Cyber Threat Exchange Liechtenstein
26. September 2023

AVANTEC
Competence. Security. Trust.

Mehrwert hochwertiger Threat Intelligence bei der Vorbereitung oder Bewältigung von Cyberangriffen

Christian Grob
Head of Security Services, grob@avantec.ch

Agenda

AVANTEC
Competence. Security. Trust.

1. Einleitung
2. Arten von Threat Intelligence
3. Bereiche und Fragestellungen
4. Stakeholder
5. Quellen & Marktübersicht
6. Threat Intelligence Lifecycle
7. Beispiele Threat Landscape
8. AVANTEC Threat Intelligence Services
9. Q&A

AVANTEC
Competence. Security. Trust.

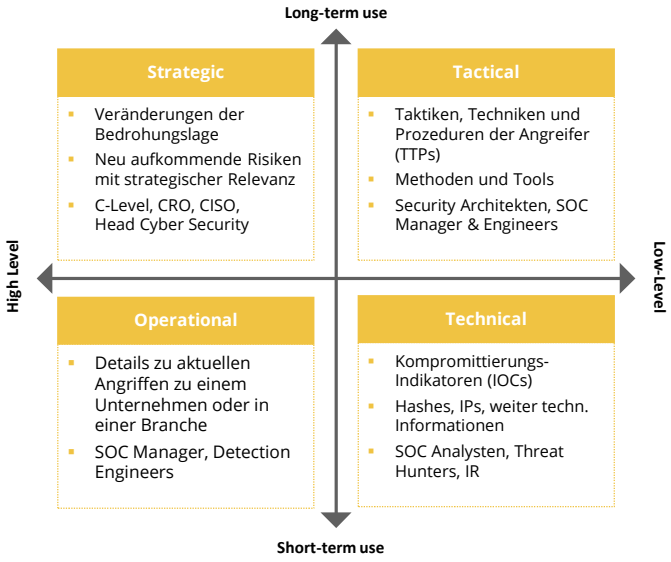
Cyber Threat Exchange Liechtenstein
26. September 2023

Einleitung

Angriffsfläche	**Wachsende Angriffsfläche** durch zunehmenden Einsatz & Komplexität der Technologie
Bedrohungen	Informationen über Bedrohungen müssen **schneller verarbeitet** werden ▪ um mit der **Geschwindigkeit** und Professionalisierung der **Angreifer mitzuhalten** ▪ und das Sicherheitsdispositiv **rechtzeitig** zu **adaptieren**
Definition	**Threat Intelligence** ▪ entsteht durch **Bewertung** vergangener, gegenwärtiger und potenzieller **Bedrohungen** ▪ unter **Berücksichtigung** des **Kontext** des jeweiligen Unternehmens ▪ um **möglichst viel Klarheit** für gute strategische, taktische und operative **Entscheide & Investitionen** zu schaffen
Status Quo	**Viele Unternehmen** nutzen Threat Intelligence **"nur" am Rande** z.B. in Form von Feeds

Threat intelligence is contextualised information about adversarial threats past, present and predicted attacks against the organisation, produced through analysis of available data and information, to inform decisions and actions. ISF

Arten von Threat Intelligence



Threat Intelligence soll:

relevant sein
Berücksichtigung der **spezifischen Gegebenheiten** des Unternehmens & konkreten Geschäftsfeldes

zeitgerecht sein
Balance zwischen **Geschwindigkeit & Qualität** der bereitgestellten Information

vertrauenswürdig sein
Verlässliche und qualitativ **hochwertige Quellen** erhöhen den effektiven **Mehrwert**

AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

Bereiche und Fragestellungen

AVANTEC
Competence. Security. Trust.

