Cyber Threat Intelligence

Assiel Taher
13.11.2018

Gliederung

- Motivation
- Einführung
- Definition
- CTI Typen
- CTI Frameworks
- Intelligence sharing
- Fazit
- Quellen

Motivation

- es gibt **IMMER** Angriffe
- neuere Angriffsmethoden
- bisherige Verteidigung greift meist erst beim Erkennen des Angriffs ein → Signatur-basiert
  → Angriff ist eine Frage der Zeit
- advanced persistent threat (APT)
  → Hacker sind **professionell**, **zielgerichtet** und sehr **raffiniert**. Sie umgehen die traditionellen Verteidigungen relativ einfach. Teilweise jahrelange Vorbereitung
- “CISOs have no direct control over threats to their organizations and can only be aware of the threats and prepared for their arrival.” - Rob McMillan, Gartner Inc.

Einführung

Also wie gewinnt man den Kampf gegen die Hacker?
→ Intelligence-based Ansatz

- die richtigen Informationen sammeln (Wer? Warum? Von Wo? Wie?)
- Angreifer sollten gar nicht erst zum Angriff kommen
- schnell und effektiv auf einen Angriff reagieren können

Einführung

Weg vom Reaktiven und hin zum Proaktiven...

- Zu viel Fokus wird auf technische Details gelegt (Was? Wann? Wo?)

→ wichtiger ist Tactic, Technique, Procedures (Wie?)
→ und die Angreifer selbst (Wer? Warum?)

Definition

“Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets to that can be used to inform decisions regarding the subject’s response to that menace or hazard.” - Rob McMillan

“Threat Intelligence is the contextualised output of a strategically-driven process of collection and analysis of information pertaining to the identities, goals, motivations, tools and tactics of malicious entities intending to harm or undermine a targeted organisation’s operations, ICT systems or the information flowing through them”- Bank of England

Definition

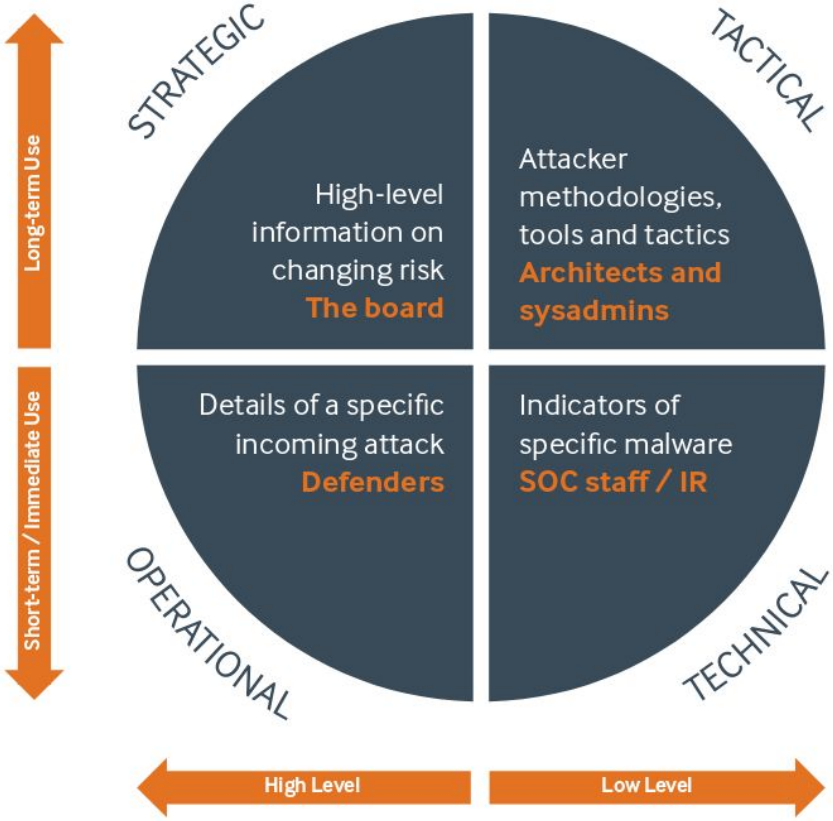
CTI sind Informationen, die helfen richtige Entscheidungen zu treffen, wie z.B:

- bestimmte Maßnahmen gegen einen bestehenden Angriff einzuleiten
- bestimmte Maßnahmen einzuleiten um einen Angriff zu verhindern
- bestimmte Maßnahmen einzuleiten Angriffe zu erkennen
- oder neue Risiken zu entdecken

CTI Typen

- Strategic Threat Intelligence
- Operational Threat Intelligence:
- Tactical Threat Intelligence
- Technical Threat Intelligence

Jeder Typ ist für eine andere Zielgruppe relevant!



