
Dräger

Cybercrime gegen Healthcare – eine neue Pandemie?

Jeff Moore, September 2021, Cham, Schweiz

Jeff Moore

Chief Product Security Officer

Er ist derzeit CPSO in der Medizintechnik der Drägerwerk AG & Co. KGaA und ein anerkannter Experte im Bereich Cybersicherheit mit mehr als 20 Jahren Erfahrung in Management und Technik.

Verantwortlich für die Entwicklung von Strategien zur Risikominderung und Compliance durch die Verbesserung von IT-Sicherheitsrichtlinien und -verfahren, Security-Operations und technischen Kompetenzen.

Jeff war zuletzt Global Head of Cybersecurity bei einem globalen Pharma- und Life-Science Unternehmen. Zuvor hatte Positionen bei Adidas AG, Bindview und Peregrine Systems inne, nachdem er seine Sicherheitskarriere bei der Europäischen Raumfahrtbehörde (ESOC) begonnen hatte.

eMail: jeff.moore@draeger.com

CISO vs. CPSO

Chief Information Security Officer (CISO)

Verantwortlichkeiten

Globale Verantwortung für die IT-Security **der Organisation**.

Field of View

Der CISO muss folgendes berücksichtigen:

- Gesamte Organisation
- Umfeld der Organisation (z. B. Netzwerk)
- Von der Organisation verwendete Technologien
- Zusammenarbeit mit Behörden (wo möglich bzw. notwendig) als Beauftragter der Organisation
- Von der Organisation gespeicherte/verwendete Informationen
- Überwachung auf gezielte, bösartige Aktivitäten

Chief Product Security Officer (CPSO)

Verantwortlichkeiten

Die Security **aller Produkte**, die das Unternehmen herstellt, während der **gesamten Lebensdauer** des Produkts.

Field of View

Der CPSO muss folgendes berücksichtigen:

- Gesamtes Produktportfolio
- Kundenumfeld: welche Produkte werden eingesetzt/verwendet
- Technologien des Produktportfolios, und mögliche Auswirkungen des Portfolios der Wettbewerber.
- Zusammenarbeit mit Behörden (wo möglich bzw. notwendig) als Beauftragter der Organisation
- Von den Produkten gespeicherte/verwendete Informationen
- Überwachung auf gefälschte oder böswillige, gezielte Aktivitäten

BIOLOGICAL PANDEMIC

INFECTION RATE

Virus infection rate (R_0) (source: WHO)
The average number of people that one person with a virus infects:

Flu: 1.3, SARS: 2-4, **Corona: 2.5**,
Ebola: 1.6-2, Zika: 2-6.6, Measles: 11-18

INFECTION PREVENTION

Best treatment: **Vaccination**
Dealing with Infection Best Practices:

1) Quarantine, Shelter-in-Place
2) Isolation
3) Contact Tracing

SAFETY BEST PRACTICES

Common treatment (until vaccination):

1) Mask
2) Hygiene
3) Social Distancing

CYBER PANDEMIC

INFECTION RATE

Malware infection rate (R_0) The average number of hosts that one host with a malware infects:

Cyber attack: >27 (source: WEF, NSTU)
Slammer: Doubled in size every 8.5 seconds
Code Red: 2,000 new hosts per minute

INFECTION PREVENTION

Best treatment: **Real Time Prevention**
Best Practices: **Continuous** process of:

1) **Quarantine:** Sandboxing, Micro-Segmentation
2) **Isolation:** Zero Trust, Segregation
3) **Tracing:** Threat Intelligence, AI, SOC, Posture Management

