OT Threat Intelligence richtig nutzen

Kai Thomsen
Strategic Outreach Lead Intelligence & Services Organization
kthomsen@dragos.com

DRAGOS

Die CART Methode

Cyber Threat Intelligence Evaluieren

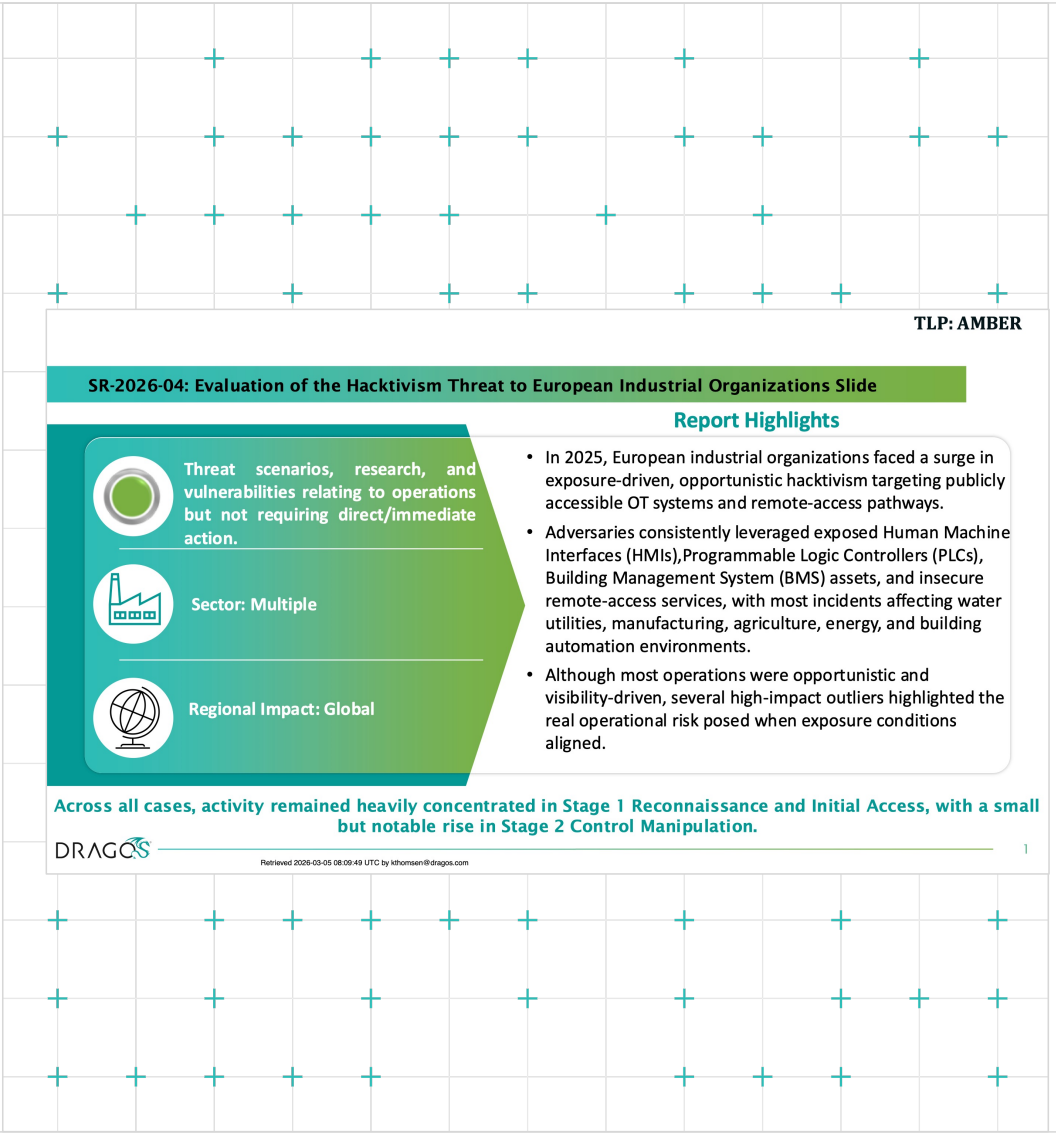
Complete
Ist der Bericht vollständig genug, um auf Basis der Informationen handeln zu können (“actionable intelligence”)?
Accurate
Ist der Bericht zutreffend oder enthält er augenscheinliche Fehler und Ungenauigkeiten?
Relevant
Ist der Bericht relevant für meine Organisation?
Timely
Erschien der Bericht ausreichend zeitnah um bei kritischen Ereignissen Handlungsempfehlungen liefern zu können?

- Berichte, die zuerst publiziert werden, sind meistens am ungenausten
- Gerade in Medien wird oft von nur einer (ungenauen) Quelle abgeschrieben, wenn schnell publiziert werden soll
- RUMINT ist weit verbreitet in deutschen Organisationen. Hype sollte immer hinterfragt und meistens ignoriert werden!

