G DATA CyberDefense

Managed **E**ndpoint **D**etection & **R**esponse

Made in Germany

Stefan Hausotte

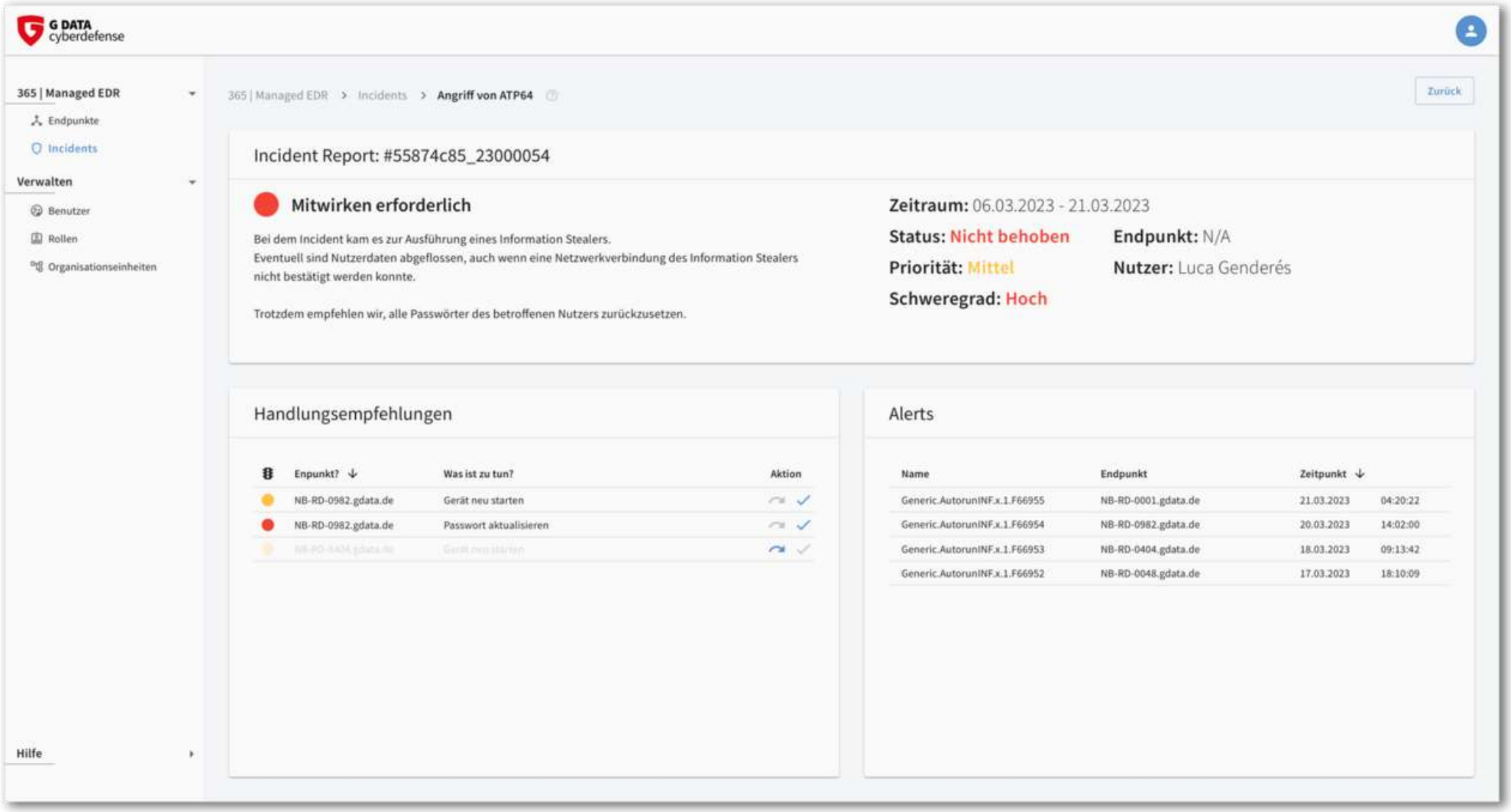
Head of Threat Intelligence

G DATA CyberDefense AG

Stefan.Hausotte@gdata.de

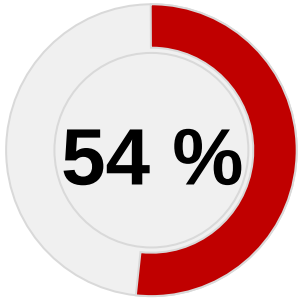
G DATA CyberDefense

Managed DER – Made in Germany



G DATA 365 Managed EDR

Zahlen, Daten, Fakten



der Cyberangriffe in den letzten zwei Jahren haben den Mitarbeitenden als Einfallstor ausgenutzt.

