T.I.S.P./T.P.S.S.E. Community Meeting 2024

Berlin, 05. – 06.11.2024

Ansätze zeitgemäßer Security Operations

Jürgen Hofmann, Technical Partner Manager
Sascha Dubbel, Sales Engineer

CATO NETWORKS

Problemstellungen in den Security Operations

Personalmangel

“Ich kann meine Stellen nicht besetzen, mein Team ist überlastet”

Fehlendes Fachwissen

“Die Geschäftsführung hat eine Cloud First Strategie vorgegeben, ich habe aber keine Cloud Kompetenz ”

Regulationsdruck

“Welche Controls habe ich um NIS2 zu entsprechen?”

Wettbewerbs- und Kostendruck

“Wir müssen jeden Tag neue Strukturen bauen, digitalisieren und mehr mit weniger erreichen”

CATO NETWORKS

Cybersecurity & Security Operations ist ein Datenproblem

Welche Daten sind überhaupt Relevant?

- Netzwerk
- Endpoint
- Verhaltensanalyse
- Threat Intelligence
- Cloud Audit Logs

Welchen Wert haben verschiedene Datenquellen?

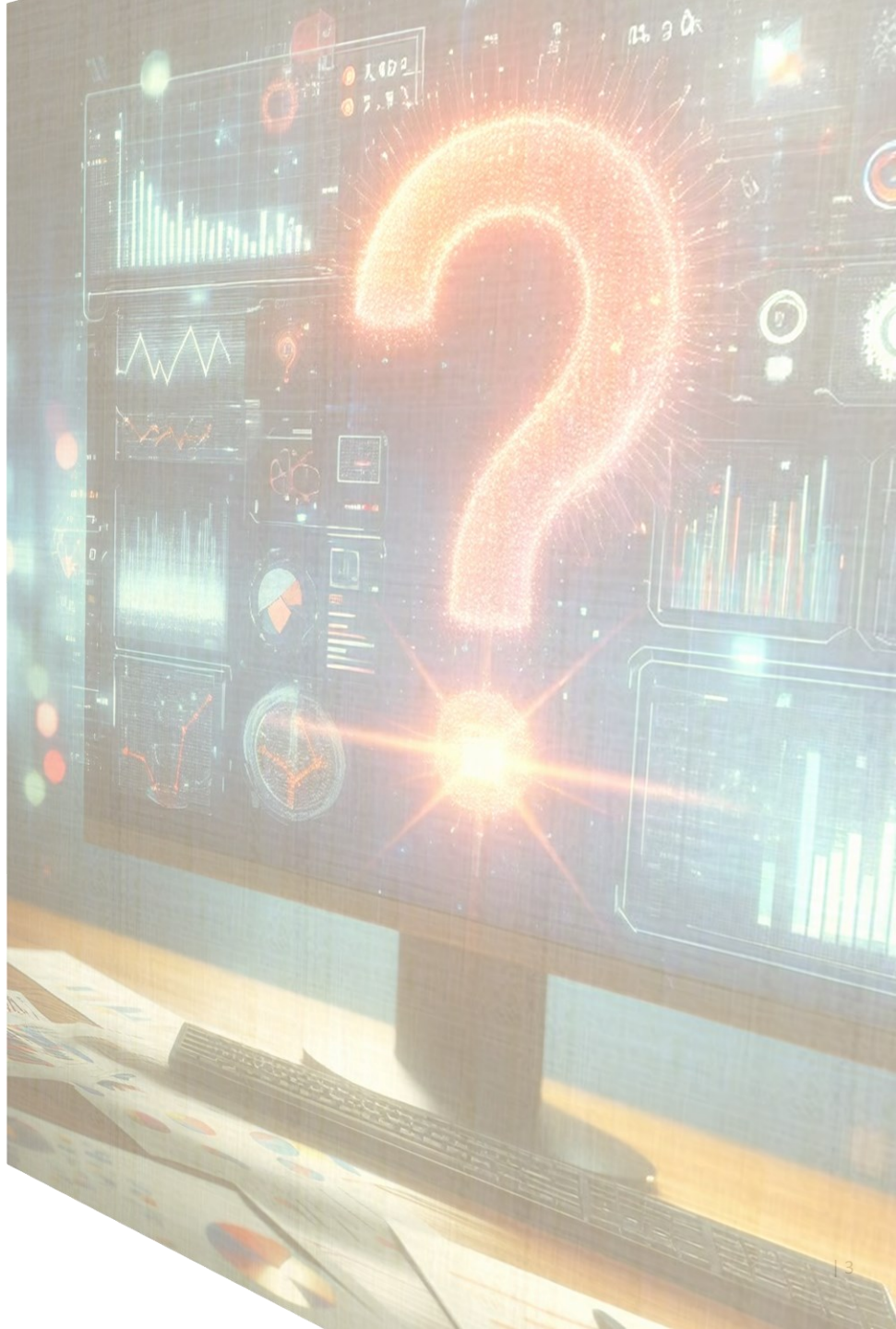
Kann ich die Sichtbarkeit in einzelne Incidents vervollständigen oder erweitern?

