SECURITY DAYS

DEFENDING AGAINST IDENTITY-BASED CYBER ATTACKS: HOW SEGURA REDUCES YOUR RISK

Joseph Carson,
Chief Evangelist & Advisory CISO

Segura® Team

Joseph Carson

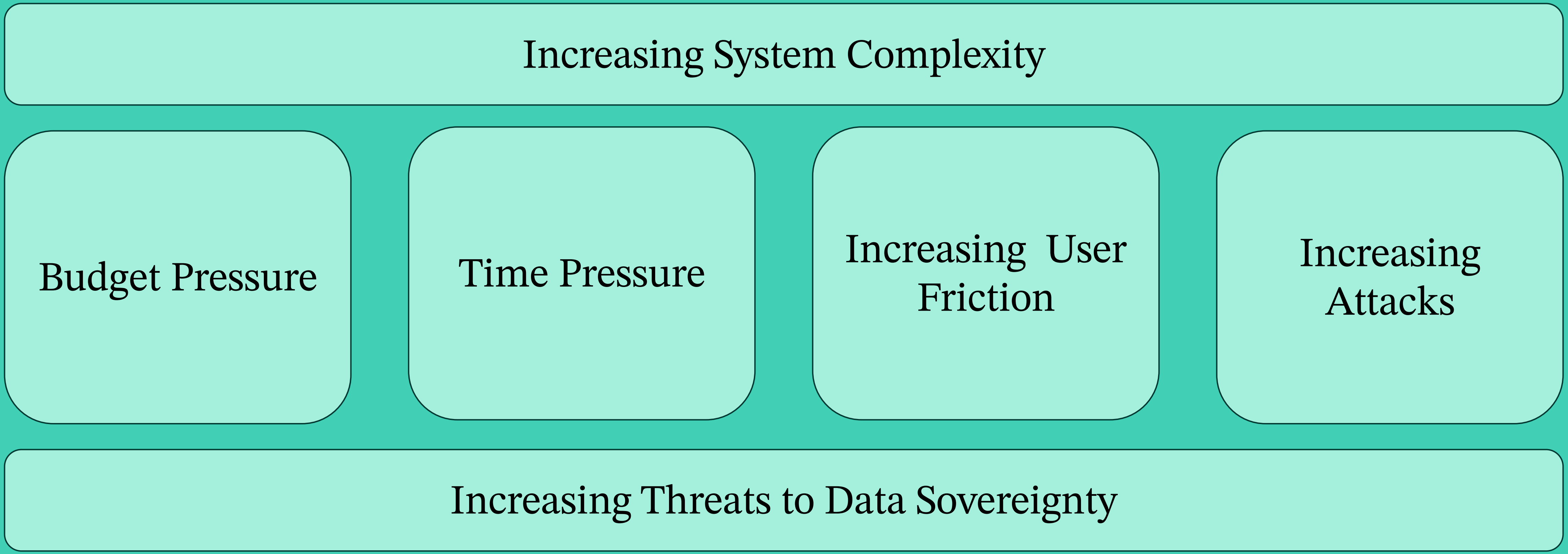
Chief Evangelist at Segura®

Joseph Carson

Chief Security Evangelist & Advisory CISO at Segura®

segura.security

The Anatomy of The Crisis



Increasing System Complexity

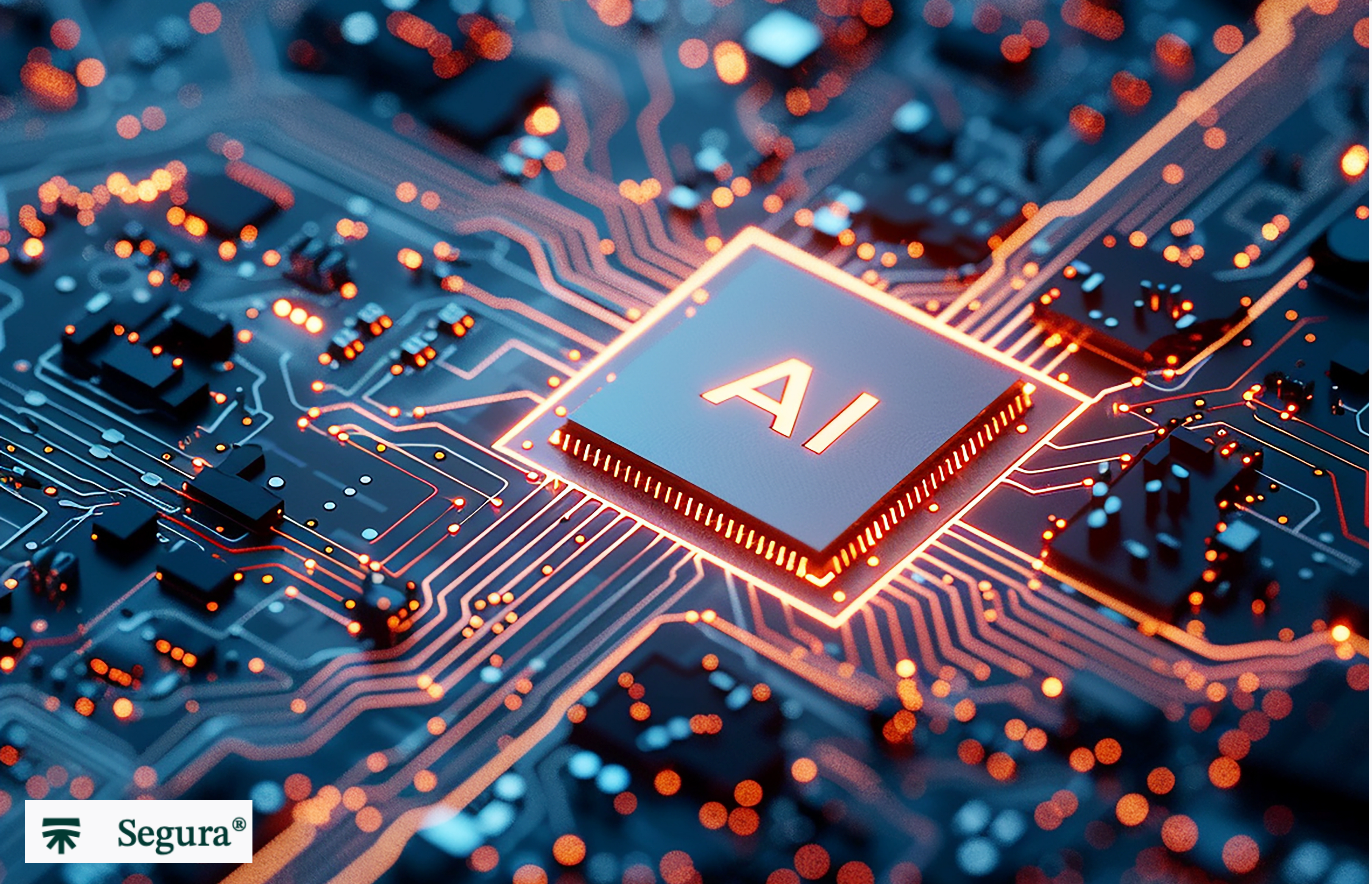
