
Agentur
Cyberschutz
Agentur
Cyberschutz
GESAMTKONZEPTE GEGEN CYBERCRIME
ganzheitliche, umfassende IT- und Cybersicherheit
für alle Branchen und Unternehmensgrößen

cybercrime
Komplettschutz

Oliver HIETZ

Keynote-Speaker - Kriminal-Analyst - Gründer, Eigentümer und GF von 2 Cybersicherheitsunternehmen

- Geb. 1978 / whft. Baden bei Wien
- Leidenschaften Fußball / Geschichte
- 1999 nach Matura und BH – Eintritt in die Gendarmerie
- 1999-2024: Polizeidienst / vorwiegend operativer Kriminaldienst

- ab 2021: Gründung und Aufbau Agentur Cyberschutz / Cyber & Crime Versicherungsmakler GmbH
- Ende 2024: Beteiligungs- und Investitionsphase / Umstrukturierungen / schnell wachsend – hochspezialisiert

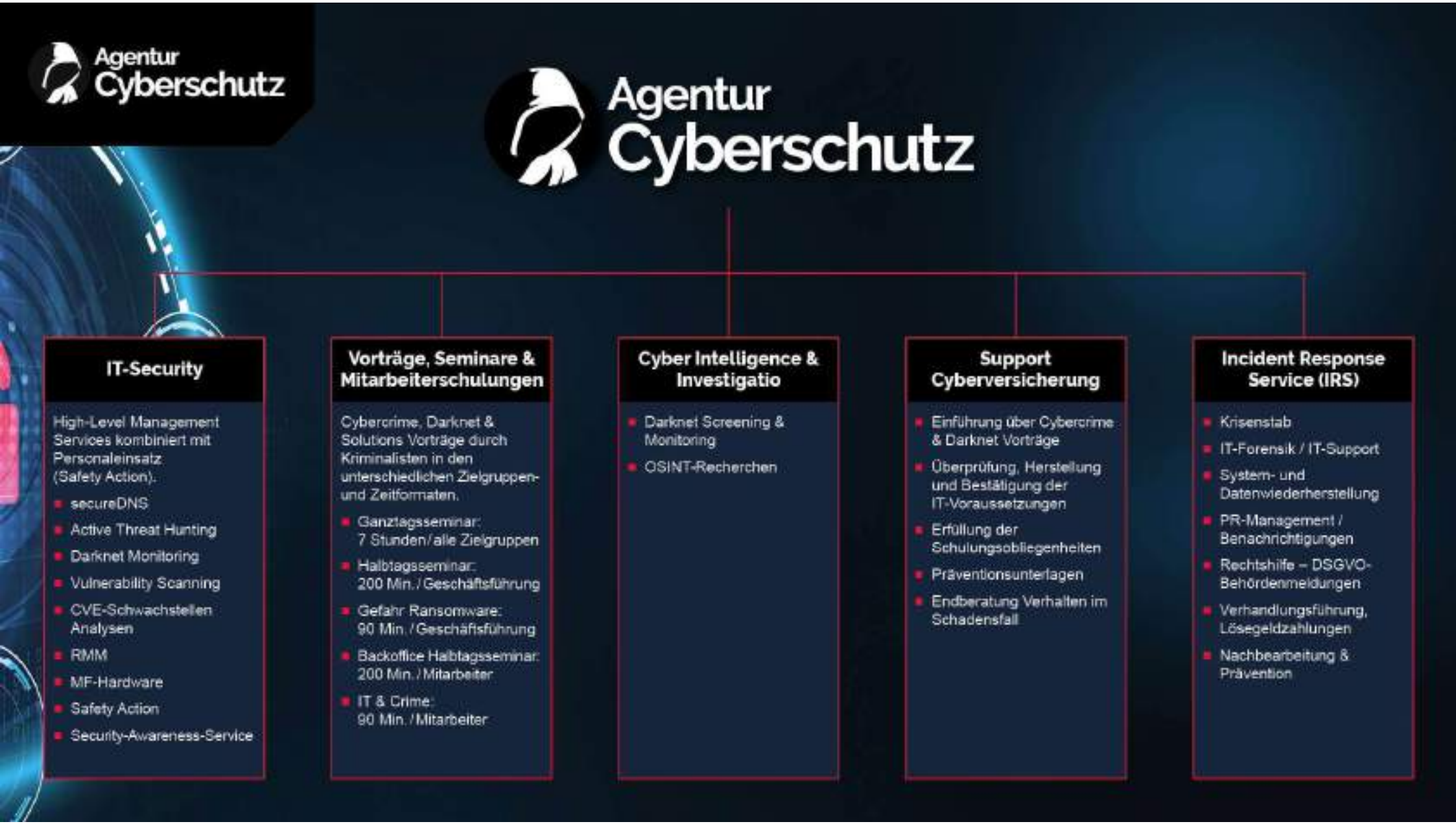
Agentur Cyberschutz

cyber & crime
Versicherungsmakler GmbH

cybercrime
Komplettschutz

cybercrime
Komplettschutz
INCIDENT RESPONSE SERVICE TEAM


cybercrime
Komplettschutz
Cybercrime Komplettschutz Netzwerk
Gesamtkonzepte für Cyber- und IT-Sicherheit
Agentur Cyberschutz
IT-Security
Vorträge – Schulungen – Awareness Training
Security-Awareness-Services
Cyber Intelligence & Investigations
Begleitung und Unterstützung im Cyberversicherungsantragsprozess
cyber & crime
Versicherungsmakler GmbH
Cyber & Crime Versicherungen
Versicherungsberatung & Vermittlung
Schadensfallbetreuung
cybercrime
Komplettschutz
SECUTEC
HORNET
SOPHOS
ATB Law
TEMS Security
Asspro Managerline
+ 50 weitere Partnerunternehmen
cybercrime
Komplettschutz
INCIDENT RESPONSE SERVICE TEAM
IT-Forensik
IT-Support
Daten- und Systemwiederherstellung
Krisenstab / Schadensfallkoordination