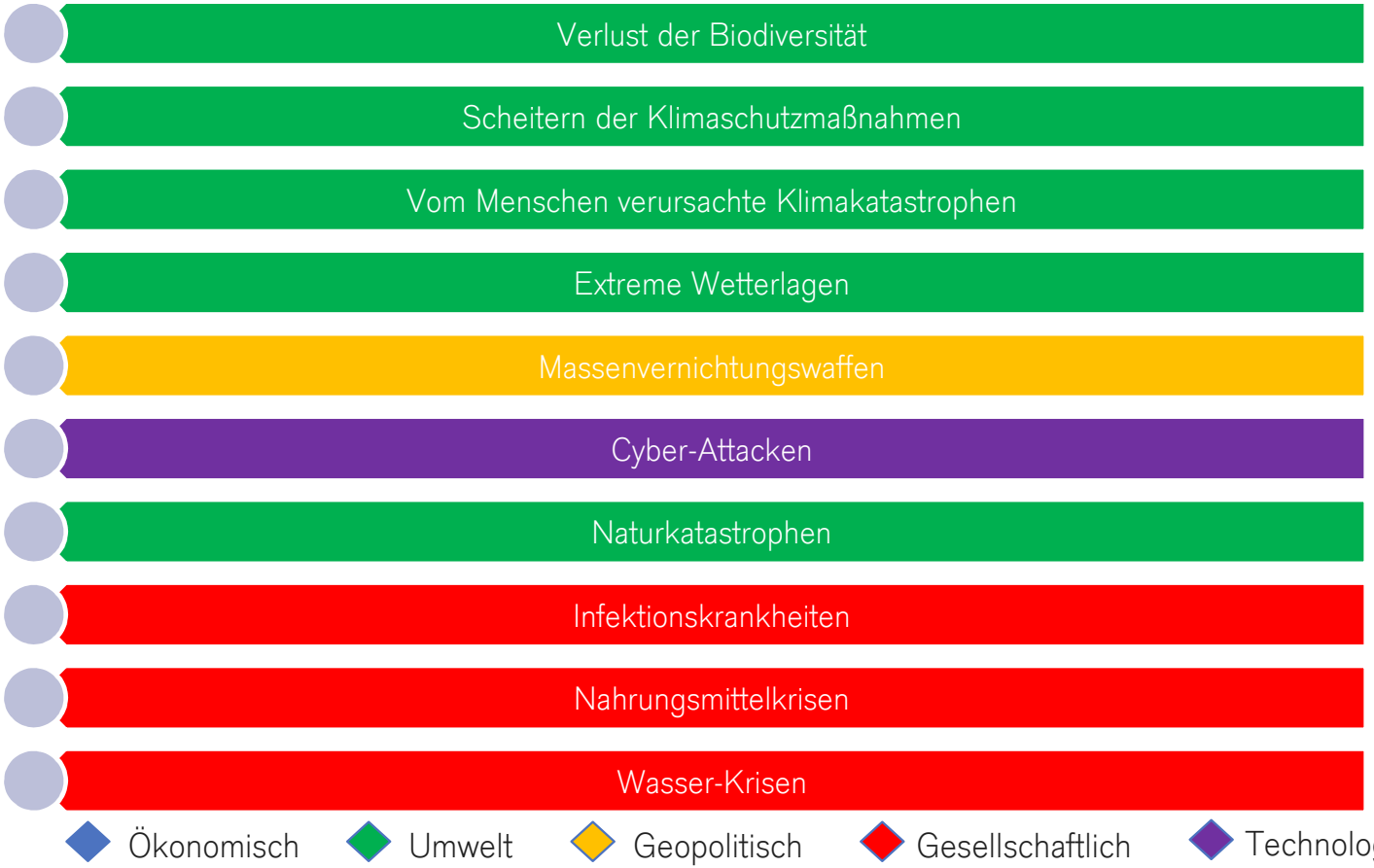
SAFETY BEST PRACTICES

1) **Awareness:** Think before you click...
2) **Cyber Hygiene:** Patches, Compliance...
3) **Asset Distancing:** Network Segmentation, Multi-Factor Authentication...

SOURCE: CHECK POINT SOFTWARE 2020

Footnote: Please insert appropriate company

WORLD ECONOMIC FORUM
Top 10 Risiken über die nächsten 10 Jahre



Some sad information

Der Fortinet FortiGuard Labs 1H 2021 Global Threat Landscape Report konzentriert sich auf die Ransomware-Landschaft:

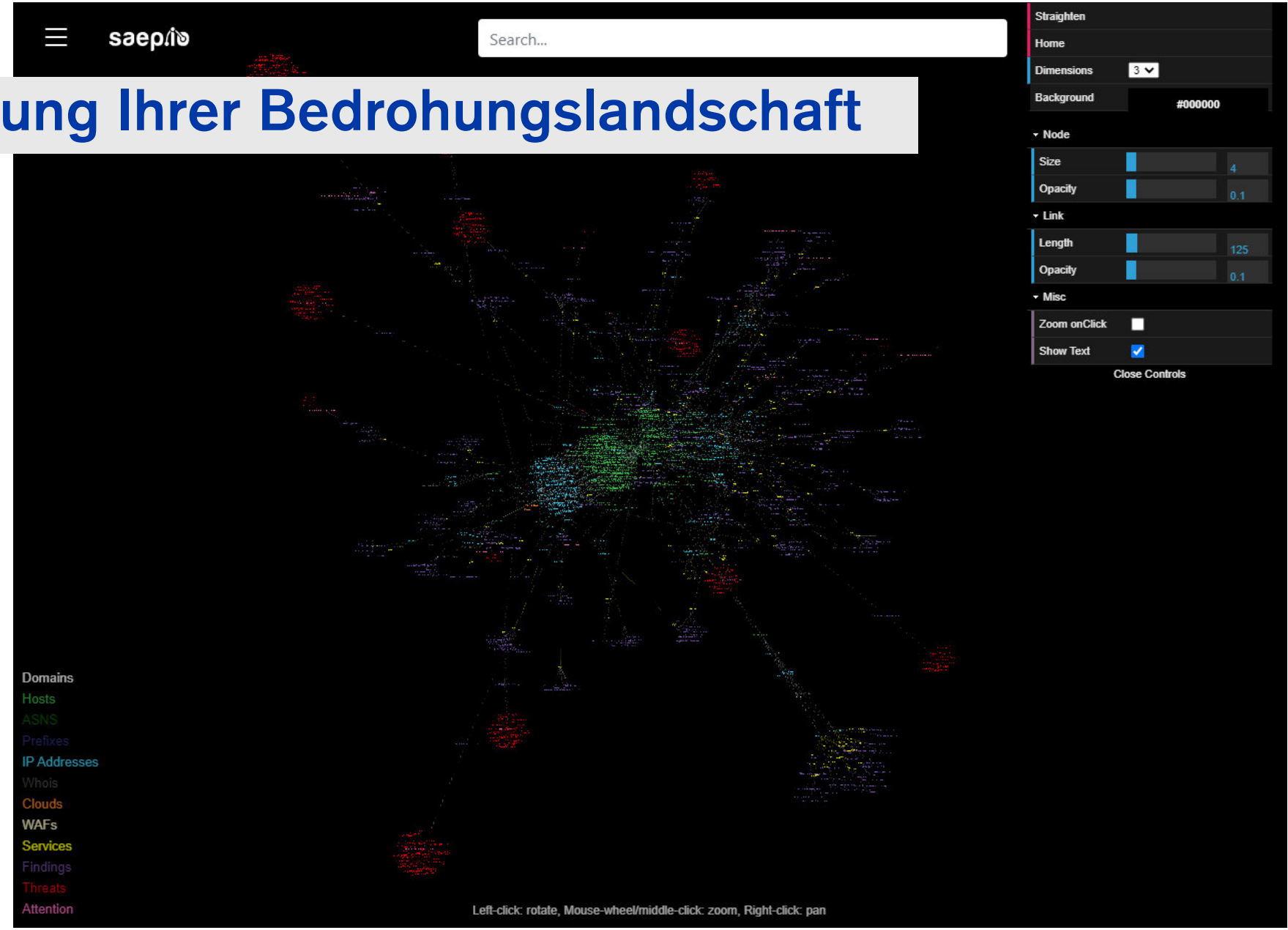
- **Durchschnittliche Anzahl wöchentlich entdeckter Ransomware-Angriffe im Juni 2021:**
  → Mehr als 149.000
  → Zwölf Monaten zuvor: 14.000 - Anstieg 966% (WOW)

- **Betroffen von der ein oder anderen Form eines Ransomware-Angriffs:**
  → Mehr als ein Drittel der Unternehmen der Automobil-, MSSP-, Regierungs- und Telekommunikationsbranche
  → Ein Viertel aller anderen Branchen

