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

Cyber Bedrohungslage

AVANTEC
Competence. Security. Trust.

Knapp 50’000 Meldungen im 2023 beim Nationalen Zentrum für Cyber Sicherheit (NCSC) – im Vergleich zum Vorjahr +30%

Terabytes sensitiver Daten von CH Unternehmen **im Dark Web** – Double Extortion beliebt bei Angreifer

Cyberkriminelle werden **professioneller** – **84 Minuten** vergehen gemäss CrowdStrike vom Initial Access -> Lateral Movement

Ungepatchete **Schwachstellen**, offene oder **falsch konfigurierte** extern erreichbare Dienste, **Supply-Chain Angriffe**

Das **Zeitfenster**, um Angriffe abzuwehren bevor diese einen grösseren Schaden anrichten, **wird immer kleiner**

Mittelständische Unternehmen vermehrt im Visier, **fehlende Ressourcen** im Bereich Cyber Sicherheit führen zu Breaches

www.ncsc.admin.ch/ncsc/de/home/aktuell/aktuelle-zahlen.html
www.crowdstrike.com/resources/reports/global-threat-report-executive-summary-2023/

Einleitung

AVANTEC
Competence. Security. Trust.

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

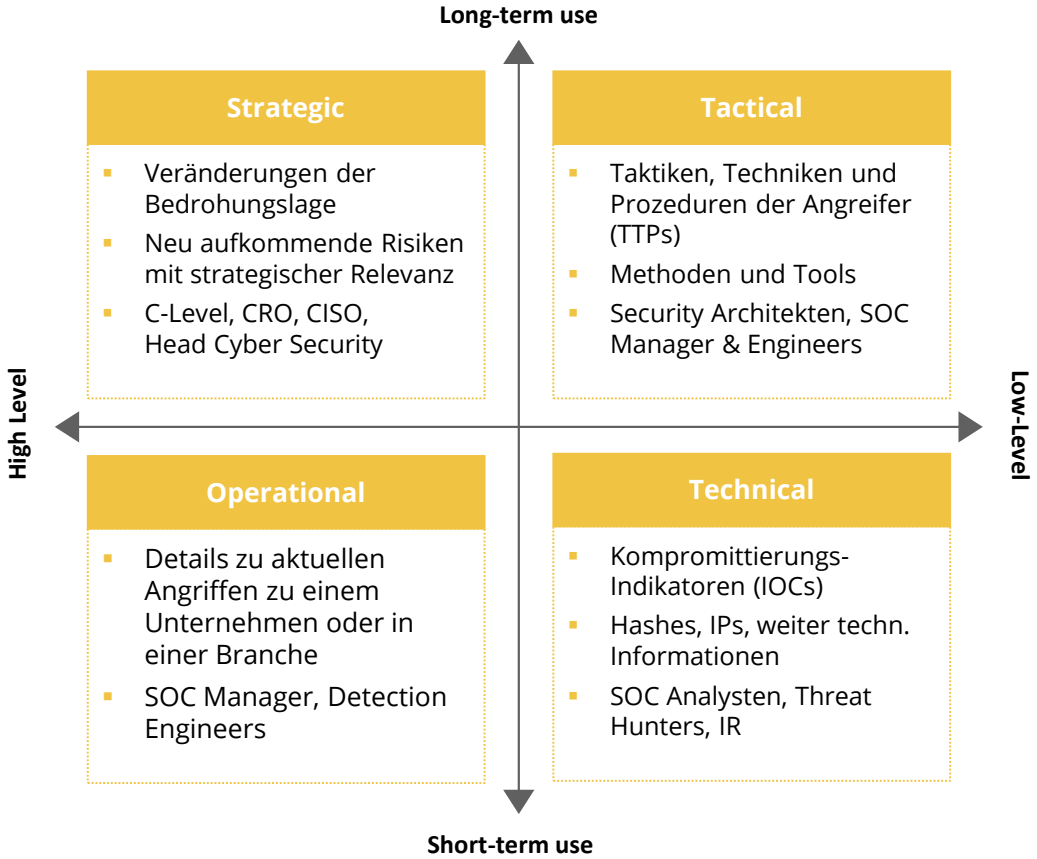
- entsteht durch **Bewertung** vergangener, gegenwärtiger und potenzieller **Bedrohungen**
- unter **Berücksichtigung** des **Kontext** des jeweiligen Unternehmens
- um **möglichst viel Klarheit** für gute strategische, taktische und operative **Entscheide & Investitionen** zu schaffen

Status Quo

Viele Unternehmen nutzen Threat Intelligence **“nur” am Rande** z.B. in Form von Feeds

Arten von Threat Intelligence

AVANTEC
Competence. Security. Trust.



