Cyber Defense in einem Unternehmen der kritischen Infrastruktur

Dipl.-Ing. Dr. Walter Fraißler
Florian-Sebastian Prack, MSc
Paul Mader, MSc

IT-Sec X
St. Pölten
7. Oktober 2022

Verbund

Inhalt

- VERBUND als Betreiber kritischer Infrastruktur
- Die Organisation von InfoSec bei VERBUND
- Hard Facts IT & Security
- Herausforderungen für die Security
- Kurzvorstellung Blue Team und Red Team
  das Katz- und Maus-Spiel
- Beispiel: Projektarbeit & Erkenntnisse
  Projekt EDR/EPP
- Beispiel: Daily Business & Erkenntnisse
  ehemalige 0-Klick Schwachstelle Follina
- Weitere Erkenntnisse und Fokuspunkte

Wer sind wir?

Dipl.-Ing. Dr. Walter Fraißler
Leiter Informationssicherheit

Aufgabengebiete
- Leitung der Abteilung InfoSec
- Aufbau des Teams
- Steuerung des strategischen „Masterplans Information Security“

Florian-Sebastian Prack
OT-Security Specialist

Aufgabengebiete
- Security Operation Center
- Endpoint Detection & Response
- Network Traffic Analysis
- Security Fragen bei OT
- Projektunterstützung bei OT