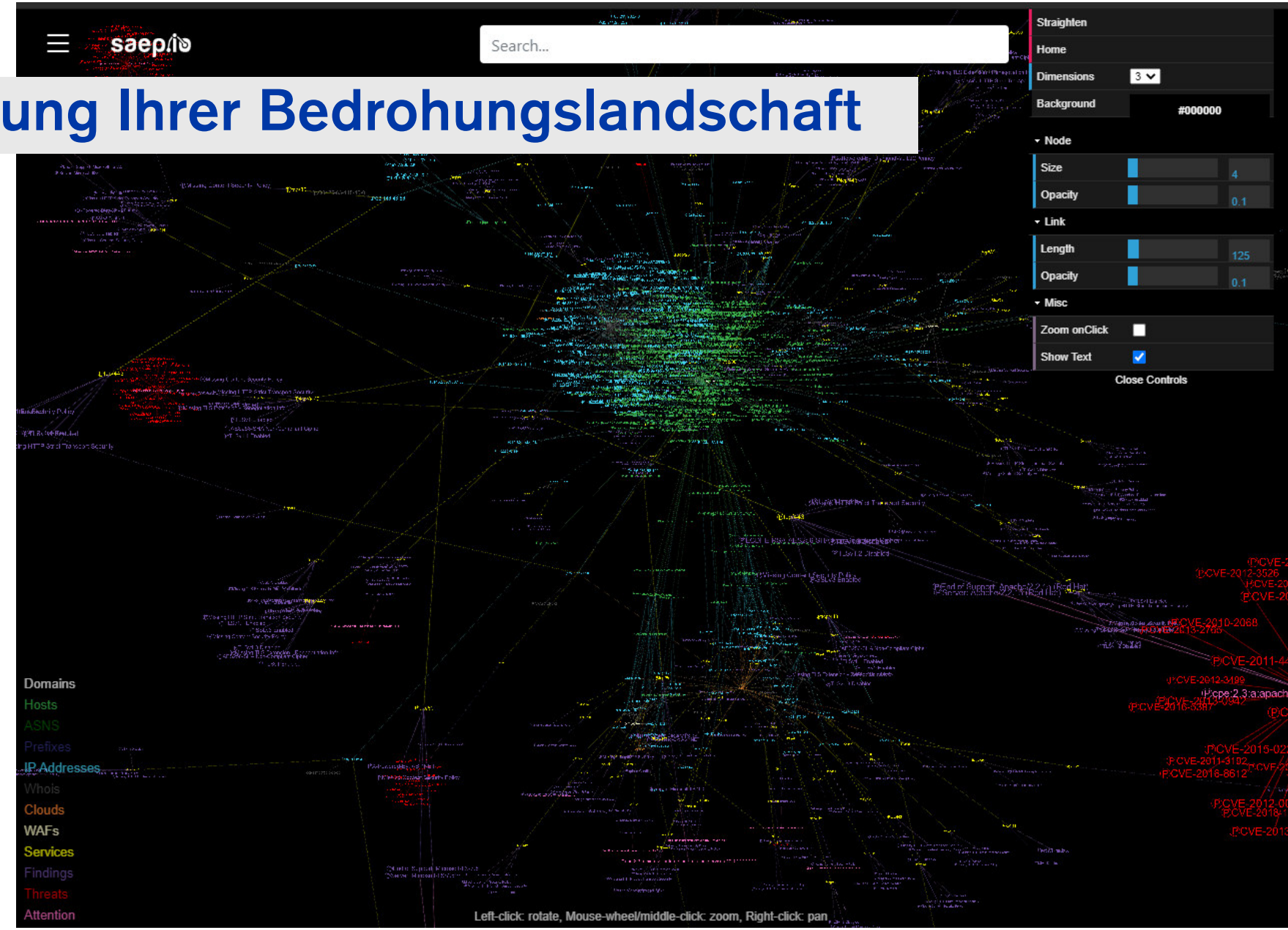
- **Vom Forbes Magazine berichteter Anstieg der Angriffe auf das Gesundheitswesen:**
  → 42%

- **Meine persönlich Zählung von Ransomware-Angriffen auf bzw. Security-Incidents in Krankenhäusern in den letzten 12 Monaten:**
  → **486 Krankenhäuser**

