Den morderne SOC

Indblik I hvad der faktisk sker derude

(Dejligt rum uden viduer)

Morten von Seelen

Vice President, Truesec Group

IKT Ingeniør, Ingeniørhøjskolen Aarhus

- Tidligere CEO i Truesec DK frem til sommer 2023.
- 6+ år hos Big4, bl.a. som leder af et Incident Response team
- Specialist i kritisk infrastruktur og Disaster Recovery
- Incident Manager på en lang række store Cyber hændelser

Certs: GCIH, GCFA, GRID, GCDA, GPEN, GSEC, ISO27001 Lead Auditor

Business Areas

TRUESEC i tal

24/7/365
Full capacity to mitigate, detect, & respond to attacks 24/7/365

>400.000
Enheder overvåget med MDR

35.000
IR Timer de sidste 12 måneder

2022
Omsætning på ca 300M DKK

300+ Medarbejdere

100+ I SOC
40+ Dedikeret IR

5.000
Standsede angreb i 2022

Internationally Acknowledged and Certified

NO MORE RANSOM

FIRST Improving Security Together

TF-CSIRT Trusted Introducer

CERTIFIERAT ISO 9001 SVENSK CERTIFIERING

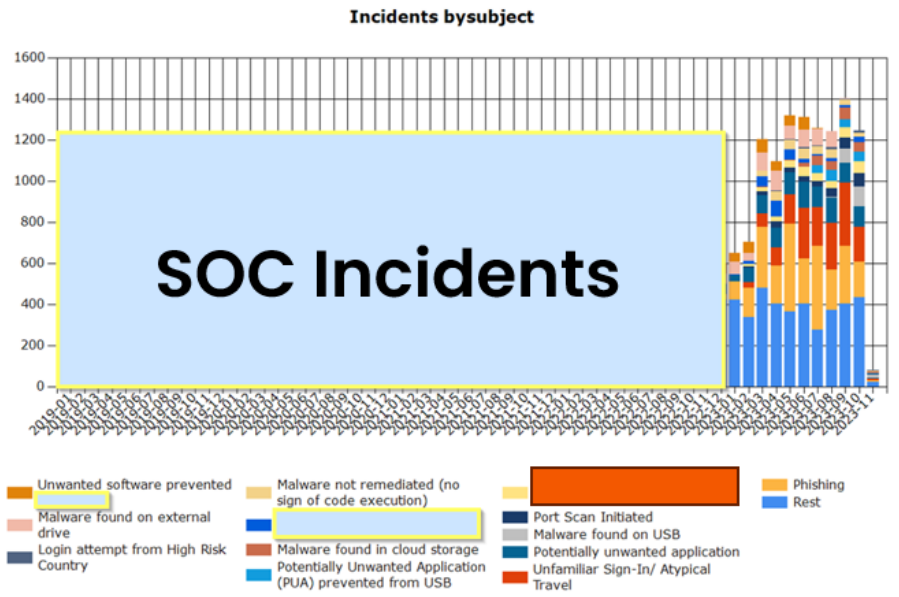
CERTIFIERAT ISO 14001 SVENSK CERTIFIERING

CERTIFIERAT ISO 27001 SVENSK CERTIFIERING

Vores SOC i tal,
Oktober 2023

400.000 Endpoints overvåget
69.211 Alarmer analyseret
***1.200+ Positive-Positive Alarmer i SOC'en**

34 Større Cyber Incidents



Dagens Agenda

- De 3 (+2) SOC Modeller
- Daglig operation af en større 24/7 SOC
- Beregninger på egen SOC

Del 1

De 3(+2) SOC modeler

Er overvågningen på plads?

Der er 8.765 timer på et år

Hvis vi arbejder
Hverdage 8-16
Ingen Ferie, Ingen Sygdom
253 arbejdsdage på et år:

2.024 timer

Såå… angriberne fokuserer

på de 6.741 timer udenfor dette vindue

Markus Lassfolk • 1st
VP Incident Response (CSIRT)
1w •

"Is a 24x7 SOC really needed? We have SIEM Setup and manage alarms during office hours and evenings when someone has time."
- You decide, but this is from the investigation in one of our latest ransomware cases:

Thursday:
22:12 An account logs on through a remote solution.
22:28 Manages to elevate to a Domain Admin account
22:40 Creates a GPO to deploy tools to all servers & clients in the environment.
22:41 Starting to check all servers in the environment, extracting data and changes root/admin passwords on servers.
01:50 Finds Backup servers and deletes them
03:10 Starts encryption of all servers and clients.

