

A photograph of two young women standing together, looking at a smartphone held by the woman on the right. The woman on the left has curly hair and is wearing glasses and a denim jacket. The woman on the right has straight hair and is wearing a light-colored jacket. The background is a bright, out-of-focus outdoor setting. The text 'semcon' is in the top right corner.

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

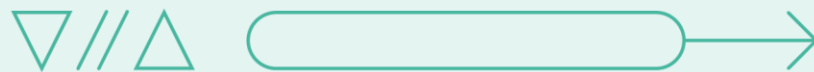
Vi sätter människan först. För oss har tekniken inget syfte i sig, det som är viktigt är värdet den skapar för människor och för planeten.





# 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 tvärvetenskapliga team hjälper kunder med varje dag.





# Hur förändring stärker 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 awarenesssträning**





# 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

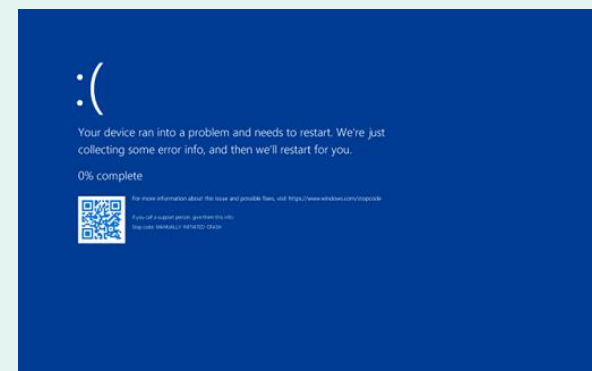
Komplettera/byt ut/behåll





# ÄNDRAT MINDSET

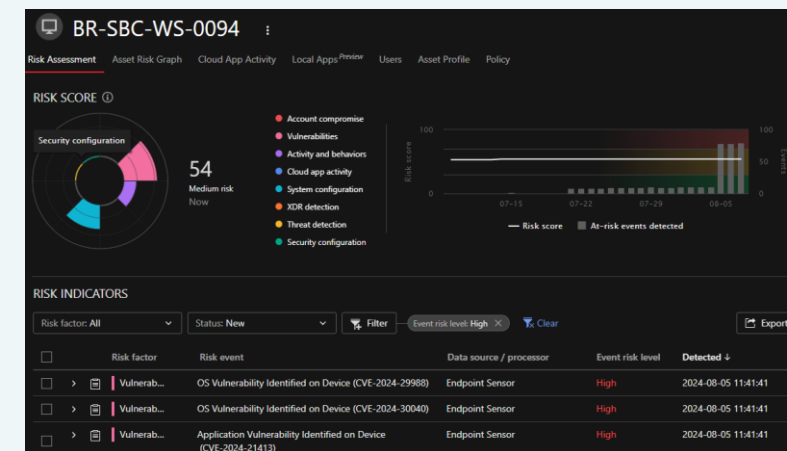
Vad är allvarligast? En windows-server eller något system som inte startar efter en patch, eller hela IT-miljön krypterad för att man inte patchat en kritisk sårbarhet i tid?





# 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



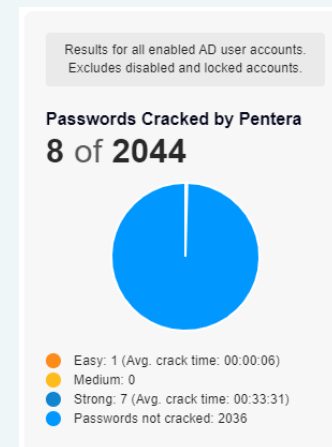
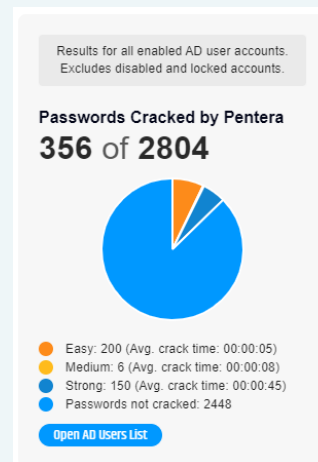




# Validera och följ upp










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

## 6 månader efter förändring av password policy





# Managed XDR

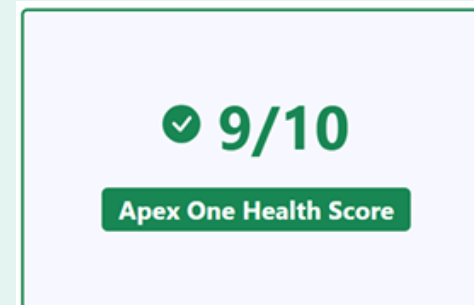
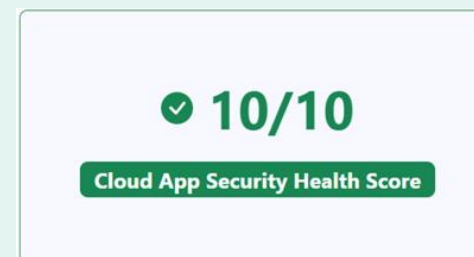
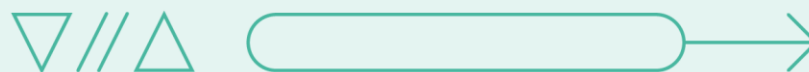
 Detections	Security Events <b>5.78M</b>	OAT Events <b>1.82M</b>	Vision One Workbenches <b>76</b>	Sweep Events <b>1,506</b>
 Analysis		Investigations <b>76</b>	Noteworthy <b>0</b>	Sweeping Hits <b>3</b>
 Response			M-XDR Alerts <b>0</b>	Incidents <b>0</b>
 Monitored Devices	<b>Active Products</b>			
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