Budget Pressure

Time Pressure

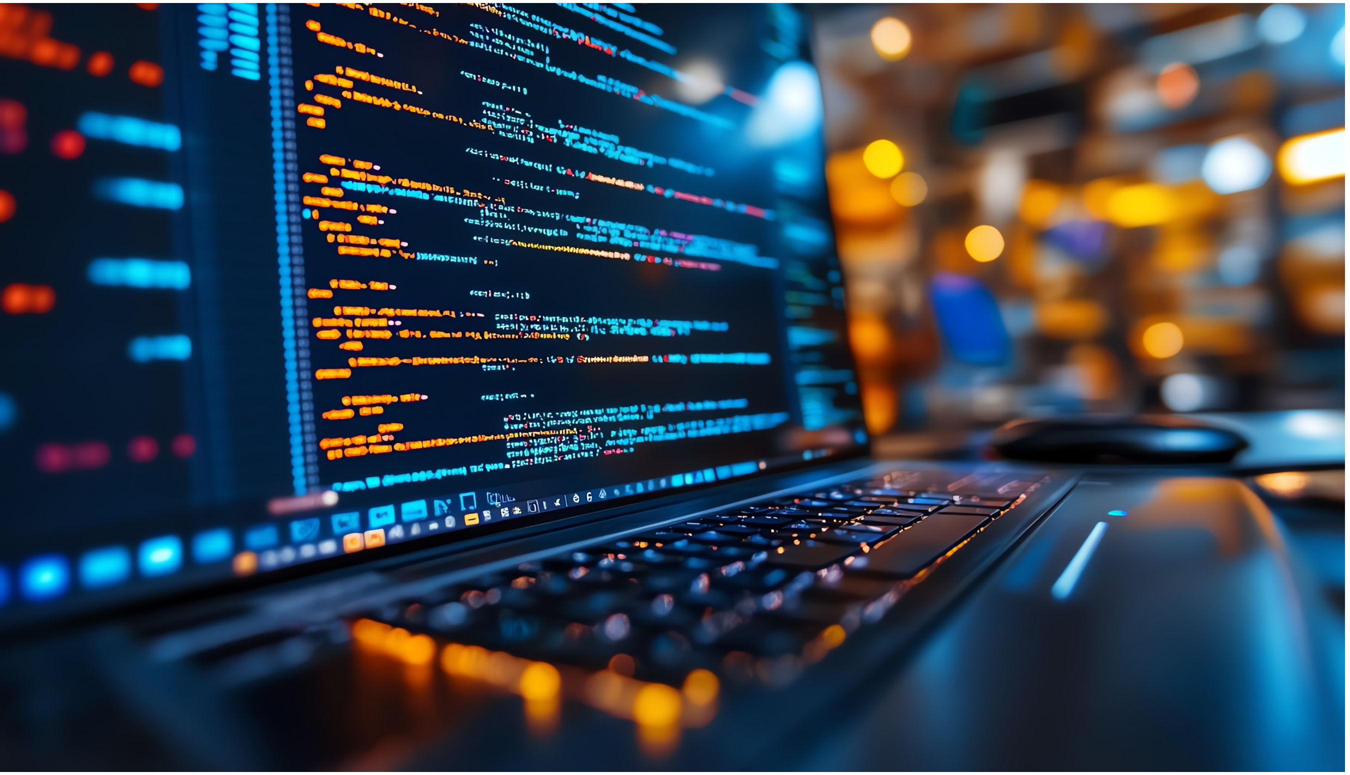
Increasing User Friction

Increasing Attacks

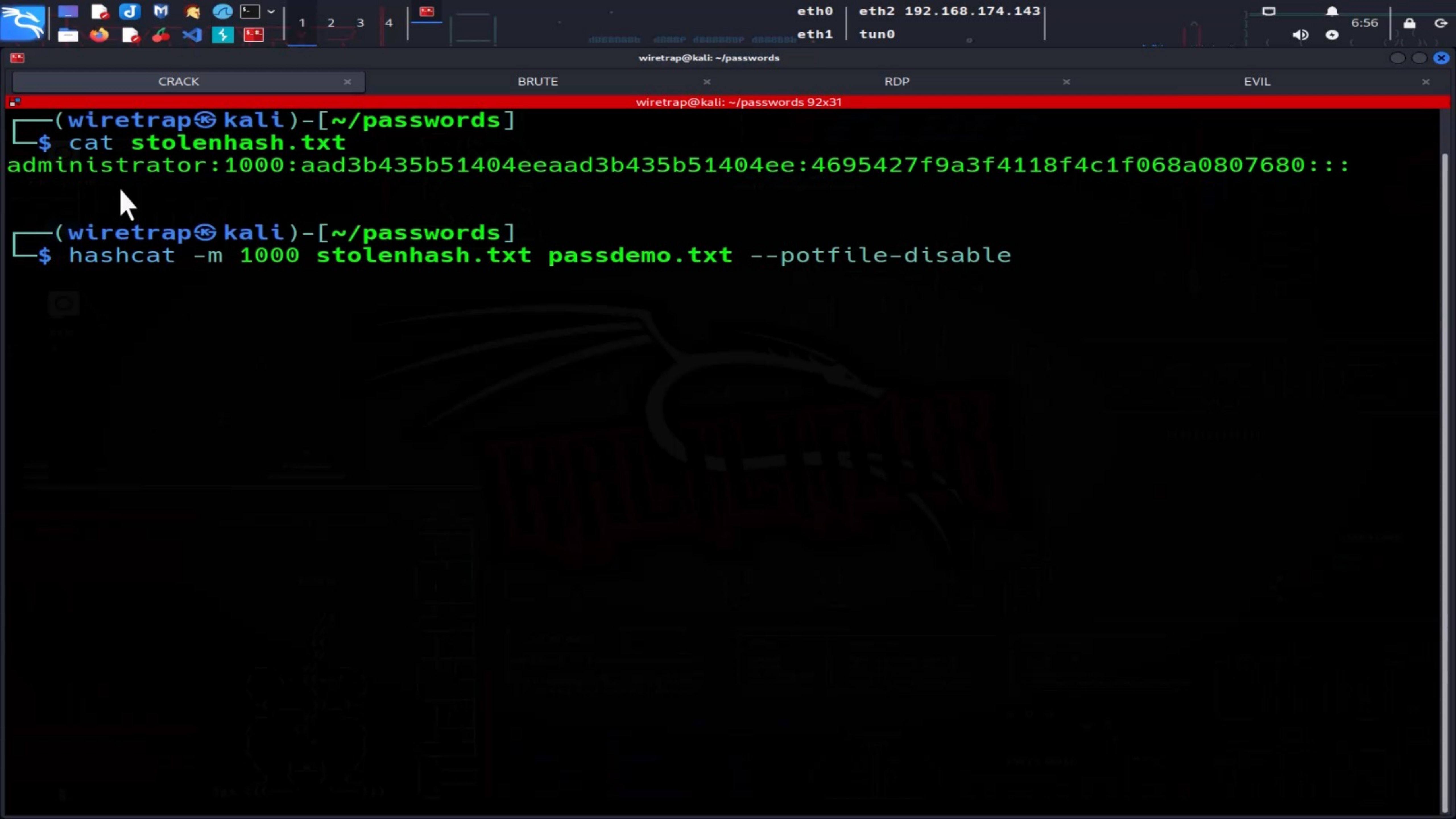
Increasing Threats to Data Sovereignty


AI
Segura®

Attack Path Techniques

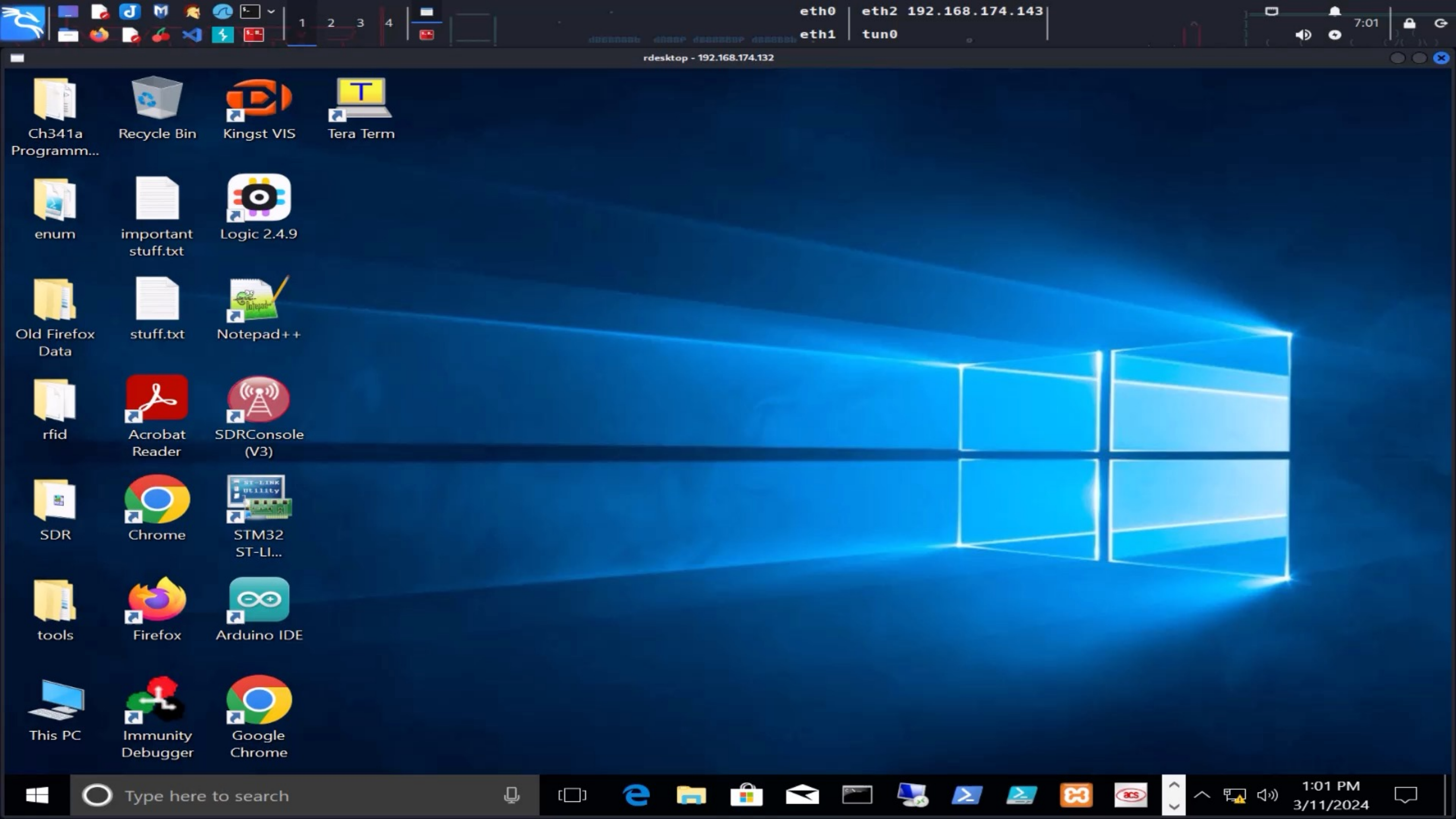


- OSINT
- Enumeration
- Vulnerability Discovery
- Exploit Creation
- Initial Access
- Remote Command Execution (RCE)
