

Finance Round Table «E-Mail Security neu gedacht» 29. Februar 2024

AVANTEC
Competence. Security. Trust.



Mehrwert hochwertiger Threat Intelligence bei der Vorbereitung oder Bewältigung von Cyberangriffen

Christian Grob
Head of Security Services
Mitglied der Geschäftsleitung

Agenda

AVANTEC
Competence. Security. Trust.

- 1 Arten von Threat Intelligence
- 2 Bereiche und Fragestellungen
- 3 Stakeholder
- 4 Quellen & Marktübersicht
- 5 Threat Intelligence Lifecycle
- 6 Beispiele Threat Intelligence
- 7 AVANTEC Cyber Defense Services
- 9 Q&A

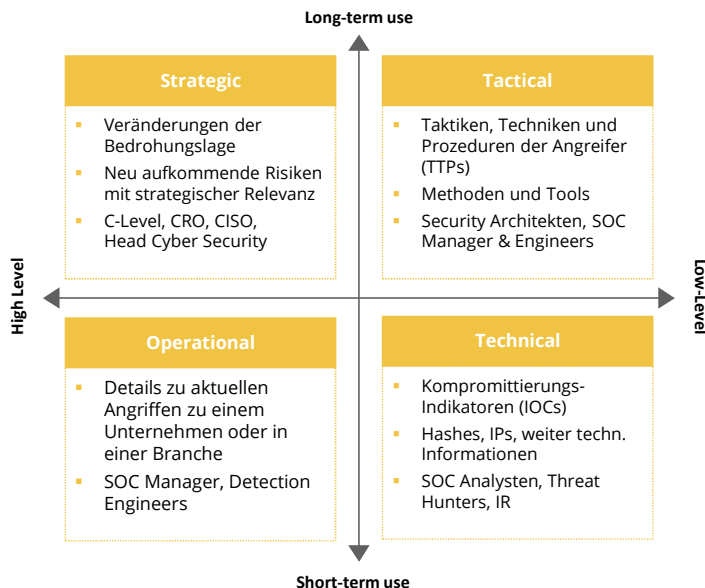
Finance Round Table «E-Mail Security neu gedacht» 29. Februar 2024

Einleitung



Angriffsfläche	Wachsende Angriffsfläche durch zunehmenden Einsatz & Komplexität der Technologie
Bedrohungen	Informationen über Bedrohungen müssen schneller verarbeitet werden <ul style="list-style-type: none"> um mit der Geschwindigkeit und Professionalisierung der Angreifer mitzuhalten und das Sicherheitsdispositiv rechtzeitig zu adaptieren
Definition	Threat Intelligence <ul style="list-style-type: none"> 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

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**

Finance Round Table «E-Mail Security neu gedacht» 29. Februar 2024

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	Gibt 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?
Geschäftspartner (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 stattgefundenen 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

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

Stakeholder

1	4	7	9	<input type="checkbox"/>
4	5	7	9	<input type="checkbox"/>
2	3	5	8	<input type="checkbox"/>
2	4	6	8	<input type="checkbox"/>
2	3	8	<input type="checkbox"/>	<input type="checkbox"/>
2	4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	4	10	<input type="checkbox"/>	<input type="checkbox"/>
2	4	6	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Finance Round Table «E-Mail Security neu gedacht» 29. Februar 2024

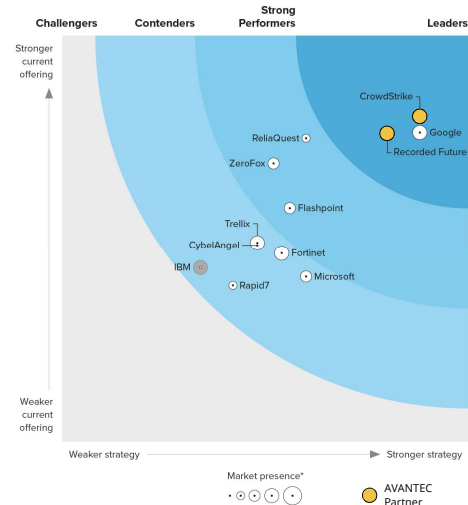
Quellen & Marktübersicht



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



Feedback

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

6

Anforderungen

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

1

Integration in Prozesse

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

5

Informationsbeschaffung

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

2

Bereitstellung Intelligence

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

4

Informationsverarbeitung

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

3

Threat Intelligence Lifecycle

Finance Round Table «E-Mail Security neu gedacht» 29. Februar 2024

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.



