MODULE ID

EINFÜHRUNG IN DIE CYBERSICHERHEIT FÜR DIE IT PROFESSIONALS

Marco

- Reitsport
- Hintergrund in der Softwareentwicklung
- Defensive AppSec-Forschung und -Bewertung
- Dozent (TH-Nürnberg) für Software-Sicherheitstechnik
- Mitverfasser von iX-Veröffentlichungen über SAP-Sicherheit

https://www.linkedin.com/in/marcohammel/

Informationen

Lernziele

- Sie sind in der Lage, Cybersicherheitsbereiche im Kontext der Anwendungssicherheit zu verstehen
- Sie kennen die Hauptursachen für Sicherheitsmängel in Software
- Sie kennen die Konzepte des gegnerischen Rahmens für Bedrohungsanalyse, Bedrohungsjagd und Emulation
- Defensivmaßnahmen können nach ihrem taktischen Ansatz kategorisiert werden
- Sie können die Anwendbarkeit trügerischer und aktiver Gegenmaßnahmen bestimmen
- Sie kennen die gängigen Verfahren und Ansätze für Abwehrmaßnahmen.

MODULE ID

GRUNDLAGEN DER ANWENDUNGSSICHERHEIT

Lernziele

- Sie wissen, wie sich die Anwendungssicherheit in ein Domänenmodell der Cybersicherheit einfügt
- Sie können die Grenzen der verschiedenen Sicherheitsebenen beschreiben
- Sie kennen die Bedeutung von Eingabevalidierung und Ausgabekodierung
- Sie können die Sicherheitsmerkmale einfacher Anwendungsworkflows bewerten
- Sie verstehen die möglichen Ursachen von Software-Sicherheitsmängeln

Kapitel

Anwendungssicherheit in der Cyberdomäne

Das Dilemma der Codesicherheit und die Grenzen von Sicherheitsbereichen und -werkzeugen

Ursachen für Sicherheitsmängel

Ursachen für Sicherheitsmängel in der Softwareentwicklung

Überprüfung der Eingaben

Überlegungen zur Sicherung von Software durch Eingabevalidierung

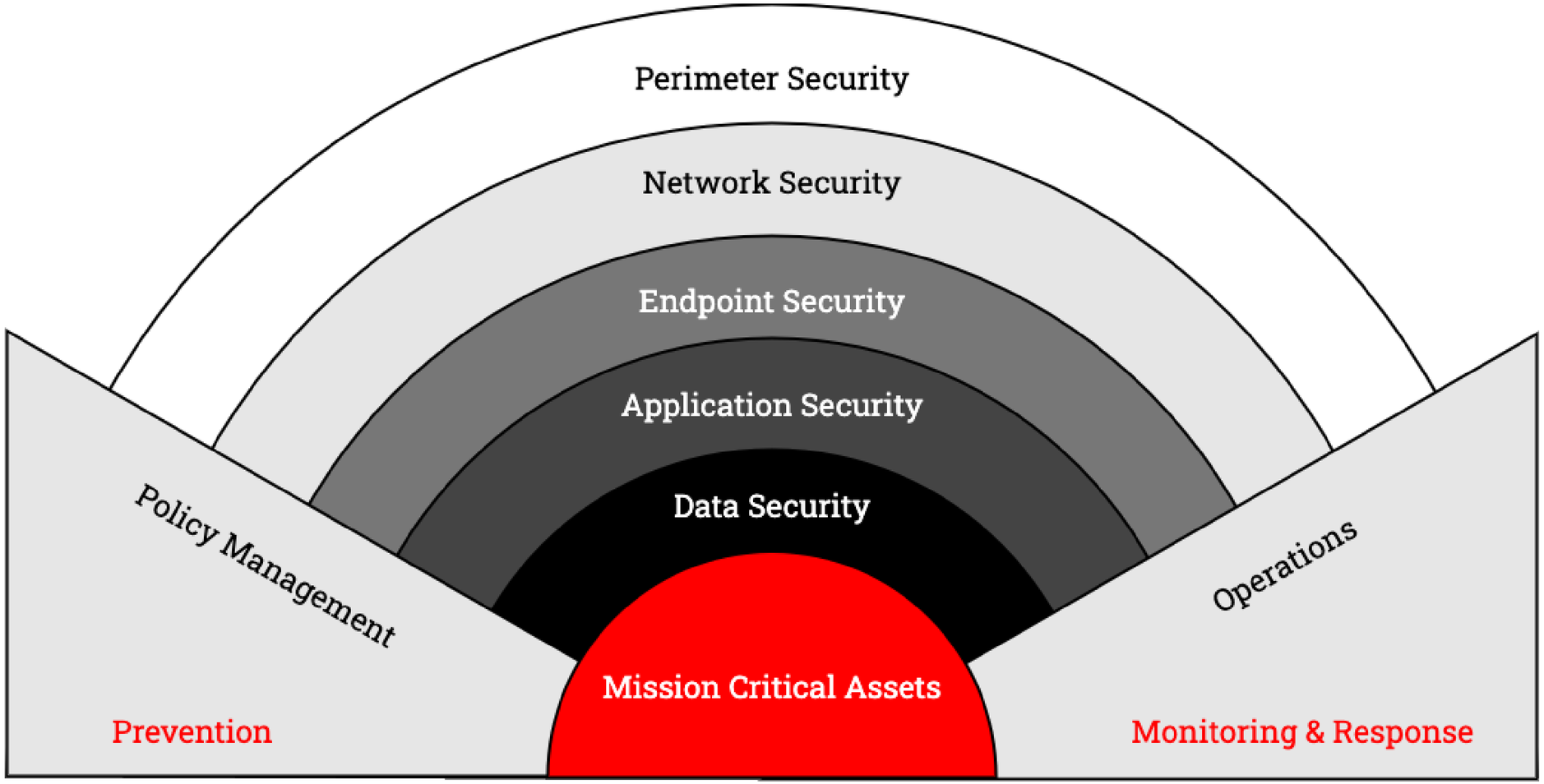
Kodierung der Ausgabe

Überlegungen zur Sicherung von Software durch Ausgangskodierung

Schlussfolgerung

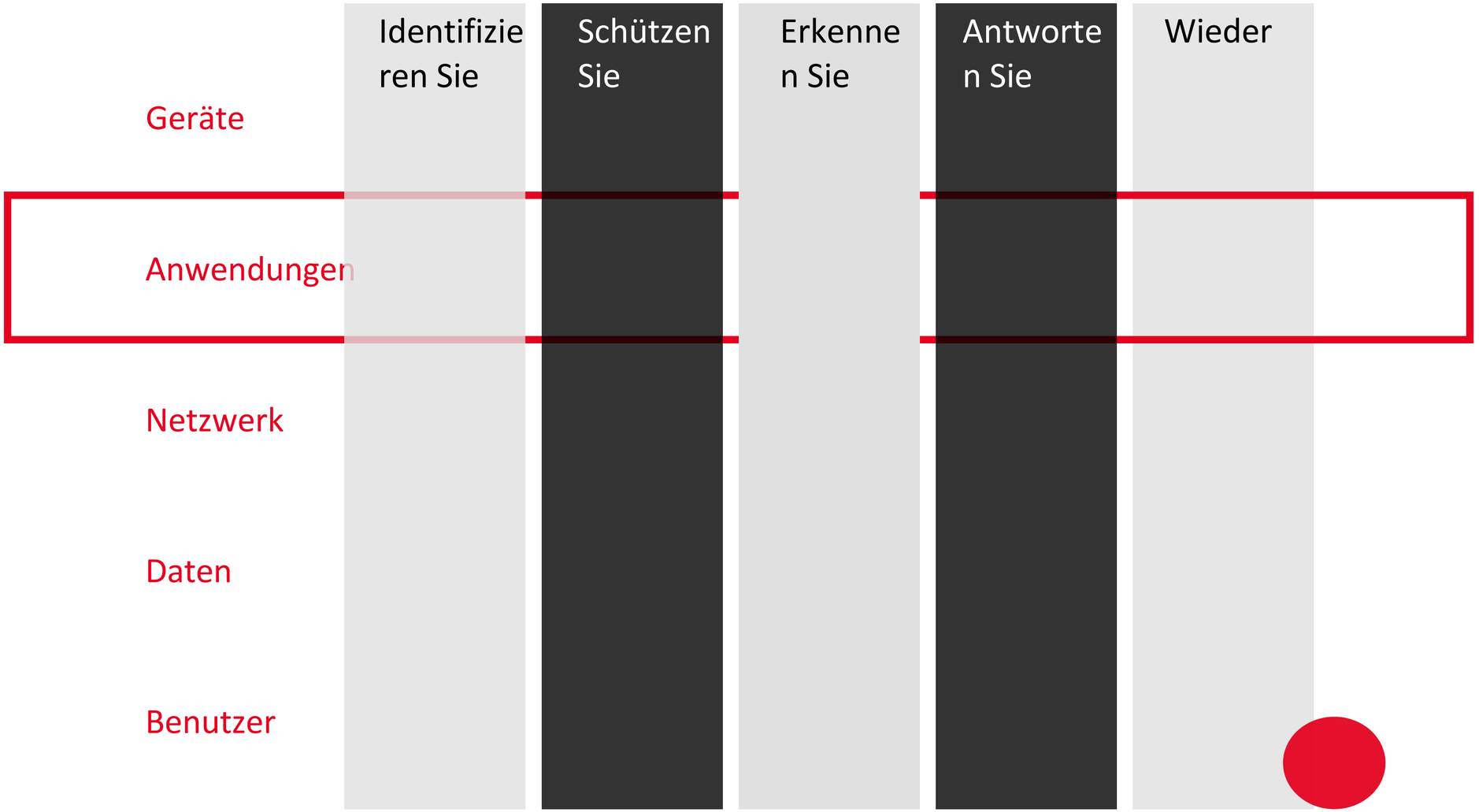
ANWENDUNGSSICHERHEIT IM CYBERBEREICH

SCHUTZBEREICHE

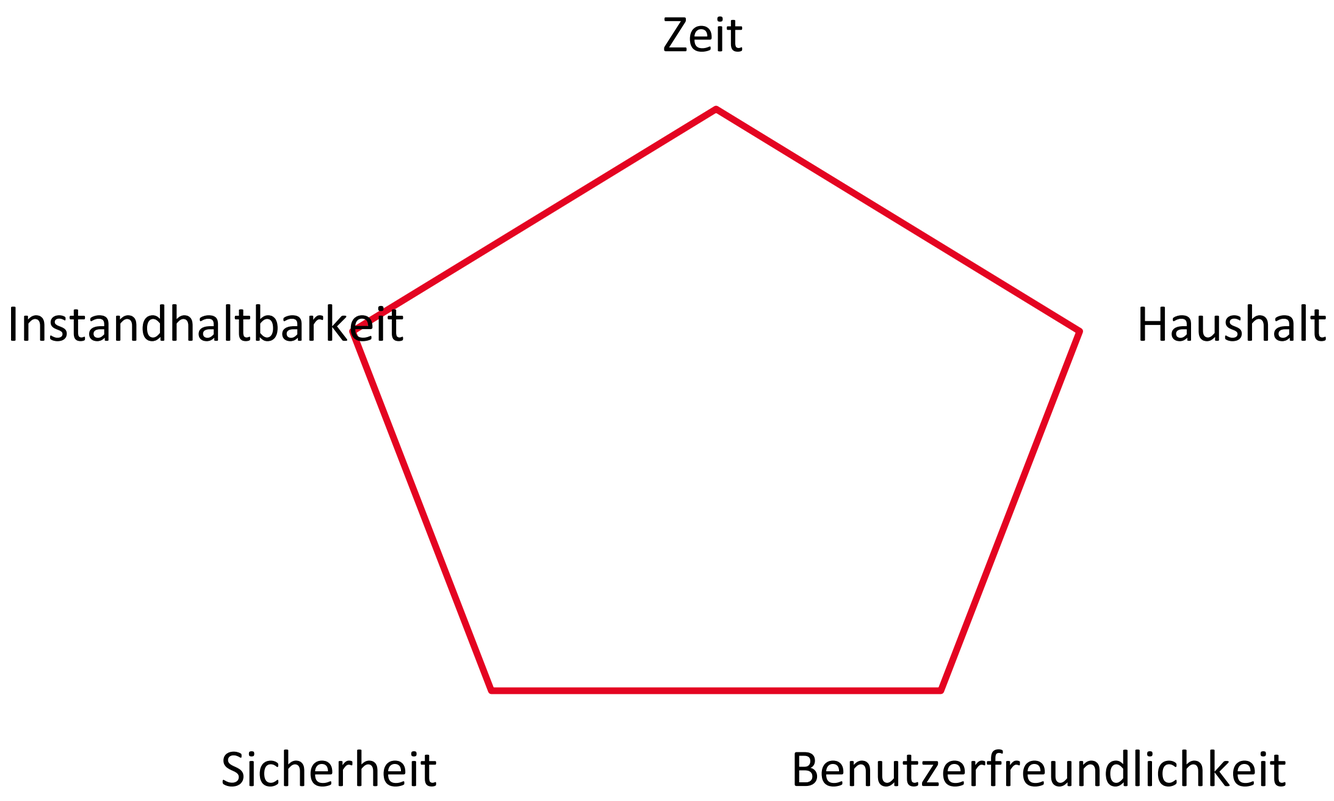


Nothrop Grumman Sicherheitsventilator

AKTIONSBEREICHE DER SICHERHEIT



DILEMMA DER SOFTWARESICHERUNG



GRENZEN DER SICHERHEITSEBENEN

- Firewalls machen Anwendungen nicht sicher -> beschränken aber den Zugang
- Systeme zur Verhinderung von Eindringlingen haben keine Anwendungen sicher machen -> aber könnte Angriffsmuster erkennen
- Verschlüsselung macht keine Anwendungen sicher -> unterstützt aber die Vertraulichkeit & Integrität der Daten bei Übertragung und Speicherung
- Die Zugangskontrolle macht keine Anwendungen sicher -> aber reduzieren die Angriffsfläche