Rechtshilfe
Cyber Schutzschirm
Berichterstattung / Dokumentation
KONTAKT:
2500 Baden, Habsburgerstraße 40 / Betriebsstätte: 2514 Traiskirchen, Wienersdorferstraße 20-24/ Objekt 54
office@agentur-cyberschutz.at / Leistungs- und Angebotsanfragen: anfrage@agentur-cyberschutz.at
0676/7088510 – HIETZ Oliver – geschäftsführender Gesellschafter


Agentur Cyberschutz
Agentur Cyberschutz
IT-Security
High-Level Management Services kombiniert mit Personaleinsatz (Safety Action).
secureDNS
Active Threat Hunting
Darknet Monitoring
Vulnerability Scanning
CVE-Schwachstellen Analysen
RMM
MF-Hardware
Safety Action
Security-Awareness-Service
Vorträge, Seminare & Mitarbeiterschulungen
Cybercrime, Darknet & Solutions Vorträge durch Kriminalisten in den unterschiedlichen Zielgruppen- und Zeitformaten.
Ganztagsseminar: 7 Stunden / alle Zielgruppen
Halbtagsseminar: 200 Min. / Geschäftsführung
Gefahr Ransomware: 90 Min. / Geschäftsführung
Backoffice Halbtagsseminar: 200 Min. / Mitarbeiter
IT & Crime: 90 Min. / Mitarbeiter
Cyber Intelligence & Investigatio
Darknet Screening & Monitoring
OSINT-Recherchen
Support Cyberversicherung
Einführung über Cybercrime & Darknet Vorträge
Überprüfung, Herstellung und Bestätigung der IT-Voraussetzungen
Erfüllung der Schulungsobliegenheiten
Präventionsunterlagen
Endberatung Verhalten im Schadensfall
Incident Response Service (IRS)
Krisenstab
IT-Forensik / IT-Support
System- und Datenwiederherstellung
PR-Management / Benachrichtigungen
Rechtshilfe – DSGVO-Behördenmeldungen
Verhandlungsführung, Lösegeldzahlungen
Nachbearbeitung & Prävention