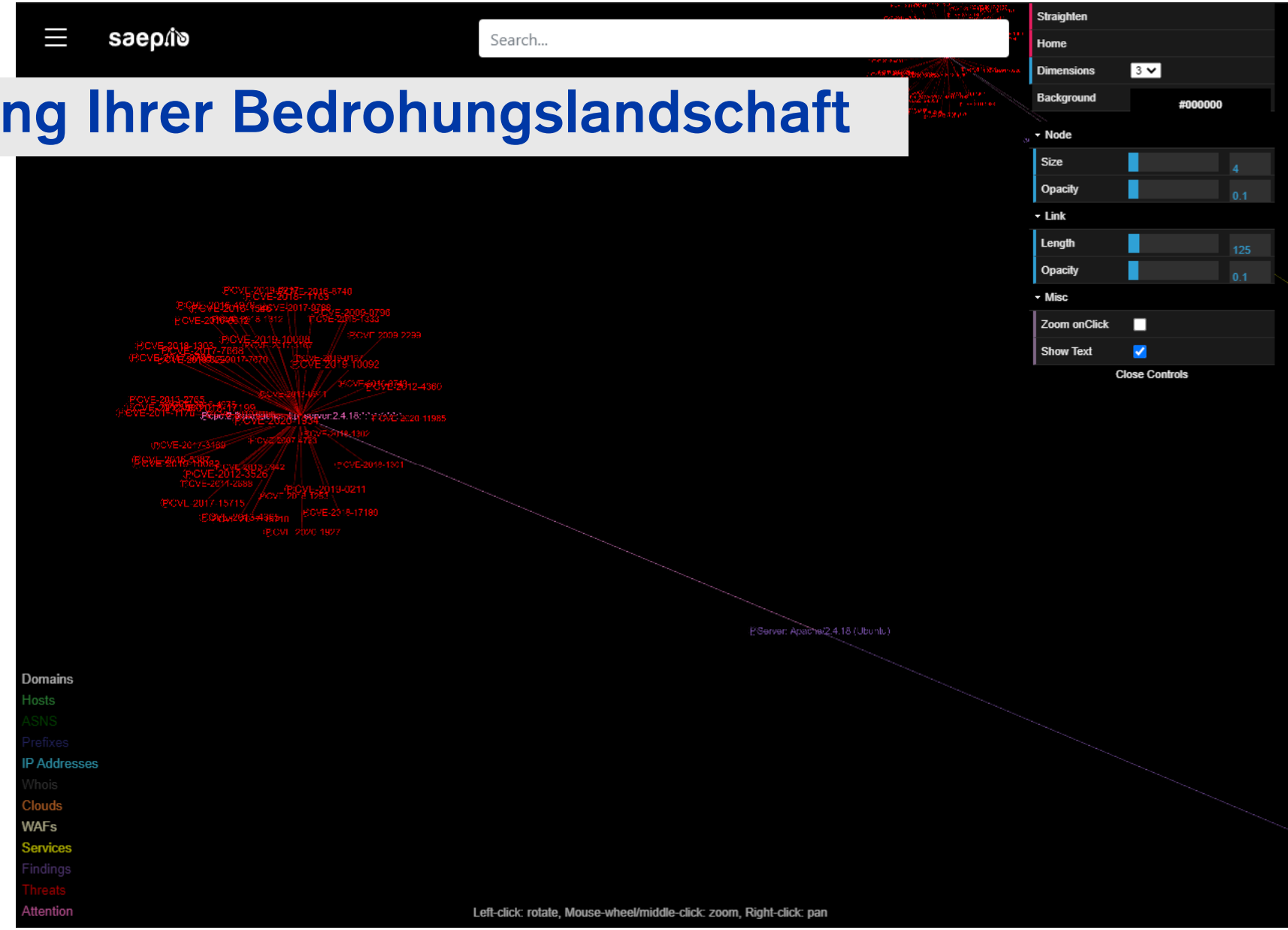
Visualisierung Ihrer Bedrohungslandschaft



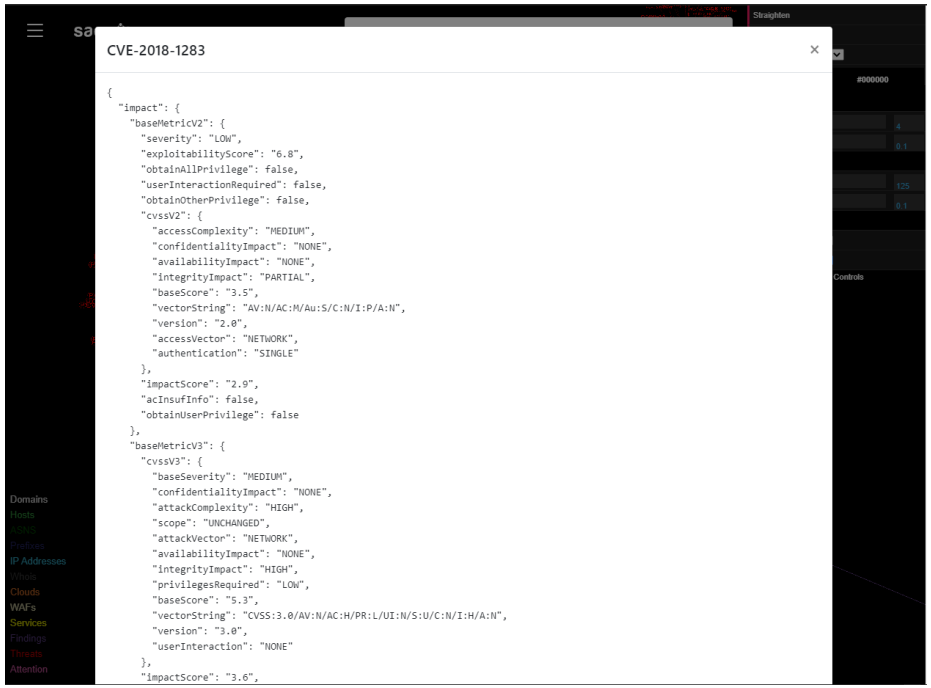
Visualisierung Ihrer Bedrohungslandschaft