# Service one complete

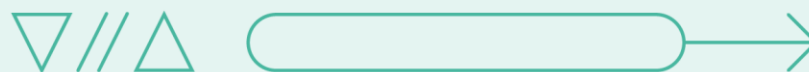
Veckovisa möten  
QBR








# Phishinsight – Utbildning/testing av medarbetare


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




Din order är nu registrerad hos Budbee

 Budbee <no\_reply@budbee.kiweski.com>  
To  Stefan Dyberg-Ek

 We could not verify the identity of the sender. Click here to learn more.



 Följesedel.html  
401 bytes



**Tack för din order** Stefan


Din leverans är registrerad hos **Budbee**. Du kan följa den och göra leveransinställningar genom hela resan i vår app eller på webben.


[Följ din leverans på webben](#)


 

**Vad händer nu?**

Vi kommer att informera dig när vi har mottagit varorna och paketet är på väg till en Budbee Box nära dig. Du kommer att få ett nytt meddelande med en kod för att öppna skåpsluckan när varorna är redo att bli upphämtade. I Budbee appen kan du följa din leverans och läsa mer om skåpets position.

 **Alltid uppdaterad**

 **Hitta din box**

 **Hämta ditt paket**

[Gå till trackingsidan](#)



# Provtryckning av M-XDR/EDR (Pentera)

Ransomware readiness

What-if attacker

Säkerhetsvalidering

The screenshot displays the Pentera v6.2 interface. At the top, there is a navigation bar with tabs for Overview, Attack Map (selected), Hosts, Actions Log, MITRE, Footprints, Report, and Details & Input. A 'Run' button is visible on the right. Below the navigation bar, the interface is divided into three main sections:

- Achievements List (Left):** A list of 34 achievements, with the top one highlighted. The achievements include:
  - 10 Completed ransomware attack kill chain on the...
  - 9.2 Encrypted files on the host
  - 8.2 Emulated termination of backup services
  - 7.9 Emulated Log deletion
  - 7.9 Emulated database services termination
  - 7.9 Emulated EDR termination
  - 7.2 Executed code remotely on the host
  - 7.2 Enumerated files on the host
  - 7.1 Found a user with privileged RCE...
- Attack Map (Center):** A visual representation of the attack path, showing a sequence of steps connected by arrows. Each step is represented by a trophy icon and a score. The scores range from 1.0 to 10.0. The final step is a red trophy with a score of 10.0.
- Details Panel (Right):** A panel providing information about the selected achievement (10 Completed ransomware attack kill chain on the host). It includes:
  - Parameters:** Ransomware Family: LockBit 3.0, Host: [redacted]
  - Insight:** Pentera was able to execute an end-to-end attack of the selected ransomware family without being blocked.
  - Details:** Time: Jul 23, 2024 09:41, IPv4: [redacted], MAC: 00:50:56:A2:26:4F, OS: Linux, Vendor: VMware, MITRE Technique(s): Application Layer Protocol (T1071), Web Protocols (T1071.001), File Transfer Protocols (T1071.002), Non-Application Layer Protocol (T1095)
  - Related Actions:** Encrypted directory's files, Execute OS commands, Completed ransomware attack kill chain on the host, Emulated termination of backup services, Emulated database services termination, Encrypted file, Deleted an encrypted file, Uploaded malware to host, Injected malicious strings to payload

# Benchmarking

Dashboard **Scorecards** Portfolio Core Tools Modules Professional Services

**A 93** 2 **Semcon** semcon.com · Information services · 17 followers Add Tag

Create Action Plan No artifacts shared Start Initial Assessment More

or Score Planner

Overview  
**Score Factors**  
History  
Issues 11  
Compliance  
Incidents  
Digital Footprint  
Vendor Detection  
Desktop Analytics  
Hierarchy  
Evidence Locker  
Company Profile  
Risk Quantification

Home > Semcon Scorecard > Score Factors

**Score Factors** Add Comment Download .pdf All possible issues Create Action Plan

High breach risk issues 0 - 0.0 score impact

Medium breach risk issues 2 - 3.3 score impact

Low breach risk issues 9 - 3.1 score impact

>>	Factor	Score	Impact	Issues	Findings
>	Network Security	B 88	- 4.0	0 4 4	30
>	Application Security	A 95	- 1.3	0 0 36	38
>	Patching Cadence	A 96	- 1.1	0 0 12	15
>	DNS Health	A 100	- 0.0	no issues	0
>	Endpoint Security	A 100	- 0.0	no issues	0
>	IP Reputation	A 100	- 0.0	no issues	0
>	Cubit Score	A 100	- 0.0	no issues	0



A woman wearing a black hard hat and a pink jacket is smiling and looking upwards. She is standing on a construction site with buildings in the background. The text "ADDING NEW PERSPECTIVES ON TECHNOLOGY." is overlaid on the left side of the image. The "semcon" logo is in the top right corner.

semcon

ADDING  
NEW  
PERSPECTIVES  
ON  
TECHNOLOGY.