DCSO ENGINEERING SECURITY

Wie erkenne ich Bedrohungen?

Ein Ausflug in die Standardisierung und Entwicklung von Regeln, Signaturen und Suchmustern.

ISACA WebCast, 2020-02-04

Thomas Hemker, CISSP, CISM, CISA
Business Director Threat Detection & Hunting (TDH)

Thomas Hemker, CISSP, CISM, CISA

Photo: Heribert Schindler für Guter Hafen Cyber-Sicherheit

thomas.hemker@dcso.de

https://www.researchgate.net/profile/Thomas_Hemker3

https://www.linkedin.com/in/themker

https://www.xing.com/profile/Thomas_Hemker/cv

https://link.springer.com/chapter/10.1007%2F978-3-030-27957-8_24

25 Jahre Cyber-Security

Business Director TDH Service

ENISA ETL Stakeholder Group
ISACA, (ISC)2, TeleTrust, (ISF AC)

Sprecher, Autor, Security CTO, Advisor

NAI, PGP, SYMC, GH

Hamburg

Dieser Vortrag

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

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

ISACA NOW BLOG

Threat Hunting and Cyberrisk Assessment Using Cyber Kill Chain

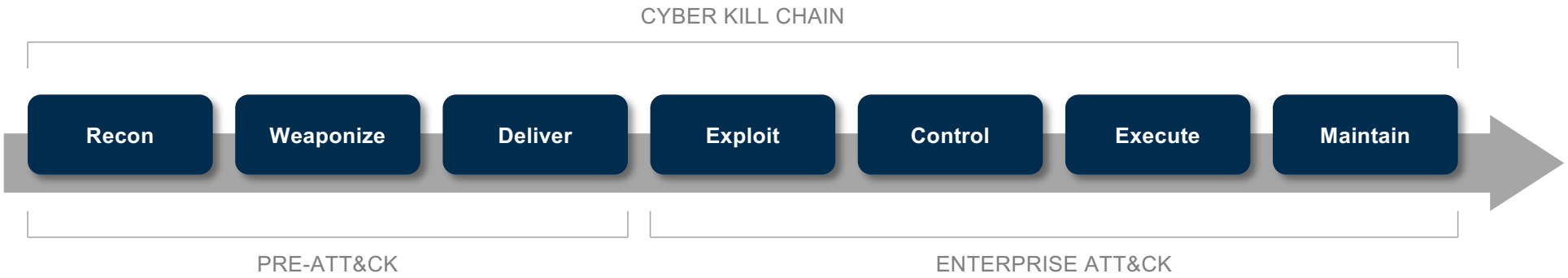
Author: Muhammad Mushfiqur Rahman, CISA, COBIT 5 Foundation, CCISO CCNA, CEH, CHFI, CISSP, CLPTP, CND, CSA, CTIA, ECI, ECSA, ISO 27001 LA, ITIL v3, LPT (Master), MCITP, MCP, MCSA, MCSE, MCT, MCTS, OCP, OSCP, PCT, PRINCE2, SCSA

Date Published: 7 January 2021

Step-by-step review of each phase in the cyberattack chain facilitates threat hunters, cybersecurity professionals and risk practitioners to identify gaps in the implemented security architecture of an organization.

Virtually ev
its employe

Cyber Security: Detection



PREVENTION

Blocken
Perimeter
Anti-Malware
Protection

DETECTION & RESPONSE

Da, wo es keine ”Protection” gibt
Angemessene Aktivitäten für die Eindämmung und Wiederherstellung
Verbessert die zukünftige Abwehr

Bedrohungslageninformation

Cyber Threat Intelligence – Welche Informationen zu der Cyber Kill Chain habe ich?

Cyber Threat Intelligence

Definition(en)

Threat

- Schaden für ein Information Asset
- Aktor, Agent, Quelle

Threat Event

- Aktion durch einen Threat ausgelöst

Intelligence

- Produkt aus Sammlung,
- Prozess, Integration, Analyse,
- Evaluation und Interpretation
- von Informationen