- Persistence
- Foothold Enumeration
- Privilege Escalation
- Lateral Movement
- Data Exfiltration



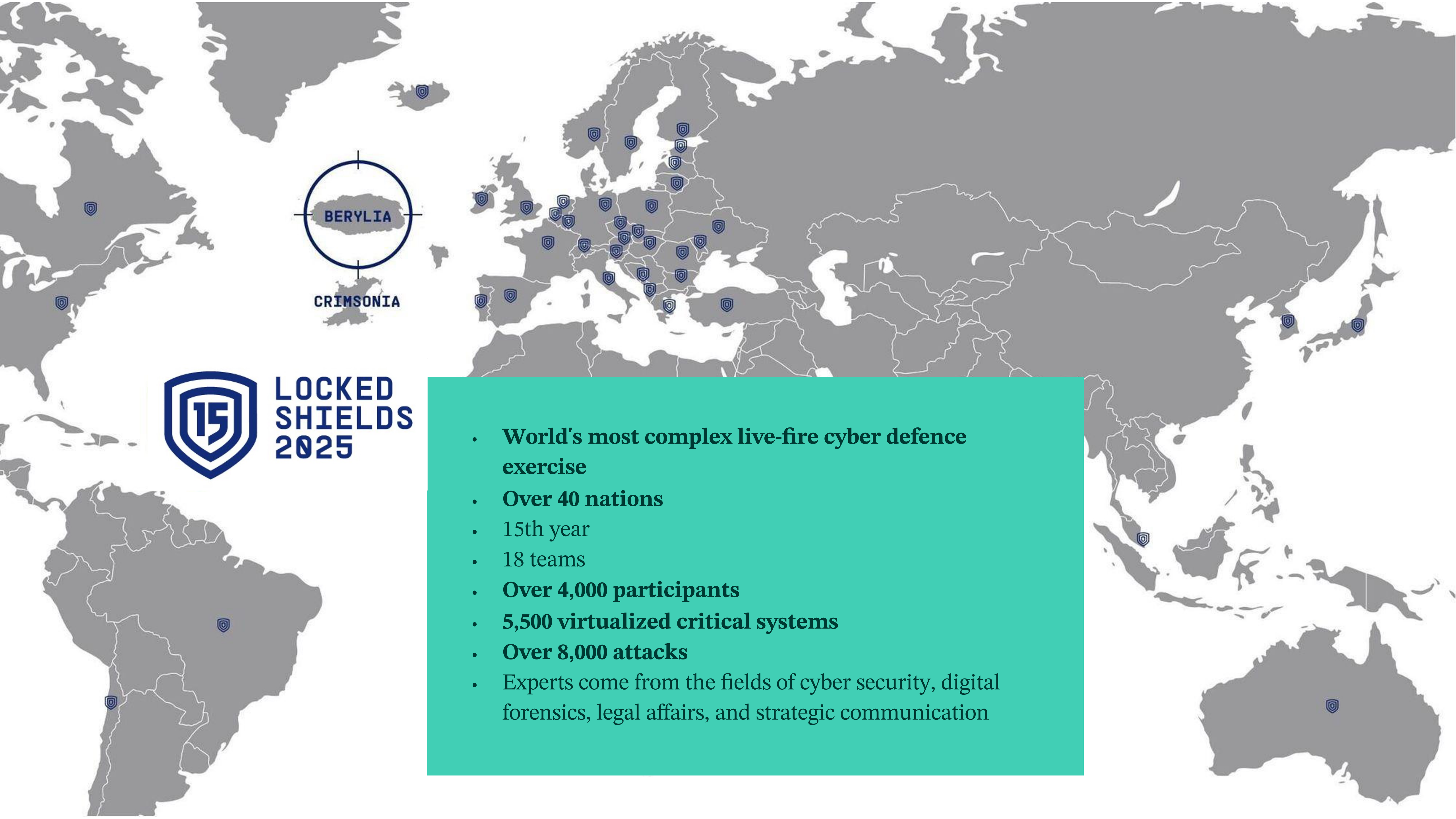
```
┌──(wiretrap㉿kali)-[~/passwords]
└─$ cat stolenhash.txt
administrator:1000:aad3b435b51404eeaad3b435b51404ee:4695427f9a3f4118f4c1f068a0807680:::


┌──(wiretrap㉿kali)-[~/passwords]
└─$ hashcat -m 1000 stolenhash.txt passdemo.txt --potfile-disable
```


