DCSO
Engineering Security.
Together.

„Keine Chance“
Ist die Zentralisierung von Logs am Ende?

Thomas Hemker, CISSP, CISM, CISA, CDPSE

2023-10-11 it-sa 2023, Nürnberg

TLP: GREEN

Mit wem sprecht Ihr?
Zur Person

Thomas Hemker, CISSP, CISM, CISA
Director Cyber Defense

- 28 Jahre Cyber-Security
- Threat Intelligence, Advisory Board
- BSI Expertenkreis
- ENISA ETL Stakeholder Group (bis 2020)
- ISACA, (ISC)2, TeleTrust, (prev. ISF Advisory Council)
- Sprecher, Autor, Lehrbeauftragter
- NAI, PGP, SYMC, DCSO
- Hamburg

researchgate.net/profile/Thomas_Hemker3

Cyber Security … … by Design or by Counterplay?

linkedin.com/in/themker

xing.com/profile/Thomas_Hemker/cv

Angriffserkennung

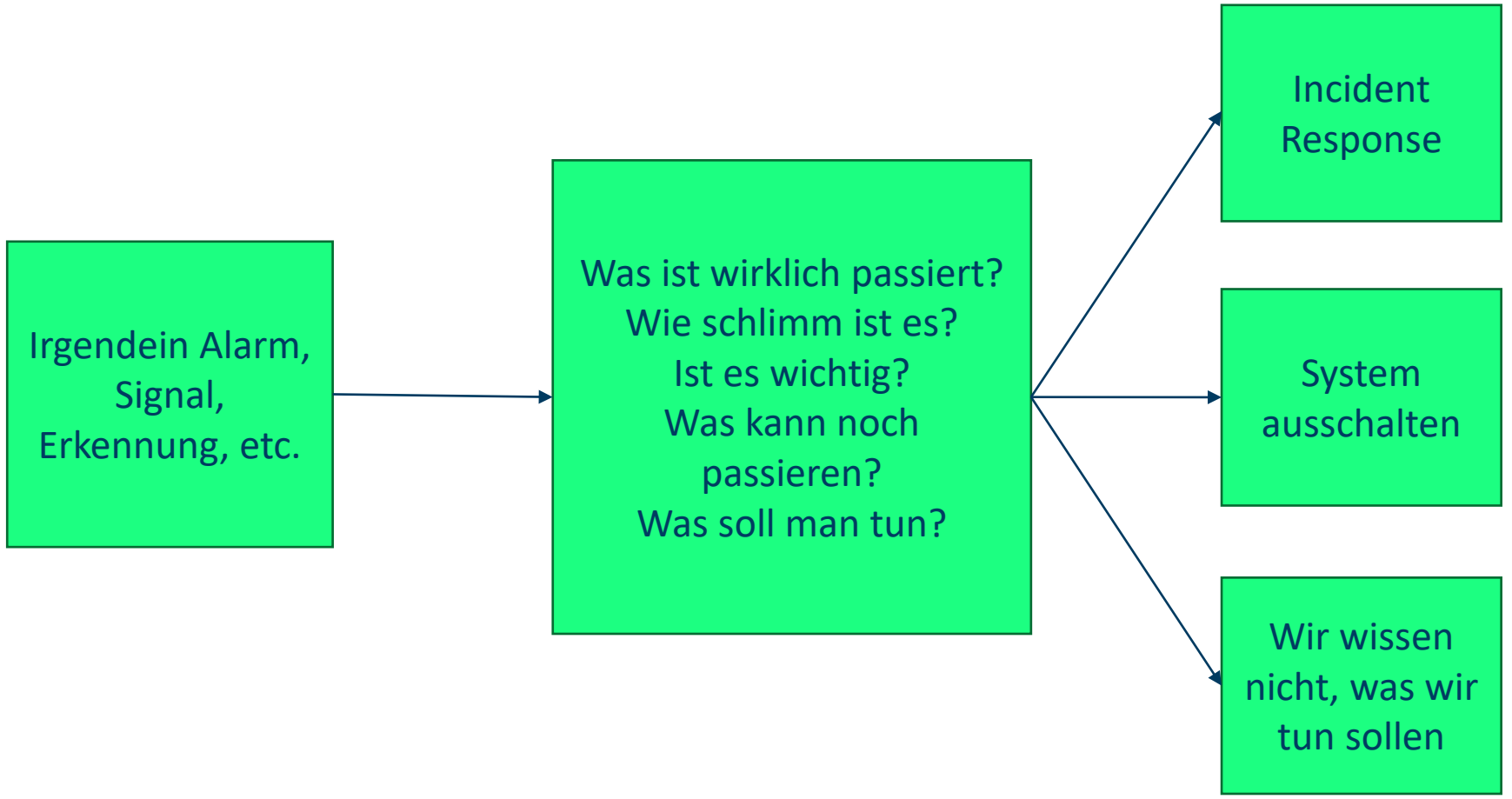
Themen, die wir besprechen wollen

- Schutz und Abwehr von Angriffen erfordert Wissen und dessen Austausch
- Grosse Datenmengen, viel Rauschen
- Schwierig zu Operationalisieren

- Threat Intelligence in der Security Architektur
- Diskussion Anwendung, Standards und Entwicklungen
- Verständnis zwischen Akteuren der Abwehrseite, wo es was zu tun gibt

Unsicherheit

Angriffserkennung muss nicht einfach sein



Wo suchen und finden?

Telemetriedaten, Alarme, Lösungen, Platzierungen

- Logdaten
- SIEM
- Datalakes
- Cloud
- …

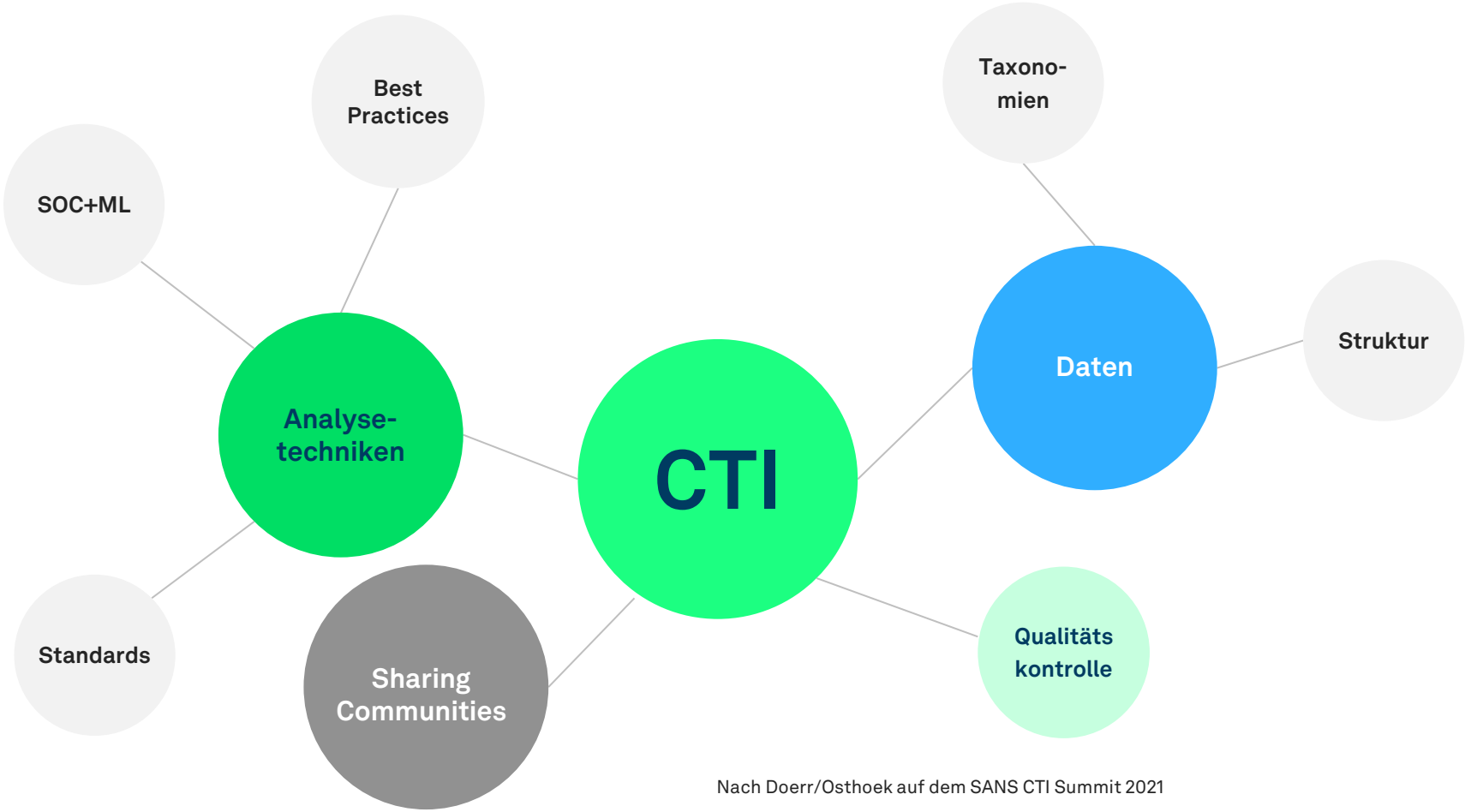
- EDR
- NDR
- xDR
- MDR
- IDS/IPS
- Firewall/Proxy

