

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



Thomas Hemker, CISSP, CISM, CISA, CDPSE



2023-10-11 it-sa 2023, Nürnberg

Mit wem spricht 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

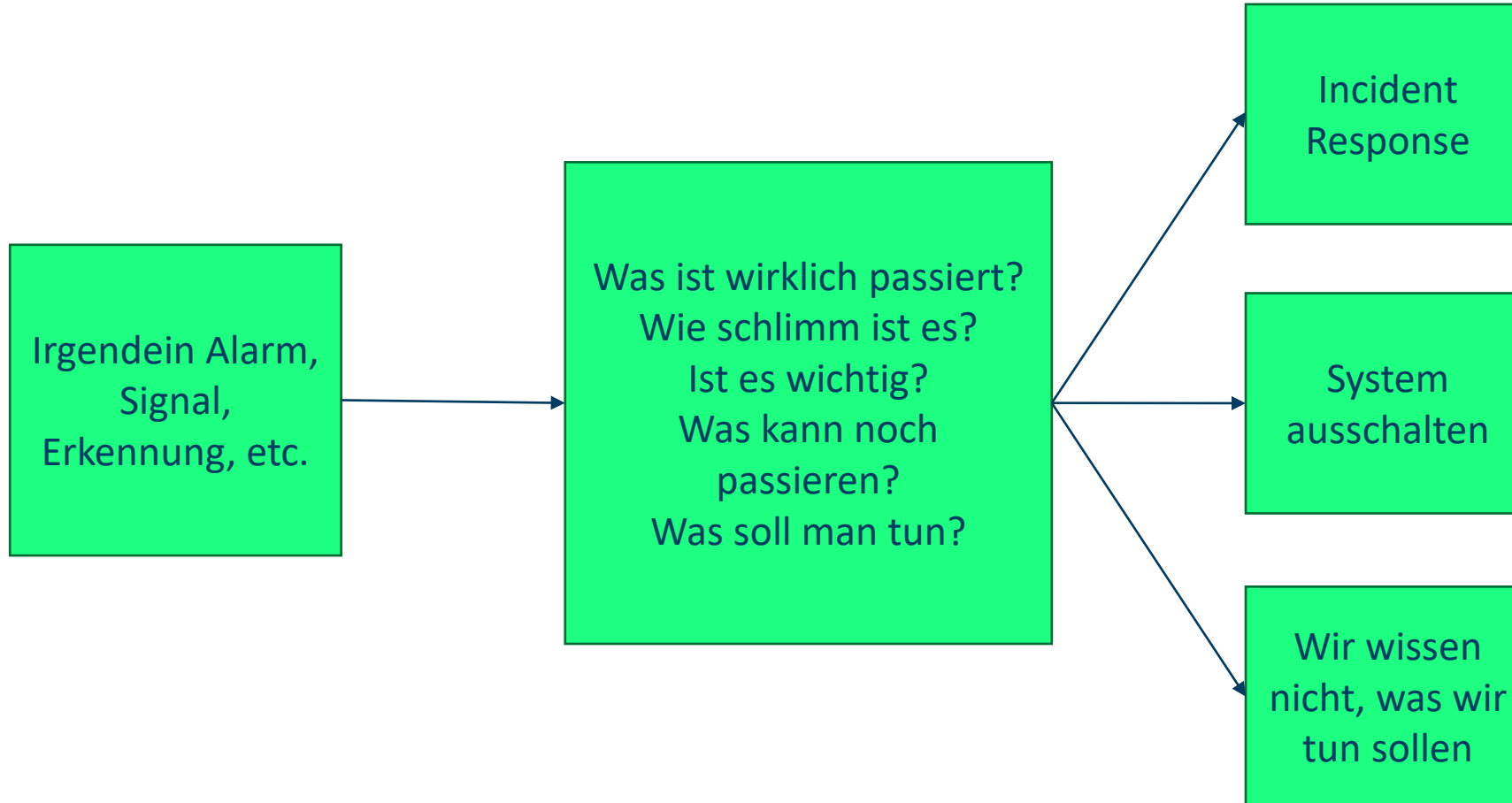
Angriffserkennung

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?

