



**SECURITY
DAYS**

**AIZSARDZĪBA PRET IDENTITĀTES
UZBRUKUMIEM:
KĀ SEGURA SAMAZINA JŪSU RISKUS**

**EDVĪNS SAVVINS
NOD BALTIC TEHNOĻĪJU KONSULTATS**



Par sevi:

Edvīns Savvins

NOD BALTIC

Tehnoloģiju konsultants

IT jomā 5+ gadus

Darba raksturs:

IT risinājumu ieviešana klienta vidē

NOD Baltic kibersardzības

risinājumi organizācijām

Kiberincidentu izmeklēšana

Apmācības

Mūsdienu krīzes anatomija

Sistēmas sarežģītības palielināšanās

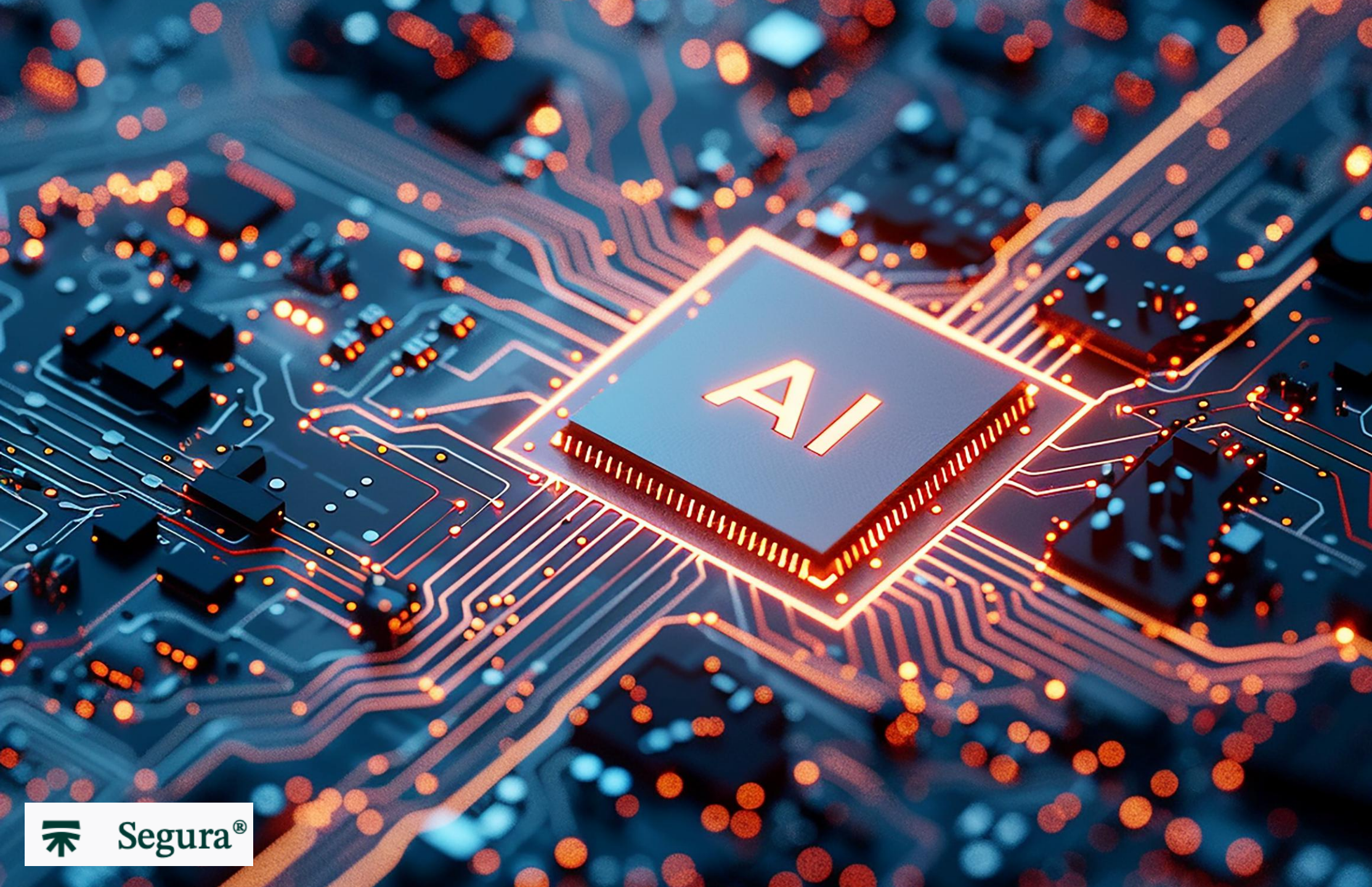
Budžeta
spiediens

Laika spiediens

Lietotāju
neapmierinātības
pieaugums

Pieaugošie
uzbrukumi

Aizvien pieaugošie draudi datu kopumam



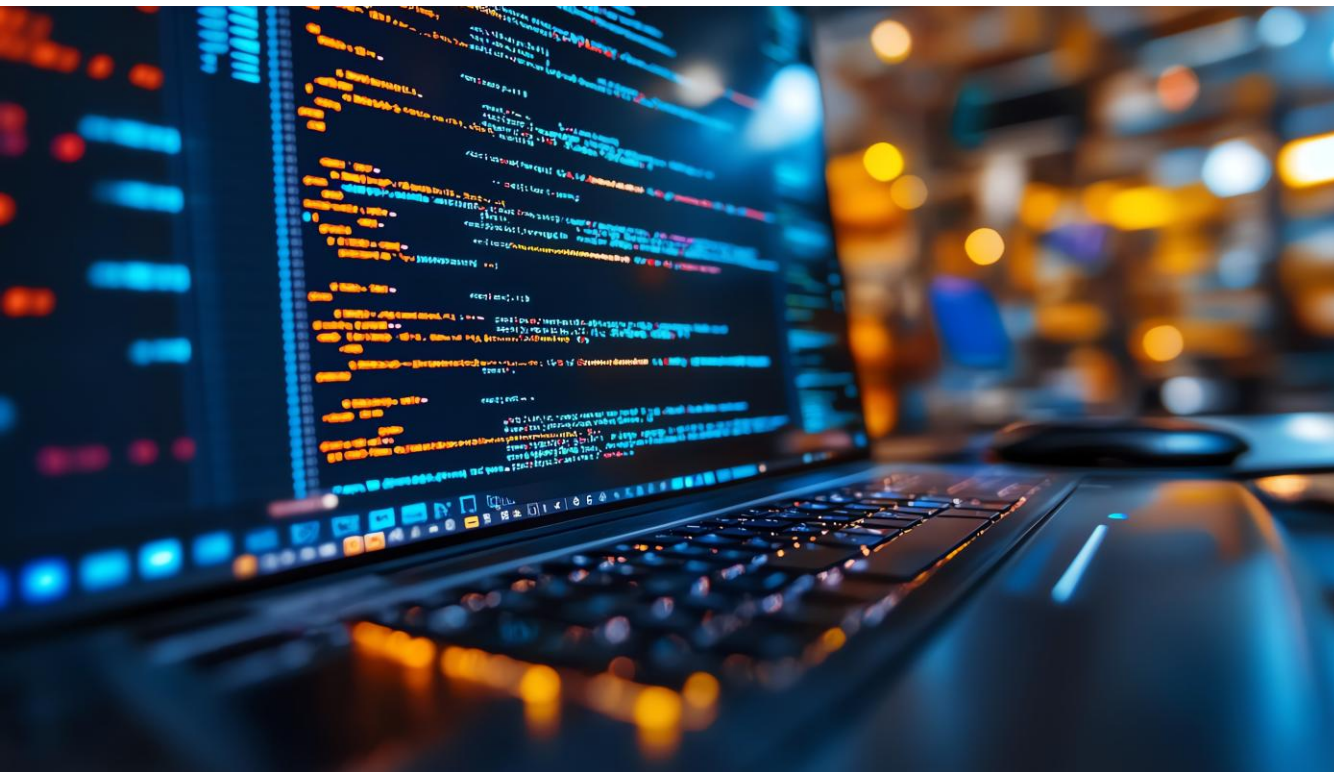
A graphic with a dark blue background featuring a complex pattern of glowing light blue circuit lines and nodes. The text "AI IS EVERYWHERE" is centered in a bold, light blue, sans-serif font. The "AI" is significantly larger than "IS" and "EVERYWHERE".