- If you can't Detect and Respond (automatic isolation, or human response) to an intrusion like this, you will either wake up to a very bad morning or just be able to watch when your Security Alarms go off but are unable to take action. In this case, 5 hours from start to encryption. We have seen much short timeframes too, but this one is fresh in my mind.

MDR

TIER 01

- Direkte Alarm forwarding
- 24/7 kun på Vagt-telefon
- Få års erfaring hos analytikere
- Ingen Analyse af alarmen
- Ingen Level 3 Analytikere
- Ingen IR
- Ingen Hands On Response
- Ingen optimering af Detection Rules
- Ingen Threat Intel.
- Kan gøres virkelig billigt!

30+ i DK

TIER 02

- 24/7 med udlandske recourser.
- Analye af alarmer, Simpel Triage
- Ofte kun lederen som er L3
- Internt IR team, men begrænset dokumenterbar erfaring
- Rådgiver kunden til hvordan det skal håndteres men ingen hands on
- Optimering af Detection Rules som konsulentydelse
- Threat Intel fra Åbne kilder

15+ i DK

TIER 03

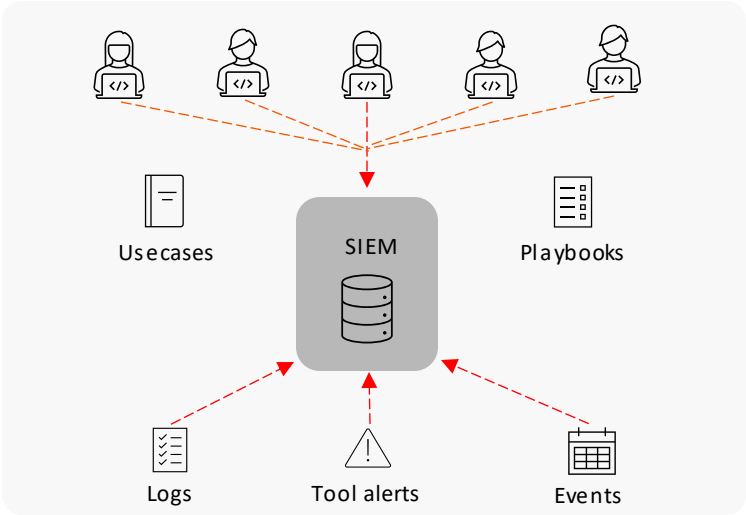
- Moden 24/7 med lokale folk
- Analyse af Alarmer og fuld Triage
- Fomel orgenisation med L1, L2, L3, hvor lederne ikke også er SME.
- Fuld Response iht. Playbooks og Rules of Engagement.
- Sikkerheds Platformen tunes og vedligeholdes løbende
- Fuld IR ydelse
- Threat Intel
- Dyrt!

