Cyber Threat Analysis

Wer, wie, wo, was, warum, weshalb? 🎶

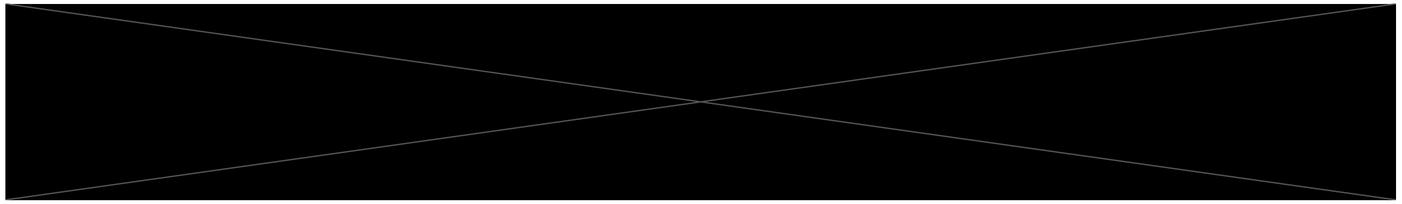
What could possibly go wrong?

The answer is: absolutely everything.

- **Meine kürzeste Woche seit Anfang August waren 54 Wochenstunden**
  - “Diamanten entstehen unter Druck” par excellence
- **Sticker bei drei verschiedenen Anbietern bestellt**
  - Einmal storniert, einmal vergessen zu drucken, ein Paket verloren gegangen
- **Ich werde mein Bestes geben - aber ich entschuldige mich jetzt schon!**

Administrivia

- **Fragen? Laut schreien / auf-sich-aufmerksam machen**
  - Gilt auch falls eine Pause gewünscht ist.
- **Bitte keine Fotos oder Videos!**
- **Alle Materialien stehen online zur Verfügung**



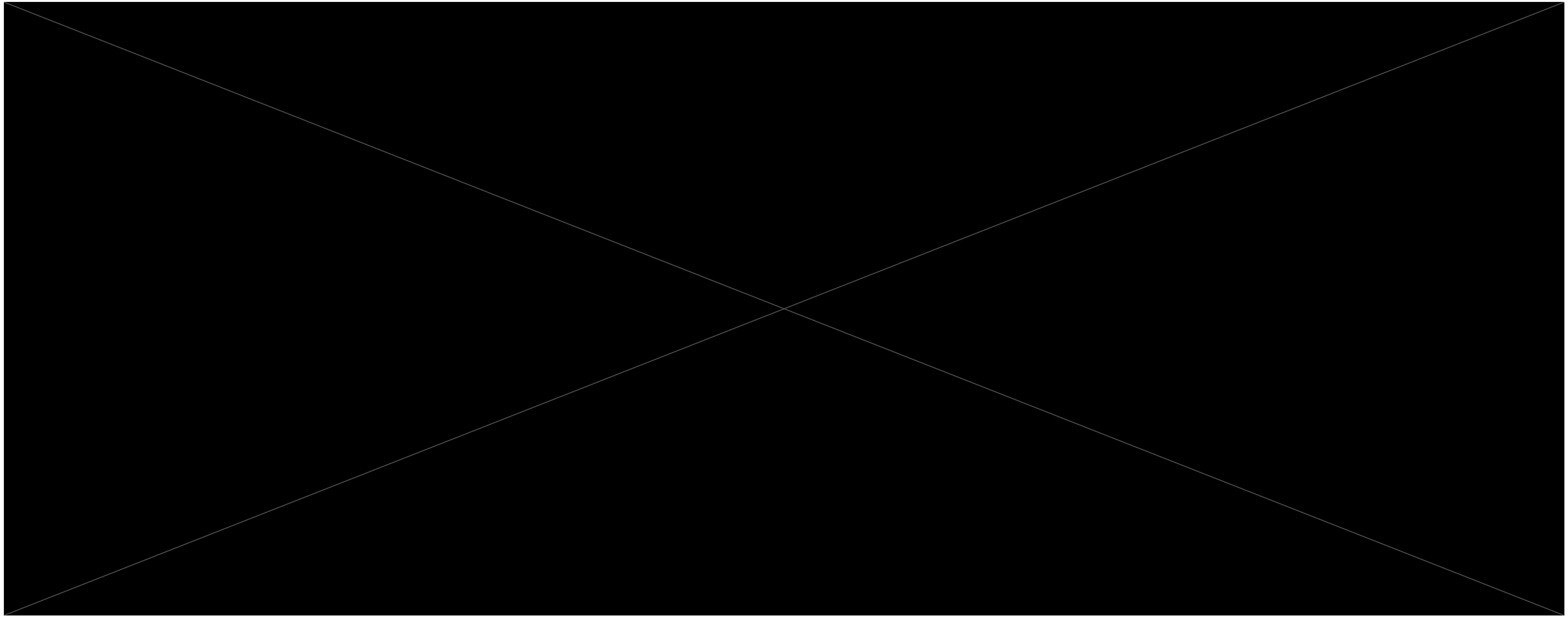
- **Es gibt Sticker, bedient euch so viel ihr wollt!**

Bitte jetzt einmal alle ihre dunkelsten Geheimnisse auspacken.

(Okay, .. nicht ganz. Kurze Vorstellungsrunde.)

Über mich, warum ich ..

(Alternativtitel: Selbstbeweihräucherung)



Warum Threat Analysis?

.. und warum dieser Workshop?

- **Cyberangriffe werden nicht weniger, ganz im Gegenteil.**
- **Gleichzeitig: Kompetente Analyst:innen werden immer weniger.**
  - Ausbildung tendenziell sehr orientiert an Produkten / kommerziellen Lösungen
  - Was “Analyse” überhaupt ist? Fehlanzeige.
- **Mein Ziel: Interesse wecken, Grundlagen vermitteln, Möglichkeiten aufzeigen**
  - (Cyber) Threat Analysis ist **extrem** weitläufig und vielseitig
  - Limitierte Zeit, bestmöglich genutzt

Was ist (Cyber) Threat Analysis?

“The systematic process of collecting, processing, and analyzing information about potential or active cyber threats to understand their nature, capabilities, and potential impact.”

Cyber Threat Analysis ist nicht (nur) festzustellen, dass etwas vorgefallen ist, sondern zu verstehen, wer oder was betroffen ist, wie ein möglicher Angriff funktionieren könnte, wie wahrscheinlich er ist und welche Gegenmaßnahmen sinnvoll sind.