9 von 10

der deutschen Unternehmen waren in den letzten zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen.

223 Mrd. € Schaden

an deutscher Wirtschaft durch analoge & digitale Angriffe pro Jahr.

Quelle: Bitkom, 2022

G DATA CyberDefense

Ressourcenmangel

- Fast immer gibt es frühzeitig Anzeichen für einen bevorstehenden oder gerade aktiven Angriff
- Meldungen der AV-Lösung, Firewall, Sandbox und E-Mail-Gateways
- Trotzdem kommt es zum Schadensfall mit Vollverschlüsselung von Kerninfrastruktur und Lösegeldforderungen

→Wieso wurde der Angriff trotz Logmeldungen nicht erkannt?

→Fehlen zur Sichtung und Bewertung von Logmeldungen Zeit und Expertise?

Die Lösung: MEDR

M Dienstleistung beauftragen (**Managed**) statt Fachkräfte aufzubauen oder einzustellen

E Daten und Meldungen auf **Endpoints** sammeln

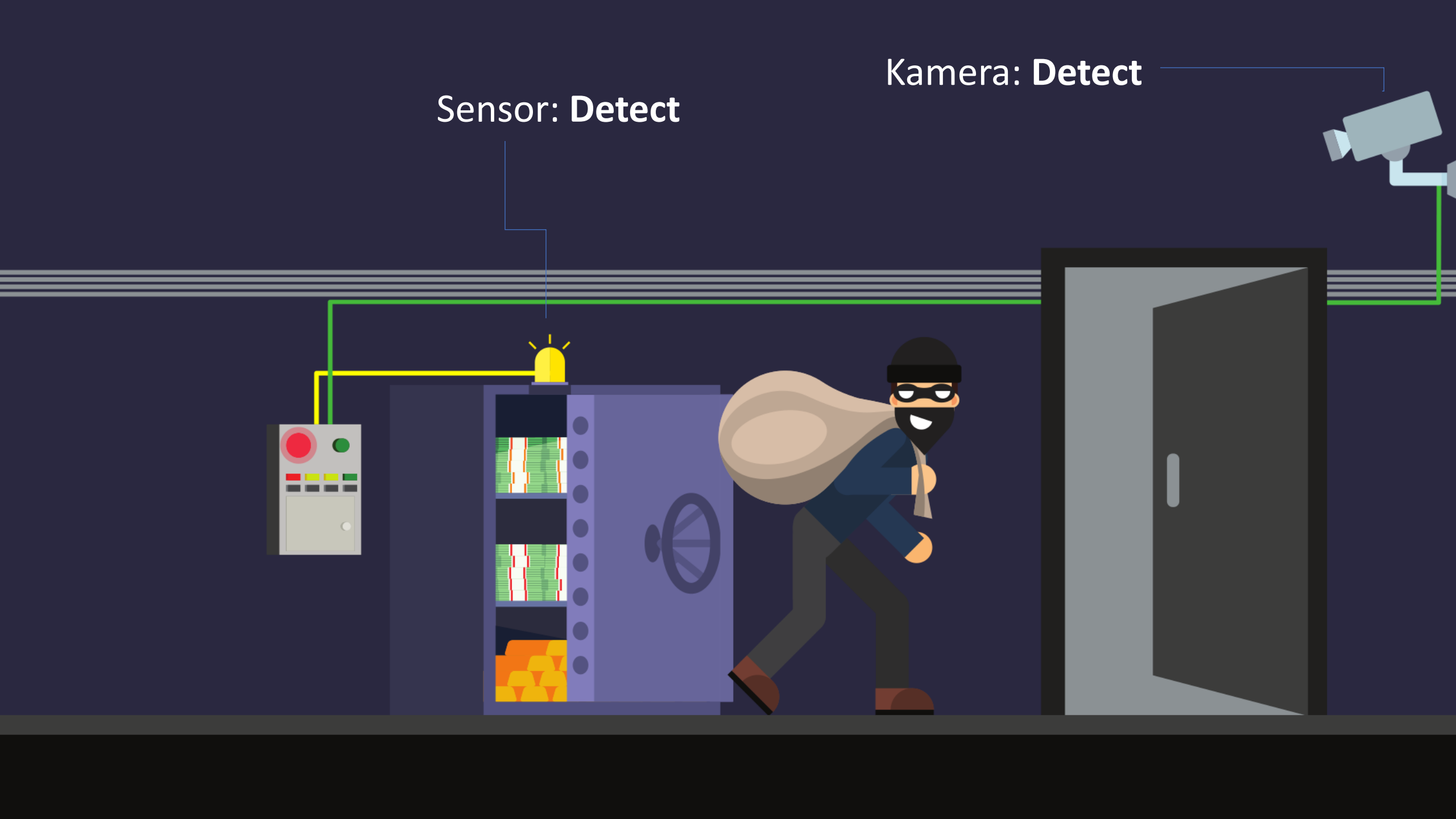
D Eventuelle Bedrohungen analysieren (**Detection**)