~5 i DK

TRUESEC

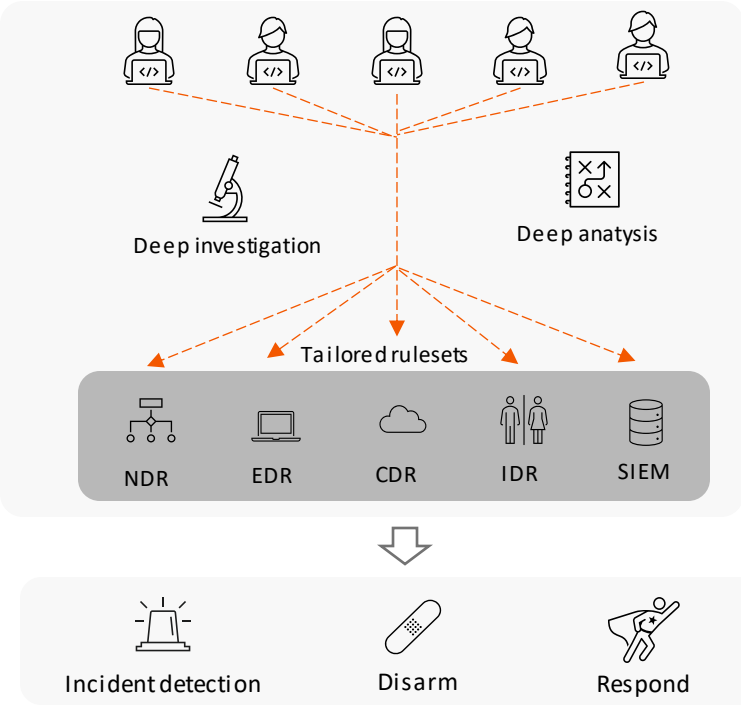
1

GENERIC **SIEM CENTRIC** DETECTION



2

MODERN XDR CENTRIC DETECTION



SIEM CENTRIC DETECTION

Multi-source collect all approach

Multi-source log/event/alert indsamling og analyse baseret på virksomhedsomfattende indsamling fra aktiver og sikkerhedsværktøjer

Threat Identification

Skaber synlighed ved at analysere log/event/alert baseret på politikbaserede usecased og playbooks.

People & process

Normaliserede regler i en one-stop shop løsning, veldefinerede ansvarsområder, højt skalerbar - minimerer menneskelig analyse

Output-Centric

Sikkerhedsalarmering baseret på aftalte politikker og compliance. Fokuserer på at logge alt. Begrænsede evner til at reagere.

XDR CENTRIC DETECTION

Tailored Incident detection approach

Asset-specifik XDR-værktøj til at opdage mistænkelige trusselsaktøraktiviteter (TAA) i missionkritiske aktivtyper. (Defender for: Endpoint, Identity, O365, Cloud osv)

Threat Detection & Response

Designet til at opdage sofistikerede trusler og til at muliggøre hurtig detektion og respons med indeslutning for at minimere indvirkningen

People & process

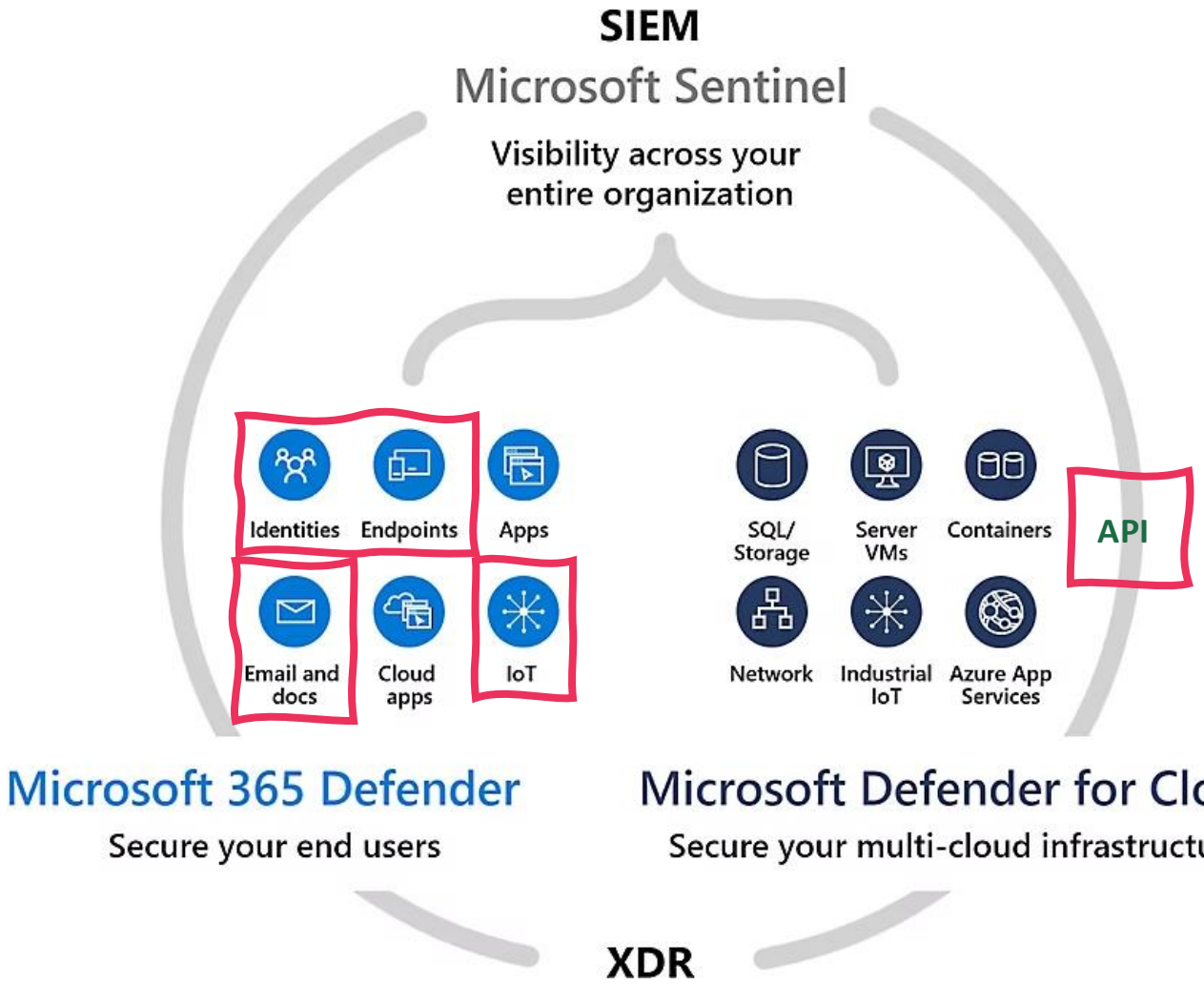
Operer direkte i XDR-værktøj for at optimere kapaciteten. Unikke regler for at fange mistanker for at optimere detektionen. Dyb analyse og undersøgelser for at levere højere værdi