AI
IS
EVERYWHERE

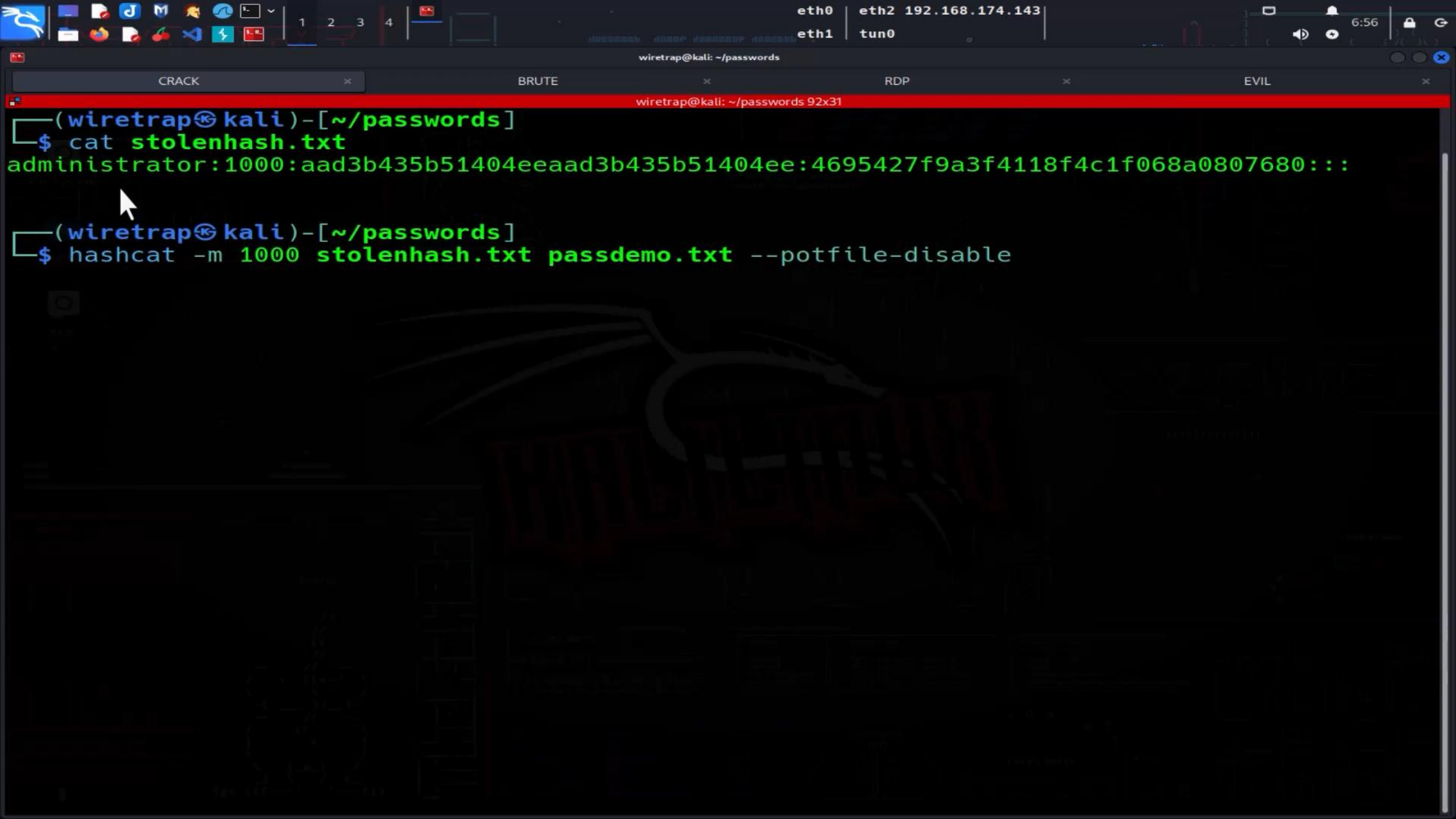


CREATED BY
**THE DOR
BROTHERS**

Uzbrukumu tehnikas



- OSINT
- Enumeration
- Vulnerability Discovery
- Exploit Creation
- Initial Access
- Remote Command Execution (RCE)
- Persistence
- Foothold Enumeration
- Privilege Escalation
- Lateral Movement
- Data Exfiltration



wiretrap@kali: ~/passwords

CRACK

BRUTE

RDP

EVIL

wiretrap@kali: ~/passwords 92x31

(wiretrap@kali) - [~/passwords]

\$ cat stolenhash.txt

administrator:1000:aad3b435b51404eeaad3b435b51404ee:4695427f9a3f4118f4c1f068a0807680:::