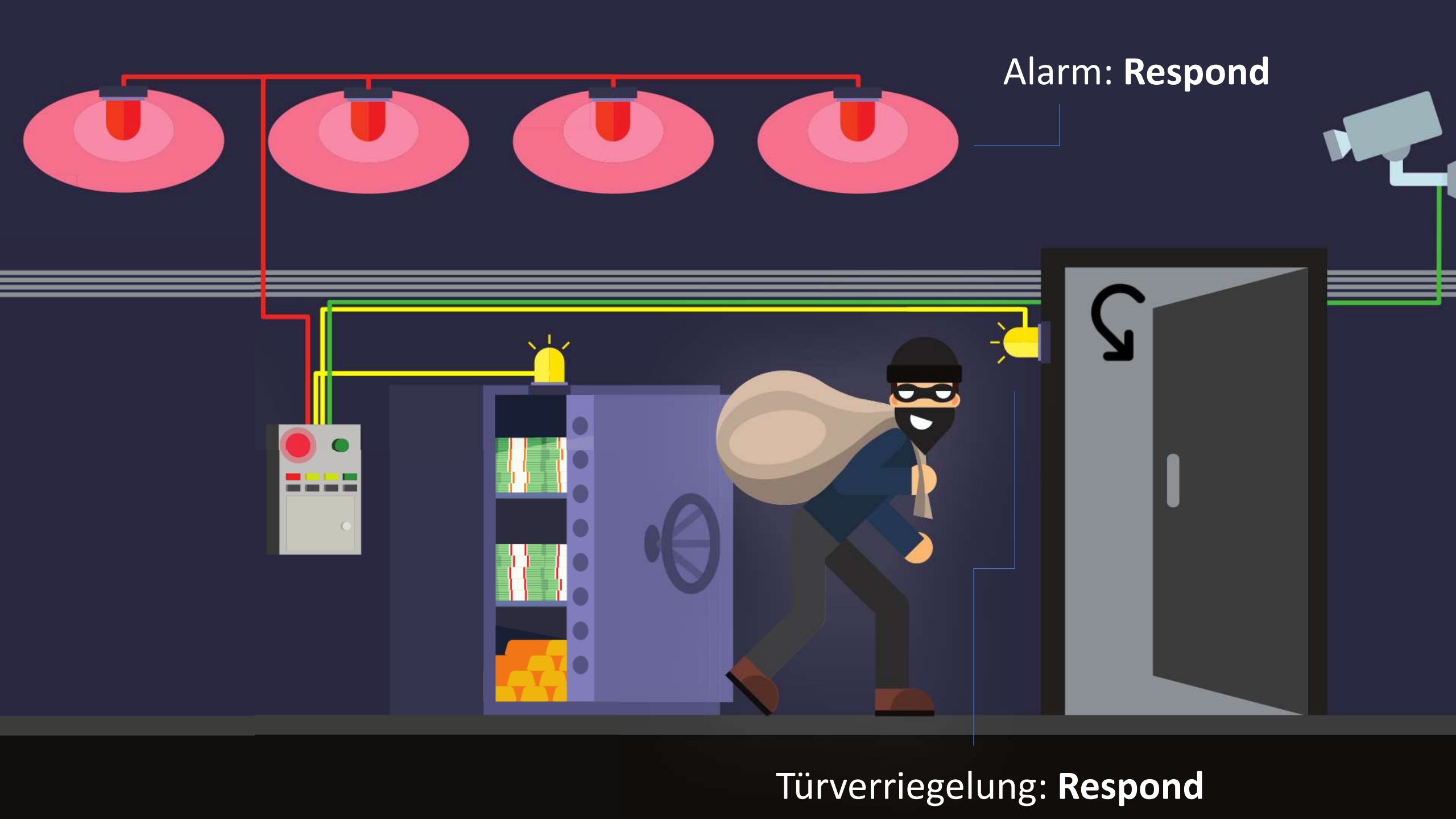
R Erkannte Bedrohungen entfernen, reporten und Handlungsempfehlungen geben (**Response**)