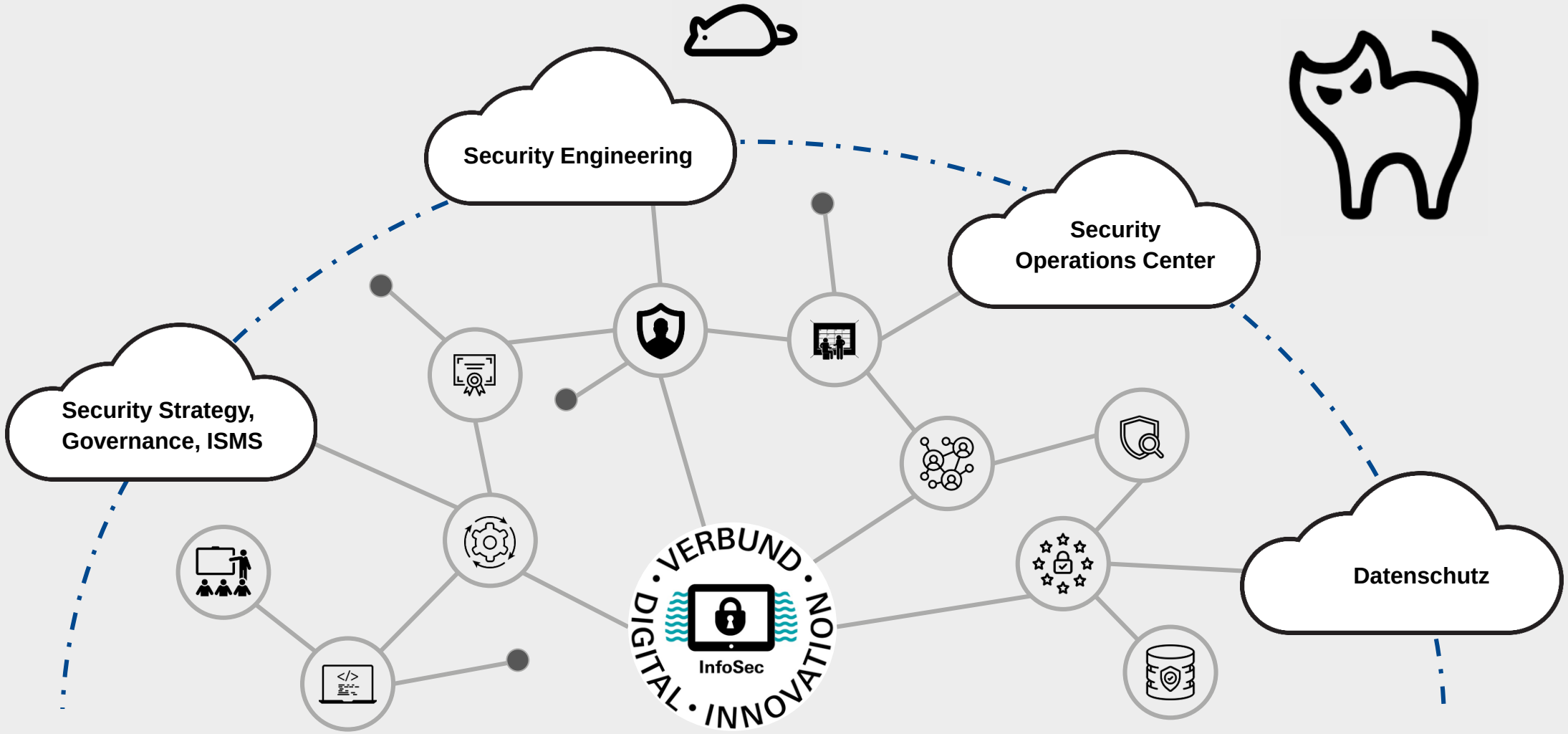
„Wachsames Auge von Mordor“

Paul Mader, MSc
IT-Security Specialist

Aufgabengebiete
- internes Red-/Purple Teaming
- Adversary Emulation
- Threat Intelligence
- Begleitung von IT Projekten

„VERBUND SOC Offender #1“

Die Abteilung Informationssicherheit



Die Herausforderungen in der Security

Womit beschäftigt sich eigentlich ein Blue- und Red Team?

- Klassische Fragen des Managements …
  - Sind wir von der Schwachstelle XYZ betroffen?
  - Bekommen wir eine Alarmierung / wird dieser Angriff blockiert?
  - Wie viele Angriffe haben wir pro Monat?

- Fragen die wir uns im Blue- und Red-Team stellen …
  - Funktionieren unsere SOC Use Cases?
  - Welche SOC Use Cases fehlen uns?
  - Funktionieren unsere Tools die Angriffe erkennen sollen?
  - Welche Angriffe funktionieren?
  - Gab es bereits bestimmte Angriffe?

Blue Team bei VERBUND

Analyse von Security Events

Kontakt für Security Fragen

Incident Response

SOC Services

Betrieb der Schnittstellen

Use Case Design und Optimierung

24/7 internes Know-how verfügbar

Red Team bei VERBUND

Pen-Testing

Begleitung bei Projekten

Adversary Emulation

Security Engineering

Vulnerability Management

Attack Surface Reduction

Malware Analyse

Beispiel 1 – Projektarbeit EDR/EPP Toolauswahl

Technischer PoC bestehend aus drei Phasen:

1. Process Injection / Shellcode Execution (9 Tests)
2. Weaponised C2 beacons - mit und ohne Obfuscation (4 Tests)
3. Full Attack Chain (4 Tests)

Ziele der Zusammenarbeit zwischen Red- und Blue Team

- Erkennungsfähigkeiten der einzelnen Tools testen
- Analysefähigkeiten der einzelnen Tools testen

- 1CreateRemoteThread-DLL.exe
- 2CreateRemoteThread-SC.exe
- 3QueueUserAPC-SC.exe
- 4EarlyBird-APC.exe
- 5FunctionStomping.exe
- 6ThreadExecution-Hijacking.exe
- 7ReflectiveDLL-Injection.exe
- 8Process-Hollowing.exe
- 9Process-Ghosting.exe

Process Injection / Shellcode Execution Tests[2]

```
22      processHandle = OpenProcess(PROCESS_ALL_ACCESS, FALSE, x);
23      remoteBuffer = VirtualAllocEx(processHandle, NULL, sizeof shellcode, (MEM_RESERVE | MEM_COMMIT), PAGE_EXECUTE_READWRITE);
24      WriteProcessMemory(processHandle, remoteBuffer, shellcode, sizeof shellcode, NULL);
25      threadHandle = CreateRemoteThread(processHandle, NULL, 0, (LPTHREAD_START_ROUTINE)remoteBuffer, NULL, 0, NULL);
26      CloseHandle(processHandle);
```

