TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

"T.I.S.P. Community Meeting 2020"

Berlin, 03.-04.11.2020

Threat Intelligence / Vulnerability Management

Dr. Gunther Schlöffel, pen.sec AG

Threat Intelligence & Vulnerability Management

Motivation

Motivation

Cyber Threat Intelligence (CTI)

Vulnerability Management (VM)

Was verbirgt sich hinter den Begriffen?

Wie können damit verbundene Techniken (m)einem Unternehmen / (m)einer Organisation nutzen?

pen.sec
Protecting Your Assets

Vorstellung

Dr. Gunther Schlöffel

- Bundeswehr (SaZ02 Reserveoffizier)
- Studium der Mathematik und Informatik
- Promotion
- Wehrwissenschaftliche Forschung
- Vorstand pen.sec AG, Penetrationstester & Threat Analyst
- Auditor KRITIS, ISO/IEC 27001, ISO 22301, RESISCAN

pen.sec
Protecting Your Assets

Vorstellung pen.sec AG

PENETRATIONSTEST

Sicherheitslücken finden und beheben

RED TEAMING

Prozesse überprüfen und trainieren

SECURITY RATING

Sicherheit messen und darstellen

AWARENESS

Sicherheit durch Kompetenz - Kompetenz durch Training

Member of FOX Group

- (zertifiziertes) Informationssicherheitsmanagement nach ISO/IEC 27001:2013
- (zertifiziertes) Qualitätsmanagement nach ISO 9001:2015

pen.sec
Protecting Your Assets

Inhalt des Vortrags

Threat Intelligence & Vulnerability Management

I Motivation

II Begriffe und Abgrenzung

III Methoden, Produkte & Maßnahmen

IV Einsatz in und Mehrwert für Organisationen und Unternehmen

pen.sec
Protecting Your Assets

Threat Intelligence & Vulnerability Management

I Motivation

II **Begriffe und Abgrenzung**

III Methoden, Produkte & Maßnahmen

IV Einsatz in und Mehrwert für Organisationen und Unternehmen

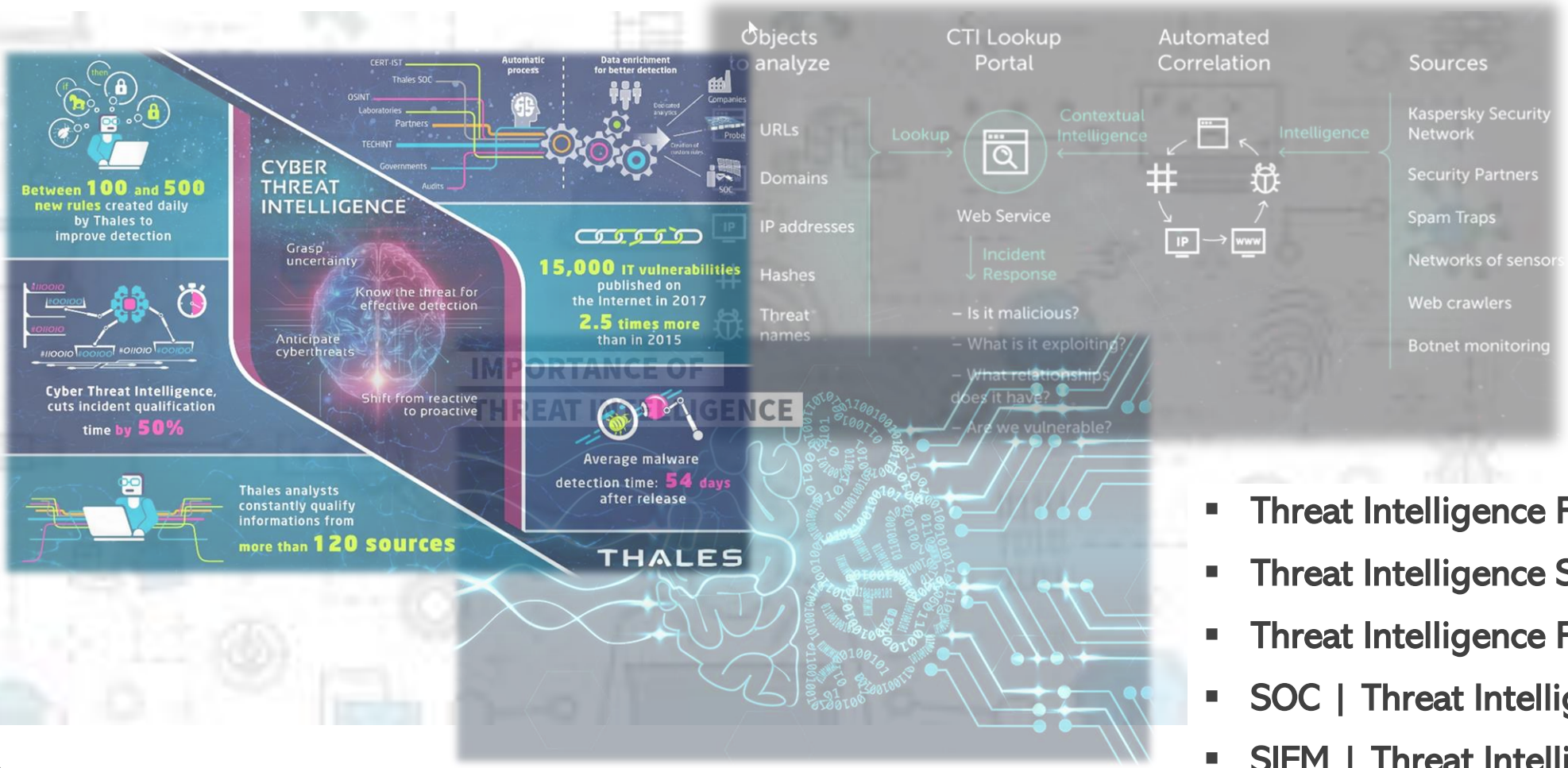
Threat Intelligence & Vulnerability Management

Begriffe und Abgrenzung

Threat Intelligence durch offene Informationen zur Gefährdungslage ?

pen.sec
Protecting Your Assets

Threat Intelligence durch kommerzielle Produkte ?



- Threat Intelligence Feed
- Threat Intelligence Service
- Threat Intelligence Platform
- SOC | Threat Intelligence
- SIEM | Threat Intelligence

pen.sec
Protecting Your Assets

Cyber Threat Intelligence – Lösungen & Produkte

https://www.kaspersky.de/enterprise-security/threat-intelligence

pen.sec
Protecting Your Assets

Definition – Cyber Threat Intelligence (CTI)

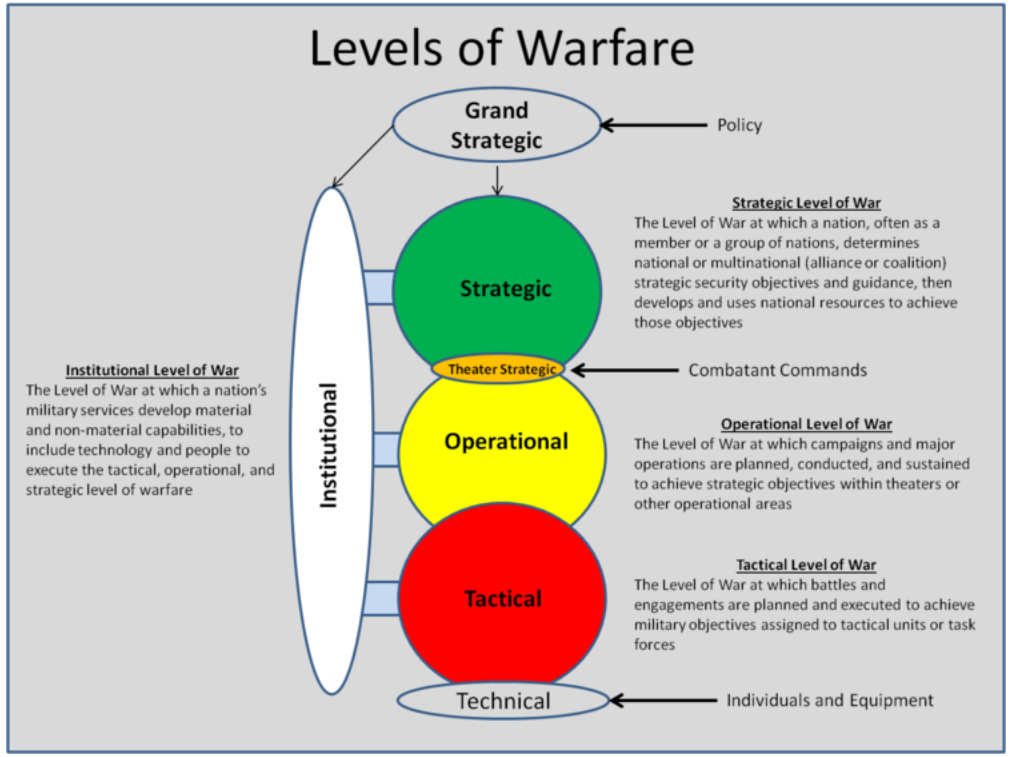
Cyber Threat Intelligence (CTI)

Information about threats and threat actors that provides sufficient understanding for mitigating a harmful event.

tactical	operational	strategic
technical intelligence such as using threat indicators to proactively hunt for and defend against adversaries	intelligence focused on the motivation's intent and capabilities (including Tactics, Techniques and Procedures, TTPs) of adversaries	intelligence about the risks and implications associated with threats used to inform business decisions and direct cyber security investment

Anmerkung zur Benennung der Handlungsebenen (Level)