1
2
3
4
eth0
eth1
eth2 192.168.174.143
tun0
7:01
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
Type here to search
1:01 PM
3/11/2024

NATO Locked Shields is the world's largest live-fire cyber defense exercise where 40+ nations protect critical infrastructure against thousands of sophisticated attacks in real-time.

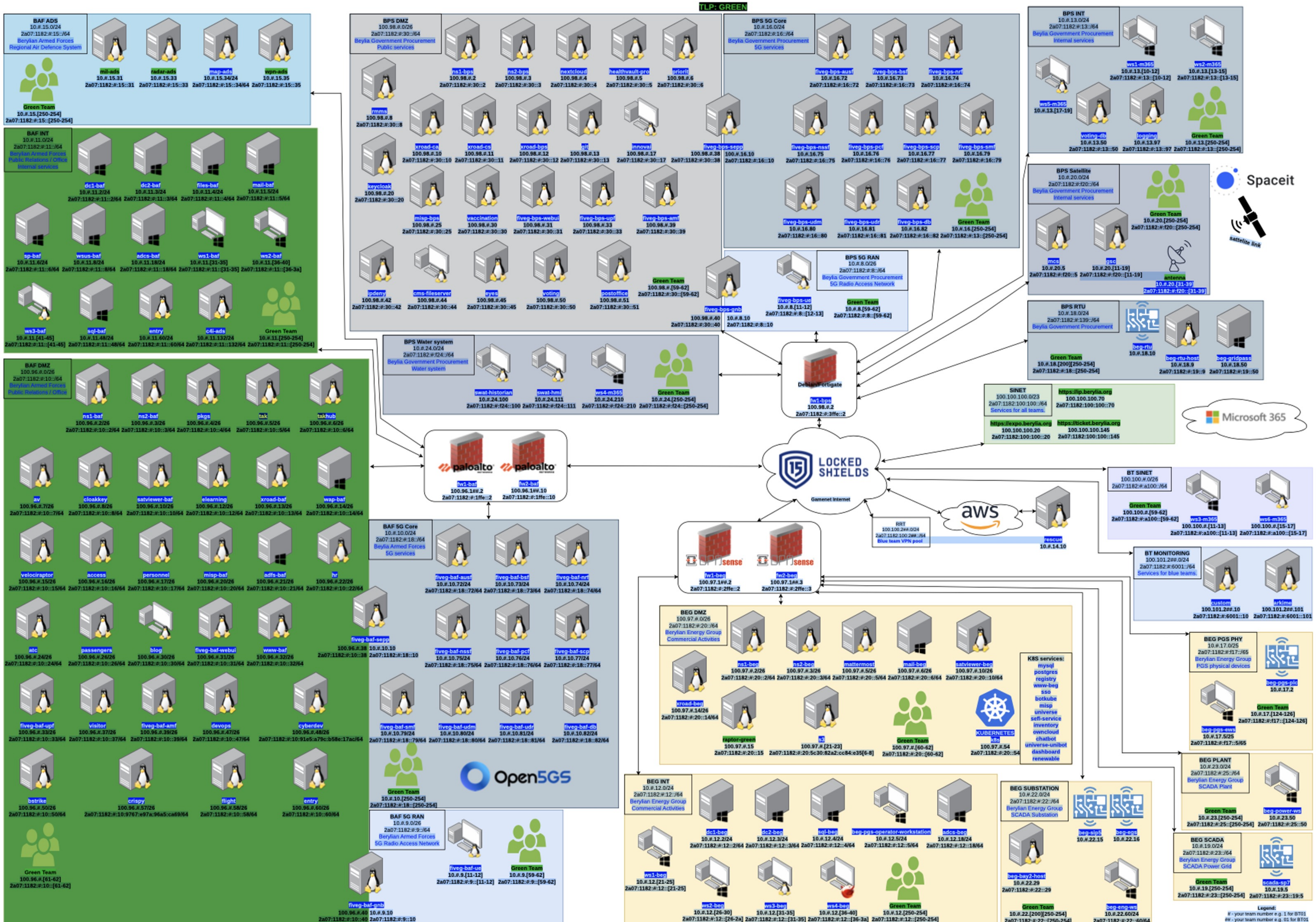
Segura provided Identity and Access Security.

