INSEYA

simply secure

Cybersicherheit mit SASE-Technologie

Bern, 6. November 2024
Inseya AG

Ihre Referenten

Kundenvortrag

Inseya

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

Ablauf

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

Top Risiken

Allianz Risk Barometer 2024

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

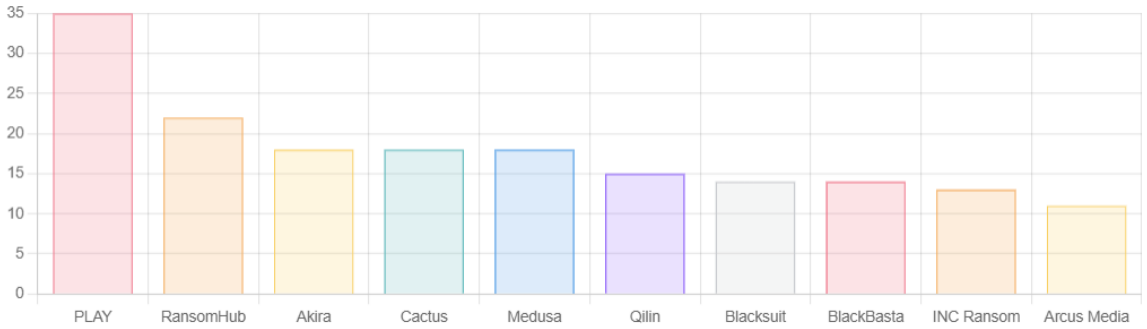
<< Wir sind an einem Punkt angelangt, an dem Cybersicherheit für Unternehmen genauso wichtig ist, wie die traditionellen Risiken >>

Quellen: Allianz Riskbarometer Schweiz, Untersuchung der wichtigsten Unternehmensrisiken 2024, 2800 Experten,
*Nennungen von Risken von Schweizer Unternehmen

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, Eraleignews, INC Ransom, Helldown, Mad Liberator, Cactus

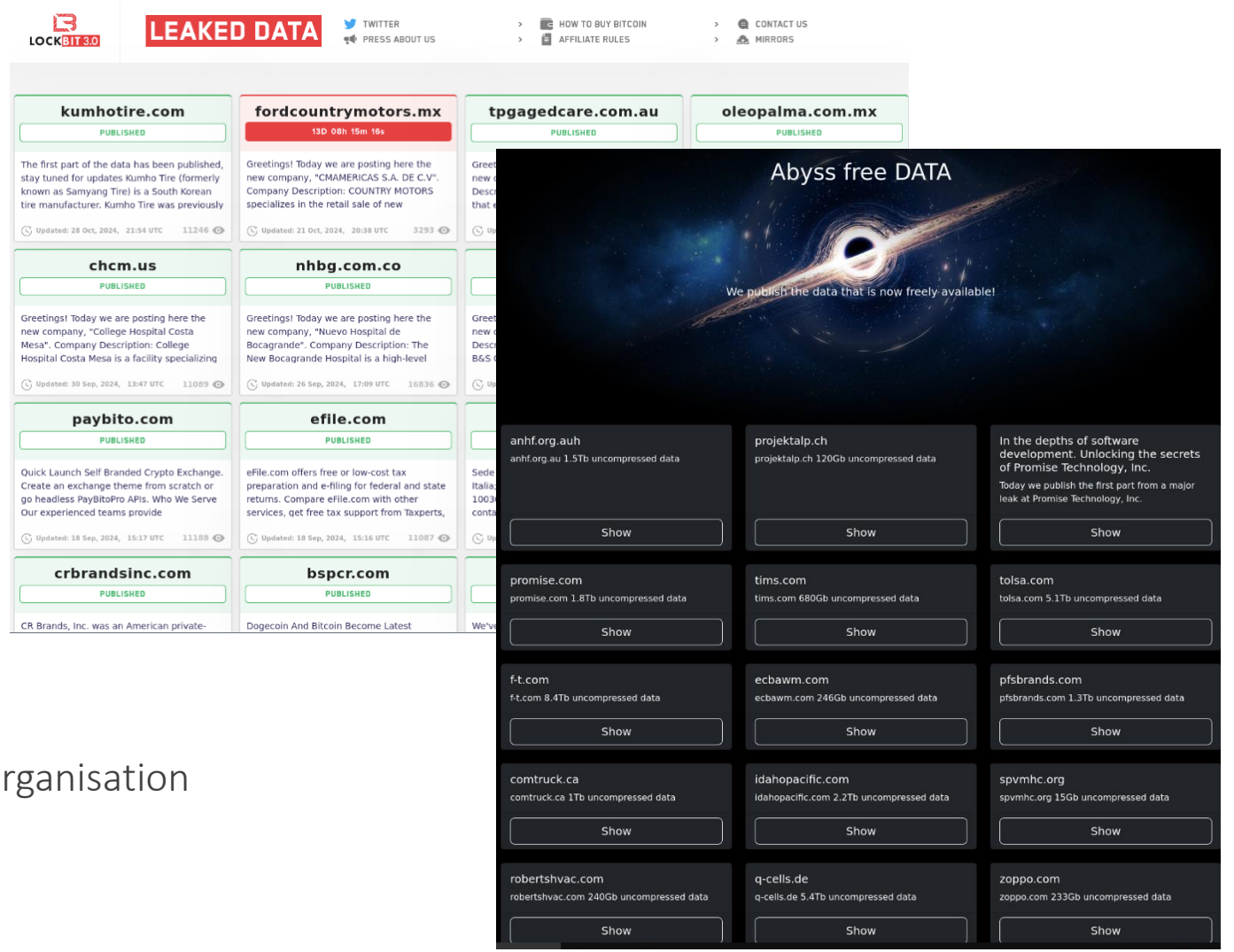
Ransomware ist ein Art Virus, welcher den Zugriff auf die Geschäftsdaten mittels Verschlüsselung verhindert, bis ein Lösegeld bezahlt wurde. Zusätzlich werden die Daten vorgängig gestohlen um bei nicht bezahlen des Lösegeldes diese zu veröffentlichen oder weiterzuverkaufen.