Es ist etwas passiert!11!1!

(Bitte jetzt den Kopf verlieren und Angst haben!)

- **Ein:e Mitarbeiter:in meldet sich Nachts von einer neuen IP-Adresse an**
  - Nach der Anmeldung werden massig Daten auf einen externen Server geladen

Es ist etwas passiert!11!1!

(Bitte jetzt den Kopf verlieren und Angst haben!)

- **Ein:e Mitarbeiter:in meldet sich Nachts von einer neuen IP-Adresse an**
  - Nach der Anmeldung werden massig Daten auf einen externen Server geladen
- **Ungewöhnlich? Ja. Verdächtig? Ja. Bösartig? Hmm ..**
- **“Threat Analysis” bedeutet Unklarheit zu minimieren**
  - “Cyber Threat Analysis” ist nur die technische Variante davon
  - “Gibt es ein Problem? Und wenn ja, wie schlimm ist es?”
  - Daraus abgeleitet: “Und was jetzt?”

Klingt komplizierter als es ist!

(Das ist ein gängiges Problem in der IT-Security.)

- **Threat Analysis kann auf vier “Teile” heruntergebrochen werden:**
  - Einer Frage.
  - Einer Recherche.
  - Einer Analyse.
  - Einem Ergebnis.

Frage

Wer, wie, wo, was, warum, weshalb? 🎶

- **Manchmal intern, manchmal extern gestellt**
  - Der Klassiker: “Was ist passiert?”
  - Bei Management beliebt: “Was wird passieren?”
- **Es ist okay wenn die initiale Frage einfach nur “Was ist passiert?” ist.**
  - Im Zuge der Beantwortung tauchen (hoffentlich) neue Fragen auf.
  - “Was könnte passiert sein?” ist ein ausgezeichneter Startpunkt für ..

Recherche

“I have Internet access, research skills and no self-control.”

- **Die Grundlage für Analyse - und genauso wichtig wie die Analyse selbst**
  - Je besser die Datenlage, desto leichter die Analyse / besser die Ergebnisse
- **Ziel ist es eine relevante Faktenbasis zu schaffen**
  - Es geht nicht darum möglichst viele Informationen und Daten zu sammeln!
  - Typische Anfrangskrankheit (ich zähle als Anfänger, reden wir nicht darüber)

“Was ist passiert?”

“Es ist ein verdächtiger Zugriff erfolgt.”

“Welche Informationen brauchen wir um festzustellen, ob der Zugriff legitim war oder ob es sich um eine Kompromittierung handelt?”

“Welche Daten wurden auf welchen Server übertragen? Dauert die Übertragung noch an? Welche Systeme, Konten, Datenbestände sind unter Umständen noch betroffen?”

Es muss nicht immer technisch sein!

Abkürzungen machen euer Leben leichter.

- **Mehr Informationen und Daten als je zuvor**
  - Moderne Unternehmensnetzwerke sind oft ein Orwell'scher Albtraum
  - CTI-Anbieter sind extrem nützlich, aber (manchmal) auch **extrem** gruselig
- **Nicht immer ist der Zugriff darauf und aufwändige Analyse notwendig!**
  - Ein Griff zum Telefon kann potentielle Vorfälle (manchmal) schnell beenden
  - Mitarbeiter:in auf Dienstreise, Test eines neuen Standortes, ..

Manchmal muss es technisch sein

Stolperfallen der Unternehmens-IT

- **Mehr Daten als je zuvor, oft weniger Daten als wir brauchen**
  - Zu kurze Aufbewahrungsfristen, Ausnahmen beim Logging, ..
- **Absoluter Albtraum: hIsToRiScH gEwAcHsEn**
  - Auch bekannt als “technical debt”
  - “Was ist dieses Asset Management von dem Sie da reden?”
  - Bereitet auch mental darauf vor, das wird euch begegnen

Manchmal muss es technisch sein

Vorbereitung hilft!

- **Vorhandene Datenquellen im Vorhinein eruieren**
  - Spart im Anlassfall Zeit und Nerven
  - Hilft unter Umständen vorhandene blinde Flecken zu finden
- **In vielen Organisationen liegt die Datenhoheit bei anderen Abteilungen**
  - Definierte, getestete **organisatorische und technische** Prozesse sind wichtig
- **Sicherstellen, dass die Daten tatsächlich vorhanden sind**
  - Kaputte Log forwarder, geändertes Datenformat, ..

Manchmal muss es technisch sein

So wenig wie möglich, so viel wie notwendig

- **Das Ziel ist die Beantwortung der Frage/n - nicht mehr, nicht weniger**
  - Man kann immer neue Informationen / Daten anfragen
  - Zu viele Informationen einzuholen behindert euch nur
- **Threat Intelligence ist verlockend, aber mit Vorsicht zu geniessen**
  - Viele bunte Dashboards, initial nicht unbedingt relevante Informationen
  - Es geht darum was passiert ist, nicht wer es war
  - CTI kann analytischen Kontext liefern

Analyse

It’s showtime, baby!

- **Das Problem ist definiert, Fragen sind gestellt, Informationen gesammelt**
- **Jetzt geht es darum ..**
  - .. Fakten und Annahmen zu trennen
  - .. Hypothesen zu sichten
  - .. Evidenz zu bewerten
  - .. zu einer Schlussfolgerung, einem Ergebnis zu kommen

Fakten, Annahme, offene Fragen

Anhand des Beispiels

- **Fakten:**
  - Der Login und der ausgehende Transfer sind in den Logs sichtbar
- **Annahme:**
  - Die unbekannte IP-Adresse gehört einem Bedrohungsakteur
- **Offene Fragen:**
  - War die Person auf Dienstreise oder nutzt ein neues VPN?
  - Welche Daten machen die $Anzahl GB aus?
  - Sind andere Konten betroffen?