cybercrime
Komplettschutz
Cybercrime, Darknet & Solutions
Tagesseminar 7 Std. – verschiedene Zielgruppen- und Zeitformate
Gefahr Ransomware – Kurzabriss über die größte gegenwärtige Cybergefahr für Unternehmen
praxisbezogener, tagesaktueller Vortrag – Cybercrime aus Sicht der Kriminalistik
Vorstellung der Tätergruppen – Verhaltensweisen, Werkzeugen, Abläufen
hochsensible, teils schockierende Inhalte
DARKNET – Erklärung und Live Einstieg
einzigartige Quellenbasis: Darknet Analyse & Nachevaluierungen von Schadensfällen / keine öffentliche Quellen
IVM www.ivm.at
VERKEHRS BUERO
K&O KASTNER & ÖHLER
Bank Austria
UniCredit
UNIQA
Aktuell
Koch
ASFINAG
ERSTE Bank
helvetia
atlas
Lebenswert WOHNEN
WIRTSCHAFTSBUND KÄRNTEN
WKO
ABTA
ÖWD SECURITY & SERVICES
oesterreichs energie
FRIEDEN
alpenland
ACP

Agentur Cyberschutz

Unser einzigartiger Wissensvorsprung für Ihre Cybersicherheit
Wir als Quelle selbst

DARKNET-Analyse & Schadensfall Nachevaluierungen

Ausdruck unseres einzigartigen Kriminalistik Zugangs – Präventionsmaßnahmen nach Täterverhalten und Angriffsvektoren – sind unsere tagtäglichen umfassenden Täter / Opfer Recherchen im Darknet und Nachevaluierungen von Schadensfällen.

Wir vertrauen demnach keinerlei öffentlichen, frei zugängigen Quellen von Medien, Behörden und Interessensvertretungen und können aufgrund unserer tagesaktuellen Datenbasis belegen, dass diese zumeist irreführend und nicht praxisnah sind.

DARKNET-Analyse

- aktive Tätergruppen / Opfer
- weltweite Opferstatistik seit 2022
- DACH-Region Detailreports
- Täterprofiling – Spezifikationen
- Statistiken / Reports

Agentur Cyberschutz

IT-Risikoanalysen

- Überprüfung, Herstellung und Bestätigung von Cyberversicherungsvoraussetzungen
- Feststellung von Schwachstellen und Problemfeldern
- Empfehlungen

Agentur Cyberschutz

Incident Reponse Service Reports

- Auswertung von IT-Forensik Reports
- Angriffsverlauf / Angriffsvektoren
- Verhandlungsverlauf
- Gesamtschadenszusammenstellung
- Nach- und Hochrüsten

cybercrime Secutec AXA MARKEL

Agentur Cyberschutz

cybercrime

Attacken auf IT

Cyberattacken

- zielgerichtete Angriffe
- Unternehmen – kritische IF - Behörden
- Netzwerksicherheitsverletzungen
- Existenzbedrohende Schäden

Werkzeuge / Angriffsvektoren

- IT-Schwachstellen
- Keylogger
- DARKNET Märkte
- Admin Accounts

Ransomware / Extortion
Ransomware / Double Extortion
DDOs
Gesamtschaden: BU – IT - Daten

RAGNAR_LOCKER

DARKNET

- Kommunikations- und Handelsplattform
- Daten- und Schwachstellenverkauf
- Cybercrime as a Service - Auftragsattacken

Social Engineering

CYBER-Betrug- und Erpressung

- Schwachstelle Mensch
- Privatpersonen / Unternehmen
- Breitgefächert / zielgerichtet

Werkzeuge / Angriffsvektoren

- Mail / Tel
- Social Engineering
- Fakemailer / Call – ID Spoofing / Fakeshops

Betrugs- und Erpressungsdelikte (12 MP):