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

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

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

Welche Angriffsvektoren werden eingesetzt?

Werden spezifische Schwachstellen ausgenutzt?

Gibt es Indicators of Compromise?

Finance Round Table «E-Mail Security neu gedacht» 29. Februar 2024

Technical Intelligence



Recorded Future

DOMAIN

xbox-ms-store-debug.com

Notes: 2 Inskit Group Notes
References: 1 000+
First Reference: Nov 21, 2020
Latest Reference: Jan 2, 2024
Recorded Future Community: Domain

70
MALICIOUS RISK SCORE
8 of 53 Risk Rules Triggered

Show recent events or cyber events

Recorded Future AI Insights

Narrative View

The domain xbox-ms-store-debug.com has been identified as a threat in multiple instances. It has been observed to be a malware site domain that leads to malicious content such as executables, drive-by infection sites, malicious scripts, viruses, trojans, or code. Additionally, it is suspected to be a phishing URL/domain that may be utilized in phishing campaigns. There have been reports of its association with the SDBot CC server and the TASSO group. It has also been mentioned in relation to the CLOP Ransomware Operation. The domain has been detected exhibiting malicious behavior and has been flagged by BitDefender. These observations highlight the potential cybersecurity risks associated with xbox-ms-store-debug.com.

Generated based on 8 Risk Rules | Analyst: Christian Grob

Recorded Future

TRIGGERED RISK RULES

Learn More

- Recently Detected Malware Operation - 1 sighting on 1 source
External Sensor Data Analysis. xbox-ms-store-debug.com is observed to be a malware site domain that navigates to malicious content including executables, drive-by infection sites, malicious scripts, viruses, trojans, or code.
- Recently Suspected Phishing Techniques - 1 sighting on 1 source
External Sensor Data Analysis. xbox-ms-store-debug.com is suspected to be a phishing URL/Domain that may be used in phishing campaigns.
- Historically Detected Malware Operation - 31 sightings on 2 sources
External Sensor Data Analysis. BitDefender. xbox-ms-store-debug.com is observed to be a malware site domain that navigates to malicious content including executables, drive-by infection sites, malicious scripts, viruses, trojans, or code.
- Historically Suspected Phishing Techniques - 13 sightings on 1 source
External Sensor Data Analysis. xbox-ms-store-debug.com is suspected to be a phishing URL/Domain that may be used in phishing campaigns.
- Historically Reported by Inskit Group - 2 sightings on 1 source
Inskit Group. 2 reports including An Overview of FIN1's CLOP Ransomware Operation. Most recent link (Jan 13, 2021): https://app.recordedfuture.com/portal/analyst-note/ctocg72MAN
- Historically Reported as a Defanged DNS Name - 2 sightings on 2 sources
@tbarabosch. @AdamTheAnalyst. Most recent tweet: is the latest #SDBot CC server xbox-ms-store-debug.com (89.40.206.124) really still up and running? It seems to respond correctly to #SDBot traffic as of now. Be sure to block it: #A505. Most recent link (Jan 12, 2021): https://twitter.com/tbarabosch/statuses/134897312099731072
- Historically Suspected Malware Operation - 1 sighting on 1 source
BitDefender. Detected malicious behavior from an endpoint agent via global telemetry. Last observed on Apr 4, 2021.
- Historically Reported in Threat List - Previous sightings on 1 source
Recorded Future Analyst Community Trending Indicators. Observed between Nov 18, 2023, and Nov 18, 2023.