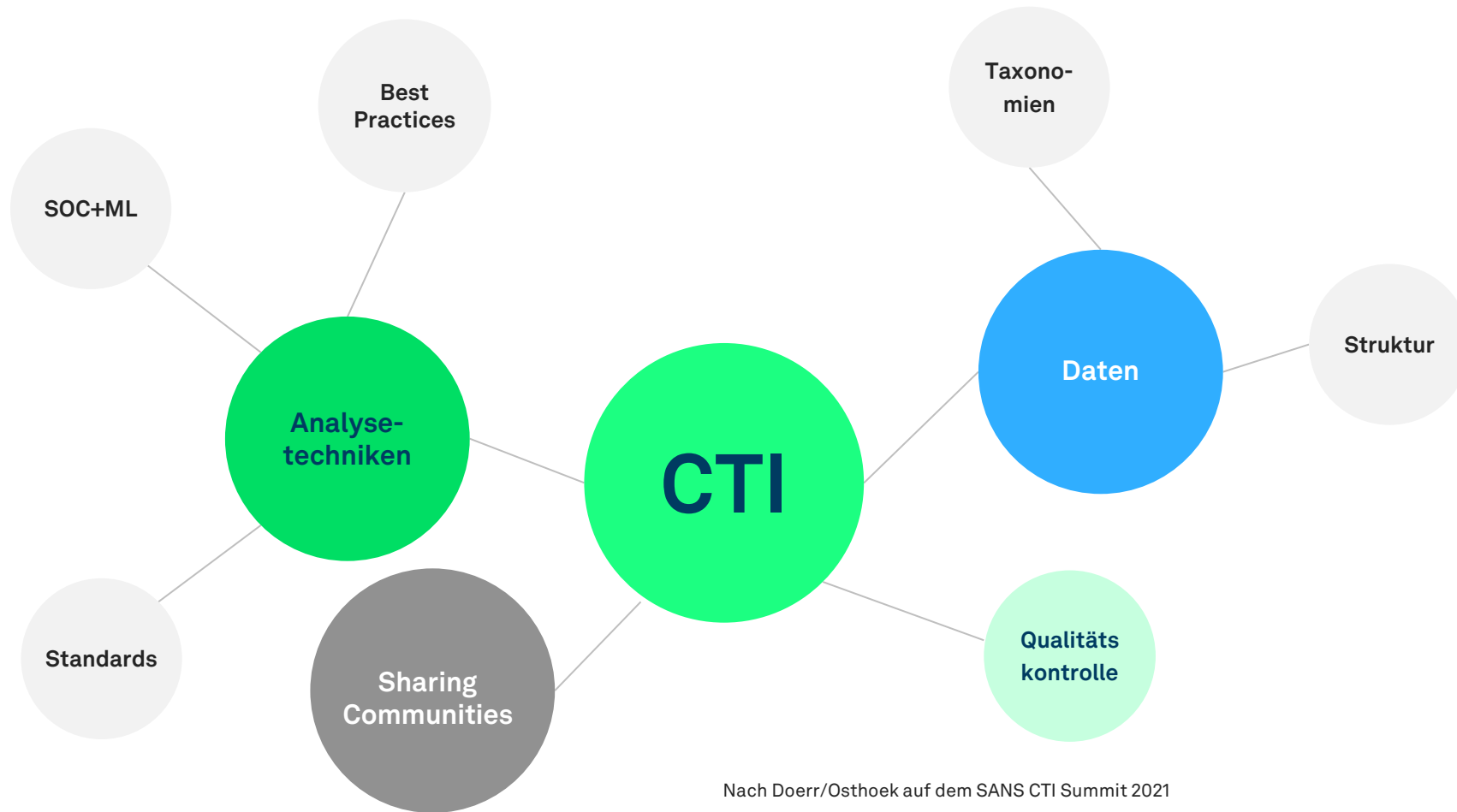
Telemetriedaten, Alarme, Lösungen, Platzierungen

- Logdaten
 - SIEM
 - Datalakes
 - Cloud
 - ...
-
- Active Directory
 - Kritische Applikationen
 - DNS
 - DHCP
 -
-
- EDR
 - NDR
 - xDR
 - MDR
 - IDS/IPS
 - Firewall/Proxy
-
- Incident Response
 - Threat Hunting
-
- Perimeter
 - Intern
 - Extern



Was und wer ist beteiligt?