Übung 1

Einen TI-Bericht auswerten

- Welche Teile sind relevant?
- Welche Empfehlungen gibt der Bericht?
- Wie würdet Ihr den Bericht für Eure Organisation zusammenfassen?
- Welche Handlungen empfehlt Ihr für Eure Organisationen auf Basis des Berichtes?



TLP: AMBER

SR-2026-04: Evaluation of the Hacktivism Threat to European Industrial Organizations Slide

Threat scenarios, research, and vulnerabilities relating to operations but not requiring direct/immediate action.

Sector: Multiple

Regional Impact: Global

Report Highlights

- In 2025, European industrial organizations faced a surge in exposure-driven, opportunistic hacktivism targeting publicly accessible OT systems and remote-access pathways.
- Adversaries consistently leveraged exposed Human Machine Interfaces (HMIs),Programmable Logic Controllers (PLCs), Building Management System (BMS) assets, and insecure remote-access services, with most incidents affecting water utilities, manufacturing, agriculture, energy, and building automation environments.
- Although most operations were opportunistic and visibility-driven, several high-impact outliers highlighted the real operational risk posed when exposure conditions aligned.

Across all cases, activity remained heavily concentrated in Stage 1 Reconnaissance and Initial Access, with a small but notable rise in Stage 2 Control Manipulation.

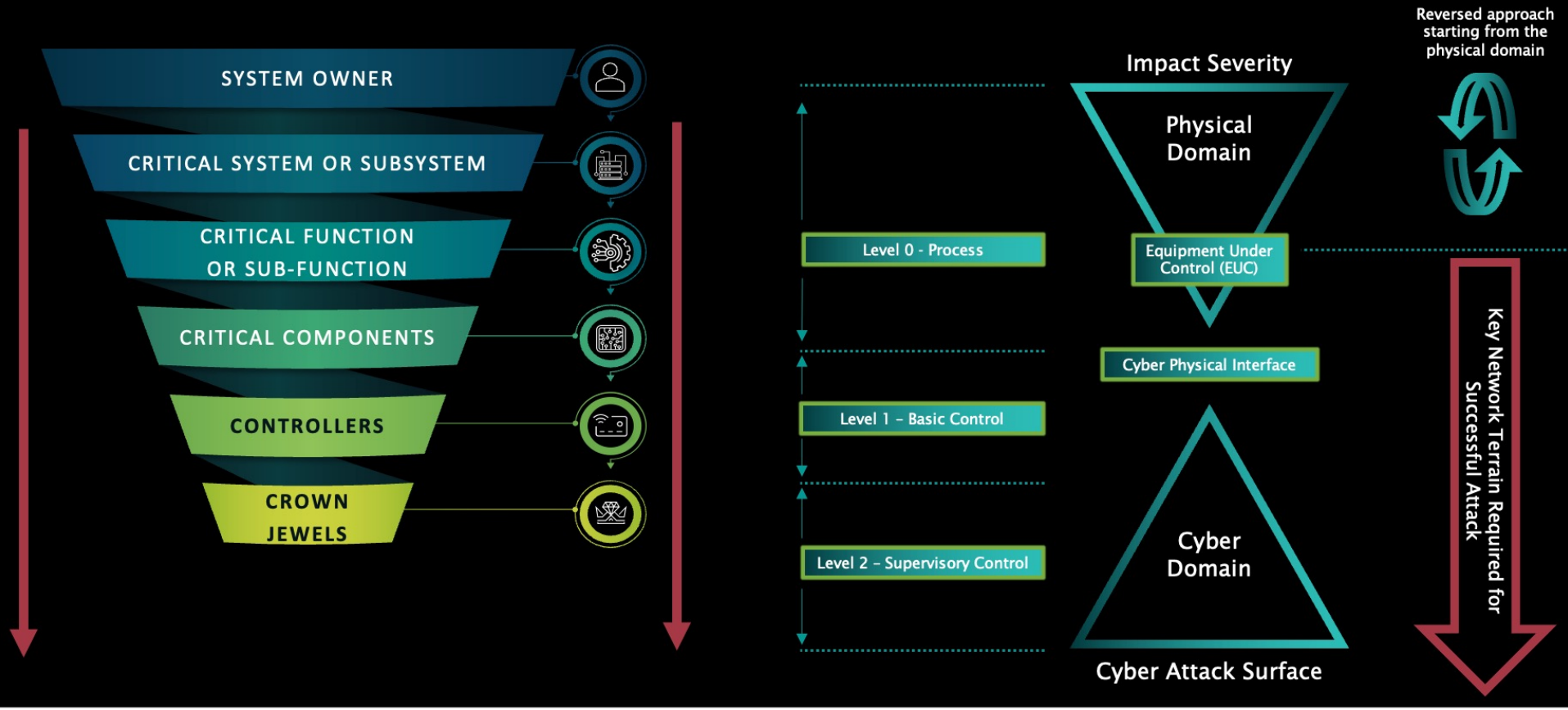
DRAGOS

Retrieved 2026-03-05 08:09:49 UTC by kthomsen@dragos.com

1

Kronjuwelenanalyse und Collection Management Frameworks

Dragos CJA



Typische Kronjuwelen

- Unterstützende Prozesse (Strom, Kühlung, Druckluft, Prozessdampf)
- Windows- und Linux Systeme in OT, die eine Interaktion mit Steuergeräten erlauben
  - Engineering Workstations (EWS) / Programmiergeräte (PGs)
  - HMIs
  - Data Historians