(Quelle: https://www.mwrinfosecurity.com/assets/Whitepapers/Threat-Intelligence-Whitepaper.pdf)

Strategic Threat Intelligence

Nutzer: Leitungs- und Kontrollgremium, die strategische Entscheidungen treffen

Inhalt: Aktuelle Hacker Aktivitäten

Zweck: Risiken verstehen, entdecken, strategische Entscheidungen treffen

Informationsquellen: Nachrichten, Artikel, Open Source Intelligence (OSINT; also aus öffentlichen Quellen)

Operational Threat Intelligence

Nutzer: Security Abteilung

Inhalt: Wann? Wer? Wo? Warum? Wie? Fähigkeiten?

Zweck: Angriffe erschweren/verhindern

Informationsquellen: Berichte über Events, Social Media, Chat rooms etc.

Probleme: Unternehmen haben nicht die Infrastruktur um Daten abzufangen. GILT NICHT FÜR NSA!

Tactical Threat Intelligence

Nutzer: Security Abteilung (technische Ebene), Administrator etc.

Inhalt: “Tactic, Technique, Procedures”

Zweck: Wie gehen Angreifer taktisch vor? Angriffe verhindern

Informationsquellen: Berichte über Angriffe, Malware Analyse

Technical Threat Intelligence

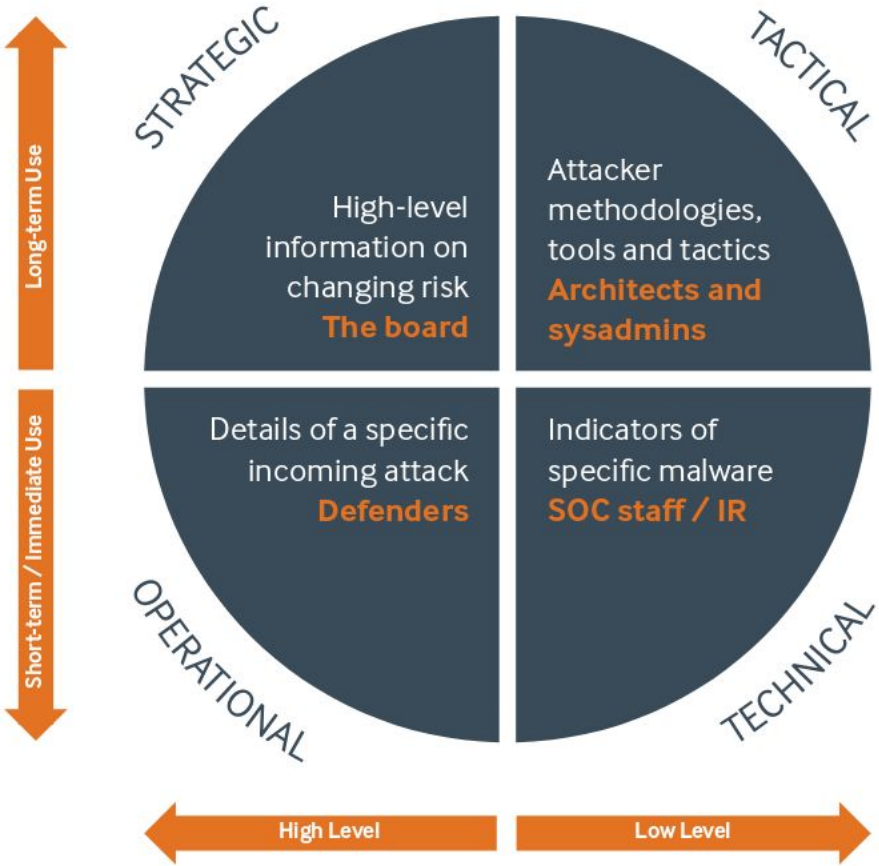
Nutzer: Security Abteilung (technische Ebene), Administrator etc.