Die Ebenen (Level), in welche Verfahren der **Threat-Intelligence** in der Literatur üblicherweise unterteilt werden, entstammen dem **US-militärischen Sprachgebrauch**:



https://thestrategybridge.org/the-bridge/2016/5/5/the-institutional-level-of-war

Im Kontext des **Organisationsmanagements** (auch des IS- sowie des BCM-Managements) werden Handlungsebenen ähnlich bezeichnet, folgen aber einer anderen hierarchischen Ordnung:

Überblick über Handlungsebenen/-dimensionen / Checkliste für Management			
Ebene	**Zeitbezug**[3]	**Wirkungsbereich überwiegend**	**verantwortlich**
strategisch	langfristig (>3 Jahre[3])	Produktbereich(e) [1] Abteilung(en), gesamtes Unternehmen Mitarbeitergruppen [2]	**oberste Leitung** (Top Management) (Präsident/ Vorstand)
taktisch	mittelfristig (1 bis 3 Jahre[3])	Produktgruppe(n) [1] Basiseinheit(en), übergeordnete Einheit (Abteilung) Mitarbeitergruppen [2]	**mittlere Leitung** (Middle Management) (Abteilungs-/ Referatsleiter)
operativ	kurzfristig (<1 Jahr[3])	Leistung, Produkt [1] Stelle, Basiseinheit (Referat) einzelne Mitarbeiter [2]	**untere Leitung / Basis** (Lower Management) (Ausführungsebene / Sachgebiets-/ Referatsleiter)

https://olev.de/o/operativ_usw.htm,
so auch ISO 44001 sowie ISO 22301

!!! ACHTUNG !!!

Anmerkung zur Benennung der Handlungsebenen (Level)

- **militärische Nomenklatur** für den Prozess der Aufklärung durch Informationsgewinnung -

tactical	operational	strategic
technical intelligence such as using threat indicators to proactively hunt for and defend against adversaries	intelligence focused on the motivation's intent and capabilities (including TTPs) of adversaries	intelligence about the risks and implications associated with threats used to inform business decisions and direct cyber security investment
operativ	**taktisch**	**strategisch**

- **Management-Handlungsebenen** in einer Organisation bzw. in einem Unternehmen -

pen.sec
Protecting Your Assets

Definition – Vulnerability Management (VM)

Vulnerability

In the contexts of information technology and cybersecurity, a vulnerability is a behaviour or set of conditions **present in** a **system, product, component, or service** that **violates** an implicit or explicit **security policy**. A vulnerability can be thought of as a weakness or exposure that allows a security impact or consequence. Attackers exploit vulnerabilities to compromise confidentiality, integrity, availability, operation, or some other security property.

ISO/IEC 29147:2018

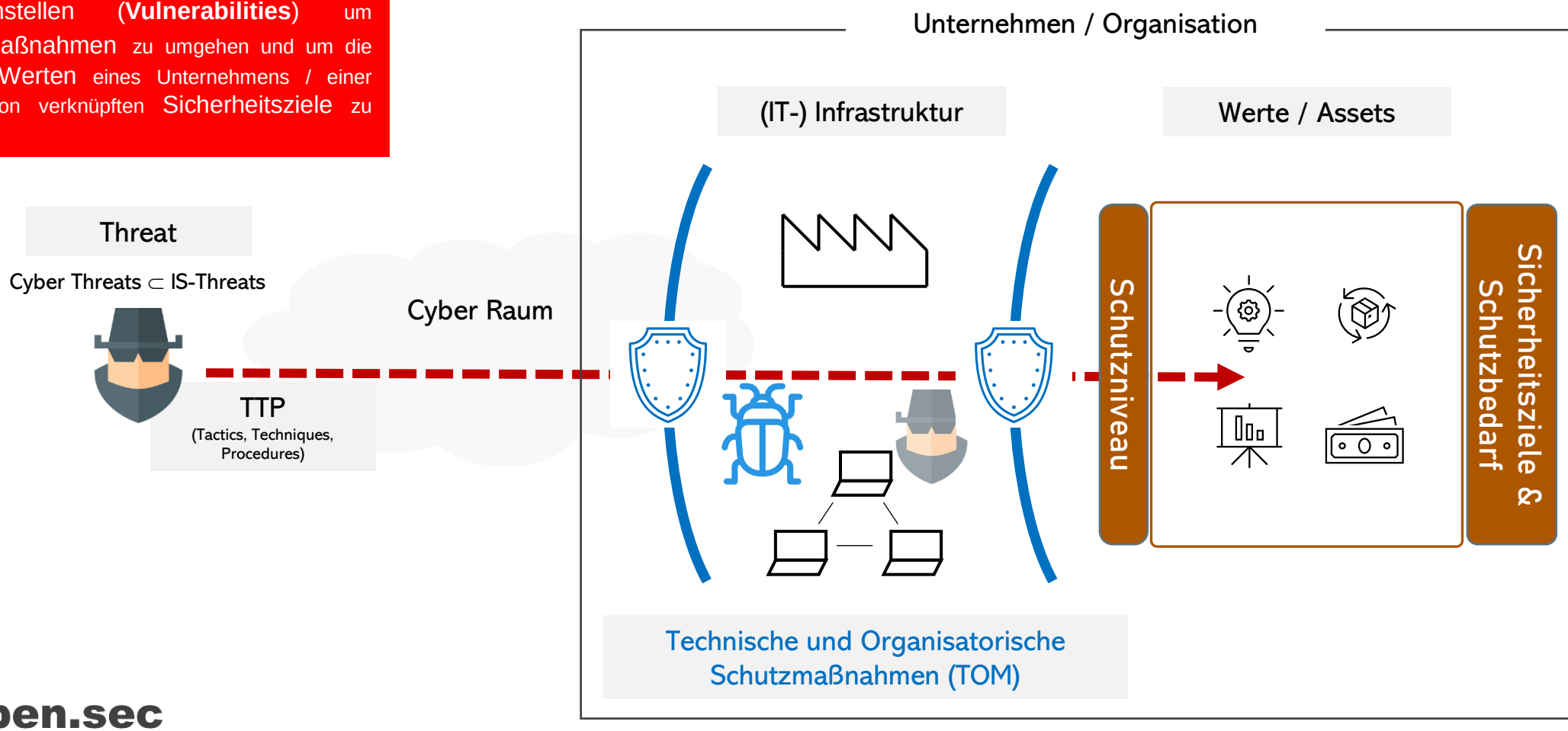
Vulnerability Management (VM)

Vulnerability management is the **process** of identifying, categorizing, prioritizing, and resolving vulnerabilities.

im Kontext der Informationssicherheit – Cyber Threats & Vulnerabilities

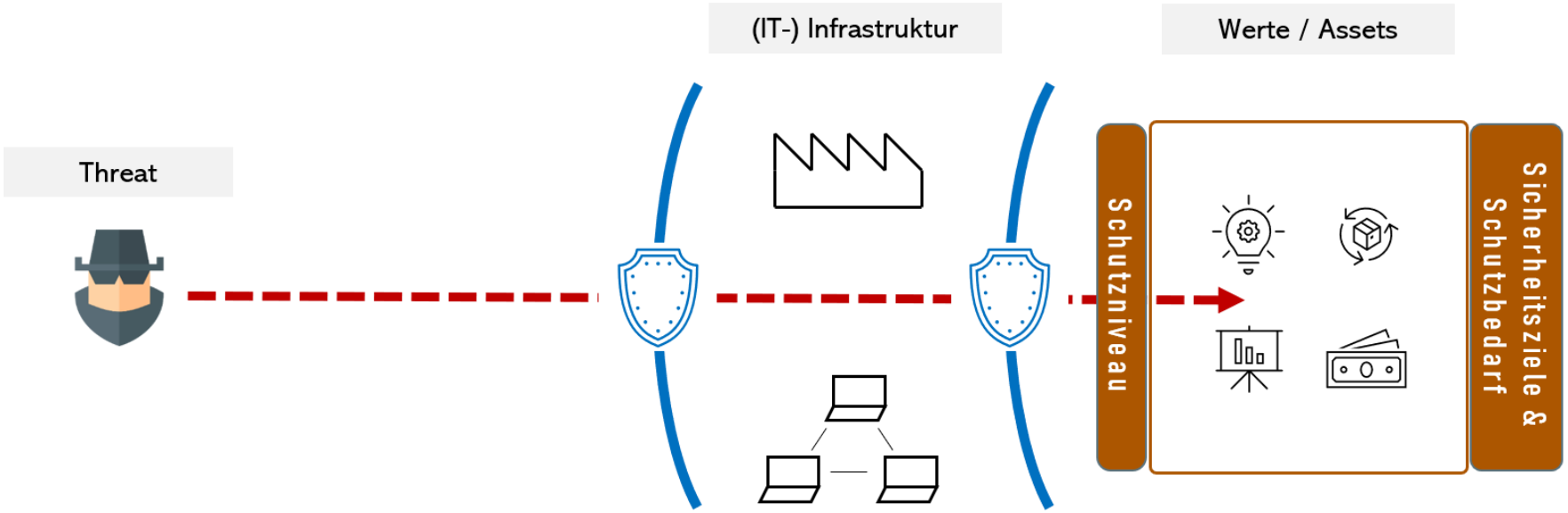
Eine Bedrohung (**Threat**) nutzt Schwachstellen (**Vulnerabilities**) um Schutzmaßnahmen zu umgehen und um die mit den Werten eines Unternehmens / einer Organisation verknüpften Sicherheitsziele zu brechen.