- Active Directory
- Kritische Applikationen
- DNS
- DHCP
- ….

- Incident Response
- Threat Hunting

- Perimeter
- Intern
- Extern

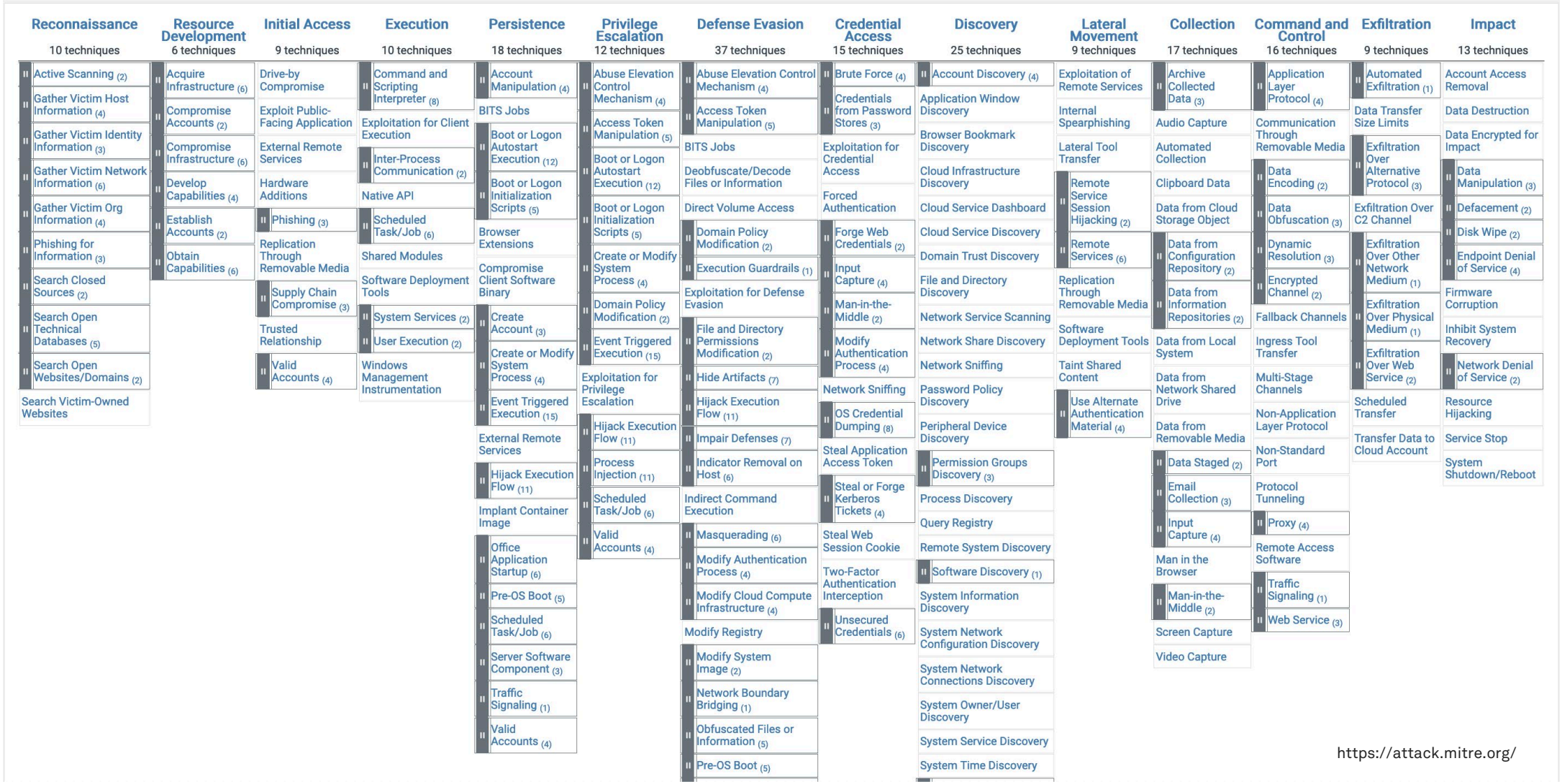
Was und wer ist beteiligt?
Grundlagen für die Operationalisierung