Wie lange halte ich die Daten vor?

Wie lang sollte die Aufklärung eines Vorfalles dauern?

An welche Frameworks kann ich mich orientieren?

Welche Kosten sind zu erwarten, was ist Verhältnismäßig?



CATO NETWORKS

SOC / SIEM / MDR / XDR !???

Reifegrade der Security Operations

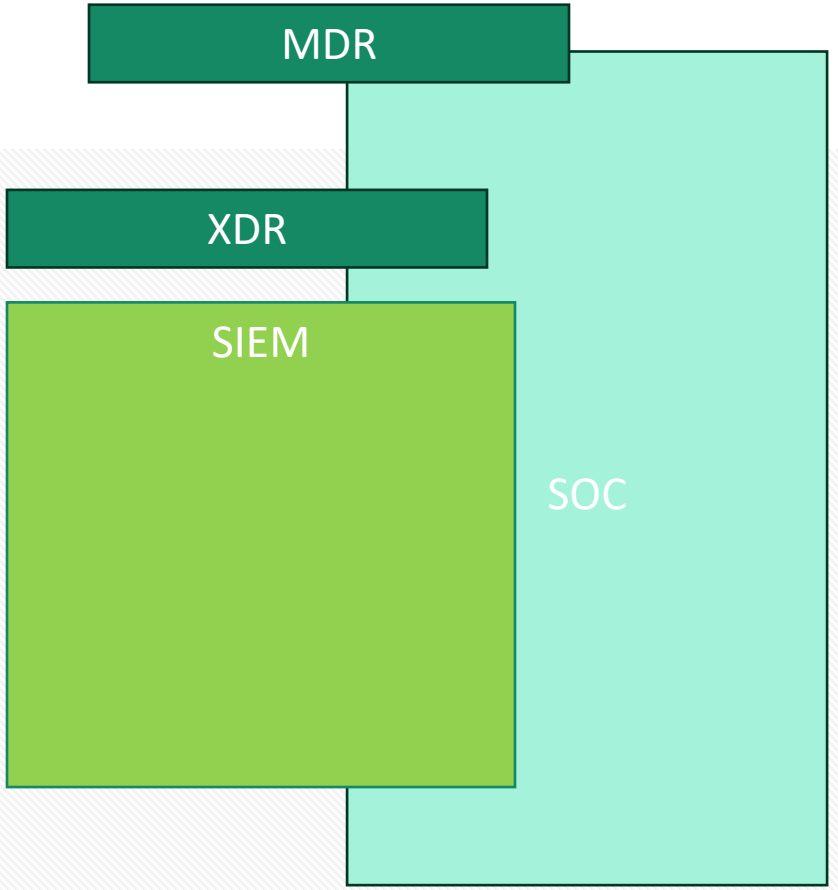
1. Ad-hoc: Sicherheitsmaßnahmen sind unkoordiniert und reaktiv. Es gibt keine definierten Prozesse oder dediziertes Personal.

2. Defined: Sicherheitsrichtlinien und -verfahren sind dokumentiert und das SOC-Personal ist geschult. Es gibt grundlegende Überwachungs- und Incident-Management-Prozesse.

3. Managed: Sicherheitsoperationen sind proaktiv und werden kontinuierlich überwacht und verbessert. Es gibt eine zentrale Koordination und effiziente Verwaltung der Sicherheitsmaßnahmen.

4. Advanced: Das SOC nutzt fortschrittliche Technologien wie Automatisierung und Orchestrierung, um Bedrohungen schneller und effizienter zu erkennen und darauf zu reagieren.

