

Cyberangriffe erkennen: Open-Source Security Operations Center (SOC) mit Wazuh



DigiFors GmbH

**Erkennen.
Ermitteln.
Aufklären.**

Über mich



Stefan Rank-Kunitz
Leiter Security Operations Center
DigiFors GmbH

Softwareentwickler

IT-Security

Open Source

Beratung

DigiFors – IT-Security für den Mittelstand

Maßnahmen zur Prävention, Erkennung, Analyse und Reaktion auf Cyber-Bedrohungen in IT-Systemen

Prävention

Identifizierung von
Schwachstellen &
Angriffsvektoren

z.B. CVE-Management,
Pentests, Patch-
Management, IR-Plan

Echtzeit- Monitoring

24/7 Analyse von
Anomalien & Angriffen

z.B. Security Operations
Center (SOC), EDR, NDR

Forensik & Analyse

Untersuchung der
Ursachen &
Angriffswege

“die 3 Fragen klären“

Incident Response

Maßnahmen zur
Eindämmung &
Behebung

... im Ernstfall & in der
Vorbereitung darauf



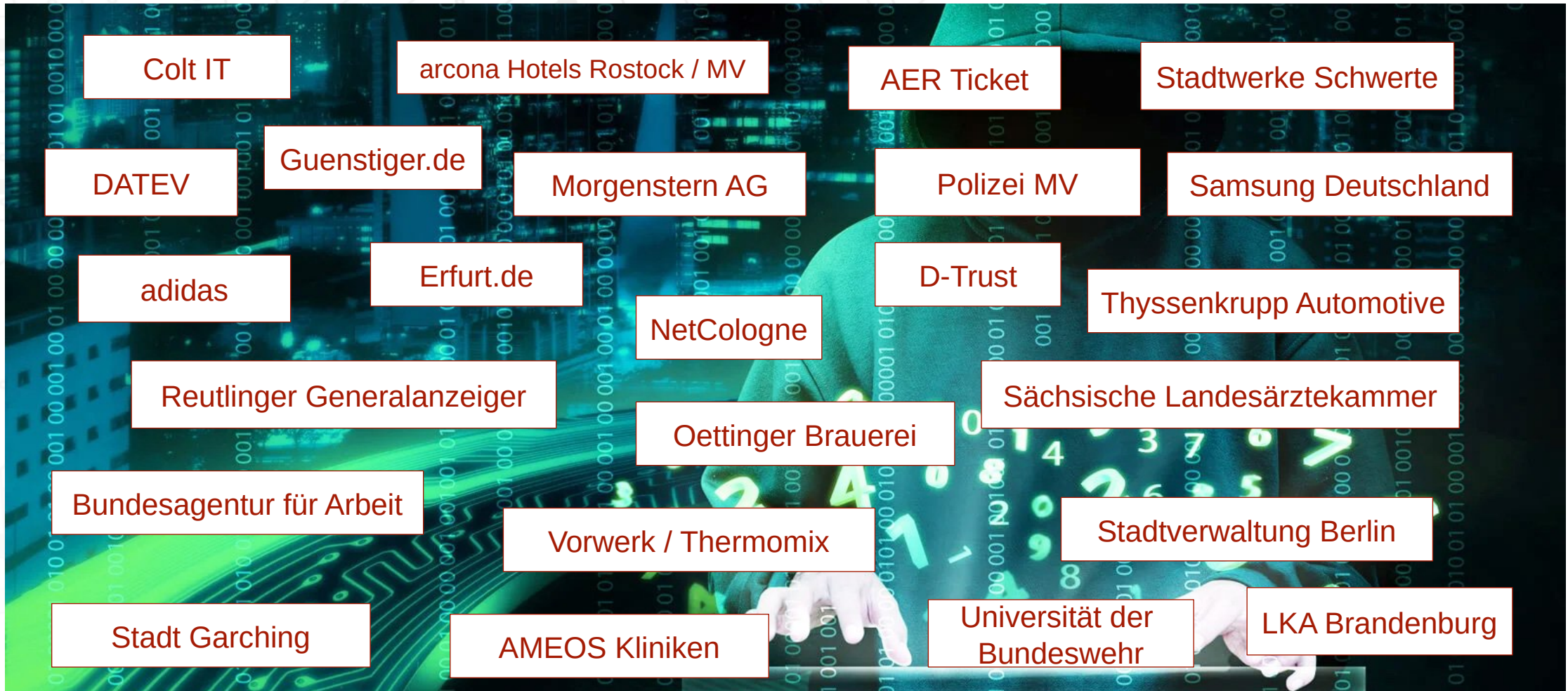
**YOU
ARE
FUCKED**

You are fucked – Deutschlands erste Cyberkatastrophe

Podcast-Reihe des Mitteldeutschen
Rundfunks (MDR) über den Hack des
Landkreises Anhalt-Bitterfeld im Juli 2021