Nach Doerr/Osthoek auf dem SANS CTI Summit 2021

MITRE Att&ck Framework

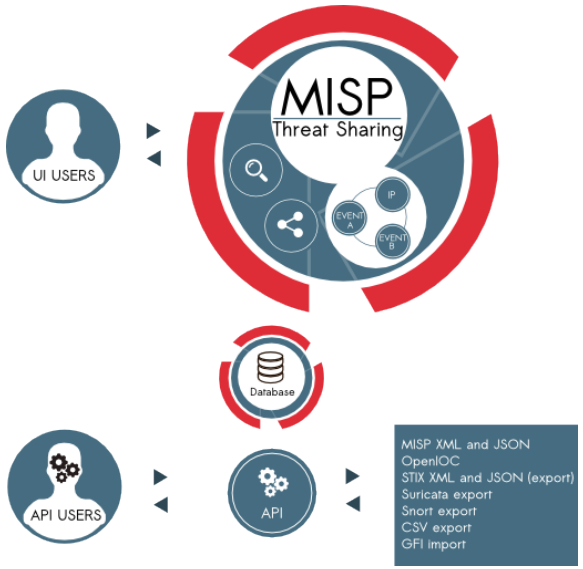
Wissen in der Anwendung - Beispiel

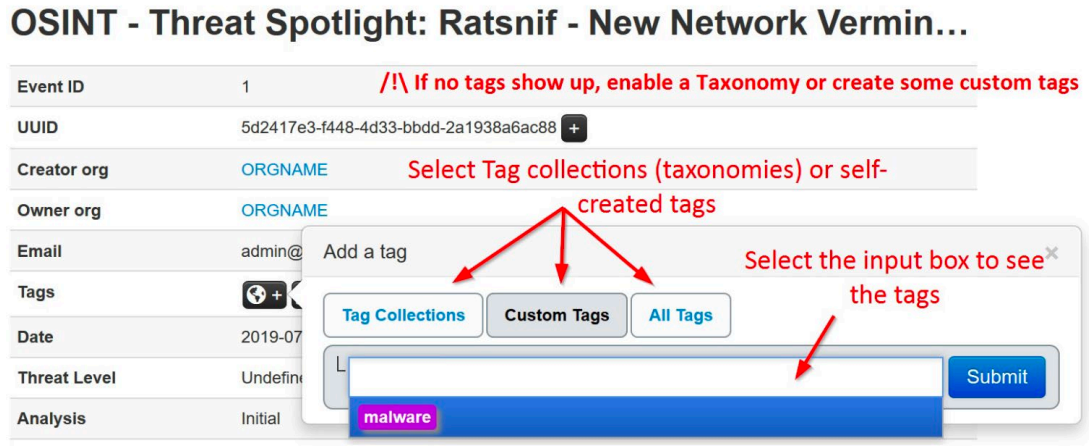


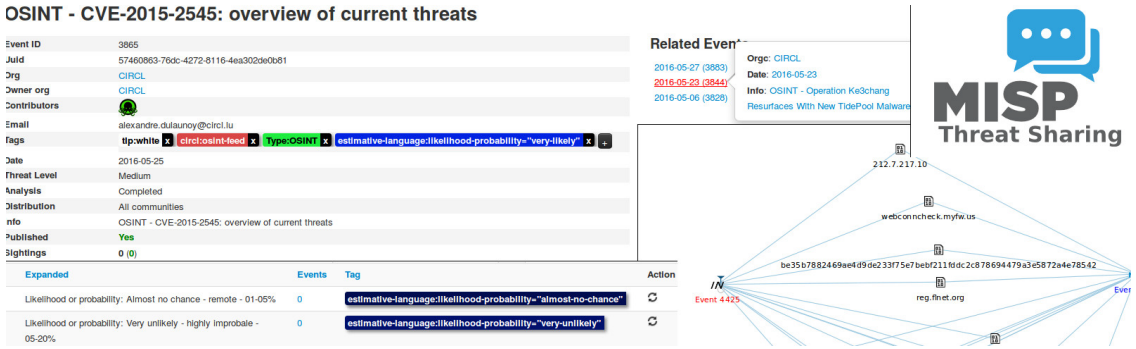
https://attack.mitre.org/

MISP