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**

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

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

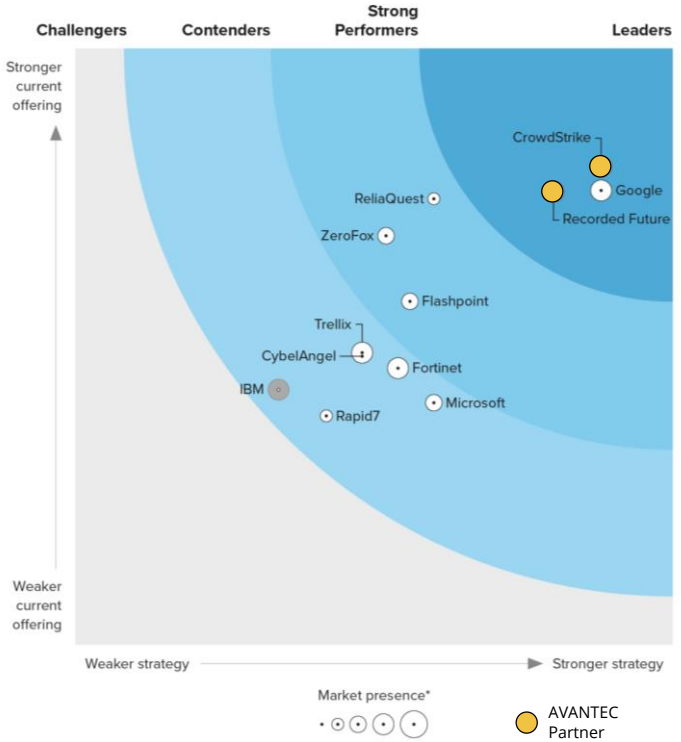
Quellen & Marktübersicht

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.

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

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

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

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

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

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

Beispiel Threat Landscape

Recorded Future®

AVANTEC
Competence. Security. Trust.

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

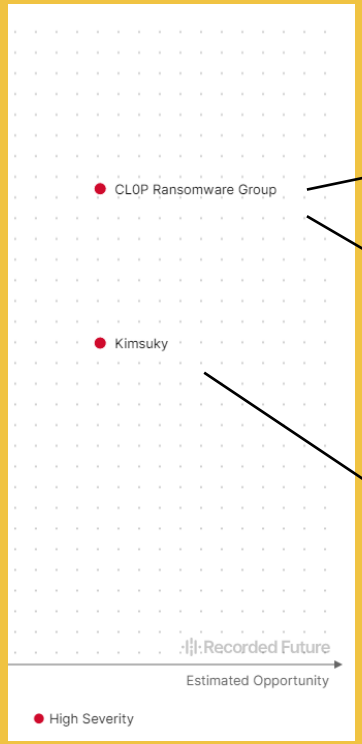
Beispiel Threat Landscape

Recorded Future®

AVANTEC
Competence. Security. Trust.

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

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

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

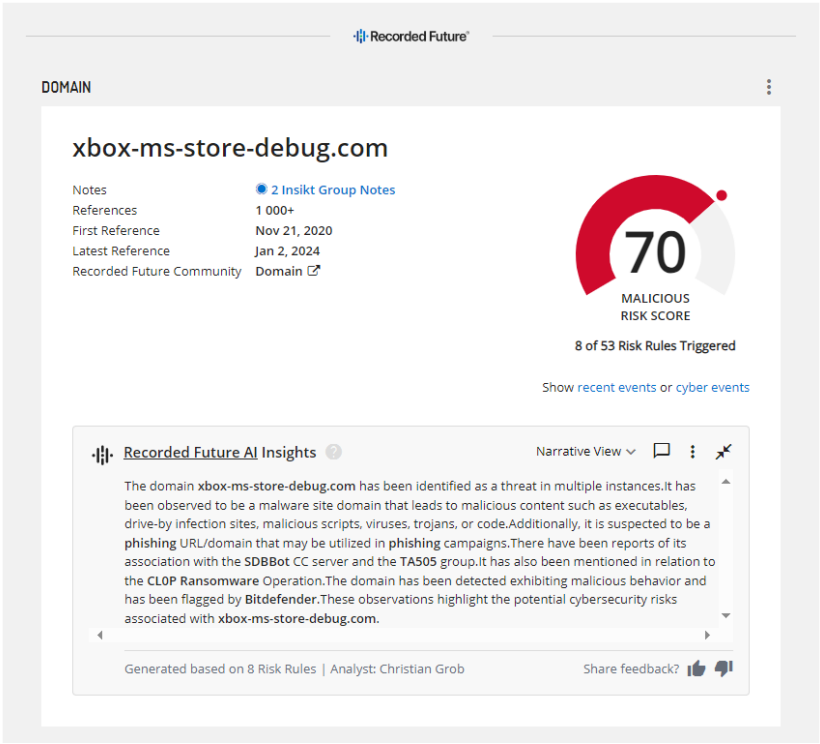
Welche Angriffsvektoren werden eingesetzt?