Der Verantwortliche der Organisation plant, etabliert und überprüft Technische und Organisatorische Schutzmaßnahmen (TOM), um die Werte der Organisation durch Sicherstellung eines allgemein anerkannten oder spezifisch festgelegten Schutzniveaus vor Bedrohungen zu schützen.



pen.sec
Protecting Your Assets

im Kontext der Informationssicherheit – Cyber Threat Intelligence

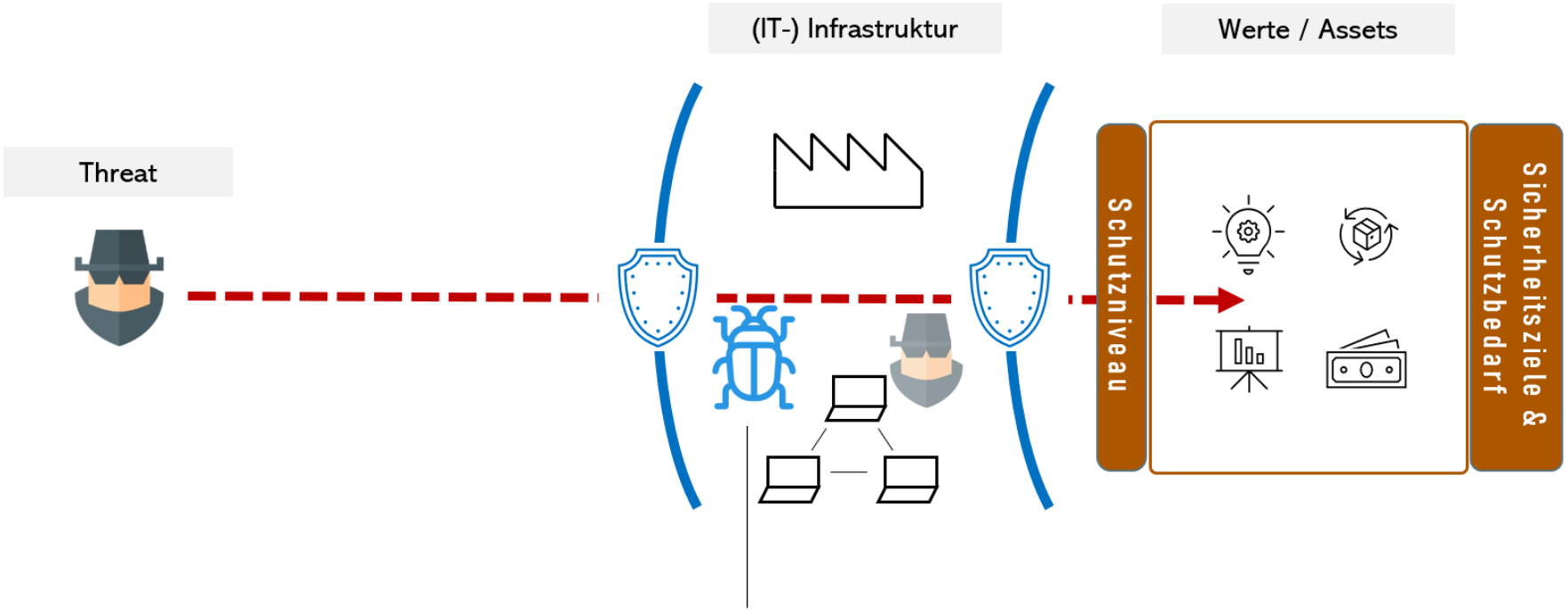


Cyber Threat Intelligence plant, sammelt, analysiert, verteilt und überprüft Daten, Informationen und Wissen zu und über relevante Bedrohungen sowie zu ihrem Vorgehen (Tactics, Techniques and Procedures, TTPs), (…)

(…) um Schutzmaßnahmen zu identifizieren und umsetzen oder anzupassen, welche das mit einer Bedrohung verbundene Risiko für die Werte einer Organisation reduzieren.

pen.sec
Protecting Your Assets

im Kontext der Informationssicherheit – Vulnerability Management



Durch ein geeignetes **Schwachstellenmanagement (Vulnerability Management)** werden Informationen über technische Schwachstellen verwendeter Informationssysteme rechtzeitig eingeholt, um die Gefährdung der Organisation durch derartige Schwachstellen zu bewerten und angemessene Maßnahmen zu ergreifen, um das dazugehörige Risiko zu behandeln.

pen.sec
Protecting Your Assets

Threat Intelligence & Vulnerability Management

I Motivation

II Begriffe und Abgrenzung

III Methoden, Produkte & Maßnahmen

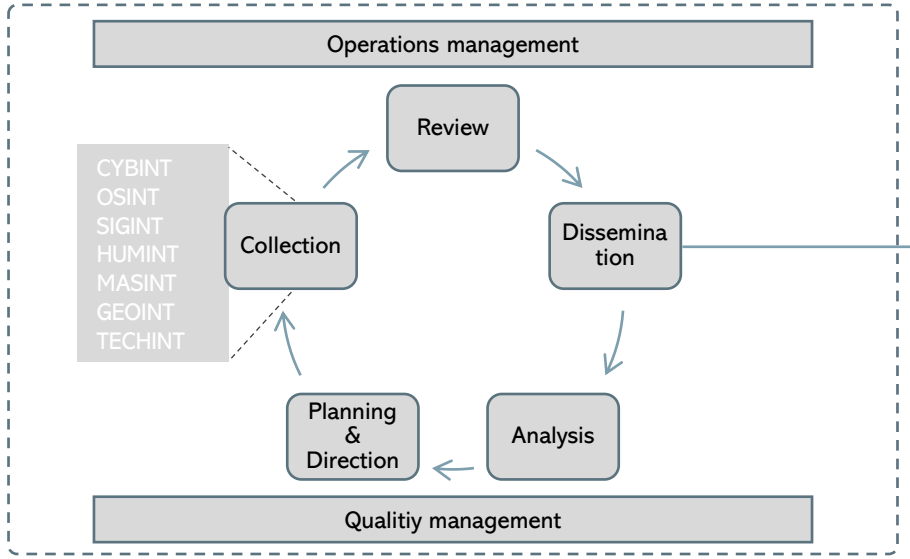
IV Einsatz in und Mehrwert für Organisationen und Unternehmen

Threat Intelligence & Vulnerability Management

Methoden, Produkte & Maßnahmen

Cyber Threat Intelligence – Lifecycle

Threat Intelligence Lifecycle:

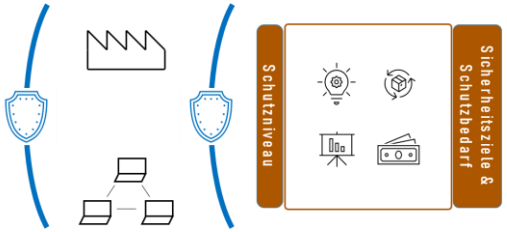


aufwandsintensiv –

in der Regel von **Security Providern** durchgeführt, die ihre Ergebnisse in Form von **Produkten** an Abnehmer wie Unternehmen / Organisationen verkaufen:

- simple alerts
- detailed reports
- machine-readable data feeds
- custom-designed output
- Application Programming Interfaces (API)
- secure online portals

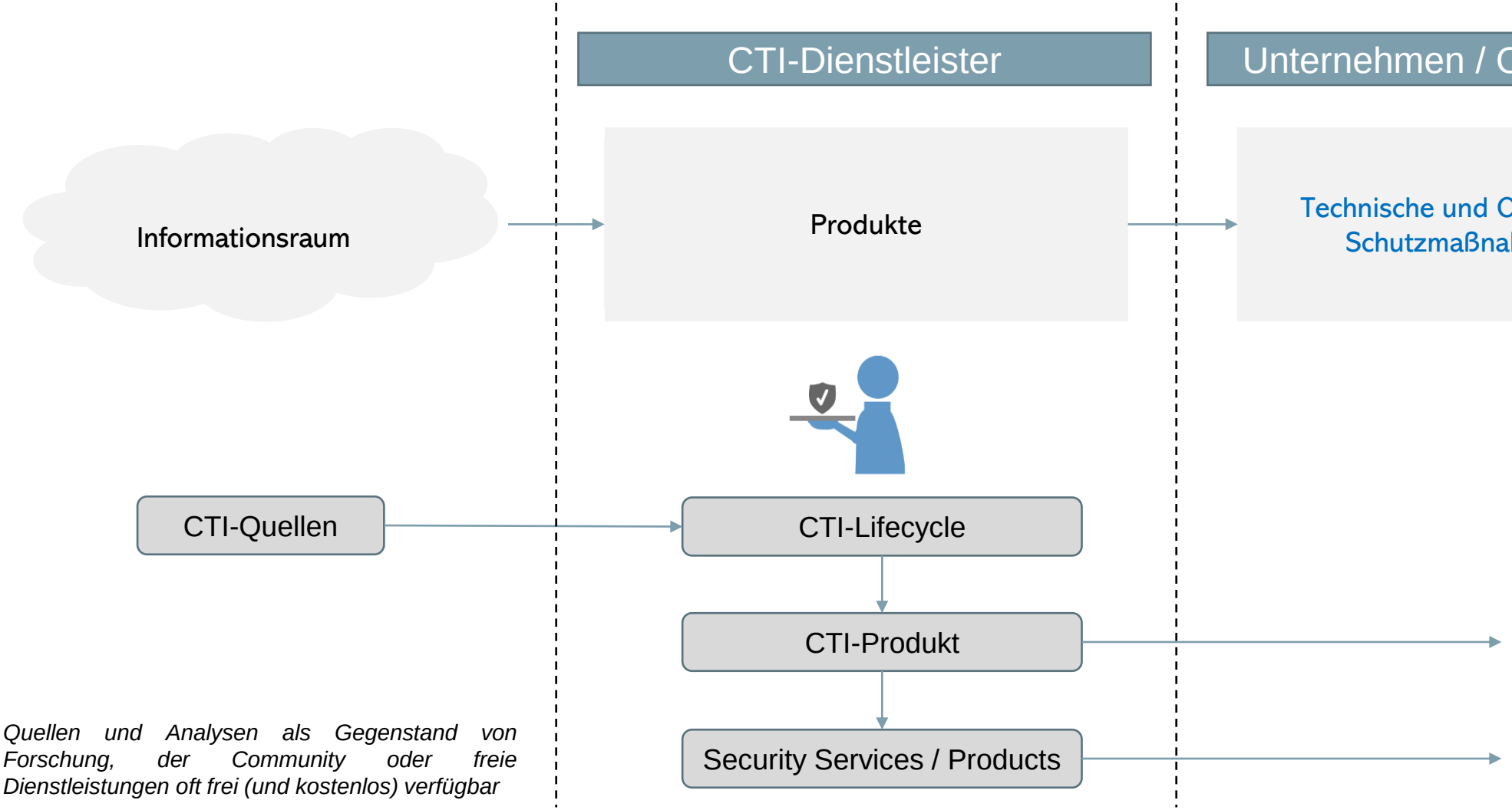
Technische und Organisatorische Schutzmaßnahmen (TOM)



