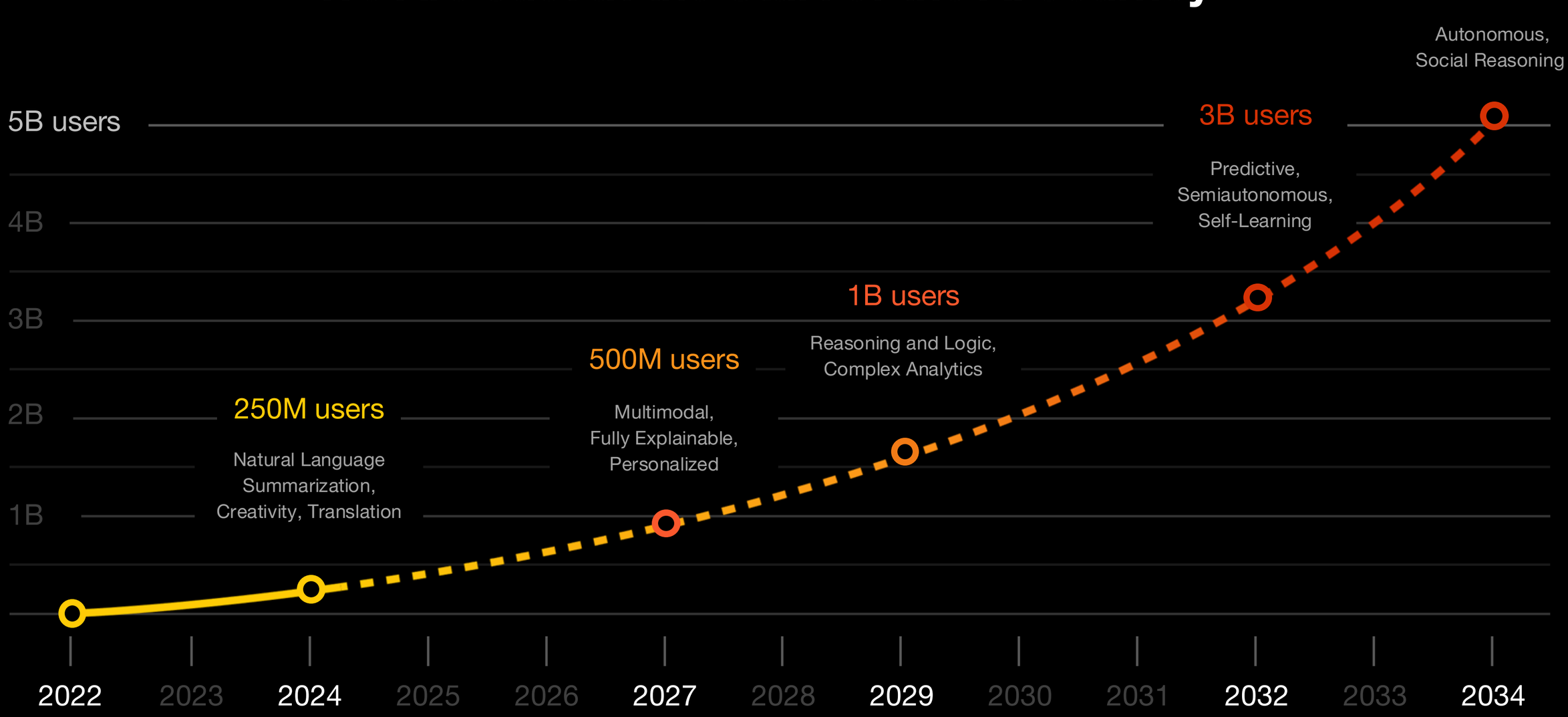
# Prebudenie sa do novej éry kybernetickej bezpečnosti

**Luboš Klokner** | Solution Consultant

May 2025

# We Are Just at the Start of the AI Journey



# Cybersecurity Has Seen Progress Toward Autonomous Security

## Signature-Based Attack Prevention

**IDS → IPS**

## ML-Based Prevention

**AV → EDR**

## Preprogrammed Workflow Automation

**RPA → SOAR**

## Automated Analytics

**Dashboards → AIOps**

# Who will win?

The Hacker News

New AI Tool 'FraudGPT' Emerges, Tailored for Sophisticated Attacks

SC MEDIA

Hacker Steals Credentials by E
on AWS

## A Sneaky Phish Just Grabbed my Mailchimp Mailing List

25 MARCH 2025

You know when you're really jet lagged and really tired and the cogs in your head are just moving that little bit too slow? That's me right now, and the penny has just dropped that a Mailchimp phish has grabbed my credentials, logged into my account and exported the mailing list for this blog. I'm deliberately keeping this post very succinct to ensure the message goes out to my impacted subscribers ASAP, then I'll update the post with more details. But as a quick summary, I woke up in London this morning to the following:


Troy Hunt

Hi, I'm Troy Hunt, I write this blog, run "Have I Been Pwned" and am a Microsoft Regional Director and MVP who travels the world speaking at events and training technology professionals →

WS

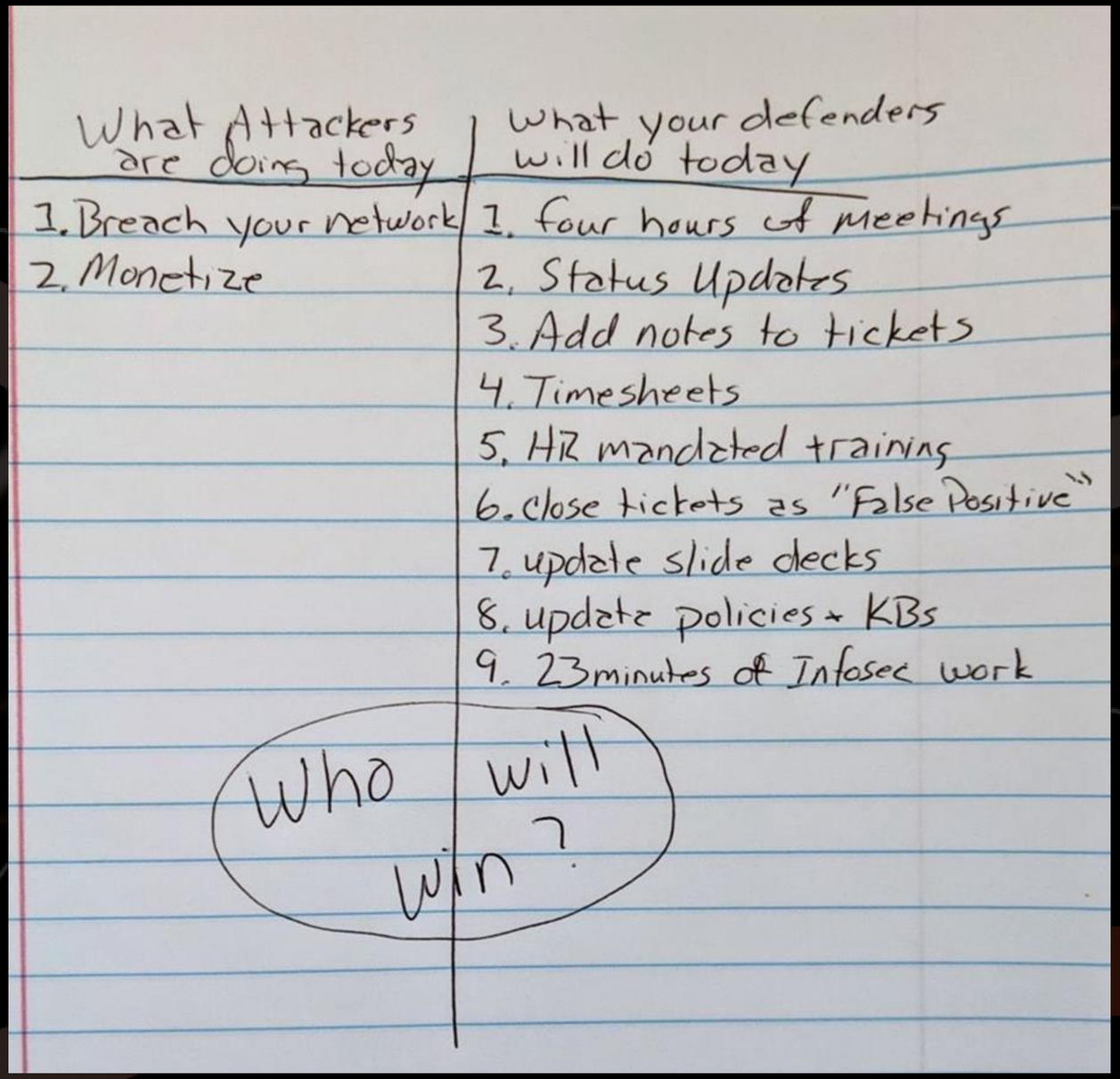
Tool Allows Cybercriminals to Launch
Sophistica ed Cyber Attacks