A proposed definition of threat intelligence

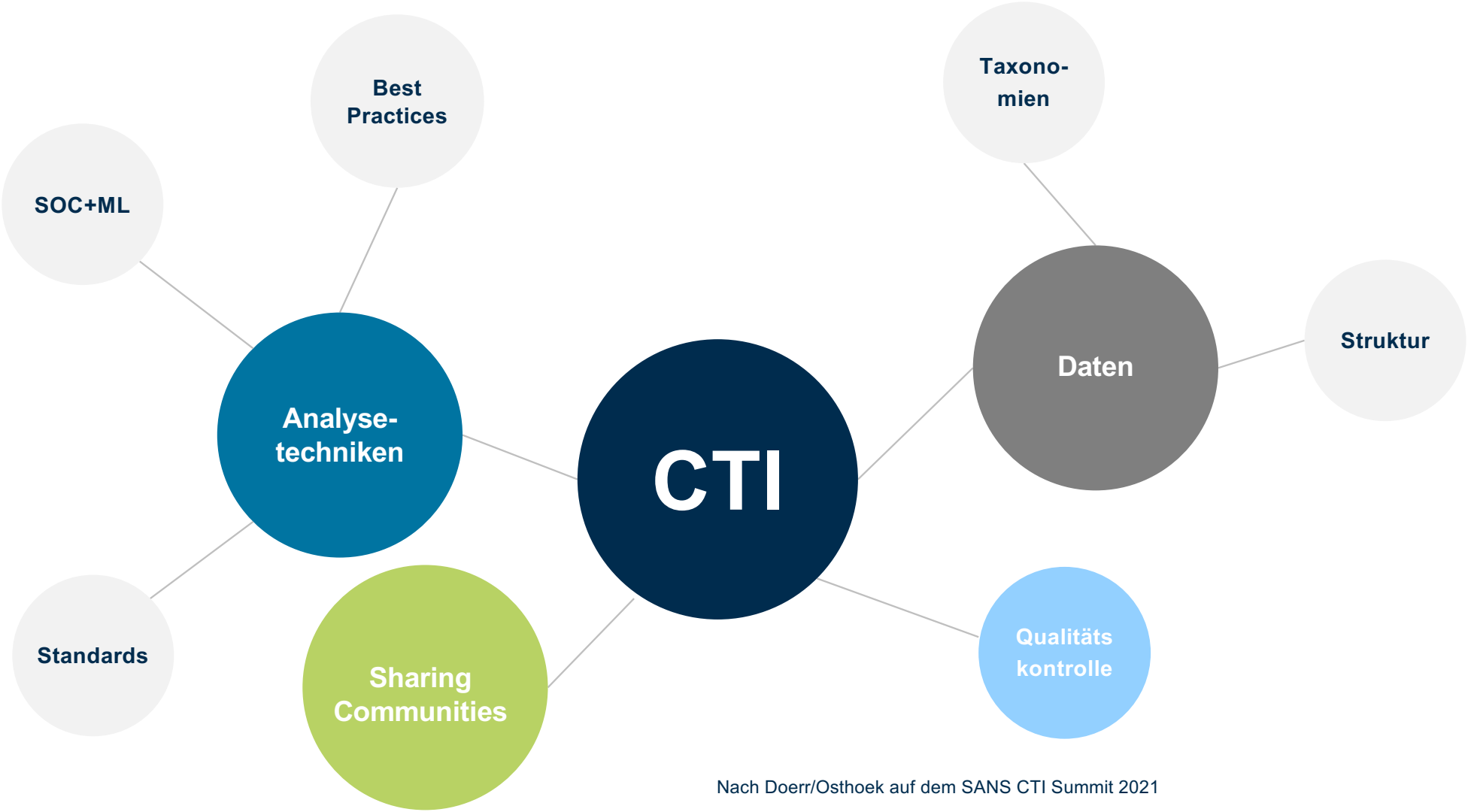
Threat intelligence is the product of analysing available information about (adversarial) threats' capabilities, intentions or activities to better inform decision or action.

www.securityforum.org (ISF)

„The purpose of threat intelligence is to understand the enemy, help anticipate future actions and plan a response“

Christian Doerr, TU Delft CTI Lab (jetzt HPI)
https://www.cyber-threat-intelligence.com/

TLP:White



Nach Doerr/Osthoek auf dem SANS CTI Summit 2021

TLP:White

Ebenen

Strategisch

Ziel: Geschäftsleitung bei Entscheidungen zu unterstützen

C-Level Exec, Group Security, Business Stakeholders, Risiko Manager

Wirtschaft & Politik

(Industrie) Spionage Sabotage

Reports

Presse

Dossiers

Operationell

Ziel: Angreifer und ihre Vorgehensweise verstehen

Fähigkeiten, Motivation, Ziel TTPs

Incident Responder, Threat Hunter, Netzwerk Architekten, System Administratoren, Schwachstellenmanagement, Red Teams, IT Manager