Unternehmen / Organisation

pen.sec
Protecting Your Assets

Cyber Threat Intelligence – Dienstleister & Wertschöpfung



Quellen und Analysen als Gegenstand von Forschung, der Community oder freie Dienstleistungen oft frei (und kostenlos) verfügbar

pen.sec
Protecting Your Assets

Cyber Threat Intelligence – Methoden

Open source collection

- BitTorrent monitoring
- Code-sharing-site monitoring
- Dark web monitoring
- Deep web monitoring
- Open source intelligence feeds
- Paste site monitoring
- Public IRC monitoring
- Social media monitoring
- Surface web monitoring

Technical collection

- Commercial intelligence feeds
- Consumer device monitoring
- DNS sinkholes
- DNS traffic
- Exploit and vulnerability monitoring
- Honey networks
- Incident response

Human collection

- Asset recruitment
- Cybercollection
- Regional assets

pen.sec
Protecting Your Assets

Cyber Threat Intelligence – Produkte

- militärische Nomenklatur -

Tactical intelligence products

- Daily media highlight analysis
- Flash/Tipper reports for rapid dissemination
- Malware analysis reports
- Raw information reports
- Real-time attack maps
- Threat intelligence feeds

Operational intelligence products

- Adversary assessments that profile specific threat actors
- In-depth technical reports that include technical analysis and course of action with appropriate signatures
- Vulnerability analysis report
- Weekly, monthly, quarterly intelligence summaries

Strategic intelligence products

- Strategic assessments for specific verticals with a 1- to 5-year forecast
- Annual intelligence summary
- Comparison of internal risk profile across different industries
- Geopolitical analysis
- Simulations that allow exploration of potential risk when contemplating entering new geographies and business sectors and when adopting new technologies
- Threat activity correlated to internal security controls/maturity

Cyber Threat Intelligence – Technische Maßnahmen

- simple alerts
- detailed reports
- machine-readable data feeds
- custom-designed output
- Application Programming Interfaces (API)
- secure online portals

Technische und Organisatorische Schutzmaßnahmen (TOM)	preventive	detective	corrective	deterrent
Firewall Rules / Proxy / DNS Sinkholes	X	X		
Detection techniques: • machine learning (AI) • anomaly • signature		X		
Intrusion Detection / Prevention System • network • host • hybrid		X	X	

Unternehmen / Organisation

Maßnahmen können mit anderen Techniken und/oder Maßnahmen zu komplexeren Produkten kombiniert werden.

Kombinierte Techniken sind technisch meist komplex, noch in der Entwicklung und deshalb noch von niedrigem Reifegrad:

- Threat Intelligence Service
- Threat Intelligence Platform
- Security Incident & Event Management (SIEM)
- Security Orchestration, Automation and Response (SOAR)
- Security Operation Center (SOC)

pen.sec
Protecting Your Assets

Threat Intelligence & Vulnerability Management

I Motivation

II Begriffe und Abgrenzung

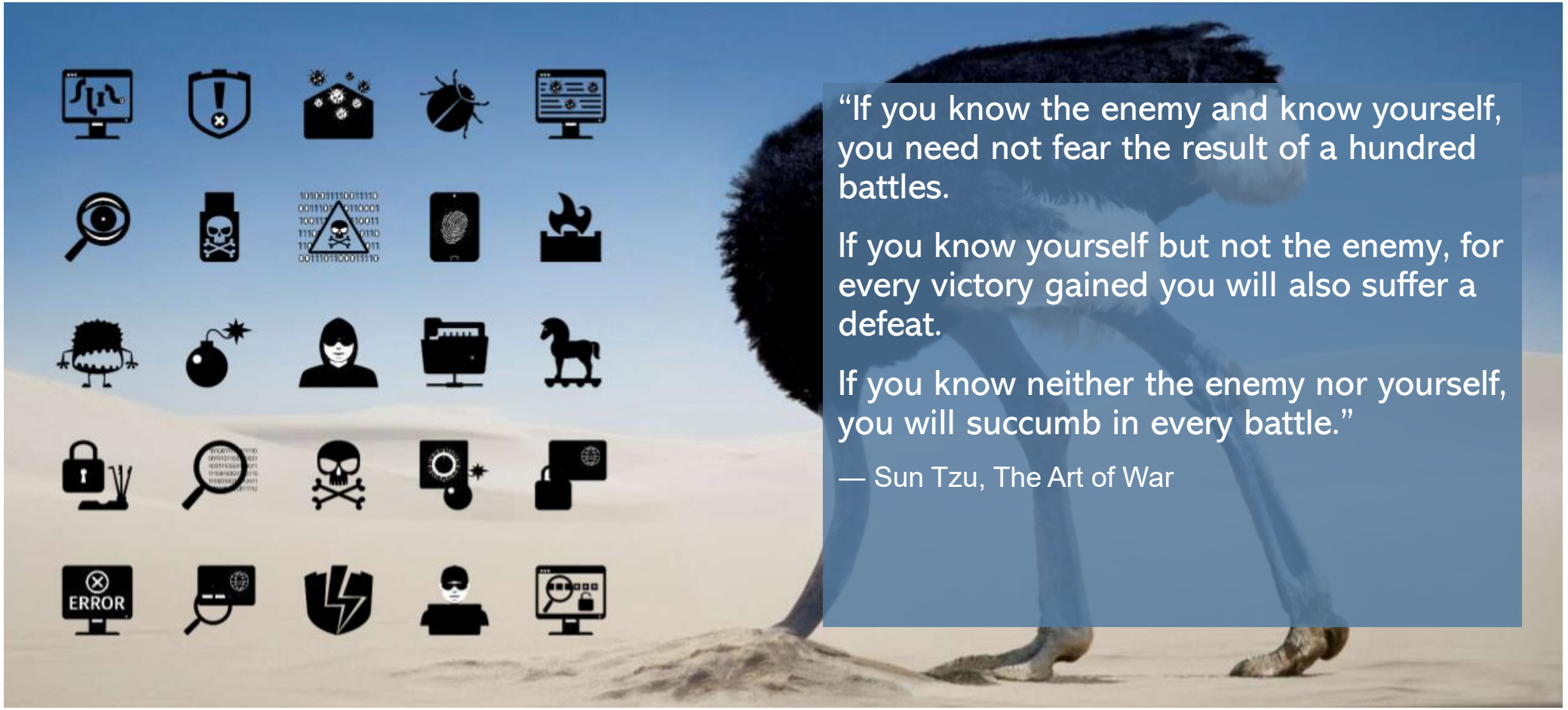
III Methoden, Produkte & Maßnahmen

IV Einsatz in und Mehrwert für Organisationen und Unternehmen

Threat Intelligence & Vulnerability Management

Einsatz in und Mehrwert für Organisationen und Unternehmen

CTI & VM – What we don‘t know we don‘t know



“If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle.”