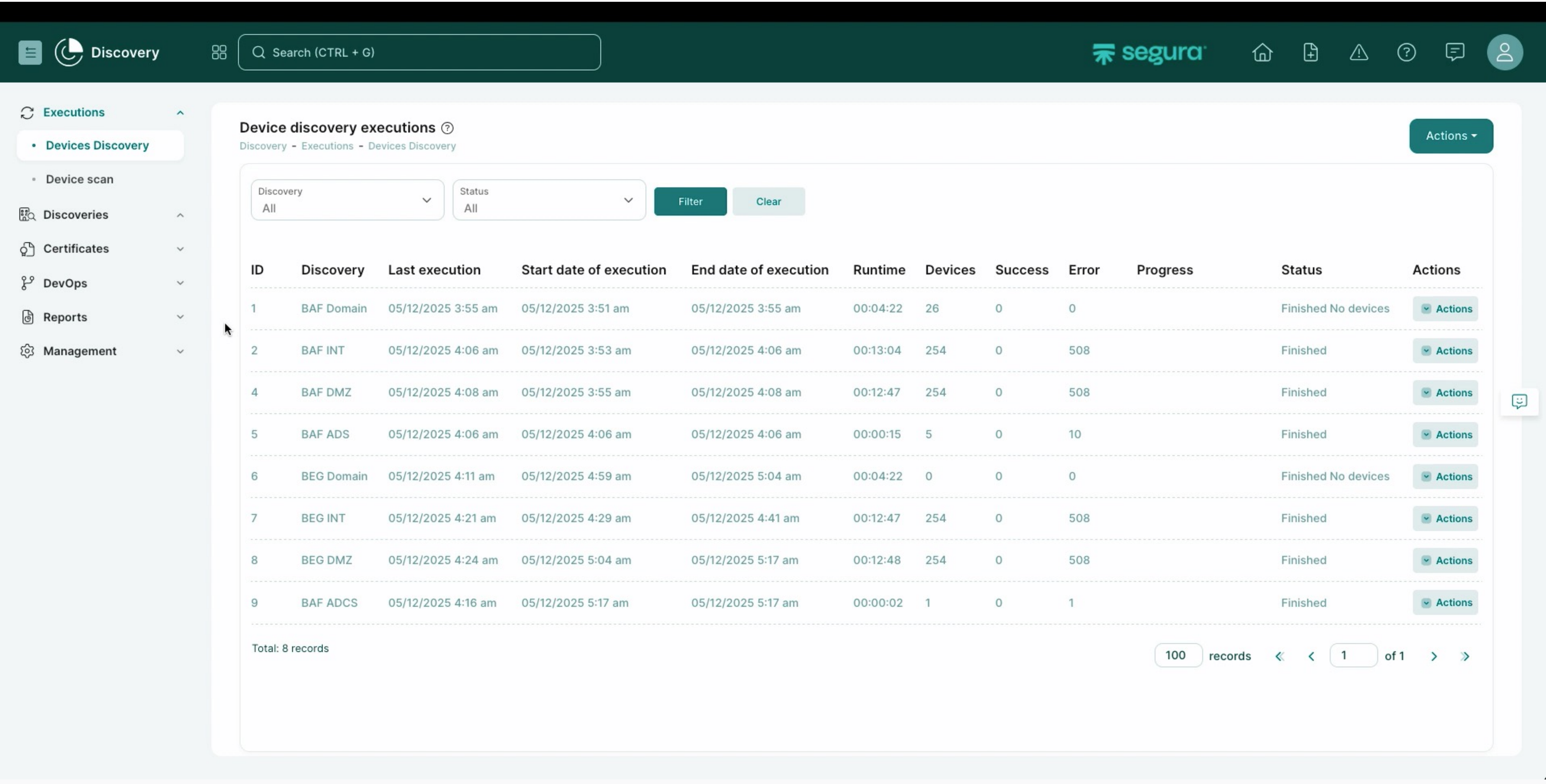


15 LOCKED SHIELDS 2025

- **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

TLP: GREEN


BAF ADS
10.#.15.0/24
2a07:1182:#:15::/64
Berylian Armed Forces
Regional Air Defence System
mil-ads 10.#.15.31 2a07:1182:#:15::31
radar-ads 10.#.15.33 2a07:1182:#:15::33
map-ads 10.#.15.34/24 2a07:1182:#:15::34/64
wpn-ads 10.#.15.35 2a07:1182:#:15::35
Green Team 10.#.15.[250-254] 2a07:1182:#:15::[250-254]
BAF INT
10.#.11.0/24
2a07:1182:#:11::/64
Berylian Armed Forces
Public Relations / Office
Internal services
dc1-baf 10.#.11.2/24 2a07:1182:#:11::2/64
dc2-baf 10.#.11.3/24 2a07:1182:#:11::3/64
files-baf 10.#.11.4/24 2a07:1182:#:11::4/64
mail-baf 10.#.11.5/24 2a07:1182:#:11::5/64
sp-baf 10.#.11.6/24 2a07:1182:#:11::6/64
wsus-baf 10.#.11.8/24 2a07:1182:#:11::8/64
adcs-baf 10.#.11.18/24 2a07:1182:#:11::18/64
ws1-baf 10.#.11.[31-35] 2a07:1182:#:11::[31-35]
ws2-baf 10.#.11.[36-40] 2a07:1182:#:11::[36-3a]
ws3-baf 10.#.11.[41-45] 2a07:1182:#:11::[41-45]
sql-baf 10.#.11.48/24 2a07:1182:#:11::48/64
entry 10.#.11.60/24 2a07:1182:#:11::60/64
c4i-ads 10.#.11.132/24 2a07:1182:#:11::132/64
Green Team 10.#.11.[250-254] 2a07:1182:#:11::[250-254]
BAF DMZ
100.96.#.0/26
2a07:1182:#:10::/64
Berylian Armed Forces
Public Relations / Office
ns1-baf 100.96.#.2/26 2a07:1182:#:10::2/64
ns2-baf 100.96.#.3/26 2a07:1182:#:10::3/64
pkgs 100.96.#.4/26 2a07:1182:#:10::4/64
tak 100.96.#.5/26 2a07:1182:#:10::5/64
takhub 100.96.#.6/26 2a07:1182:#:10::6/64
av 100.96.#.7/26 2a07:1182:#:10::7/64
cloakkey 100.96.#.8/26 2a07:1182:#:10::8/64
satviewer-baf 100.96.#.10/26 2a07:1182:#:10::10/64
elearning 100.96.#.12/26 2a07:1182:#:10::12/64
xroad-baf 100.96.#.13/26 2a07:1182:#:10::13/64
wap-baf 100.96.#.14/26 2a07:1182:#:10::14/64
velociraptor 100.96.#.15/26 2a07:1182:#:10::15/64
access 100.96.#.16/26 2a07:1182:#:10::16/64
personnel 100.96.#.17/26 2a07:1182:#:10::17/64
misp-baf 100.96.#.20/26 2a07:1182:#:10::20/64
adfs-baf 100.96.#.21/26 2a07:1182:#:10::21/64
hr 100.96.#.22/26 2a07:1182:#:10::22/64
atc 100.96.#.24/26 2a07:1182:#:10::24/64
passengers 100.96.#.26/26 2a07:1182:#:10::26/64
blog 100.96.#.30/26 2a07:1182:#:10::30/64
fiveg-baf-webui 100.96.#.31/26 2a07:1182:#:10::31/64
www-baf 100.96.#.32/26 2a07:1182:#:10::32/64
fiveg-baf-sepp 100.96.#.38 2a07:1182:#:10::38 10.#.10.10 2a07:1182:#:18::10
fiveg-baf-upf 100.96.#.33/26 2a07:1182:#:10::33/64
visitor 100.96.#.37/26 2a07:1182:#:10::37/64
fiveg-baf-amf 100.96.#.39/26 2a07:1182:#:10::39/64
devops 100.96.#.47/26 2a07:1182:#:10::47/64
cyberdev 100.96.#.48/26 2a07:1182:#:10:91e5:a79c:b58e:17ac/64
bstrike 100.96.#.50/26 2a07:1182:#:10::50/64
crispy 100.96.#.57/26 2a07:1182:#:10:9767:e97a:96a5:ca69/64
flight 100.96.#.58/26 2a07:1182:#:10::58/64
entry 100.96.#.60/26 2a07:1182:#:10::60/64
Green Team 100.96.#.[61-62] 2a07:1182:#:10::[61-62]
fiveg-baf-gnb 100.96.#.40 2a07:1182:#:10::40 10.#.9.10 2a07:1182:#:9::10
BAF 5G Core
10.#.10.0/24
2a07:1182:#:18::/64
Beylia Armed Forces
5G services
fiveg-baf-ausf 10.#.10.72/24 2a07:1182:#:18::72/64
fiveg-baf-bsf 10.#.10.73/24 2a07:1182:#:18::73/64
fiveg-baf-nrf 10.#.10.74/24 2a07:1182:#:18::74/64
fiveg-baf-nssf 10.#.10.75/24 2a07:1182:#:18::75/64
fiveg-baf-pcf 10.#.10.76/24 2a07:1182:#:18::76/64
fiveg-baf-scp 10.#.10.77/24 2a07:1182:#:18::77/64
fiveg-baf-smf 10.#.10.79/24 2a07:1182:#:18::79/64
fiveg-baf-udm 10.#.10.80/24 2a07:1182:#:18::80/64
fiveg-baf-udr 10.#.10.81/24 2a07:1182:#:18::81/64
fiveg-baf-db 10.#.10.82/24 2a07:1182:#:18::82/64
Green Team 10.#.10.[250-254] 2a07:1182:#:18::[250-254]
Open5GS
BAF 5G RAN
10.#.9.0/26
2a07:1182:#:9::/64
Berylian Armed Forces
5G Radio Access Network
fiveg-baf-ue 10.#.9.[11-12] 2a07:1182:#:9::[11-12]
Green Team 10.#.9.[59-62] 2a07:1182:#:9::[59-62]
BPS DMZ
100.98.#.0/26
2a07:1182:#:30::/64
Beylia Government Procurement
Public services
ns1-bps 100.98.#.2 2a07:1182:#:30::2
ns2-bps 100.98.#.3 2a07:1182:#:30::3
nextcloud 100.98.#.4 2a07:1182:#:30::4
healthvault-pro 100.98.#.5 2a07:1182:#:30::5
priorit 100.98.#.6 2a07:1182:#:30::6
rmms 100.98.#.8 2a07:1182:#:30::8
xroad-ca 100.98.#.10 2a07:1182:#:30::10
xroad-cs 100.98.#.11 2a07:1182:#:30::11
xroad-bps 100.98.#.12 2a07:1182:#:30::12
git 100.98.#.13 2a07:1182:#:30::13
innovai 100.98.#.17 2a07:1182:#:30::17
fiveg-bps-sepp 100.98.#.38 2a07:1182:#:30::38 100.#.16.10 2a07:1182:#:16::10
keycloak 100.98.#.20 2a07:1182:#:30::20
misp-bps 100.98.#.25 2a07:1182:#:30::25
vaccination 100.98.#.30 2a07:1182:#:30::30
fiveg-bps-webui 100.98.#.31 2a07:1182:#:30::31
fiveg-bps-upf 100.98.#.33 2a07:1182:#:30::33
fiveg-bps-amf 100.98.#.39 2a07:1182:#:30::39
ipdeny 100.98.#.42 2a07:1182:#:30::42
cms-fileserver 100.98.#.44 2a07:1182:#:30::44
eyes 100.98.#.45 2a07:1182:#:30::45
voting 100.98.#.50 2a07:1182:#:30::50
postoffice 100.98.#.51 2a07:1182:#:30::51
Green Team 100.98.#.[59-62] 2a07:1182:#:30::[59-62]
fiveg-bps-gnb 100.98.#.40 2a07:1182:#:30::40 10.#.8.10 2a07:1182:#:8::10
BPS 5G Core
10.#.16.0/24
2a07:1182:#:16::/64
Beylia Government Procurement
5G services
fiveg-bps-ausf 10.#.16.72 2a07:1182:#:16::72