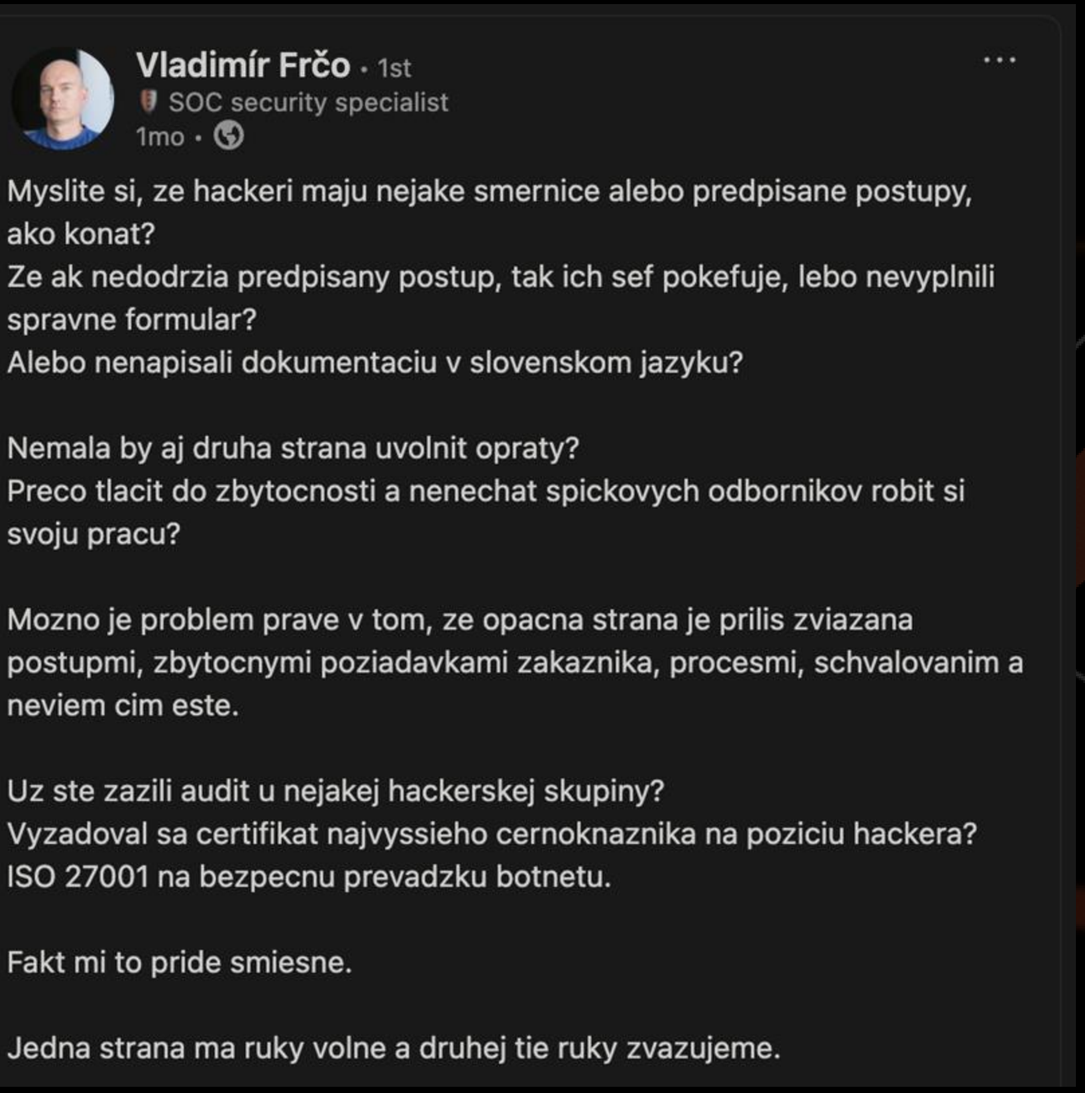


paloalto NETWORKS

# Who will win?

# Who will win?



**Vladimír Frčo** · 1st
SOC security specialist
1mo ·

Myslite si, ze hackeri maju nejake smernice alebo predpisane postupy, ako konat?
Ze ak nedodrzia predpisany postup, tak ich sef pokefuje, lebo nevyplnili spravne formular?
Alebo nenapisali dokumentaciu v slovenskom jazyku?