Hypothesen

.. damit die plausible Geschichte nicht zur “Wahrheit” wird

- **Gute Analyse prüft nicht nur die erste, naheliegende Erklärung**
- **Zum Beispiel:**
  - ???
  - ???
  - ???
  - ???.
- **Es gibt einen Grund für den Vergleich mehrerer Hypothesen ..**

Hypothesen

.. damit die plausible Geschichte nicht zur “Wahrheit” wird

- **Gute Analyse prüft nicht nur die erste, naheliegende Erklärung**
- **Zum Beispiel:**
  - H1: Das Konto wurde kompromittiert, Daten wurden exfiltriert.
  - H2: Der Datentransfer war ungewöhnlich, aber legitim.
  - H3: Ein automatischer Prozess, eine Fehlkonfiguration erzeugte den Alert
  - H4: Die Anmeldung ist legitim, das Endgerät aber dennoch kompromittiert.
- **Es gibt einen Grund für den Vergleich mehrerer Hypothesen ..**

Stolz und Vorurteil

Vor allem Vorurteil

- **Überraschung - Menschen sind keine Maschinen**
  - Unsere Gehirne sind nicht “professionell”, sie sind menschlich
- **Wir machen systematische Denkfehler, “Analytical Biases”**
  - Das heißt nicht, dass wir schlechte Analysten sind!
  - Gehirne müssen komplexe, unvollständige, mehrdeutige Informationen vereinfachen, sonst gäb’s uns gar nicht mehr
- **Sie führen zu falschen Prioritäten und voreiligen Schlussfolgerungen**

Stolz und Vorurteil

Vor allem Vorurteil.

- **“Das ist ein illegitimer Zugriff und es wurden Daten gestohlen”**
  - Diese Aussage kann stimmen, ist aber nur eine Hypothese
- **Analytischer Bias entsteht, wenn wir uns nur auf die Hypothese konzentrieren**
  - Nur nach bestätigenden Hinweisen suchen
  - Widersprechende Hinweise zu schnell wegwischen
  - …

Stolz und Vorurteil

Vor allem Vorurteil.

- **Confirmation Bias**
  - Wir suchen nach Beweisen die unsere erste Annahme unterstützen.
- **Anchoring Bias**
  - Die erste Information prägt die spätere Bewertung unverhältnismäßig stark
- **Groupthink**
  - Wir passen uns einer dominanten oder früh geäußerten Meinung an
- **Mirror Imaging**
  - Man unterstellt anderen Akteuren eigene Werte, Ziele oder Vorgehensweisen

Stolz und Vorurteil

Vor allem Gegenmaßnahmen zum Vorurteil

- **Fakten, Annahmen und Schlussfolgerungen trennen**
- **Konkurrierende Hypothesen aufstellen**
  - Nicht nur die wahrscheinlichste Variante in Betracht ziehen, kreativ sein!
- **Nach widerlegenden Beweisen suchen**
  - Nicht nur fragen “Wie beweise ich xyz?” sondern auch “Wie widerlege ich xyz?”
- **Analytical Biases sind ein riesiges Thema, zu groß für detaillierte Behandlung**
  - In den Ressourcen zu dem Workshop findet ihr mehr Material.

Stolz und Vorurteil

Vor allem Gegenmaßnahmen zum Vorurteil

- **Frameworks helfen doppelt**
  - Bieten verschiedene “Kameraperspektiven” auf einen Vorfall an
  - Ermöglichen ein analytisches Gerüst an dem man sich festhalten kann
- **Es gibt viele, viele verschiedene Threat Analysis Frameworks**
  - MITRE ATT&CK, Cyber Kill Chain, Diamond Model ..
- **Nutzt das was für die Aufgabe passt, nicht was der Hype vorgibt!**
  - Die Branche hat eine leichte Tendenz zur Fetischisierung.

Frameworks

Die unterschiedlichen Kameraperspektiven

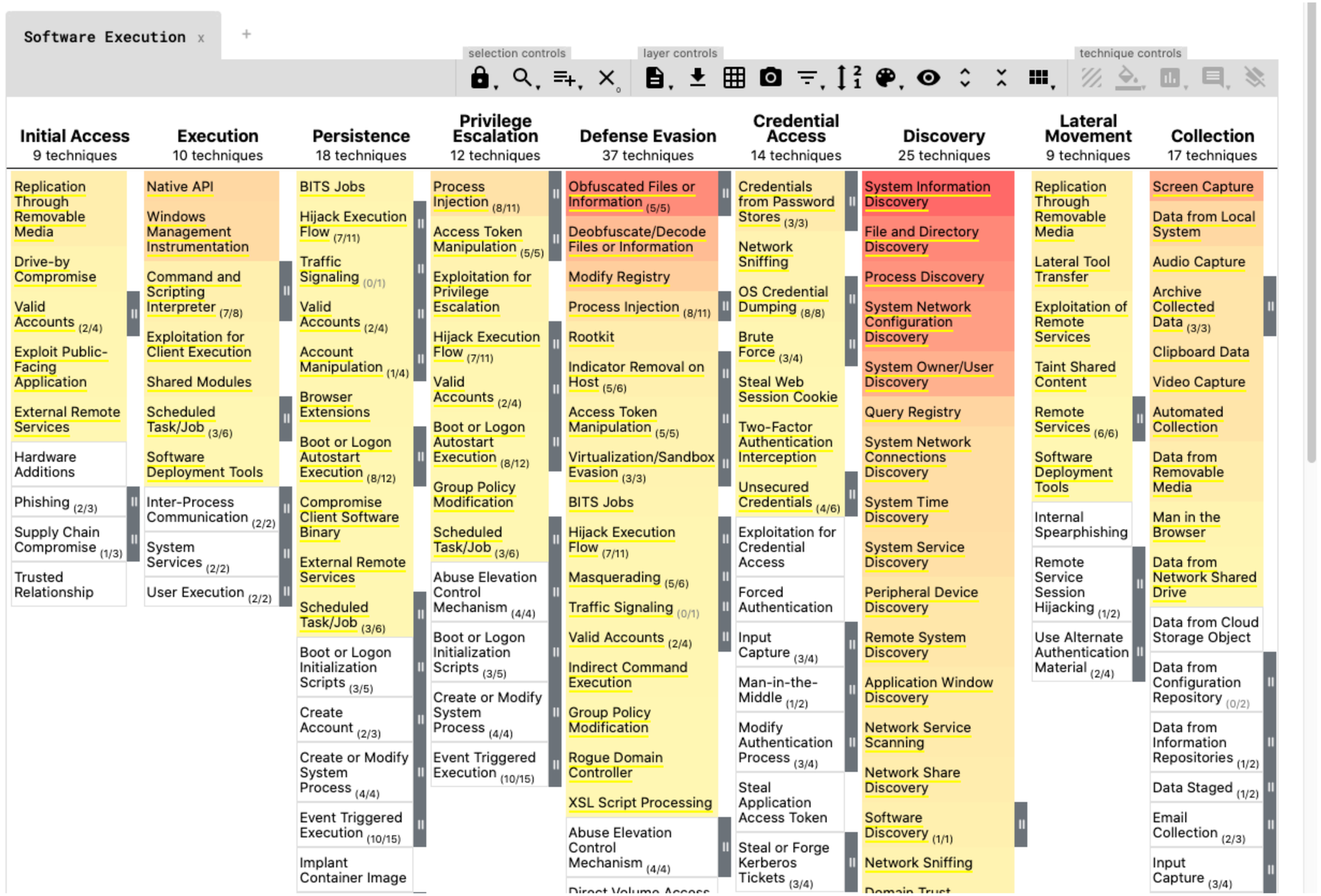
- **MITRE ATT&CK**
  - Verhalten - was tun Angreifer:innen?
- **(Lockheed Martin) Cyber Kill Chain**
  - Phasen - wie verläuft ein Angriff?
- **Diamond Model**
  - Zusammenhänge - was verbindet Entitäten?

