
semcon
ADDING
NEW
PERSPECTIVES
ON
TECHNOLOGY.

Klas Elmby

Teknisk bakgrund

Jobbat i IT-branchen sedan 1988.

Haft CIO rollen över 30 år


semcon
VAD ÄR SEMCON

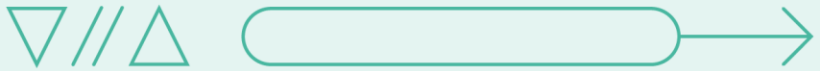
- En internationell teknikpartner som grundades 1980 i Sverige.
- Semcon kombinerar ingenjörskonst med digital expertis och hållbarhetskompetens i ett unikt erbjudande inom produkt-, produktions- och tjänsteutveckling.
- 1 600 medarbetare på mer än 20 kontor i Sverige, Norge och Brasilien.
- Stöttar ledande och framgångsrika kunder världen över.
- Verksamma i många branscher, såsom energi, life science, industri, mobility, och offentlig sektor.

Vårt syfte

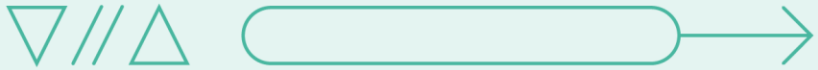
Vi sätter människan först. För oss har tekniken inget syfte i sig, det som är viktigt är värdet den skapar för människor och för planeten.

Vårt bidrag

Att utveckla teknik som förbättrar människors liv samtidigt som vi respekterar de planetära gränserna och värnar mänskliga rättigheter är ingen enkel uppgift. Den kräver att vi tänker nytt. Vi behöver nya perspektiv på teknik. Och det är vad våra experter och tvär-vetenskapliga team hjälper kunder med varje dag.



Hur förändring stärkt vår cybersäkerhet



Hur såg det ut innan

- Microsoft Defender “AV”
- Pentest en gång om året
- Open Source SIEM
- Interna resurser
- Beredskap, men inte monitorering utanför kontorstid
- Patch management via SCCM (och validering via rapporter)
- Osv..

Hur ser det ut idag

- Trend Micro XDR / Service one complete
- 24/7 via Trend Managed XDR
- Säkerställning av patchning via XDR plattform/EDR agent
- Benchmarking via Security Scorecard och Vision One
- Ständig validering av miljön (Pentera)
- Simuleringar av attacker (Pentera)
- Automatisering (API)
- Phishingsimulering och awarenessträning

VÄGEN TILL FÖRÄNDRING

SÄTT MÅL

UTBILDA LEDNING & STYRELSE

- Vad är viktigt
- Varför är det viktigt
- Vad är huvudskälet till att man "åker dit"
- Vad är vanliga attackvektorer
- Var är vi som bolag sårbara
- Vad kan skyddas
- Vad kan inte skyddas (med rimliga medel/kostnader)
- Vilka risker kan vi leva med och varför