Nemala by aj druha strana uvolnit opraty?
Preco tlacit do zbytocnosti a nenechat spickovych odbornikov robit si svoju pracu?

Mozno je problem prave v tom, ze opacna strana je prilis zviazana postupmi, zbytocnymi poziadavkami zakaznika, procesmi, schvalovanim a neviem cim este.

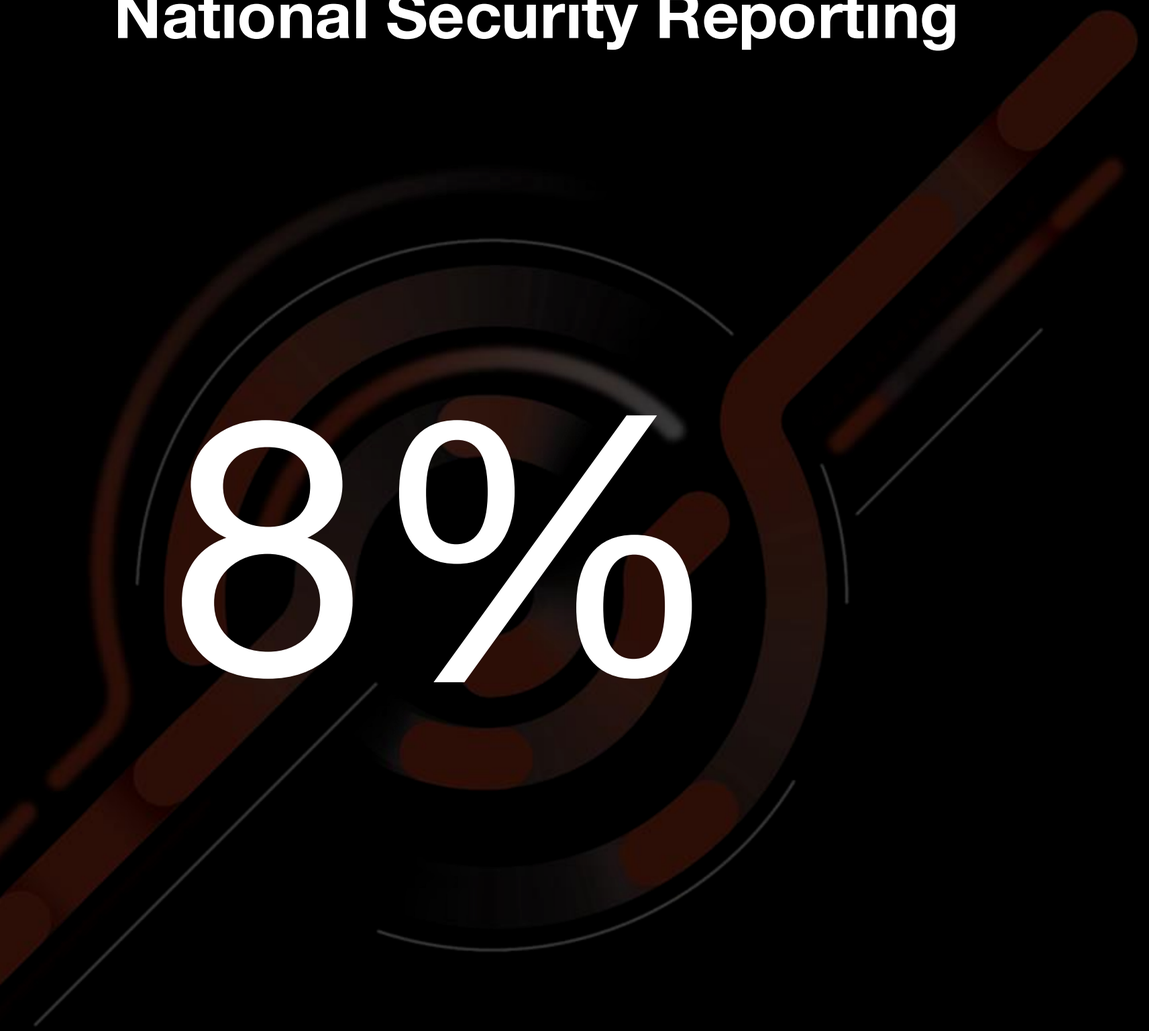
Uz ste zazili audit u nejakej hackerskej skupiny?
Vyzadoval sa certifikat najvyssieho cernoknaznika na poziciu hackera?
ISO 27001 na bezpecnu prevadzku botnetu.