5. Cyber Fusion Center: Dies ist die höchste Reifestufe. Ein Cyber Fusion Center integriert verschiedene Sicherheitsfunktionen wie Bedrohungsanalyse, Incident Response und IT-Operationen in einer zentralen Einheit. Es fördert die Zusammenarbeit und Kommunikation zwischen Teams und nutzt fortschrittliche Tools zur Bedrohungserkennung und -reaktion.



CATO NETWORKS

Trends in Security Automatisierung und KI

1. **Integration von Generativer KI**: Generative KI, wie große Sprachmodelle, wird erforscht, um Sicherheitsoperationen zu unterstützen. Obwohl es einige Skepsis hinsichtlich ihrer unmittelbaren Auswirkungen gibt, sind die langfristigen Aussichten vielversprechend.
2. **KI und Maschinelles Lernen**: Diese Technologien werden genutzt, um sich entwickelnde Angriffsmuster zu erkennen und darauf zu reagieren, wodurch die Gesamtresilienz der Cybersicherheitsabwehr verbessert wird.
3. **Automatisierung in Sicherheitsoperationen**: Automatisierung wird zunehmend in Sicherheitsoperationszentren (SOC) eingesetzt, um sich wiederholende Aufgaben wie Identitäts- und Zugriffsmanagement (IAM) und Incident Response zu bewältigen. Dadurch können sich menschliche Analysten auf komplexere Probleme konzentrieren.
4. **Zero-Trust-Architektur**: Automatisierung spielt eine entscheidende Rolle bei der Implementierung von Zero-Trust-Sicherheitsmodellen, die eine kontinuierliche Überprüfung der Benutzeridentitäten und Zugriffsrechte erfordern.
5. **Compliance und Berichterstattung**: Automatisierte Tools werden verwendet, um Compliance-Prozesse zu optimieren und Berichte zu erstellen, wodurch der manuelle Aufwand reduziert und die rechtzeitige Einhaltung von Vorschriften sichergestellt wird.
6. **Ergebnisorientierte Metriken**: Organisationen übernehmen ergebnisorientierte Metriken, um die Effektivität ihrer Investitionen in die Cybersicherheit besser an nicht-technische Stakeholder zu kommunizieren. Dies hilft, Sicherheitsmaßnahmen mit den Geschäftszielen in Einklang zu bringen.

Praxisbeispiel Machine Learning -Threat Intelligence Sourcing

Homographsquatting

catonetworks.com

(xn--ctonetworks-yij.com in Punycode). Das “a” ist ein Nicht-ASCII Zeichen aus dem Kyrillischen Alphabet.

Typosquatting

catonetwrks.com

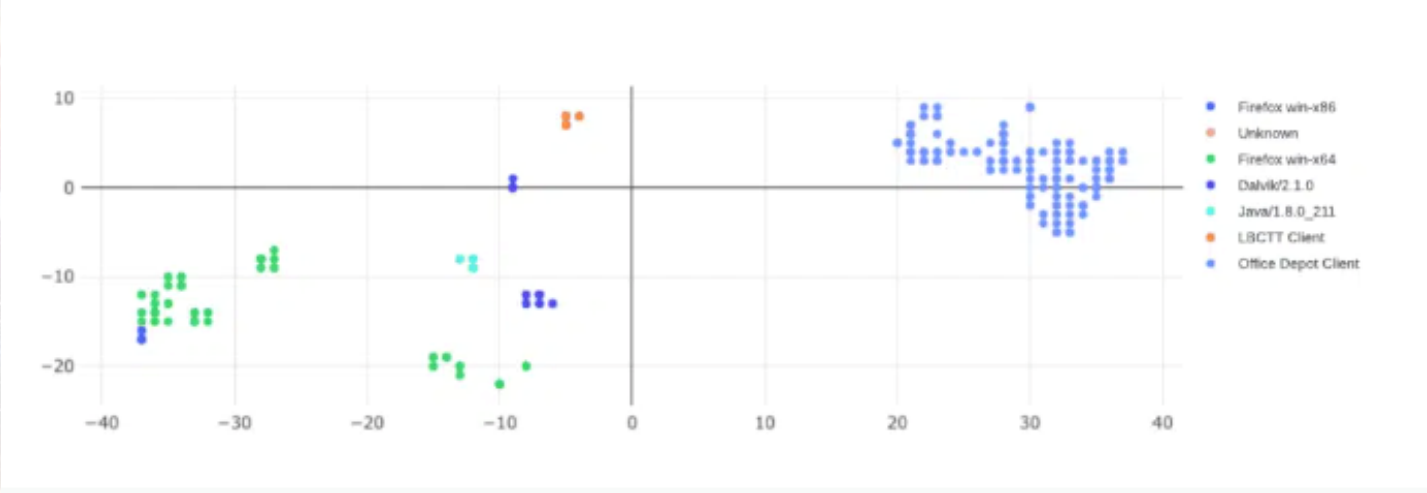
das ‘o‘ fehlt. Typische Tippfehler leiten User auf schädliche Webseiten und verleiten zur Preisgabe von Zugangsdaten oder liefern Malware