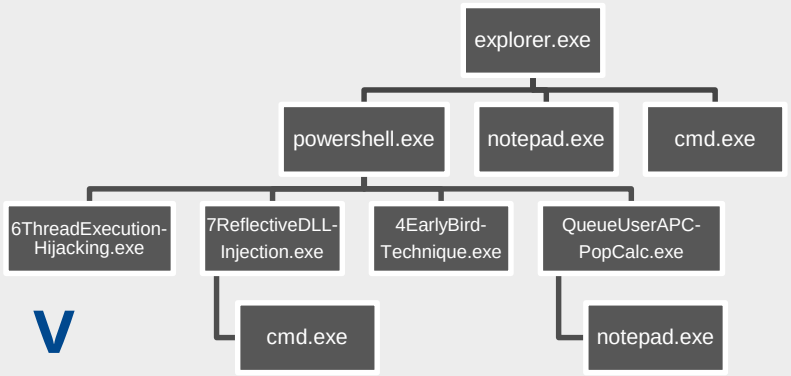
Beispiel „CreateRemoteThread“ Process Injection in C++ [1]

[1] Quelle: https://www.ired.team/offensive-security/code-injection-process-injection/process-injection
[2] PoCs von unterschiedlichen Autoren (u.A. idov31, hasherezade)