Bereiche	Beispiel Fragestellungen
Branche (Industrie)	Welche Angriffe sind in unserer Branche wahrscheinlich? Von welchen Angriffen sind meine direkten Konkurrenten betroffen?
Geographisch	Welche Angriffe sind in unserer Land/Region wahrscheinlich? Welche Angreifer Gruppen sind besonders in unserem Land/Region aktiv?
Technologie	Gibst es Angriffe die speziell auf von uns eingesetzte Technologien abzielen? Werden spezifische Schwachstellen in eingesetzten Technologien ausgenutzt?
Geplante Angriffe	Gibt es Anzeichen für einen bevorstehenden Angriff auf unser Unternehmen? Bieten wir Angriffsfläche die für Angreifer ein leichtes Ziel darstellen könnte?
Kunden	Werden unsere Kunden angegriffen und könnte dies unserem Unternehmen schaden? Könnte ich meine Kunden frühzeitig über bevorstehende Angriffe informieren?
Gechäftspartner (3rd Parties)	Werden unsere Geschäftspartner angegriffen & könnte dies unserem Unternehmen schaden? Stellen gewisse Geschäftspartner ein erhöhtes Risiko dar?
Erfolgreiche Angriffe	Gibt es Indikatoren für einen bereits erfolgreich stattgefunden Angriff? Sind Accounts teil eines Dumps oder werden Accounts im Dark Web verkauft?

Stakeholder & Art der Information

AVANTEC
Competence. Security. Trust.

Beispiele für Art der Information	Stakeholder
Strategische Intelligence Reports (Trends, Ausblick, Einschätzung)	1 4 7 9
Aktuelle Bedrohungslage (Threat Landscape, Angreifer Gruppen)	4 5 7 9
Threat Models, TTPs, Tools	2 3 5 8
Vulnerability Intelligence / Patch Priorisierung (Criticals, Zero Days)	2 4 6 8
Indicators of Compromise (IOC) (Hashed, URLs, IPs)	2 3 8
Auffälligkeiten im Dark Web (Accounts, Foren etc.)	2 4
3rd Party Risiken, Ratings, Auffälligkeiten, Leaks, Erpressungen	2 4 10
Veränderungen in der externen Angriffsfläche	2 4 6
Threat Hunting Kampagnen (Yara Rules etc.)	2
Registration von verdächtigen Domains (Typosquatting)	2 4

AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

Quellen & Marktübersicht

AVANTEC
Competence. Security. Trust.

Gängige Informationsquellen

- **Intern**
  - Security Incident Daten
  - Security Analytics / SIEM / Logs
- **Interessensgruppen**
  - Industrie Gruppen, ISACs
  - Austausch mit Peers
- **Öffentlich**
  - Internet, News, Foren, Soziale Netzwerke
  - Freie Feeds, IP, Domain, URL Listen etc.
- **Regierungsnahe**
  - Nationale Gruppen, NCSC
  - Internationale Gruppen, Enisa, CISA
- **Kommerziell**
  - Threat Intelligence Anbieter/Services
  - Recorded Future, CrowdStrike etc.

Forrester Wave Q3 2023

Threat Intelligence Lifecycle

AVANTEC
Competence. Security. Trust.

Feedback
Einholen von Stakeholder Feedback, kontinuierliche Anpassung & Verbesserung der Threat Intelligence

Anforderungen
Erarbeitung der Anforderungen, Definition der relevanten Bereiche, Fragestellungen, Stakeholder, Art der Information, Intervall, Format

Integration in Prozesse
Integration der Threat Intelligence in die relevanten (Entscheidungs-) Prozesse, Einleitung von Massnahmen

Informationsbeschaffung
Auswahl der Quellen & Sammlung der benötigten Informationen für die Erfüllung der Anforderungen

Bereitstellung Intelligence
Aufbereitung in den Formaten die für die Stakeholder definiert wurden & Kommunikation auf den vereinbarten Kanälen

Informationsverarbeitung
Verarbeitung & Analyse der Informationen zur Findung der Antworten auf die definierten Fragestellungen

AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

Beispiel Threat Landscape

Recorded Future® AVANTEC Competence. Security. Trust.

Welche Angreifer Gruppen sind in unserer Region & in der Finanz-industrie aktiv?

Beispiel Threat Landscape

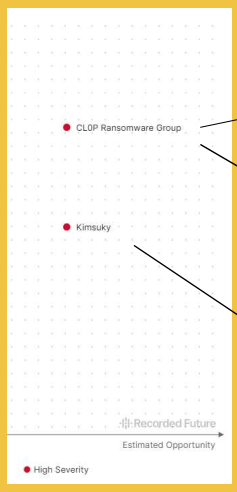
Recorded Future® AVANTEC Competence. Security. Trust.

Welche Angreifer Gruppen sind in unserer Region & in der Fertigungs-industrie aktiv?

AVANTEC Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

Beispiel Threat Landscape



Attack Vector
C&C Server
Data Encrypted for Impact
Drive-by compromise
File and Directory Permis...
Network Share Discovery
Phishing
Virtualization/Sandbox E...
Zero Day Exploit

Welche Angriffsvektoren werden eingesetzt?