Outcome-Centric

Forebyg cyberhændelser ved at handle på detektion og respons på bekræftede trusler - Beskyt forretningen mod negativ indvirkning

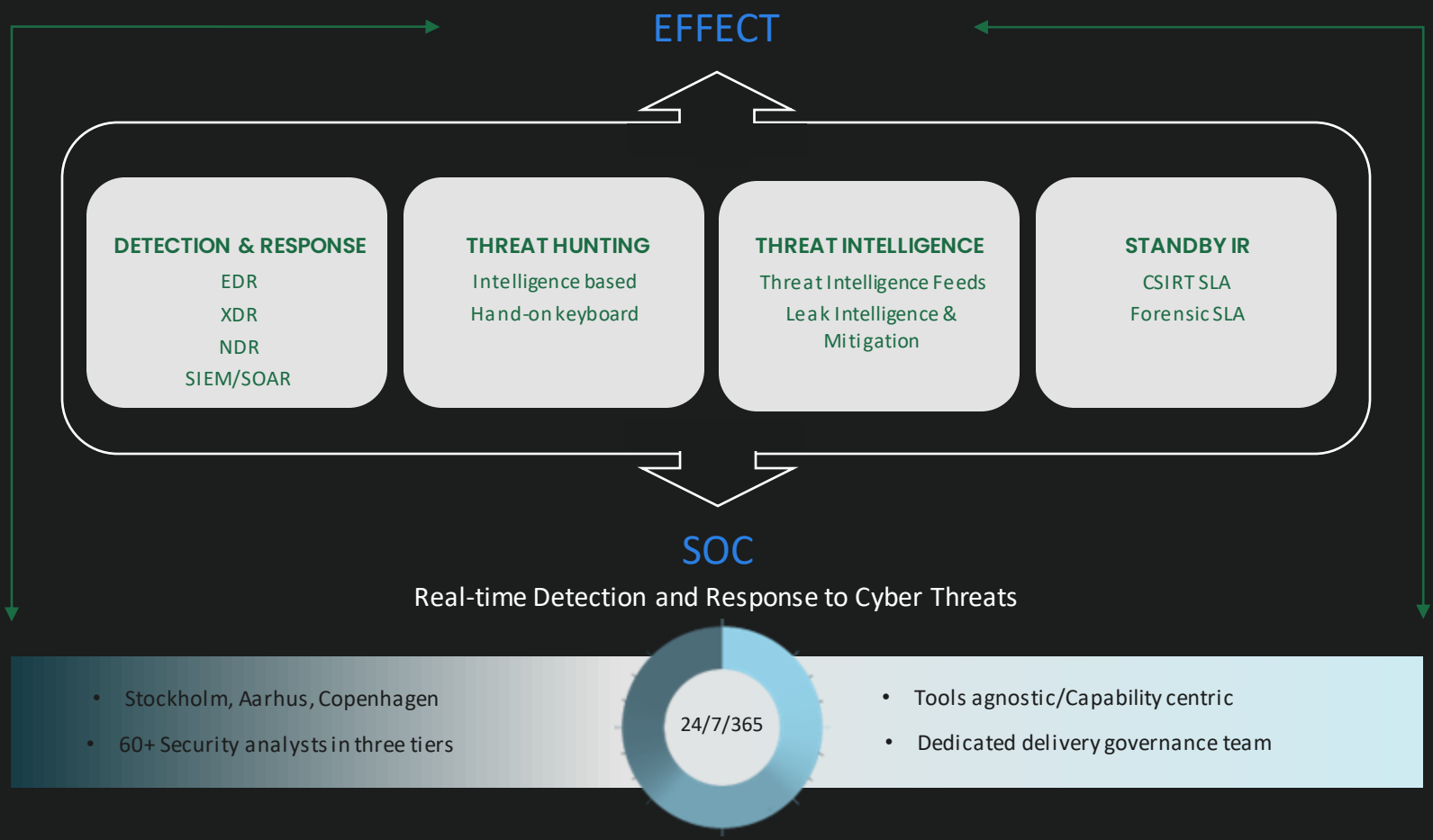
Del 2

Praktisk Operation

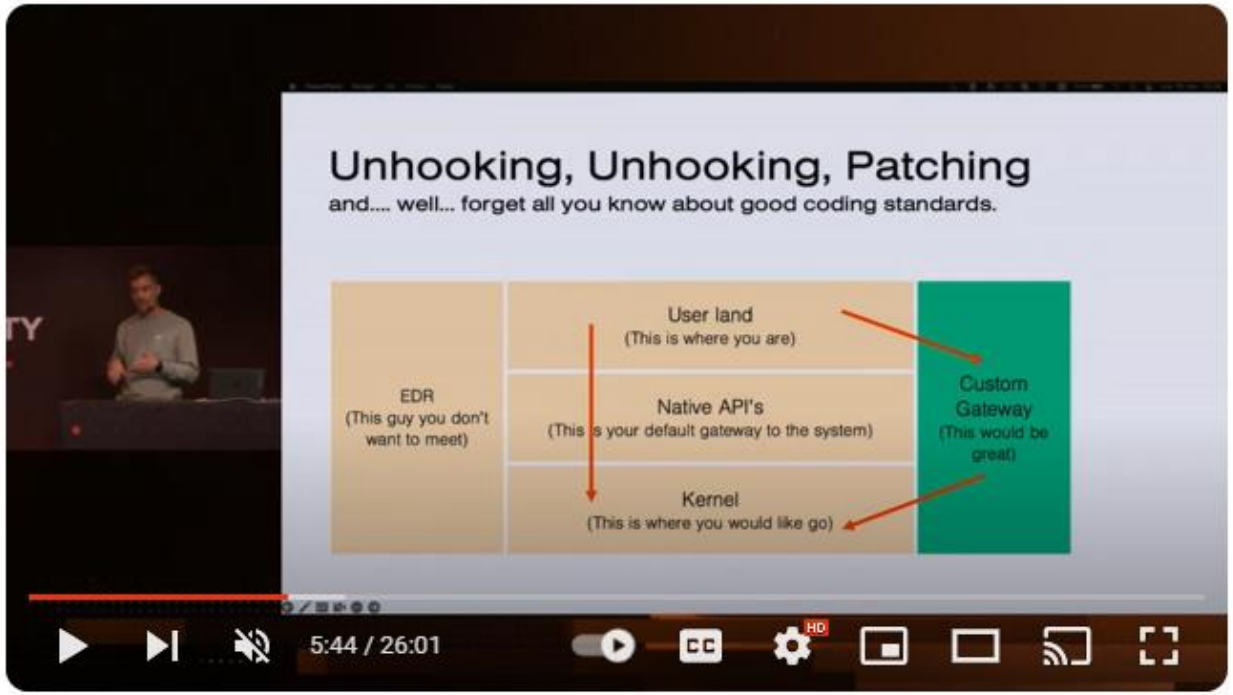

SIEM
Microsoft Sentinel
Visibility across your entire organization
Identities
Endpoints
Apps
Email and docs
Cloud apps
IoT
SQL/ Storage
Server VMs
Containers
API
Network
Industrial IoT
Azure App Services
Microsoft 365 Defender
Secure your end users
Microsoft Defender for Cloud
Secure your multi-cloud infrastructure
XDR