Engagemang och beslutsfattande

- Engagemang från top-management
- Korta och snabba beslutsvägar

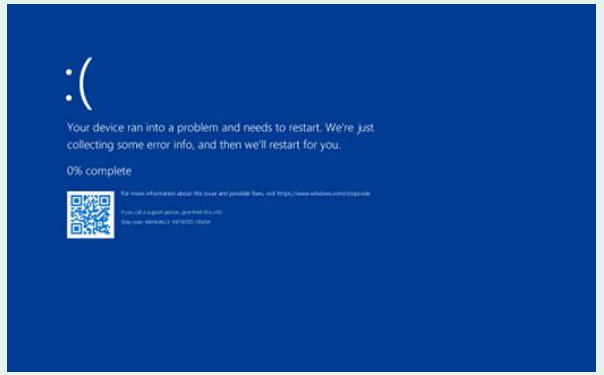
VÄLJ LEVERANTÖRER/PRODUKTER

Se över befintlig stack

Komplettera/byt ut/behåll

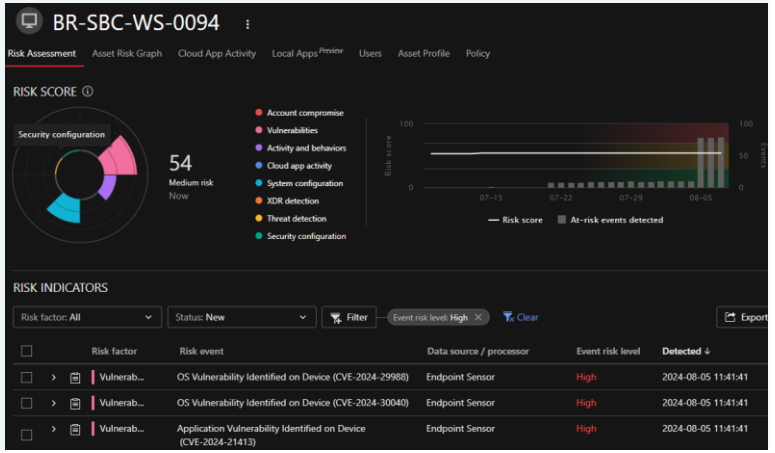
ÄNDRAT MINDSET

Vad är allvarligast? En windows-server eller något system som inte startar efter en patch, eller hela IT-miljön krypterad för att man inte patchat en kritisk sårbarhet i tid?



Agera

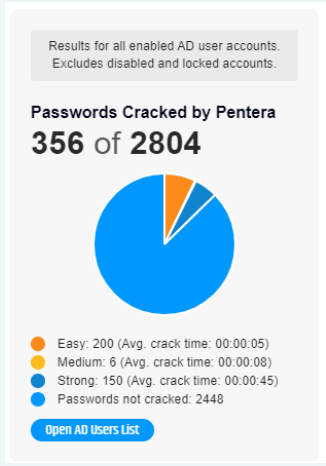
- Leta upp root cause till så mycket som möjligt
  - Varför har inte 5% av våra klienter rätt patchnivå trots att SCCM säger det?
  - Undersök alla workbenches i Vision One
- Patcha, förändra, täpp till när något hittas

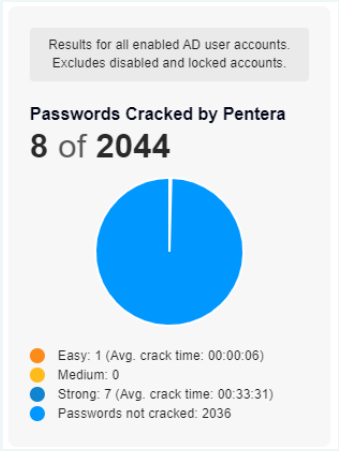


Validera och följ upp

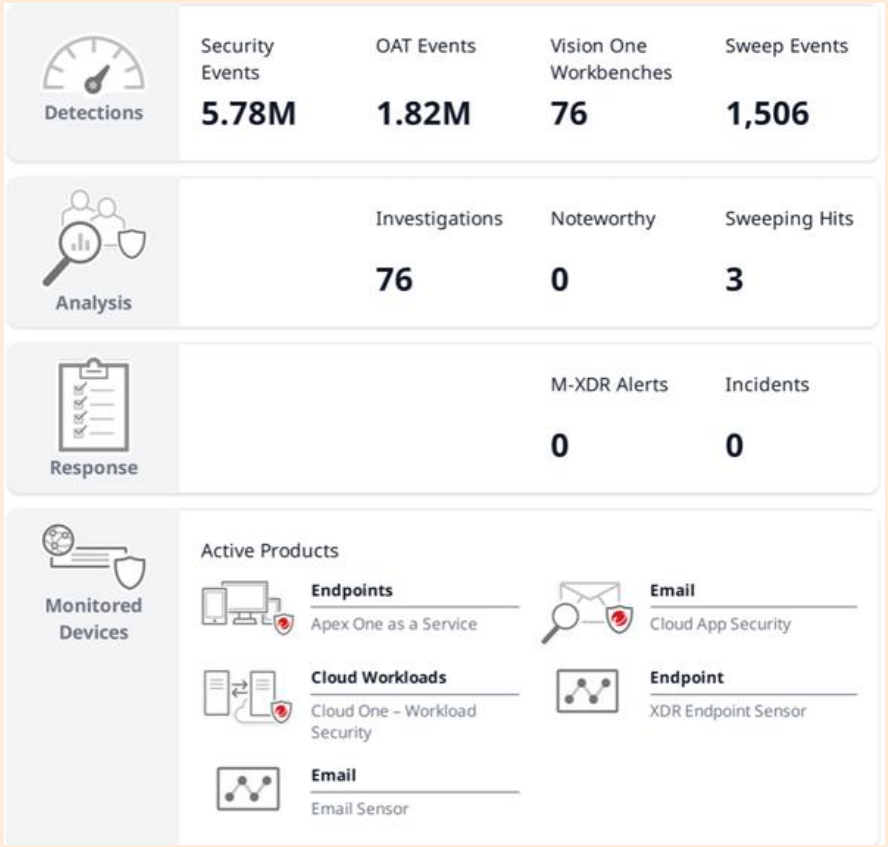
- Trend Vision One
  - Exposure overview
  - Risk overview
  - Attack Surface
- Pentera
- Security Scorecard
- QBR