- CEO Fraud / Fake Prs.
- Rechnungsbetrug
- Lieferumleitung
- Phishing – 148a

Prävention nach Angriffsvektor / Ziele: EPU – KMU – Konzern / extern – intern – Darknet / Gesamtkonzept

Unternehmen	Zielgruppen	Privatpersonen - Buchhaltung
Netzwerksicherheitsverletzungen	Angriffsvektor	Social Engineering – Mail – Telefon
Ransomware / DDos	Angriffe	Cyberbetrugs- Erpressungsdelikte / mindergefährliche Cyberattacken
eigene Darknet-Webseiten	Darknet	Darknet-Märkte / Foren
existenzbedrohende Schäden	Gesamtschäden	Bagatellbereich – empfindliche Schäden
Krypto-Währungen	Vermögensabfluss	sämtliche Zahlungsmodalitäten
hochspezialisierte Schadsoftware	Werkzeuge	psycholog. Tricks – einfache IT-Tools
in Verantwortung der GF	Lösegeldzahlungen	niemals

cybercrime
Komplettschutz

Praxisbeispiel

■ letztes Lockbit 2.0 Opfer – EPU Bestatter

Cryptolocker – 50.000 Euro Lösegeld – Austausch und Neuaufsetzung IT
Back-Up auf USB 2.0 Stick – **Folgen? Schaden?**

Breitgefächerter / zielgerichteter Angriff

Breitgefächerter Angriff

- keine Recherchetätigkeiten
- „Schuss ins Blaue“
- Täter nützt günstige Umstände
- SpamMing, Smishing – 6% Erfolgschance
- Massenerpressungsmails
- Gewinnversprechen
- „günstige Angebote“
- **Risiko gering**

Praxisbeispiel SEXTORTION / Vergleich §129 StGB
Gelegenheitsattacke (analog / digital)
Handlungsempfehlungen

Zielgerichteter Angriff

- gezielte Attacke auf ausgesuchte Person oder Unternehmen
- Recherchetätigkeiten des Täters
- Cybercrime as a service
- psychologische Tricks und raffinierte Software kommen zum Einsatz
- **Risiko sehr hoch - gewiss**
- Entschlossenheit / hohe Intensität / Beharrlichkeit

Ransomware Gangs / „Ragnar Locker“

- IT-Experten / IT-Spezialisten / klass. Hacker
- Einzeltäter – Gruppen - Firmennetzwerke
- Programmieren hochkomplexe Schadsoftware
- zielgerichtete Attacken - CaaS
- Ransomware / DDoS / Datendiebstahl
- **Zielgruppen:** Unternehmen aller Größen und Branchen – Gebietskörperschaften – Behörden – kritische Infrastruktur / Privatpersonen?
- **Länder: Zentraleuropa / USA – insbesondere DACH**

RAGNAR_LOCKER

Werkzeuge der Täter

Ransomwaregang

- Cryptolocker – Verschlüsselungssoftware
- Double / Triple EXTORTION
- Trojaner / Bot Netzwerke
- sonstige Schadsoftware

- DARKNET: Websites – Cybercrime as a service (bietet seine Dienste an)

- Vermögensabschöpfung:
  Kryptowährungen

cybercrime
Komplettschutz

Ransomware Gangs

- seit 01.01.2022 – 75 Gruppierungen
- derzeit 60 aktiv
- agieren länder- und branchenübergreifend
- identes Konzept – geringfügige Unterscheidungen

Spezifikationen – Lösegeldbemessung – Affiliate System – Vorverhandlungen

cybercrime
Rompilattacchi

Ransomware Gangs

15

cybercrime
Komplettschutz

Zielgruppen

Bildungs-einrichtungen
(Schulen, UNIs, Fortbildungen, etc.)

Dienstleister
(Industrie, Klein- und Mittelbetriebe, Einzelunternehmer.)