CATO NETWORKS

https://www.catonetworks.com/blog/cato-networks-adds-protection-from-the-perils-of-cybersquatting/

Vom Fingerprinting zum Clustering

“In den letzten Jahren sind Fingerabdrücke, die ausschließlich auf ungesicherten Netzwerkverkehrsmerkmalen basieren (z. B. dem HTTP-User-Agent Header), obsolet geworden, da sie leicht zu fälschen sind und bei gesicherten Verbindungen nicht anwendbar sind. TLS-Fingerabdrücke, die auf Merkmalen der Client-Hello-Nachricht des TLS-Handshakes basieren, leiden hingegen nicht unter diesen Nachteilen und werden von Sicherheitsanbietern zunehmend adaptiert.” Das Fingerprinting erfordert ein hohes Maß an manueller Analyse.




```
{
record_tls_version: 0x0301,
tls_version: 0x0301,
ciphersuite_length: 0x001C,
ciphersuite: 0xC00A 0xC009 0xC014 0xC013 0x0039
0x0033 0x0035 0x002F 0x000A 0x0038 0x0032 0x0013
0x0005 0x0004,
compression_length: 1,
compression: 0x00,
extensions: 0x0000 0x000A 0x000B 0x0023 0x0017
0xFF01,
e_curves: 0x0017 0x0018,
ec_point_fmt: 0x00
}
```

Clustering bietet einen automatisierbaren und zuverlässigen Ansatz, um mit der Basis aus Fingerprinting in Kombination mit einem Datalake aus Flowdaten eine verlässliche Client Identifikation zu ermöglichen

https://www.catonetworks.com/blog/inside-cato-how-a-data-driven-approach-improves-client-identification-in-enterprise-networks/

DGA?

Angreiferstrukturen verstehen und Domain Generation Algorithmen erkennen

- Erkennen von Mustern oft schwierig und manueller Aufwand

cajato..

- Analyse Erfordert eine große Informationsbasis, die idealerweise organisationsübergreifend ist

- Controls müssen die Erkenntnisse zeitnah wirksam umsetzen
  - Angriffswellen teilweise nur für wenige Stunden aktiv