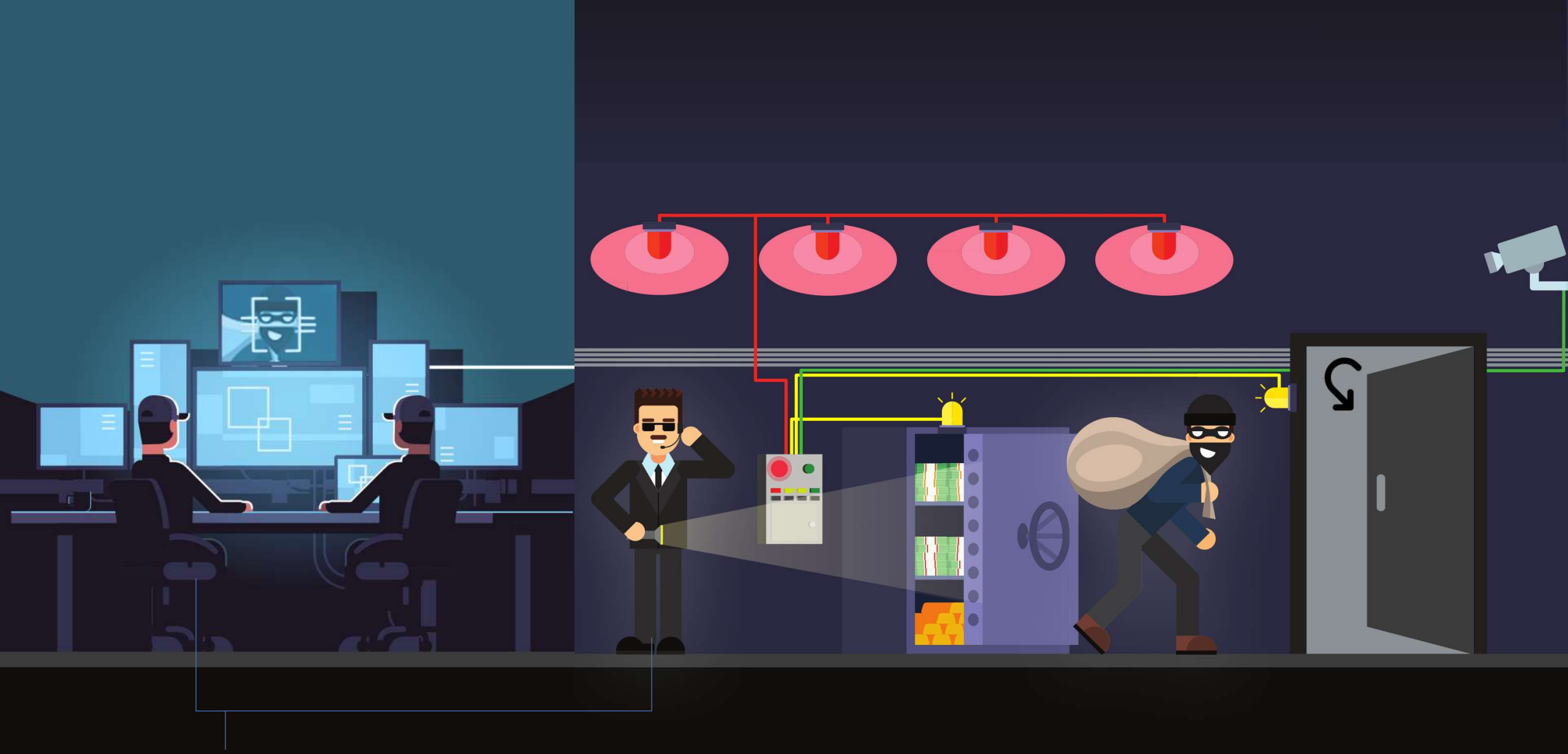
Tresor: **Prevent**

Kamera: **Detect**

Sensor: **Detect**




Alarm: **Respond**
Türverriegelung: **Respond**



Wachpersonal: Managed **Detect & Respond**

Self-Managed EDR: Eine kostspielige Angelegenheit

Beispielrechnung für eine SOC/EDR-Plattform

8 Analysten