MITRE ATT&CK

(Ja, es gibt auch MITRE D3FEND.)

- **ATT&CK ist eine Wissensbasis für beobachtete Taktiken und Techniken**
  - Taktik beschreibt das Ziel der Angreifer, das “warum”
  - Technik beschreibt das konkrete Vorgehen der Angreifer, das “wie”
- **ATT&CK gibt Teams eine gemeinsame Sprache**
  - Hilft bei der Suche nach weiteren Spuren
  - Hilft bei dem Aufbau von Analysen

MITRE ATT&CK

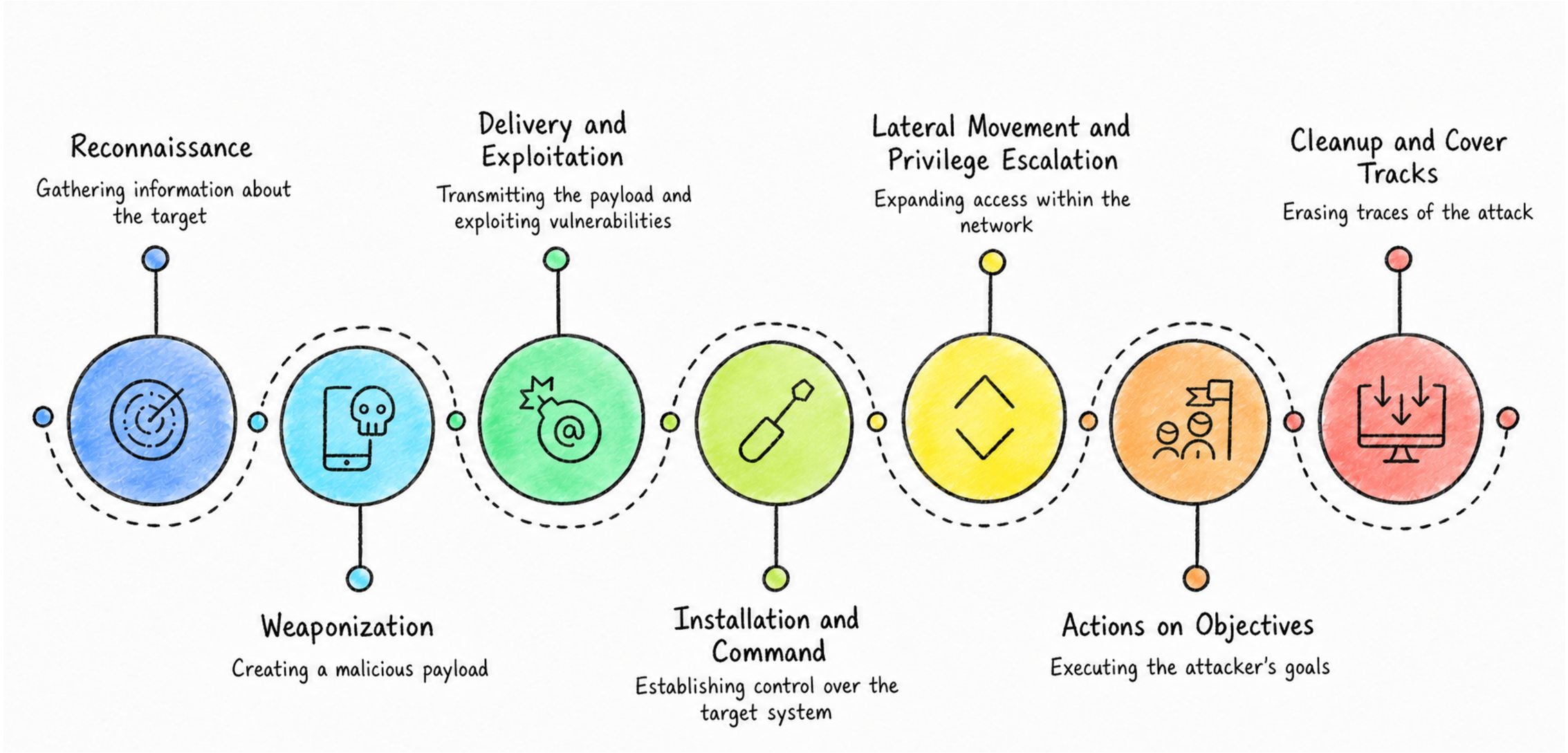

Software Execution x
selection controls
layer controls
technique controls
Initial Access
9 techniques
Replication Through Removable Media
Drive-by Compromise
Valid Accounts (2/4)
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (2/3)
Supply Chain Compromise (1/3)
Trusted Relationship
Execution
10 techniques
Native API
Windows Management Instrumentation
Command and Scripting Interpreter (7/8)
Exploitation for Client Execution
Shared Modules
Scheduled Task/Job (3/6)
Software Deployment Tools
Inter-Process Communication (2/2)
System Services (2/2)
User Execution (2/2)
Persistence
18 techniques
BITS Jobs
Hijack Execution Flow (7/11)
Traffic Signaling (0/1)
Valid Accounts (2/4)
Account Manipulation (1/4)
Browser Extensions
Boot or Logon Autostart Execution (8/12)
Compromise Client Software Binary
External Remote Services
Scheduled Task/Job (3/6)
Boot or Logon Initialization Scripts (3/5)
Create Account (2/3)
Create or Modify System Process (4/4)
Event Triggered Execution (10/15)
Implant Container Image
Privilege Escalation
12 techniques
Process Injection (8/11)
Access Token Manipulation (5/5)
Exploitation for Privilege Escalation
Hijack Execution Flow (7/11)
Valid Accounts (2/4)
Boot or Logon Autostart Execution (8/12)
Group Policy Modification
Scheduled Task/Job (3/6)
Abuse Elevation Control Mechanism (4/4)
Boot or Logon Initialization Scripts (3/5)
Create or Modify System Process (4/4)
Event Triggered Execution (10/15)
Defense Evasion
37 techniques
Obfuscated Files or Information (5/5)
Deobfuscate/Decode Files or Information
Modify Registry
Process Injection (8/11)
Rootkit
Indicator Removal on Host (5/6)
Access Token Manipulation (5/5)
Virtualization/Sandbox Evasion (3/3)
BITS Jobs
Hijack Execution Flow (7/11)
Masquerading (5/6)