Vores SOC

- Drevet af R.I: Real Intelligence. Ægte mennesker uddannet i sikkerhed bag skærmen. Ingen sort bokse
- Håndteret af 3-Tier Analytiker teams
  - Niveau 1 operatører (Unge 0-3 års erfaring)
  - Niveau 2 trusselsanalytikere (3-7 års erfaring)
  - Niveau 3 senior trusselsanalytikere (Ofte 10+ års operativ erfaring)
- Detection Engineers optimerer XDR/EDR direkte frem for SIEM.
- SOC-analytikere er de første til at modvirke eventuelle angreb og iværksætte selvstændigt nødvendige forsvarsforsøg. (Rules of engagement)
- Beliggende i centrum af Stockholm, i sikkerhedsklassificerede lokaler, tekniske Account Management fra DK.
- Vi arbejder altid på vores kunders systemer - i deres systemer. De kan forlade os i morgen


EFFECT
DETECTION & RESPONSE
EDR
XDR
NDR
SIEM/SOAR
THREAT HUNTING
Intelligence based
Hand-on keyboard
THREAT INTELLIGENCE
Threat Intelligence Feeds
Leak Intelligence & Mitigation
STANDBY IR
CSIRT SLA
Forensic SLA
SOC
Real-time Detection and Response to Cyber Threats
• Stockholm, Aarhus, Copenhagen
• 60+ Security analysts in three tiers
24/7/365
• Tools agnostic/Capability centric
• Dedicated delivery governance team

Research



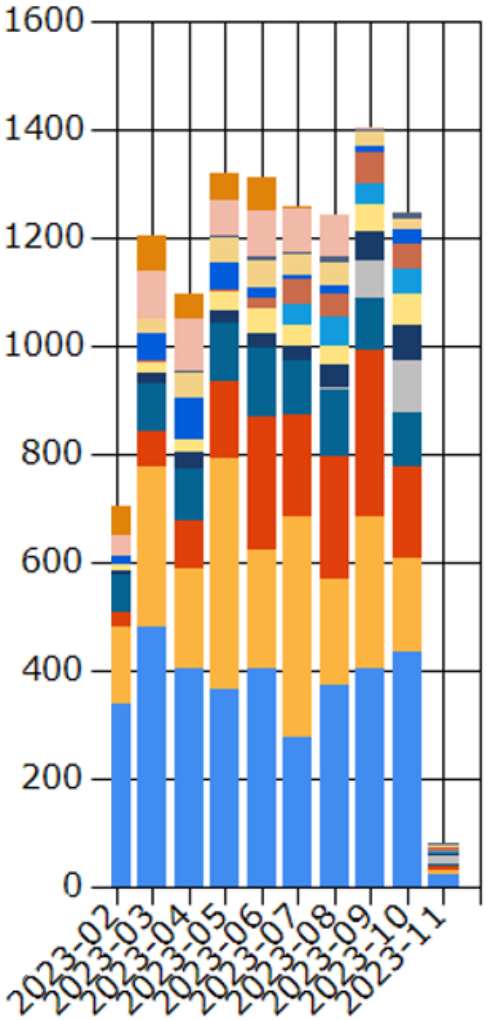
Malware Development: Evading Microsoft Defender for Endpoint w. Mikkel Ole Rømer - Truesec Summit

Truesec
3.6K...