SCREENSHOTS

URL: https://xbox-ms-store-debug.com/ Image Actions

Real World Data Sample



```
"subject": "Username",
"dumps": [
  {
    "name": "Stealer Malware Logs 2023-08-31",
    "description": "This credential data was derived from stealer malware logs.",
    "downloaded": "2023-09-18T16:44:43.666Z",
    "compromise": {
      "exfiltration_date": "2023-08-31T19:35:00.000Z",
      "os": "Windows 10 Enterprise 64 Bit",
      "os_username": "Username",
      "malware_file": "C:\\FRS7\\taskhostw.exe",
      "computer_name": "DESKTOP-6000BHM",
      "antivirus": [
        "Windows Defender"
      ]
    },
    "infrastructure": {
      "ip": "IP",
      "location": {
        "country": "AT"
      }
    }
  },
  {
    "first_downloaded": "2023-09-18T16:44:43.666Z",
    "latest_downloaded": "2023-09-18T16:44:43.666Z",
    "exposed_secret": {
      "type": "clear",
      "hashes": [
        {
          "algorithm": "SHA1",
          "hash_prefix": "913c"
        },
        {
          "algorithm": "SHA256",
          "hash_prefix": "ddcf"
        },
        {
          "algorithm": "NTLM",
          "hash_prefix": "02d0"
        },
        {
          "algorithm": "MD5",
          "hash_prefix": "f4bc"
        }
      ]
    }
  }
]
```

```
"details": {
  "properties": [
    "Letter",
    "Number",
    "UpperCase",
    "LowerCase",
    "AtLeast12Characters"
  ],
  "clear_text_hint": "DN",
  "effectively_clear": true
},
"compromise": {
  "exfiltration_date": "2023-08-31T19:35:00.000Z"
},
"authorization_service": {
  "url": "https://secure.Username/",
  "domain": "Username",
  "fqdn": "secure.Username",
  "technology": [],
  "protocols": [
    "https"
  ]
},
"malware_family": {
  "name": "Dark Crystal RAT",
  "id": "ZEgKiv"
}
```

Username

Infection details

Credential age

MD5, SHA1, SHA256 and NTLM Hashes

Password Properties

Login URL

Malware Family

Finance Round Table «E-Mail Security neu gedacht»

29. Februar 2024

AVANTEC Cyber Defense Portfolio

AVANTEC
Competence. Security. Trust.

Managed EDR

CROWDSTRIKE

- Erkennung & Verhinderung der Ausbreitung von Cyberangriffen mittels schlankem Endpoint Agent
- Next GEN AV, EDR, Threat Hunting
- Umfangreiche Handlungsoptionen, direkter Eingriff auf Endpoints

Managed NDR

VECTRA

- Erkennung & Verhinderung der Ausbreitung von Cyberangriffen durch Überwachung des Netzwerkverkehrs
- Kombination verschiedener Analyse-Verfahren u.a. ML/AI
- Ohne Agent auf den Endpoints

Threat Intel Services

Recorded Future

Threat Intelligence

- Bereitstellung hochwertiger Threat Intelligence
- Unternehmensspezifische Threat Landscape
- Betrieb einer MISP Instanz inkl. Bereitstellung von Feeds - Indicators of Compromise (IOC)

Vulnerability Scanning

tenable

- Identifikation von Schwachstellen mit regelmässigen Scans von extern oder intern
- Verwaltung der Scan Policies
- Regelmässiges Reporting mit Empfehlungen
- Verwalten der False-Positives

Managed Security Analytics

Hunters.

- Korrelation & Analyse von sicherheitsrelevanten Daten auf Basis der Hunters SOC Plattform
- Moderne SOC Plattform mit «Detection Engineering als Service» - 75-95%
- Keine Limiten für Log Ingestion

Dark Web Monitoring

KADUU

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