fiveg-bps-bsf 10.#.16.73 2a07:1182:#:16::73
fiveg-bps-nrf 10.#.16.74 2a07:1182:#:16::74
fiveg-bps-nssf 10.#.16.75 2a07:1182:#:16::75
fiveg-bps-pcf 10.#.16.76 2a07:1182:#:16::76
fiveg-bps-scp 10.#.16.77 2a07:1182:#:16::77
fiveg-bps-smf 10.#.16.79 2a07:1182:#:16::79
fiveg-bps-udm 10.#.16.80 2a07:1182:#:16::80
fiveg-bps-udr 10.#.16.81 2a07:1182:#:16::81
fiveg-bps-db 10.#.16.82 2a07:1182:#:16::82
Green Team 10.#.16.[250-254] 2a07:1182:#:13::[250-254]
BPS 5G RAN
10.#.8.0/26
2a07:1182:#:8::/64
Beylia Government Procurement
5G Radio Access Network
fiveg-bps-ue 10.#.8.[11-12] 2a07:1182:#:8::[12-13]
Green Team 10.#.8.[59-62] 2a07:1182:#:8::[59-62]
BPS Water system
10.#.24.0/24
2a07:1182:#:f24::/64
Beylia Government Procurement
Water system
swat-historian 10.#.24.100 2a07:1182:#:f24::100
swat-hmi 10.#.24.111 2a07:1182:#:f24::111
ws4-m365 10.#.24.210 2a07:1182:#:f24::210
Green Team 10.#.24.[250-254] 2a07:1182:#:f24::[250-254]
Debian/Fortigate
fw1-bps 100.98.#.2 2a07:1182:#:3ffe::2
paloalto
fw1-baf 100.96.1##.2 2a07:1182:#:1ffe::2
paloalto
fw2-baf 100.96.1##.10 2a07:1182:#:1ffe::10
LOCKED SHIELDS
Gamenet Internet
OPNsense
fw1-beg 100.97.1##.2 2a07:1182:#:2ffe::2
OPNsense
fw2-beg 100.97.1##.3 2a07:1182:#:2ffe::3
BPS INT
10.#.13.0/24
2a07:1182:#:13::/64
Beylia Government Procurement
Internal services
ws1-m365 10.#.13.[10-12] 2a07:1182:#:13::[10-12]
ws2-m365 10.#.13.[13-15] 2a07:1182:#:13::[13-15]
ws5-m365 10.#.13.[17-19]
voting-db 10.#.13.50 2a07:1182:#:13::50
logging 10.#.13.97 2a07:1182:#:13::97
Green Team 10.#.13.[250-254] 2a07:1182:#:13::[250-254]
BPS Satellite
10.#.20.0/24
2a07:1182:#:f20::/64
Beylia Government Procurement
Internal services
Green Team 10.#.20.[250-254] 2a07:1182:#:f20::[250-254]
mcs 10.#.20.5 2a07:1182:#:f20::5
gsc 10.#.20.[11-19] 2a07:1182:#:f20::[11-19]
antenna 10.#.20.[31-39] 2a07:1182:#:f20::[31-39]
Spaceit
sattelite link
BPS RTU
10.#.18.0/24
2a07:1182:#:139::/64
Beylia Government Procurement
Green Team 10.#.18.[200][250-254] 2a07:1182:#:18::[250-254]
beg-rtu 10.#.18.10
beg-rtu-host 10.#.18.9 2a07:1182:#:19::9
beg-gridpass 10.#.18.50 2a07:1182:#:19::50
SINET
100.100.100.0/23
2a07:1182:100:100::/64
Services for all teams.
https://ip.berylia.org 100.100.100.70 2a07:1182:100:100::70
https://expo.berylia.org 100.100.100.20 2a07:1182:100:100::20
https://ticket.berylia.org 100.100.100.145 2a07:1182:100:100::145
Microsoft 365
BT SINET
100.100.#.0/26
2a07:1182:#:a100::/64
Green Team 100.100.#.[59-62] 2a07:1182:#:a100::[59-62]
ws3-m365 100.100.#.[11-13] 2a07:1182:#:a100::[11-13]
ws6-m365 100.100.#.[15-17] 2a07:1182:#:a100::[15-17]
aws
rescue 10.#.14.10
RRT
100.100.2##.0/24
2a07:1182:100:2##::/64
Blue team VPN pool
BT MONITORING
100.101.2##.0/24
2a07:1182:#:6001::/64
Services for blue teams.
custom 100.101.2##.10 2a07:1182:#:6001::10
arkime 100.101.2##.101 2a07:1182:#:6001::101
BEG DMZ
100.97.#.0/26
2a07:1182:#:20::/64
Berylian Energy Group
Commercial Activities
ns1-beg 100.97.#.2/26 2a07:1182:#:20::2/64
ns2-beg 100.97.#.3/26 2a07:1182:#:20::3/64
mattermost 100.97.#.5/26 2a07:1182:#:20::5/64
mail-beg 100.97.#.6/26 2a07:1182:#:20::6/64
satviewer-beg 100.97.#.10/26 2a07:1182:#:20::10/64
xroad-beg 100.97.#.14/26 2a07:1182:#:20::14/64
raptor-green 100.97.#.15 2a07:1182:#:20::15
s3 100.97.#.[21-23] 2a07:1182:#:20:5c30:82a2:cc84:e35[6-8]
Green Team 100.97.#.[60-62] 2a07:1182:#:20::[60-62]
KUBERNETES k8s 100.97.#.54 2a07:1182:#:20::54
K8S services:
mysql
postgres
registry
www-beg
sso
botkube
misp
universe
sefl-service
inventory
owncloud
chatbot
universe-unibot
dashboard
renewable
BEG INT
10.#.12.0/24
2a07:1182:#:12::/64
Berylian Energy Group
Commercial Activities
dc1-beg 10.#.12.2/24 2a07:1182:#:12::2/64
dc2-beg 10.#.12.3/24 2a07:1182:#:12::3/64
sql-beg 10.#.12.4/24 2a07:1182:#:12::4/64
beg-pgs-operator-workstation 10.#.12.5/24 2a07:1182:#:12::5/64
adcs-beg 10.#.12.18/24 2a07:1182:#:12::18/64
ws1-beg 10.#.12.[21-25] 2a07:1182:#:12::[21-25]
ws2-beg 10.#.12.[26-30] 2a07:1182:#:12::[26-2a]
ws3-beg 10.#.12.[31-35] 2a07:1182:#:12::[31-35]
ws4-beg 10.#.12.[36-40] 2a07:1182:#:12::[36-3a]
Green Team 10.#.12.[250-254] 2a07:1182:#:12::[250-254]
BEG SUBSTATION
10.#.22.0/24
2a07:1182:#:22::/64
Berylian Energy Group
SCADA Substation
beg-sip5 10.#.22.15
beg-egs 10.#.22.16
beg-bay2-host 10.#.22.29 2a07:1182:#:22::29
Green Team 10.#.22.[200][250-254] 2a07:1182:#:22::[250-254]
beg-eng-ws 10.#.22.60/24 2a07:1182:#:22::60/64
BEG PGS PHY
10.#.17.0/25
2a07:1182:#:f17::/65
Berylian Energy Group
PGS physical devices
beg-pgs-plc 10.#.17.2
Green Team 10.#.17.[124-126] 2a07:1182:#:f17::[124-126]
beg-pgs-ews 10.#.17.5/25 2a07:1182:#:f17::5/65
BEG PLANT
10.#.23.0/24
2a07:1182:#:25::/64
Berylian Energy Group
SCADA Plant
Green Team 10.#.23.[250-254] 2a07:1182:#:25::[250-254]
beg-power-ws 10.#.23.50 2a07:1182:#:25::50
BEG SCADA
10.#.19.0/24
2a07:1182:#:23::/64
Berylian Energy Group
SCADA Power Grid
Green Team 10.#.19.[250-254] 2a07:1182:#:23::[250-254]
scada-sp7 10.#.19.5 2a07:1182:#:23::19:5
Legend:
# - your team number e.g. 1 for BT01
## - your team number e.g. 01 for BT01