Beispiel für die Übermittling von technischen Indikatoren







https://circl.lu/services/misp-malware-information-sharing-platform/#what-is-misp

- Open Source Platform
- CIRCL. LU

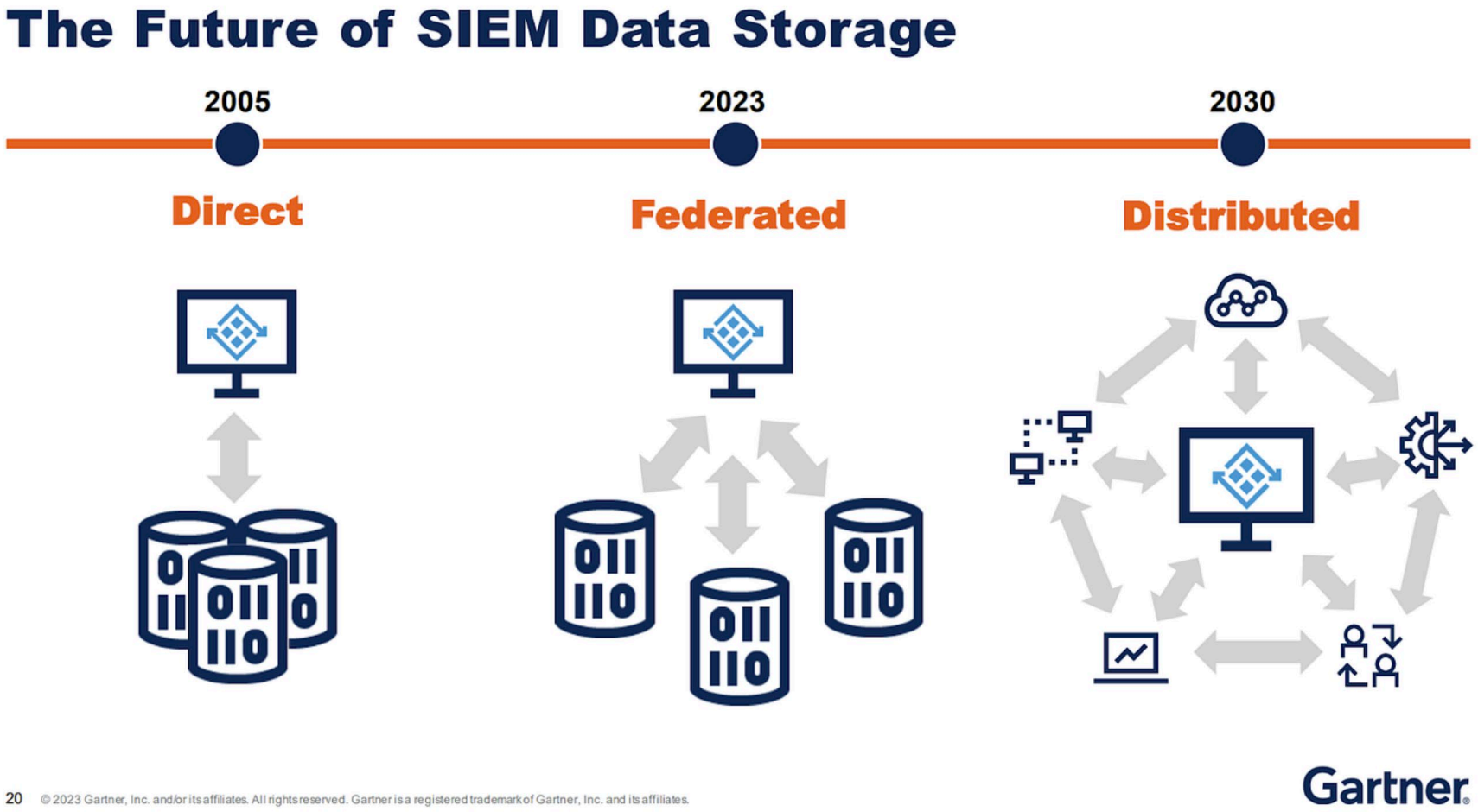
- IoCs
- Actor Information
- Fraud Information
- Kontext