Subscribed

72

Share



Unwanted software prevented

Malware found on external drive

Login attempt from High Risk Country

Port Scan Initiated

Malware found on USB

Potentially unwanted application

Unfamiliar Sign-In/ Atypical Travel

Phishing

Rest

Malware not remediated (no sign of code execution)

Malware found in cloud storage

Potentially Unwanted Application (PUA) prevented from USB

69.211 Alarmer analyseret

Analyse af 1200+ Positive/Positive Oktober 2023

*Ikke alle oktober sager er lukket endnu

Custom Detections

70%

Of Positive-Positive

Detected by Custom EDR/XDR Rules

95%

Red Teams Detected by

Detected by Custom EDR/XDR Rules first

Mikkel

Is undetected by

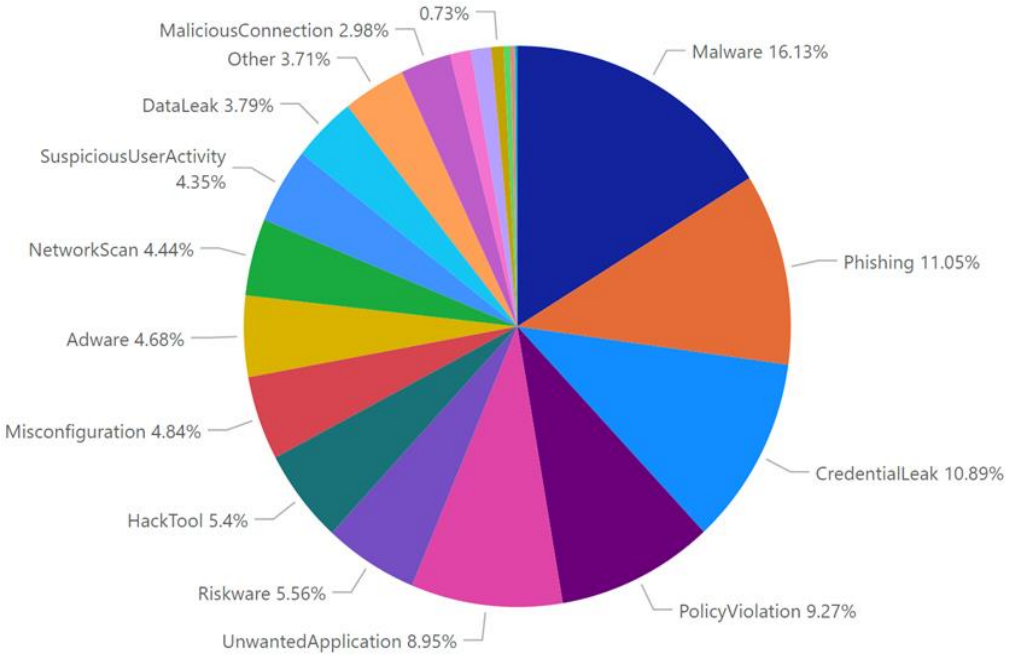
95%

of the Standard-Rules.