TTPs

Diamond Model

Fähigkeiten

Taktisch

Ziel: Wissen anwenden um Angriffe aufzuspüren

Informationen direkt in Detektions, Korrelations und Abwehrsysteme einspeisen

SOC Team, SIEM, Sicherheitstechnologie

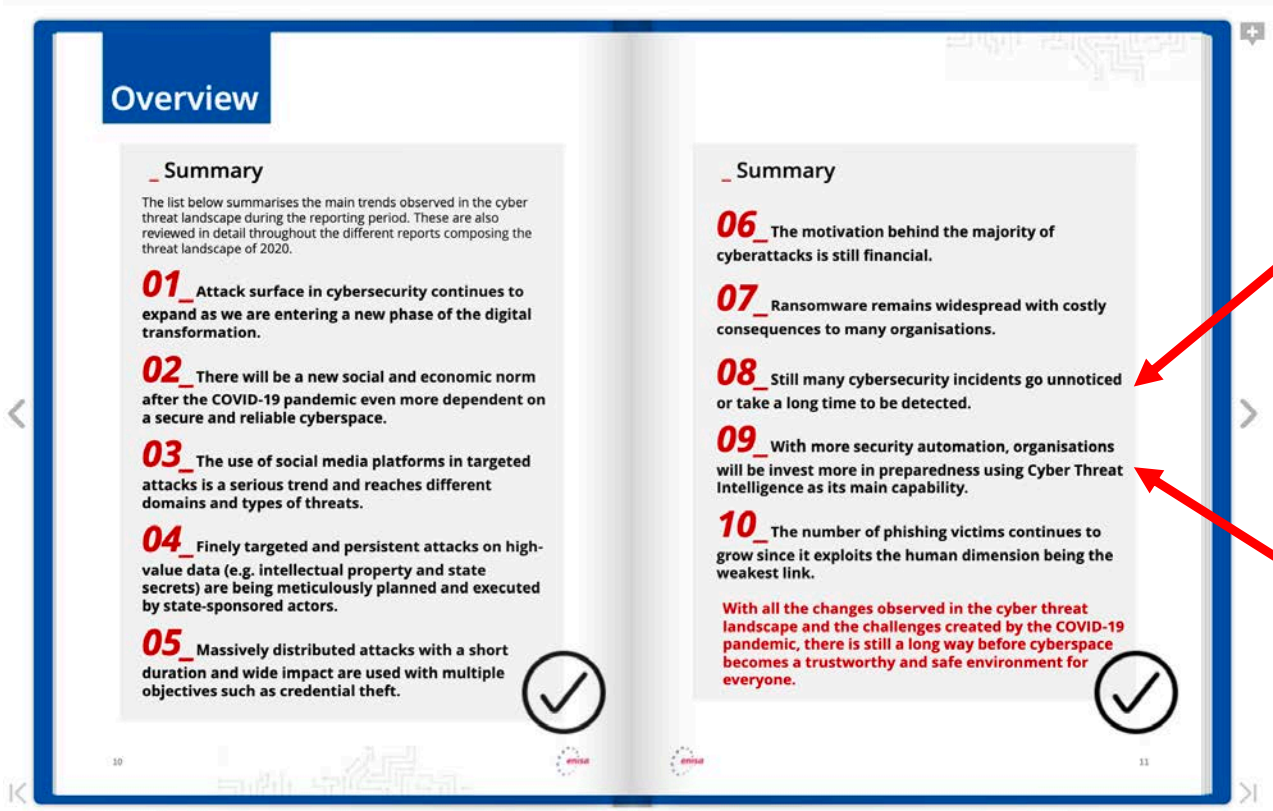
File Hashes

URLs, IPs

Domains, pDNS

Signatures

Bedrohungslage - Threat Landscape



Overview

_ Summary

The list below summarises the main trends observed in the cyber threat landscape during the reporting period. These are also reviewed in detail throughout the different reports composing the threat landscape of 2020.

01_ Attack surface in cybersecurity continues to expand as we are entering a new phase of the digital transformation.

02_ There will be a new social and economic norm after the COVID-19 pandemic even more dependent on a secure and reliable cyberspace.

03_ The use of social media platforms in targeted attacks is a serious trend and reaches different domains and types of threats.

04_ Finely targeted and persistent attacks on high-value data (e.g. intellectual property and state secrets) are being meticulously planned and executed by state-sponsored actors.

05_ Massively distributed attacks with a short duration and wide impact are used with multiple objectives such as credential theft.

_ Summary

06_ The motivation behind the majority of cyberattacks is still financial.

07_ Ransomware remains widespread with costly consequences to many organisations.

08_ Still many cybersecurity incidents go unnoticed or take a long time to be detected.

09_ With more security automation, organisations will be invest more in preparedness using Cyber Threat Intelligence as its main capability.

10_ The number of phishing victims continues to grow since it exploits the human dimension being the weakest link.

With all the changes observed in the cyber threat landscape and the challenges created by the COVID-19 pandemic, there is still a long way before cyberspace becomes a trustworthy and safe environment for everyone.