Fakt mi to pride smiesne.

Jedna strana ma ruky volne a druhej tie ruky zvazujeme.

# Last year

# National Security Reporting



# National Security Reporting

Visibility only to…

8%

…compared to Threat Intelligence provided by Palo Alto Networks

# Attack Surface Management

## Post mortem analýza perimetra Katastra

**Martin Fabry**
Critical Infrastructure Cybersecurity Consultant & Owner

January 9, 2025

Dal som si tú námahu spraviť post mortem analýzu perimetra hacknutého Katastra z verejných zdrojov.

Analyzovaný bol IP CIDR rozsah patriaci Katastru 195.28.70.0/25

This is the RIPE Database search service. The objects are in RPSL format. The RIPE Database is subject to Terms and Conditions.

Responsible organisation: Slovanet a.s.
Abuse contact info: abuse00@slovanet.net

```
inetnum:        195.28.70.0 - 195.28.70.175
netname:        GEODESYNET
descr:          Geodesy and Cartography institution of Slovak Republic
country:        SK
admin-c:        LG3103-RIPE
tech-c:         SNET-RIPE
status:         ASSIGNED PA
mnt-by:         SLOVANET-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2007-01-22T11:39:14Z
source:         RIPE# Filtered

route:          195.28.64.0/19
descr:          Slovanet (ViaPVT)
origin:         AS8778
mnt-by:         SLOVANET-MNT
created:        2003-09-22T08:20:32Z
last-modified:  2003-09-22T08:20:32Z
source:         RIPE# Filtered
```