(wiretrap@kali) - [~/passwords]

\$ hashcat -m 1000 stolenhash.txt pasdemo.txt --potfile-disable

rdesktop - 192.168.174.132

- Ch341a Programm...
- Recycle Bin
- Kingst VIS
- Tera Term
- enum
- important stuff.txt
- Logic 2.4.9
- Old Firefox Data
- stuff.txt
- Notepad++
- rfid
- Acrobat Reader
- SDRConsole (V3)
- SDR
- Chrome
- STM32 ST-LI...
- tools
- Firefox
- Arduino IDE
- This PC
- Immunity Debugger
- Google Chrome



NATO Locked Shields

ir pasaulē lielākās kiberdrošības mācības, kurās vairāk nekā 40 valstis tiešsaistē aizsargā kritisko infrastruktūru pret tūkstošiem sarežģītu uzbrukumu.

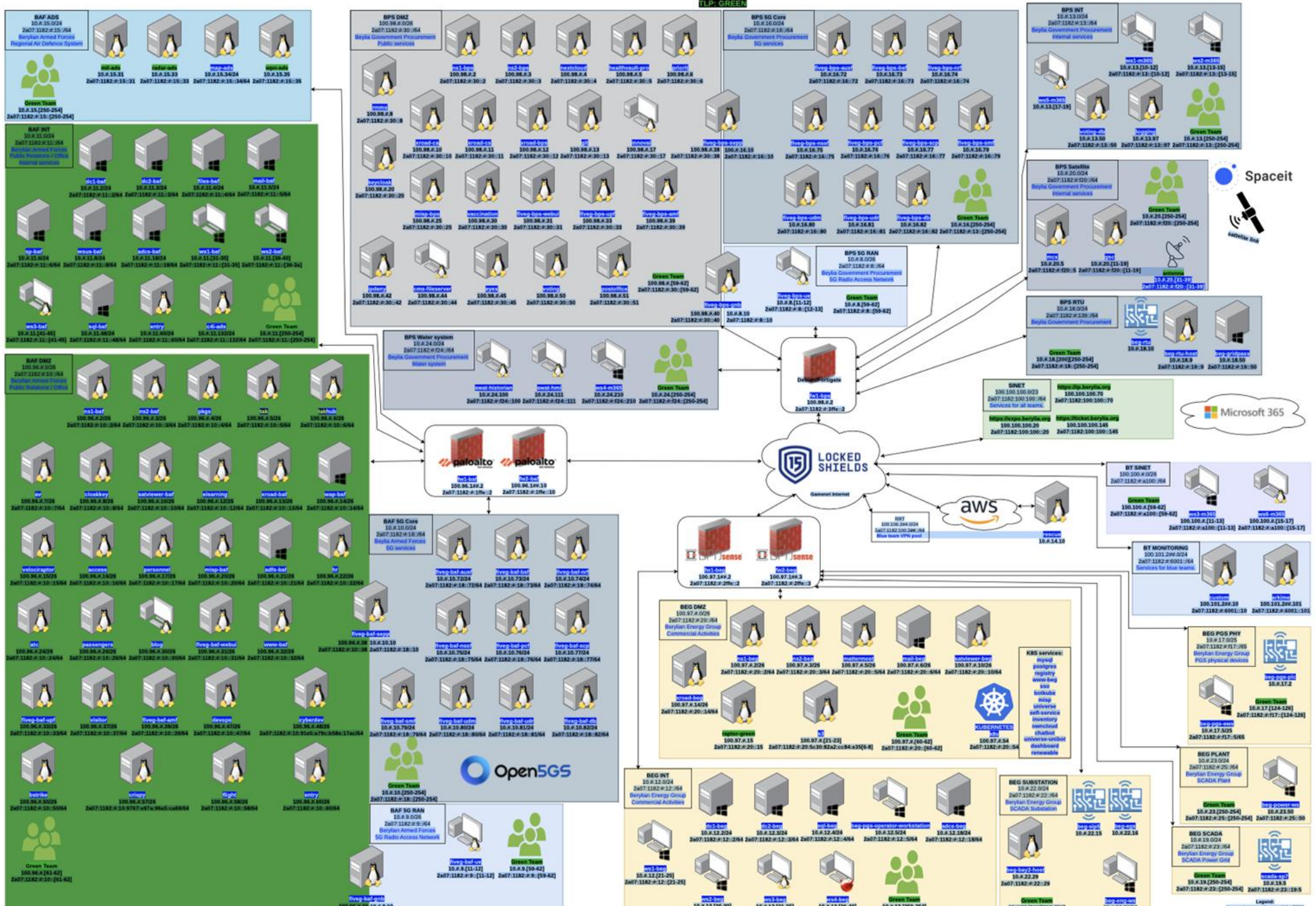
Segura nodrošināja identitātes un piekļuves drošību.