(ARD Audiothek)

Hacks 2025 (Auszug)



Chronologie einer Katastrophe

„der Montag“

- alle IT-Systeme kaputt
- Produktion steht still
- kein Email & Telefon
- keine vordefinierten Verantwortlichkeiten
- kein Notfall-Budget

Incident Response

- „die mit den Feldbetten“
- Eindämmung
- Was ist betroffen?
- „die 3 Grundfragen“
- Zahlen oder Neuanfang?
- Analyse vor Ort oder remote?

Wiederaufbau

- Backups wiederherstellen
- „Waschstraße“
- Dienste nach Prio wieder aktivieren
- Was wollen wir „besser“ neu aufbauen?

SOC

- „Das brauchen wir nicht nochmal!“
- Echtzeit-Monitoring von Ereignissen
- präventive Maßnahmen
- 2te Meinung zur IT-Sicherheit

Wie funktioniert ein SOC?

Ereignisse in der IT-Infrastruktur

z.B.:

- ① Logins & Login-Versuche jeder Art
- ① User in Admin-Gruppe einfügen
- ① Datei-Downloads
- ① System-Dienste starten
- ① Programme mit Adminrechten starten
- ① Netzwerkverkehr über die Firewall
- ① Meldungen von EDR / AntiVirus
- ① Anmeldungen in Cloud-Diensten (z.B. M365)
- ① Netzwerk-Scans
- ① Malware, Rootkits, Ransomware