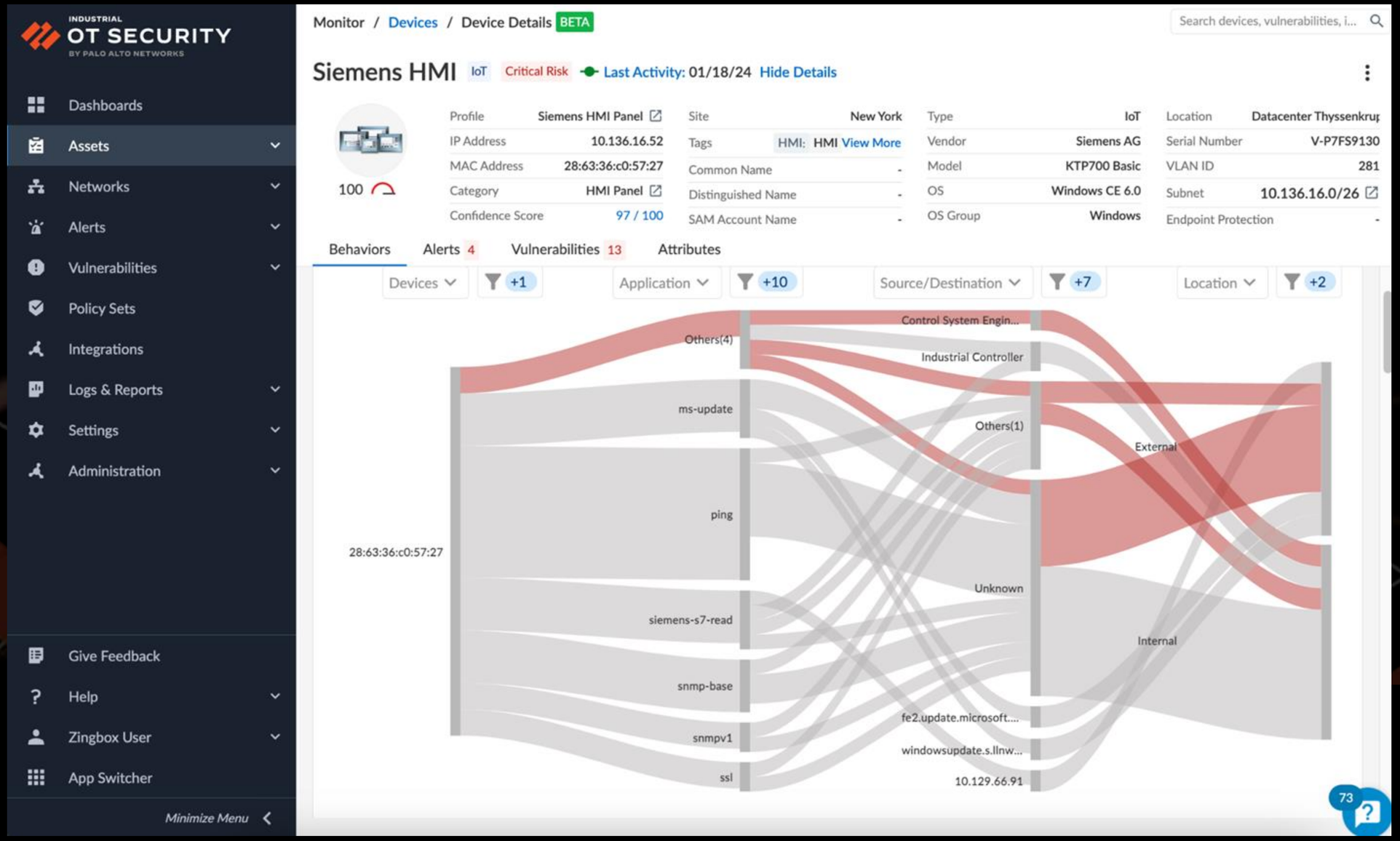
RIPE Database Software Version 1.114

Cortex® Xpanse

# Attack Surface Management


Cortex® Xpanse

# OT Security



# Security Platform

# Platformization Addresses Critical Cybersecurity Challenges Through Integration & Innovation

## Network Security
**STRATA**

Best-in-class security delivered across hardware, software and SASE

## Cloud Security
**PRISMA CLOUD**

Comprehensive platform to secure everything that runs in the cloud

## Security Operations
**CORTEX**

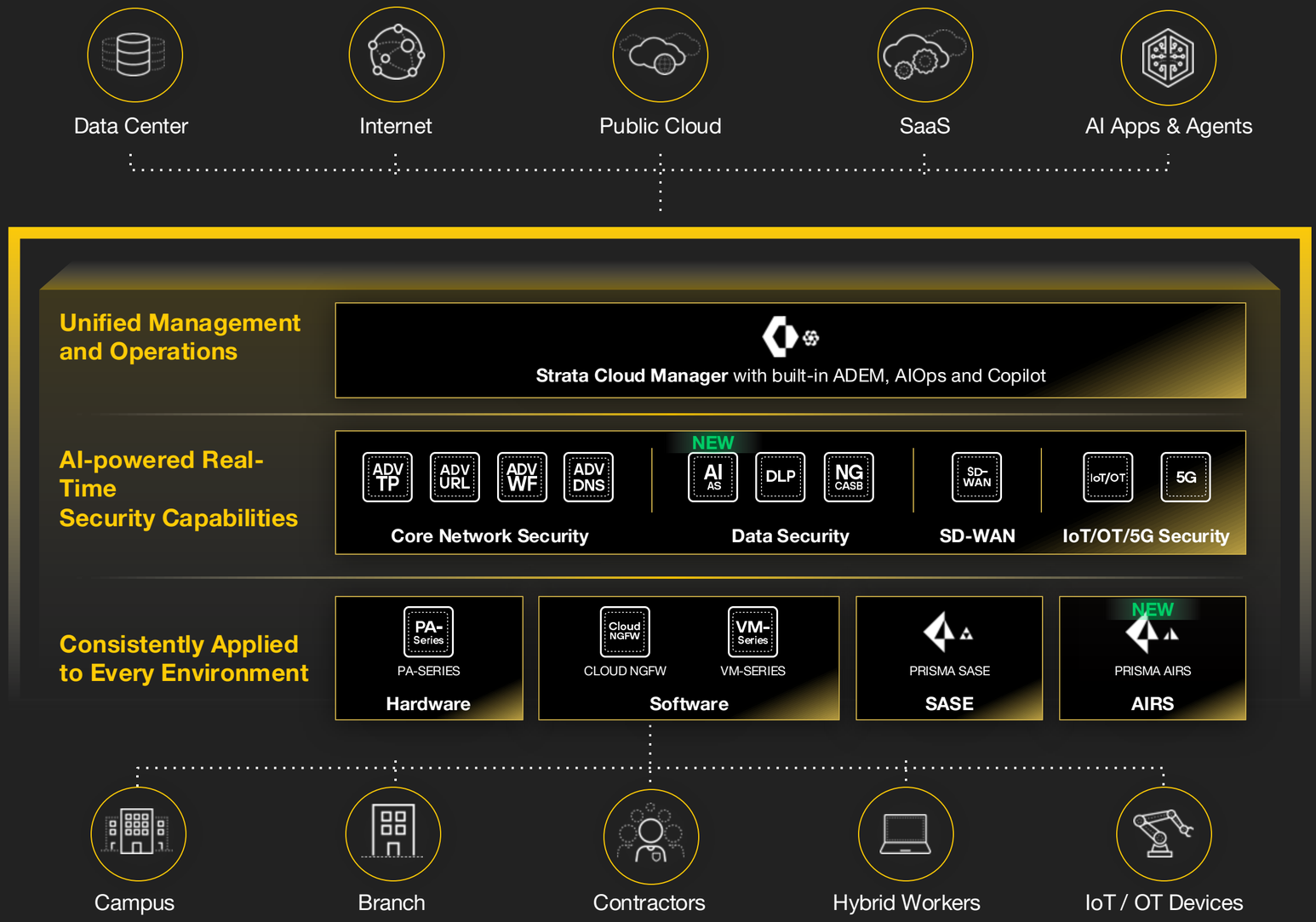
A new approach to SOC with fully integrated data, analytics and automation