LOCKED SHIELDS 2025

- **World's most complex live-fire cyber defence exercise**
- **Over 40 nations**
- 15th year
- 18 teams
- **Over 4,000 participants**
- **5,500 virtualized critical systems**
- **Over 8,000 attacks**
- Experts come from the fields of cyber security, digital forensics, legal affairs, and strategic communication





Spaceit

Microsoft 365

LOCKED SHIELDS
Government Internet

aws

OpenSGS

Legend
* your team number e.g. 10.0.10.10
your team number e.g. 2807.1182.F:10:04

Mūsdienīgā identitātes drošības un piekļuves pārvaldes pārskats

Kāpēc tas ir svarīgi uzņēmuma elastīgumam un riska samazināšanai

Identitātes un piekļuves pārvaldība

1. Privilēģētas piekļuves pārvaldība (PAM) – privilēģētu kontu un privilēģētu datu droša izmantošana
2. Privilēģēti konti (objekti) – privilēģētu autentifikācijas datu droša uzglabāšana
3. Privilēģēti dati (mērķis) – droša piekļuve privilēģētiem datiem

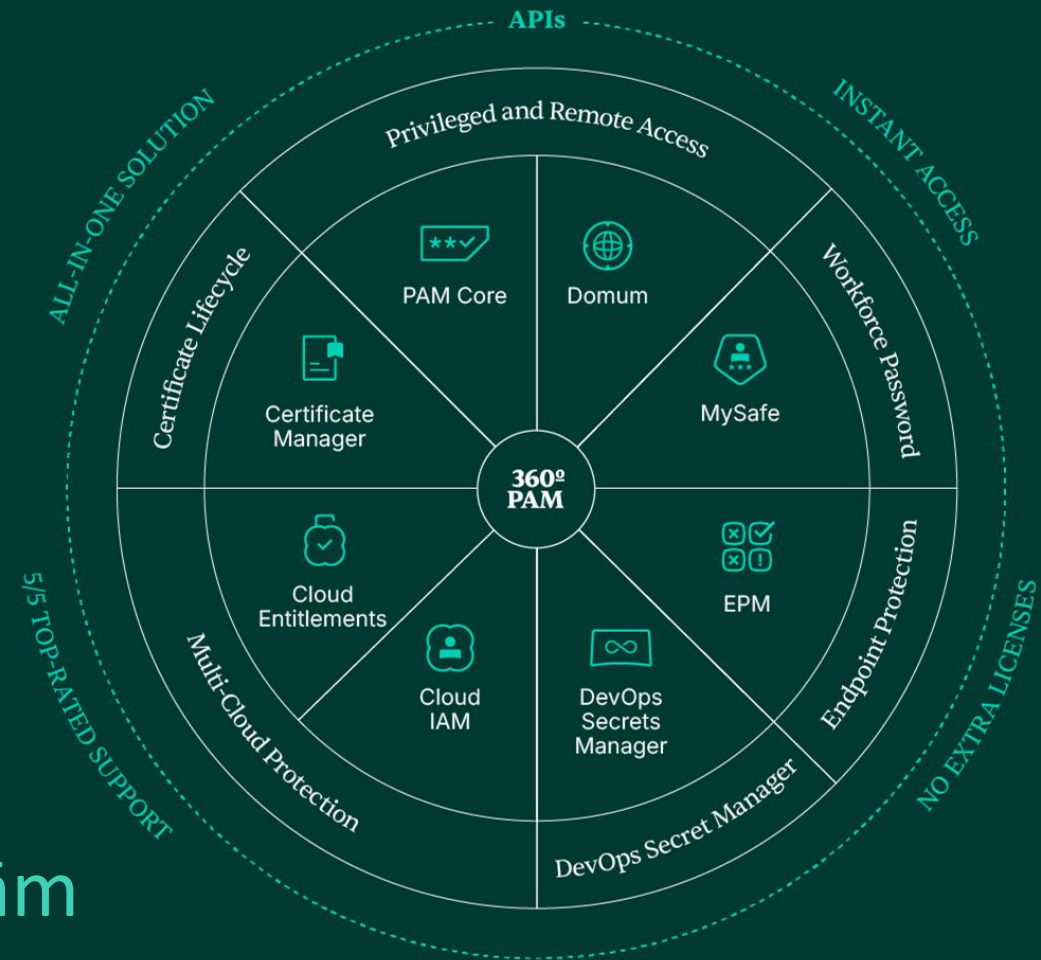
Biznesa riski un grūtības	Privilēģētas un jutīgas piekļuves veidi	Kas tos izmanto vai paļaujas uz tiem	Kur tie pastāv	Kā tiek izmantota piekļuve	Kā tiek nodrošināta piekļuve	Kāpēc tie ir svarīgi biznesam
<ul style="list-style-type: none"> • Kiberuzbrukumi (Ransomware, Data Exfiltration) • Regulējošo iestāžu uzliktās soda naudas (GDPR, NIS2, PCI-DSS) • Biznesa darbības pārtraukumi/darbības pārtraukumi • Trešo personu un piegādes ķēdes pārkāpumi • Iekšnieku draudi / uzbrukumi • Finanšu un darbības krāpšana (BEC, Invoice Fraud) • Reputācijas bojājums un klientu uzticības zaudējums 	<ul style="list-style-type: none"> • Privilēģētie lietotāju konti (Admin, Root, Domain) • Pakalpojumu un lietojumprogrammu konti • Ne-cilvēku un mašīnu identitātes (APIs, Bots, Automation) • Trešo personu piekļuve (Vendors, MSPs) • Ārkārtas/stikla laušanas konti • DevOps & CI/CD lietotāji • API Keys & Tokens • Legacy sistēmu autentifikācijas dati 	<ul