10

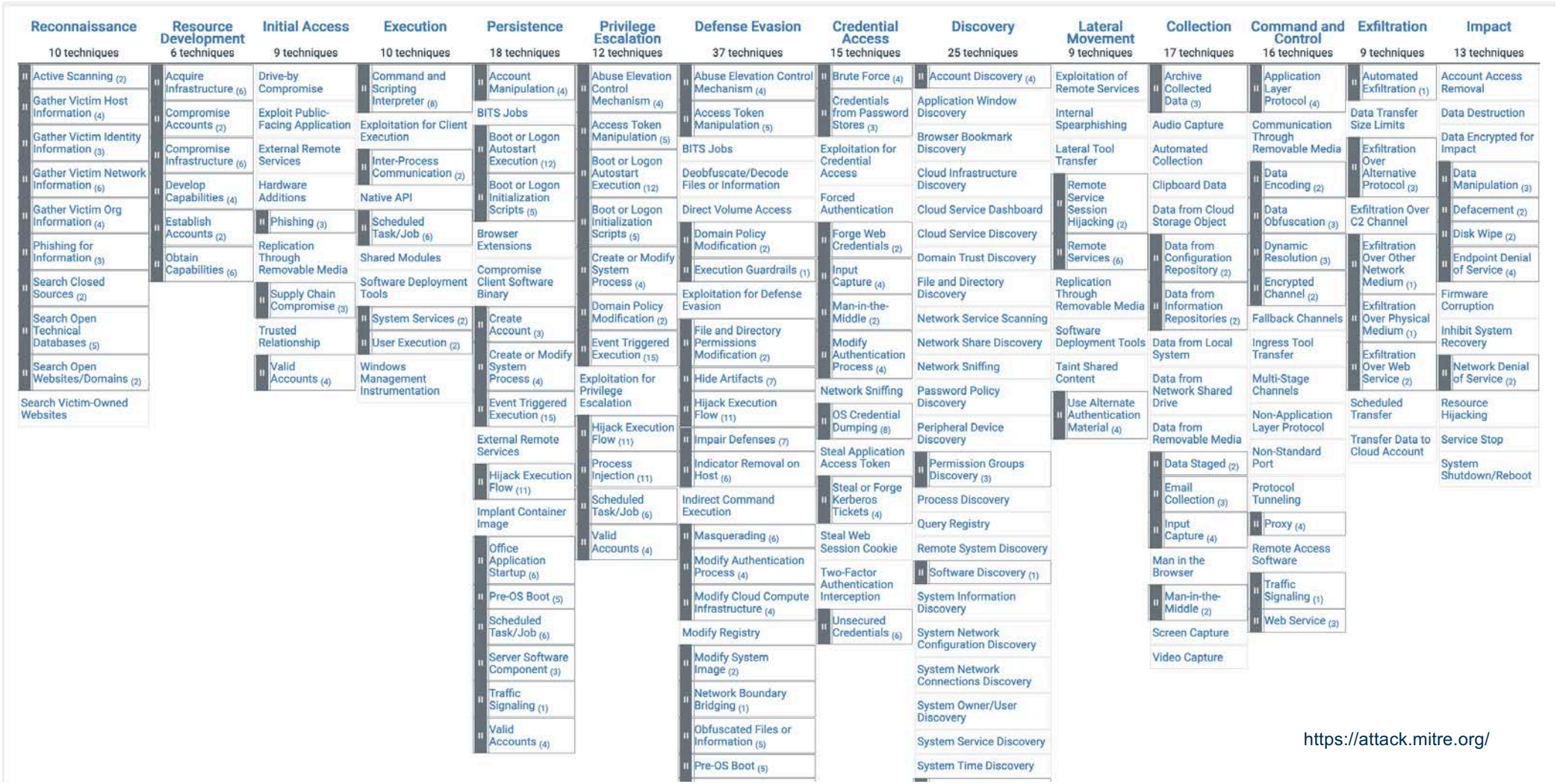
11

Notwendigkeit für schnellere Erkennung

Operationalisierung von Threat Intelligence

https://www.enisa.europa.eu/publications/year-in-review

MITRE Att&ck Framework



https://attack.mitre.org/

TLP:White

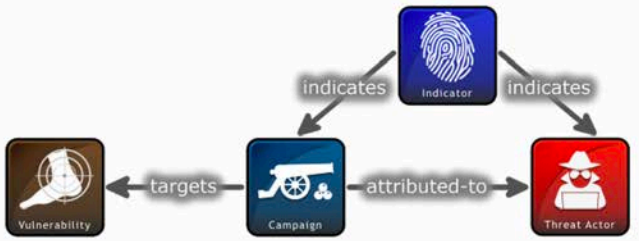
STIX / TAXII

- OASIS Consortium
- STIX
  - Autauschformat
  - JSON
  - Objekte
  - Beziehungen
  - Sightings
- TAXII
  - Austauschprotokoll
  - App-Layer
  - Kommunikation
  - Collections
  - Channels
  - Server

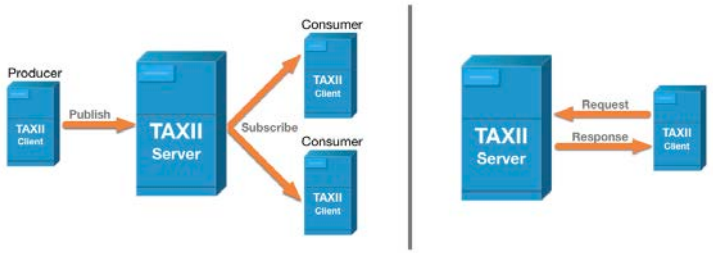
STIX 2 objects are represented in JSON. The following is a JSON-based example of a STIX 2.1 Campaign object:

```
{
    "type": "campaign",
    "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "spec_version": "2.1",
    "created": "2016-04-06T20:03:00.000Z",
    "modified": "2016-04-06T20:03:23.000Z",
    "name": "Green Group Attacks Against Finance",
    "description": "Campaign by Green Group against targets in the financial services sector."
}
```

Complete information for STIX 2 is available on the OASIS Cyber Threat Intelligence (CTI) Technical Committee (TC) website. Specification documents, schemas and tools are also available.



STIX 2 Relationship Example



https://oasis-open.github.io/cti-documentation/stix/intro

TLP:White

MISP

- OpenSource Platform
- CIRCL. LU

- IoCs
- Actor Information
- Fraud Information

- Verteilung
- Speicherung
- Korrelation

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

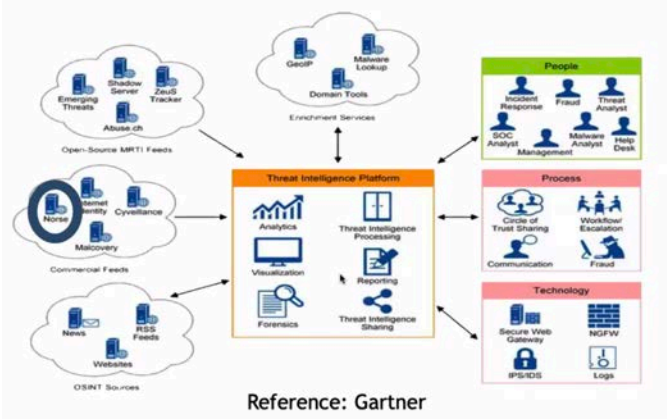
TLP:White

Threat Intelligence Platforms

- Excel?
- Sammlung verschiedener Tools
- Intelligence Lifecycle
- OpenSource, Community und kommerzielle Tools