Quellen: darkfeed.io
NAIS: North American Industry Classification https://www.naics.com/search/

Ablauf eines Ransomware-Angriffs

Zielerreichung – entwendete & verschlüsselte Daten

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



Auswirkungen von Datenschutzverletzungen

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

Quellen: RunsomHub, 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?

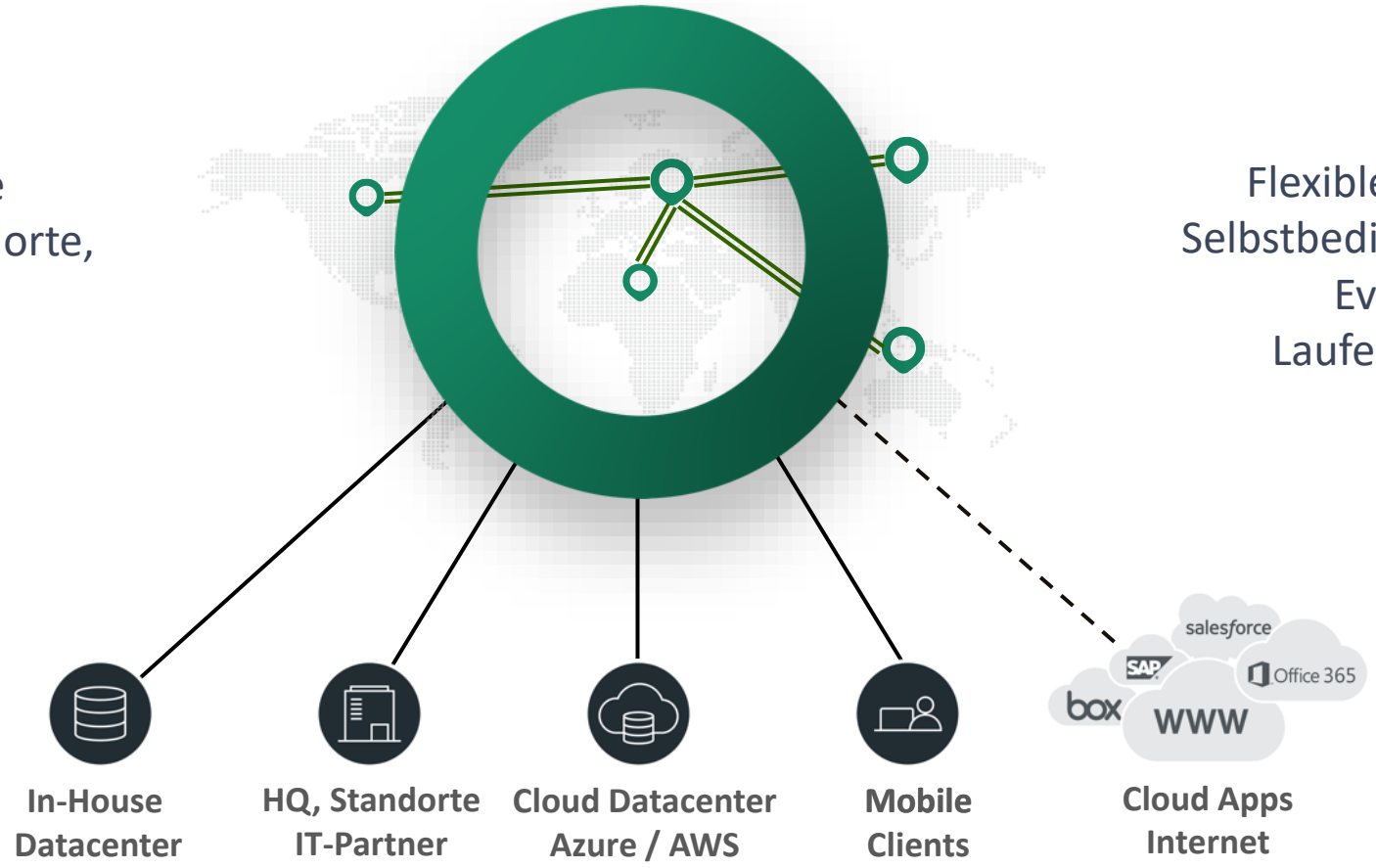
SASE – als konvergente Antwort

Sicherheit

Schutz des gesamten Datenverkehres

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

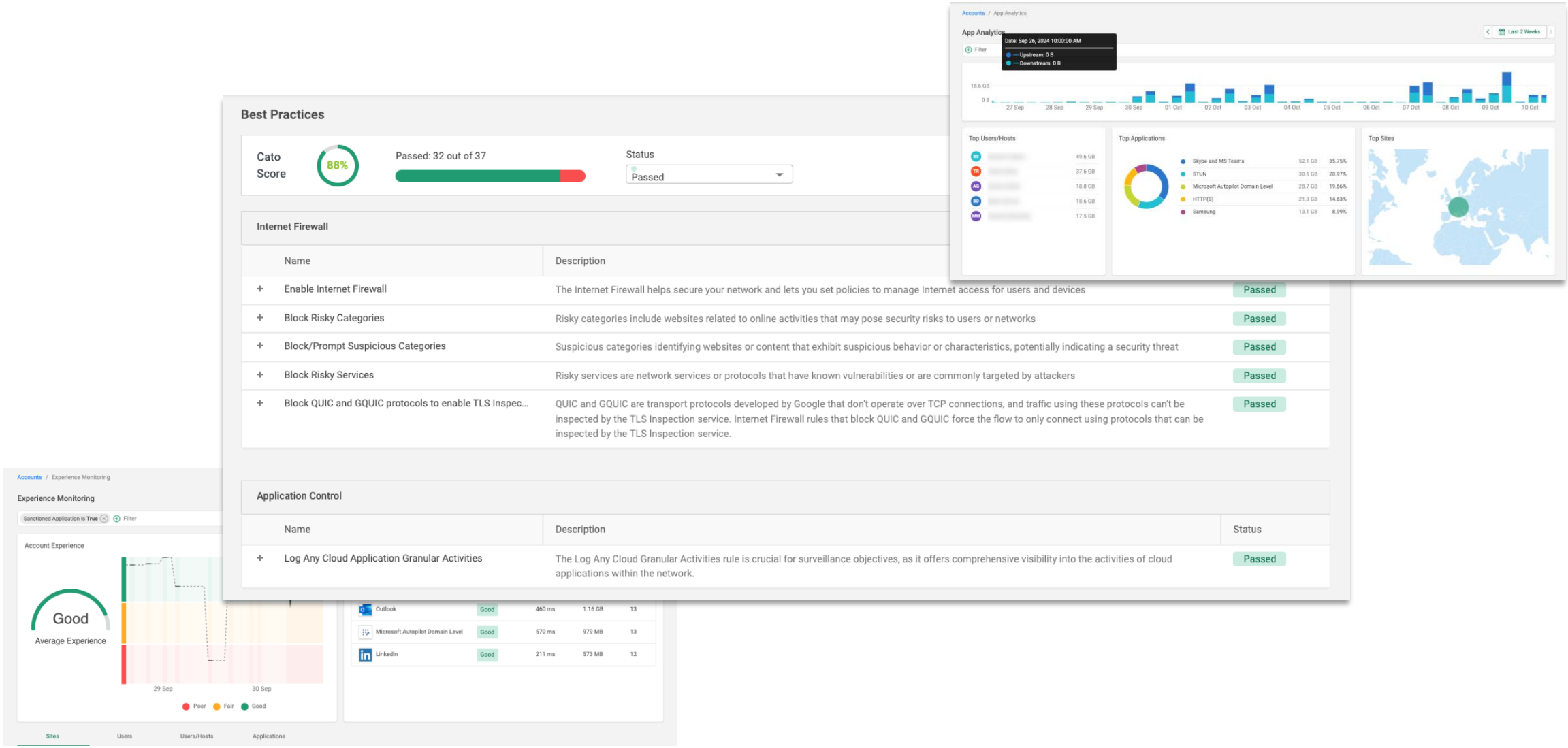
Kundenvortrag

Aus Vertraulichkeitsgründen wird die Kundenpräsentation nicht veröffentlicht.

Agenda

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

Cato Einblicke



Demo