style="list-style-type: none"> • IT & Drošības komandas • Aplikāciju īpašnieki • Izstrādātāji & DevOps • Procesu automatizācijas • Trešo personu pārdevēji • Būvuzņēmēji un partneri • AI/ML Workloads • Galalietotāji (netieši ietekmēti) 	<ul style="list-style-type: none"> • Cloud (IaaS, SaaS, PaaS) • On-Prem Infrastructure • APIs & Mikroservisi • Programmatūras piegādes ķēde • CI/CD Pipelines • Datubāzes • IoT & OT Iekārtas • Datu apstrādes vides 	<ul style="list-style-type: none"> • Administratīvie uzdevumi • Programmatūras ieviešana un atjauninājumi • Piekļuve kritiskajām sistēmām • Automatizācija un integrācija • Attālināta piekļuve (VPN, RDP) • DevOps Pipeline izpilde • Trešo personu apkopes pakalpojumi • Reakcija uz incidentiem un 	<ul style="list-style-type: none"> • Privilēģēto lietotāju piekļuve (PAM) • Identitātes apdraudējumu atklāšana un reaģēšana (ITDR) • Zero Trust • Just-in-Time (JIT) Access • Bezparolles & MFA • Uzvedības analīze • Noslēpumi • API un automatizācijas pārvaldība • Nepārtraukta piekļuve pārskatiem un sertifikātiem 	<ul style="list-style-type: none"> • Biznesa nepārtrauktība un darbības laiks • Samazināta uzbrukuma vektors • Normatīvo aktu ievērošana • Paātrināta mākoņpakalpojumu un digitālā transformācija • Drošās inovācijas (DevOps, MI automatizācijas) • Aizsargāta zīmola reputācija • Uzticamas attiecības ar klientiem un partneriem • Zemākas izmaksas par pārkāpumiem un sodiem

avārijas situācijām

Segura 360° Identitātes aizsardzības platforma

- ✓ Mēs esam neitrāli
- ✓ Mēs esam neatkarīgi
- ✓ Mēs esam saderīgi ar prasībām

Your Complete PAM Platform



Kāpēc **identitāte** ir kļuvusi par galveno uzbrukuma vektoru?

Visbiežāk izmantotie veidi, kā uzbrucēji **kompromitē kontus** un **privilēģijas**?

Identitātes risku nepārtrauktas uzraudzības nozīme. Praktiski soļi un rīki, lai ātri stiprinātu aizsardzību.

p.s.

Q un A



Paldies!



Segura®

info@nodbaltic.lv