— Sun Tzu, The Art of War

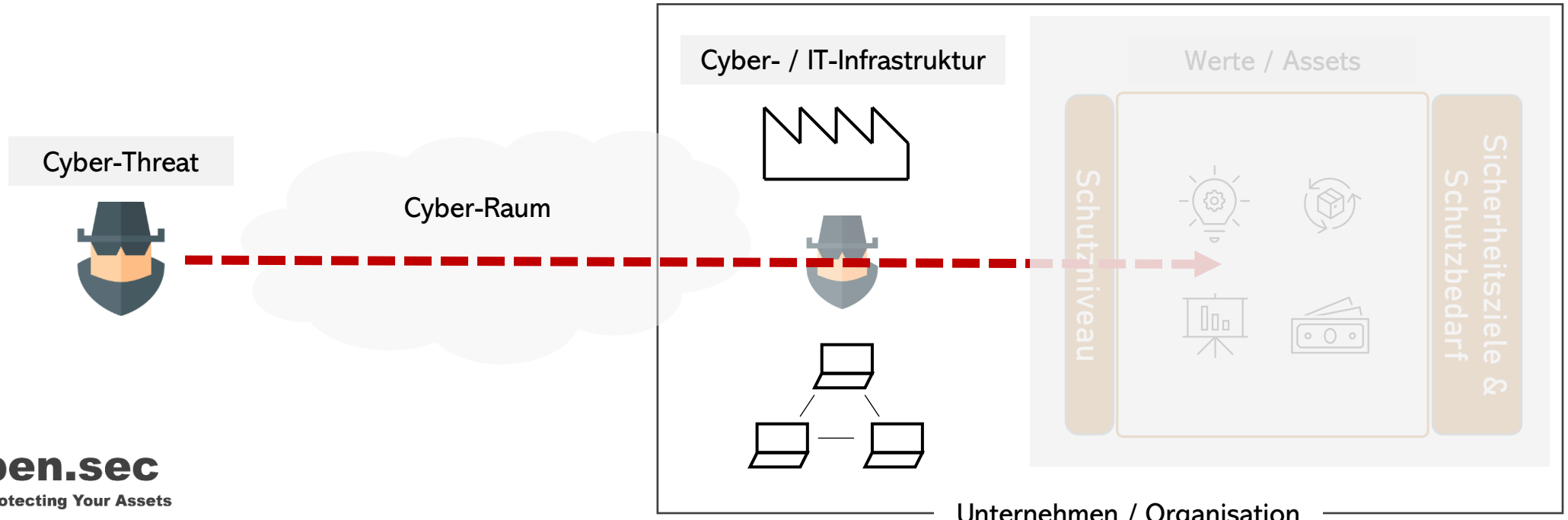
pen.sec
Protecting Your Assets

Ziele Cyber-Sicherheit

Cyber-Sicherheit ist ein einem Cyber-System zugeordnetes Attribut, welches die Fähigkeit des Systems, sich vor internen oder externen Angriffen zu schützen, beschreibt.

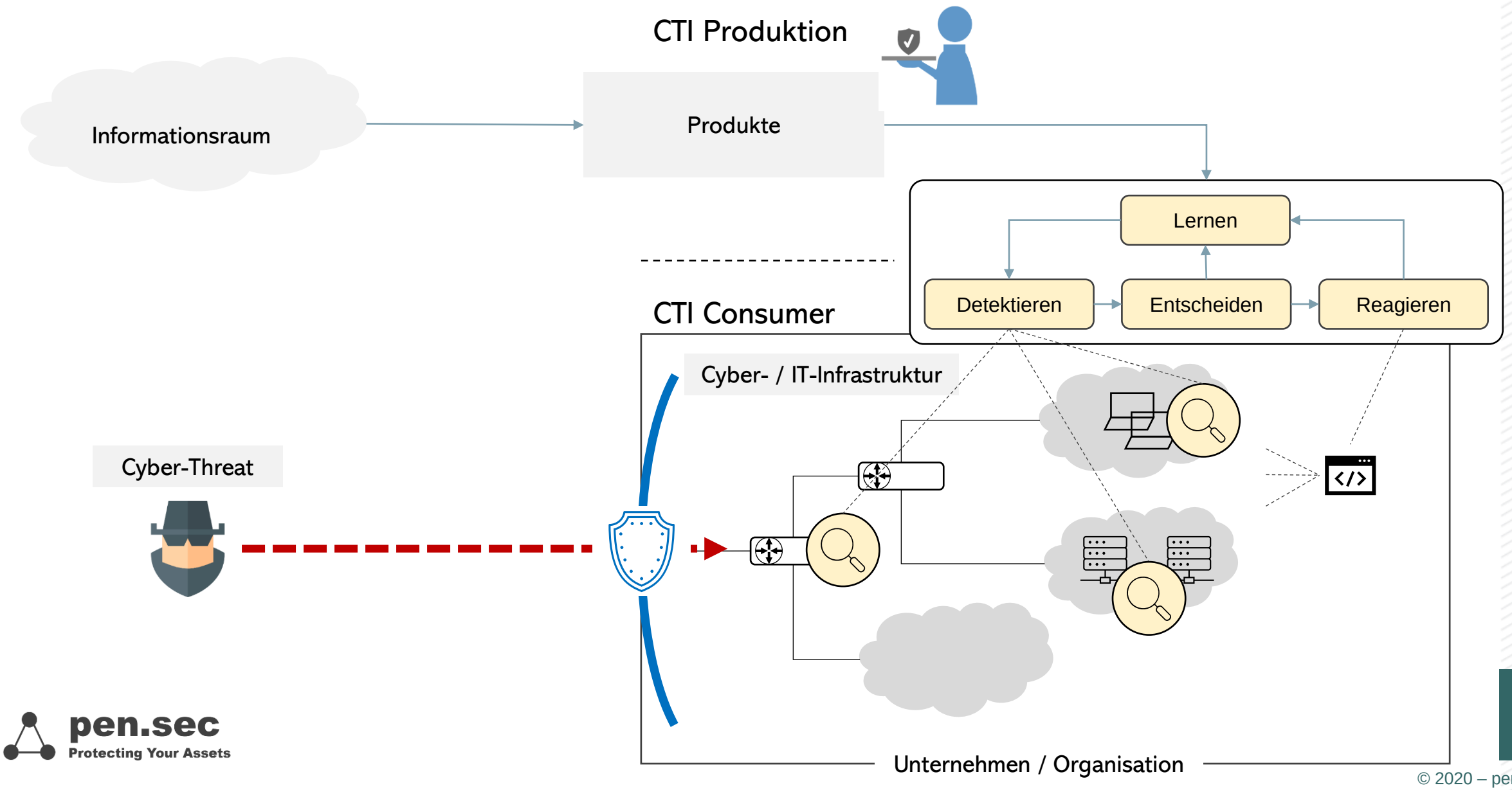
Die Sicherheit eines Systems wird durch Maßnahmen mit dem Ziel gesteigert, dass das System:

1. internen oder externen Angriffen widersteht
2. mit den Angriffen, denen es nicht widersteht, umgehen kann
3. sich von den Angriffen, mit denen es nicht umgehen kann, schnell und zuverlässig erholt und ein gegebenenfalls entstehender Schaden begrenzt bleibt