- Reverse Proxies machen Anwendungen nicht sicher -> aber die Beschränkung des Zugangs von Clients
- Web Application Firewalls machen keine Anwendungen sicher -> aber möglicherweise verdächtige Nutzung zu erkennen und zu verhindern, wenn sie geschult sind
- Scanner sind nicht ausreichend, um alle Schwachstellen -> weil sie nicht den geschäftlichen Kontext zu verstehen

URSACHEN FÜR SICHERHEITSMÄNGEL

GRUNDURSACHE VON SICHERHEITSMÄNGELN

Sicherheitsmängel können an verschiedenen Stellen des Softwareentwicklungsprozesses auftreten

SPEZIFIKATION

Fehlende Anforderungen

DESIGN

Ungeeignete Architektur / Entwurf

IMPLEMENTIERUNG

Mängel bei der Umsetzung

TEST

Ungeeignete Sicherheitstests

Meistens falsche implizite Annahmen

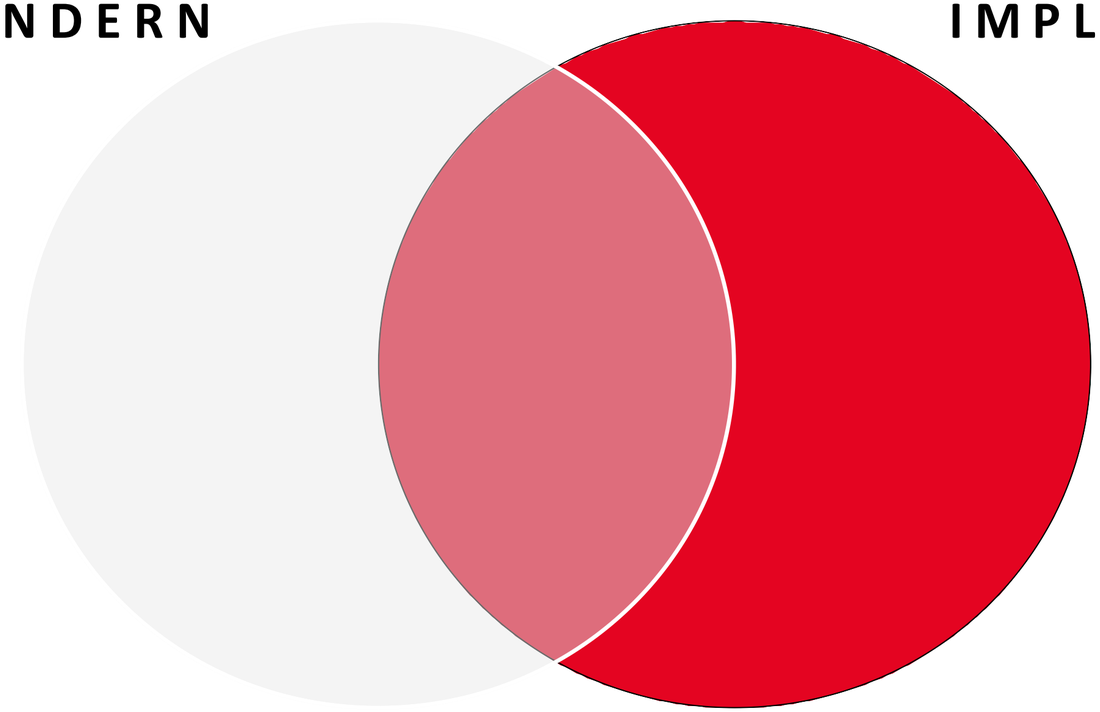
URSACHEN FÜR SICHERHEITSMÄNGEL

SPEZIFIKATION

URSACHEN FÜR SICHERHEITSMÄNGEL

SPEZIFISCHENDERN

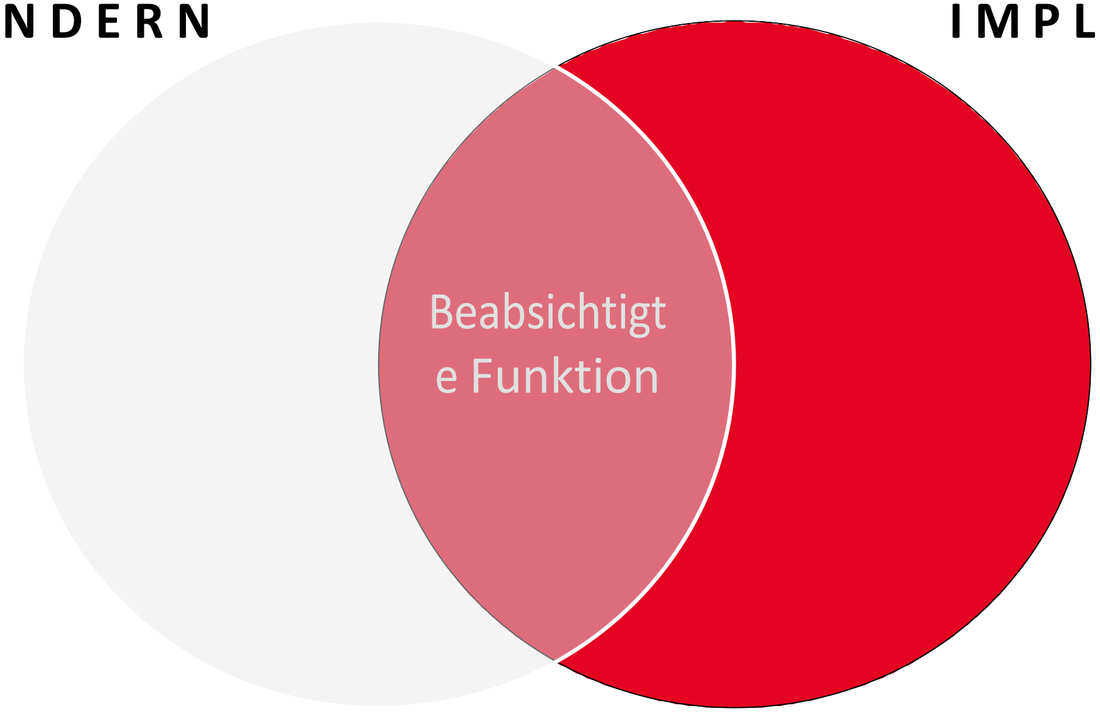
IMPLEMENTATION



URSACHEN FÜR SICHERHEITSMÄNGEL

SPEZIFISCHENDERN

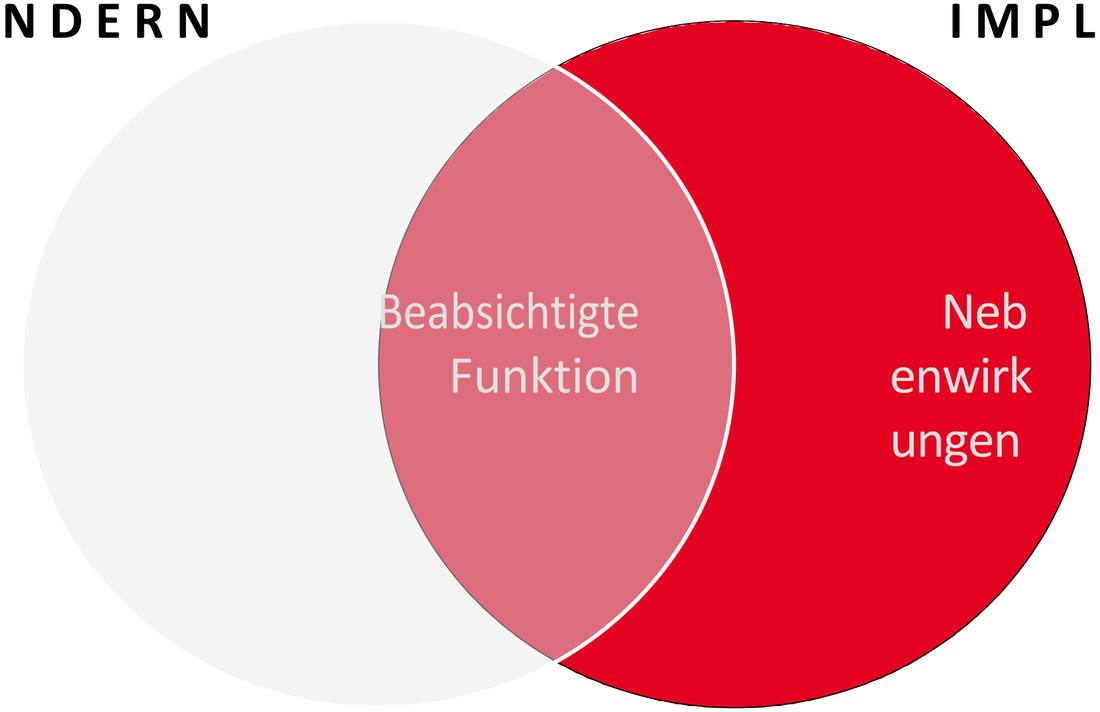
IMPLEMENTATION



URSACHEN FÜR SICHERHEITSMÄNGEL

SPEZIFISCHENDERN

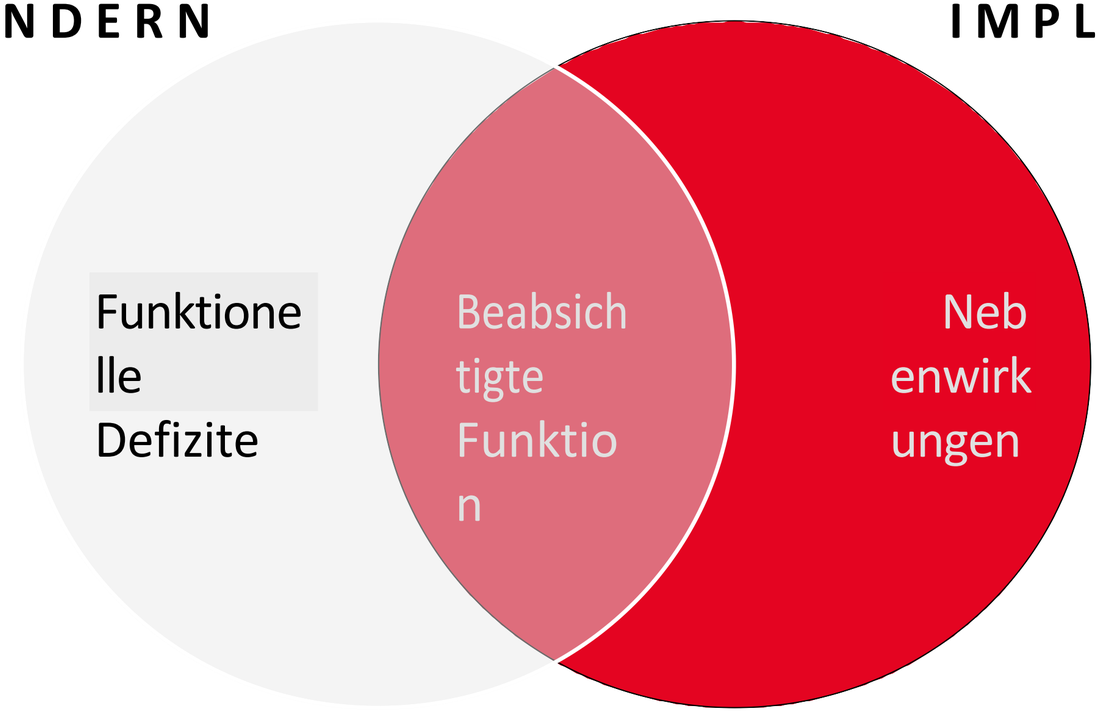
IMPLEMENTATION



URSACHEN FÜR SICHERHEITSMÄNGEL

SPEZIFISCHENDERN

IMPLEMENTATION



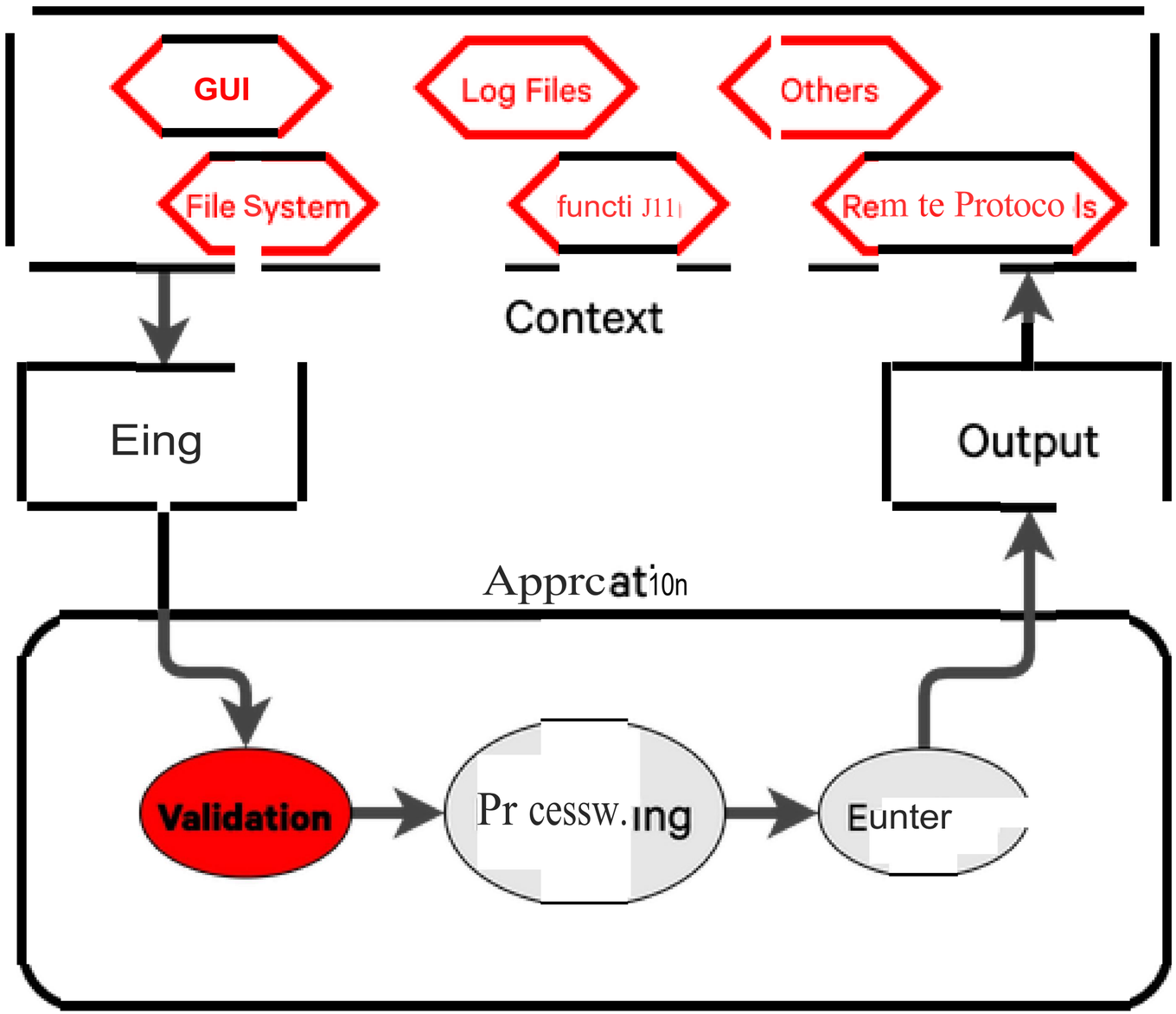
EINGABEÜBERPRÜFUNG

PRIAM

KÖNIG VON TROY

"Wir hätten eine Eingabevalidierung durchführen sollen"

HOW INPUT VALIDATION SHOULD LOOK LIKE
HOW IT ACTUALLY LOOKS LIKE
imgflip.com

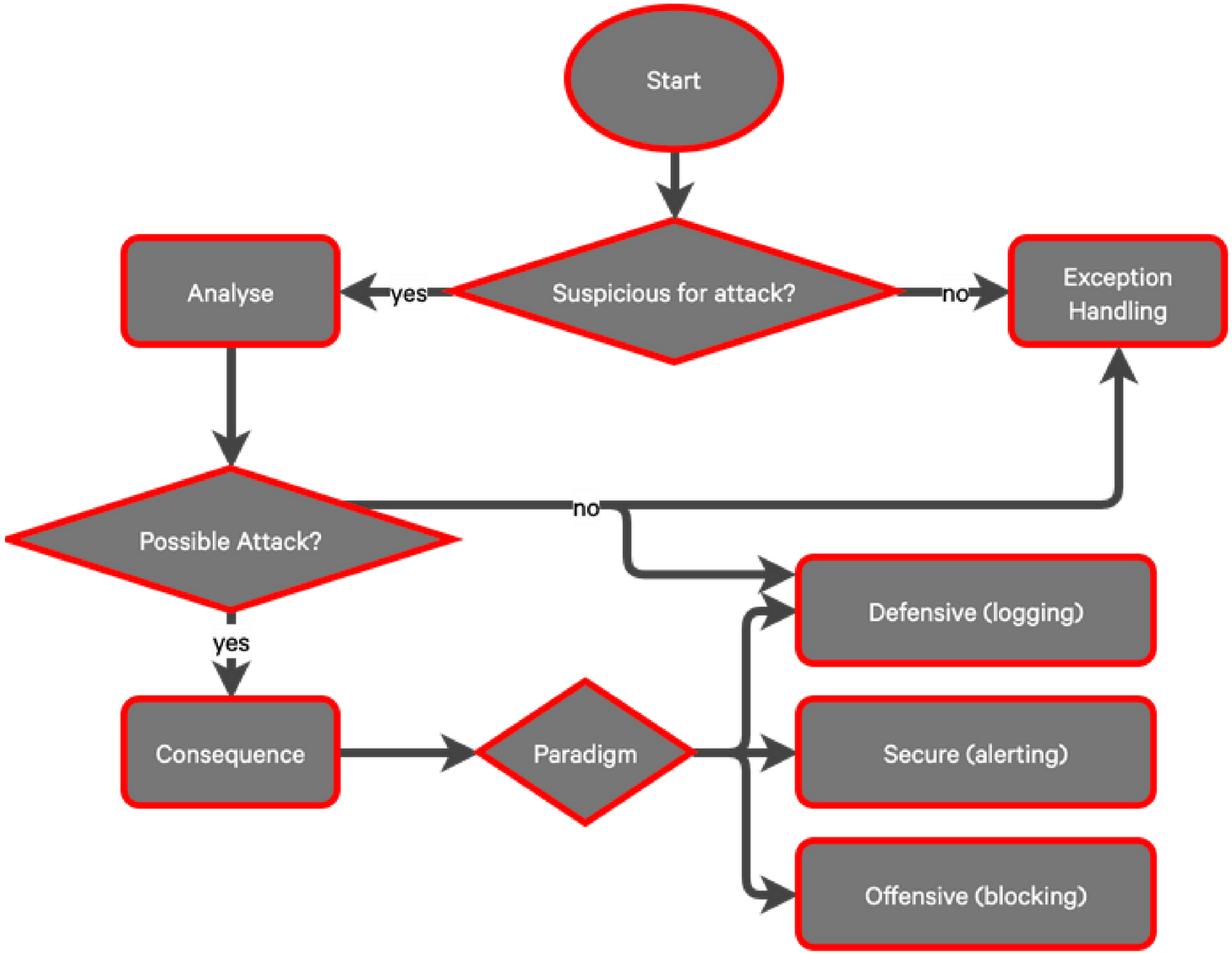