Grundlagen für die Operationalisierung



MITRE Att&ck Framework

Wissen in der Anwendung - Beispiel

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	15 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection		Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Encoding (2)		Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Create or Modify System Process (4)	Domain Policy Modification (2)	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Data Obfuscation (3)	Exfiltration Over C2 Channel	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools		Domain Policy Modification (2)	Exploitation for Defense Evasion	Man-in-the-Middle (2)	Domain Trust Discovery	Data from Information Repositories (2)	Data from Network Shared Drive	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create Account (3)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Modify Authentication Process (4)	File and Directory Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Create or Modify System Process (4)	Exploitation for Privilege Escalation	Hide Artifacts (7)	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer		Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	Event Triggered Execution (15)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	OS Credential Dumping (8)	Network Sniffing	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels	Scheduled Transfer	Resource Hijacking
				External Remote Services	Process Injection (11)	Indicator Removal on Host (6)	Steal Application Access Token	Permission Groups Discovery (3)		Data Staged (2)	Non-Application Layer Protocol	Transfer Data to Cloud Account	Service Stop
				Hijack Execution Flow (11)	Scheduled Task/Job (6)	Indirect Command Execution	Steal or Forge Kerberos Tickets (4)	Process Discovery		Email Collection (3)	Non-Standard Port		System Shutdown/Reboot
				Implant Container Image	Valid Accounts (4)	Masquerading (6)		Query Registry		Input Capture (4)	Protocol Tunneling		
				Office Application Startup (6)		Modify Authentication Process (4)	Steal Web Session Cookie	Remote System Discovery		Man in the Browser	Remote Access Software		
				Pre-OS Boot (5)		Modify Cloud Compute Infrastructure (4)	Two-Factor Authentication Interception	System Information Discovery	Software Discovery (1)	Man-in-the-Middle (2)	Traffic Signaling (1)		
				Scheduled Task/Job (6)		Modify Registry	Unsecured Credentials (6)	System Network Configuration Discovery		Screen Capture	Web Service (3)		
				Server Software Component (3)		Modify System Image (2)		System Network Connections Discovery		Video Capture			
				Traffic Signaling (1)		Network Boundary Bridging (1)		System Owner/User Discovery					
				Valid Accounts (4)		Obfuscated Files or Information (5)		System Service Discovery					
						Pre-OS Boot (5)		System Time Discovery					

https://attack.mitre.org/

<https://attack.mitre.org/>



MISP

Beispiel für die Übermittlung von technischen Indikatoren



OSINT - Threat Spotlight: Ratsnif - New Network Vermin...

Event ID	1	/!\ If no tags show up, enable a Taxonomy or create some custom tags
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88	+
Creator org	ORNAME	Select Tag collections (taxonomies) or self-
Owner org	ORNAME	created tags
Email	admin@	
Tags		Add a tag
Date	2019-07	
Threat Level	Undefined	
Analysis	Initial	

Tag Collections Custom Tags All Tags

Select the input box to see the tags

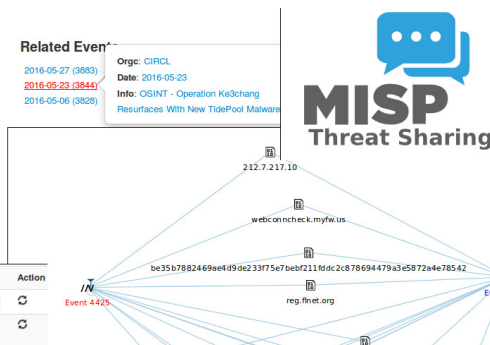
malware

Submit

OSINT - CVE-2015-2545: overview of current threats

Event ID	3865
Uuid	57460863-76dc-4272-8116-4ea302de0b81
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	ttp:white x circl:osint-feed x Type:OSINT x estimative-language:likelihood-probability~"very-likely" x
Date	2016-05-25
Threat Level	Medium
Analysis	Completed
Distribution	All communities
Info	OSINT - CVE-2015-2545: overview of current threats
Published	Yes
Sightings	0 (0)