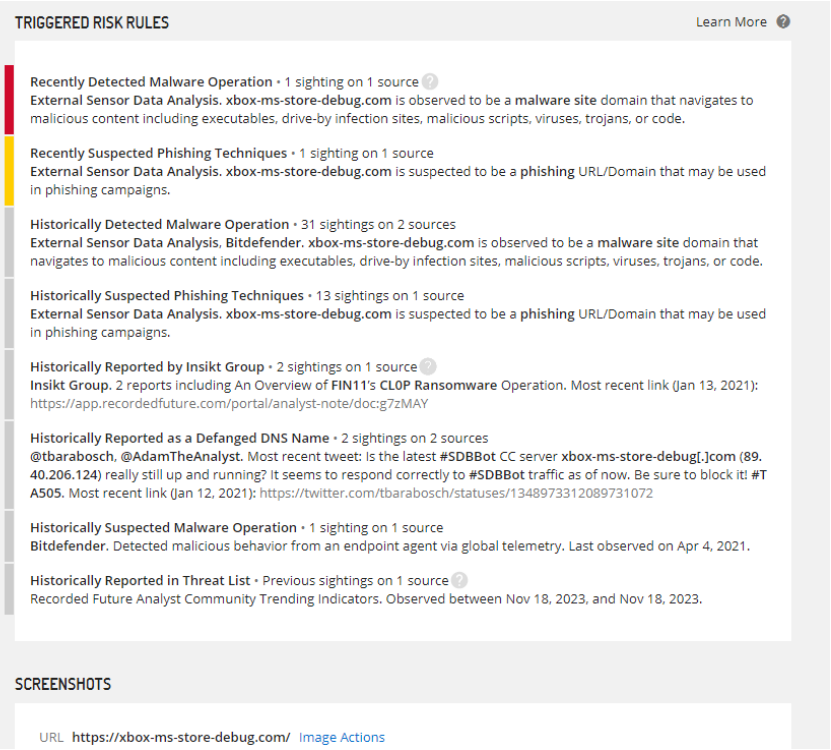
Werden spezifische Schwachstellen ausgenutzt?

Gibt es Indicators of Compromise?

Technical Intelligence

AVANTEC
Competence. Security. Trust.





Real World Data Sample

AVANTEC
Competence. Security. Trust.


```
"subject": [redacted],
"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": [redacted],
            "malware_file": "C:\\FRST\\taskhostw.exe",
            "computer_name": "DESKTOP-6OO0BHN",
            "antivirus": [
                "Windows Defender"
            ]
        },
        "infrastructure": {
            "ip": [redacted]
        },
        "location": {
            "country": "AT"
        }
    }
],
"first_downloaded": "2023-09-18T16:44:43.663Z",
"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"
        }
```


Username

Infection details

Credential age

MD5, SHA1, SHA256 and NTLM Hashes


```
        "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.[redacted]\/",
        "domain": [redacted],
        "fqdn": "secure[redacted],
        "technology": [],
        "protocols": [
            "https"
        ]
    },
    "malware_family": {
        "name": "Dark Crystal RAT",
        "id": "ZEqKiV"
    }
```


Password Properties

Login URL

Malware Family

Real World Data Sample


```
"subject": [redacted]
"dumps": [
    {
        "name": "Stealer Malware Logs 2023-06-11",
        "description": "This credential data was derived from stealer malware logs. These logs are
        "downloaded": "2023-06-12T12:26:50.996Z",
        "compromise": {
            "exfiltration_date": "2023-06-11T13:44:33.000Z",
            "os": "Windows 10 Home Single Language [x64]",
            "os_username": [redacted],
            "malware_file": "C:\\Users\[redacted]\AppData\\Local\\Programs\\NvNode\\Speech\\dwm.exe",
            "timezone": "UTC-06:00",
            "computer_name": [redacted]
        },
        "infrastructure": {
            "ip": [redacted]
        },
        "location": {
            "country": "MX"
        }
    }
],
"first_downloaded": "2023-06-12T12:26:50.996Z",
"latest_downloaded": "2023-06-12T12:26:50.996Z",
"exposed_secret": {
    "type": "clear",
    "hashes": [
        {
            "algorithm": "SHA1",
            "hash_prefix": "3900"
        },
        {
            "algorithm": "SHA256",
            "hash_prefix": "857b"
        },
        {
            "algorithm": "NTLM",
            "hash_prefix": "438b"
        },
        {
            "algorithm": "MD5",
            "hash_prefix": "c285"
```