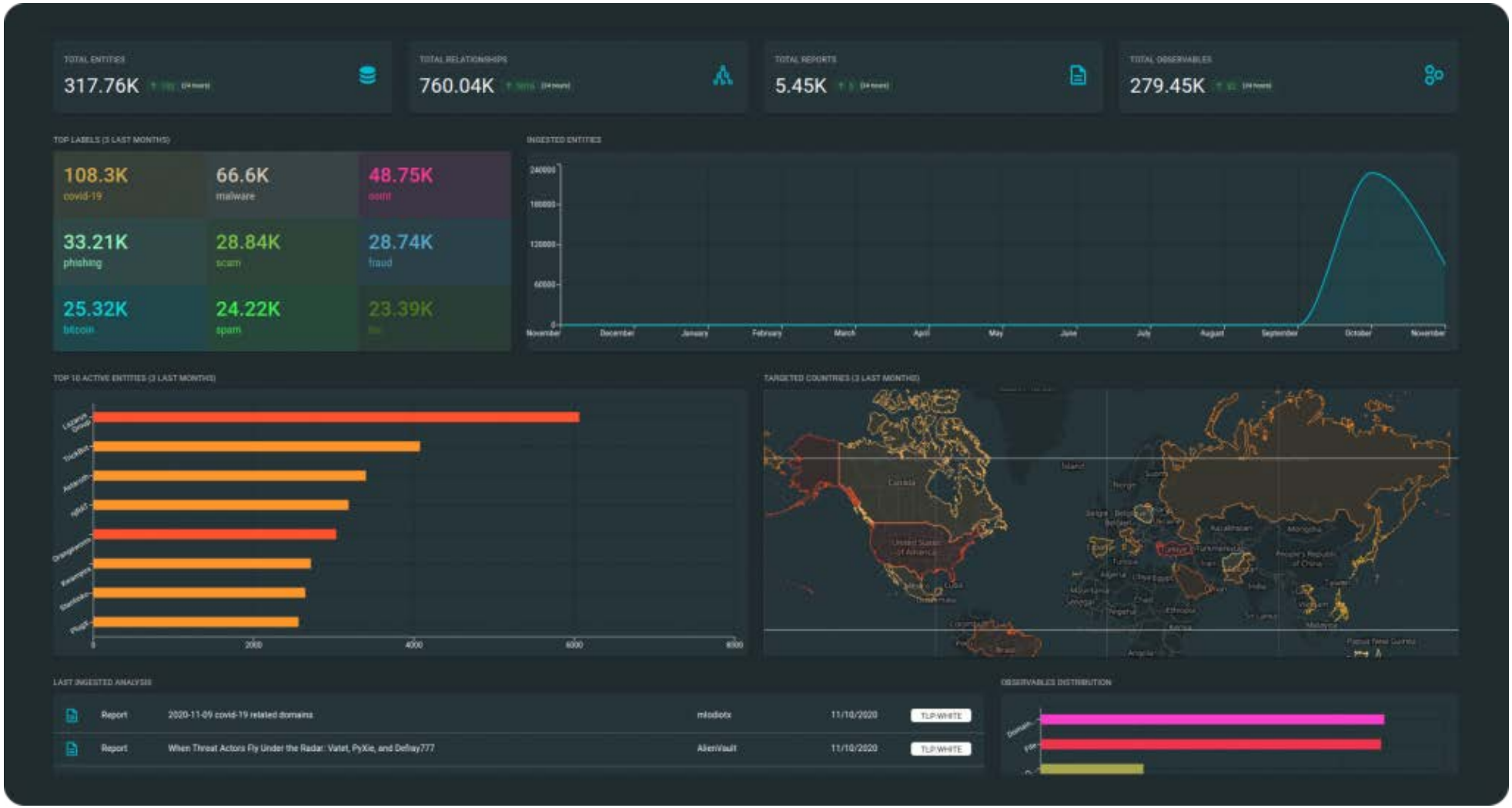
1,4	Direction	KPIs			Process and manage stakeholders' Requests for Information (RFI). Stakeholders with or without access to the TIP should be able to send an RFI to the TIP about a specific
2,1	Collection	Data ingestion			Capability to ingest threat data from different sources. What is challenging here is the wide variety of different sources: open source feeds, Information Sharing and Anal
2,2	Collection	Data ingestion			Capability to ingest threat data in as many different data models and standards: STIX 1.x, STIX 2.x , OpenIOC , CybOX , IODEF , custom, etc.
2,3	Collection	Data ingestion			Capability to ingest threat data via a variety of different transport mechanisms: TAXII , HTTPS, REST API, RSS, email, SFTP, shared folders (SMB), etc. TIP should also suppo
2,4	Collection	Data ingestion			Capability to import threat data in a variety of data formats (XML, JSON, YAML, CSV, TSV, PDF, DOCX, TXT). This also includes emails, PDFs, via free text, via browser plugi
2,5	Collection	Data ingestion			Capability to collect tactical, operational and strategic intelligence.
2,6	Collection	Data ingestion			TIP should be also able to collect structured, semi-structured and unstructured intelligence.
2,7	Collection	Data ingestion			Capability to collect threat data from local and internal sources (e.g. internal organisation sandbox).
2,8	Collection	Data ingestion			Capability for customizable polling of feed sources (customizable periodicity).
2,9	Collection	Data storage			Capability to store the collected data securely.
2,10	Collection	Data storage			Capability to store the collected data at scale.
2,11	Collection	Data storage			Capability to store collected data and apply retain based on policies.
2,12	Collection	Data storage			Capability to index collected data for faster searching functionality.
2,13	Collection	Data storage			Capability to store collected data and enforce privacy laws, regulations and other restrictions.
3,1	Process and Exploitation	Normalisation and data model			TIP should have the capability to normalise all stored data in a common format/standard/data model.
3,2	Process and Exploitation	Normalisation and data model			Capability to manage many different standards / data models and provide compatibility and correlation functions among them.

https://github.com/sfakiana/SANS-CTI-Summit-2021/blob/main/TIP_Functional_Requirements_v1.0.xlsx