Visualisierung Ihrer Bedrohungslandschaft



Verwertbare Informationen



saepio

Findings

Copy CSV Print JSON

Show 100 entries Search:

IP	Hostname	Transport	Port	Compliance	Description
1.1.1.1		tcp	80	OWASP Top Ten 2017	Missing Content Security Policy
104.102.192.127		tcp	443	OWASP Top Ten 2017	Missing Content Security Policy
104.102.192.127		tcp	443	NIST SP 800-52r2 NIST SP 800-53r5	TLSv1.1 Enabled
104.102.192.127		tcp	443	OWASP Top Ten 2017	Missing HTTP Strict Transport Security
104.102.192.127		tcp	80	OWASP Top Ten 2017	Missing Content Security Policy
104.102.196.237		tcp	443	OWASP Top Ten 2017	Missing Content Security Policy
104.102.196.237		tcp	443	NIST SP 800-52r2 NIST SP 800-53r5	TLSv1.1 Enabled
104.102.196.237		tcp	443	OWASP Top Ten 2017	Missing HTTP Strict Transport Security
104.102.196.237		tcp	80	OWASP Top Ten 2017	Missing Content Security Policy
104.102.209.116		tcp	443	OWASP Top Ten 2017	Missing HTTP Strict Transport Security
104.102.209.116		tcp	80	OWASP Top Ten 2017	Missing Content Security Policy
104.102.209.116		tcp	443	OWASP Top Ten 2017	Missing Content Security Policy
104.107.23.92		tcp	443	OWASP Top Ten 2017	Missing HTTP Strict Transport Security
104.107.23.92		tcp	80	OWASP Top Ten 2017	Missing Content Security Policy
104.107.23.92		tcp	443	OWASP Top Ten 2017	Missing Content Security Policy

Die Mäuse werden immer schlauer...

Kriminelle Organisationen wachsen exponentiell und..

- verfügen über bessere Tools zur **Zusammenarbeit**
- entwickeln neue **Geschäftsmodelle**
- führen **gezielte Angriffe** auf unsere Lieferketten und **kritische Infrastruktur** durch
- jüngstes Beispiel: Colonial Gas

Die Zahl der kriminellen Organisationen und Websites wächst, und damit der...

- **Verkauf** von IP, Schwachstellen und Tools zur Zerstörung und Ausnutzung von Schwachstellen
- im open, deep und **dark Web**

Unternehmen sind sich des Wertes und der Risiken bewusst ...

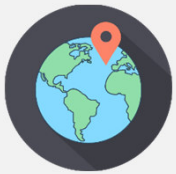
- in Bezug auf Marke, **Vermögenswerte**, Führungskräfte, Mitarbeiter und Kunden, aber...
- **es fehlt an Einblick** in Ursprünge dieser Bedrohungen, und...
- **Ressourcen** und kontextbezogene **Informationen**, um...
- **zu erkennen**, welche Bedrohungen auf die Netzwerke, Produkte, die Lieferketten und die Mitarbeiter ihres Unternehmens abzielen.

Conclusion

- Threat Intelligence spielt eine wichtige Rolle bei der Security.
- sowohl für diejenigen, die das Unternehmen schützen, als auch für diejenigen, die die Produkte sichern.

Was ist Threat Intelligence?

Auswirkungen auf die Produkt-Security



The “Real” World

Beliebtes Ziel: "Internet der Dinge"-Geräte (IoT)

- kriminelle Malware-Aktivitäten, insbesondere für Botnetze
- die Kriminelle für DDoS- oder Brute-Force-Angriffe oder andere bösartige Zwecke nutzen.