GUI
Log Files
Others
File System
functi J11
Rem te Protoco ls
Context
Eing
Output
Apprcat10n
Validation
Pr cessw.ing
Eunter

EIN ALLGEMEINER ANSATZ

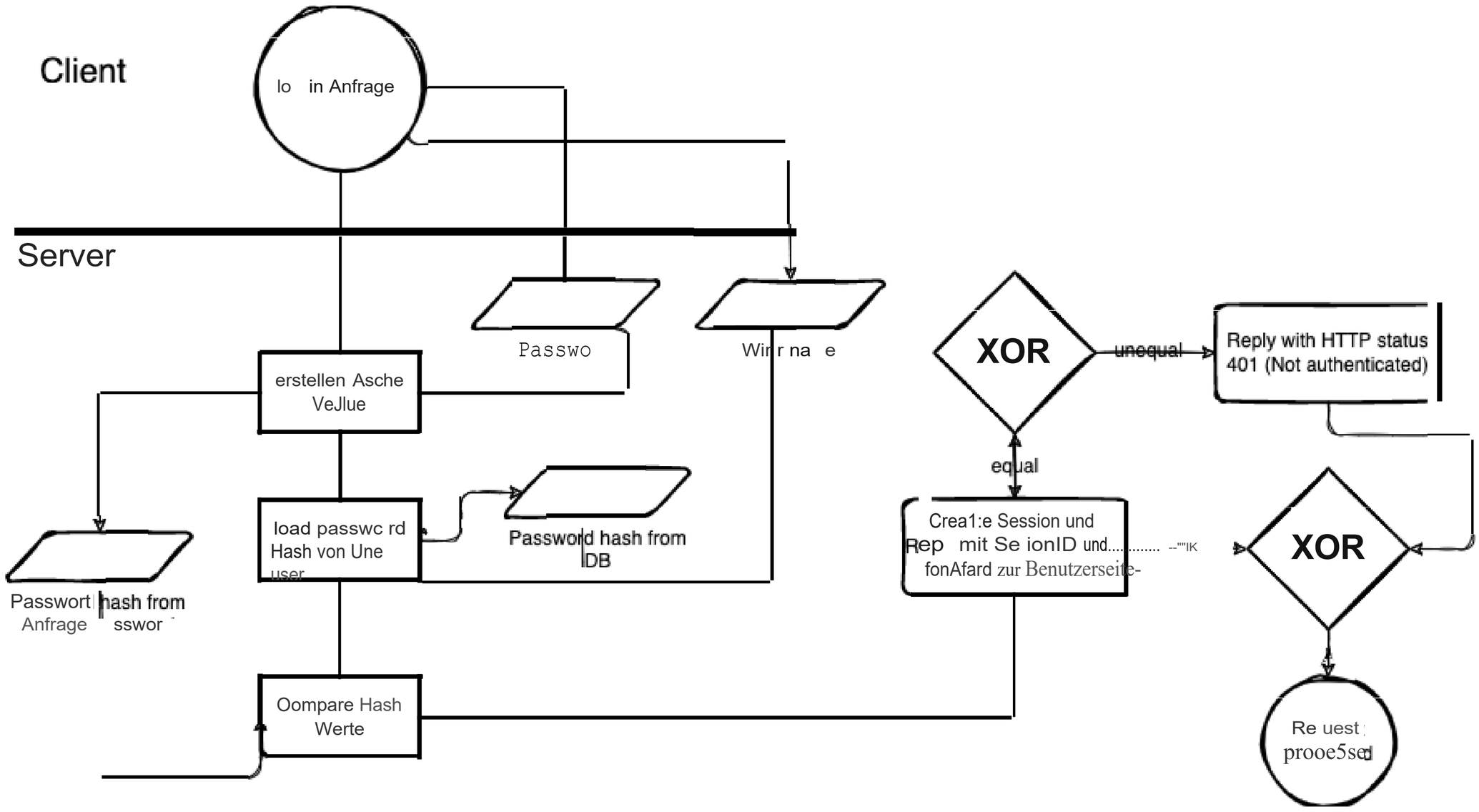
1. Eingangsquellen und Eingänge entdecken
2. Annahmen über die Eingabe explizit machen
3. Bestätigen Sie die Eingabe
4. Entscheiden Sie über die Validierungsergebnisse

1. Vorhandensein / Länge
2. Canonice
3. Typ prüfen
4. Wertebereich prüfen
5. Filter
   1. Schwarze Liste
   2. Whitelist

KONSEQUENZEN ZIEHEN



- Welche Eingabeüberprüfung fehlt in der folgenden Implementierung einer Login-Routine?
- Wie können wir die Implementierung der Anmeldungsroutine verbessern?
- Welche Art von Paradigma halten Sie hier für angemessen und Waru


Client
lo in Anfrage
Server
Passwo
Wir r na e
erstellen Asche VeJlue
load passwc rd Hash von Une user
Passwo d hash from DB
Passwort Anfrage
hash from sswor
Oompare Hash Werte
XOR
unequal
Reply with HTTP status 401 (Not authenticated)
equal
Crea1:e Session und Rep mit Se ionID und.....
fonAfard zur Benutzerseite-
XOR
Re uest prooe5sed

GRÜNDE FÜR DIE HEILIGSPRECHUNG

Gültige Darstellung des Zeichens **<** in HTML

%3C
&lt
<
&LT
<
&#60
&#060
&#0060
&#00060
&#000060
&#0000060
<
<
<
<
<
<
&#x3c
&#x03c
&#x003c
&#x0003c
&#x00003c
<
<
<
<
<
<
&#X3c
&#X03c
&#X003c
&#X0003c
&#X00003c
&#X000003c
<
<
<
<
<
<
&#x3C
&#x03C
&#x003C
&#x0003C
&#x000003C
<
<
<
<
<
<
&#X3C
&#X03C
&#X003C
&#X0003C
&#X00003C
&#X000003C
<
<
<
<
<
<
\x3c
\x3C
\u003c