Vulnerability
CVE-2021-35211
CVE-2022-31199
CVE-2022-47986
CVE-2023-0669
CVE-2023-27350
CVE-2023-34362
CVE-2023-27351

Werden spezifische Schwachstellen ausgenutzt?

Domain
naversecurity.us
nknews.pro
yonsei.lol
cloudsecurityservice.net

Gibt es Indicators of Compromise?

AVANTEC Threat Intelligence Services

Threat Intelligence Beratung

- Unterstützung beim Aufbau eines Threat Intelligence Programmes
- Beratung bei der Wahl der Quellen und Anbieter
- Gemeinsame Erarbeitung der Anforderungen in Abstimmung mit den Stakeholder Bedürfnissen

Threat Intelligence Services

- Bereitstellung hochwertiger Threat Intelligence
- Unternehmensspezifische Threat Landscape
- Option für Betrieb einer MISP Instanz inkl. Bereitstellung der Feeds - Indicators of Compromise

Dark Web Monitoring

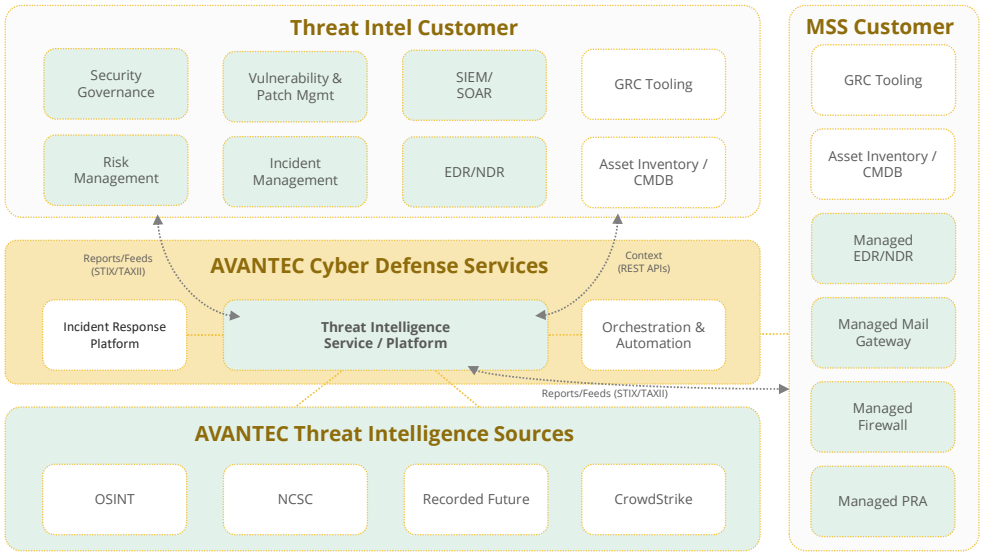
- Überwachung des Dark Web auf Data Leaks, Account Leaks & auffällige Erwähnungen in Foren
- Überwachung von Paste Sites, Onion Sites, Git
- Überwachung Ransomware Extortion Sites

AVANTEC
Competence. Security. Trust.

Cyber Threat Exchange Liechtenstein
26. September 2023

Backup Slides

Threat Intelligence Services



Cyber Threat Exchange Liechtenstein
26. September 2023

Stakeholder & Art der Information

AVANTEC
Competence. Security. Trust.

Beispiele für Art der Information	Stakeholder
Strategische Intelligence Reports (Trends, Ausblick, Einschätzung)	1 4 7 9
Aktuelle Bedrohungslage (Threat Landscape, Angreifer Gruppen)	4 5 7 9
Threat Models, TTPs, Tools	2 3 5 8
Vulnerability Intelligence / Patch Priorisierung (Criticals, Zero Days)	2 4 6 8
Indicators of Compromise (IOC) (Hashed, URLs, IPs)	2 3 8
Auffälligkeiten im Dark Web (Accounts, Foren etc.)	2 4
3rd Party Risiken, Ratings, Auffälligkeiten, Leaks, Erpressungen	2 4 10
Veränderungen in der externen Angriffsfläche	2 4 6
Threat Hunting Kampagnen (Yara Rules etc.)	2
Registration von verdächtigen Domains (Typosquatting)	2 4