Traffic Signaling (0/1)
Valid Accounts (2/4)
Indirect Command Execution
Group Policy Modification
Rogue Domain Controller
XSL Script Processing
Abuse Elevation Control Mechanism (4/4)
Credential Access
14 techniques
Credentials from Password Stores (3/3)
Network Sniffing
OS Credential Dumping (8/8)
Brute Force (3/4)
Steal Web Session Cookie
Two-Factor Authentication Interception
Unsecured Credentials (4/6)
Exploitation for Credential Access
Forced Authentication
Input Capture (3/4)
Man-in-the-Middle (1/2)
Modify Authentication Process (3/4)
Steal Application Access Token
Steal or Forge Kerberos Tickets (3/4)
Discovery
25 techniques
System Information Discovery
File and Directory Discovery
Process Discovery
System Network Configuration Discovery
System Owner/User Discovery
Query Registry
System Network Connections Discovery
System Time Discovery
System Service Discovery
Peripheral Device Discovery
Remote System Discovery
Application Window Discovery
Network Service Scanning
Network Share Discovery
Software Discovery (1/1)
Network Sniffing
Lateral Movement
9 techniques
Replication Through Removable Media
Lateral Tool Transfer
Exploitation of Remote Services
Taint Shared Content
Remote Services (6/6)
Software Deployment Tools
Internal Spearphishing
Remote Service Session Hijacking (1/2)
Use Alternate Authentication Material (2/4)
Collection
17 techniques
Screen Capture
Data from Local System
Audio Capture
Archive Collected Data (3/3)
Clipboard Data
Video Capture
Automated Collection
Data from Removable Media
Man in the Browser
Data from Network Shared Drive
Data from Cloud Storage Object
Data from Configuration Repository (0/2)
Data from Information Repositories (1/2)
Data Staged (1/2)
Email Collection (2/3)
Input Capture (3/4)

Cyber Kill Chain

Lockheed Martin baut nicht nur Waffen und Flugzeuge

- **Die Cyber Kill Chain teilt Angriffe in sieben Phasen auf**
  - Verhindert, dass man sich nur auf das sichtbare Event konzentriert
  - Was war davor, was war danach?
- **Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Actions on Objectives**

Cyber Kill Chain

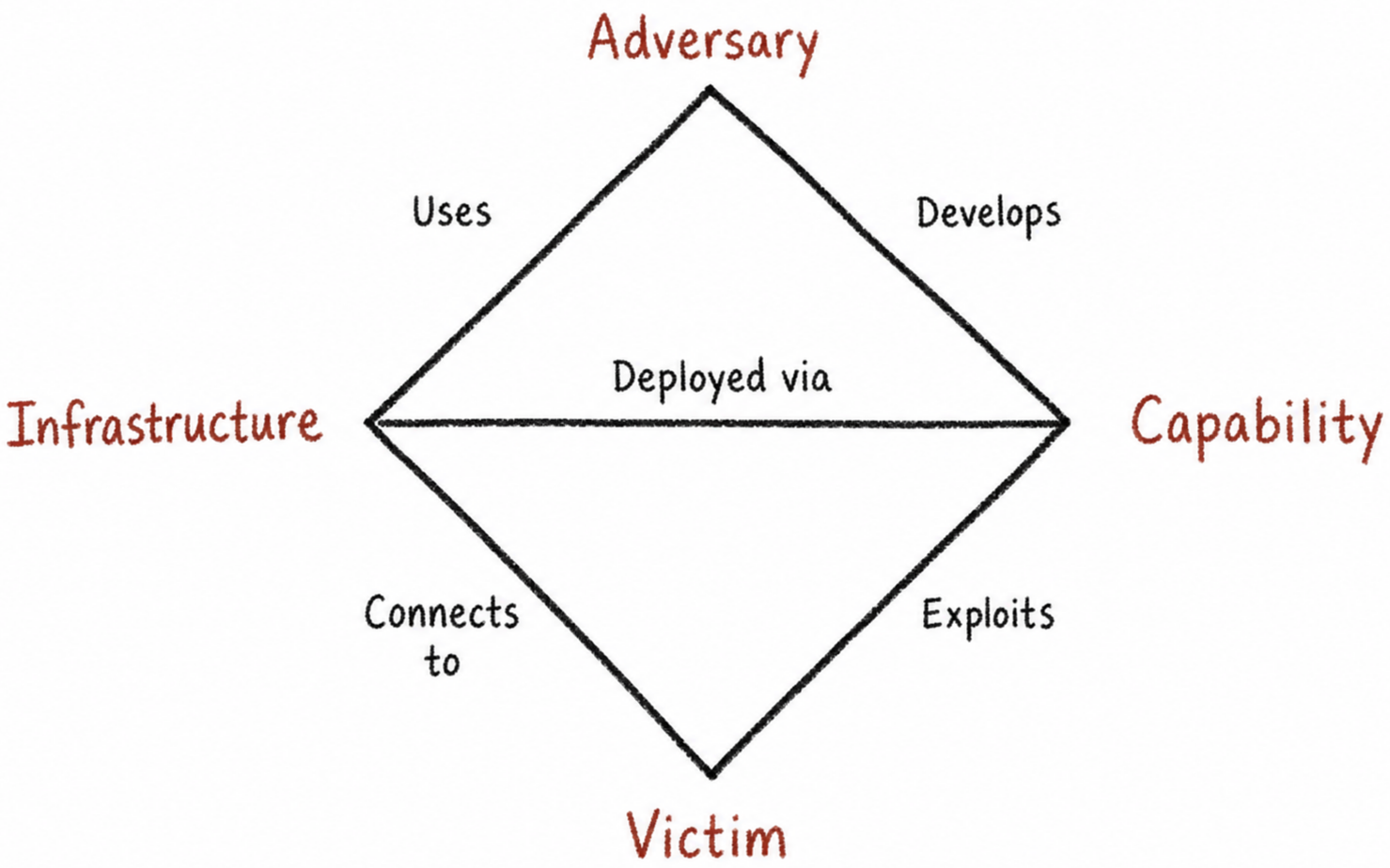


Diamond Model

Marilyn Monroe hatte Recht, Diamonds are our best friends.