&#x000003c

&#x00003C

\u003C

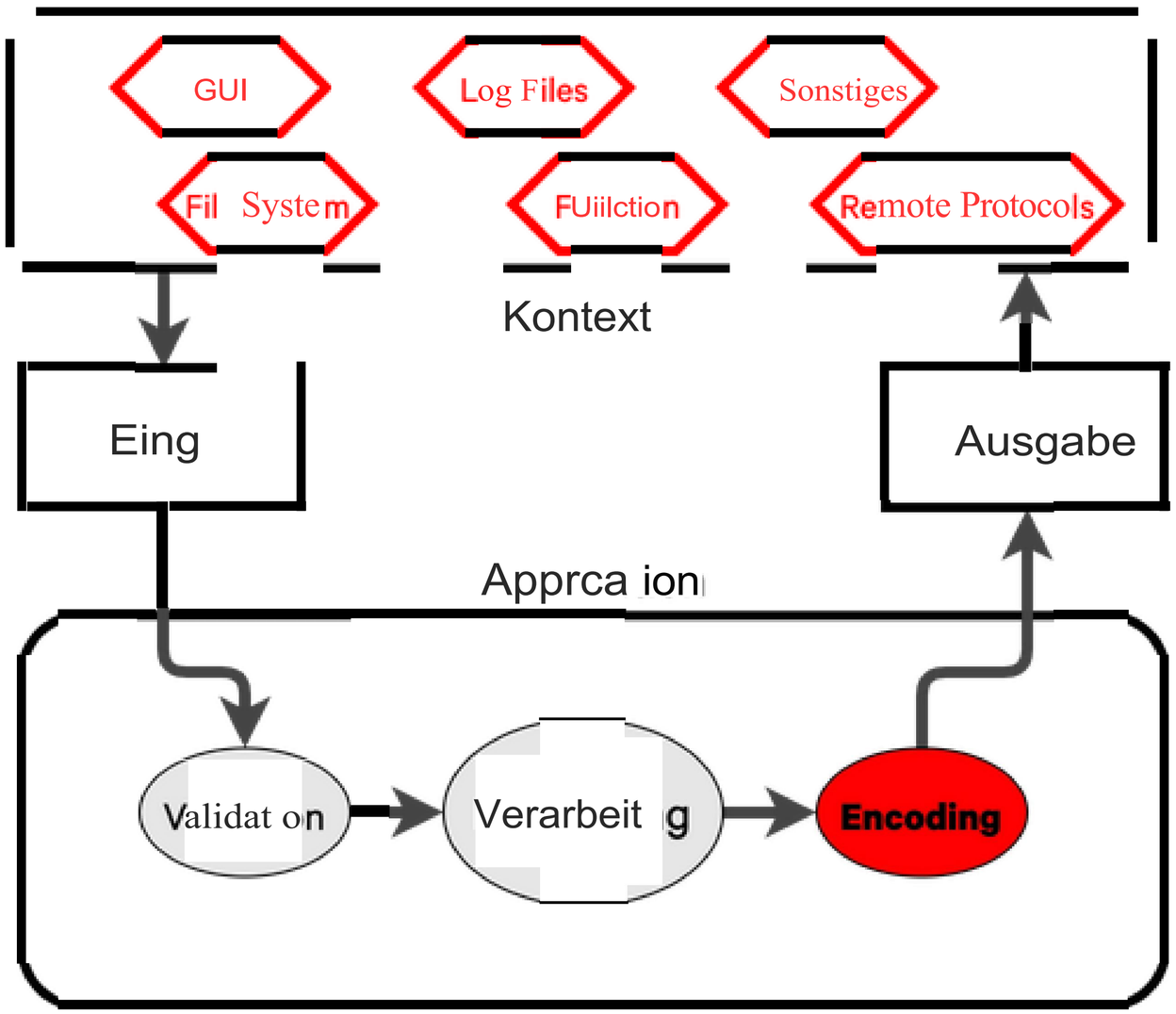
KODIERUNGEN OBENAUF

Kodierung	Kodierter Text
klar	Demo Text<TAG attr='value' />
URL	%22Demo%20Text%22%3cTAG%20attr='value'%20/%3e
URL-Hex	%22%44%65%6d%6f%20%54%65%78%74%22%3c …
URL-Unicode	%u0022%u0044%u0065%u006d … %u003c …
HTML-benannt	&quotDemo Text&quot&ltTAG attr&equals'value' &sol&gt
HTML-Dezimal	&#34&#68&#101&#109&#111&#32 … &#60 …
HTML-Hex	&#x22&#x44&#x65&#x6d&#x6f&#x20 … &#x3c …
HTML-Hex lang	&#x0022&#x0044&#x0065&#x006d … &#x003c …
JS entkam	\"Demo Text\"<TAG attr=\'value\' />
XML entkommen	"Demo Text"<TAG attr='value' />

CHAPTER TITLE

DAS GOLDENE TICKET UNSCHARF MACHEN

AUSGANGSKODIERUNG


GUI
Log Files
Sonstiges
Fil System
FUiilction
Remote Protocols
Kontext
Eing
Ausgabe
Apprca ion
Validat on
Verarbeit g
Encoding

DRIVER

STUCKIN ADEADEND

"Aber das Navigationssystem sagte ..."

FREE BEER
imgflip.com

WAS KODIERT WERDEN MUSS

Befehlssignaturen und Sonderzeichen, die für den Parser befehlsähnliche Auswirkungen haben.

Code: <script>… <script>

- In Band gesungene Befehle: DROP TABLE
- Zeichen wie: ; , Leerzeichen, Return

EIN ALLGEMEINER ANSATZ

1. Ausgabeziel entdecken
2. Annahmen über die Ausgabeverarbeitung explizit machen
3. Ausgabe entsprechend kodieren
4. Sicherstellen, dass die Dekodierung ordnungsgemäß

funktioniert

1. Gegebenenfalls Überprüfung auf Angriffsmuster
2. Entscheiden Sie sich für die Validierung
3. Kodierung in der Nähe des Kontextübergangs

CHAPTER TITLE

WARUM FILTER SCHLECHT FÜR DIE LEISTUNG SIND

SCHLUSSFOLGE

ZUM MITNEHMEN

- Festlegung einer Code-Sicherheitspolitik
- Ableitung technologiespezifischer Sicherheitsrichtlinien für Entwickler und Prüfer
- Entwickler brauchen geeignete Anforderungen, um sicheren Code zu erstellen. Durchsetzung von Sicherheitstechnik und -design im Entwicklungsprozess
- Prüfen Sie auch die Codesicherheit von externen Anbietern
- Einrichtung und Automatisierung von Codequalitäts- und Sicherheitstests für die gesamte Software-Pipeline

ENDE

VERSTEHEN DES GEGNERS

Lernziele

- Verstehen, wie das MITRE Attack Framework als mittlerer Ansatz zur Angriffssimulation und -reaktion verwendet werden kann.
- Bestimmung der tatsächlichen Techniken anhand von Beispielen von Sicherheitsereignissen.

- Bestimmen Sie anhand von Beispielen mögliche gegnerische Taktiken.

Grundlagen der Cyber Kill Chain

Einführung in die Cyber-Kill-Chain

Was ist die Cyber-Kill-Chain, und warum verwenden wir sie?

Einführung in Threat Intelligence

Was sind Bedrohungsdaten und was können Sie damit anfangen?

Der MITRE ATT&CK-Rahmen

Eine Einführung in MITRE ATT&CK als Rahmenwerk auf mittlerer Ebene zur Operationalisierung der Sicherheit

MITRE ATT&CK in Betrieb nehmen

Ein Überblick über die Optionen zur Nutzung und zum Start von MITRE ATT&CK

Schlussfolgerung

EINFÜHRUNG IN DIE CYBER KILL CHAIN

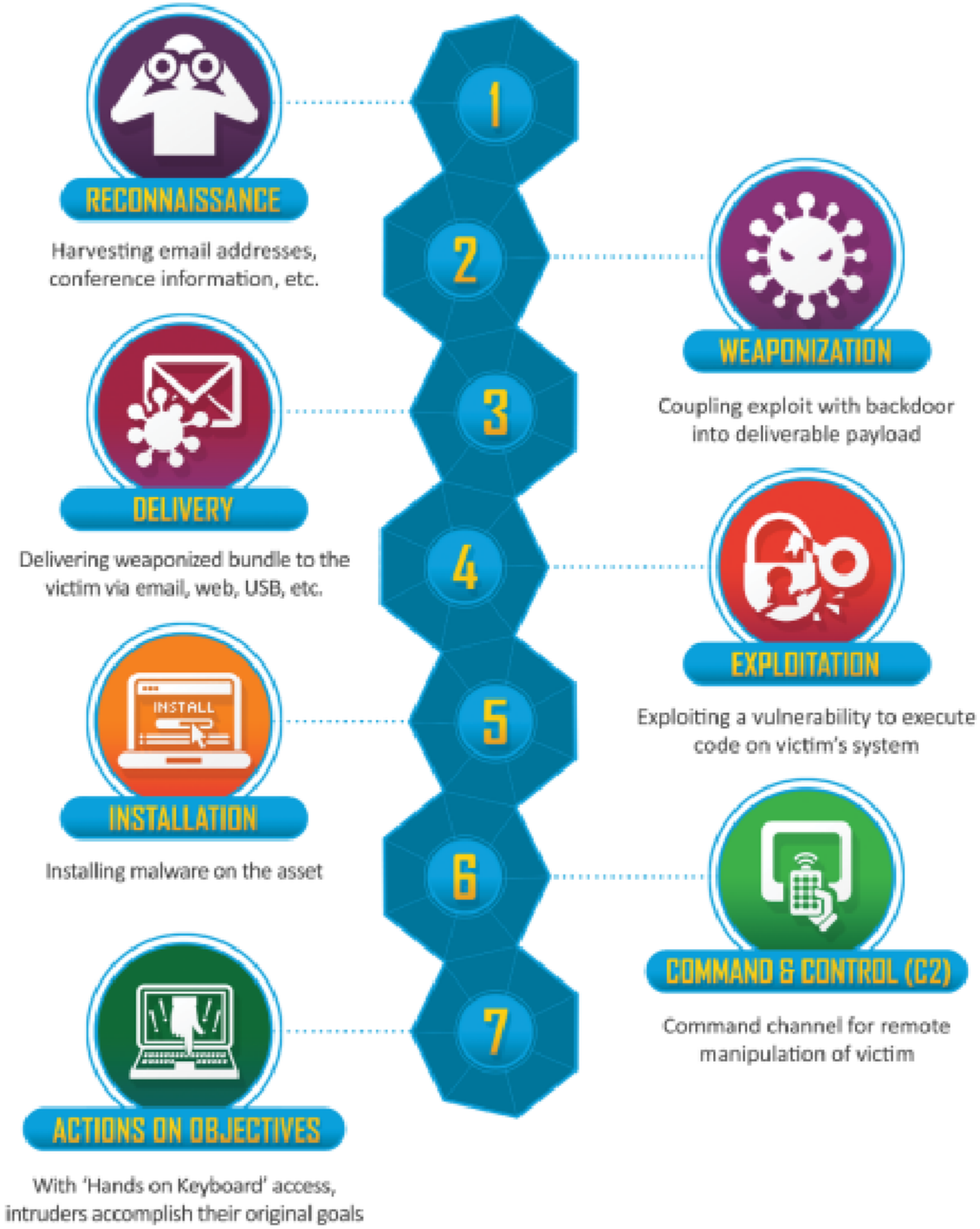
Cyber Kill Chain

- Abgeleitet aus militärischen Operationen
- Erstmals von Lockheed Martin im Jahr 2011 eingeführt
- Erweitert und vereinigt mit dem MITRE ATT&CK-Rahmenwerk

- Vorteile:
- Positionierung von Sicherheitskontrollen auf der Grundlage des Rahmens

Dieses Foto CC BY-ND

Lockheed Martin Kill Chain



EINFÜHRUNG IN DIE BEDROHUNGSANALYSE

Intelligente Bedrohung

- Härtet die Cyberabwehr durch:
  - Daten über Taktiken, Techniken und Verfahren des Gegners
    - Malware-Hashes
    - Bekannte bösartige Domains / Ips
    - Bekannte Ausbeutungskampagnen
    - …

Dieses Foto von Unbekannter Autor ist lizenziert unter CC

BY-NC

Quellen für Bedrohungsdaten / Protokolle / Tools

STIX

Strukturierte Bedrohungsinformationsexpression.
Der Name ist eindeutig: Es handelt sich um einen Standard zur strukturierten und eindeutigen Darstellung von Informationen über Computerbedrohungen.
Basierend auf JSON

TAXII

Trusted Automated Exchange of Intelligence Information, ist ein Protokoll für den Austausch nachrichtendienstlicher Informationen über HTTPS. Der Standard definiert eine Reihe von Anforderungen für Clients/Server und eine REST-API

MITRE-KRITIKEN

CRITs ist ein Open-Source-Repository für Malware und Bedrohungen, das andere Open-Source-Software nutzt, um ein einheitliches Tool für Analysten und Sicherheitsexperten zu schaffen, die sich mit der Abwehr von Bedrohungen beschäftigen.