**24/7 Echtzeit-
Alarme**

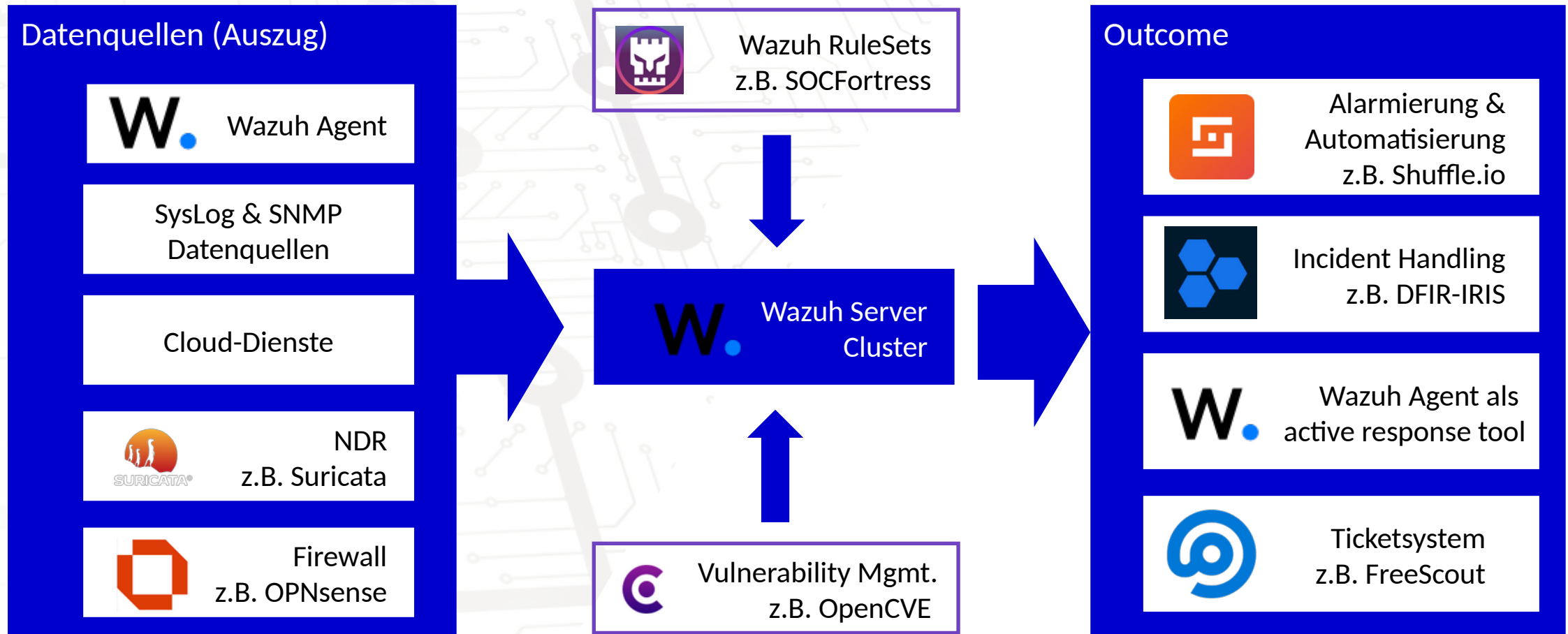


**Eindämmung
„active response“**



**Präventions-
Maßnahmen**

Umsetzung mit Open-Source



Wie hilft mir ein SOC?

aktive Sicherheit & Sichtbarkeit

Transparenz und
Nachvollziehbarkeit von
Vorgängen in einer IT-
Infrastruktur,
Alarmierung & Analyse
in Echtzeit

Infrastruktur- Verbesserung

Identifizierung von
Altlasten und
Sicherheitsproblemen,
Engpässen (z.B.
Netzwerk) und Fehlern
(z.B. Anmelde-
Probleme)

Prävention

Sichtbarkeit auf
Präventivmaßnahmen
(z.B. CVEs, Updates &
Patches, ...)

Der Blick von außen

Security Checks und
Empfehlungen, z.B.
Hardening und
Pentesting

Aufbau einer SOC-Dienstleistung

Phase 1: Bestandsaufnahme

- Kennenlernen
- IT-Infrastruktur Aufnahme
- Cloud-Dienste
- Client- und Server-Systeme
- Defensivsysteme
- Authentifizierungssysteme
- usw.

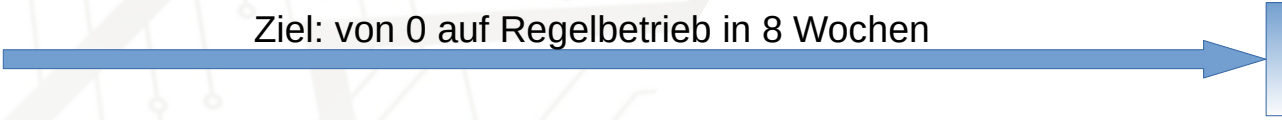
Phase 2: Aufbau

- Installation SIEM-Systeme
- Anschluss Datenquellen (Clients, Server, Firewall, ...)
- Einrichtung Alarme
- Wöchentl. Regelmeeting

Phase 3: Regelbetrieb

- 24/7 Echtzeit Monitoring
- Regelm. Wartung der Monitoring-Systeme
- Stetige Weiterentwicklung
- Monatl. Regelmeeting

Ziel: von 0 auf Regelbetrieb in 8 Wochen



Fragen oder Anregungen?



Vielen Dank für Ihre Aufmerksamkeit!

Nico Müller
Geschäftsführer

Stefan Rank-Kunitz
Leiter Security Operations Center



<https://digifors.de/>



<https://www.linkedin.com/company/digifors/>