- **Diamond Modell sieht ein Event als Beziehung zwischen vier Kernelementen**
  - Adversary <-> Capability <-> Infrastructure <-> Victim
- **Adversary**: Bedrohungsakteur
- **Capability**: Werkzeug, Malware, Technik, Vorgehensweise
- **Infrastructure**: Ressourcen für Angriff, Steuerung, Datenabfluss - Domains, IP-Adressen, Benutzer:innenaccounts, ..
- **Victim**: Angegriffenes Konto, Gerät, System, Team, Organisation, Benutzer:in ..

Diamond Model



Diamond Model

Marilyn Monroe hatte Recht, Diamonds are our best friends.

- **Wenn ein Element bekannt ist kann man damit andere suchen**
- **Aus dem Beispiel: Die Adresse des Servers ist bekannt**
  - Welche Geräte haben sich noch zu dieser Adresse verbunden?
  - Hatten wir ähnliche Verbindungen in der Vergangenheit?
  - Lassen sich (z.B. über whois-Informationen) ähnliche Server finden?

Und jetzt alle zusammen!

(Bitte nicht singen)

- **MITRE ATT&CK**
  - Status: Exfiltration von Daten.
  - Nächste Frage: Welche Prozesse, Systeme zeigen dasselbe Uploadverhalten?
- **Cyber Kill Chain**
  - Status: Actions on Objectives
  - Nächste Frage: Gab es vorher Phishing, Token-Diebstahl, gegen das System?
- **Diamond Model**
  - Status: Verbindung von Laptop zu unbekannter Infrastruktur
  - Nächste Frage: Betrifft dieselbe Domain, IP weitere Konten / Geräte?

Ergebnis ist Ergebnis

(Mehr oder weniger) egal wie man hinkommt

- **Jeder Fall, jede Untersuchung verläuft anders.**
  - Manchmal endet die Analyse bevor ein Modell überhaupt zum Einsatz kommt.
  - Manchmal passen klassische Modelle nicht.
- **Schlussendlich geht es darum, dass aus dem Gemisch aus Fragen, Daten / Informationen, Hypothesen, Analysevorgang am Ende ein Ergebnis wird.**
- **Das Ergebnis kann verschiedenste Formen annehmen.**

Ergebnis

Das (manchmal gar nicht so grosse) Finale

- **Das Ergebnis kann viele Farben und Formen annehmen**
  - Von kurzer Chatnachricht bis hin zu Konferenzvortrag
- **Gemeinsamer Nenner im Alltag: Ermöglichen einer Entscheidung**
  - Ergebnis liefert Fakten und Bewertung, klar getrennt
  - Ereignisse sollen nachvollziehbar, verständlich gemacht werden
- **Das Ergebnis ist nie der Datenhaufen, es ist die belastbare Antwort auf Fragen**

“Das Ergebnis ist dann gut, wenn es den Verantwortlichen ermöglicht ohne weitere Grundsatzrecherchen eine Entscheidung zu treffen.”

Namen sind Schall und Rauch!

Vorfallsbericht, Incident Report, Casefile, ..

- **Im Regelfall werdet ihr irgendein Dokument verfassen.**
  - Ja, ich hatte auch gehofft weniger uncoolen Papierkram machen zu müssen ..
- **Die Zielgruppe ist oft fachfremd, .. oder zumindest nicht (mehr) nahe am Fach**
  - Dementsprechend: Auf die Bedürfnisse des Zielpublikums anpassen
- **Meist findet ihr in Unternehmen Vorlagen oder alte Berichte als "Inspiration"**
  - Gerade wenn die Organisation ISO27001-zertifiziert ist. Auditoren stehen unglaublich auf solche Berichte.

Beispielstruktur

So und ~~nicht~~ oft anders!

- **Executive Summary**
- **Zeitleiste**
- **Technische Befunde**
- **Unsicherheiten / offene Fragen**
  - Kann auch Dinge beinhalten die aus Zeitgründen noch offen sind
- **Lessons Learned**
  - Auch wenn’s schwer ist, ehrlich sein - nur so verbessert sich was

Am 10. September 2026 meldete sich das Konto vorname.nachname um 02:14 Uhr von einer bisher nicht genutzten IP-Adresse an. Die Anmeldung erfolgte über eine neu beobachtete Session; die Ursache der Authentifizierung ist noch in Prüfung. Zwischen 02:19 und 03:07 Uhr wurden über den Cloud-Speicherdienst 18,4 GB aus drei Projektbereichen auf den externen Dienst example-transfer.tld übertragen. Betroffen sind 426 Dateien, darunter 38 als „vertraulich“ klassifizierte Dokumente.

Es liegen derzeit keine bestätigten Hinweise auf weitere kompromittierte Konten oder laterale Bewegung vor; die Prüfung ist jedoch noch nicht abgeschlossen. Die Sitzung wurde beendet, Tokens wurden widerrufen, das Konto zurückgesetzt und die Ziel-Domain am Secure Web Gateway blockiert. Der Vorfall wird als hoch priorisiert. Offen sind die Identifikation des initialen Zugriffspfads, die abschließende Bewertung der betroffenen Daten sowie die Prüfung möglicher Meldepflichten.

Kurze Pause?

.. und weiter geht’s!

Übung macht Meister:innen!

(Endlich kann ich mal nerviger Lehrer spielen.)

- **Schließt euch zu Gruppen von 3-5 Personen zusammen**
  - Ihr könnt natürlich auch alleine arbeiten, aber das mindert die Übung ein wenig.
- **Seht euch die Aufgaben an, löst sie gemeinsam.**
  - Die Aufgaben finden sich im Discord und auf der Begleitwebseite.
- **Zeitlimit: 30 Minuten**
  - Das ist kein hartes Limit, in beide Richtungen. Wir finden einen gangbaren Weg.