DER MITRE ATT&CK-RAHMEN

MITRE ATT&CK Rahmenwerk

ATT&CK - Taktiken, Techniken und allgemeines Wissen des Gegners

Konzentriert sich auf TTPs (Taktiken, Techniken und Verfahren)

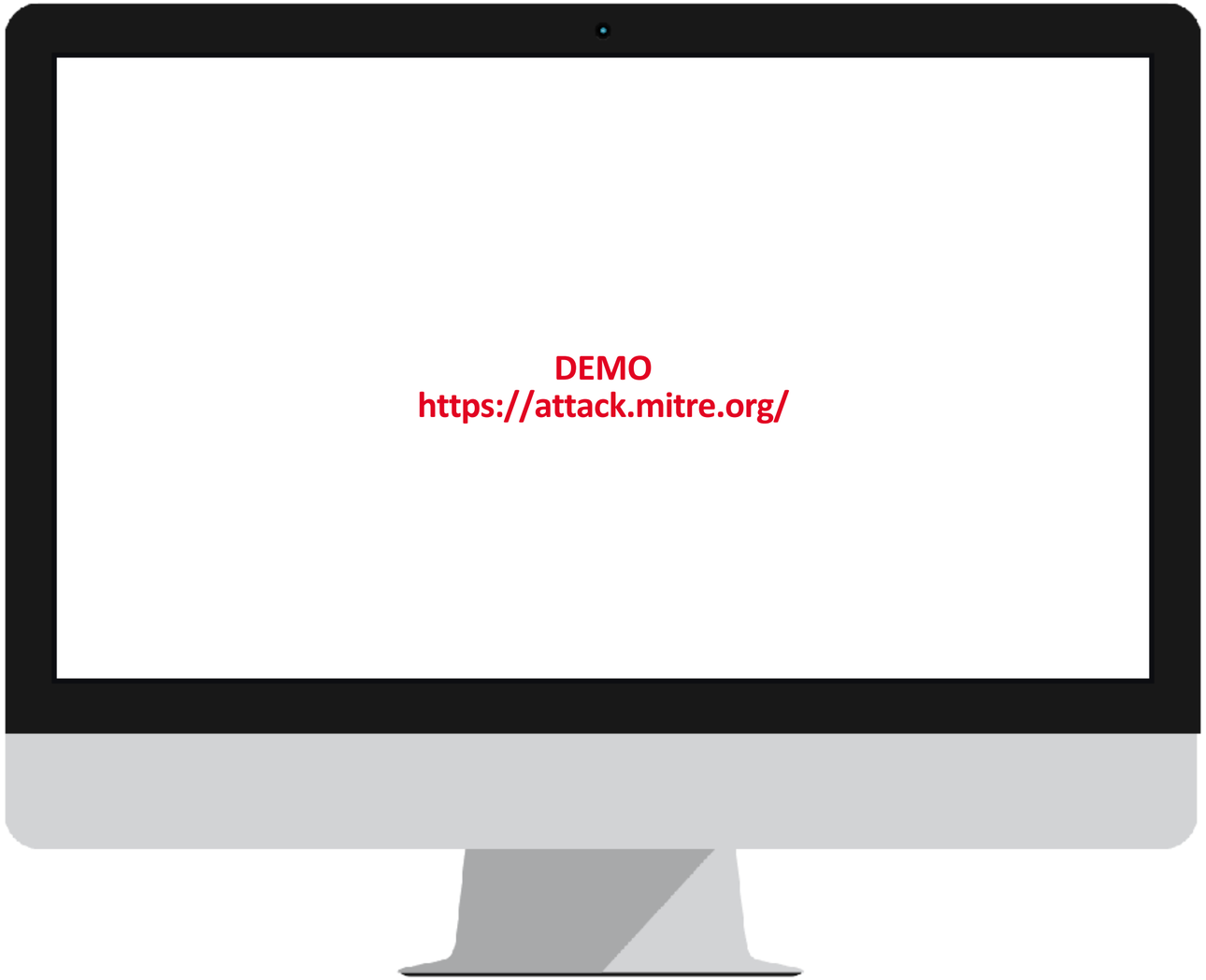
Unterstützung der blauen Teams bei der

- Leichtere Erstellung von Anwendungsfällen
- Identifizierung fehlender Sicherheitskontrollen oder -

Rote Teams können Emulationen durchführen

Violette Teams kombinieren die Funktionen von roten und

MITRE ATT&CK Rahmenwerk



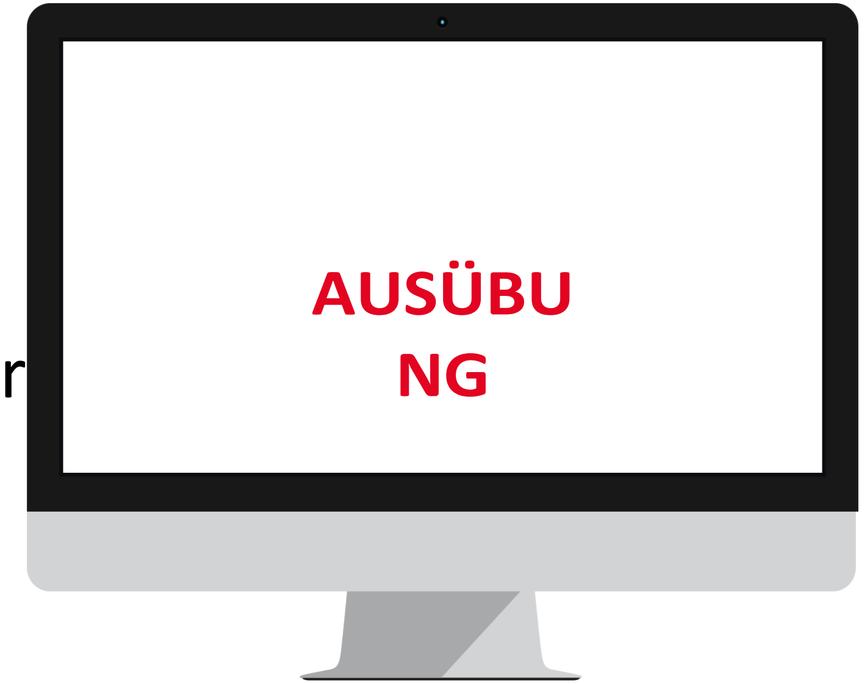
Praktische operative Tätigkeiten

1. Intelligente Bedrohung
2. Erkennung und Analyse
3. Emulation des Gegners und Red Teaming

Intelligente Bedrohung

- Wir untersuchen einen Vorfall in unserem Unternehmen und haben festgestellt, dass er mit einer Bedrohungsgruppe namens Fox Kitten zusammenhängt. Nachdem sie sich Zugang zum Netzwerk verschafft hatten, konnten sie mit den systeminternen Windows-Tools (PsExec) ein Domänenkonto erstellen, um den Zugang zum Netzwerk aufrechtzuerhalten.

1. Navigieren Sie zu den Bedrohungsgruppen auf der Mitre-Website (https://attack.mitre.org/groups/)
2. Suchen Sie im Szenario nach der Bedrohungsgr
3. Finden Sie die Software, die sie für die Aufrechterhaltung des Zugangs verwendet haben, und nennen Sie vier Techniken, für die das Tool verwendet werden kann
4. Sehen Sie sich den ATT&CK-Navigator in der Vorschau an, um festzustellen, für



welche Taktiken das Tool nützlich sein kann

OPERATIONALISIERUNG VON GEHRUNGSATT&CK

Emulationsprozess:

Wählen Sie
- Wählen Sie eine Technik

Wählen Sie
- Wählen Sie die Art der

Test
- Testen Sie das Verfahre

Analysieren Sie
- Analysieren Sie die

Verbessern Sie
- Verbesserung der

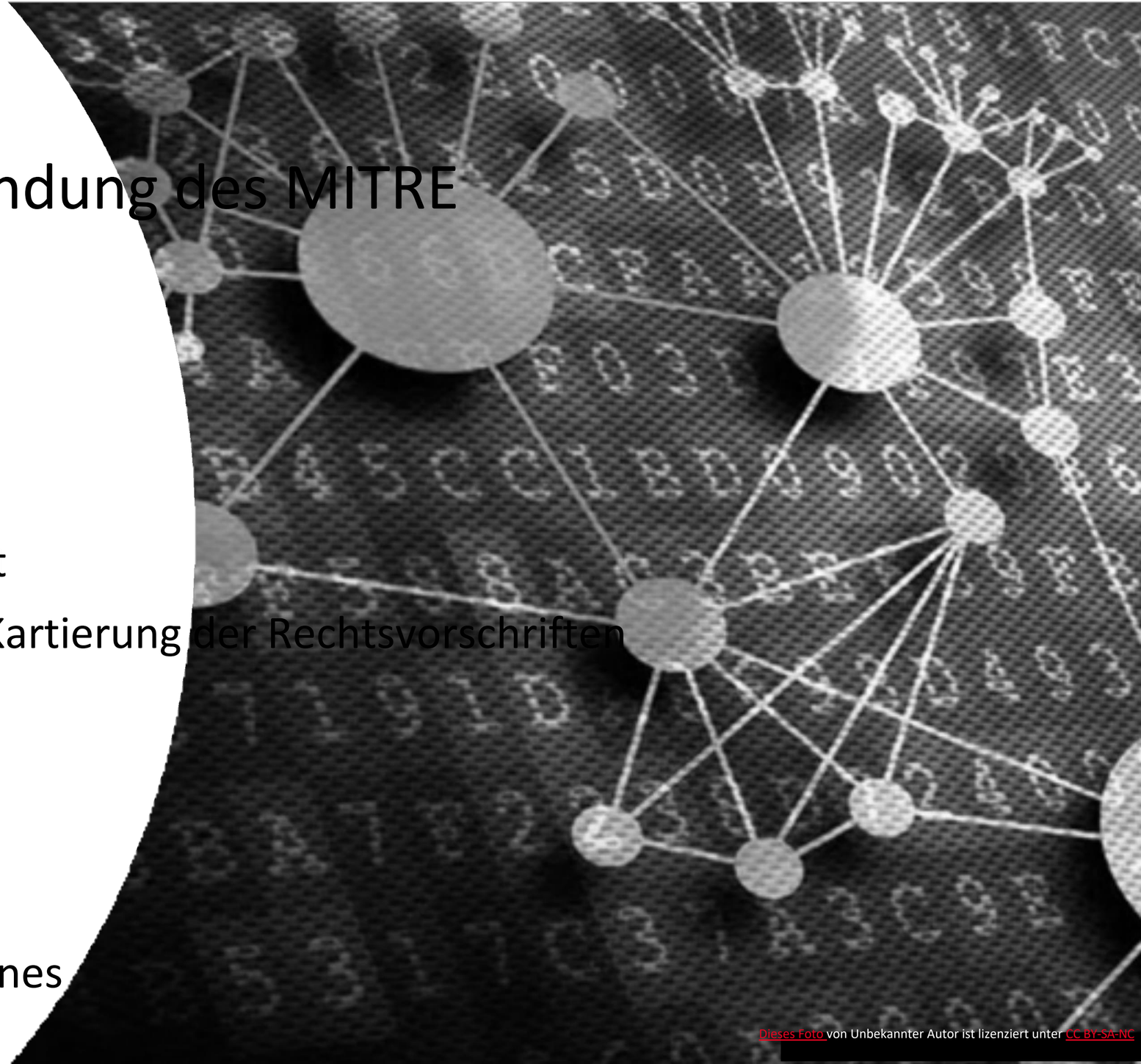
Emulationswerkzeuge und Bibliotheken

- AtomicAtomic Red
- CALDERA von MITRE
- MITRE Engenuitys Adversary-Emulationsbibliothek

Dieses Foto von Unbekannter Autor ist lizenziert unter CC BY-NC

Möglichkeiten der Anwendung des MITRE ATT&CK

- Intelligente Bedrohung
- Jagd auf Bedrohungen
- Automatisierte Prüfung und Audit
- Einhaltung der Vorschriften und Kartierung der Rechtsvorschriften
- Risikomanagement und Strategie
- Ausbildung und Übungen
- Priorisierung und Bewertung von Sicherheitslösungen
- Validierung von Sicherheits-Pipelines



Dieses Foto von Unbekannter Autor ist lizenziert unter CC BY-SA-NC

SCHLUSSFOLGERUN

Schlussbemerkungen

- **Kenne deine Feinde**

  Cyberangriffe sind real und Sie sollten Ihre Verteidigung gegen Angriffe aus der realen Welt organisieren

- **Emulation als Ansatz zur Schaffung von Sichtbarkeit**

  Die Emulation eines Angreifers kann einfach sein. Verstehen Sie, was für Sie wichtig ist, um zu sehen und zu überprüfen, ob Sie es tun

- **Sie kontrollieren MITRE ATT&CK**

  Es handelt sich um einen Best-Practice-Ansatz, der Sie auf Ihrem Weg begleiten soll. Es ist nicht dazu gedacht, alle Kästchen abzuhaken

- **Es kostet kein Vermögen**

  Das Sammeln von Bedrohungsdaten kann beginnen, ohne dass ein kommerzieller Dienst abonniert werden muss.

ENDE

GEGENMASSNAHMEN UND TÄUSCHUNGSMANÖVER FÜR DEN VERTEIDIGER

Lernziele

- Lernen Sie den Unterschied zwischen aktiver und passiver Verteidigung und Prävention
- Lernen Sie das allgemeine Konzept der OODA-Schleife kennen und wie es als Modell zur Abwehr von Angriffsstrategien funktioniert
- Verstehen des Konzepts der Endpunkt-Erkennung und -Reaktion (EDR)
- Verstehen des allgemeinen Konzepts der Bedrohungsanalyse
- Lernen Sie die grundlegenden Konzepte und Vorteile von SOAR (Security Orchestration, Automation and Response) kennen.
- Befolgen Sie den gesamten Lebenszyklus eines Vorfallsreaktionsplans, um einen Vorfallsreaktionsplan und/oder eine Aktivität auf der

Grundlage eines erfolgreichen Angriffsszenarios zu erstellen.