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

SASE - Cyberkillchain

Stunden bis Monate

Sekunden

Tage bis Monate

1	Reconnaissance	• Ziel(e) identifizieren • Aufklärungsarbeiten, Kaufen-, Datensammeln
2	Weaponization	• Vorbereitung des Angriffes • Payload in Dokumenten, Webseiten, Files
3	Delivery	• Angriffsmedium wählen • E-Mail, Apps, Soziale Medien, Phishing (Webseite), Datenträger
4	Exploitation	• Systematisches Aufspüren von Sicherheitslücken • Code nachladen (CVE's, Zero-Day Exploit) • Erweiterung der Privilegien
5	Installation	• Systematisches Aufspüren von Sicherheitslücken • Code nachladen (CVE's, Zero-Day Exploit) • Erweiterung der Privilegien
6	Command & Control	• Implementieren von Backdoors • Dauerhafter & versteckter Zugriff • Anti Forensik & Lateral Movement
7	Action on Objective	• Zielerreichung ausführen • Exfiltration, destruction of data, Ransomware • Weitere Ziele finden

Vorbereitung

Einbruch

aktive Verletzung

steigende Kosten für die Eindämmung und Behebung des Risikos

- ✓ Cyber Threat Intelligence (CTI)
  Aufklärung, Hersteller Austausch
  Darknet, einschlägige Foren
- ✓ Managed Rule Set (Hash, CVE
  Aktivitäten erkennen blockieren
- ✓ Content-, Malware-Filter
  DNS-Analyse, GEO-Block
  Remote Browser Isolation (RBI)
- ✓ CVE - Netzwerk Massnahmen (IPS)
  Endpoint Protection
- ✓ Managed Detection and Response
  Detection & Response (DR)
- ✓ Command Control blockieren
  VLAN-Security Lateral Movement
  verhindern
- ✓ Exfiltrierung verhindern mit DLP

Vorteile

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

Abschluss

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

INSEYA

simply secure

Besten Dank für Ihre Aufmerksamkeit!