Diese Geräte erhalten häufig

- nicht den gleichen Security-Support wie Desktops, Laptops oder Mobiltelefone
- was sie für kriminelle Botnetz-Betreiber zu einem leichteren und damit begehrteren Ziel macht.

The “Regulated” World

Medizintechnikbranche

- vernetzt ihre Geräten zunehmend
- nutzen die Vorteile künstlicher Intelligenz (KI) und anderer verfügbarer Technologien.

Regulierungsbehörden

- müssen die Interoperabilität noch in vollem Umfang erkennen

GxP-Praktiken

- beginnen, das Konzept der dynamisch vernetzten Medizinprodukte zu berücksichtigen.

Threat Intelligence: 3-Minuten-Fibel

Daten und Informationen

- sammeln, analysieren und bewerten

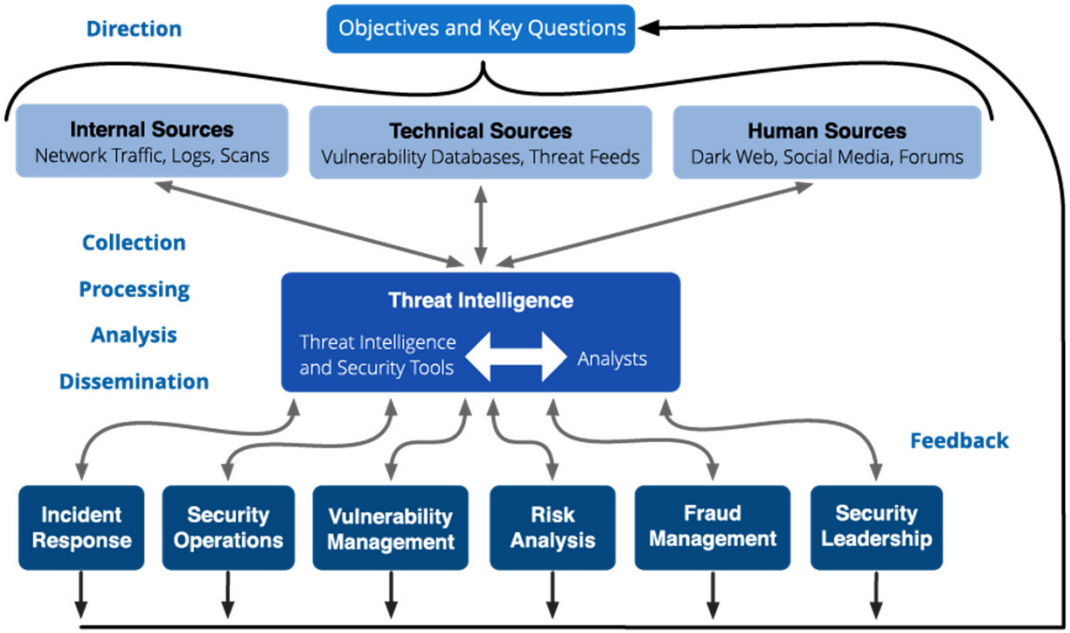
um die **Bedrohungen zu verstehen,** die auf das Unternehmen zielen: gestern, heute und morgen.

Diese Informationen dienen der

- Vorbereitung auf
- Prävention für
- Identifizierung von Bedrohungen

die **wertvolle Ressourcen als Ziel** haben, z. B:

Brand	Services	Products	Supply Chain
Assets	Customers	Executives	Employees



Bedrohungsdaten für die Produkt-Security

	Primary benefit	Operational KPIs	Business KPIs
SecOps efficiency gains	Improved speed, scope, & productivity of SecOps & analysts	↑% Events investigated ↑% Relevant events reviewed Mean-time-to-detect (MTTD)	↑# Current FTE hrs recovered ↑# New/future FTE hrs averted
Risk reduction	Lower probability of successful cyber events	↓# Triggered security incidents ↓# Audit findings and reviews ↓# Account resets or escalations	↓# Cyber-related loss events ↓$ Fines & penalties (number & size) ↓$ Incident response costs
Minimized impact exposure	Reduction in the consequences & costs of successful cyber events	MTTR Internal (proxies, gateways, firewalls, etc.) MTTR External (takedowns, data recovery) ↓% Account resets (size & scope)	↓$ Losses due to cyber events ↓# Fines & penalties ↓$ Incident response costs
Optimized security stack	Improved security technology & data from TI integrations.	↑# IOCs proactively blocked by NGFW, mail gateway, or EDR ↑% Enriched SIEM data & analytics	↑# FTE hrs recovered ↓$ Costs saved from other technology investments
Business outage savings	Improved user productivity from fewer cyber-related outages.	↓# Cyber-related events causing business disruption ↓% Scope duration of business disruption from remaining events	↑# FTE hrs recovered due to fewer and shorter events ↑$ Productivity gains from other affected business units
Domain-specific benefits	Additional ROI from specific use-cases	Time to detect insider threats ↑% Relevant & TI-prioritized CVEs	↑$ Protected asset value-at-risk (VaR) ↓$ Vulnerability management efficiency gains
All-in-one ETI solution advantages	Advantages of a unified external threat intelligence product suite	↑% Threat data quality from data processing and enrichment Seamless investigations, threat hunting, and pivoting	↑# FTE productivity gains, improved dashboard fatigue ↓$ Bundle savings, two TI tools in one solution suite ↓$ Shortened payback period