Kapitel

Taktik des Verteidigers

Überblick über Verteidigungstaktiken für die aktive und passive Verteidigung

Die OODA-Schleifen des Verteidigers

Eine Einführung in die OODA-Schleife als Gegenstrategie zur Cyber-Kill-Chain

Der Werkzeugkasten des Verteidigers

Überblick über die Endpunkt-Erkennung und -Reaktion (EDR) als Teil von SOAR

Schlussfolgerung

TAKTIK DES VERTEIDIGERS

Passive Verteidigung und Prävention

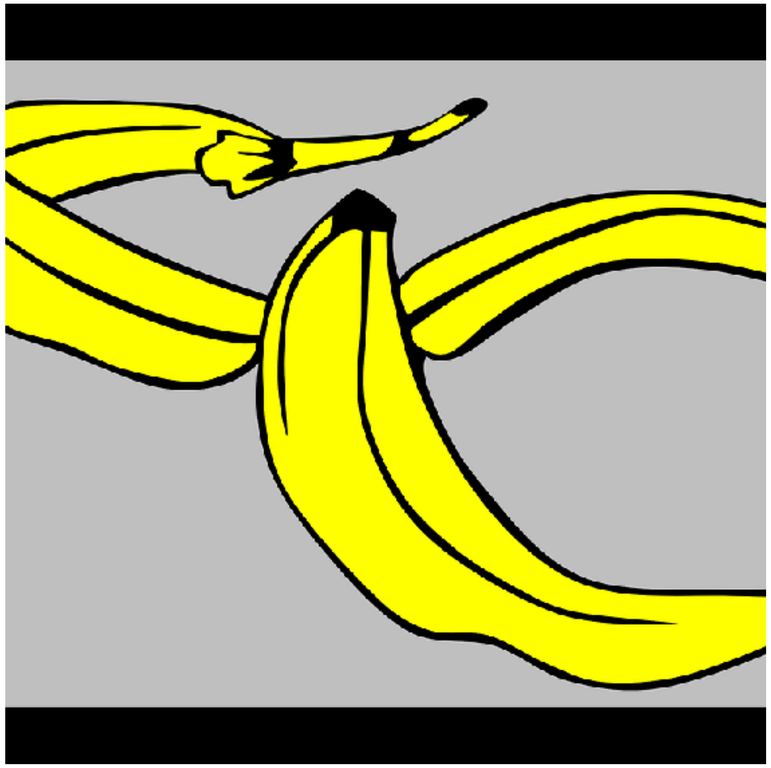
Maßnahmen, die ergriffen werden, um die Wahrscheinlichkeit von Schäden durch feindliche Handlungen zu verringern und deren Auswirkungen zu minimieren, ohne die Absicht, die Initiative zu ergreifen (d. h. auf das Beste zu hoffen)

- Netzwerk-Zugangsmanagement
- Geräte-Management
- Identitätsmanagement
- Verweigern- Zulassen-Listening
- Schwachstellen- und Patchmanagement
- Aushärtung
- Lockpolicies
- …

Aktive Defensiv- und Offensiv-Gegenmaßnahmen

- Der Einsatz begrenzter Offensivaktionen und Gegenangriffe, um dem Feind ein umkämpftes Gebiet oder eine umkämpfte Stellung zu verweigern.
- Proaktive, vorausschauende und reaktive Maßnahmen gegen Angreifer
- Die Widersacher haben die Tore bereits durchbrochen...
- Offensive Gegenmaßnahmen setzen offensive Techniken ein, während die Angreifer in einer defensiven Haltung angreifen.

Offensive Gegenmaßnahmen - Cyber-Täuschung



Bewusster und kalkulierter Prozess der Täuschung von Angreifern in dem Bemühen, eine bessere Verteidigung zu erreichen

- Verlangsamen Sie sie, verwirren Sie sie, täuschen Sie sie ... lassen Sie sie härter arbeiten - Das erhöht Ihre Chancen auf Entdeckung erheblich
- Entwickelt, um die $\text{Erkennung}_t + \text{Reaktion}_t < \text{Angriff}_t$ ($D_t + R_t < A_t$)
- Es ersetzt keine anderen Bemühungen oder Verteidigungsschichten
- Sie sollte die anderen Schichten ergänzen und nähren

- Seit Anbeginn der Zeit haben Militärs Täuschungsstrategien eingesetzt. Warum tun wir das nicht auch?

Brian Krebs

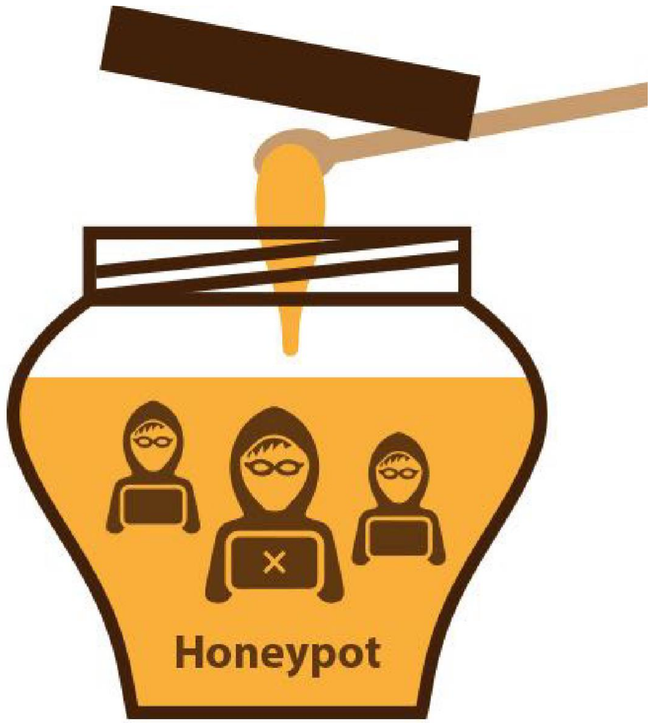
"Täuschungstechnologien sind nett, aber nur dann ratsam, wenn Ihr Unternehmen bereits 99 % des Restes erledigt.

"Es gibt einen offensichtlichen Mangel an Täuschungstechnologie".

Jeff Moss

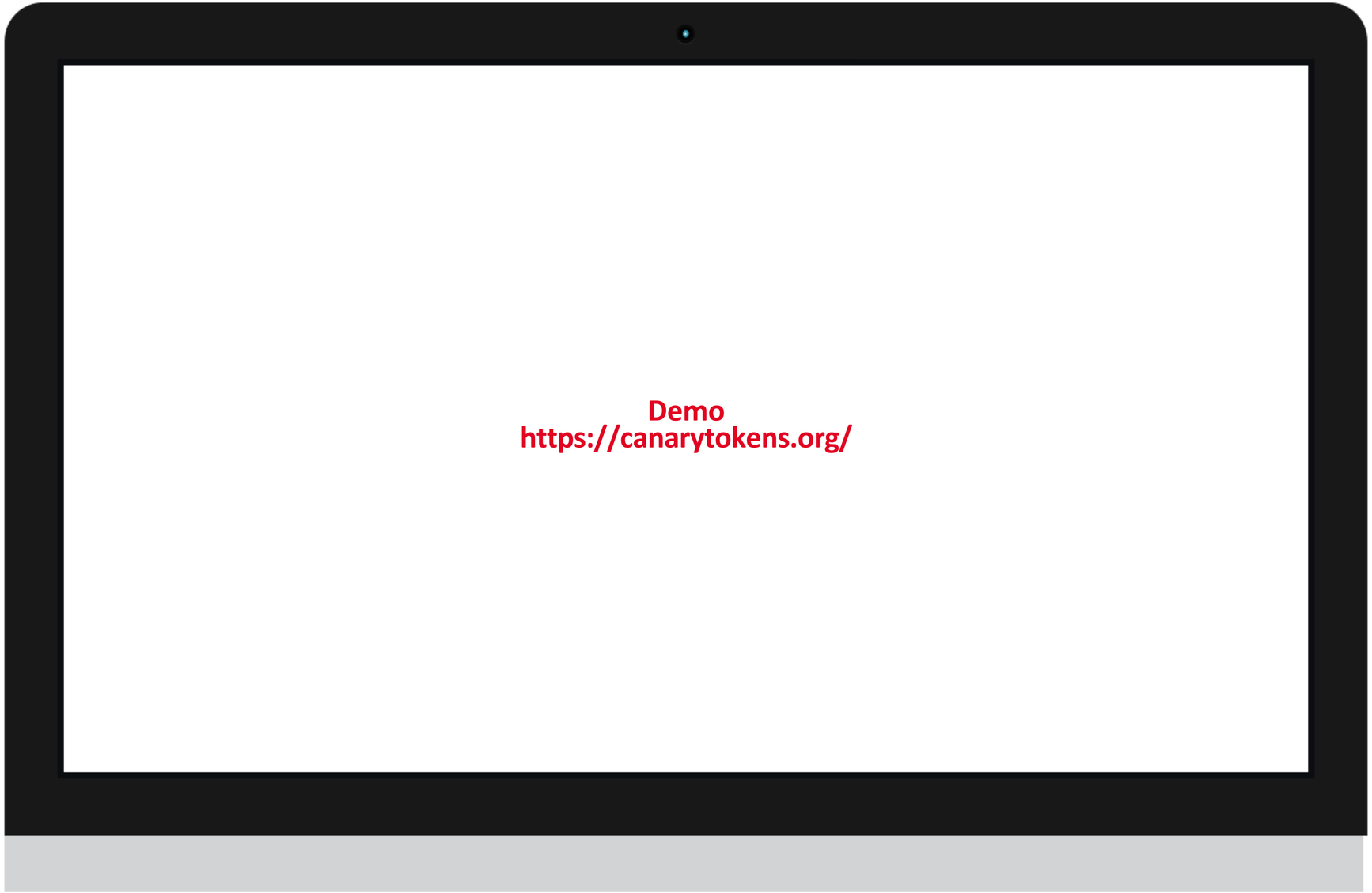
Offensive Gegenmaßnahmen - Cyber-Täuschung

- Honey Ports / Dienstleistungen / Töpfe / Netze
- Honey Docs / Benutzer
- Gegenangriffe
  - Malware
  - …
- Zuschreibung
  - Kanarienvogel-Münzen
  - Interne Bedrohungsanalyse



Schon eine Idee?

Kanarienvogel-Token



NVIDIA Counter Hack

Nvidia hacked by ransomware group, steals its stolen data back

by Chadley Kemp

Sources suggest that Nvidia launched a cyber attack on hacker group Lapsu$ after the hackers stole 1TB of proprietary data.

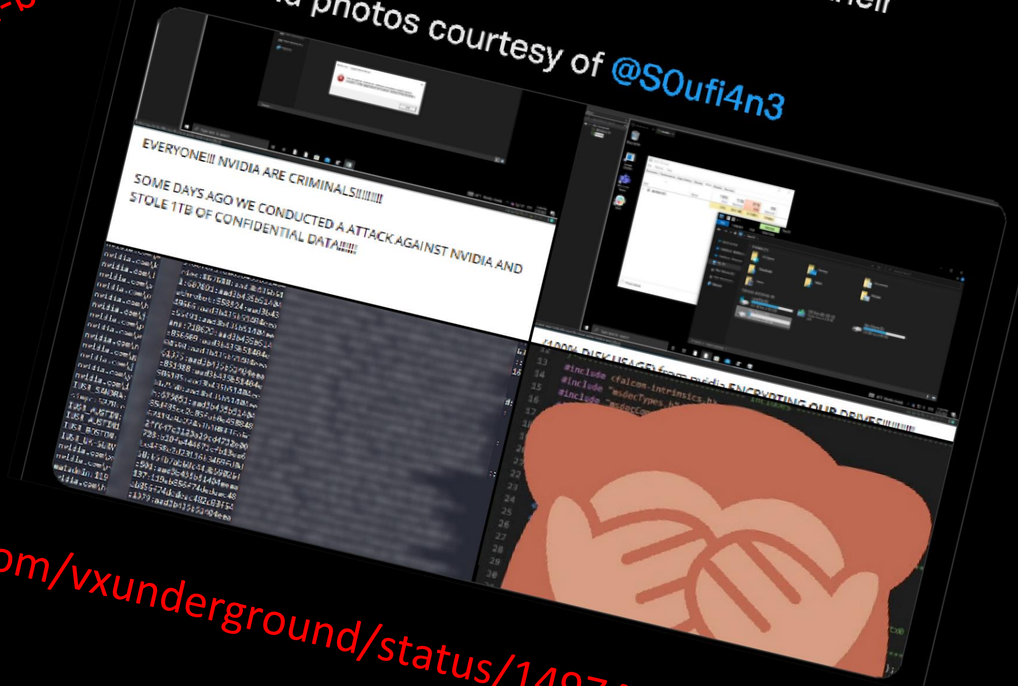
https://www.ginx.tv/en/video-games/nvidia-hacked-ransomware-steals-data-back

vx-underground
@vxunderground

LAPSU$ extortion group, a group operating out of South America, claim to have breached NVIDIA and exfiltrated over 1TB of proprietary data.