## Threat Intelligence and Advisory Services

World-renowned threat intelligence, cyber risk management and advisory services

# Strata Network Security Platform

## Simplify and unify network security.




### Unified Management and Operations

Write policy once and enforce everywhere. Proactively strengthen security and prevent outages using Generative AI.

### AI-powered Real-Time Security

Prevent threats in real time using ML and Deep Learning applied to rich data from **70,000+ customers**.

### Consistently Applied to Every Environment

Secure AI and non-AI workloads against network and AI-specific threats. Deploy in clouds, containers and data centers.

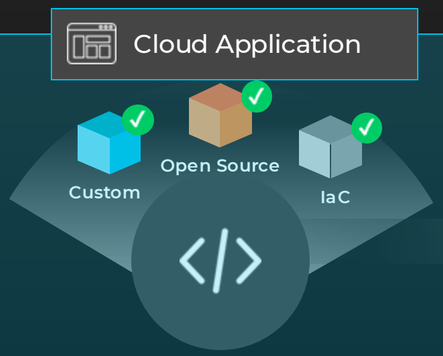


paloalto NETWORKS | STRATA

# Prisma Cloud

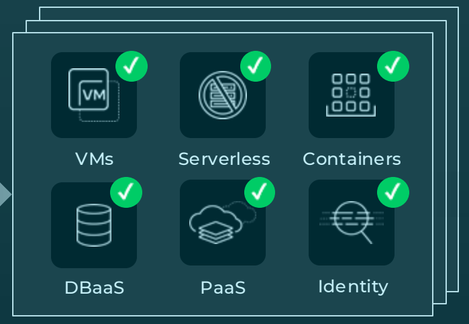
## Code to Cloud Platform

### Code




CI/CD pipeline

### Cloud Infrastructure




CI/CD pipeline

### Cloud Runtime


**Risk Prevention**

Complete and contextualized security in Code Phase:
**IaC, SCA, CI/CD, Secrets**

**Secure The Source**

**Visibility & Control**

Unmatched visibility: Applications, Workloads, Data, Identity, Services, APIs, Unsanctioned Clouds
**CSPM, CIEM, DSPM, CDEM**

**Secure The Infrastructure**

**Runtime Protection**

Proactive Runtime Detection and Prevention:
**CWPP, WAAS, CNS**

**Secure The Runtime**



paloalto NETWORKS | PRISMA

# Cortex

## One Platform for Proactive and Reactive Security




paloalto NETWORKS | CORTEX

# Thank You

paloaltonetworks.com