Informationen aus den einzelnen Tools

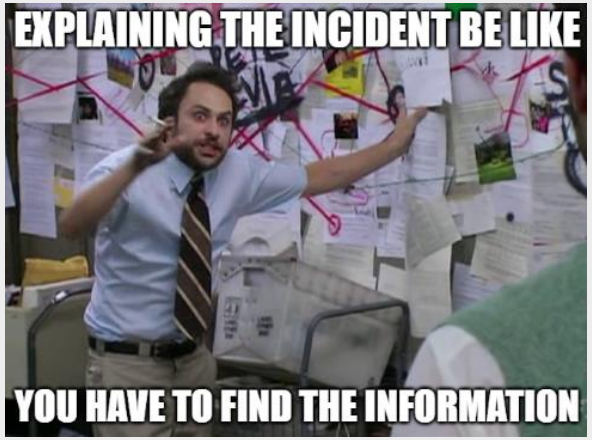
EDR Tool #1

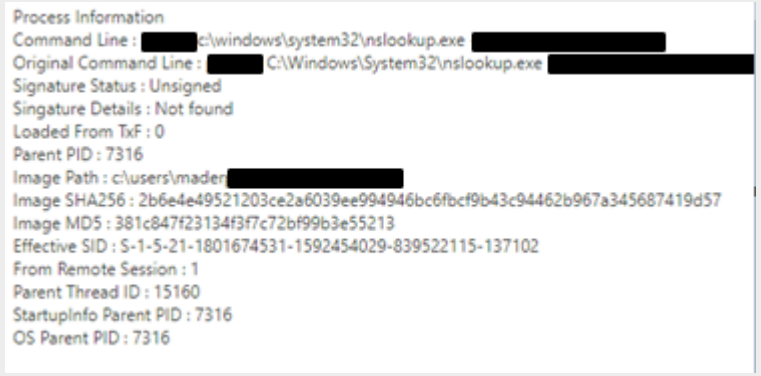
- 10 Medium Incidents



EDR Tool #2

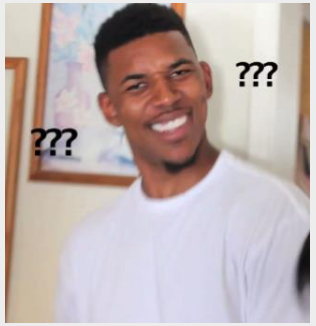
- 1 High, 2 Medium Incidents





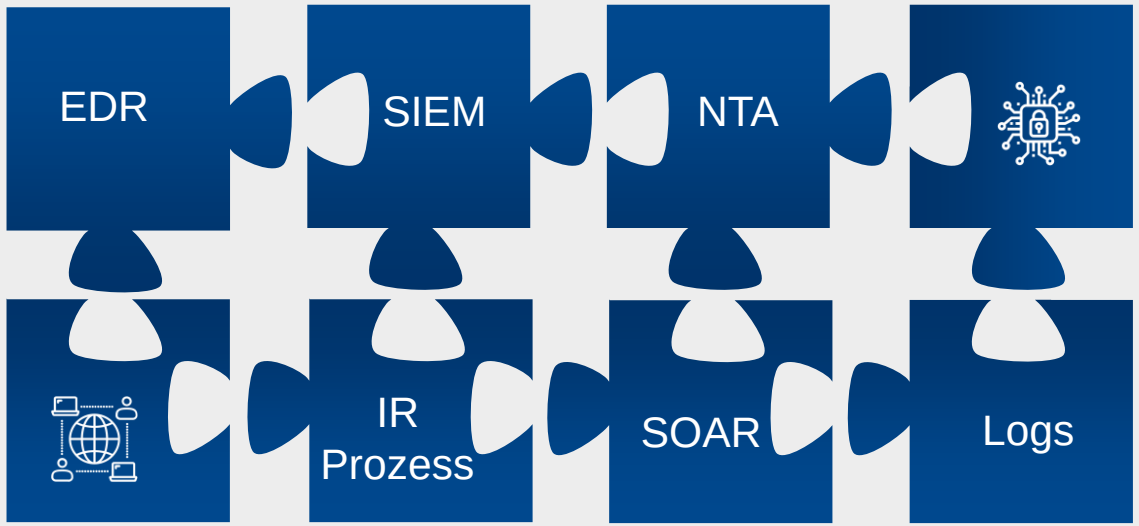
EDR Tool #3

- Kein Incident, wenige Detections



Erkenntnis aus Beispiel #1

Jedes Tool hat seine Stärken und Schwächen. Security Teams müssen sich auf die eingesetzten Tools einstellen!
Das perfekte Tool existiert nicht. Erst das Zusammenspiel mehrerer Werkzeuge erzeugt ein komplettes Bild.

