

INSEYA
simply secure





Cybersicherheit mit SASE-Technologie

Bern, 6. November 2024

Inseya AG



Kundenvortrag

Inseya

- Daniel Bieri – Security Consultant
- Lars Dänzer – Security Engineer

Ablauf



- Cyberrisiken
- Kundenvortrag
- Demo
- Zusammenfassung
- Apéro



Allianz Risk Barometer 2024

- Platz 1 – Cybervorfälle wie Ransomware-Angriffe oder Datenschutzverletzungen (57%*)
- Platz 2 – Energie Risiken (48%*)
- Platz 3 – Betriebsunterbrechungen (CH 41%*)

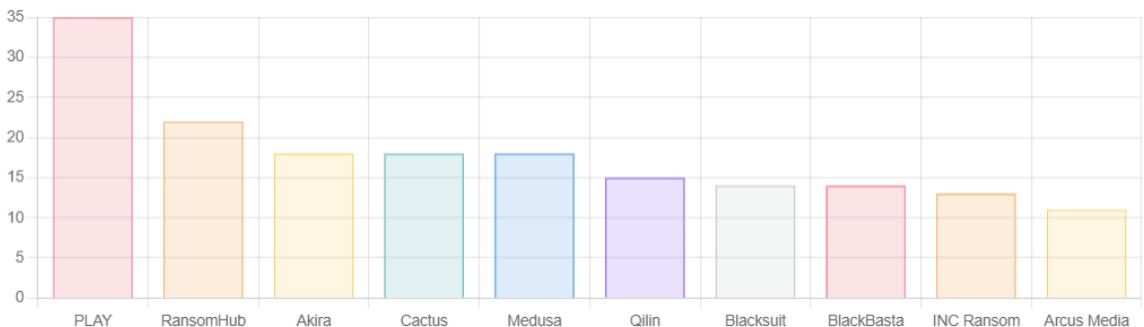
<< Wir sind an einem Punkt angelangt, an dem Cybersicherheit für Unternehmen genauso wichtig ist, wie die traditionellen Risiken >>

Angreifer Markt - Ransomware



- Bisher weltweit 3800 / Schweiz 31 (45) erfolgreiche Datendiebstähle
- Zwischen 260 – 510 Firmen pro Monat
- Daten Online von 2624 / Schweiz 21

Top Angreifer weltweit (bekannt ca. 450)



Top Angreifer Schweiz

- 8Base, Lockbit 3.0, BlackBasta, RansomHub, Akira, Ciciada3301
- Rhysida, Qilin, Cloak, Play, Eraleighnews, INC Ransom, Helldown, Mad Liberator, Cactus



Ransomware ist ein Art Virus, welcher den Zugriff auf die Geschäftsdaten mittels Verschlüsselung verhindert, bis ein Lösegeld bezahlt wurde. Zusätzlich werden die Daten vorgängig gestohlen um bei nicht bezahlen des Lösegeldes diese zu veröffentlichen oder weiterzuverkaufen.

Ablauf eines Ransomware-Angriffs



Zielerreichung – entwendete & verschlüsselte Daten



- Ransom (Entgeld) Umsatz und zeitabhängig
- Aufwandsentschädigung
- Bezahlung in Kryptowährung (Bitcoin)
- Russland, Nordkorea

The screenshot shows a grid of compromised websites with their data sizes. The websites include kumhotire.com, fordcountrymotors.mx, tpgagedcare.com.au, oleopalma.com.mx, chcm.us, nhbg.com.co, paybito.com, efile.com, crbrandsinc.com, bspcr.com, anhf.org.auh, projektalp.ch, promise.com, tims.com, ft.com, ecbawm.com, comtruck.ca, idahopacific.com, robertshvac.com, q-cells.de, and zoppo.com. The data sizes range from 1.5Gb to 8.4Tb. The website has a dark theme with a central image of a black hole labeled 'Abyss free DATA'.

Website	Data Size
kumhotire.com	11246 Gb
fordcountrymotors.mx	13D 08h 15m 16s
oleopalma.com.mx	PUBLISHED
chcm.us	11089 Gb
nhbg.com.co	16836 Gb
paybito.com	11188 Gb
efile.com	11087 Gb
crbrandsinc.com	CR Brands, Inc. was an American private-
bspcr.com	Dogecoin And Bitcoin Become Latest
anhf.org.auh	anhf.org.au 1.5Tb uncompressed data
projektalp.ch	projektalp.ch 120Gb uncompressed data
promise.com	promise.com 1.8Tb uncompressed data
tims.com	tims.com 680Gb uncompressed data
ft.com	ft.com 8.4Tb uncompressed data
ecbawm.com	ecbawm.com 246Gb uncompressed data
comtruck.ca	comtruck.ca 1Tb uncompressed data
idahopacific.com	idahopacific.com 2.2Tb uncompressed data
robertshvac.com	robertshvac.com 240Gb uncompressed data
q-cells.de	q-cells.de 5.4Tb uncompressed data
zoppo.com	zoppo.com 233Gb uncompressed data

Auswirkungen von Datenschutzverletzungen

- 30% erfahren emotionaler Stress
- 25% erhalten keine Unterstützung durch ihre Organisation
- 32% Erfahren es aus den Medien

Quellen: RansomHub, Abyss, Lockbit 3.0

Quelle: Ripple effect: the devastating impact of data breaches | ICO

Wir begegnen diesen Herausforderungen mit...



