TeleTrusT
Pioneers in IT security.

TeleTrusT-interner Workshop

Berlin, 05./06.07.2018

Threat Intelligence

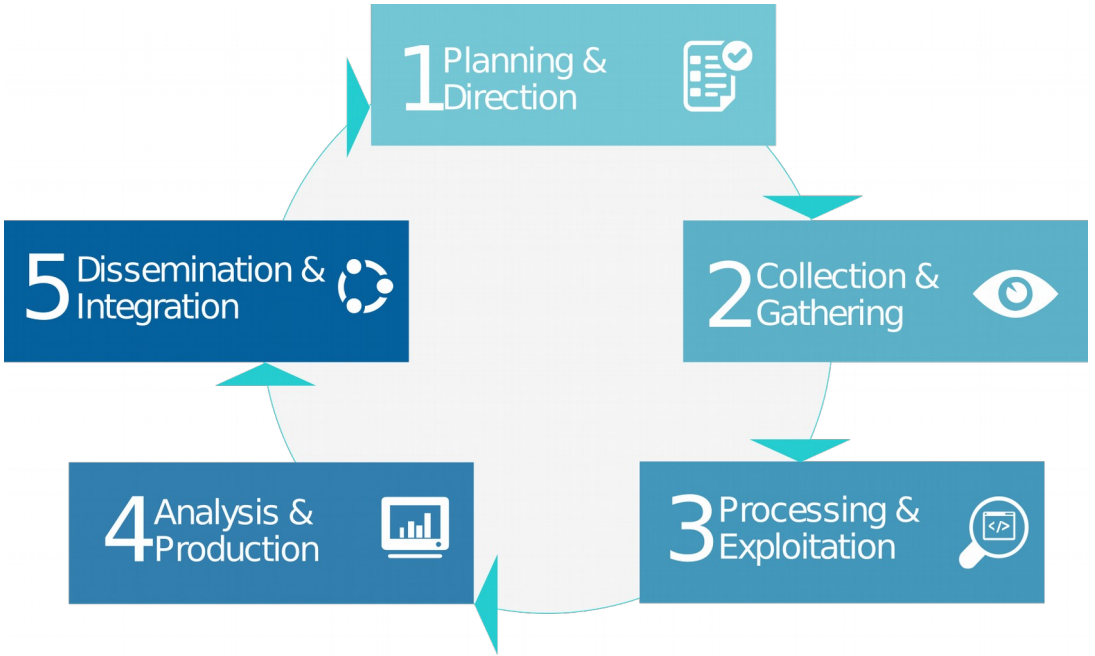
Kontext

- zu mir:
  - Name: Tobias Börtitz
  - Software Engineer bei cognitix GmbH

- zu cognitix GmbH:
  - Netzwerk Security Vendor
  - HQ: Leipzig
  - Beschäftigt mit Threat Intelligence seit ~9 Monaten

Generelles – Threat Intelligence

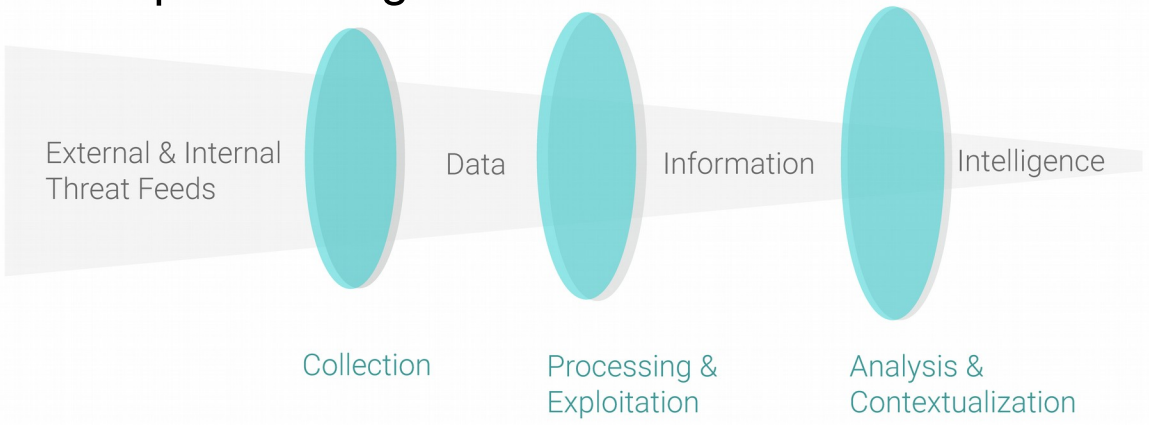
- Daten & Kontext über Cyber Angriffe
  - Planen
  - Sammeln
  - Aggregieren
  - Kontextualisieren
  - Verteilen & Integrieren



→ Cybersecurity Intelligence Cycle

Was?

- Sammeln, Aufbereiten & Kontextualisierung von Merkmalen
- Problematik:
  - Breite Masse an auffälligen Daten (z.B. Port Scans)
  - Schwierige Datenbeschaffung (z.B. Botnetz Kommunikation)
  - Auswahl von relevanten & potentiell gefährlichen Merkmalen
  - Herstellung von Kontext (Zusammenhänge erkennen, Relationen aufbauen)



Was II?

- Wissensdatenbank
  - Enthält Wissen & Kontext zu derzeit relevanten und aktiven Cyber Angriffen
  - Datensätze untereinander verbundene Daten über
    - TTPs (Tactics, Techniques & Procedures)
      → Was & wie wird angegriffen?
    - Indikatoren (actionable intelligence - IoC, IoA)
      → Woran erkennt man, dass ein Angriff stattfindet?
    - Kampagnen
      → Wer steckt dahinter & was sind die Ziele/Absichten?

Woher?

- Sammlung von Thread Intelligence Daten in Feeds
  - Verschiedenste Formate
    - MISP
    - STIX
    - TAXII
  - Unterschiedliche Quellen
    - Kommerziell
    - Open Source
  - z.T. spezialisiert auf Einsatzgebiete

Woher II? (Tools)

- Where to start?
  - MITRE‘s Collaborative Research Into Threads (CRITs)
    (https://crits.github.io/)
  - Collective Intelligence Framework (CIF)
    (https://csirtgadgets.org/)
  - MISP
    (https://www.misp-project.org/)
  - Yeti
    (https://yeti-platform.github.io/)

→ Sammlung von Feeds
(Reihenfolge ohne Wertung)

Warum?

- Beurteilung der Bedrohungs- & Sicherheitslage eines Unternehmens
  - Notifikation über neue / andauernde Bedrohungen
  - Anauernde Beurteilung aufgrund von vorliegendem Wissen & Kontext
  - Effiziente Re-Evaluation der Lage nach Auftreten eines Indikators
- Aktives Vergleichen des Netzwerk Verkehrs auf bekannte Indikatoren (actionable intelligence)
  - Indikatoren können an verschiedensten Stellen abgeglichen werden (z.B. Firewall, SIEM, endpoint security)
  - Abgleich von Indikatoren ist effizient (Vgl. IDS/IPS)

Ende

Fragen?