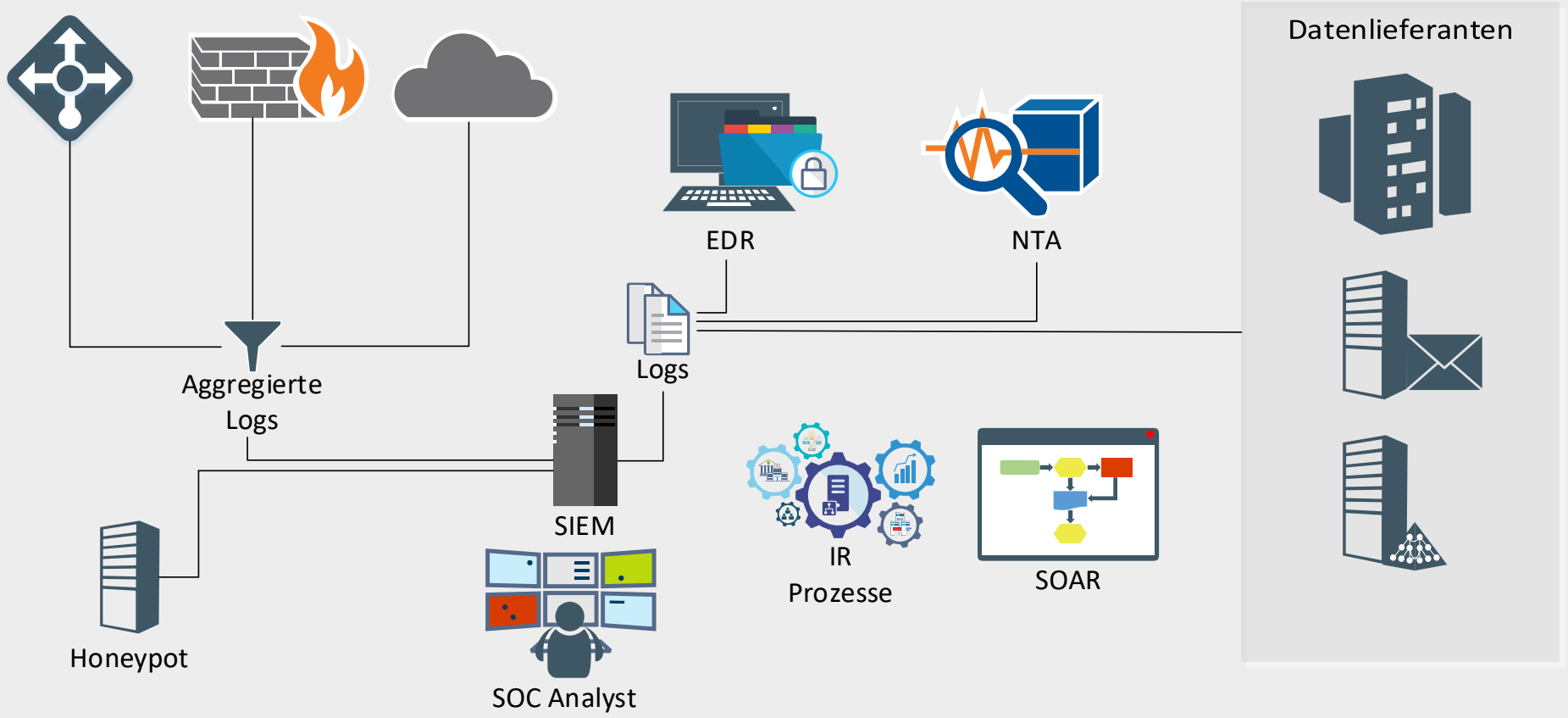


Normalerweise hat man keine C2 Beacons / Malware im Netzwerk

- Wie würden diese ausschauen?

Beispiel einer Security Landscape

Für den reibungslosen Betrieb eines SOC sind mehrere Systeme und deren Anbindung, sowie zahlreiche Datenquellen erforderlich.



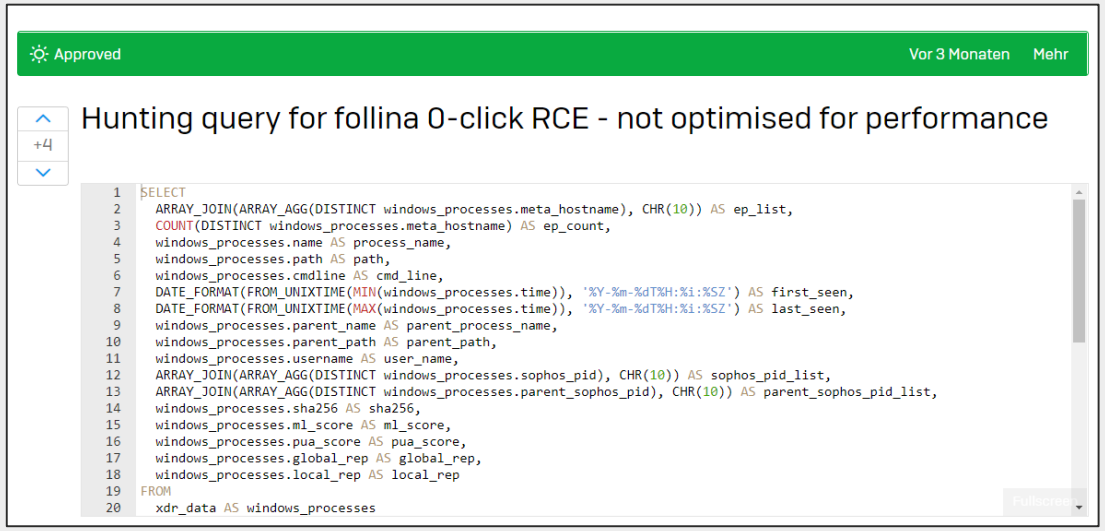
Beispiel 2 – Daily Business

Ehemalige 0-Klick RCE Schwachstelle Follina (CVE-2022-30190)

- Erstellung eines Proof-of-Concept
  - Oftmals gar nicht so leicht…
  - Ist der Angriff erfolgreich?
  - Wurde der Angriff lokal erkannt?