Noch mehr Abschotten?



+



= besser?

Noch mehr Silo-Sicherheit?

SASE – als konvergente Antwort



Sicherheit

Schutz des gesamten Datenverkehrs

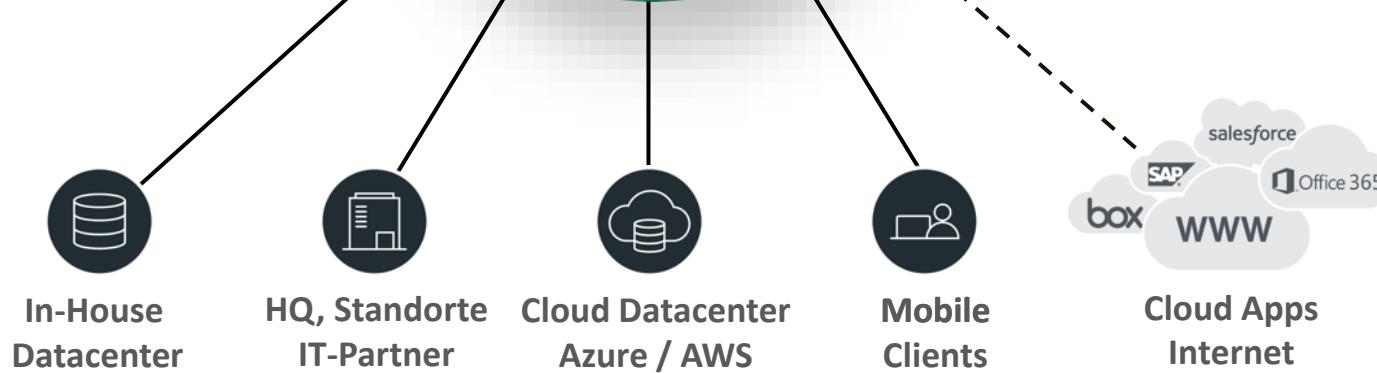


Vernetzung

End-to-End-optimierte
Konnektivität für alle Standorte,
Clouds und Benutzer

Betrieb

Flexibles Management mit
Selbstbedienung, Automatismen,
Eventmonitoring,
Laufenderüberwachung



Agenda



- Cyberrisiken
- **Kundenvortrag**
- Demo
- Zusammenfassung
- Apéro

Kundenvortrag



Aus Vertraulichkeitsgründen wird die Kundenpräsentation nicht veröffentlicht.

Agenda



- Cyberrisiken
- Kundenvortrag
- Demo
- Zusammenfassung
- Apéro

Cato Einblicke



Best Practices

Cato Score 88% Passed: 32 out of 37 Status Passed

Internet Firewall

Name	Description	Status
+ Enable Internet Firewall	The Internet Firewall helps secure your network and lets you set policies to manage Internet access for users and devices	Passed
+ Block Risky Categories	Risky categories include websites related to online activities that may pose security risks to users or networks	Passed
+ Block/Prompt Suspicious Categories	Suspicious categories identifying websites or content that exhibit suspicious behavior or characteristics, potentially indicating a security threat	Passed
+ Block Risky Services	Risky services are network services or protocols that have known vulnerabilities or are commonly targeted by attackers	Passed
+ Block QUIC and GQUIC protocols to enable TLS Inspection	QUIC and GQUIC are transport protocols developed by Google that don't operate over TCP connections, and traffic using these protocols can't be inspected by the TLS Inspection service. Internet Firewall rules that block QUIC and GQUIC force the flow to only connect using protocols that can be inspected by the TLS Inspection service.	Passed

App Analytics

Date: Sep 26, 2024 10:00:00 AM Filter: Upstream: 0 B Downstream: 0 B

Top Users/Hosts

User/Host	Bandwidth
1	49.6 GB
2	37.6 GB
3	18.8 GB
4	18.6 GB
5	17.5 GB

Top Applications

Application	Bandwidth	Percentage
Skype and MS Teams	52.1 GB	35.75%
STUN	30.6 GB	20.97%
Microsoft Autopilot Domain Level	28.7 GB	19.66%
HTTP(S)	21.3 GB	14.63%
Samsung	12.1 GB	8.99%