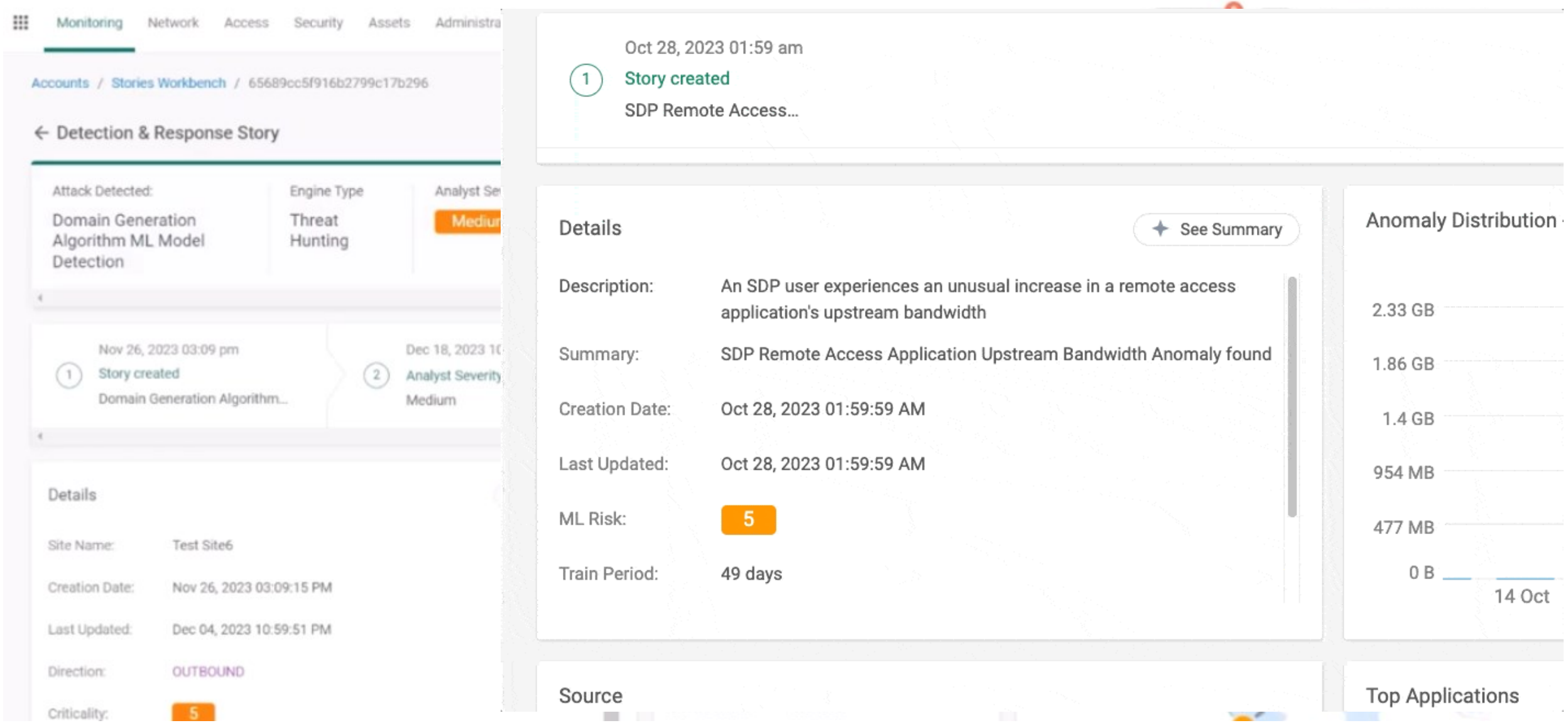
IOC

```
bacugo[.]com
bagoj[.]com
baguhoh[.]com
bosojojo[.]com
bowocofa[.]com
buduguh[.]com
bujot[.]com
bunafo[.]com
bunupoj[.]com
cagodobo[.]com
cajato[.]com
copamu[.]com
cusupuh[.]com
dafucah[.]com
dagaju[.]com
dapowar[.]com
dubahu[.]com
```

https://www.catonetworks.com/blog//?utm_source=blog&utm_medium=botthe-dga-algorithm-used-by-dealply-and-bujotom_cta&utm_campaign=dga_algorithm

CATO NETWORKS

Gen AI statt Notepad++



https://www.catonetworks.com/blog/cato-xdr-storyteller-integrating-generative-ai-with-xdr-to-explain-complex-security-incidents/