Behörden
(Gemeinde, Magistrate, Länder, Verwaltungsbehörden)

Versicherungen

Ärzte

Banken

Notare, Anwälte

Handel

Onlinehandel

IT-Dienstleister/ Mailhoster

Soziale Netzwerke
(Facebook, Instagram)

Hotellerie, Tourismus, Fluglinien

RANSOMWARE ATTACK

Zielgruppen RANSOMWARE Gangs

cybercrime
Komplettschutz

Ablauf von RANSOMWARE Attacken
4 PHASEN

Phase 1:
Vorbereitungshandlungen / Kompromittierung des IT-Systems

Phase 2:
EXTORTION – IT-Verschlüsselung

Phase 3:
Vorverhandlungen

Phase 4:
DOUBLE EXTORTION – Opfereintrag

cybercrime
Komplettschutz

Gesamtschaden – kein Datendiebstahl

- **branchenspezifisch / BU – IT – Daten** **1 Dienstleister**
- **Betriebsunterbrechung – Ertragsausfall – Personalkosten – Regress**
- **IT-Forensik – Entschlüsselung - Systemwiederherstellung - Datarecovery**
- **Hardwareschäden – Leihgerätschaften – Neuanschaffungen**

cybercrime
Komplettschutz

Gesamtschaden - Datenverlust

- **branchenspezifisch / BU – IT – Daten** — **6-7 Dienstleister**
- Betriebsunterbrechung – Ertragsausfall – Personalkosten – Regress
- IT-Forensik – Entschlüsselung - Systemwiederherstellung - Datarecovery
- Hardwareschäden – Leihgerätschaften – Neuanschaffungen

- Verhandlungsführung – Zahlungsabwicklung - Lösegeld
- PR-Maßnahmen – Kommunikation – Benachrichtigungen
- DSGVO – Behördenstrafe – Zivilrechtssammelklagen – Prozesse
- Vertragsstrafen – Regressforderungen
- Anwalts- Sachverständigen- Gerichtskosten
- Reputations- und Imageschaden / Vertragskündigungen

cybercrime
Komplettschutz

cybercrime
Komplettschutz

INCIDENT RESPONSE SERVICE TEAM

Agentur Cyberschutz

ATB. LAW
AZEM | TAUDES | BLÖCH

Secutec
Cybersecurity Intelligence

PR:AG

tems security

tems
See the world with Emil

cybercrime Komplettschutz
INCIDENT RESPONSE SERVICE TEAM

Timeline Cybercrime Komplettschutz
INCIDENT RESPONSE SERVICE

PHASE 1
Die kritischen 48 Stunden

- Krisenstab – INTRO – Täterinfos – Ablauf – Vollmachten
- IT-FORENSIK
- IT-SUPPORT
- Erstmeldungen (DSGVO – Behörden – Polizei)
- Schutzschirm
- Rechtshilfe

Ziele

- Erst-Report
- Erstmeldungen
- Schutzschirm

PHASE 2
EXIT - Systemwiederherstellung

- Erst-Report (Datenabfluss, Angriffsvektor, Back-up)
- Verhandlungsführung
- Sonderfall Lösegeld
- Sanktions- und Embargo-Checks
- Kryptobereitstellung / Zahlung
- System- und Datenwiederherstellung
- Leihgerätschaften / Neuanschaffungen
- DSGVO Obliegenheiten
- PR- Management
- Benachrichtigungen

Ziele

- Exit-Strategie
- Schadenseindämmung
- Systemwiederherstellung

PHASE 3
Nachbearbeitung

- Rechtshilfe – Prozessvorbereitung – Prozessführung
- Gesamtschadenszusammenstellung
- Aufrüsten – Nachevaluierung
- Endreporting

Ziele

- Refundierung des Gesamtschadens
- Eindämmung Reputations- und Imageschäden
- Absicherung / Aufrüstung

Agentur Cyberschutz
tems security
Secutec
ATB
AZEM | TAUDES | BLÖCH
tems
See the world with Emil

Wie komme ich ins Darknet?