Device discovery executions

Discovery - Executions - Devices Discovery

Discovery: All

Status: All

ID	Discovery	Last execution	Start date of execution	End date of execution	Runtime	Devices	Success	Error	Progress	Status	Actions
1	BAF Domain	05/12/2025 3:55 am	05/12/2025 3:51 am	05/12/2025 3:55 am	00:04:22	26	0	0		Finished No devices	Actions
2	BAF INT	05/12/2025 4:06 am	05/12/2025 3:53 am	05/12/2025 4:06 am	00:13:04	254	0	508		Finished	Actions
4	BAF DMZ	05/12/2025 4:08 am	05/12/2025 3:55 am	05/12/2025 4:08 am	00:12:47	254	0	508		Finished	Actions
5	BAF ADS	05/12/2025 4:06 am	05/12/2025 4:06 am	05/12/2025 4:06 am	00:00:15	5	0	10		Finished	Actions
6	BEG Domain	05/12/2025 4:11 am	05/12/2025 4:59 am	05/12/2025 5:04 am	00:04:22	0	0	0		Finished No devices	Actions
7	BEG INT	05/12/2025 4:21 am	05/12/2025 4:29 am	05/12/2025 4:41 am	00:12:47	254	0	508		Finished	Actions
8	BEG DMZ	05/12/2025 4:24 am	05/12/2025 5:04 am	05/12/2025 5:17 am	00:12:48	254	0	508		Finished	Actions
9	BAF ADCS	05/12/2025 4:16 am	05/12/2025 5:17 am	05/12/2025 5:17 am	00:00:02	1	0	1		Finished	Actions

