

# ***State Of The Art Prevention***

***PŘÍPADOVÁ STUDIE A PREZENTACE VÝSLEDKŮ NASAZENÍ ŘEŠENÍ PALO ALTO NETWORKS.  
JAK TATO PLATFORMA POMOHLA SE ZAJIŠTĚNÍM SOULADU S POŽADAVKY GDPR***

Jakub Jiříček, CISSP, CNSE

*Systems Engineer, Eastern Europe*

*[jjiricek@paloaltonetworks.com](mailto:jjiricek@paloaltonetworks.com)*



# ***Co mají tyto dva nové předpisy společného?***

## **Network and Information Security Directive**

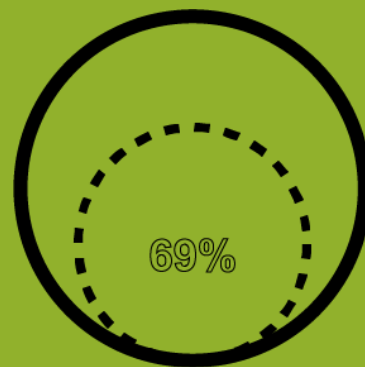
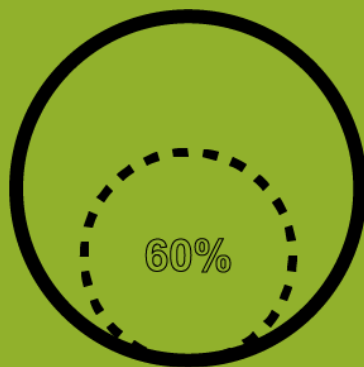
- Ensure they are at least at “**State of the Art**” in terms of technical and organisational measures to manage their risks
- Notify without undue delay\*

\*(more exact timeframes will likely be laid out in implementing acts) to Member States' competent authorities or CSIRTS security incidents that have defined impacts on their services

## **General Data Protection Regulation**

- Regard for “**State of the Art**”
- “Without undue delay” time limit (72hrs) to notify of **breach**\* of personal data

\* - “A breach should be considered as severely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation”



## Detekce – následná náprava



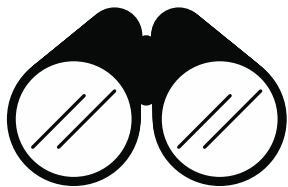
## Prevence - zastavení



styl myšlení



# ***Základní filosofie prevence***



**COMPLETE  
VISIBILITY**

**ÚPLNÁ  
VIDITELNOST**



**REDUCE  
ATTACK  
SURFACE**

**MENŠÍ PLOCHA  
PRO ÚTOK**



**PREVENT  
KNOWN  
THREATS**

**ZAMEZENÍ VŠEM  
ZNÁMÝM HROZBÁM**



**PREVENT  
UNKNOWN  
THREATS**

**ZJIŠTĚNÍ A ZASTAVENÍ  
NOVÝCH HROZEB**

## ÚPLNÁ VIDITELNOST

### COMPLETE VISIBILITY

- All applications
- All users
- All content
- Encrypted traffic
- SaaS
- Cloud
- Mobile

## MENŠÍ PLOCHA PRO ÚTOK

### REDUCE ATTACK SURFACE

- Enable business apps
- Block “bad” apps
- Limit app functions
- Limit file types
- Block websites

## ZAMEZENÍ VŠEM ZNÁMÝM HROZBÁM

### PREVENT KNOWN THREATS

- Exploits
- Malware
- Command & control
- Malicious websites
- Bad domains
- Stolen credentials

## ZJIŠTĚNÍ A ZASTAVENÍ NOVÝCH HROZEB

### PREVENT UNKNOWN THREATS

- Dynamic analysis
- Static analysis
- Attack techniques
- Anomaly detection
- Analytics



# ***Přirozená integrace***

## COMPLETE VISIBILITY

- All applications
- All users
- All content
- Encrypted traffic
- SaaS
- Cloud
- Mobile

## REDUCE ATTACK SURFACE

- Enable business apps
- Block “bad” apps
- Limit app functions
- Limit file types
- Block websites

