

Palo Alto Networks

Securing businesses in the age of AI

Bezpečnosť AI modelov

Zsolt Géczi, Regional sales manager, Slovakia

Platformizácia rieši kritické výzvy v oblasti kybernetickej bezpečnosti prostredníctvom **Integrácie & Inovácie**



Zero Trust Network Security

Najlepšia sieťová bezpečnosť vo svojej triede, ktorá umožňuje celopodnikové zabezpečenie typu Zero Trust



AI-Driven Security Operations

Transformácia SecOps pomocou AI a automatizácie novej generácie



Real-Time Cloud Security

Zabezpečenie Cloudu v reálnom čase od Kódu cez Cloud až po SOC



UNIT 42, Incident Response, Advisory Services and Threat Intelligence

Strategický partner v oblasti bezpečnosti prostredníctvom proaktívnych a reaktívnych bezpečnostných služieb a svetovo uznávaných spravodajských služieb



Products & Services Portfolio

Secure AI

AI Access Security

Prisma AIRS

Unit 42 Security Assessment

Next Generation Firewalls

PA-Series Hardware NGFWs

Cloud Native NGFW

Advanced SD-WAN

PAN-OS

VM-Series Software NGFWs

Strata Cloud Manager

Panorama

Quantum Readiness

Cloud Delivered Security Services

Advanced Threat Prevention

Advanced WildFire

Enterprise Data Loss Prevention

SaaS Security

Advanced URL Filtering

Advanced DNS Security

Device Security

Secure Access Service Edge

Prisma SASE

Prisma Access Browser

Autonomous Digital Experience Mgmt

5G Security

Prisma Access

Prisma SD-WAN

Application Acceleration

Remote Browser Isolation

Cloud Security

Application Security

Cloud Posture Security

Cloud Runtime Security

Cortex Detection & Response

AI-Drive SOC

Cortex XSIAM

Cortex XSOAR

Cortex XDR

Cortex Xpanse

Threat Intelligence & Incident Response

Assess

Unit 42 Retainer

Transform

Managed Detection & Response

Respond

Managed Threat Hunting

Precision AI

AI Access Security

Strata Copilot

Prisma Copilot

Prisma AIRS

Cortex Copilot

Unit 42 Security Assessment

Global Services

Services Portfolio

Professional Services

Support Services

Education & Training

Success Tools

Customer Success

Ecosystems

Nextwave Program

Technology Partners

Cloud Service Providers

Partner Portal

Service Providers

Global System Integrators

Company

Industry Recognition

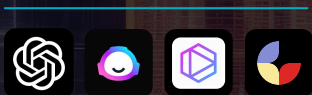
Acquisitions

Product Certifications



AI Adaptácia Transformuje Produktivitu Práce

KONVERZAČNÉ CHATY



ASISTENTOVIA KÓDU A GENERÁTORY



GENERÁTORY VIDEA A OBRAZOV



ASISTENTI PRE PÍSANIE



A. mnoho ďalších...

Nativné AI aplikácie expandujú

12,000+

Odhad na 2030.

Source: Pitchbook's Generative AI Emerging Space, Artificial Intelligence & Machine Learning Analyst Curated Vertical and SaaS Vertical

Aplikácie a Agenti umelej inteligencie vo firmách **raketovo rastú**

83%

podnikov používa alebo
experimentuje s AI v cloude¹

1.3Mld

agentov bude v
prevádzke do roku
2028²

S rastúcim využívaním GenAI aplikácií rastú aj Bezpečnostné Riziká

55%

zamestnancov
využilo
**neschválené
GenAI nástroje** v
práci.



Aplikácie Shadow AI
vytvárajú bezpečnostné slepé
miesta.



Strata citlivých údajov
pramení z neoverených otázok
a odpovedí GenAI.



Škodlivý obsah
z GenAI odpovedí predstavuje
riziko pre používateľov.



**IOTW: Samsung employees allegedly leak proprietary
information via ChatGPT**

Three separate employees have allegedly leaked information to the AI chatbot



**US House forbids staff members from using AI chatbot
Microsoft Copilot**

House Office of Cybersecurity has deemed Microsoft Copilot a risk to users because of the threat of leaking House data to non-House approved cloud services.



**Microsoft accidentally exposes 38TB of internal data via
GitHub repository**

38 terabytes of internal data, including passwords, publicly accessible through a GitHub repository that Microsoft's artificial intelligence research group uses

Source: Salesforce 2023

AI Security



AI Access Security

Umožnite svojim zamestnancom bezpečne využívať výkon Gen AI aplikácií.



Prisma AIRS

Chráňte svoje AI aplikácie, modely a dáta pred hrozbami umelej inteligencie a základnými hrozbami v reálnom čase.

Unit 42 AI Security Assessment



Predstavujeme **AI Access Security** ktoré umožňuje zamestnancom bezpečné využívanie umelej inteligencie, LLM modelov



Prehľad o využívaní AI v reálnom čase

Zistíte, ktoré AI aplikácie sa používajú a kto ich používa.

Riadenie prístupu

Blokujte neschválené aplikácie, uplatňujte zásady informačnej bezpečnosti a chráňte sa pred hrozbami.

Komplexná ochrana údajov

Skontrolujte, aké údaje, utajované informácie a IP adresy sú zdieľané.

Prisma AIRS

AI Runtime Security



AI Model Scanning

Skontrolujte open-source modely na prítomnosť injektovaných hrozieb.



AI Posture Management

Získajte prehľad o rizikách bezpečnostného stavu týkajúce sa Vášho AI ekosystému.



AI Red Teaming

Vykonávajte automatizované penetračné testy na Vaše AI aplikácie a modely



AI Runtime Security

Chráňte svoje LLM aplikácie, modely a data pred runtime hrozbami



AI Agent Security

Zabezpečenie AI agentov proti novým autonómnym agentickým hrozbám.

Najkomplexnejšia platforma pre AI bezpečnosť na svete



Funkcia AI Runtime Security cez **Network aj Code**

Network-centric

Zmeňte **sieť** bez zmeny kódu aplikácie.

Vynucovanie bezpečnosti
na úrovni siete



AI, cloud a container
security in a single firewall



Centralizovaná platforma

Developer-centric

Zmeňte **kód aplikácie**
bez zmeny siete.

Vynucovanie bezpečnosti
na úrovni kódu



AI **security-as-code**



Rýchle nastavenie
za pár minút

Použite jeden alebo oba prístupy.

Nastavte si politiky raz a uplatňujte ich konzistentne.

Ďakujem

paloaltonetworks.com