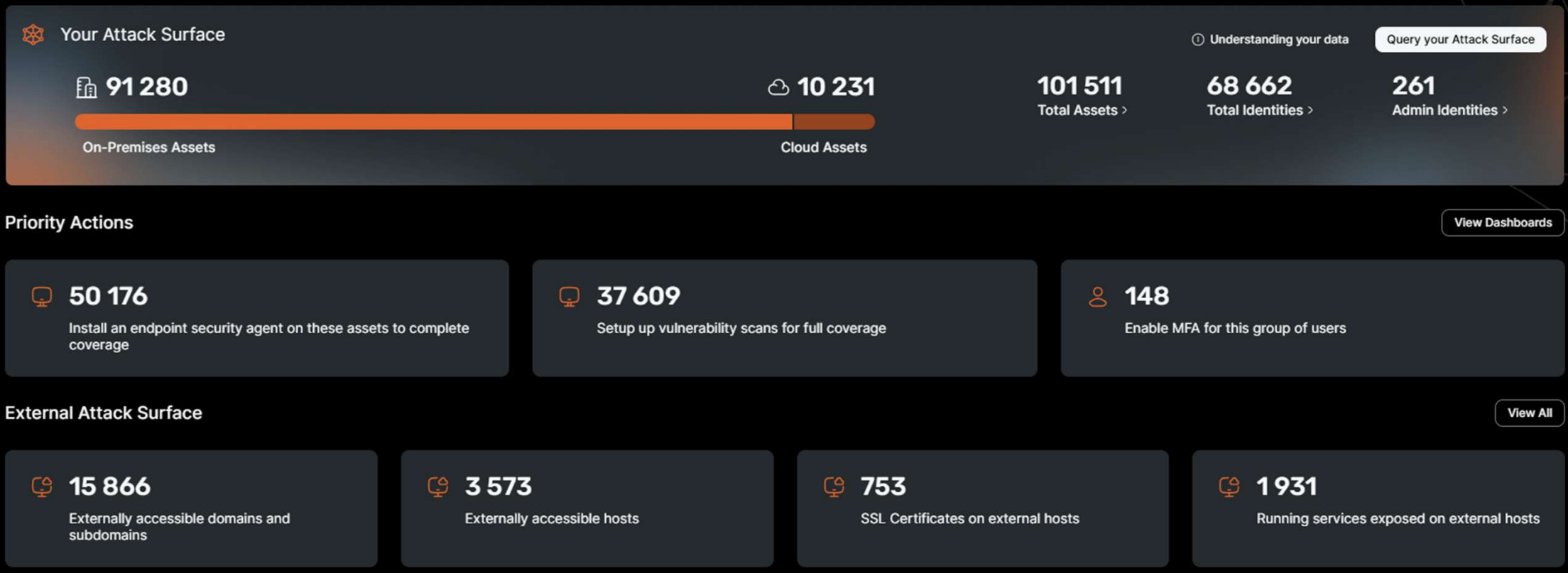
2024-10 Cumulative Update for Microsoft Windows 11, version 21H2 (KB5044280)

2020-10 Security Update for Adobe Flash Player for Windows 10 Version 1607 for x64-based Syste...

DER BPN ANSATZ

REPORTING ANS RISKMANAGEMENT

BPN



PB1

TECHNOLOGY

Protection

- Full Protection with Auto Containment

End Customer Management

- Customer SOC Portal
- Integrated Ticketing
- Customizable Security Reporting

Big Data & Analytics

- Cloud-based SIEM (GER/UAE)
- Threat Detection & Alerting
- Stream Processing for Security Events
- ML-Driven Behavioral Analytics

SOC Platform

- Multi-Tenant SOC Portal
- Investigation Management
- SOAR-Driven Response Automation
- Threat Intelligence Sharing & Collaboration
- SLA Monitoring & Performance Insights

Threat Intelligence

- Dynamic Analysis
- Signature & Heuristic Analysis
- Expert-Led Threat Evaluation
- ML & Behavioral Threat Modeling
- Adversary Profiling & TTP Mapping
- Darknet & Deep Web Monitoring