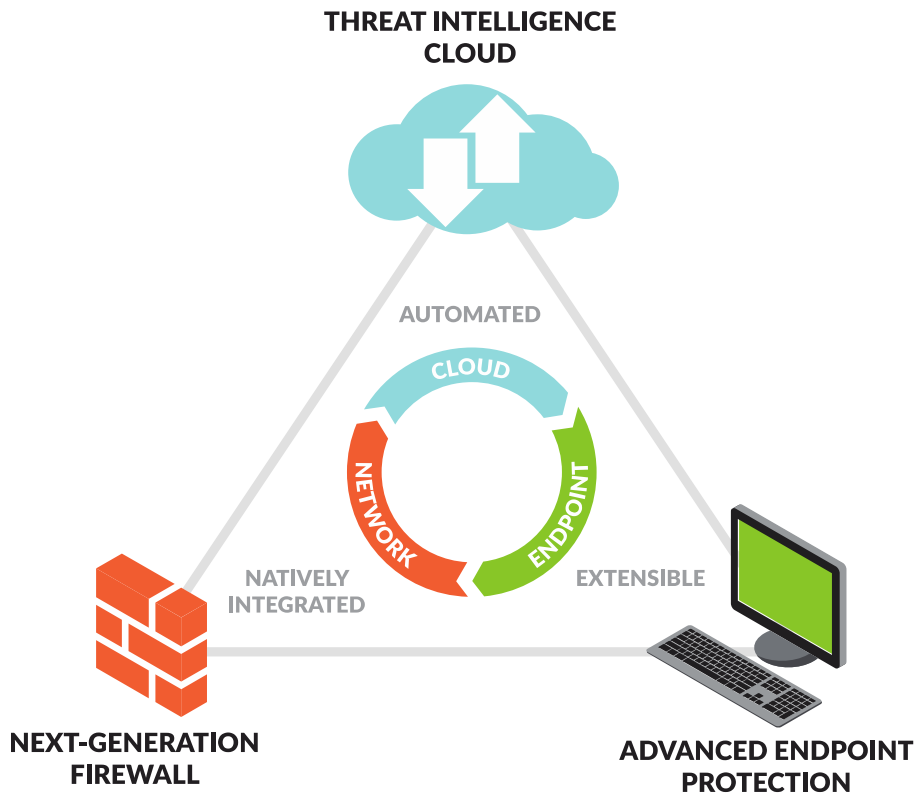
## PREVENT KNOWN THREATS

- Exploits
- Malware
- Command & control
- Malicious websites
- Bad domains
- Stolen credentials

## PREVENT UNKNOWN THREATS

- Dynamic analysis
- Static analysis
- Attack techniques
- Anomaly detection
- Analytics

# Prevence musí fungovat sama



- Přirozená integrace všech komponent – vč. 3-rd party



- Uživatelé, aplikace, umístění
- **Automaticky (a rychle)** mění své fungování podle nových hrozeb
- Vlastní výzkum bezpečnosti – unit42



<http://researchcenter.paloaltonetworks.com/unit42/>





# ***Novinky ve výzkumné automatizaci WildFire***



# ***MineMeld a AutoFocus***



**Příjem zpravodajských informací o hrozbách z různých zdrojů**  
– připojení libovolného externího zdroje informací do AutoFocus