6 månader efter förändring av password policy





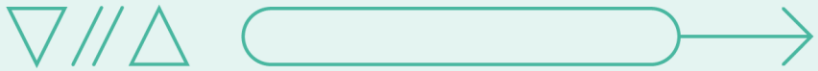
Managed XDR

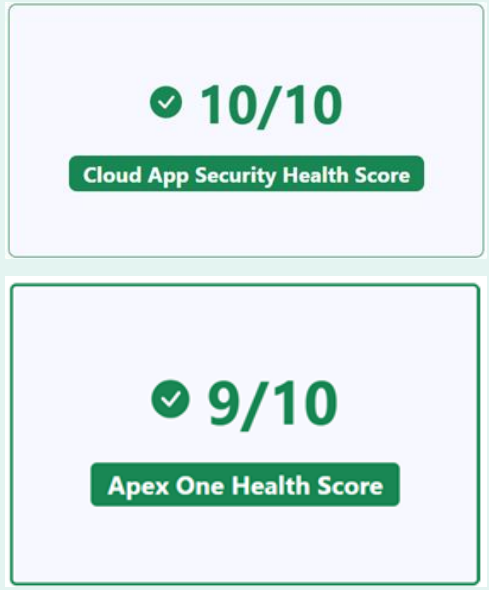

Detections
Security Events
5.78M
OAT Events
1.82M
Vision One Workbenches
76
Sweep Events
1,506
Analysis
Investigations
76
Noteworthy
0
Sweeping Hits
3
Response
M-XDR Alerts
0
Incidents
0
Monitored Devices
Active Products
Endpoints
Apex One as a Service
Email
Cloud App Security
Cloud Workloads
Cloud One – Workload Security
Endpoint
XDR Endpoint Sensor
Email
Email Sensor