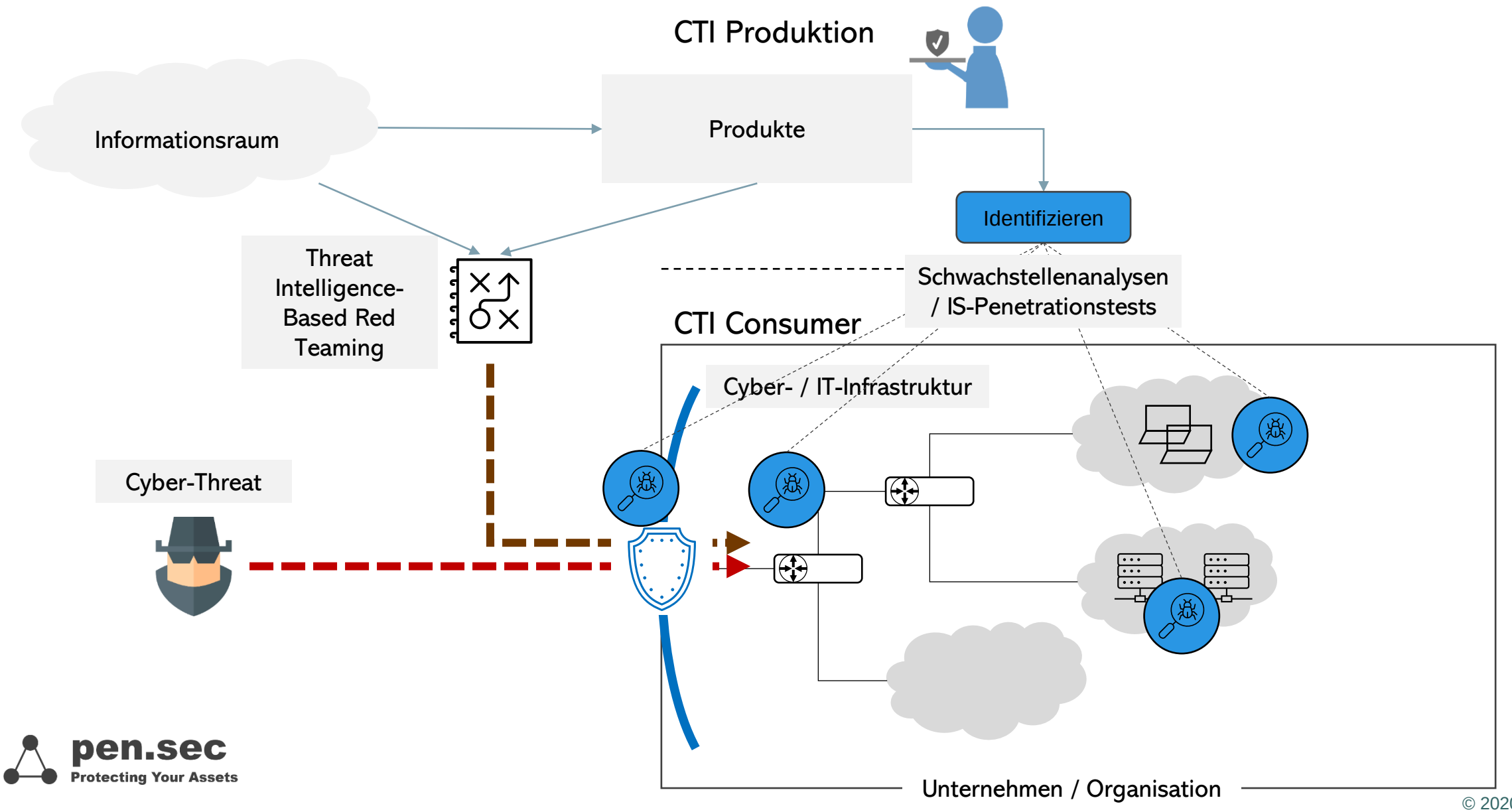
pen.sec
Protecting Your Assets

Cyber Threat Intelligence zur Steigerung der Cyber-Sicherheit



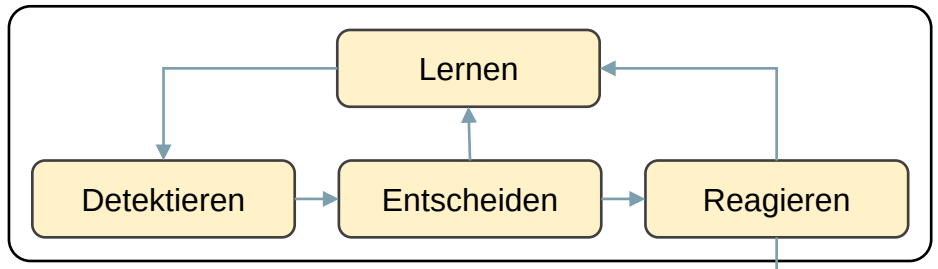
pen.sec
Protecting Your Assets

Vulnerability Management zur Steigerung der Cyber-Sicherheit

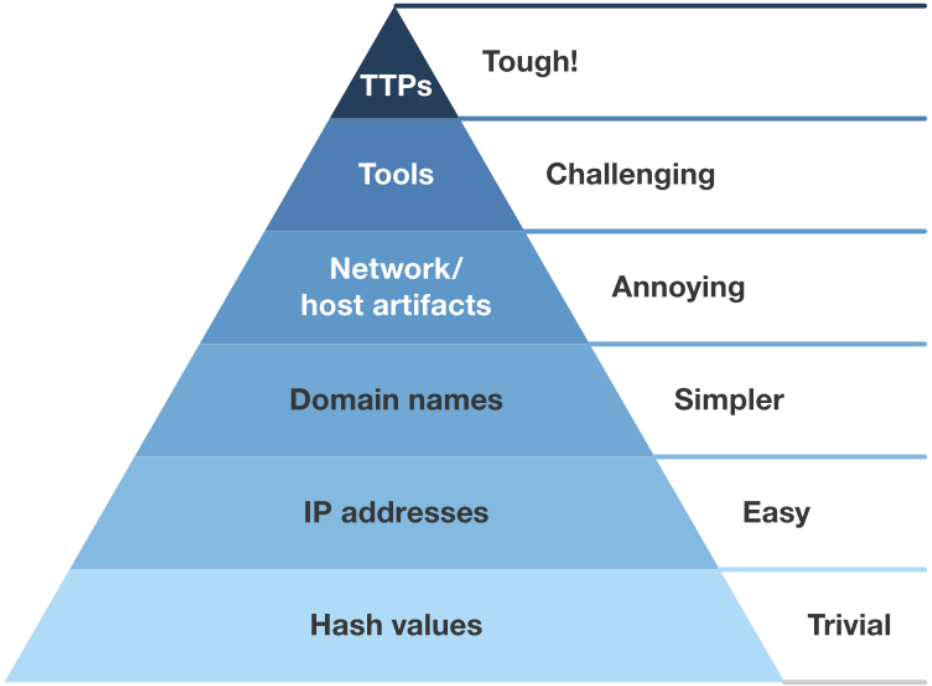


pen.sec
Protecting Your Assets

Cyber Threat Intelligence – Kill Chain & Pyramid of pain



Unterbrechen der Cyber Kill Chain



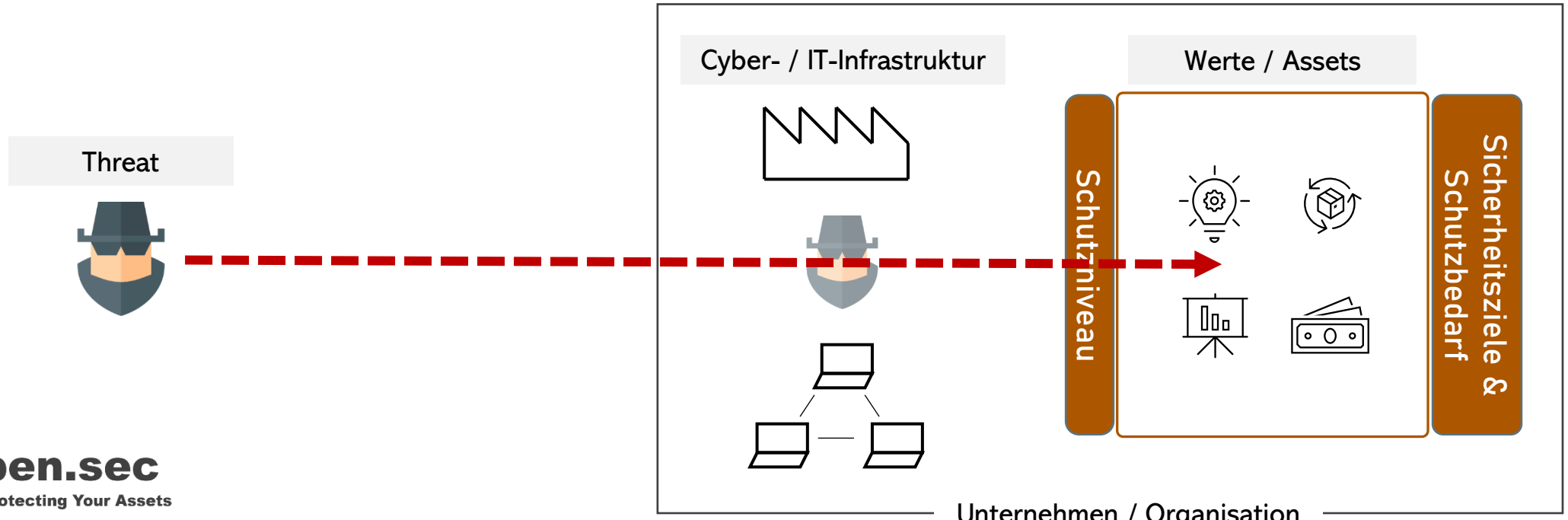
http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Gaining Access → Lateral Movement → Goal

pen.sec
Protecting Your Assets

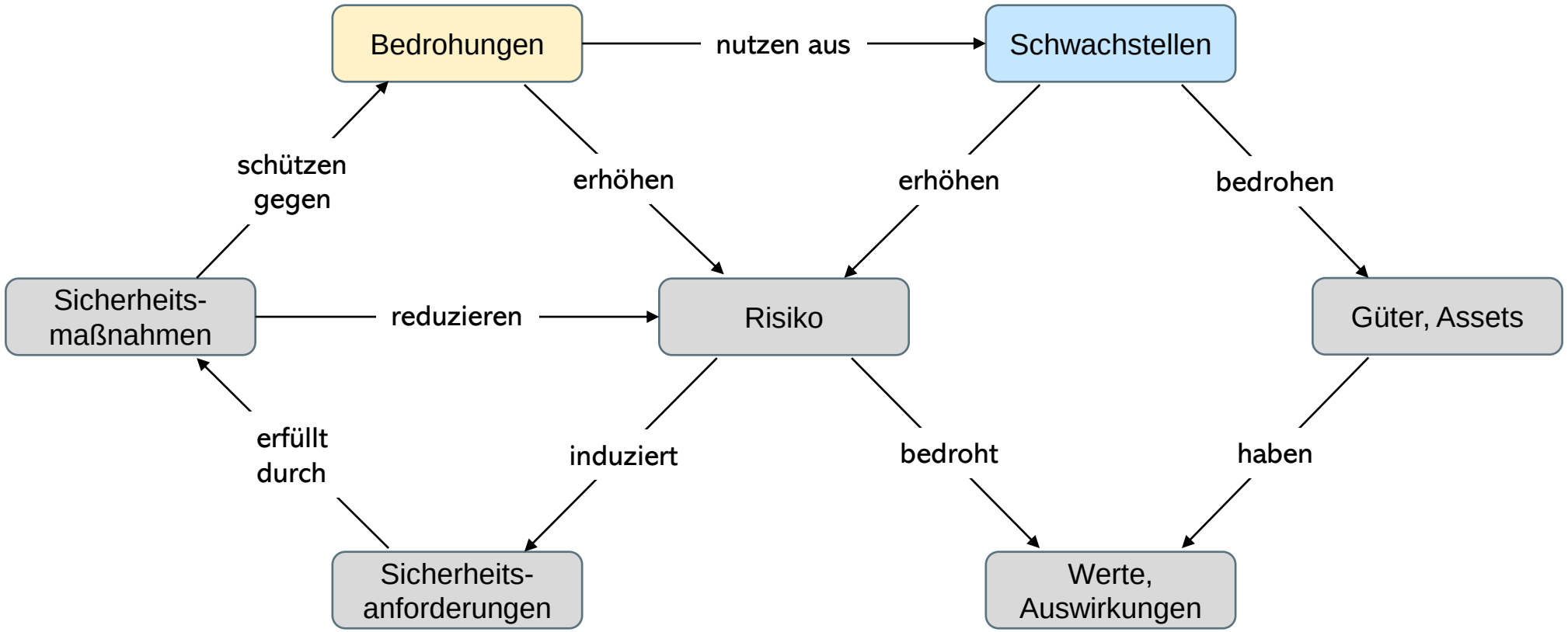
Ziele Informationssicherheit

Schutz der Informations-Werte eines Unternehmens / einer Organisation vor Bedrohungen durch Sicherstellung eines allgemein anerkannten oder spezifisch festgelegten Schutzniveaus.