Username

Infection details

Credential age

MD5, SHA1, SHA256 and NTLM Hashes


```
        "details": {
            "properties": [
                "Letter",
                "Number",
                "UpperCase",
                "LowerCase",
                "AtLeast10Characters"
            ],
            "clear_text_hint": "Je"
        },
        "effectively_clear": true
    },
    "compromise": {
        "exfiltration_date": "2023-06-11T13:44:33.000Z"
    },
    "authorization_service": {
        "url": "https:\/\/[redacted]vpn\/tmindex.html",
        "domain": "[redacted].com",
        "fqdn": "auth[redacted].com",
        "technology": [
            {
                "name": "Citrix NetScaler Access Gateway",
                "id": "Qtqzc7",
                "category": "CAfZv"
            },
            {
                "name": "VPN",
                "id": "CAfZv"
            }
        ],
        "protocols": [
            "https"
        ]
    },
    "malware_family": {
        "name": "Vidar",
        "id": "YuDlEm"
    },
    "cookies": [
        {
            "dns": [redacted]
            "name": "_ga",
            "http": true,
            "expiration": "2024-06-07T17:32:58.000Z",
            "secure": true
        },
        {
            "dns": [redacted]
            "name": "_gid",
            "http": true,
            "expiration": "2023-05-05T17:32:58.000Z",
            "secure": true
        }
```


Password Properties

Login URL

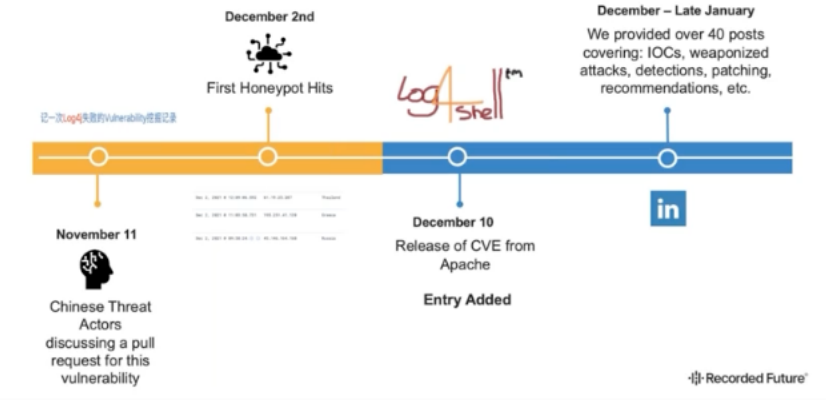
Malware Family

Cookies

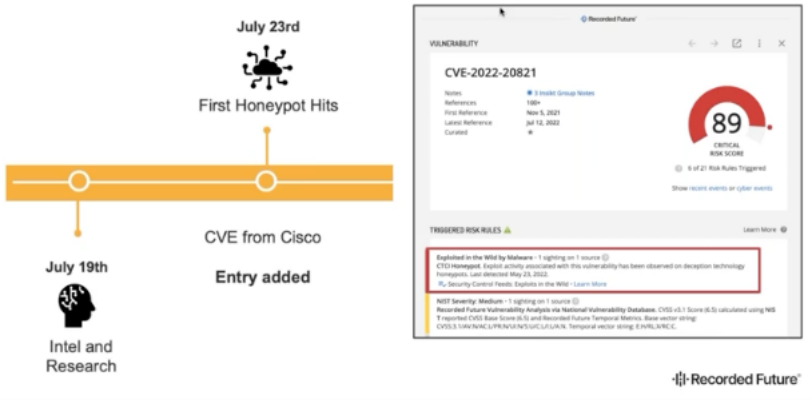
Vulnerability Intelligence

AVANTEC
Competence. Security. Trust.