Expanded	Events	Tag	Action
Likelihood or probability: Almost no chance - remote - 01-05%	0	estimative-language:likelihood-probability~"almost-no-chance"	
Likelihood or probability: Very unlikely - highly improbable - 05-20%	0	estimative-language:likelihood-probability~"very-unlikely"	



<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?

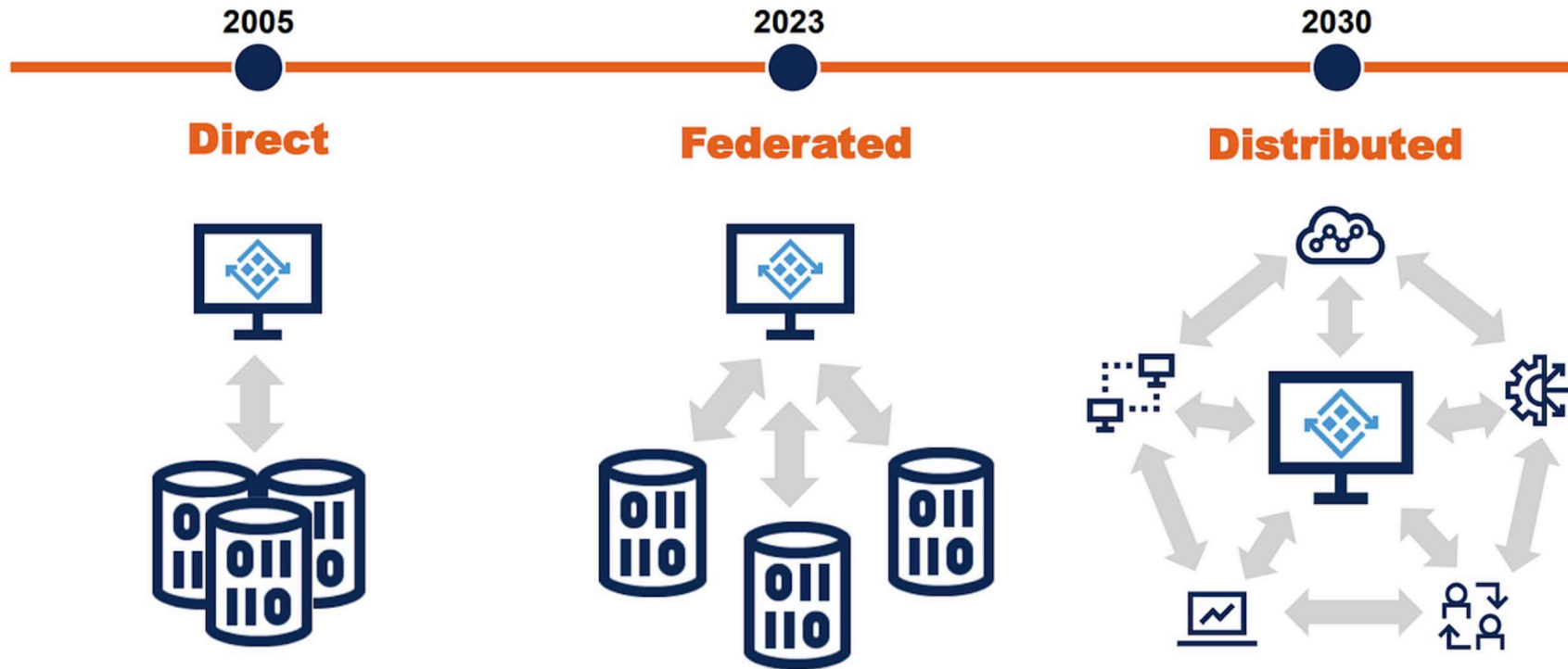
...und die Anwendung von Threat Intelligence