Inhalt: technische Details wie IP Adressen, Tools, Indicator of Compromise, Infrastruktur etc.

Zweck: Wie gehen Angreifer technisch vor? Angriffe verhindern

Informationsquellen: Logs

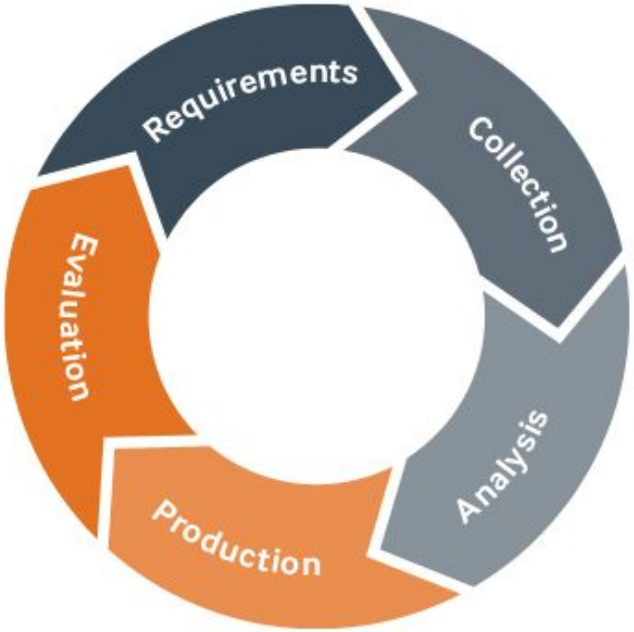
Probleme: verliert schnell an Wert, da z.b. IP Adressen leicht ausgetauscht werden können etc.


Long-term Use
Short-term / Immediate Use
STRATEGIC
TACTICAL
OPERATIONAL
TECHNICAL
High-level information on changing risk
The board
Attacker methodologies, tools and tactics
Architects and sysadmins
Details of a specific incoming attack
Defenders
Indicators of specific malware
SOC staff / IR
High Level
Low Level

CTI Frameworks

- Jeder der CTI betreibt muss selbst entscheiden wie er vorgehen wird.
- z.B. Anforderungen Basierter Ansatz:
  - Anforderungen
  - Sammeln → wichtigster Punkt
  - Analyse
  - Ausführung
  - Evaluation
- Die richtigen Quellen sind von größter Bedeutung!

CTI Zyklus



(Quelle: https://www.mwrinfosecurity.com/assets/Whitepapers/Threat-Intelligence-Whitepaper.pdf)

Intelligence sharing

- andere Organisationen profitieren von den geteilten Informationen
- viele Informationen sind nicht nur Unternehmensspezifisch, sondern Sektorspezifisch
- Angreifer haben meist einen bestimmten Sektor im Auge und greifen mehrere Organisationen des Sektors an

Intelligence sharing

Es hat aber auch Nachteile!

- man gibt sensible Informationen raus (z.B. man wurde angegriffen)
- Angreifer wissen was man über sie weiß
- Angreifer ändern ihre Taktiken

Intelligence sharing

Also mit wem teilen?

- Vertrauen ist wichtig
- geschlossene Gruppen bilden z.B. mit bestimmten Firmen eine Partnerschaft eingehen
- Enge Beziehungen mit Leuten aus anderen Firmen nutzen
- Es gibt aber auch öffentliche Gruppen wie Foren → nicht empfehlenswert

Fazit

- CTI kann Sicherheit stark erhöhen, wenn man es richtig macht und sich Zeit nimmt
- Qualität geht über Quantität
- Einführung von machine-learning kann Arbeit erleichtern
- Momentan sind Menschen in diesem Bereich nicht zu ersetzen

Quellen

- Röcher, DJ. Datenschutz Datensich (2018) 42: 623. https://doi.org/10.1007/s11623-018-1013-2
- https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf
- https://reprints.forrester.com/#/assets/2/1456/RES143275/reports
- https://www.cisecurity.org/blog/what-is-cyber-threat-intelligence/
- https://reprints.forrester.com/#/assets/2/1456/RES143275/reports
- https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf?la=en&hash=4B42B0382D1D33402689478433E2E1E0FFA93055