Log4Shell (CVE-2021-44228)

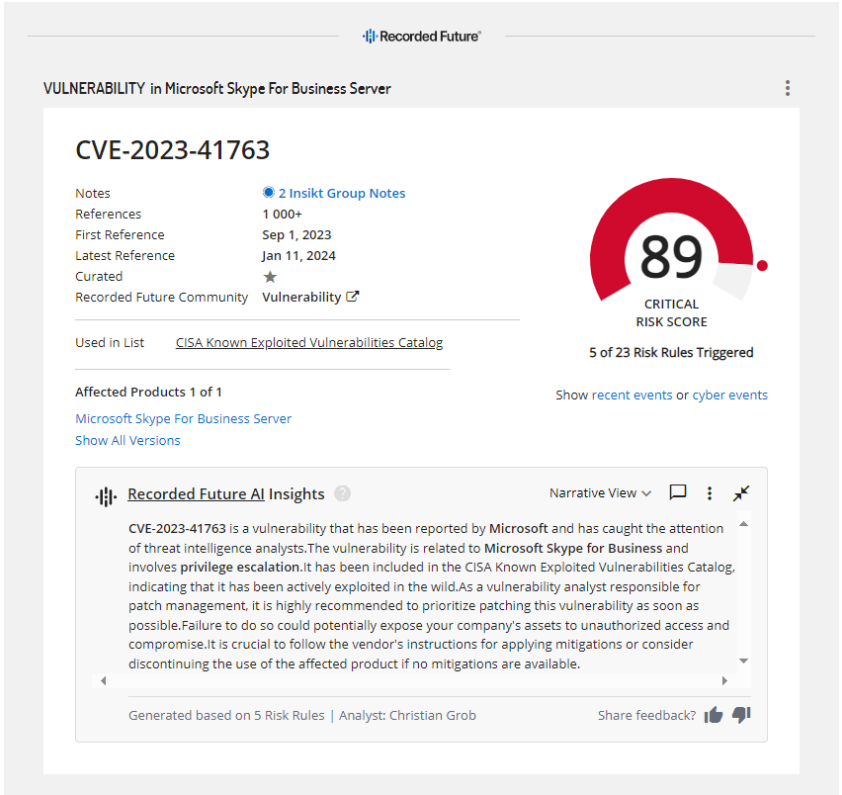


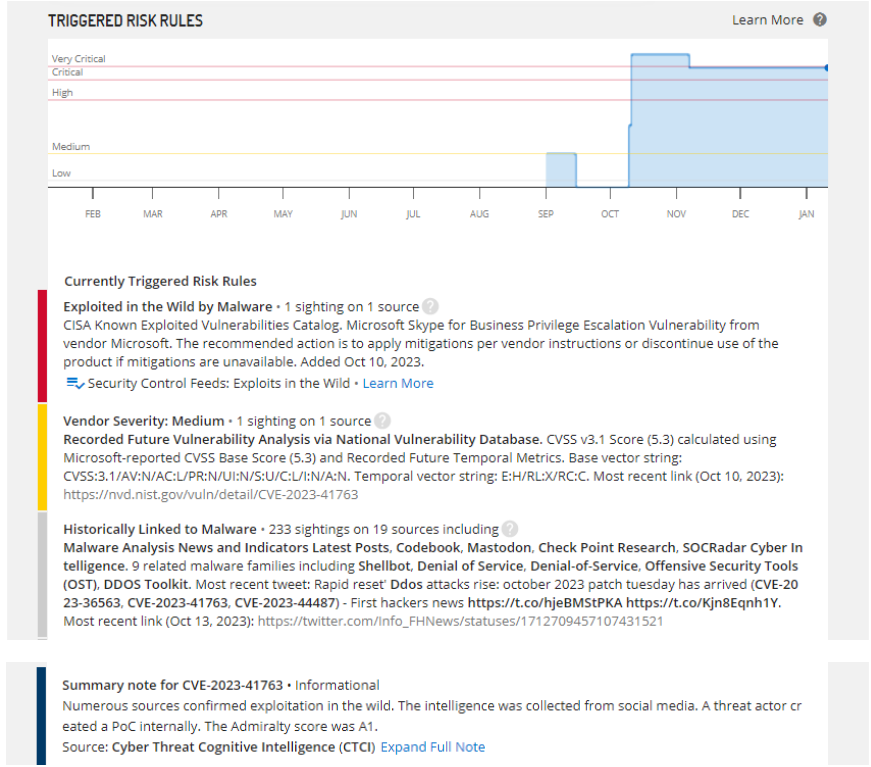
Cisco IOS XR Software (CVE-2022-20821)



Vulnerability Intelligence

AVANTEC
Competence. Security. Trust.





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

Vulnerablity 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

Threat Intel Services

Threat Intelligence

Recorded Future

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

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

Kontakt

AVANTEC AG
Christian Grob
Head Security Services

+41 44 457 13 13
c.grob@avantec.ch

https://www.linkedin.com/in/christian-grob-34529557

https://www.tec-bite.ch/author/christian-grob/