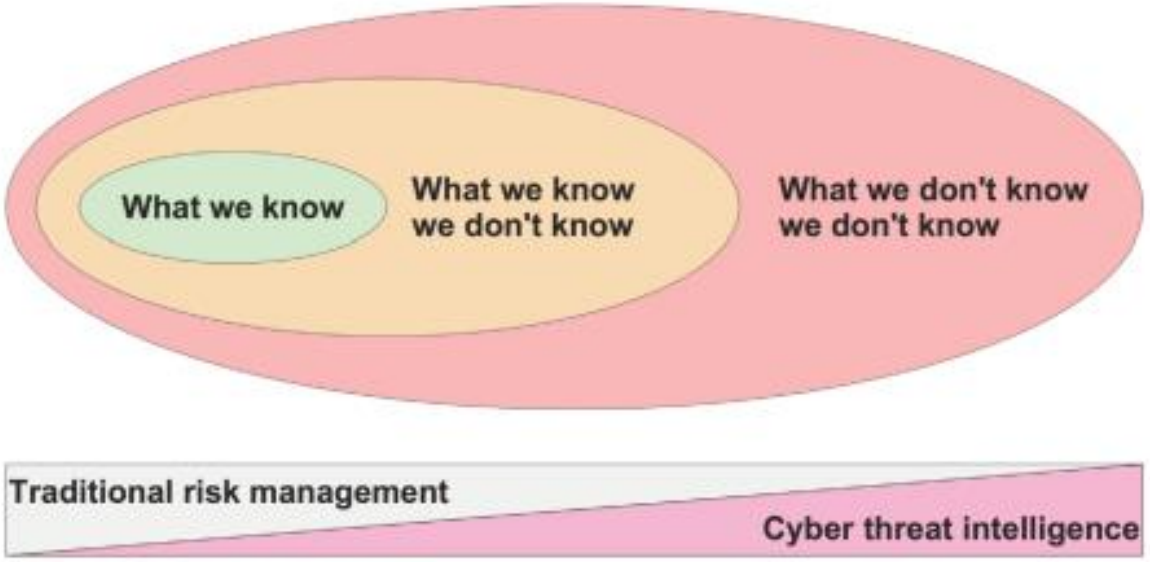
pen.sec
Protecting Your Assets

Semantik der Informationssicherheit



pen.sec
Protecting Your Assets

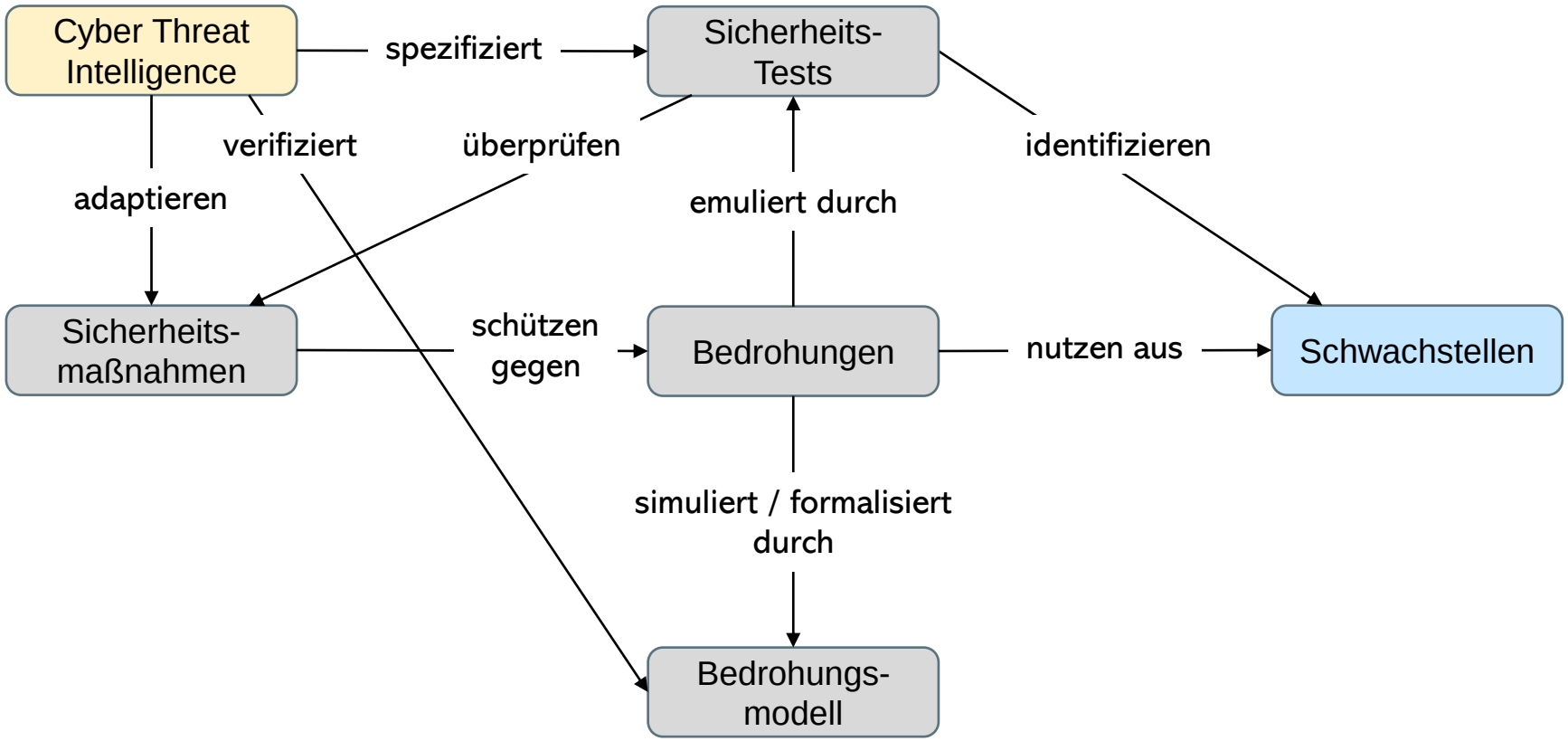
Intelligence Consumption – Schichtenmodell



- **„What we know“**: z.B. erkannter, identifizierter Angriff
- **„What we know we don‘t know“**: z.B. wissen, dass eine bestimmte Klasse von Bedrohungen nicht behandelt wurde
- „**What we don‘t know we don‘t know**“: z.B. ein faktisch bestehendes Risiko ist nicht erkannt, nicht identifiziert und nicht behandelt

pen.sec
Protecting Your Assets

insbesondere Reduzierung des „What we don‘t know we don‘t know“:



pen.sec
Protecting Your Assets

Beispiel: Bewerbung & Kaffee – Szenario

ein kleines Mittelstandsunternehmen:

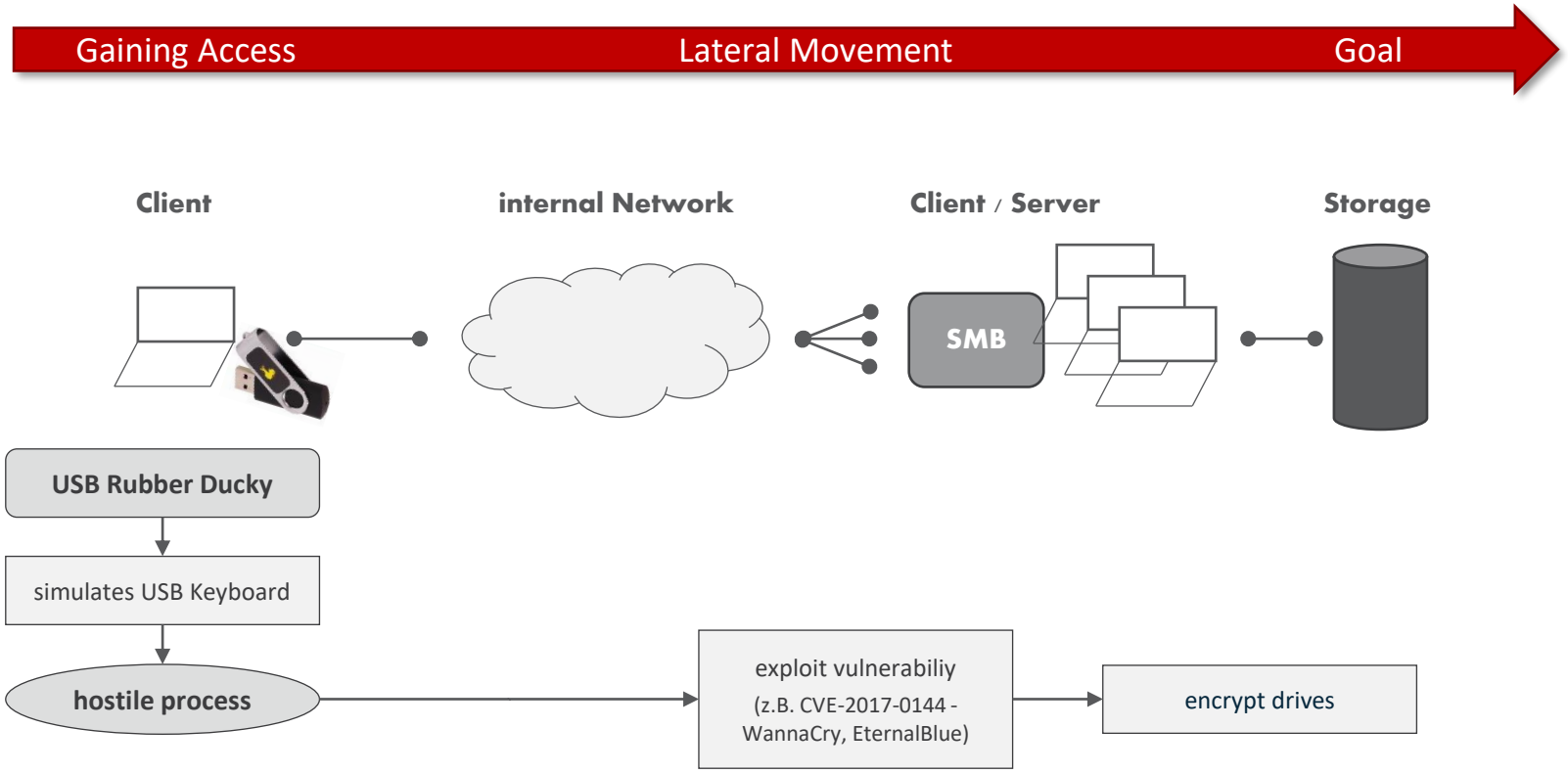
Person kommt mit Bewerbungsunterlagen an den Empfang eines kleinen Unternehmens, stellt sich kurz vor und berichtet, dass sie in nur 30 Minuten ein Bewerbungsgespräch bei dem Personalleiter Herrn Y einer benachbarten Firma habe.