Fazit

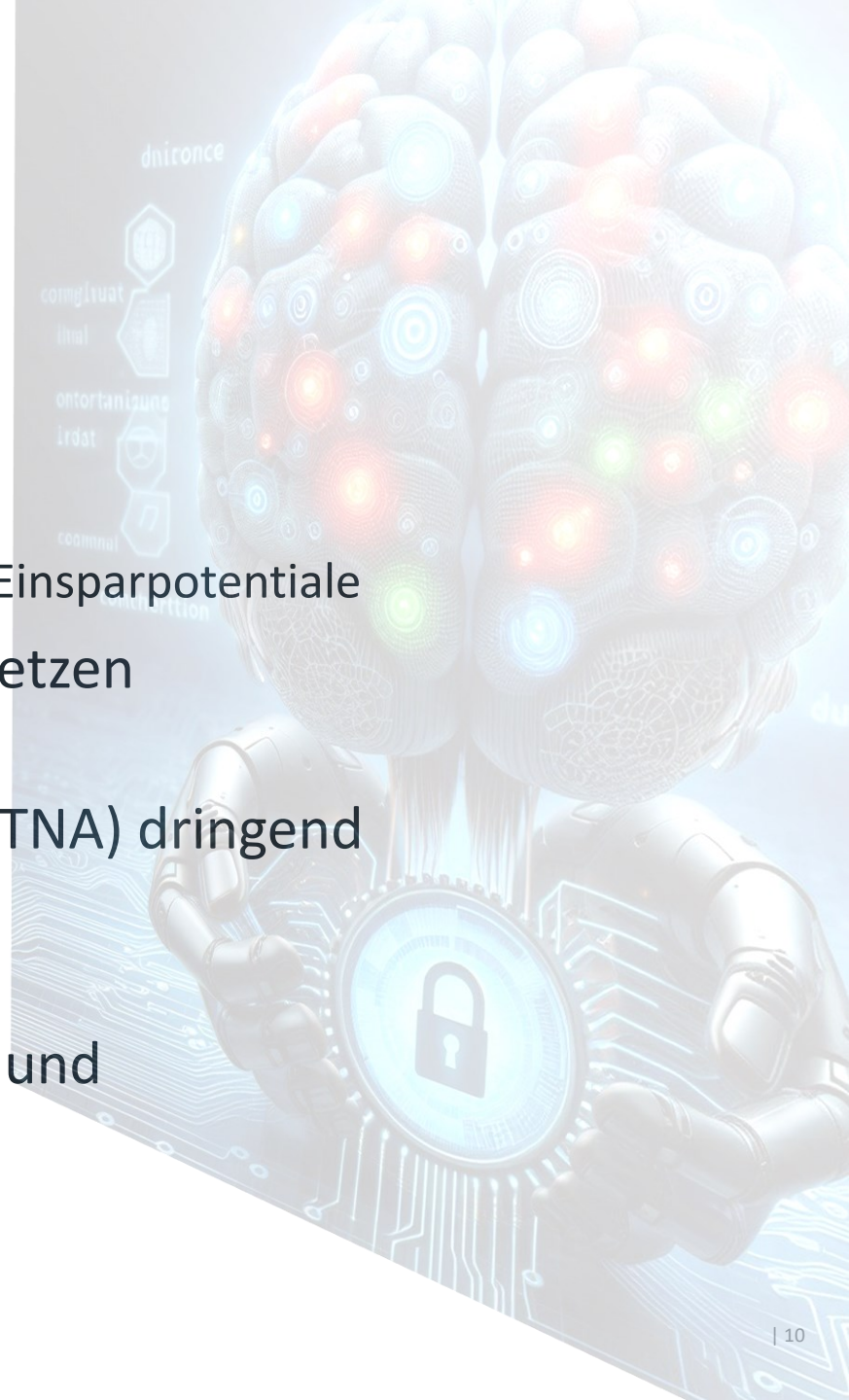
- Unternehmen leiden unter Fachkräftemangel

  -> Automatisierung hilft „Mehr mit Weniger“ zu leisten

  -> „as-a-Service“ reduziert Arbeitslast
- Datenquellen müssen sinnvoll korreliert werden

  ->XDR bietet vielen Unternehmen Konsolidierungsmöglichkeiten & Einsparpotentiale
- Anomalieerkennung und Machine Learning ergänzen und ersetzen regelwerkbasierte SOC/SIEM Usecases
- Segmentierung auf User/Device/Status/Applikationsebene (ZTNA) dringend empfehlenswert

  -> Eindämmung, Umsetzung Least-Privilege-Prinzip
- Generative AI ermöglicht Verbesserung der Informationslage und Automatisierung von Abwehrmaßnahmen
- Orientierung am Stand der Technik in der IT-Sicherheit



CATO NETWORKS

Secure Access Service Edge

Secure.