- Prüfung im SOC
  - Gibt es IOCs oder IOAs?
  - Wurde der Angriff bereits durchgeführt?
    - → Erstellung Hunting Query (last 30 days)
    - → Alarmierung bei erneuten Events

Implementierung Workaround mit IT
- Überprüfen ob Workaround / Alarmierung funktioniert



Approved Hunting Query

Erkenntnis aus Beispiel #2

Eine gute Zusammenarbeit zwischen Red und Blue Team ist essenziell
Red und Blue Teams haben andere Prioritäten und Sichtweisen

Des Weiteren ist auch zu beachten:

- Prominente Schwachstellen (z.B. EternalBlue, SeriousSAM, Follina) gehören sofort behandelt
- Ein SOC muss aktuelle und realistische Attack Techniques in der Produktivumgebung gesehen haben, um adäquat darauf reagieren zu können
- Internen Blue- und Red-Teams lernen bei der Zusammenarbeit voneinander, insbesondere deren Werkzeuge und Arbeitsweisen 

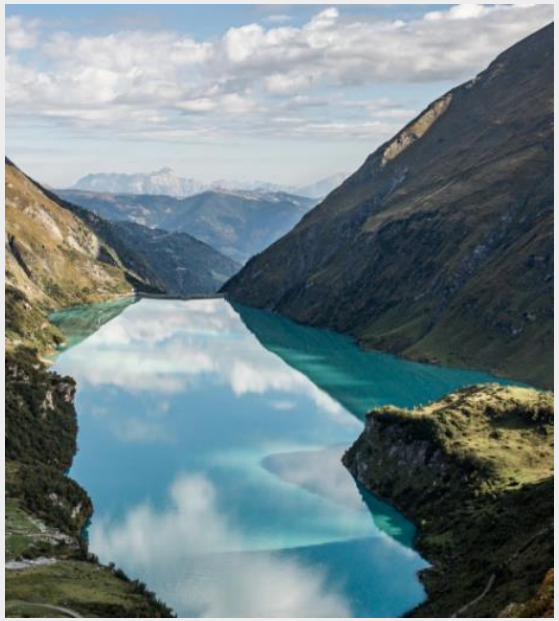
Weitere Erkenntnisse und Fokuspunkte

Herausforderungen in der Zusammenarbeit

- Kommunikation zwischen den Teams
- Wie viel darf das jeweils andere Team wissen?
- Was sind No-Go‘s in der Zusammenarbeit?
- Definition allgemeiner Spielregeln (ähnlich zur PtA bei externen)

Besonders spannend in der kritischen Infrastruktur

- Attraktives Ziel für Angreifer
- Hohe gesetzliche und regulatorische Anforderungen
- Hohe Vorsicht bei Pen-Tests / Red-Teamings erforderlich



Die Herausforderungen in der Security

Womit beschäftigt sich eigentlich ein Blue Team und ein Red Team?

- Klassische Fragen des Managements …

Sind wir von der Schwachstelle XYZ betroffen?	Kann das Red Team beantworten 
Erfolgt eine Alarmierung, wird dieser Angriff blockiert?	Kann das Blue Team beantworten 
Wie viele Angriffe haben wir pro Monat?	Kommt darauf an … ☺

- Fragen die wir uns im Blue- und Red-Team stellen …

Funktionieren unsere SOC Use Cases?	Sehen wir wenn das Blue Team grinst 
Welche SOC Use Cases fehlen uns?	Sehen wir wenn das Red Team grinst 
Funktionieren unsere Tools die Angriffe erkennen sollen?	Kann das Blue Team beantworten 
Welche Angriffe funktionieren?	Ausprobieren! Have fun, red team… 

Wir suchen!

Projektmanager:in OT Cyber Security Lab
(Vollzeit, Wien)

- Koordinieren von Kooperationen
- Gemeinsame Arbeit an Lösungsansätzen
- Überblick über Projektarbeiten und -entwicklungen rund um das OT Cyber Security Lab
- Anpassen der Projekte auf Basis von Marktbedürfnissen
- Schnittstelle zu internen und externen Stakeholder:innen, aufbereiten Entscheidungsgrundlagen

https://www.verbund.com/de-at/ueber-verbund/jobs-karriere/job/1555508

Entwickler:in Cyber-Security
(Voll- oder Teilzeit, Wien)

