

Tatort Digital: Wie eine Spurensuche auf dem Computer abläuft

Know-How to go: Response

HiSolutions AG

Nicolas Sprenger

Nicolas Sprenger

Consultant



- Experte für IT-Forensik
 - Forensische Beweissicherung und Analyse
 - Threat-Hunting
 - Schulungsreferent
- Mitverantwortlich für den Bereich Threat-Intelligence
 - Wissenschaftlicher Background in der Militär- und Digitaethik
- Technische Unterstützung bei Incident-Response-Einsätzen

A long cable-stayed bridge spans across a body of water under a dramatic, cloudy sky at sunset. The bridge features a prominent central pylon with two towers and numerous stay cables. The sun is low on the horizon, casting a warm glow over the scene.

Agenda

1. Was ist Forensik?

2. Ziele der (IT-)Forensik

3. Durchführung und Vorbereitung einer IT-forensischen Analyse

Was ist Forensik?

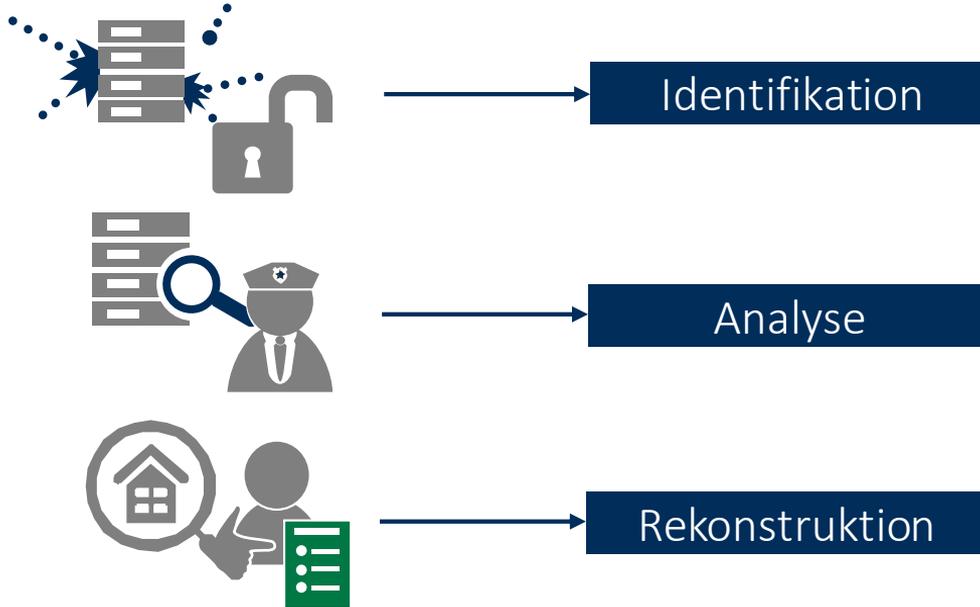
CRIME SCENE DO NOT CROSS



” Überall dort, wo er geht, was er berührt,
was er hinterlässt, auch unbewusst,
all das dient als stummer Zeuge gegen ihn. ”

Edmond Locard

Erkenntnisse über (kriminelle) Handlungen



Ziele der Forensik

Alt Gr



Strg



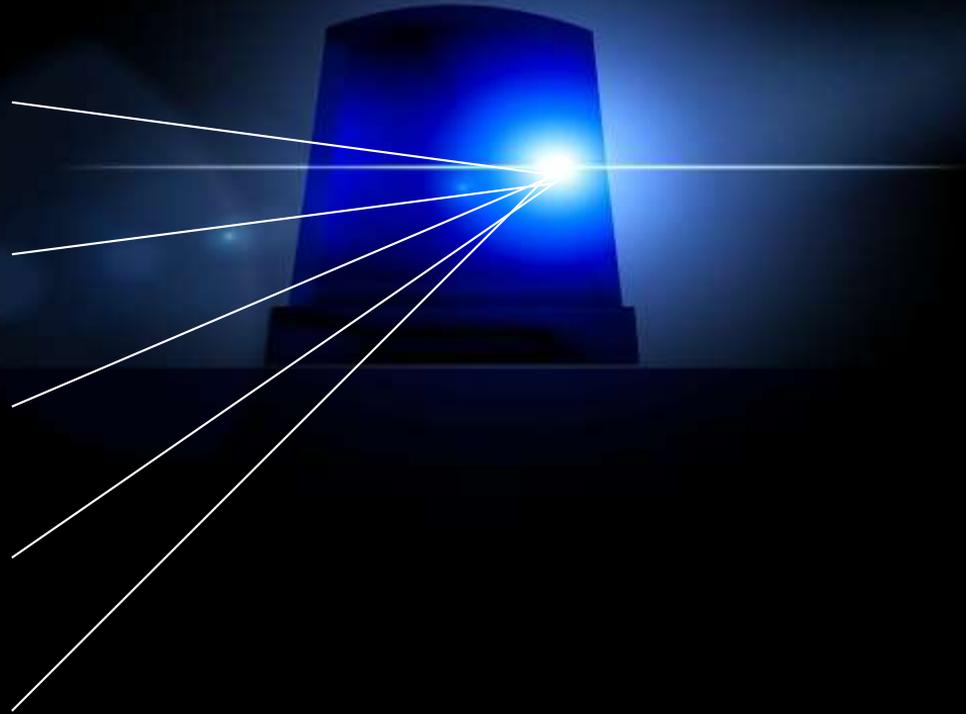
Was ist geschehen?