<insert notification sound here>

Die Lage hat sich geändert.

- **Um 02:11 gab es vier fehlgeschlagene Login-Versuche für dasselbe Konto.**
- **Um 02:16 wurde ein MFA-Push bestätigt und die Anmeldung war erfolgreich**
  - Der Nutzer sagt auf Nachfrage, dass ihn das Gebimmel vom Handy gestört hat und er irgendwann einfach eine Anfrage bestätigt hat um schlafen zu können.
- **Die Zieladresse des Uploads ist neu und dem Unternehmen nicht bekannt.**
- **Auf dem Endgerät wurde um 02:21 ein lokales Archiv mit der Endung .zip erstellt.**

<insert notification sound here>

Die Lage hat sich geändert.

- **Logs vom Fileshare zeigen, dass kurz vor dem Upload 164 Dateien aus einem Projektbereich heruntergeladen worden sind.**
  - Darunter befinden sich technische Zeichnungen, Preislisten, Kund:innendaten
- **Der Upload ist inzwischen beendet.**
- **Das Konto und die Anmeldesitzung sind noch aktiv.**

Hit me!

Analyse liefert nicht immer eine einfache Antwort. Aber sie hilft dabei, Beobachtungen, Hypothesen und überprüfbare Fakten in eine nachvollziehbare Entscheidung zu verwandeln.

Ich, heute morgen um kurz vor 05:00 bei dem Versuch einen klugen Abschlusssatz für diesen Abschnitt des Workshop zu finden.

Mehr braucht ihr nicht!

.. außer technisches Wissen, kein Sozialleben, Inspiration & Transpiration, ..

- **Das waren die wichtigsten Grundlagen von Bedrohungsanalyse!**
  - Egal ob große oder kleine Firmen, technisch oder nicht, ..
- **Allgemein anwendbar, in (so gut) wie jedem Fall**
- **Folgend einige Tips, Tricks, Erfahrungen ..**
  - Basierend auf meinen Erfahrungen - YMMV!

It’s all about the ~~base~~ basics!

(Ich entschuldige mich nicht für den Ohrwurm.)

- **Auch wenn es langweilig ist, Grundlagenwissen!**
  - Netzwerke, Betriebssysteme, Authentifizierung, Konzepte ..
- **Sinnerfassendes Lesen hebt von der breiten Masse ab**
  - .. nein, ernsthaft. Das ist ein Problem.
- **Ihr müsst keine Expert:innen werden - aber wissen was ihr suchen müsst!**
  - Wenn euch etwas Neues begegnet, einfach mal 30 Minuten reinschauen

Analyse zur Gewohnheit machen

Routinen für Alerts, statt Routinealerts

- **Analytisches Denken lässt sich quasi überall anwenden**
- **Beobachtung -> Frage -> Recherche -> Analyse -> Bewertung / Entscheidung**
  - Egal ob in der Arbeit oder beim seltsamen Rechner des Schwiegervaters
- **Bitte nicht übertreiben!**
  - Wenn die Pizzabestellung vier Stunden dauert wird’s problematisch ..

Kommunikation lässt sich lernen

(Für die meisten Menschen. Ich scheitere daran.)

- **Kommunikation ist nicht nur Reporting am Ende**
  - Sie ist Teil der Sicherheitsmaßnahme selbst
- **Klar, zeitnah, belegbar, konsistent, zielgruppengerecht**
  - Jede Zielgruppe ist anders, reagiert anders, hat andere Bedürfnisse
- **Kommunikation ist, oft unbeabsichtigt, mächtig**
  - z.B. “Hat nicht stattgefunden” versus “Keine Hinweise auf”

Agatha Christie muss neidisch werden!

(Ich bin kein Schriftsteller, ich hab einfach “meistverkaufte Autorin” gesucht)

- **Schriftliche Kommunikation wird oft Erst- oder sogar Hauptmedium sein**
  - Dementsprechend ist die Qualität eurer Schreibarbeit besonders wichtig.
- **Gute Hilfe am Anfang: “Drei-Ebenen-Regel”**
  - **Beobachtungsebene** - “Das Proxy-Log zeigt ..”
  - **Analysebene** - “Der Befund erhöht mit Wahrscheinlichkeit ..”
  - **Empfehlungsebene** - “Priorität hat ..”
- **Sprachliche Klarheit und Sorgfalt ist wichtig, oft sogar entscheidend.**

Diese Branche hat Eigenheiten.

Dieser Teil von ihr noch mehr.

- **Kreisberichterstattung**
  - Ein Blogpost behauptet etwas, drei Firmen und zwei Nachrichtenseiten wiederholen es, .. et voilà, neue “Wahrheit”
- **Alarmismus**
  - Diese Branche belohnt (leider) Alarmismus. Lasst es trotzdem sein.
- **Attribuierung**
  - Aktivitäten Clustern ist Analyse, Zurechnung (meist) nicht euer Job.
  - APT29, Cozy Bear, Midnight Blizzard sind nicht gleich, egal was die Industrie sagt!

Nehmt analytische Arbeit ernst!

“this is what separates analysis from tech blogging”

- **Unterschiede klar benennen und kommunizieren**
  - Beobachtung, Ableitung, Bewertung
- **Beginnt bei eurer Organisation, nicht einem Bedrohungsakteur**
  - Siehe auch: Alarmismus
- **Das Ziel ist Veränderung (im weitesten Sinn)**
  - Ihr wollt, dass aus eurer Arbeit Ergebnisse entstehen
  - “otherwise you’re just writing a newsletter”

Professionalität

Hat nichts mit Haarfarbe oder Hosenwahl zu tun - aber mit Sauberkeit (der Arbeit)

- **Aus Fehlern, Feedback, Fehlalarmen lernen**
  - Erfahrene Kolleg:innen können helfen, nicht nur beim Ergebnis
  - Ein False Positive ist kein Misserfolg wenn danach Detection-Regeln besser sind.
- **Rechtlich und ethisch sauber arbeiten**
  - Auch wenn es einfach und verlockend ist, Zugriff auf personenbezogene oder anderweitig sensible Daten muss minimal sein.
  - Analyse ist Einschätzung, keine Wertung.
- **Lautstärke != Relevanz (vor allem bei Alerts)**

Nicht beirren lassen.