- Einstieg über Tor-Browser
- Darknet unsichtbar für Standardbrowser
- Anonymität für Sender und Empfänger
- unkonventionell – keine Clear Adressen
- nicht illegal / nicht strafbar
- kein großes Netz – 35.000 Zielseiten
- Underground Economy – Silk Road

http[:]//3kp6j22pz3zkv76yutctosa6djpj4yib2icvdqxuc daxxedumhqicpad[.]onion (ARVIN CLUB)


Agentur
Cyberschutz
DARKNET MÄRKTE
Drogen
Waffen
Kinderporno
Fälschungen
Identitätsdokumente
Hacking
Kreditkartendaten
Auftragsmorde

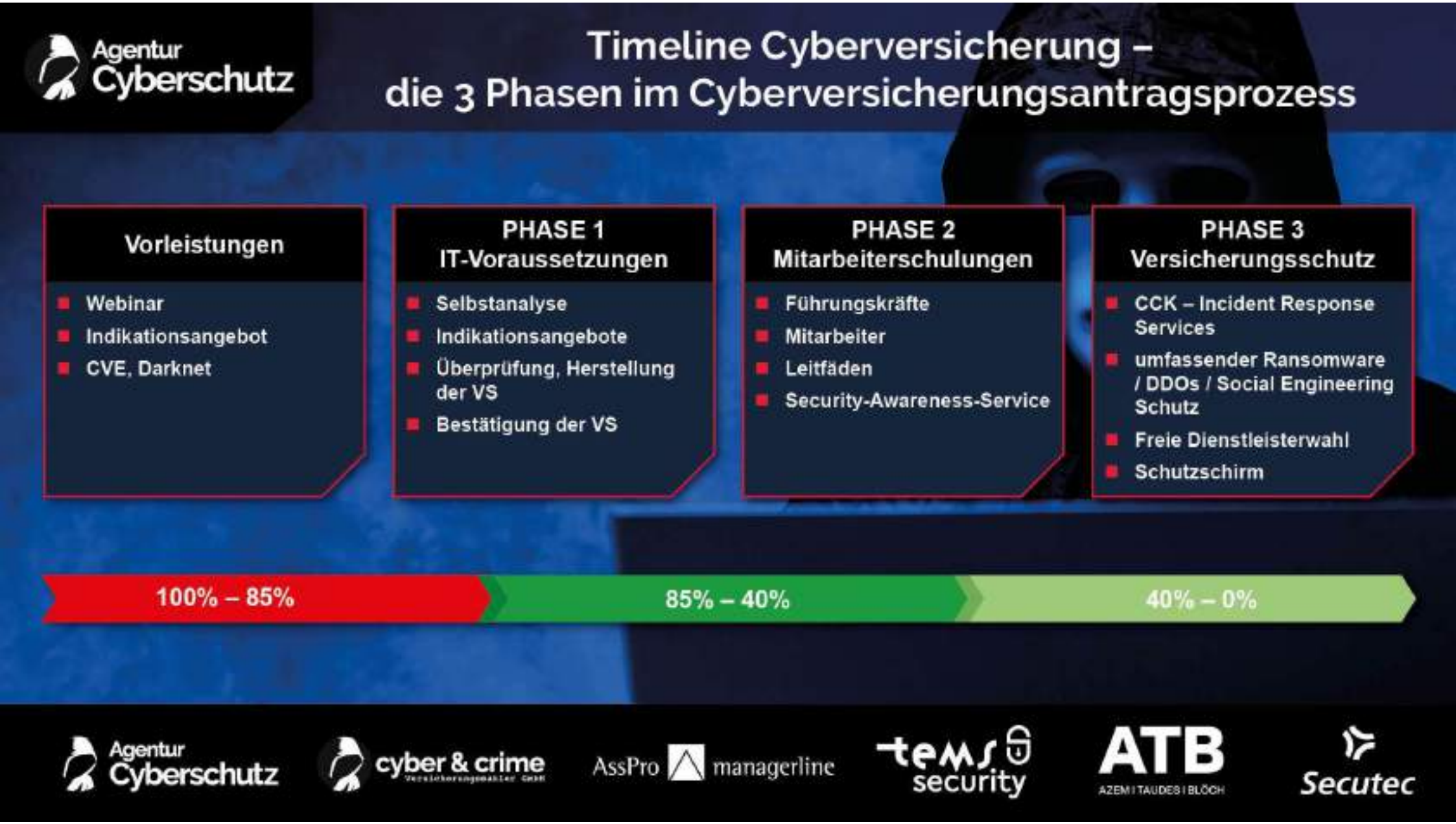

cybercrime
Komplettschutz
Gesamtkonzepte Cyber- und IT-Sicherheit
Vulnerability Scan
Active Threat Hunting
Darknet Monitoring
Secure DNS
IT Security
CVE, RMM, MFA, Safety Action, EDR
Awareness Trainings
Cybercrime, Darknet & Solutions
IT & Crime - Sicher im Netz - Info Portal
Security Awareness
Back-Up
Virenschutz
Firewall
Cyber & Crime Versicherung
Incident Response Service
Ransomware
DDoS
Betrug
Erpressung
Umfassend – ohne Lücken und Ausnahmen
Gegen alle Angriffsvektoren
Durchgehend – 24/7/52
Automatisiert + Personaleinsatz
Intern / extern
Vorbereitung Schadensfall
breitgefächert vs. zielgerichtet
Unternehmen vs. Privatperson
Angriffsvektoren:
VPN
CVE
Infizierte Keylogger
Daten und Passwort Phishing
Bankdaten Phishing
Credential Stuffing
Mail