Service one complete

Veckovisa möten

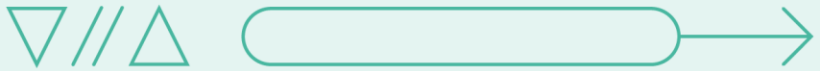
QBR

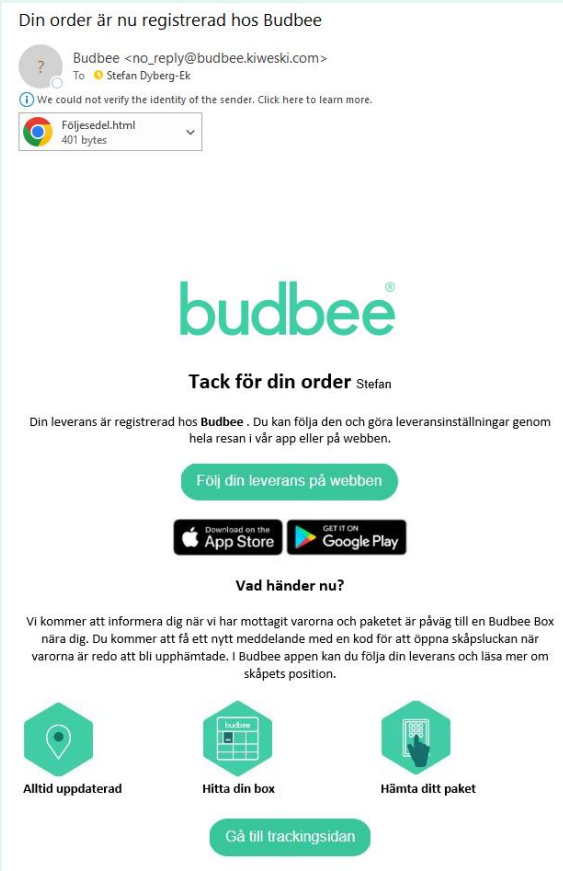




Phishinsight – Utbildning/testing av medarbetare

- Schemalagd träning för nyanställda
- “On-demand” testing
- Utbildning



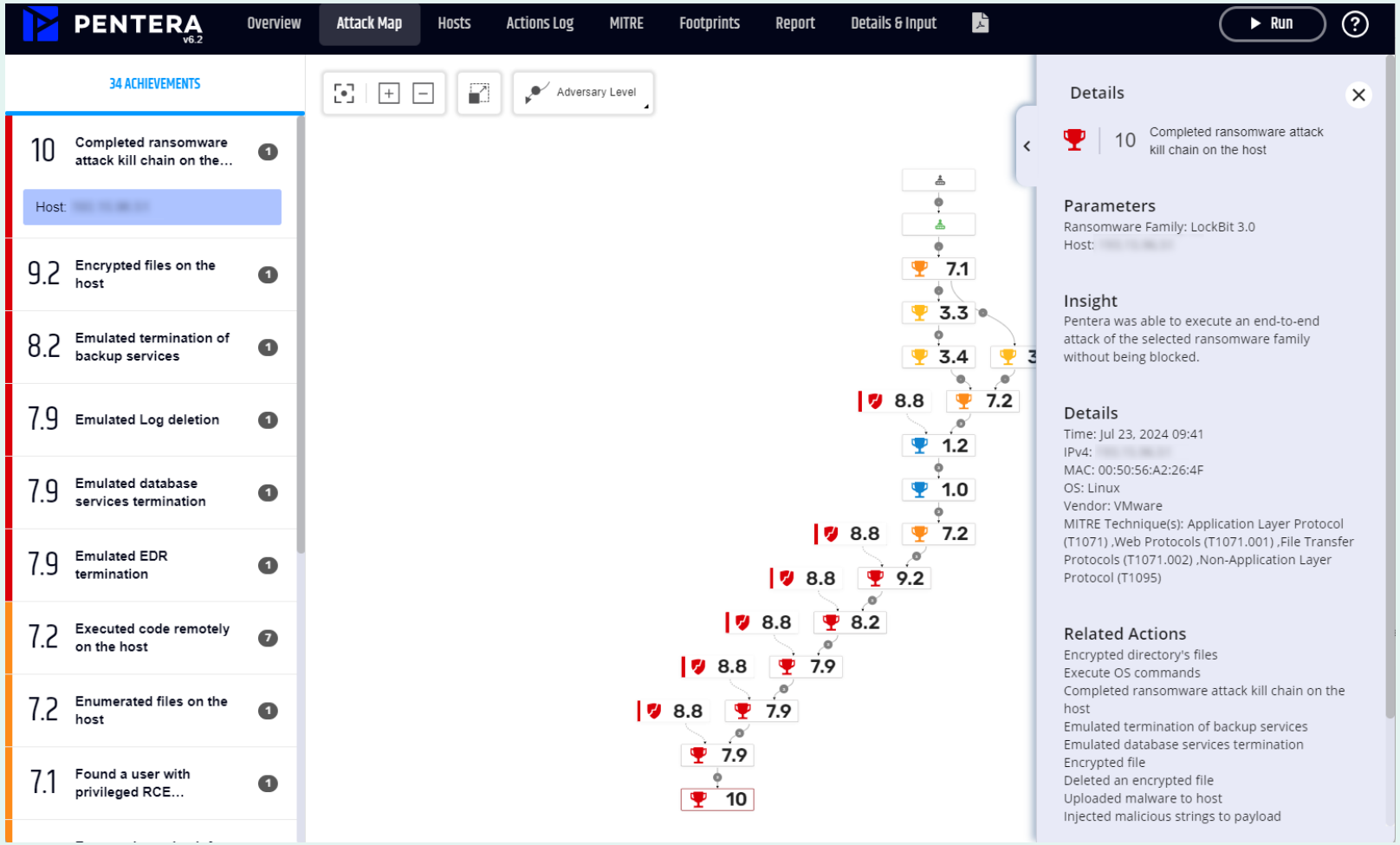


Provtryckning av M-XDR/EDR (Pentera)