Vor allem nicht von Arschlöchern

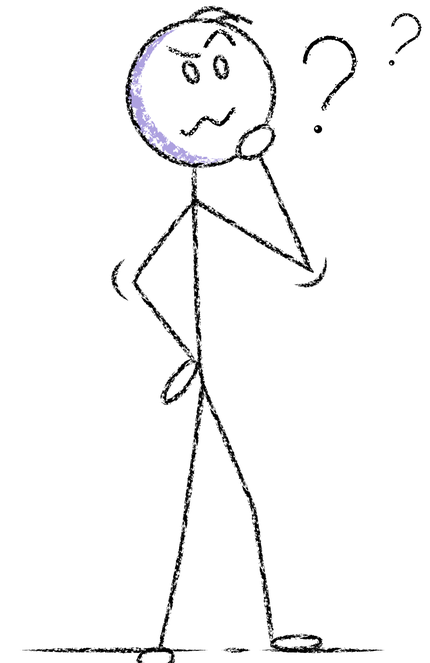
- **Kritik ist gut, wichtig, sinnvoll - wenn sie sachlich, fachbezogen ist.**
  - Das ist sie nicht immer, auch wenn sie vorgibt es zu sein.
- **Kurz und knapp: Sexismus ist immer noch ein Thema, trotz aller Fortschritte**
  - Und das auf allen Ebenen, nicht nur im Management.
- **Ich hab’s als Mann nie selbst so erlebt, nur mitbekommen, aber:**
  - Manchmal muss man es hinnehmen, so beschissen es ist.
  - Niemals den Glauben in die eigenen Fähigkeiten unterminieren lassen, auch wenn es schwer fällt.

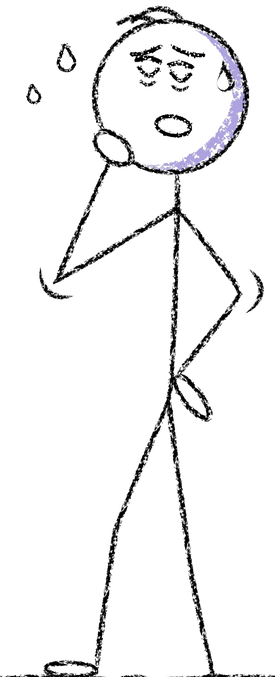
Was die Zukunft bringen wird *

*** vielleicht, ich bin nicht Nostradamus**

- **Künstliche Intelligenz**
  - .. als “Brandbeschleuniger” für Bedrohungsakteure
  - .. als Ziel für Angreifer:innen
  - .. als Unterstützung für Verteidiger:innen
- **Lieferketten**
  - .. Angriffe gegen Organisationen richten sich nicht immer gegen Organisationen
  - .. Ökosysteme werden relevanter für die eigene Sicherheit

Das war jetzt viel auf einmal.

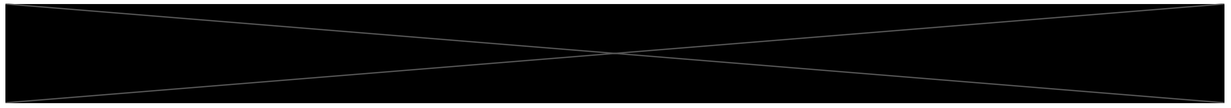




Ich will mehr lernen!

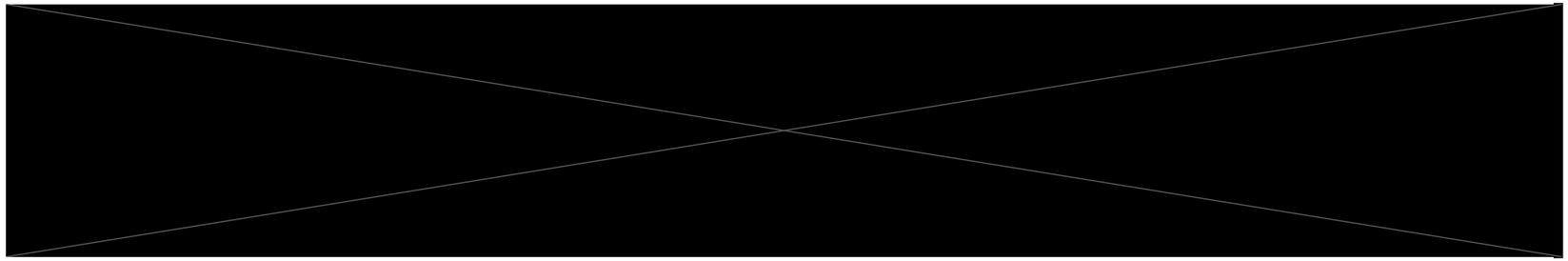
(Come to the dark side, we have .. expensive books.)

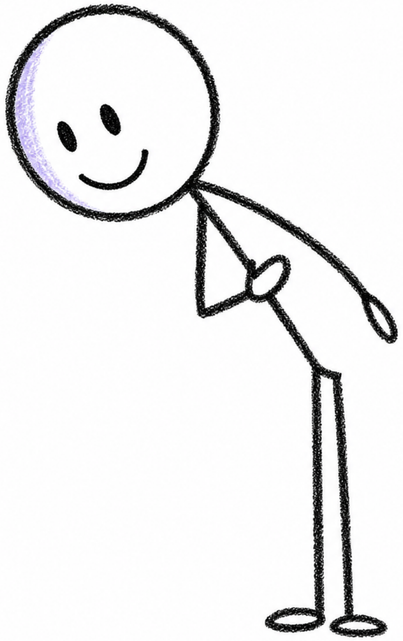
- **Bücher!**
- **Professionelles Training? Zertifizierungen?**
  - Qualität schwankt extrem, selbst bei teuren Angeboten
  - ISC, ISACA, CompTIA, CEH sind alle nett am Papier, praktisch aber .. jo.
  - **SANS ist viel zu teuer für die Qualität (I'm willing to die on this hill.)**
- **Fangt einfach an!**
  - Egal ob im privaten Labor oder in der Arbeit



Danke für eure Aufmerksamkeit!

- **Kontakt**:
  - contact@bytesandborscht.com
  - @bytesandborscht.bsky.social





Falls Fragen auftauchen - bitte meldet euch. **Ernsthaft**.