Wo ist es passiert?

Wann ist es passiert?

Wie ist es passiert?

Wer hat es getan?



Erkenntnisse in der IT-Forensik

Was ist geschehen?

Kill Chain/Kompromittierung

Wo ist es passiert?

Betroffene Systeme

Wann ist es passiert?

Angriffszeitpunkt

Wie ist es passiert?

Einfallsvektor

Wer hat es getan?

Attributierung

Anforderungen an eine forensische Analyse



Akzeptanz



Integrität



Glaubwürdigkeit



Ursache und Auswirkungen



Wiederholbarkeit

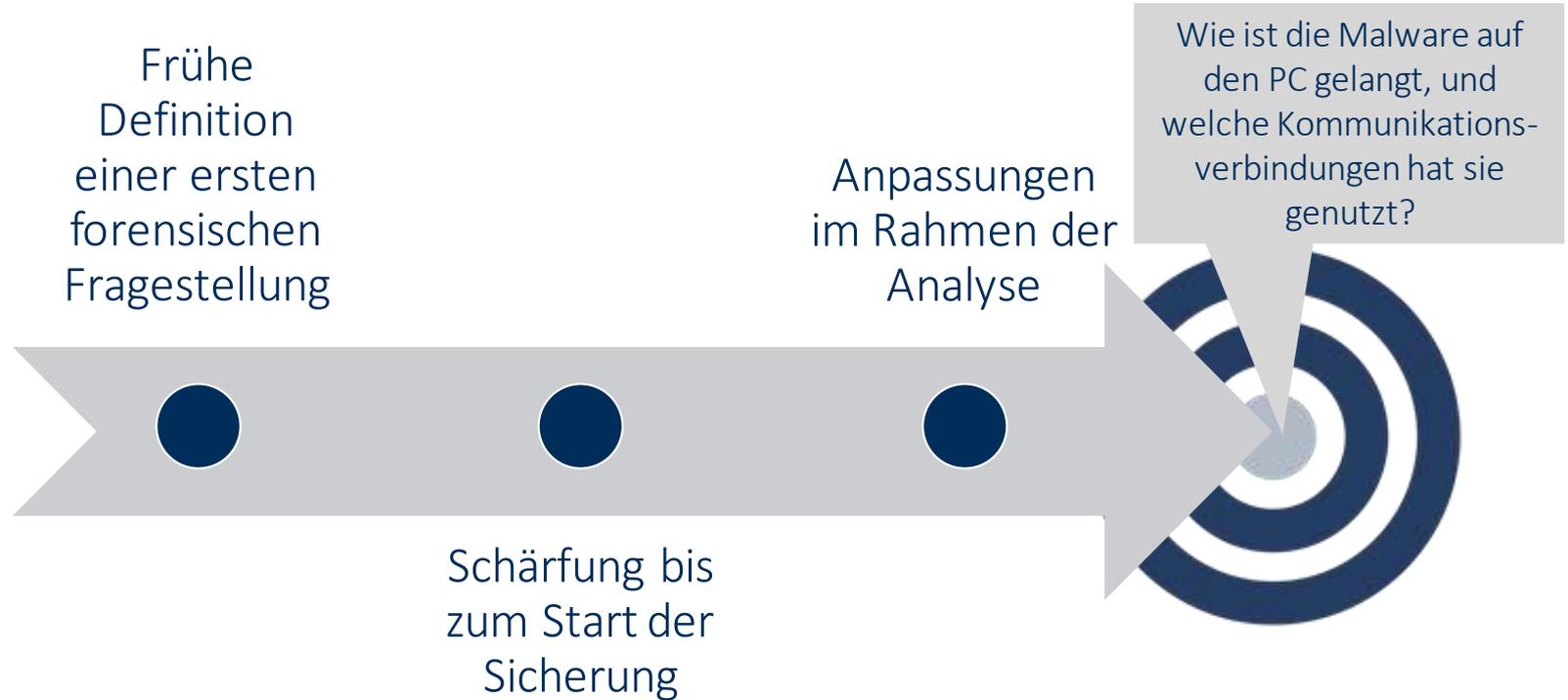


Dokumentation

Durchführung und Vorbereitung einer IT-forensischen Analyse



Definition einer forensischen Fragestellung



Ablauf einer forensischen Analyse



Vorbereitung für den Fall der Fälle?



Wie es nicht sein sollte: IT-Forensik-Edition



[Quelle](#)



[Quelle](#)

Logging: ein konstantes Spannungsfeld

Maximale Aufklärung

- Zeitraum (90 Tage+)
- Fokus auf Userinteraktion und Security-/Errorlogs
 - Nachvollziehbarkeit von Angriffswegen
- Zentrale Speicherung

Datenschutz/Compliance

- Möglichst geringe Speicherdauer
- Adäquater Umfang der Logs
- Zugriffsschutz und Zugriffsregelung für Logdaten

Was sollte geloggt werden?

- ~~„Es kommt drauf an.“~~
- Baseline-Logging:
 - [OWASP-Logging-Cheat-Sheet](#)
 - [Microsoft Audit Policy Recommendations](#)
 - [Logging Recommendations for Internet-Facing Servers \(RFC6302\)](#)
 - [Draft: DSGVO-Konformität RFC6302](#)
 - [BSI: Configuration Recommendations for Windows 10 Logging](#)

” You can have data without information,
but you cannot have information without data.

”

Daniel Keys Moran

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com