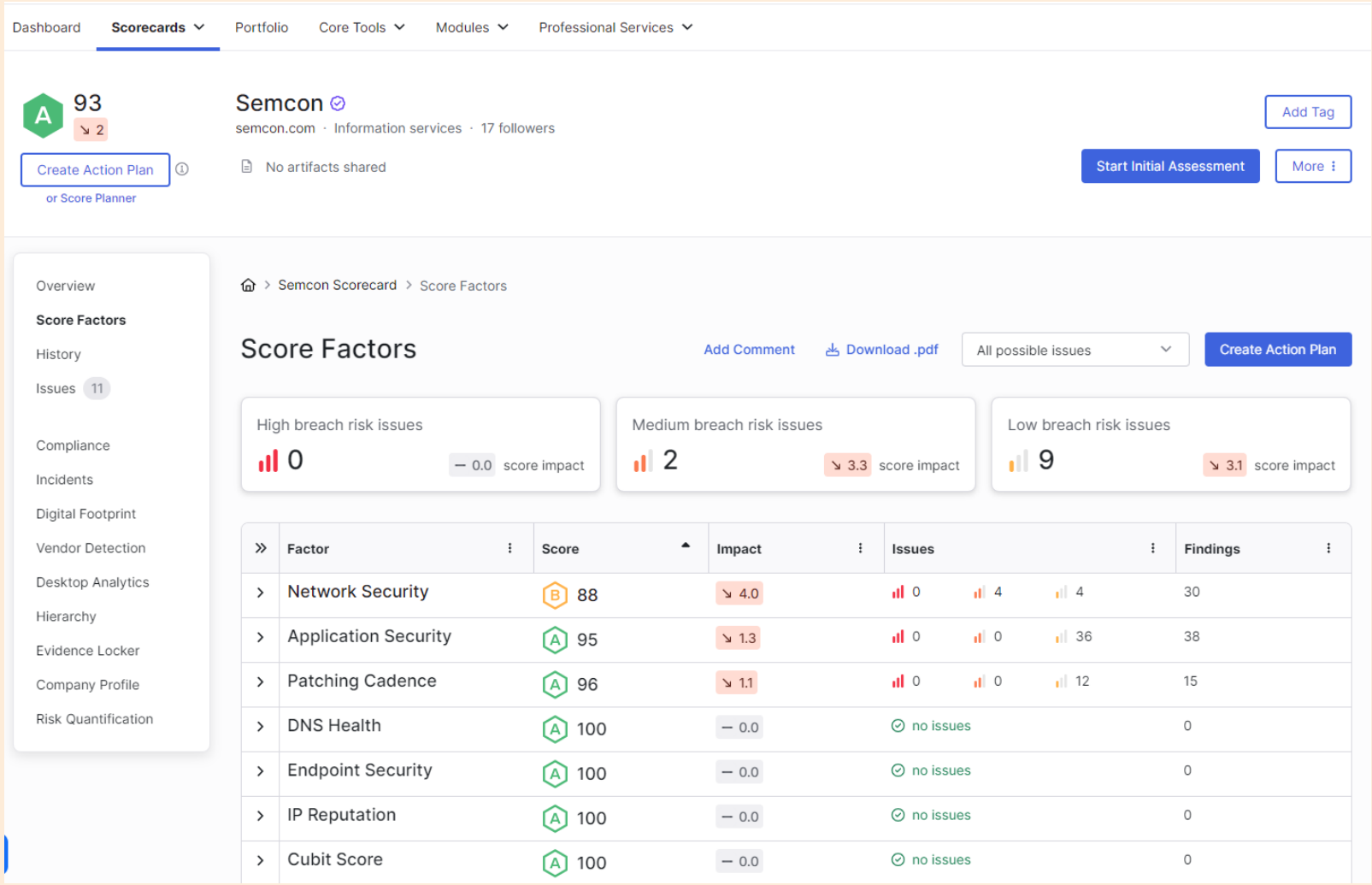
Ransomware readiness

What-if attacker

Säkerhetsvalidering



Benchmarking




semcon
ADDING
NEW
PERSPECTIVES
ON
TECHNOLOGY.