Dummerweise hat die Person sich grade einen Kaffee über die Bewerbungsunterlagen gekippt. Sie bittet die Dame am Empfang das Dokument auf dem USB-Stick, den sie dabei hat, noch einmal auszudrucken.

Threat Actor	(Klein)-Krimineller, externer Angreifer
TTP	Ransomware

pen.sec
Protecting Your Assets

Beispiel: Bewerbung & Kaffee – Kill Chain



pen.sec
Protecting Your Assets

Beispiel: Bewerbung & Kaffee – Analyse

Complexity of Attack

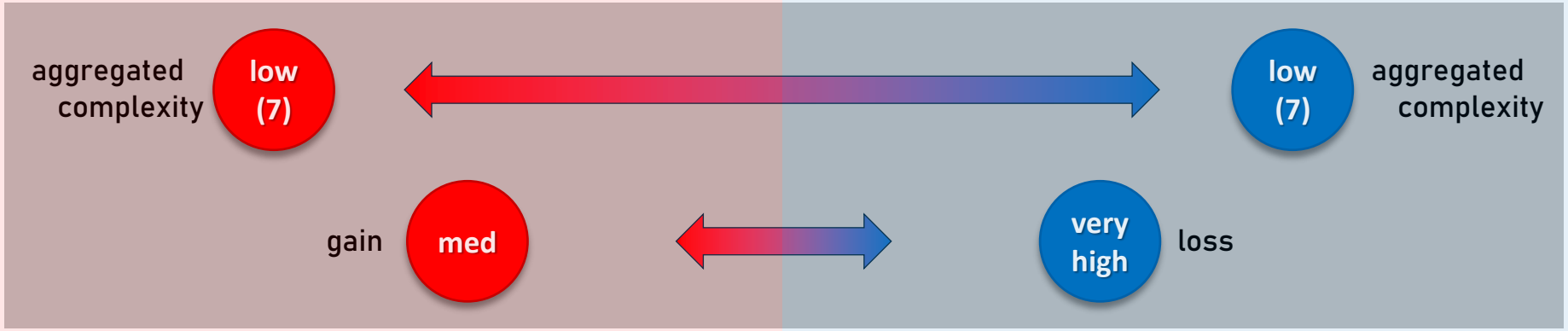
Expertise	Equipment
Social Engineering + Equipment	Rubber Ducky + Ransomware
medium (3)	**low (2)**

Knowledge of TOE	Window of Opportunity
keine	jeden Werktag
very low (1)	**very low (1)**

Complexity of (most basic) Countermeasure

Expertise	Equipment
Awareness	-
medium (3)	**very low (1)**

Feasibility	Costs
keine Abhängigkeiten	Training
very low (1)	**low (2)**



pen.sec
Protecting Your Assets

Beispiel: Fish the Automotives – Szenario

ein mittelgroßer IT-Dienstleister im Automotive-Bereich:

Der IT-Dienstleister betreibt als Dienstleistung ein Portal, welches Prozessabläufe zwischen OEM und seinen Zulieferern koordiniert.

Das Web-Interface des Portals wird durch einen Angreifer kompromittiert, der für den normalen Nutzer nicht sichtbar einen Link auf eine eigene „Web-Seite“ integriert.

Nach einiger Zeit bemerkt die IT-Abteilung die Kompromittierung und bereinigt das Web-Interface. Die Analyse der IT-Abteilung ergibt, dass das Ziel des Angreifers das Sammeln von Klicks war.

Threat Actor	unbekannt
TTP	???

pen.sec
Protecting Your Assets

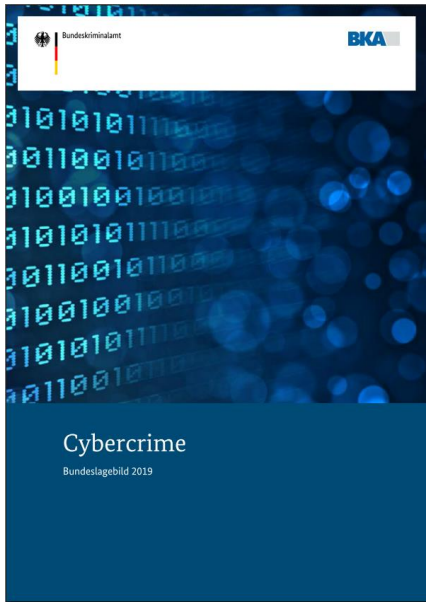
CTI & VM im Unternehmen / in der Organisation

Handlungsebenen des Unternehmens / der Organisation

	operativ	taktisch	strategisch
Cyber Threat Intelligence (Products)	▪ Proxy / DNS Sinkholes ▪ Virenschutz ▪ End-Point-Protection ▪ Log-Analyzer ▪ Intrusion Detection / Prevention ▪ SIEM & SOC ▪ Security Orchestration, Automation and Response Solutions (SOAR) ▪ …	▪ IS-Risikobewertung ▪ Threat-Landscape ▪ Awareness ▪ Fortbildung ▪ …	▪ IS-Risikomanagement ▪ Lageberichte ▪ …
Vulnerability Management	▪ manuelle / automatisierte Schwachstellnanalysen ▪ IS-Penetrationstests ▪ Version- & Patch-Management ▪ …	▪ IS-Risikobewertung ▪ Red-Teaming-Kampagnen ▪ …	▪ IS-Risikomanagement ▪ …

pen.sec
Protecting Your Assets

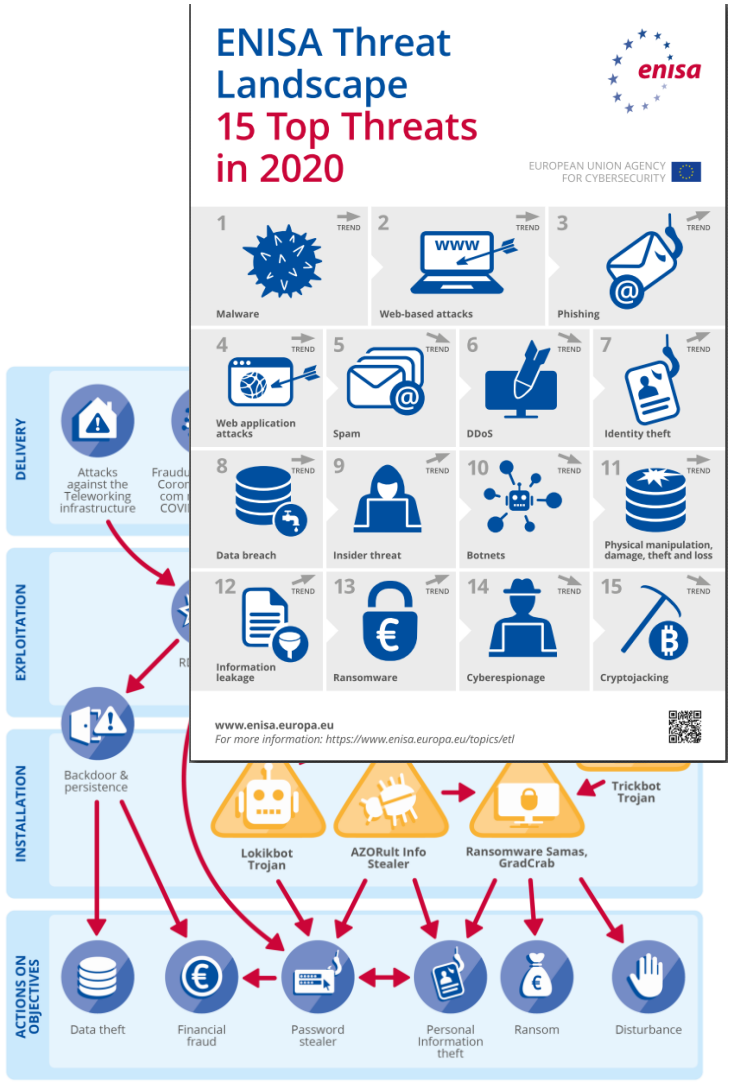
Fangen wir an ☺



enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

THREAT LANDSCAPE MAPPING

Exploitation by cybercriminals and advanced persistent threat (APT) groups of the current coronavirus (COVID-19) global pandemic.



pen.sec
Protecting Your Assets

pen.sec
Protecting Your Assets

pen.sec AG

https://pen-sec.de
info@pen-sec.de
+49 8623 364970

Edt 4
84558 Kirchweidach

Basler Str. 115
79115 Freiburg im Breisgau