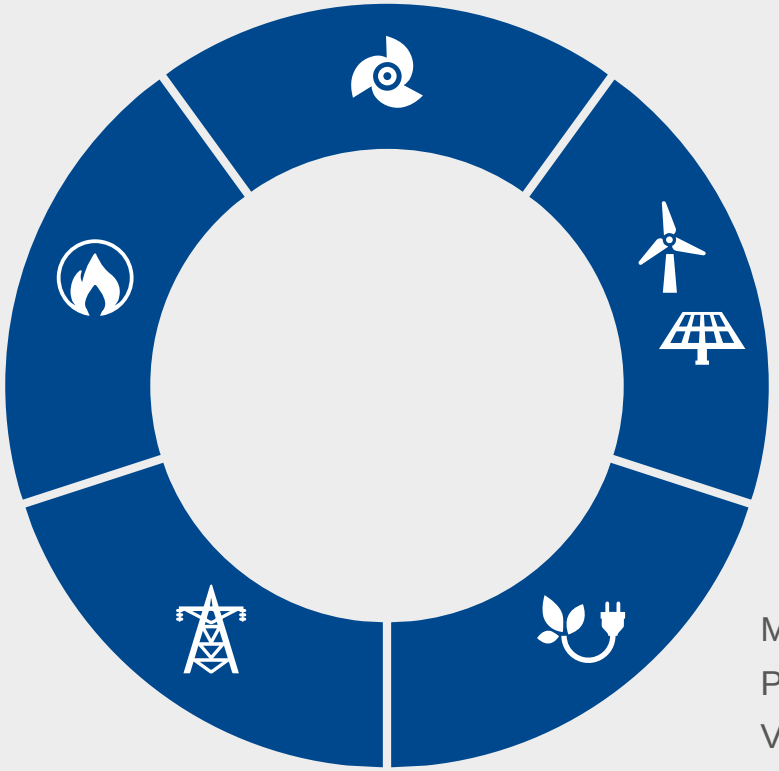
- Entwickeln von Erweiterungen und Anpassungen innerhalb der Security-Systeme
- Entwickeln automatisierter Schnittstellen von und zu diesen Systemen
- Mitarbeit beim Patch- und Versionsmanagement dieser Systeme
- Mitarbeit im „Tagesgeschäft“ des Security Operations Centers (SOC)

https://www.verbund.com/de-at/ueber-verbund/jobs-karriere/job/1555489

VERBUND auf einen Blick

129 Wasserkraftwerke von VERBUND mit über 8.300 MW Leistung.

Rund **900** Kilometer ist das Erdgas-Hochdruckleitungsnetz der GCA lang.



Bis zu **1/4** der Gesamterzeugung soll bis 2030 aus Sonnen- und Windkraft kommen.

Rund **3.400** Kilometer Trassenlänge hat das überregionale Stromnetz der APG.

Mehr als **500.000** Privatkund:innen setzten 2021 auf VERBUND.