(Minimalanforderung für 24/7-Schichtbetrieb)

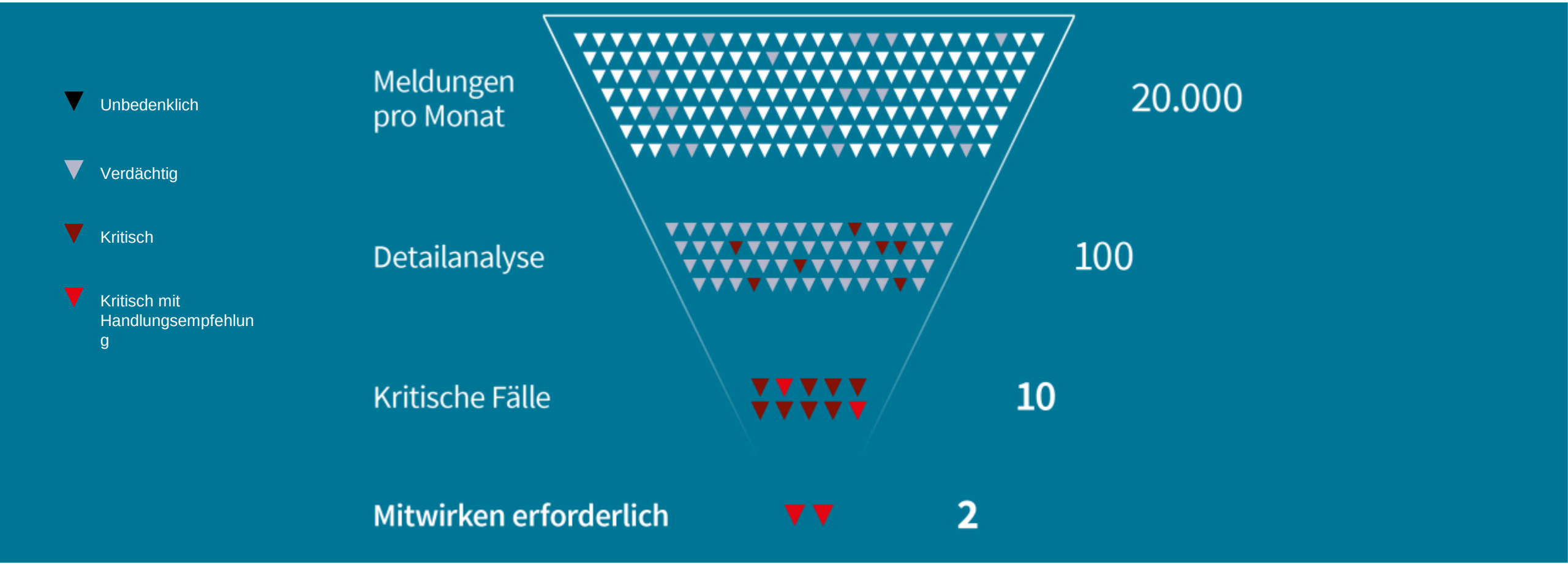
1-2
Führungskräfte

Benötigte Infrastruktur und Software

Threat Intelligence Databases

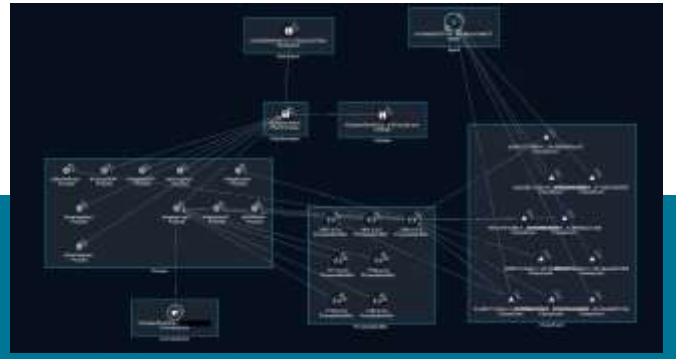
Kosten: ca. 1.000.000 € pro Jahr

Self-Managed EDR: Analyse Funnel



G DATA 365 Managed EDR

Wie läuft MEDR ab?