Collection Management Framework (CMF)

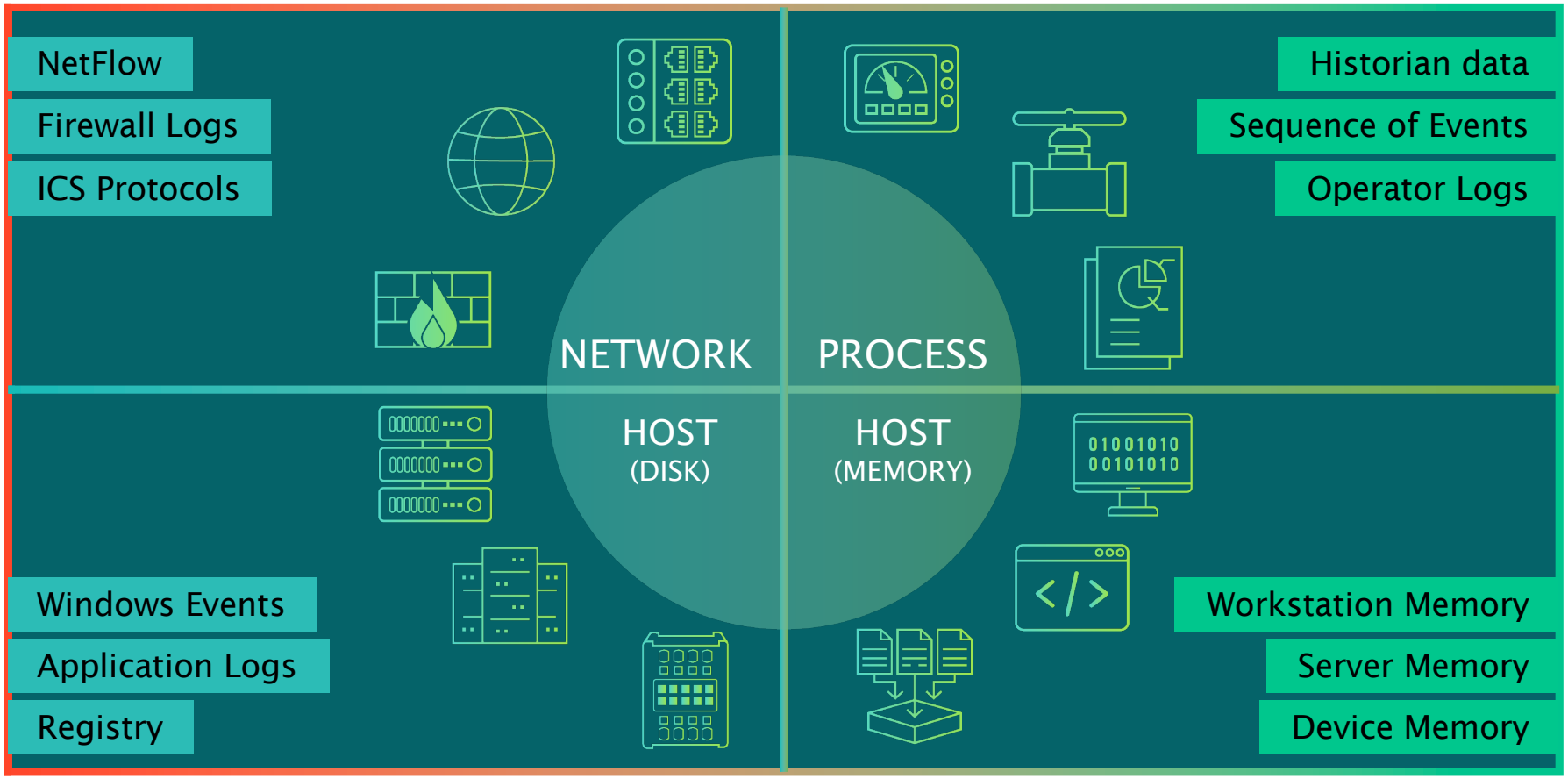
- In typischen OT-Umgebungen gibt es nur wenig relevante Daten für Security Analysen/DFIR
- Zu wissen, welche Systeme welche Daten erzeugen, wo diese liegen und für wie lang die Daten gespeichert werden, ist äußerst wichtig.
- Ein Collection Management Framework ist ein systematischer Ansatz, um diese Daten zu erheben.
- Prozesswissen ist dabei wichtiger als Security Know-How
- Prozessingenieure und Techniker können ein einfaches CMF in 20 Minuten erstellen

Übung 2: Ein CMF erstellen

Freiwillige vor!

- Wer kennt sich mit OT Prozessen aus? Ab ans FlipChart ☺

Collection Datasets for OT



https://hub.dragos.com/whitepaper/incident-response-for-operational-technology

Thank you