- Verteilung
- Speicherung
- Korrelation

- TIP/TIM
- STIX/TAXII

Wie entwickelt sich die Verarbeitung von Logs?
...und die Anwendung von Threat Intelligence

Entwicklung der SOC Werkzeuge
Daten



(source: Gartner Security Summit 2023 presentation)

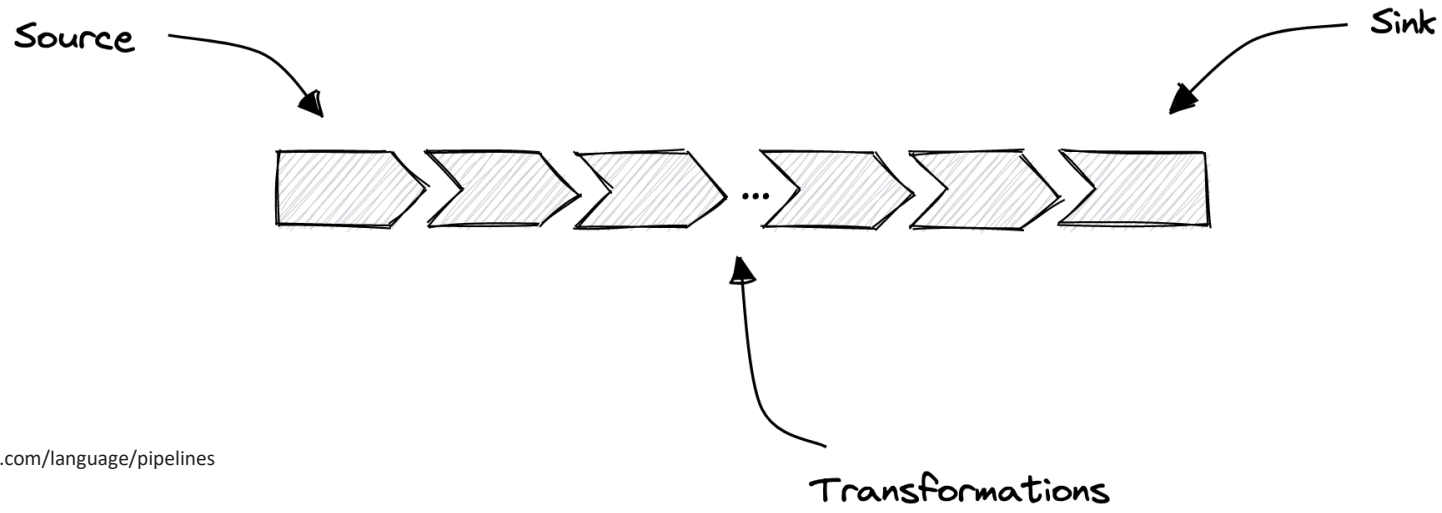
Zentral definiert und verteilt gespeichert