Nachhaltige Energiezukunft
97 % Erzeugung aus erneuerbaren Energien

Wasserkraft[1]
>93 % der Stromerzeugung
129 Wasserkraftwerke
29.340 GWh Strom

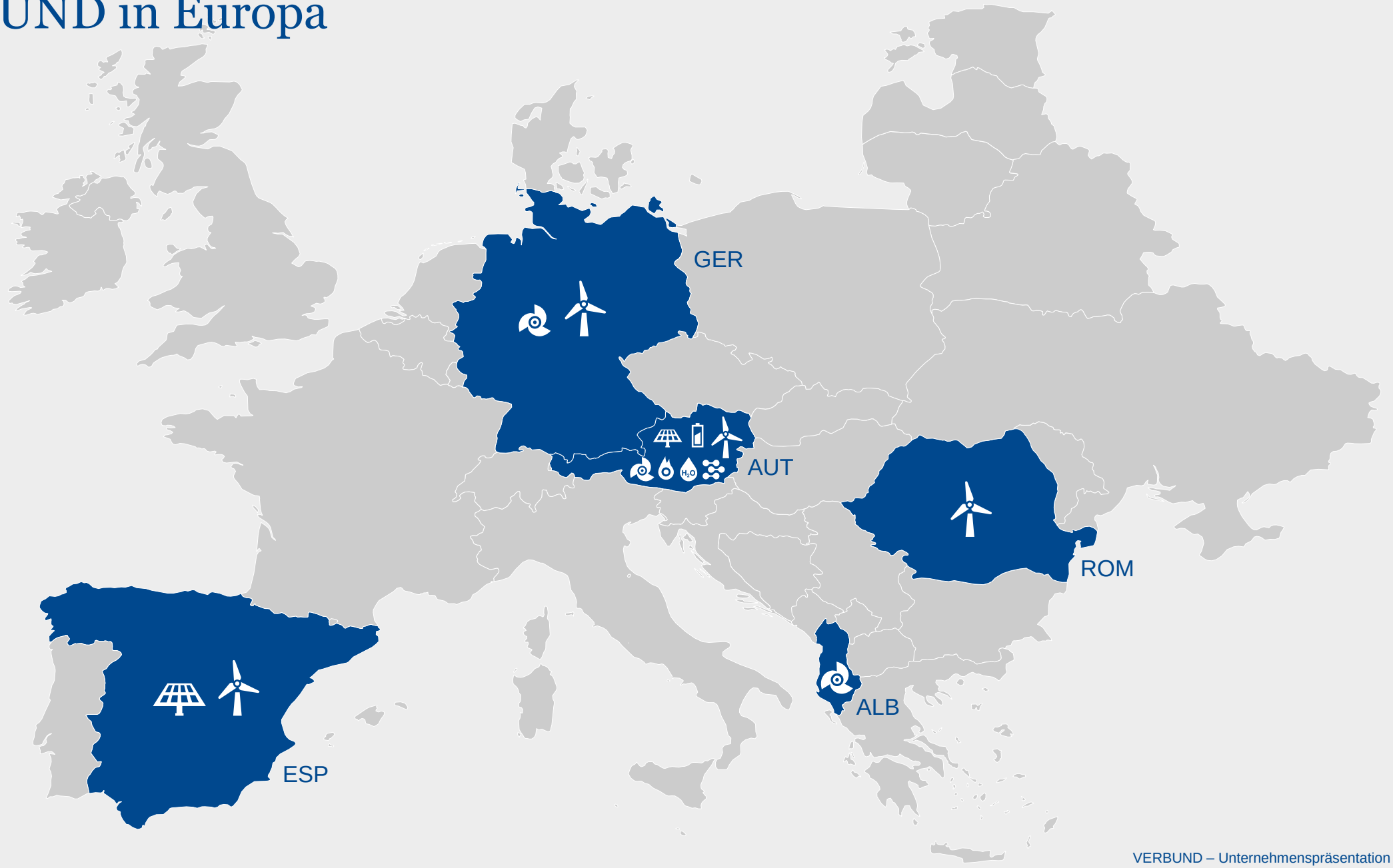
Wärmekraft
>4 % der Stromerzeugung
2 Wärmekraftwerke
1.125 GWh Strom

Windkraft
<3 % der Stromerzeugung
153 Windkraftanlagen
839 GWh Strom

Sonnenkraft[2]
<1 % der Stromerzeugung
5 Photovoltaikparks
2 GWh Strom

1 inklusive Bezugsrechte; ohne nicht-vollkonsolidierte Anlagen (Ashta 1&2 sowie Nussdorf)
2 ohne Leasing-/Contracting-Anlagen
Alle Werte IST Erzeugung 2021

VERBUND in Europa



Digitalisierung – Werkzeug der Energiezukunft?

#Vorangehen #Digitalisieren #Befähigen

- Digitalisierung und Innovation entlang der gesamten Wertschöpfungskette
- Kompetenzzentrum für effizienten und sicheren Einsatz von Technologie
- Bereitstellen moderner, sicherer Infrastruktur und Lösungen

Digitalisierung als Baustein

- der nachhaltigen Erzeugung und Verbesserung des Kundenerlebnisses
- für weitere Optimierung und Automatisierung
- zur Implementierung Digitaler Hilfsmittel

Technologie Masterplan

- umfasst Projekte der Digitalisierung, Informationssicherheit, IT und Telekommunikation
- dient der Planung und Koordination digitaler Innovationen
- ermöglicht eine optimale Vernetzung im Konzern

Vielen Dank!

Verbund