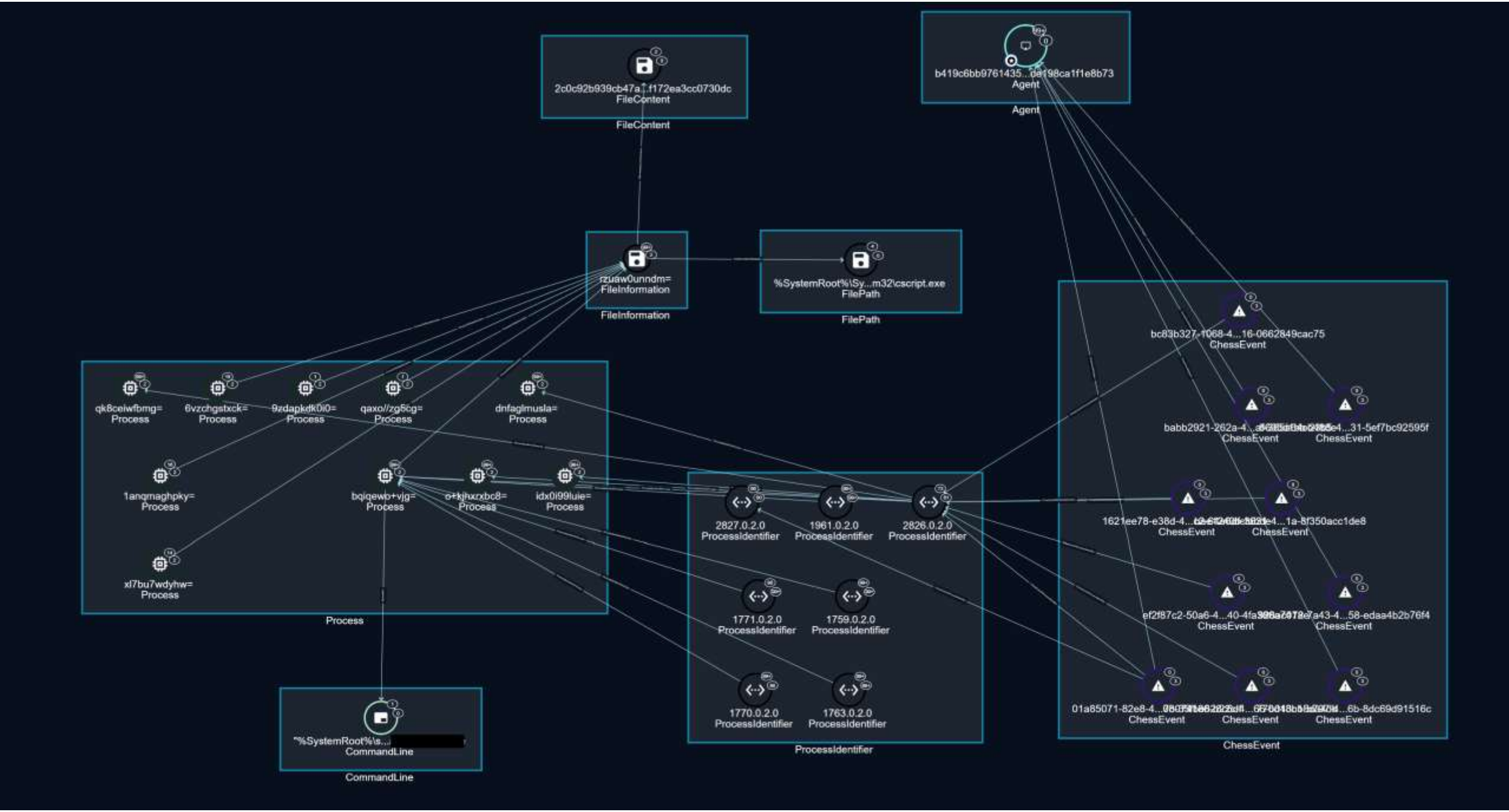


Alert auf einem Endpoint

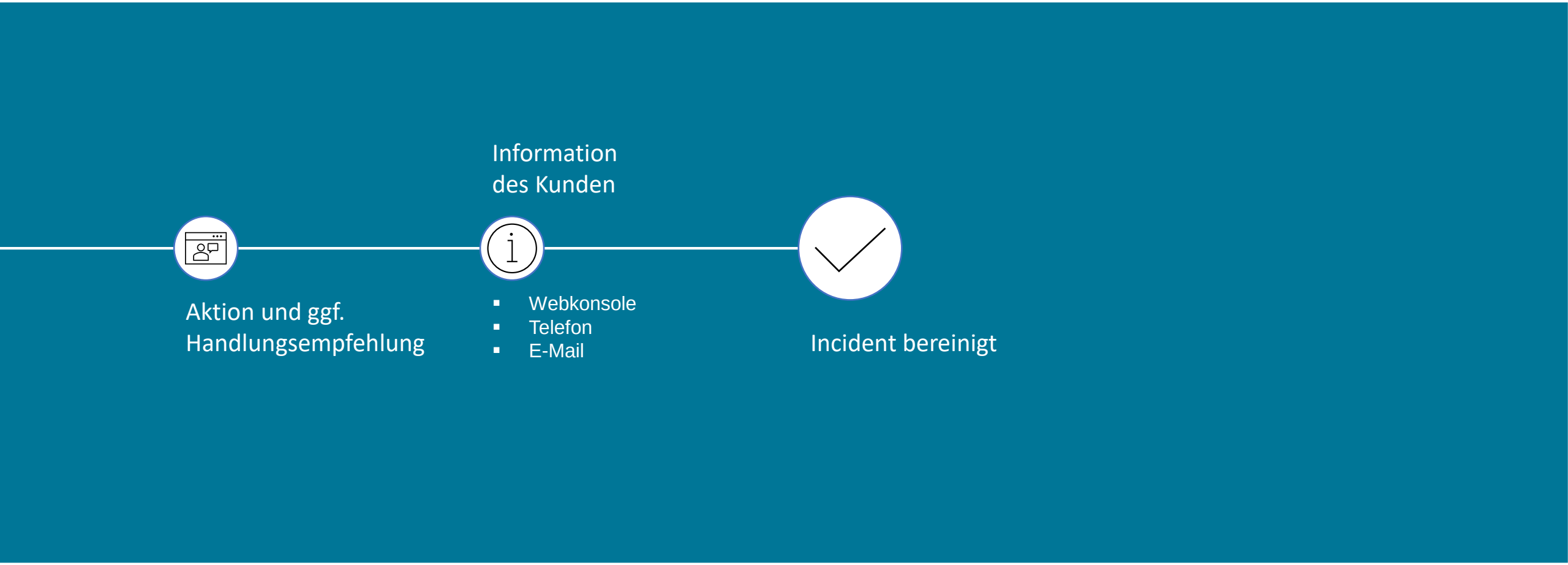
Anlegen eines Incidents

Incident wird Analyst*in zugewiesen

Analyst*in betrachtet Incident genauer


2c0c92b939cb47a...f172ea3cc0730dc
FileContent
FileContent
b419c6bb9761435...0a198ca1f1e8b73
Agent
Agent
rzuaw0unndm=
FileInformation
FileInformation
%SystemRoot%\Sy...m32\cscript.exe
FilePath
FilePath
qk8ceiwfbmg=
Process
6vzchgstxck=
Process
9zdapkdk0i0=
Process
qaxo//zg5cg=
Process
dnfaglmusla=
Process
1anqmaghpky=
Process
bqiqewp+vjg=
Process
o+kjhxrxbc8=
Process
idx0i99luie=
Process
xl7bu7wdyhw=
Process
Process
2827.0.2.0
ProcessIdentifier
1961.0.2.0
ProcessIdentifier
2826.0.2.0
ProcessIdentifier
1771.0.2.0
ProcessIdentifier
1759.0.2.0
ProcessIdentifier
1770.0.2.0
ProcessIdentifier
1763.0.2.0
ProcessIdentifier
ProcessIdentifier
"%SystemRoot%\s...
CommandLine
CommandLine
bc83b327-1068-4...16-0662849cac75
ChessEvent
babb2921-262a-4...31-5ef7bc92595f
ChessEvent
ChessEvent
1621ee78-e38d-4...1a-8f350acc1de8
ChessEvent
ChessEvent
ef2f87c2-50a6-4...58-edaa4b2b76f4
ChessEvent
ChessEvent
01a85071-82e8-4...6b-8dc69d91516c
ChessEvent
ChessEvent
ChessEvent
ChessEvent

Wie läuft MEDR ab?



Managed EDR Made in Germany

Gebündelte Expertise direkt vom Unternehmenshauptsitz in Bochum:

- Team von Security-Analysten
- Deutschsprachiger Support (mehrfach für hohe Qualität ausgezeichnet)
- Entwicklung der Managed EDR Software
- BSI-qualifiziertes Incident Response Team