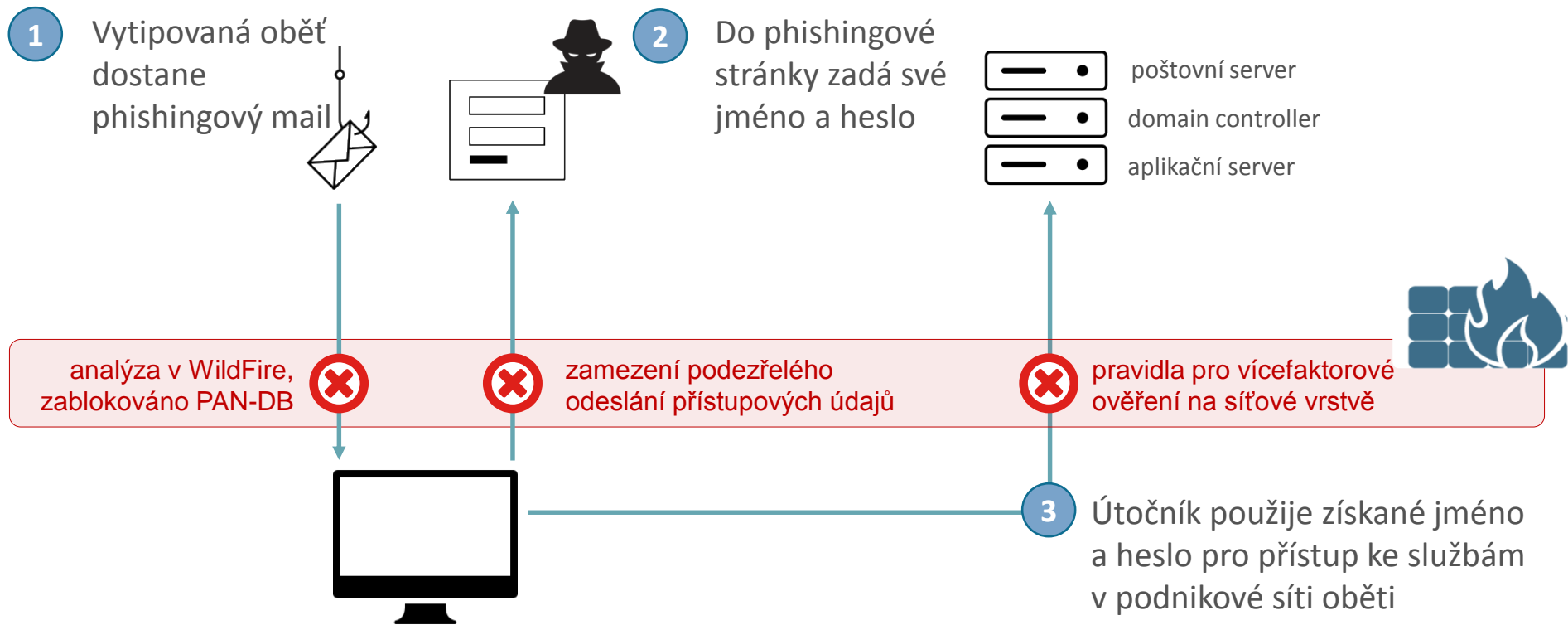


**Korelace a ověření zpravodajských informací s externími zdroji informací a interní databází událostí AutoFocus**



**Automatická prevence** pro zařízení Palo Alto Networks a nebo pro další zpracování jinými bezpečnostními systémy

# Zamezení zcizení přístupových údajů



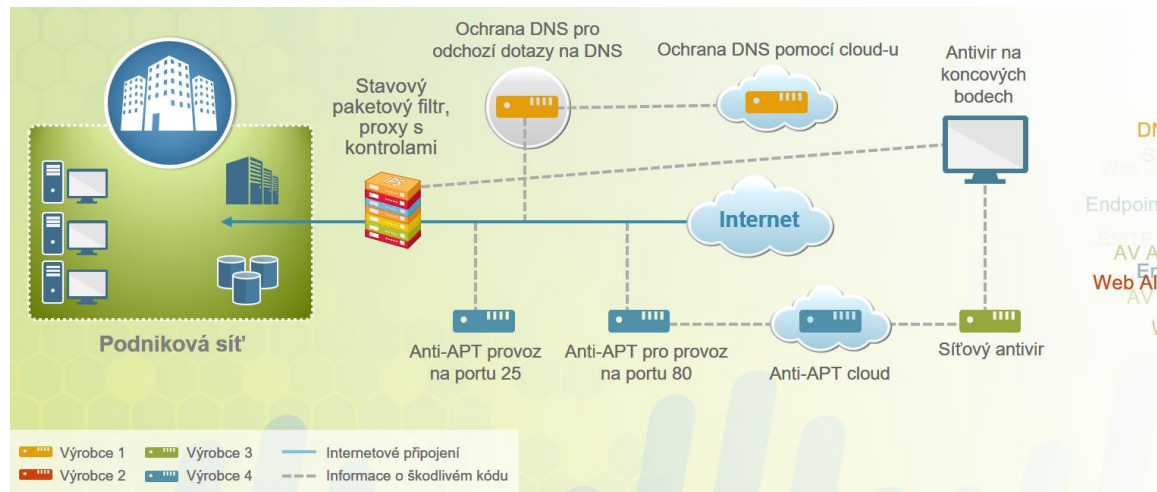
# ***Příklad implementace u zákazníka v ČR – expozice\****

Osoby a obsazení

- Zákazník: Energetická společnost v ČR
- Partner: **H-Square ICT Solutions**  
<http://www.h-square.cz>