Del 3

Beregninger på egen SOC

~1207 cyber attacks disarmed in October

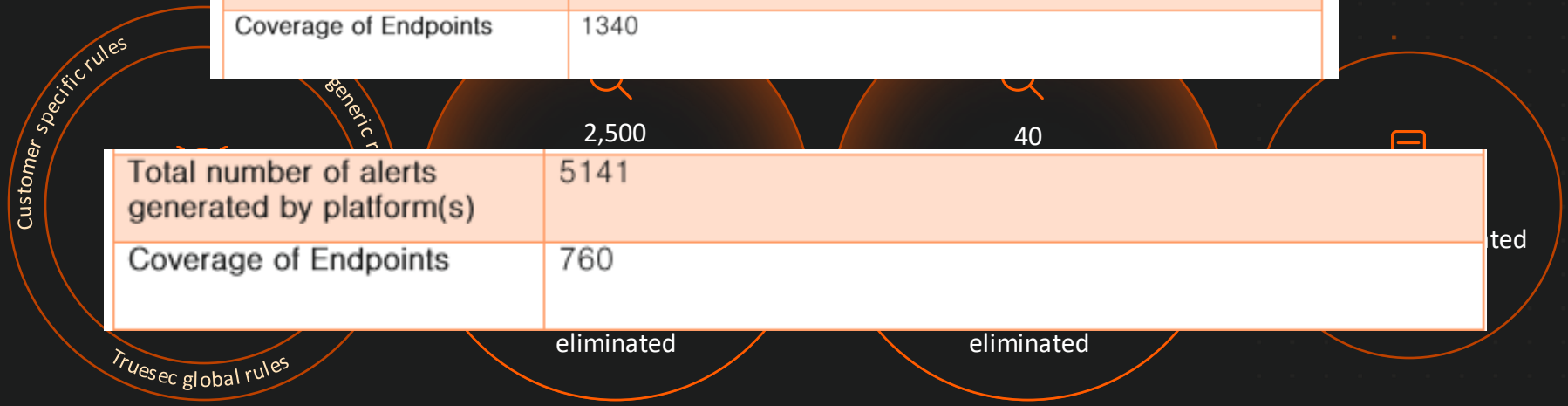


69.211 Alarmer analyseret

Alert Qualification

Every alert is analyzed without additional costs and with true positive delivery

Total number of alerts generated by platform(s)	2549
Coverage of Endpoints	1340



Total number of alerts generated by platform(s)	5141
Coverage of Endpoints	760

No. of alerts reported → Rapid investigation → Deep investigation → Threat confirmed

*Monthly based on 1000 monitored devices

24 timer i SOC'en

TRUESEC

	A	B	C	D	E	F
1	**Alarmer**	69.211		Incidents	1207	
2	**Antal dage**	30		**Antal dage**	30	
3	**Alarmer pr. dag**	2.307		**Incidents pr. dag**	40	
4	**Alarmer pr. time**	96		**Incidents pr. time**	2	
5						
6	**L1 Tid pr. alarm**	5	minutter	**L1 Tid pr. alarm**	60	
7				**L2 Tid pr. Alarm**	30	
8				**L3 tid til QA**	15	
9						
10						
11	**Forbrugt tid pr dag**	192	timer	**Forbrugt tid pr dag**	70	timer
12	**Antal L1 Medarb.**	50	medarbejd	**Antal L1 Medarb.**	50	
13	**L1 medarbejder pr dag**	4	timer	**Antal L2 Medarb.**	6	
14				**Antal L3 Medarb.**	4	
15						
16		**L1 Timer pr. medarbejder pr dag**			0,8	time
17		**L2 Timer pr. medarbejder pr dag**			3,4	time
18		**L3 Timer pr. medarbejder pr dag**			2,5	time
19						

Overvejelser og Cost

1. **Lokaler og ophold**
   Lokaler godkendt til ophold 24/7
   Bespisning
   Toiletforhold
   Ventilation

2. **Staffing og ansættelser**
   Rekruttering af medarbejdere
   Træning af medarbejdere
   Vidensdeling. Hvordan?
   Staffing ved Sygdom. Små team er sårbare

3. **Detection Optimering**
   Angriberne kender standard-indstillingerne i de fleste værktøjer
   Hvordan tilpasses miljøet løbende
   Optimering af Regler og filtrering

4. **Intern Cost – Næste side ->**

Overvejelser og Cost

1. **Eksempel på interne beregninger på 24/7.**
   Statistisk historik

Stordrift – F.eks. Sammen med andre Universiteter: (Delt L2 og L3)
1.000 enheder: ca. 70.000 DKK pr. måned. (1,5 FTE) + Diverse
2.000 enheder: ca. 115.000 DKK pr. måned. (2,5 FTE) + Diverse
5.000 enheder: ca. 165.000 DKK pr. måned. (3 FTE) + Diverse
10.000 enheder: ca. 230.000 DKK pr. måned. (4 FTE) + Diverse
20.000 enheder: ca. 348.000 DKK pr. måned. (6 FTE) + Diverse

Stand Alone utopisk drift UDEN SYGDOM OG FERIE: (3 stk L1 + 1 stk L3)
1.000 enheder: ca. 230.000 DKK pr. måned. (4 FTE) + Diverse
2.000 enheder: ca. 230.000 DKK pr. måned. (4 FTE) + Diverse
5.000 enheder: ca. 230.000 DKK pr. måned. (4 FTE) + Diverse
10.000 enheder: ca. 230.000 DKK pr. måned. (4 FTE) + Diverse
20.000 enheder: ca. 348.000 DKK pr. måned. (6 FTE) + Diverse

Ingen XDR: -25%

Low Noice Miljø: -15%
High Noice Miljø: +50%

Samarbejde

I er ikke så forskellige. Arbejd sammen!

Fælles SOC
Fælles Detection Optimering
Fælles Threat Intel
Fælles Vidensdeling
Fælles Træning

Thank You!

Extra Questions ->

www.truesec.com x.com/truesec linkedin.com/company/truesec