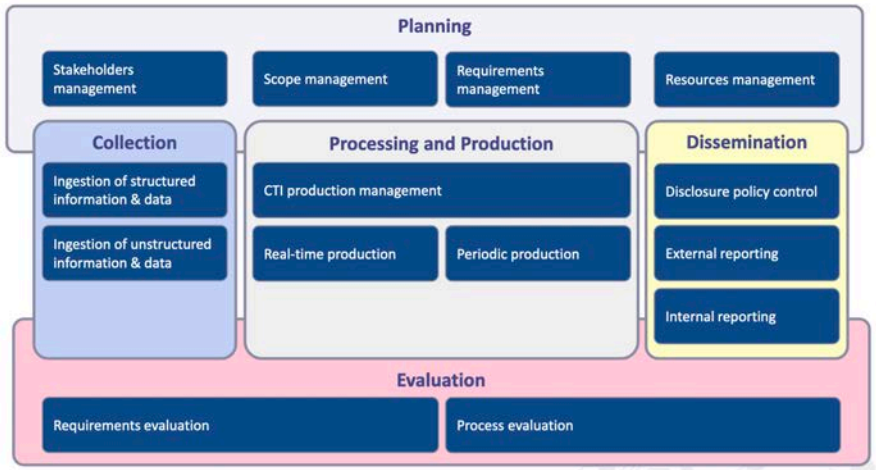


TLP:White

https://www.opencti.io/en/



ENISA CTI Capability Maturity Framework

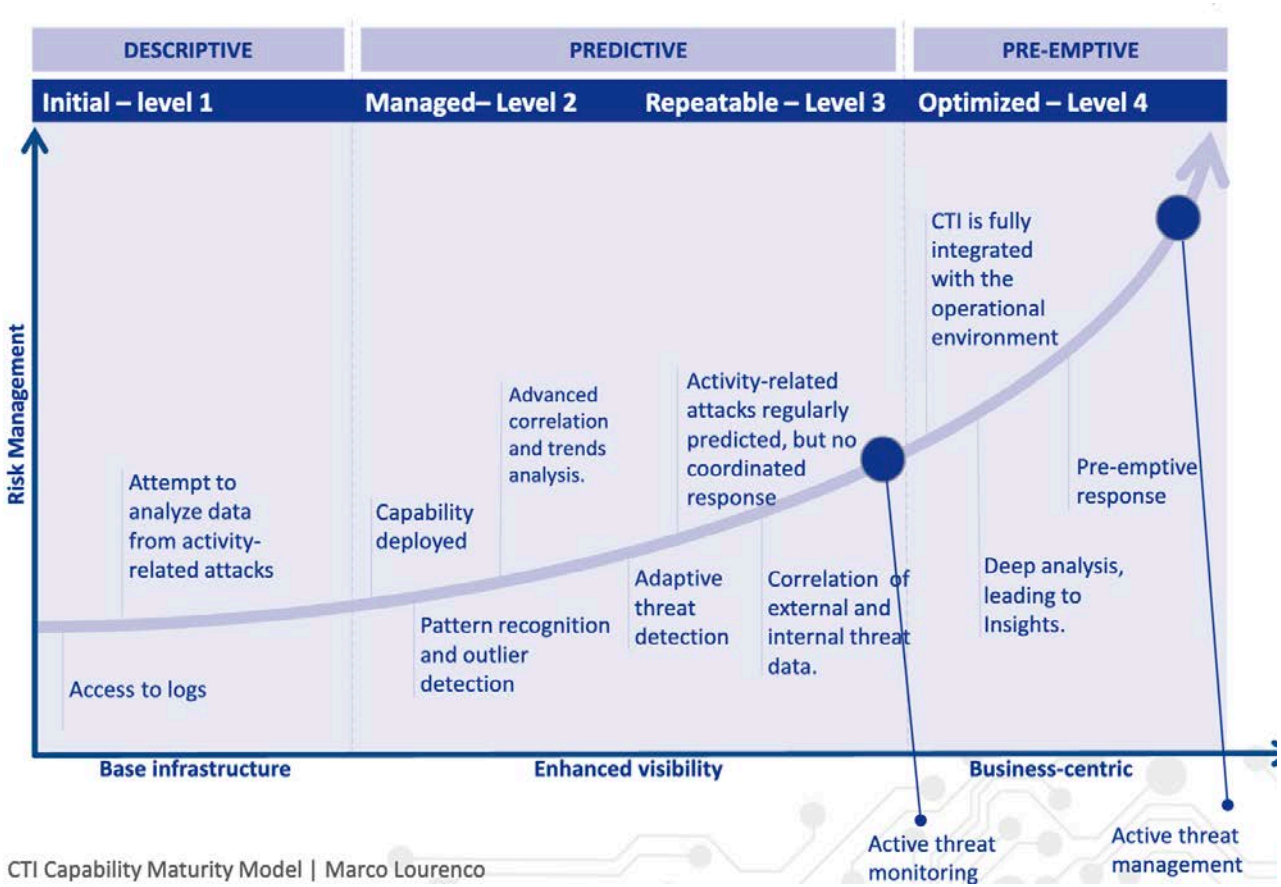


Maturity scorecard - collection

enisa

Ingestion of structured information & data | Ingestion of unstructured information & data

Type/level	Initial	Managed	Repeatable	Optimized
Strategic	None	Small number of sources consumed. A focus on 'overview' style articles or reading other people's analysis on the same topic	A focus on reputable, well-known sources of information in key areas.	Large range of sources, including economic, socio-political, foreign language journals, press articles, and products of other CTI types.
Operational	Attempt to analyze data from activity-related attacks	Attempts made to find an activity or event correlated to attack types	Activity-related attacks regularly predicted, but no coordinated response	Activities that result in attacks robustly understood, and appropriate monitoring in place. Response planned;
Tactical	No tactical information collected	Irregular decision making on source acquisition. Mostly open- or sources of unknown reputation	Regular decision making on source acquisition and re-alignment. Wider range of mostly reputable sources	Established procures to acquire, evaluate and re-alignment sources.
Technical	No collection	Ad-hoc collection, e.g. from occasional reports. Indicators are manually actioned, e.g. by logging onto hosts to check for registry paths or looking at firewall logs.	Collection from public feeds. Automatic searching for host-based indictors across the whole infra, probably utilising third-party software.	Collection from public feeds, and private feeds such as sharing relationships. Indicators of all types automatically searched for in network traffic and on hosts;



https://www.enisa.europa.eu/events/2018-cti-eu-event/cti-eu-2018-presentations/cti-eu-cti-capability-maturity-model.pdf

TLP:White

Bedrohungserkennung

Threat Detection & Hunting – Wie kann ich innerhalb der Kill-Chain den Angriff stoppen?

TLP:Amber

Was benötigt man (unter anderem) für Threat Detection?

Kurzüberblick

Sichtbarkeit

- Sensorik, Telemetrie
- Operations, Monitoring und Wartung
- Baselining

Threat Intelligence

- Security Content (kuratiert)
- Enrichment
- Indikatoren, Regeln

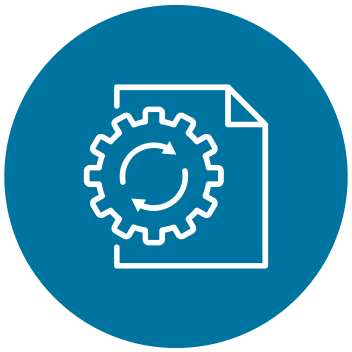
Analyse

- Analyse und Validierung von Alarmen
- Klassifizierung, Triage,
- Handlungsempfehlung

Fähigkeiten

THREAT DETECTION

”Ost-West” Sichtbarkeit
Tranzparenz (Netzwerk)
Suche verstehen
Security Content
Priorisierung
Asset Klassifizierung