Total: 8 records

100 records 1 of 1

Segura®

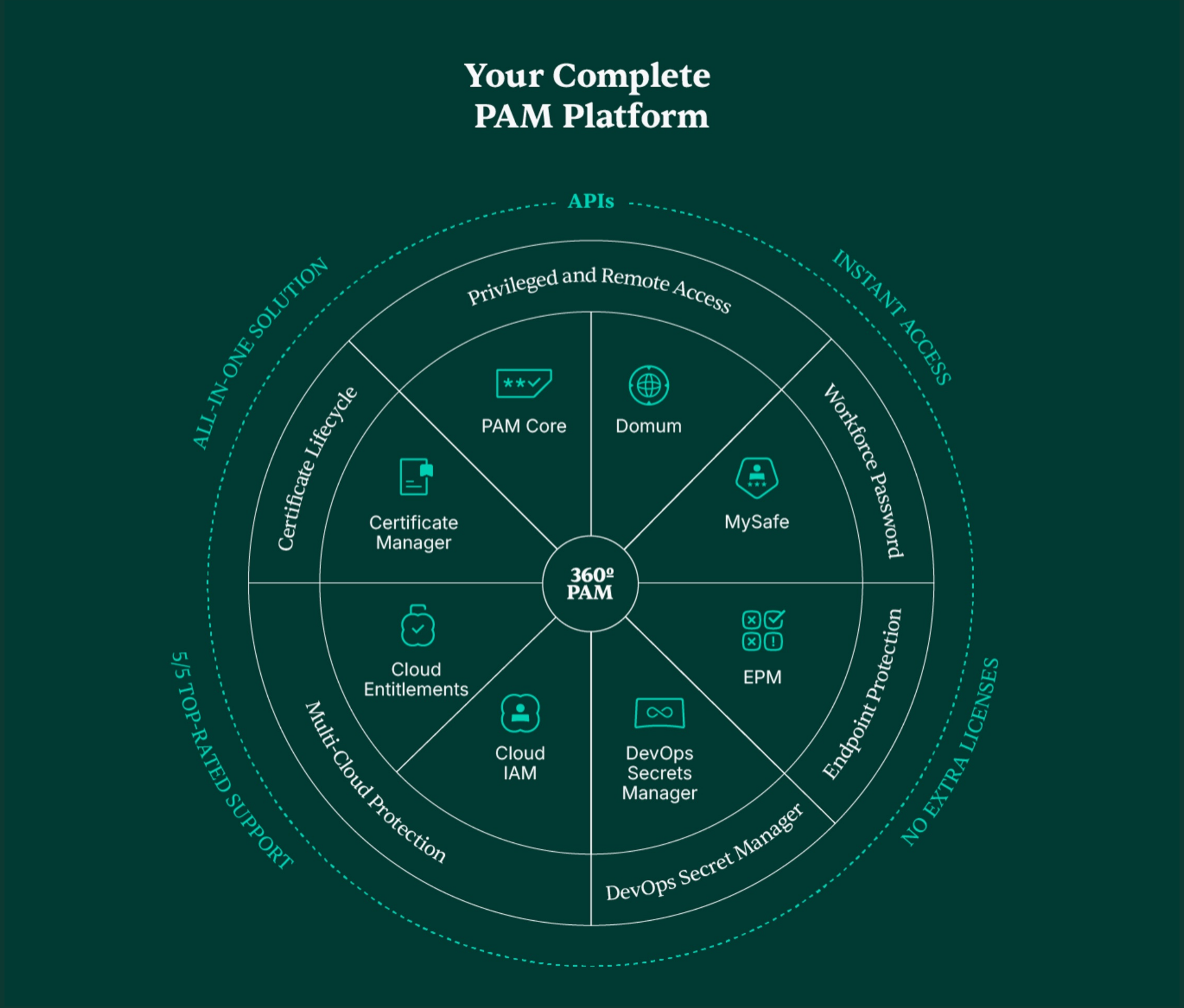
Modern Identity Security & Access Management Matrix

Why It Matters for Business Resilience and Risk Reduction

1. Identity & Access Management
   - Privileged Access Management (PAM) - Secure Usage of Privileged Accounts and Privileged Data
     - Privileged Accounts (Objects)- Secure Vaulting of Privileged Credentials
     - Privileged Data (Target) - Secure Access to Privileged Data

Business Risks & Pains	Types of Privileged & Sensitive Access	Who Uses or Relies on Them	Where They Exist	How Access is Used	How Access is Secured	Why They Are Critical for Business
• Cyber Attacks (Ransomware, Data Exfiltration) • Regulatory Fines (GDPR, NIS2, PCI-DSS) • Business Disruption/Downtime • Third-Party & Supply Chain Breaches • Insider Risks • Financial & Operational Fraud (BEC, Invoice Fraud) • Reputational Damage & Customer Trust Loss	• Privileged User Accounts (Admin, Root, Domain) • Service & Application Accounts • Non-Human & Machine Identities (APIs, Bots, Automation) • Third-Party Access (Vendors, MSPs) • Emergency/Break Glass Accounts • DevOps & CI/CD Credentials • API Keys & Tokens • Legacy Systems Credentials	• IT & Security Teams • Application Owners • Developers & DevOps • Automation Processes • Third-Party Vendors • Contractors & Partners • AI/ML Workloads • End Users (indirectly impacted)	• Cloud (IaaS, SaaS, PaaS) • On-Prem Infrastructure • APIs & Microservices • Software Supply Chain • CI/CD Pipelines • Databases • IoT & OT Devices • Edge Computing Environments	• Administrative Tasks • Software Deployment & Updates • Access to Critical Systems • Automation & Integration • Remote Access (VPN, RDP) • DevOps Pipeline Execution • Third-Party Maintenance • Incident Response & Break Glass	• Privileged Access Management (PAM) • Identity Threat Detection & Response (ITDR) • Zero Trust • Just-in-Time (JIT) Access • Passwordless & MFA • Behavioral Analytics • Secrets Management for APIs & Automation • Continuous Access Reviews & Certifications	• Business Continuity & Uptime • Reduced Attack Surface • Regulatory Compliance • Accelerated Cloud & Digital Transformation • Secure Innovation (DevOps, AI, Automation) • Protected Brand Reputation • Trusted Customer & Partner Relationships • Lower Cost of Breaches & Fines

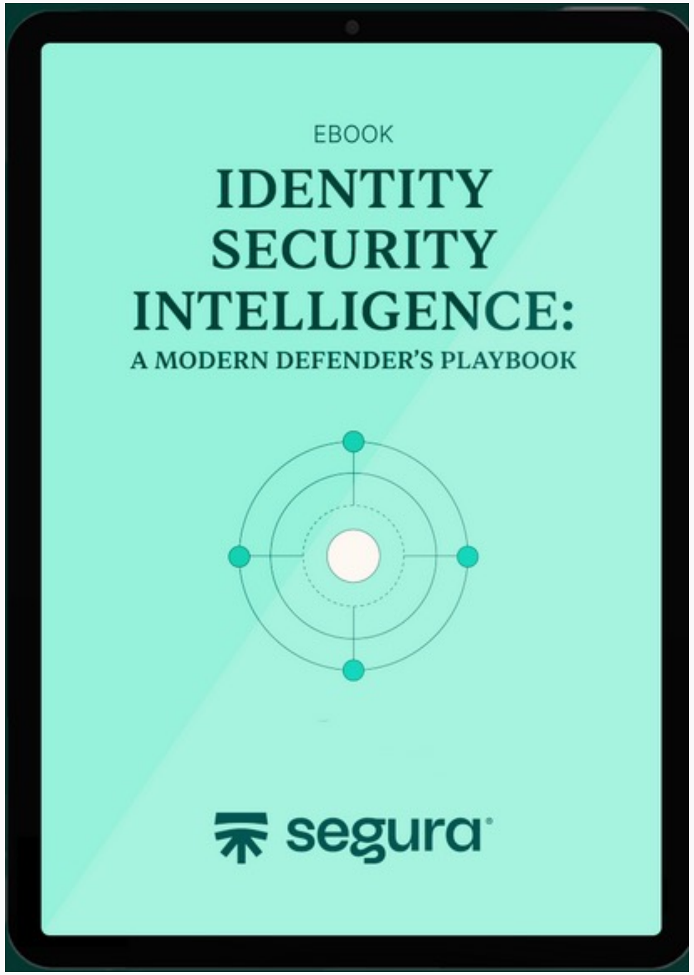
Segura 360° Identity Protection Platform



Segura® Team

Joseph Carson

Chief Evangelist at Segura®



EBOOK

IDENTITY SECURITY INTELLIGENCE:

A MODERN DEFENDER'S PLAYBOOK

segura

Joseph Carson

Chief Security Evangelist &
Advisory CISO at Segura®

segura.security

THANK YOU

Segura®