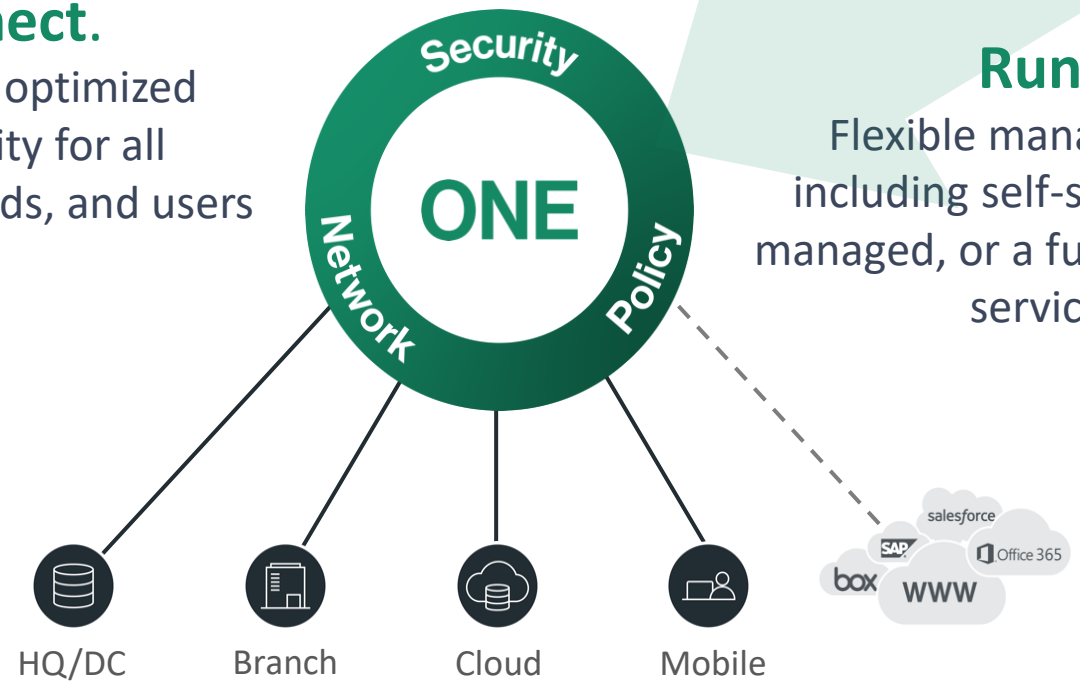
Protect all traffic with built-in security as a service

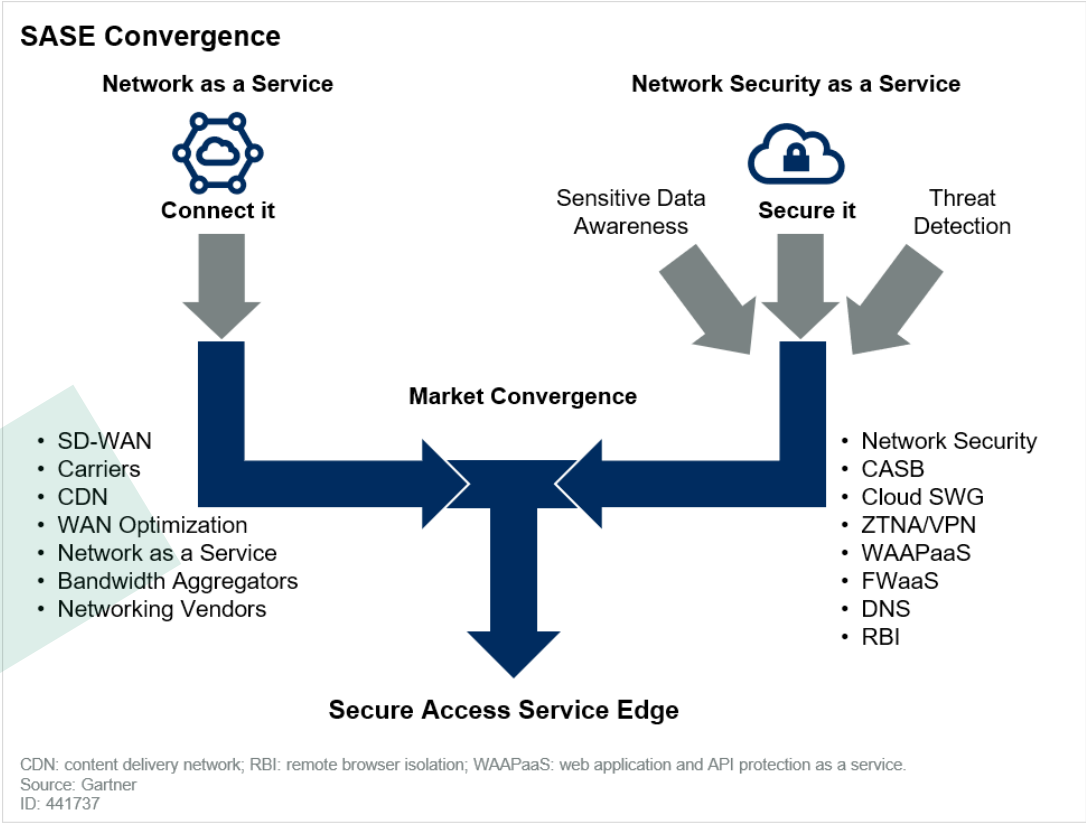
Connect.

End-to-end optimized connectivity for all locations, clouds, and users

Run.

Flexible management including self-service, co-managed, or a fully managed service





Fragen und Diskussion