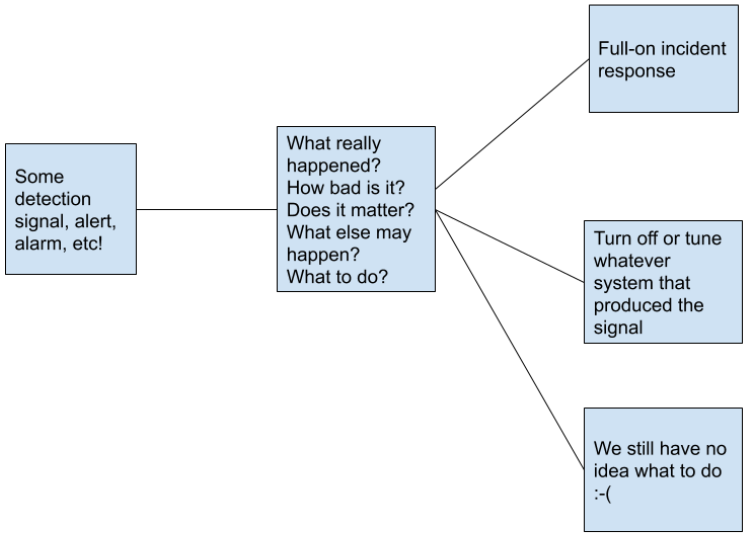
HUNTING

Metadaten
Telemetrie Daten
Kontext
Frameworks
Klassifizierung

RESPONSE

Cyber-Skills Gap
Managed Service
Aktionen
Experten
Best-Practices
Kommunikation

Warum ist Bedrohungserkennung gar nicht so leicht?



- „Komplexe“ Umgebungen
- Richtige Anzahl an richtigen Personen
- Daten aus unterschiedlichen Quellen und mit Kontext
- Triage ist notwendig
- Unsicherheit

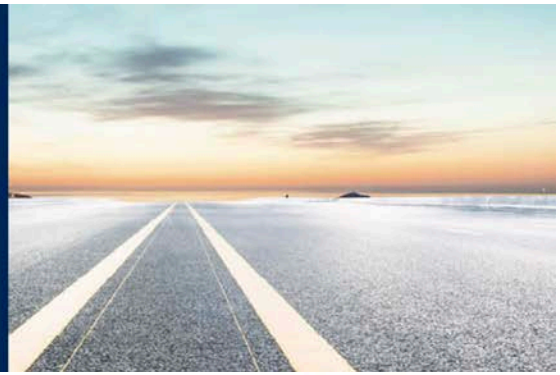
- Angreifer wollen nicht entdeckt werden
- Absicht erkennen / nicht nur Aktivität

https://medium.com/anton-on-security/on-threat-detection-uncertainty-7eac9b22adb6

NDR, EDR, MDR …… xDR

Gartner Top 9 Security and Risk Trends for 2020

Security | Live from #GartnerSEC



September 17, 2020 | Contributor: Christy Pettey

CISOs should understand these trends to practice strong planning and execution of security initiatives.

The shortage of technical security staff, the rapid migration to cloud computing,

Trend No. 1: Extended detection and response capabilities emerge to improve accuracy and productivity

Extended detection and response (XDR) solutions are emerging that automatically collect and correlate data from multiple security products to improve threat detection and provide an incident response capability. For example, an attack that caused alerts on email, endpoint and network can be combined into a single incident. The primary goals of an XDR solution are to increase detection accuracy and improve security operations efficiency and productivity.

"Centralization and normalization of data also helps improve detection by combining softer signals from more components to detect events that might otherwise be ignored," said Firstbrook.

https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020/

TLP:White

Beispiel: NDR oder Network Security Monitoring (NSM)

IDS - Beispiel: Suricata Regeln

A rule/signature consists of the following:

- The **action**, that determines what happens when the signature matches
- The **header**, defining the protocol, IP addresses, ports and direction of the rule.
- The **rule options**, defining the specifics of the rule.

An example of a rule is as follows:

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USA
+..)"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-
activity; sid:2008124; rev:2;)
```

In this example, red is the action, green is the header and blue are the options.

https://oisf.net/

```
outputs:
  # Extensible Event Format (nicknamed EVE) event log in JSON format
  - eve-log:
      enabled: yes
      filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
      filename: eve.json
      # Enable for multi-threaded eve.json output; output files are amended
      # with an identifier, e.g., eve.9.json
      #threaded: false
      #prefix: "@cee: " # prefix to prepend to each log entry
      # the following are valid when type: syslog above
      #identity: "suricata"
      #facility: local5
      #level: Info ## possible levels: Emergency, Alert, Critical,
                   ## Error, Warning, Notice, Info, Debug
      #redis:
      #  server: 127.0.0.1
      #  port: 6379
      #  async: true ## if redis replies are read asynchronously
      #  mode: list ## possible values: list|lpush (default), rpush, channel|publish
      #             ## lpush and rpush are using a Redis list. "list" is an alias for lpush
      #             ## publish is using a Redis channel. "channel" is an alias for publish
      #  key: suricata ## key or channel to use (default to suricata)
      # Redis pipelining set up. This will enable to only do a query every
      # 'batch-size' events. This should lower the latency induced by network
      # connection at the cost of some memory. There is no flushing implemented
      # so this setting as to be reserved to high traffic suricata.
      #  pipelining:
      #    enabled: yes ## set enable to yes to enable query pipelining
      #    batch-size: 10 ## number of entry to keep in buffer

      # Include top level metadata. Default yes.
      #metadata: no

      types:
        - alert:
            # payload: yes             # enable dumping payload in Base64
            # payload-buffer-size: 4kb # max size of payload buffer to output in eve-log
            # payload-printable: yes   # enable dumping payload in printable (lossy) format
            # packet: yes              # enable dumping of packet (without stream segments)
            # http-body: yes           # Requires metadata; enable dumping of http body in Base
            # http-body-printable: yes # Requires metadata; enable dumping of http body in prin

            # Enable the logging of tagged packets for rules using the
            # "tag" keyword.
            tagged-packets: yes

            # Configure the metadata to be logged along with an
            # alert. The following shows the default configuration
            # which is used if this field is not provided or simply
            # set to a truthful value. Setting of this section is only
            # required if you wish to enable/disable specific fields.
            #metadata:

              # Include the decoded application layer (ie. http, dns)
              app-layer: true

              # Log the the current state of the flow record.
              flow: true
```

Analyse

Security Operations Center oder Cyber Defense Center

- Klassifizierung, True/False Positive, Enrichment, Kontext, MITRE Att&ck
- Triage, Filterung, Korrelation, Eventmanagement
- Validierung, Qualitätskontrolle, Berichtswesen
- Servicekatalog (Inhouse, Outsourcing)

SIEM

- Information Management
- Event Management
- Echtzeitanalyse
- Korrelation
- Datenquellen
- **Regeln**
- **Signaturen**

SOAR

- Orchestration, Automation
- Sammlung von Tools
- Priorisierung
- Standardisierung
- Vorfallsbehandlung
- Prozesse
- Richtlinien

Case Management

- Workflow
- Tickets
- Prozess, Integration
- Service Mgmt.
- Beispiel: The Hive

SIGMA Regeln

Sigma

Generic Signature Format for SIEM Systems

What is Sigma

Sigma is a generic and open signature format that allows you to describe relevant log events in a straightforward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts can describe their once developed detection methods and make them shareable with others.

Sigma is for log files what Snort is for network traffic and YARA is for files.

This repository contains:

1. Sigma rule specification in the Wiki
2. Open repository for sigma signatures in the `./rules` subfolder
3. A converter named `sigmac` located in the `./tools/` sub folder that generates search queries for different SIEM systems from Sigma rules

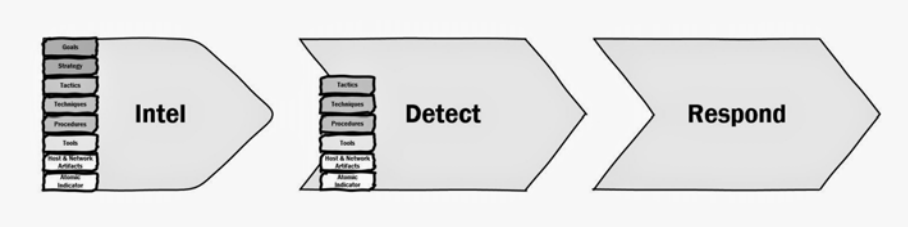
web_webshell_keyword.yml ● | win_alert_mimikatz_keywords.yml

```
1   title: Webshell Detection by Keyword
2   description: Detects webshells that use GET requests by k
3   author: Florian Roth
4   logsource:
5       type: webserver
6   detection:
7       keywords:
8           - '=whoami'
9           - '=net%20user'
10          - '=cmd%20/c%20'
11      condition: selection and keywords
12  falsepositives:
13      - Web sites like wikis with articles on os commands a
        URLs
14      - User searches in search boxes of the respective webs
15  level: high
16
```

https://github.com/Neo23x0/sigma

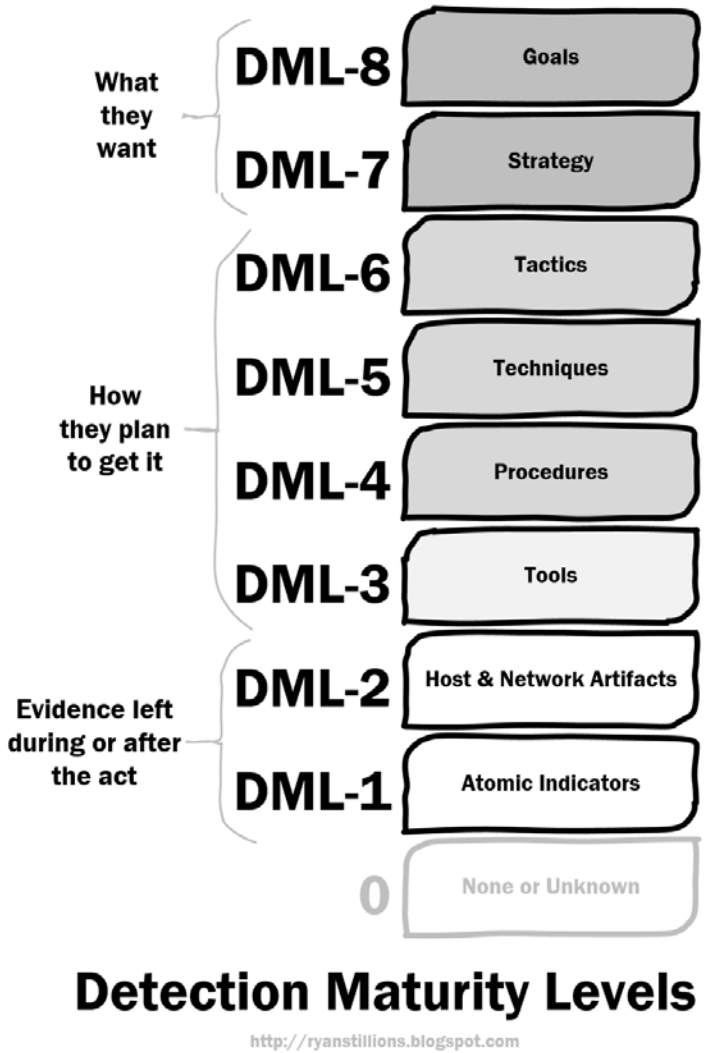
Reifegrade für Threat Detection

- DML Model
- Die Qualität der Threat Intelligence determiniert den Reifegrad der Detektion



- Beispiel: „Directory Listings“
  - Folgende Aktivitäten des Angreifers
  - Metadaten
  - Verschiedene Datenquellen/Detektionen

http://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html



Diskussion

- Bedrohungslageninformation
  - Austausch
  - Qualität
  - Operationalisieren
- Bedrohungserkennung
  - Einfach anfangen
  - Unterstützung
- Bleibt gesund!

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

E: info@dcso.de

P: +49-30-726219-0