Managed Enpoints/Threat Sensors

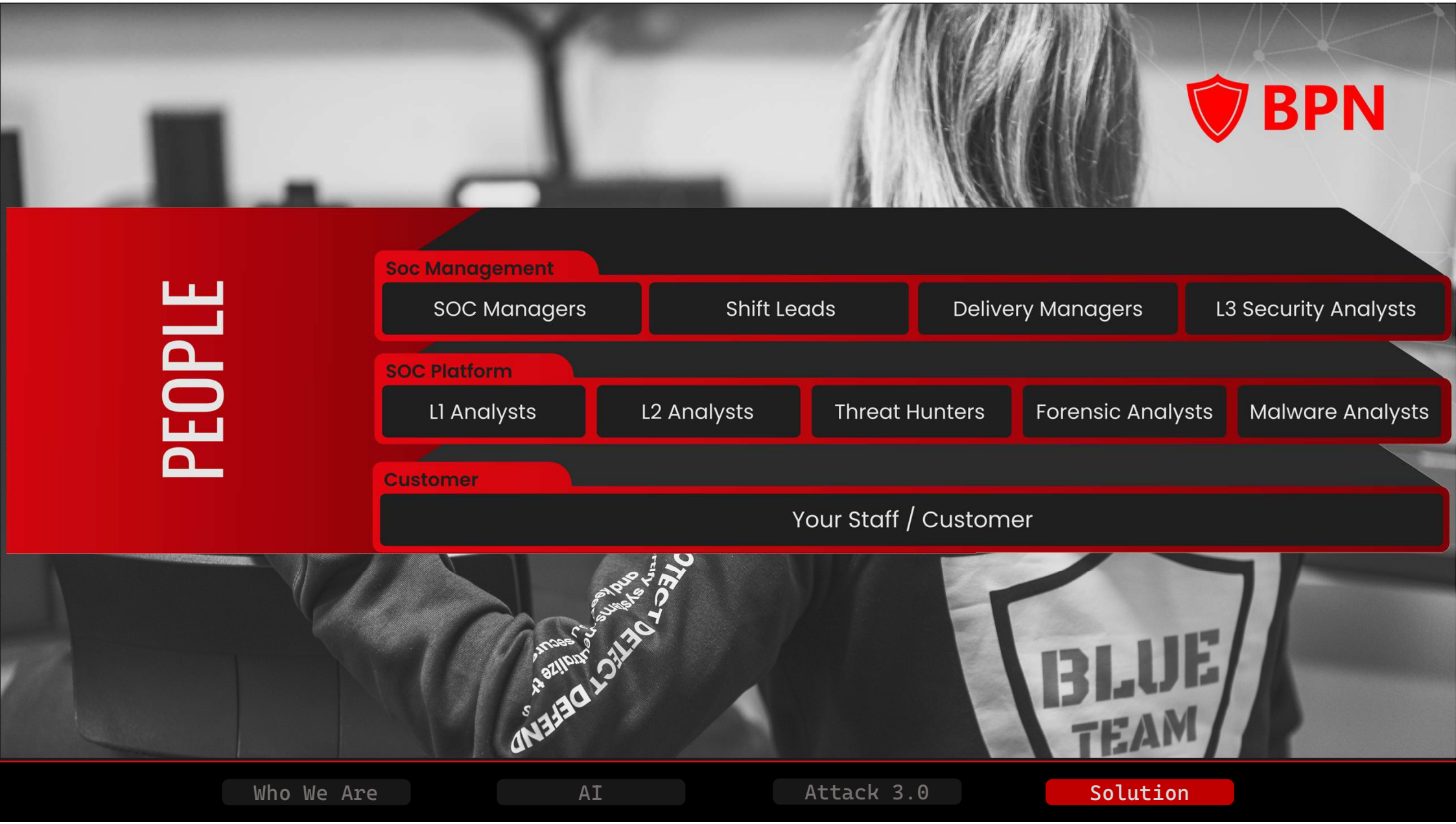
- Customer Endpoint
- BPN EDR
- BPN Lightweight Network Sensor
- Automated Asset Discovery
- Vulnerability Scanner
- Clourity Patch Management
- PAM Remote Access
- Log Collectors

Network Sensors

- BPN Lightweight Network Sensors
- Enterprise-Grade Network Sensor

PB1 Bitte hochauflösende Grafiken - die Pixeln aus [@KRAINER Bernhard | [BPN/AT]]
BARDEL Patrick | [BPN]; 2025-05-14T14:26:14.111

1 0 Ginge ev noch höher die auflösung, wird dann aber der rechner nicht schaffen. Tut sich jetzt schon schwer.
KRAINER Bernhard | [BPN/AT]; 2025-05-14T15:19:46.015


BPN
PEOPLE
Soc Management
SOC Managers
Shift Leads
Delivery Managers
L3 Security Analysts
SOC Platform
L1 Analysts
L2 Analysts
Threat Hunters
Forensic Analysts
Malware Analysts
Customer
Your Staff / Customer
BLUE TEAM

PROCESS

Notification and Escalation Management

- Notification Management
- Structured Escalation Handling
- Post-Incident Review & Knowledge Retention

Operational Guides & KB

- Incident Response Guides and Repositories
- Trainings and Certification
- Continuous Improvement