LAPSU$ claims NVIDIA performed a hack back and states NVIDIA has successful ransomed their machines

Intel and photos courtesy of @S0ufi4n3



https://twitter.com/vxunderground/status/1497484483494354946

Offensive Gegenmaßnahmen - rechtliche Perspektive

Mit ein paar einfachen Tipps kann man viel erreichen...

- Verteilen Sie Malware nicht an öffentlich zugänglichen Orten.
- Vermeidung von Kollateralschäden
- Bringen Sie die Angreifer dazu, zuerst zu Ihnen zu kommen
- Verwendung von Warnbannern und Nutzungsbedingungen (TOU)

- Warnung vor "bösen" Dingen im Netz
- Konsultieren Sie einen Anwalt

Dieses Foto ist lizenziert unter CC BY-ND

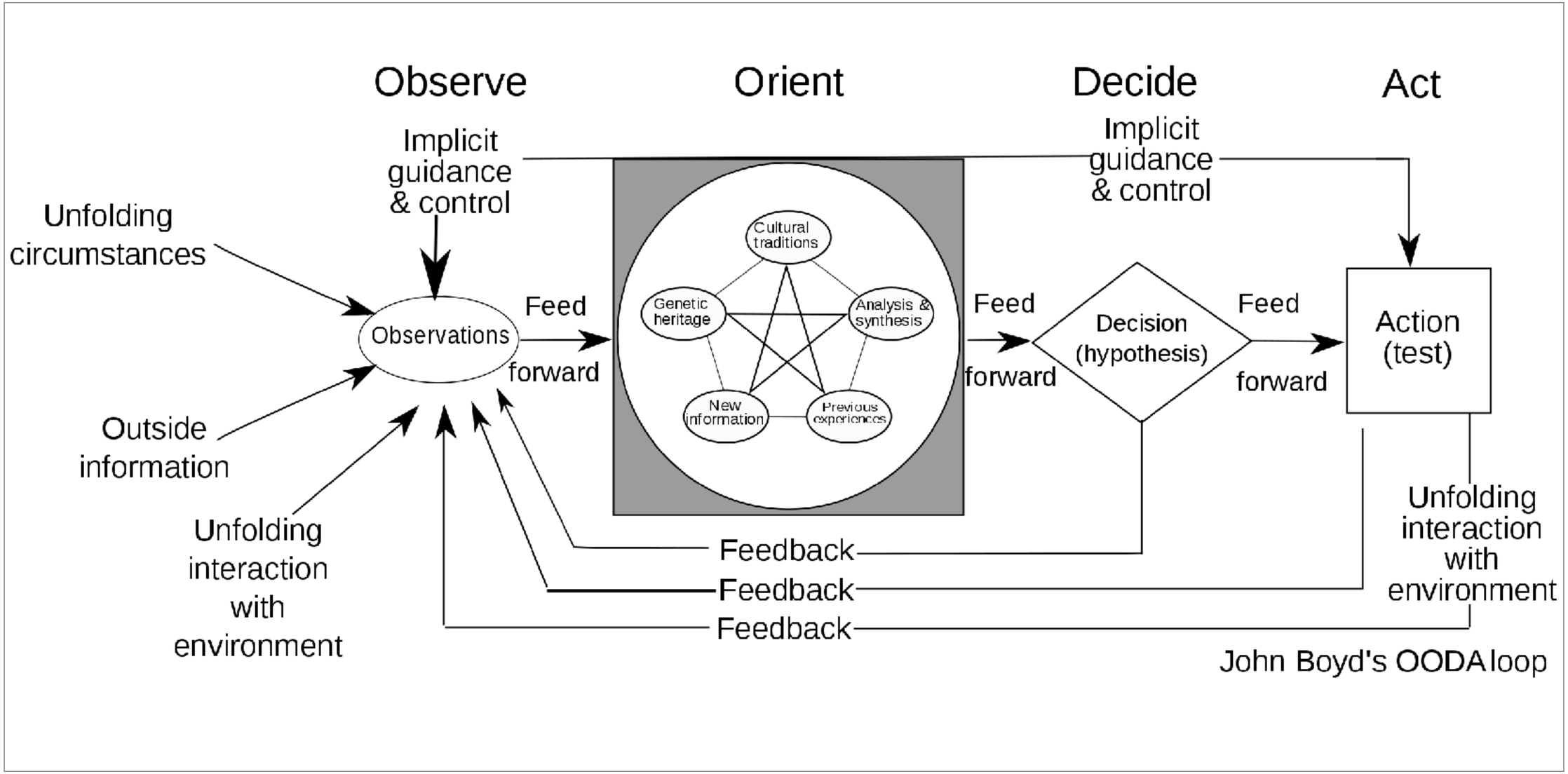
DIE OODA-SCHLEIFE

Die Cyber-OODA-Schleife

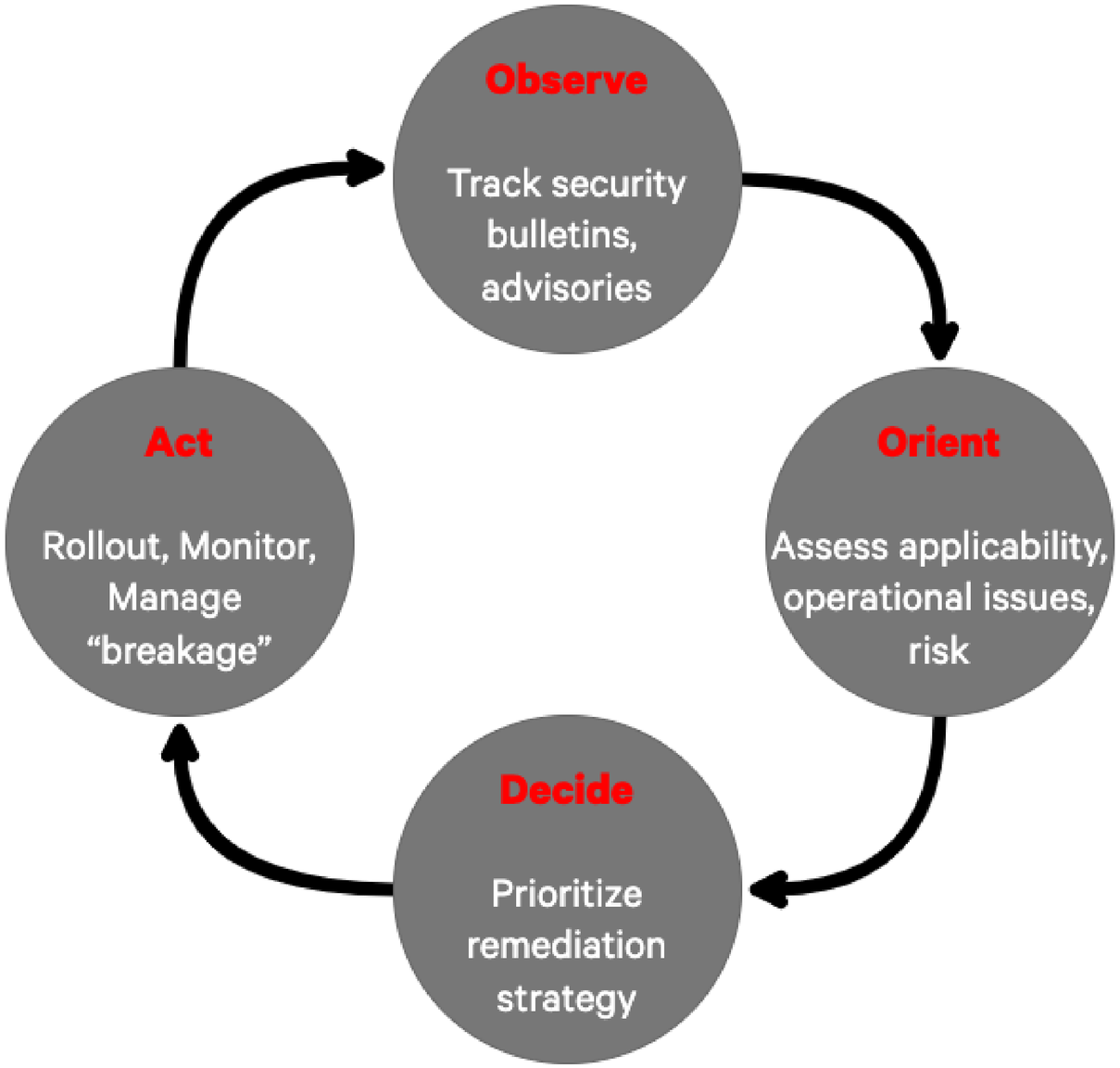
Wie Ihr Angreifer Ihnen helfen sollte, Ihre Verteidigung zu gestalten, denn:

$$Risk = f\{\frac{Vulnerability,\ Threat,\ Consequence}{countermeasures}\}$$

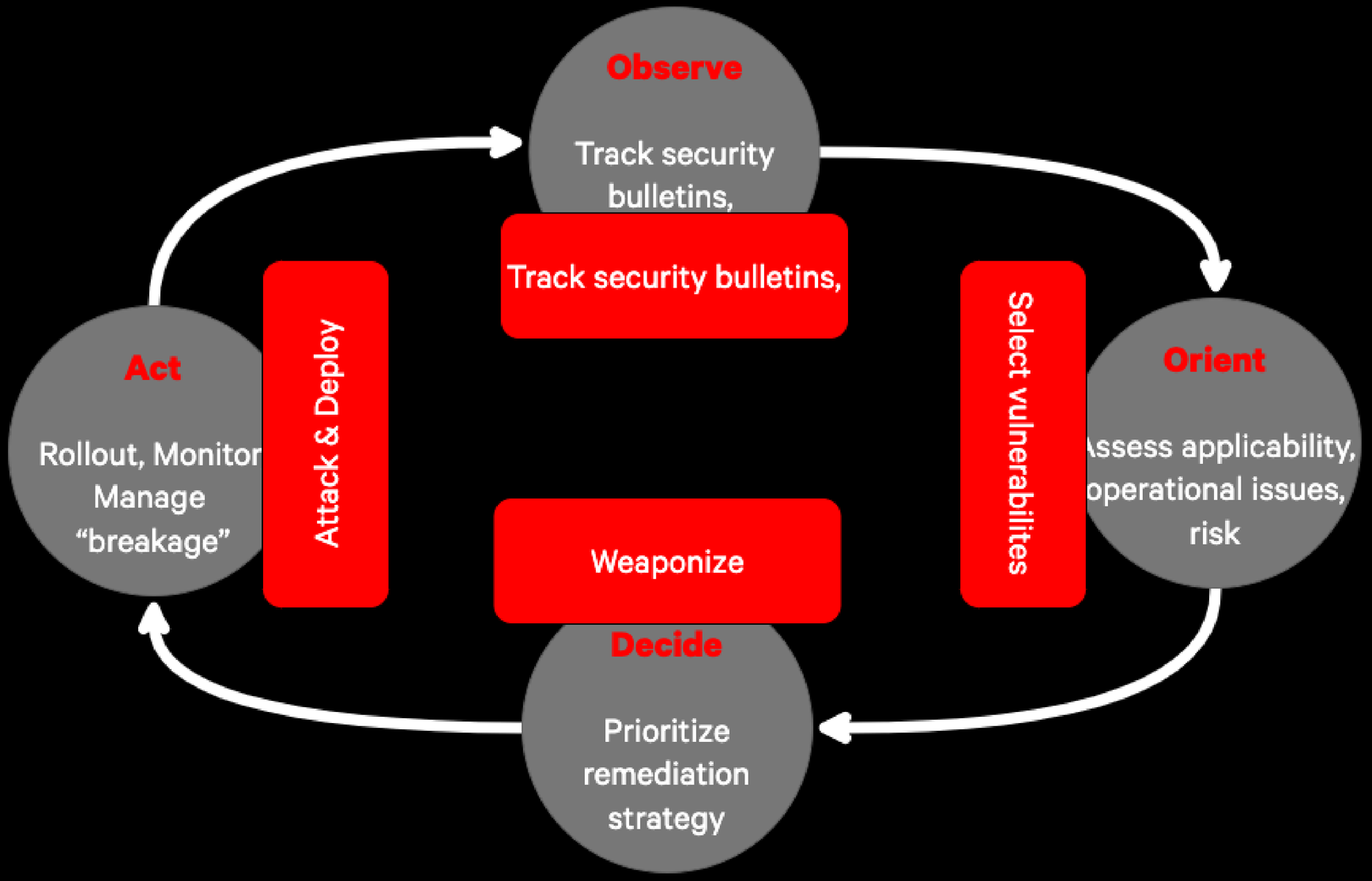
Die allgemeine OODA-Schleife



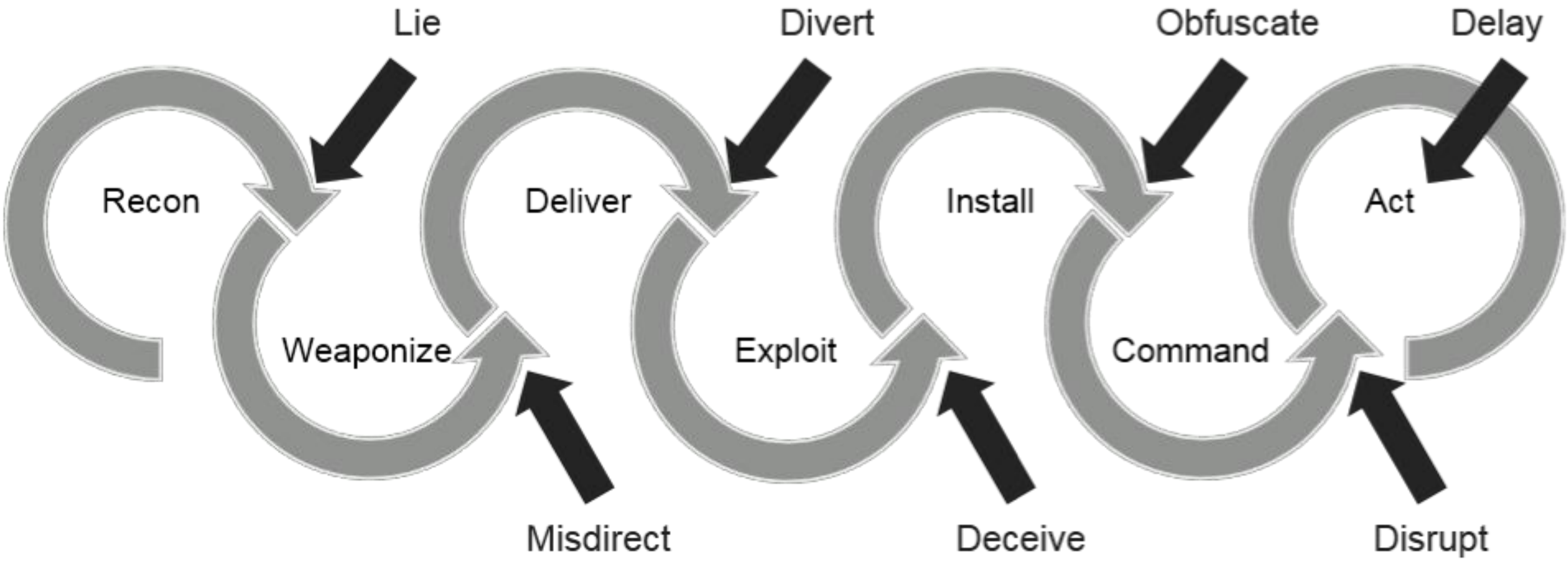
Patching-Schleife



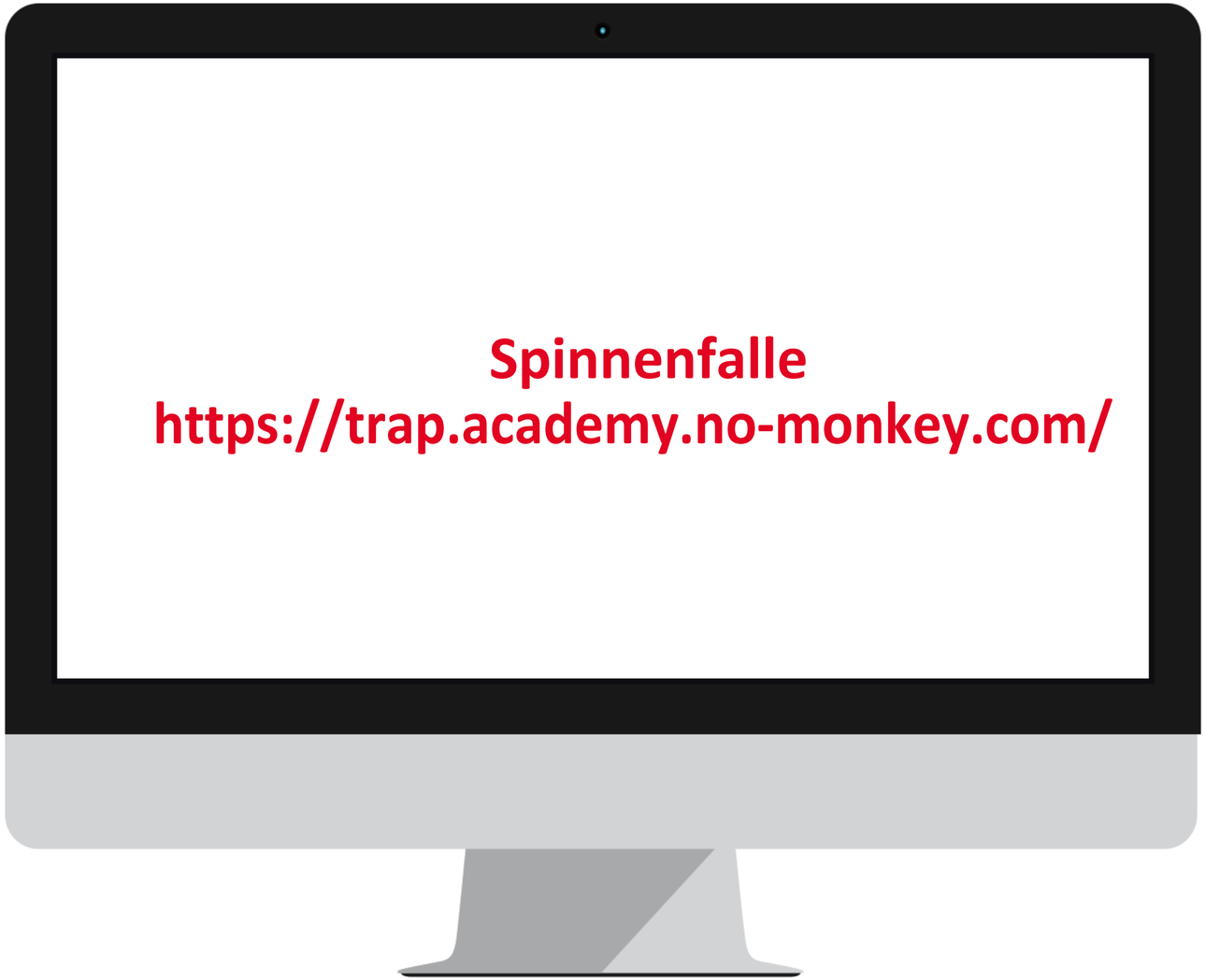
Patching-Schleife - Angreiferperspektive



Das OODA-System des Angreifers durchbrechen



Demo

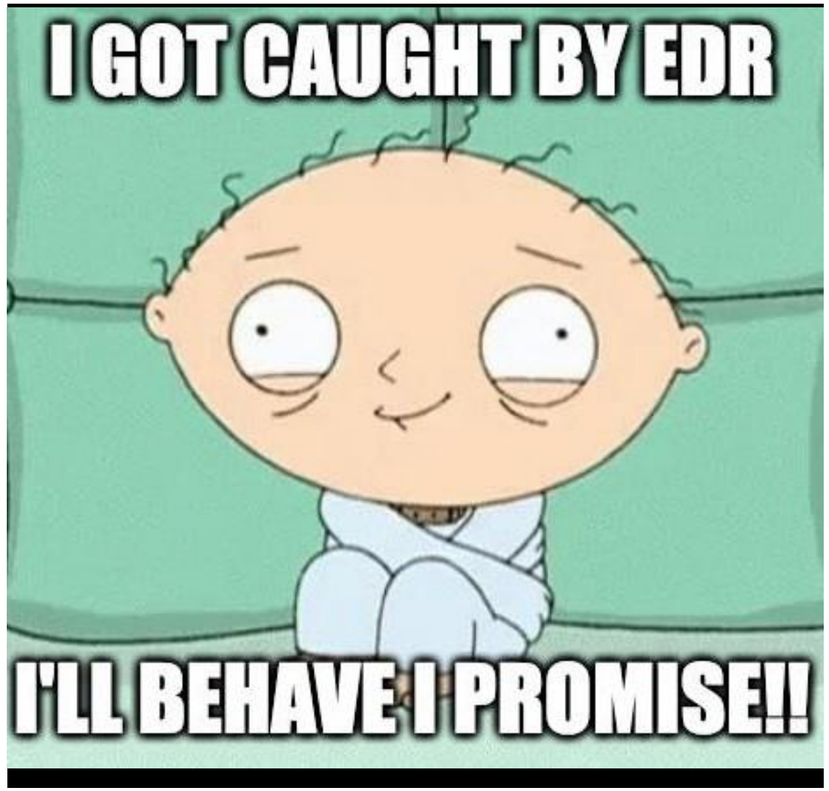


DER WERKZEUGKASTEN DES VERTEIDIGERS

Warum Endpoint Detection & Response

Denn ohne sie wird die Reaktion auf Vorfälle sehr schwierig.
Bei EDR geht es mehr um Fähigkeiten als um Tools

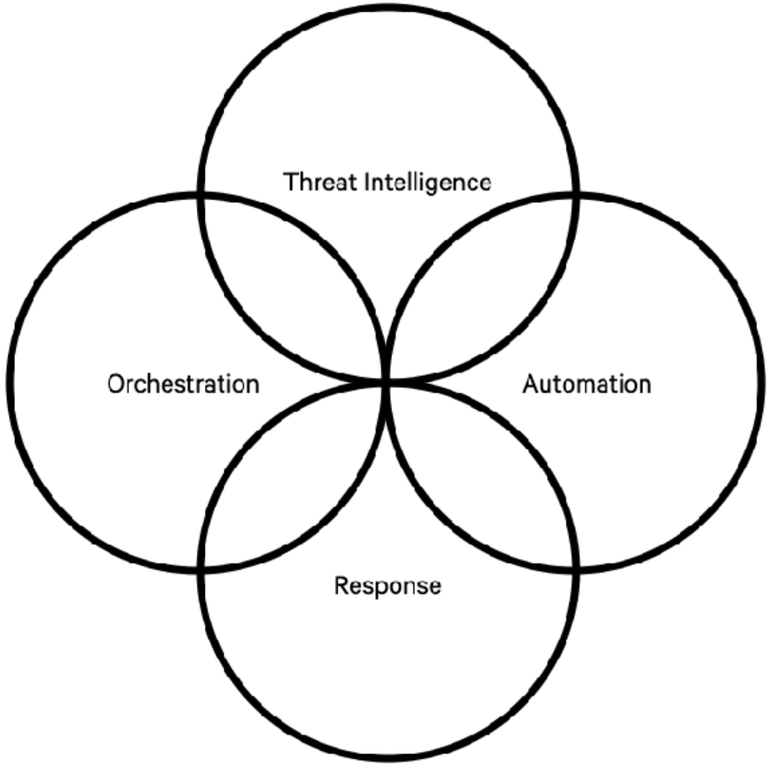
- Schnelles Abrufen von Informationen aus mehreren Quellen
- Korrelieren von Ereignissen von verschiedenen Endpunkten und Bereitstellen von Bedrohungsdaten
- Kombination von signaturbasierter und verhaltensbasierter Malware-Erkennung mit der Bewertung des Nutzerverhaltens
- Blockierversuche für seitliche Bewegungen



Was ist mit eXtended Detection and Response (XDR)?

EDR-Lösungen im Vergleich

Warum Security Orchestration, Automation und Response?



Denn ohne sie lässt sich die Reaktion auf Vorfälle nicht skalieren und wird zu langsam. Bei SOAR geht es mehr um Fähigkeiten als um Tools

- Sicherheitsinformationen aus verschiedenen Quellen verständlich und nachvollziehbar machen
- Verringern Sie die Ermüdung des Sicherheitsbetriebs, indem Sie die langweiligen Dinge automatisieren.
- Definiert einen Prozess zur Erstellung von Playbooks

Warum ist dies kein SIEM?

Aufschlüsselung - Warum SOAR

Orchestrierung der Sicherheit

- Sicherheitsinformationen aus verschiedenen Quellen sind nicht normalisiert
- Die IT-Landschaft wird heterogen und wächst
- Der Betrieb weiß nicht, welche Vermögenswerte für das Unternehmen am wichtigsten

sind

Automatisierung und Reaktion

- Verkürzung der Reaktionszeit durch Verwendung von Playbooks und Automatisierung von Aktivitäten
- Verringerung des Zeitaufwands für die Schadensbegrenzung durch Automatisierung sich wiederholender Arbeiten
- Automatisieren Sie die Erkennung auf der Grundlage von koordinierten Sicherheitsinformationen.

SCHLUSSFOLGERUN

Schlussbemerkungen

- **Denken Sie wie ein Angreifer**
  Sie sind Menschen. Verstehen Sie, wovor sie Angst haben, was sie demotiviert und ihnen das Leben schwer macht
- **Eindämmung erfordert Koordination**
  Es gibt keine einzige Maßnahme zur Eindämmung einer Sicherheitsverletzung in Ihrem Netz. Die Kommunikation untereinander verstehen und aufeinander abstimmen
- **Das ist keine Raketenwissenschaft**
  Sie tun bereits eine Menge. Nutzen und testen Sie alle Taktiken, die in Ihrem Umfeld anwendbar sind.
- **Aktive Verteidigung ist auch für kleine Unternehmen wichtig**
  Wenn Sie es sich nicht leisten können, zu fliehen oder eine SOC zu bezahlen, ist das vielleicht die einzige Möglichkeit zu erkennen, ob jemand wirklich hinter Ihnen her ist.

ENDE