Entwicklung der SOC Werkzeuge

Daten

The Future of SIEM Data Storage



20 © 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner

(source: Gartner Security Summit 2023 presentation)

Zentral definiert und verteilt gespeichert

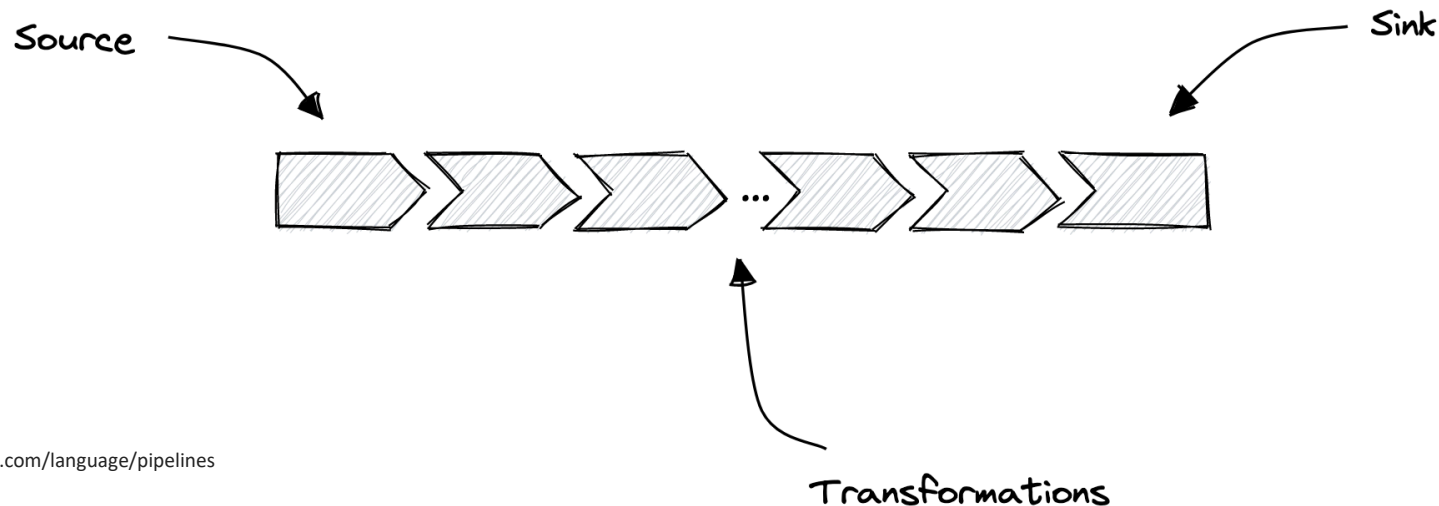
Federated Security Log Management



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

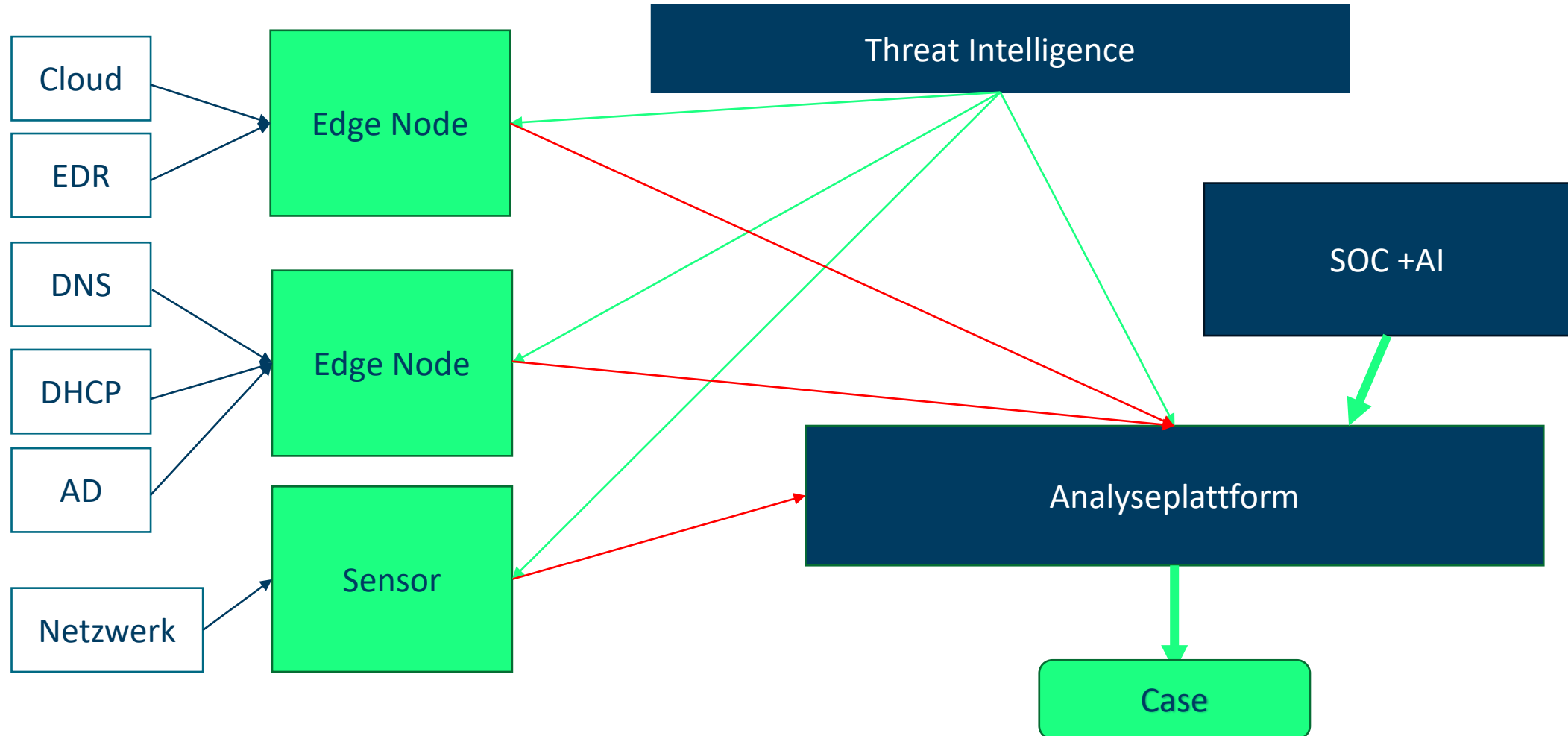
- IBM, Splunk, AWS, Cloudflare, PAN, Salesforce, TrendMicro, Rapid7, ZScaler etc.
- Datenmodell für Logs
- Taxonomy
 - Data Types, Attributes an arrays, Attribute Dictionary, Event classes, Categories, Profiles and Extensions
- Enrichment; Kategorisierung - Starke Verbindung zu MITRE Att&ck
- <https://github.com/ocsf/>

OCSF Schema					
Categories					
Initial working list of categories (work in progress).					
System Activity [1]	Findings [2]	Identity & Access Management [3]	Network Activity [4]	Discovery [5]	Application Activity [6]
File System Activity [1001] Kernel Extension Activity [1002] Kernel Activity [1003] Memory Activity [1004] Module Activity [1005] Scheduled Job Activity [1006] Process Activity [1007]	Security Finding [2001]	Account Change [3001] Authentication [3002] Authorize Session [3003] Entity Management [3004] User Access Management [3005] Group Management [3006]	Network Activity [4001] HTTP Activity [4002] DNS Activity [4003] DHCP Activity [4004] RDP Activity [4005] SMB Activity [4006] SSH Activity [4007] FTP Activity [4008] Email Activity [4009] Network File Activity [4010] Email File Activity [4011] Email URL Activity [4012]	Device Inventory Info [5001] Device Config State [5002]	Web Resources Activity [6001] Application Lifecycle [6002] API Activity [6003] Web Resource Access Activity [6004]



Operationalisierung

Events – TI – Alarme – Analyse - Cases



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