Incident Handling

- L1 - L2 Incident Management
- Escalation Handling Workflow
- False Positive Management
- Coordinated Incident Response

Threat Hunting

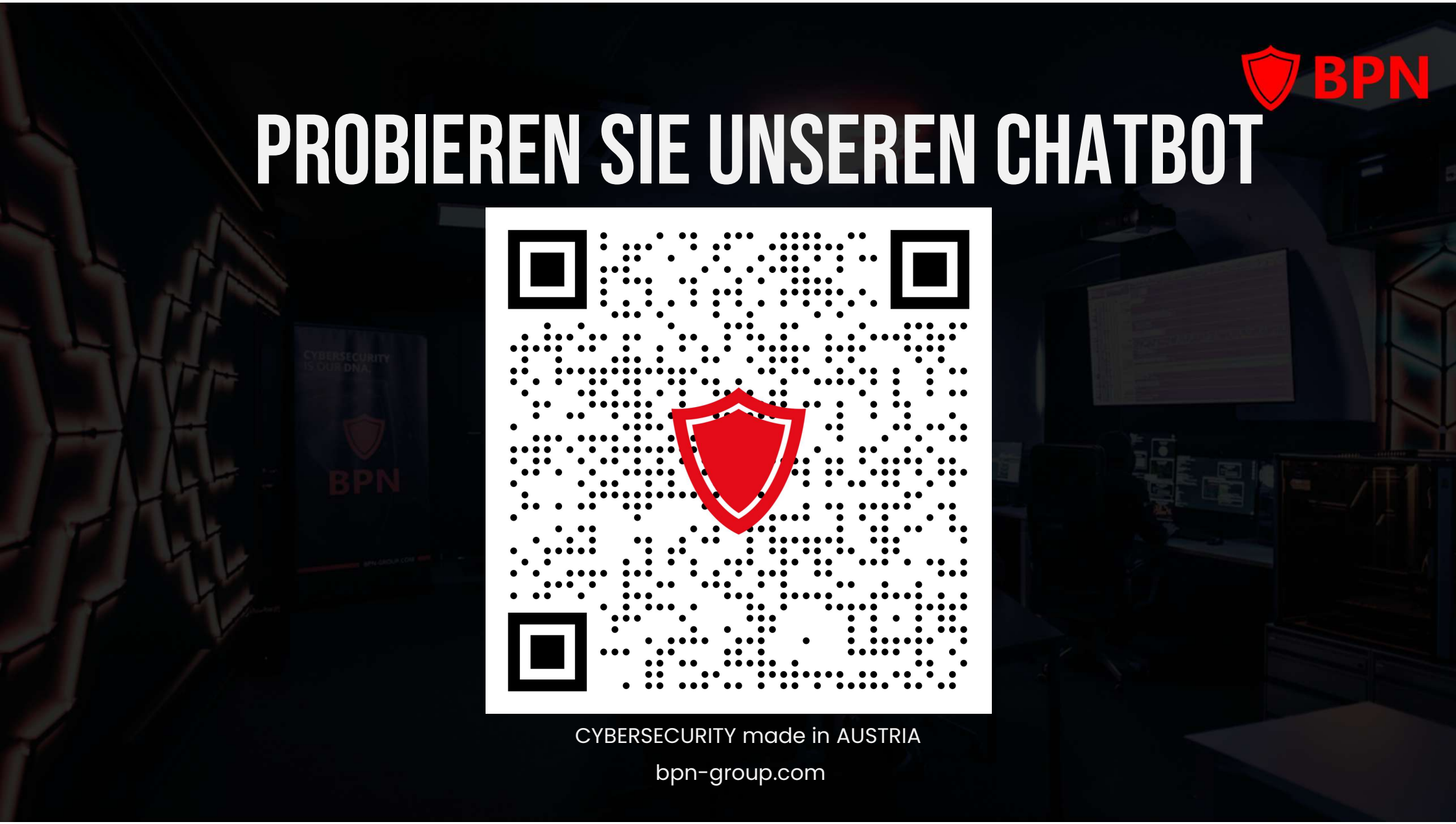
- Threat Hypothesis Generation & Validation
- Cross-Correlation of Security Events
- Attack Kill Chain Analysis
- Advanced Incident Discovery

Threat Intelligence

- Proactive Threat Discovery
- IOC Collection & Enrichment
- Custom Correlation Rule Engineering
- Threat Intelligence Service PDF

Reporting

- Operational Security Reporting
- Custom Report Engineering
- Regulatory & Compliance Reporting
- Digital Forensics Reporting


BPN
PROBIEREN SIE UNSEREN CHATBOT
CYBERSECURITY made in AUSTRIA
bpn-group.com