Top Sites

Experience Monitoring

Sanctioned Application is True Filter

Account Experience

Good Average Experience

29 Sep 30 Sep

Poor Fair Good

Site	Experience
Outlook	Good
Microsoft Autopilot Domain Level	Good
LinkedIn	Good

Application Control

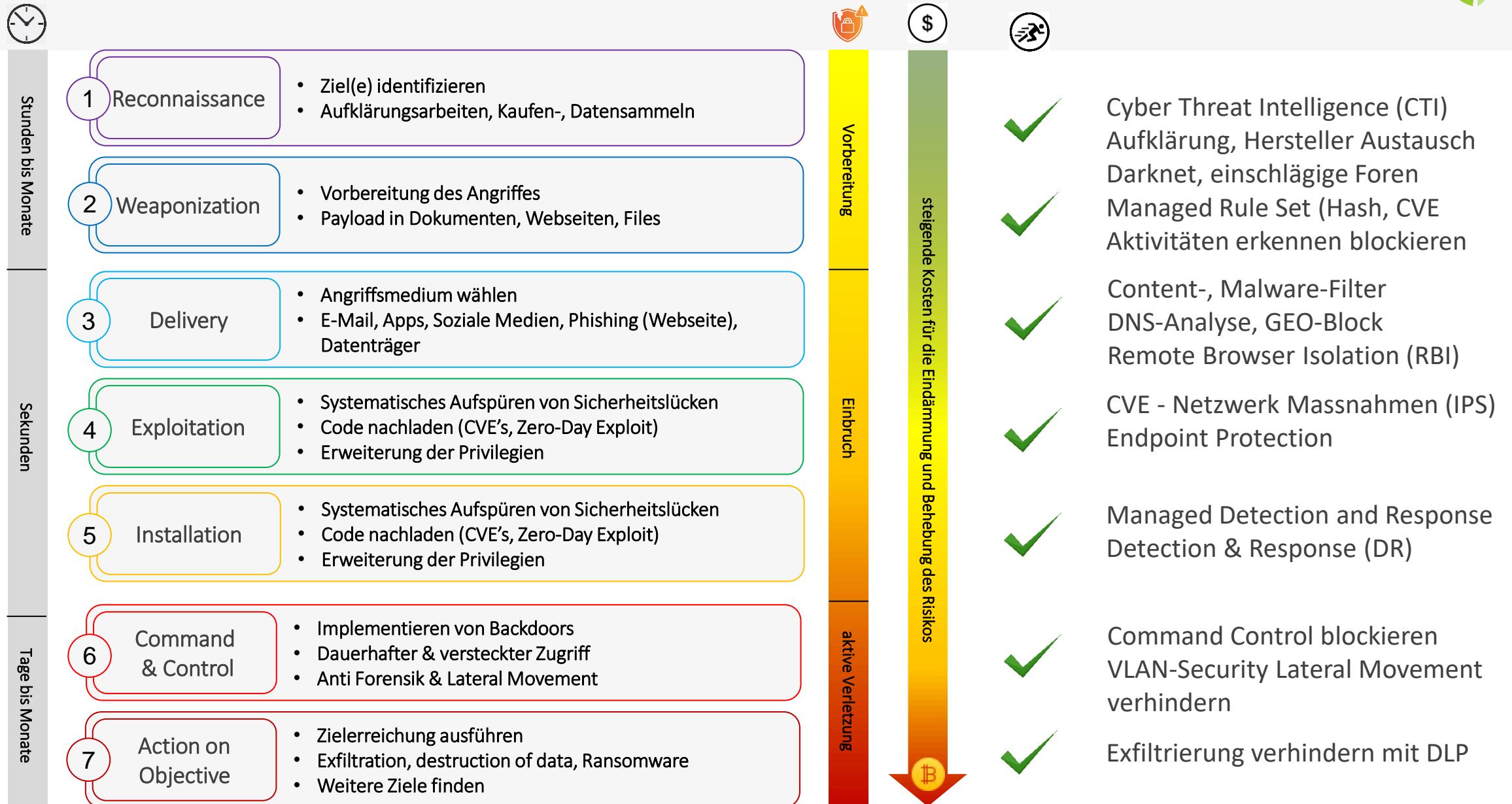
Name	Description	Status
+ Log Any Cloud Application Granular Activities	The Log Any Cloud Granular Activities rule is crucial for surveillance objectives, as it offers comprehensive visibility into the activities of cloud applications within the network.	Passed

Demo



- Dashboard
- Kundenvortrag
- Demo
- **Zusammenfassung**
- Apéro

SASE - Cyberkillchain





Wichtige konvergente Bestandteile sind Vernetzung, Sicherheit und Betrieb.

Vorteile:

- Cato Networks im **Gartner Leader Quadrant**
- Lösung SASE und SSE
- Eine Lösungsplattform für Vernetzung & Sicherheit
- Flexibel, skalierend ausbaubar
- **Hoch-Verfügbarkeit** inklusive
- Einfache und schnelle Erschliessung von Standorten in der Schweiz und / oder weltweit
- **Überall die gleiche Sicherheit**
- Alle Verbindungen werden auf Malware analysiert
- Remote Benutzer inklusive
- Managed Service, immer auf dem neusten Stand
- Keine Ressourcen für Erneuerungen & Wartung



- Fragen
- Frühling 2025 nächstes Security Event
- Aktuelle Schwachstellenausnutzung
 - Known Exploited Vulnerabilities Catalog
 - <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



Besten Dank für Ihre Aufmerksamkeit!