Federated Security Log Management

Tenzir distinguishes three types of operators:

1. **Source**: generates new data
2. **Transformation**: modifies data
3. **Sink**: consumes data

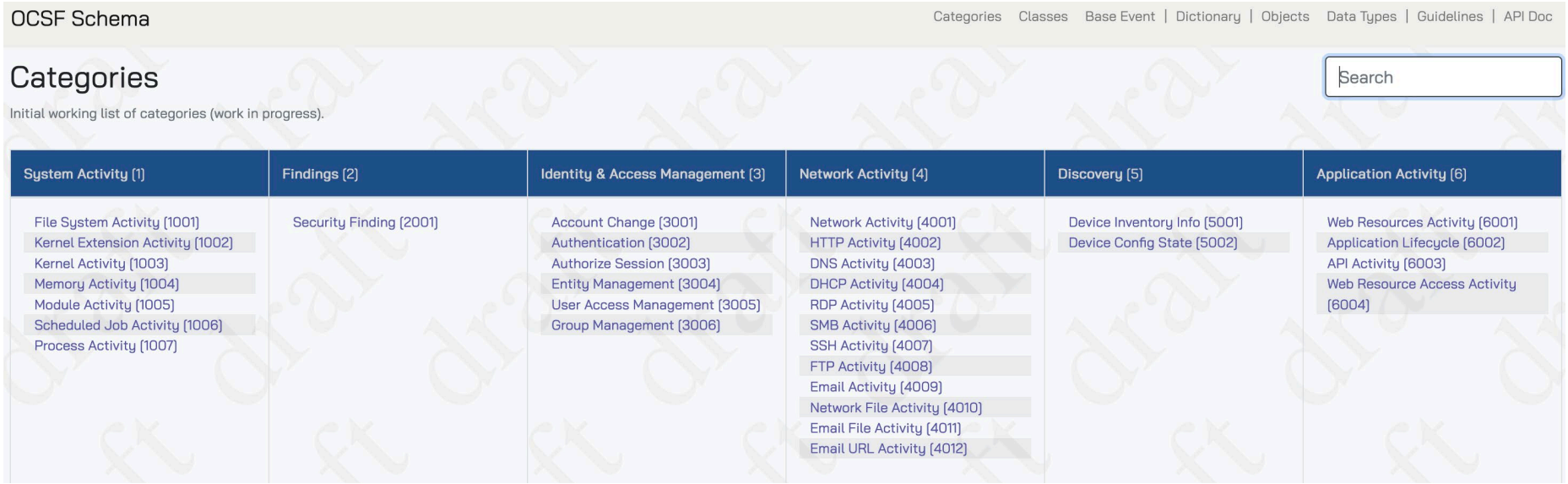
A pipeline consists of one source, one sink, and zero or more transformations. The diagram below illustrates the operator chaining:



https://docs.tenzir.com/language/pipelines

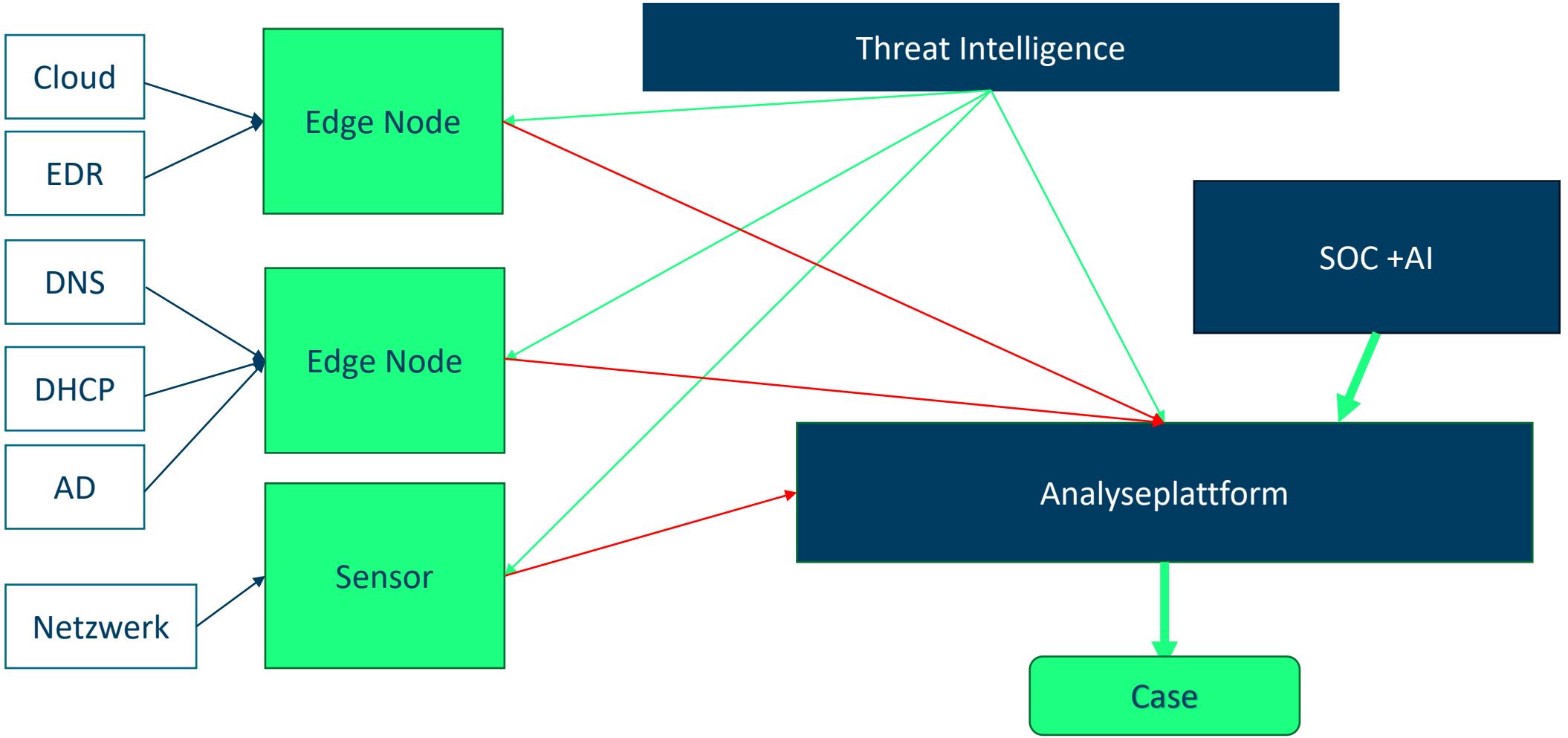
OCSF
Open Cybersecurity Schema Framework

- IBM, Splunk, AWS, Cloudflare, PAN, Salesforce, TrendMicro, Rapid7, ZScaler etc.
- Datenmodel für Logs
- Taxonomy
  - Data Types, Attributes an arrays,Attribute Dictionary, Event classes, Categories, Profiles and Extensions
- Enrichment; Kategorisierung - Starke Verbindung zu MITRE Att&ck
- https://github.com/ocsf/



Operationalisierung

Events – TI – Alarme – Analyse - Cases



DCSO
Engineering Security.
Together.

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
EUREF-Campus 22
10829 Berlin

TLP: GREEN