Agentur Cyberschutz

Angriffsvektoren - Gegenmaßnahmen

Vorbereitungshandlungen – Angriffsvektoren – Präventionsmaßnahmen

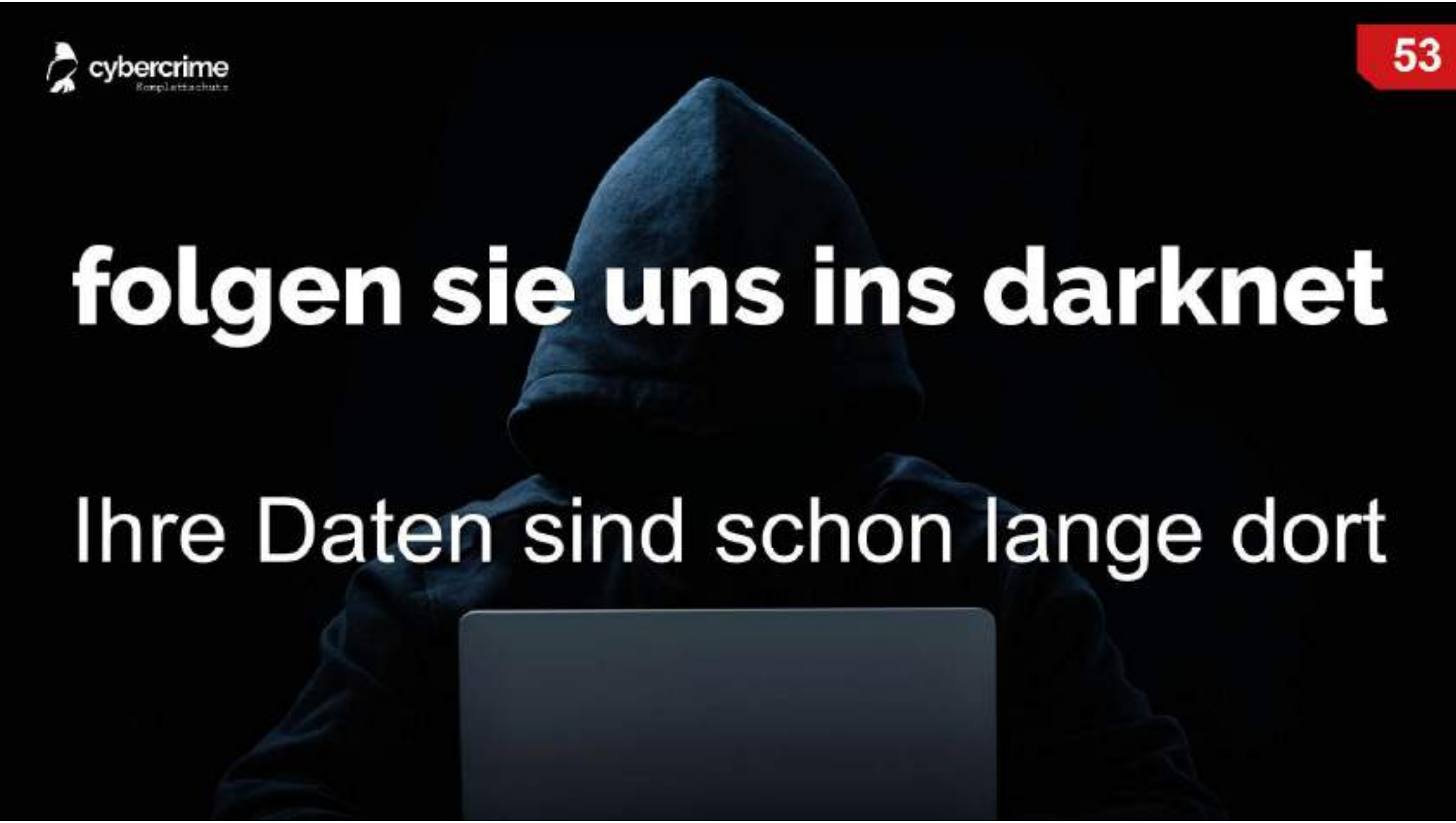
Vorbereitungshandlung	Angriff / Anschlussdelikt	Gegenmaßnahme
CVE-Schwachstellen	Cyberattacke (Ransomware / DDOs)	CVE- SCAN + SAFETY Action - Schließen der aufgezeigten Lücken
Keylogger	Account Hacking Ransomware Cyberbetrug	DARKNET Monitoring + SAFETY Action MF-Hardware
Phishing Mails	Schadsoftware Account-Hacking	Security-Awareness-Service
Darknet Datenleck	Cyberbetrugsdelikte	Vorträge – Schulungen durch Kriminalisten
Passwort Phishing / Darknet Datenleck	Accounthacking Cyberbetrug 148a - Überweisungen	MF-Hardware


Agentur Cyberschutz
Timeline Cyberversicherung – die 3 Phasen im Cyberversicherungsantragsprozess
Vorleistungen
Webinar
Indikationsangebot
CVE, Darknet
PHASE 1
IT-Voraussetzungen
Selbstanalyse
Indikationsangebote
Überprüfung, Herstellung der VS
Bestätigung der VS
PHASE 2
Mitarbeiterschulungen
Führungskräfte
Mitarbeiter
Leitfäden
Security-Awareness-Service
PHASE 3
Versicherungsschutz
CCK – Incident Response Services
umfassender Ransomware / DDOs / Social Engineering Schutz
Freie Dienstleisterwahl
Schutzschirm
100% – 85%
85% – 40%
40% – 0%
Agentur Cyberschutz
cyber & crime
AssPro managerline
tems security
ATB
AZEM | TAUDES | BLÖCH
Secutec

Agentur Cyberschutz

Unser Angebot

- **Cyber-Risk Erstreport:** einmalige, punktuelle, externe Sicherheitsüberprüfung
  - CVE-Schwachstellenscan
  - Darknet Domain Scan – infizierte interne und externe User Keylogger / Passwort-Leaks
  - Darknet Datenlecks
  - Rabattcode: Ort und Datum
- **Webinare**
  - Cybercrime & Solutions – Unternehmensberatung
  - How the Darknet Works - SECUTEC



folgen sie uns ins darknet

Ihre Daten sind schon lange dort