Die Rolle von Threat Intelligence in der Produkt-Security

Einblicke in potenzielle Datenverluste und den Diebstahl von geistigem Eigentum

Identifizierung und Warnung

vor Angriffen auf
- Produkte
- Dienstleistungen
- Unternehmen & Branche
- Lieferketten

Einsparung von Zeit

indem Sie
- wichtigen Kontext bereitstellen
- die Erfassung sowie die Analyse der Anforderung an Produkt-Security Intelligence automatisieren

Überwachung und Warnung

- vor externen Risiken in der kundenbezogenen Infrastruktur
- mit negativen Auswirkungen auf Marke und Kunden

Generierung von Verständnis für

- die Bedrohungslandschaft
- Schwachstellen, die von Angreifern ausgenutzt werden
- gezielt oder ungezielt

Beispiel: Ein Anbieter von Bedrohungsdaten entdeckte kürzlich mehrere Versuche von Insider-Bedrohungen gegen einen großen Pharmahersteller, der versuchte, Patente im Dark Web zu verkaufen, bevor eine seiner anstehenden Biotech-Übernahmen abgeschlossen wurde.

ROI von Threat Intelligence in der Security medizinischer Geräte

Verringerung des Risikos von Datenschutzverletzungen

a. die Bedrohung zu verhindern, indem der Angriff Pre-Exploit bereits in der Planungsphase erkannt wird oder bevor die gestohlenen Daten verbreitet werden können

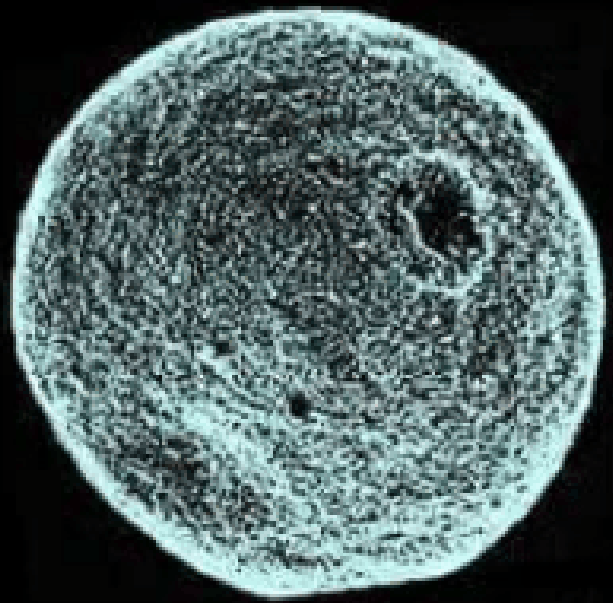
b. Engagement für die Security signalisieren, so dass die kompromittierten Daten entdeckt und die Bedrohung so schnell wie möglich beseitigt wird

Verkürzung der Mean-Time-To-Remediate (MTTR)

Vor zwei Jahren wurden Tausende von Konten der Tesco Bank kompromittiert, was zu Kundenverlusten von mehr als 2,5 Millionen Pfund und Geldstrafen von über 33,5 Millionen Pfund führte. Durch die aktive Überwachung von Dark-Web Foren hätte die Bank gesehen, dass Cyberkriminelle zwei Monate vor dem gezielten Angriff mit der Sicherheitslücke prahlten.

POLLEN

DEATH STAR



ANY QUESTIONS?

Many thanks

Jeff Moore | Chief Product Security Officer

Mail: jeff.moore@draeger.com

Dräger. Technology for Life®