Výchozí stav – cca 01/2016

- Požadavek na skutečně fungující IPS
- Úvahy nad změnou konceptu bezpečnostní architektury – „state of the art“ – NIS, GDPR
- Konsolidace perimetru – přechod na BGP peering



\*<https://cs.wikipedia.org/wiki/Drama>

# Příklad implementace u zákazníka v ČR – kolize

- Testování vedoucích technologií dle Gartner MQ
- Významná zjištění během testů – **Security Lifecycle Review**
  - Plná viditelnost provozu a ohrožení, risk assessment
  - Informace a souvislosti neviditelné pro L3/L4 síťové prvky



WE PUT THE  
DEVICE ON THE  
NETWORK



WE PASSIVELY  
MONITOR TRAFFIC  
FOR 1 WEEK



WE DELIVER THE  
REPORT & EXPLAIN  
THE FINDINGS

# slideshare-uploading

application function

## PowerPoint

file type

## slideshare

application

## “Confidential and Proprietary”

content

## prodmgmt

group

## HTTP

protocol

## file-sharing

URL category

## mjacobsen

user

## SSL

protocol

## canada

destination country

## 172.16.1.10

source IP

## TCP/443

destination port

## 64.81.2.23

destination IP

# 344KB

EXE

file type

web-browsing

application

shipment.exe

file name

finance

group

HTTP

protocol

unknown

URL category

stomlinson

user

SSL

protocol

china

destination country

172.16.1.10

source IP

TCP/443

destination port

64.81.2.23

destination IP

344KB

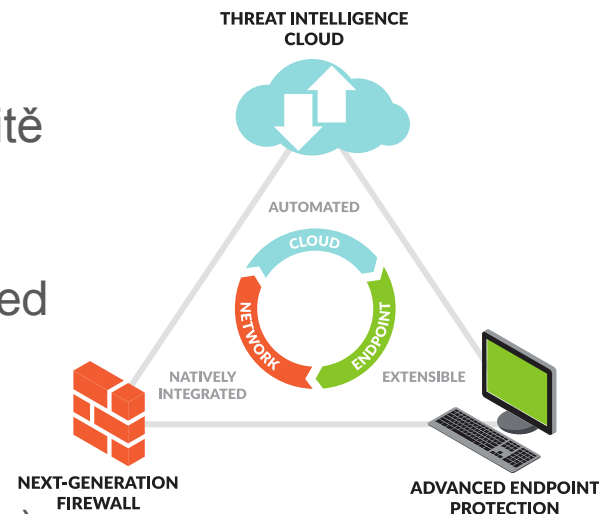


# ***Příklad implementace u zákazníka v ČR – krize***

- Nový scope projektu:
  - Náhrada IPS sond
  - Náhrada proxy serveru – transparentní přístup + bezpečnostní kontroly vázané na identitu
  - Náhrada perimetrového FW
  - Otevírání odchozích SSL spojení
  - Přestavba pobočkové sítě a jejího propojení s HQ
- Testovací provoz, postupný přechod do provozu – celkem cca 6-9 měsíců

# ***Příklad implementace u zákazníka v ČR - katarze***

- Migrace ze stávajících stavových paketových filtrů
  - Využití free migračního nástroje
  - Velká podpora partnera – minimální odstávky v řádu desítek sekund
- Nasazení cca desítky HA párů Palo Alto Networks FW
  - Různé modely dle požadované propustnosti v lokalitě (PA500 – PA5xxx, 500Mbps -- 20Gbps)
- Vynikající výsledky provedených penetračních testů externími subjekty, vč. vyšetřování incidentů (ACC, unified logy)
- Doplnění stejné ochrany i pro DC
- Plány na doplnění o NG ochranu koncových bodů (Traps)



# ***Konzistentní ochrana a správa***

**COMPLETE  
VISIBILITY**

**ÚPLNÁ  
VIDITELNOST**

**REDUCE  
ATTACK  
SURFACE**

**MENŠÍ PLOCHA  
PRO ÚTOK**

**PREVENT  
KNOWN  
THREATS**

**ZAMEZENÍ VŠEM  
ZNÁMÝM HROZBÁM**

**PREVENT  
UNKNOWN  
THREATS**

**ZJIŠTĚNÍ A ZASTAVENÍ  
NOVÝCH HROZEB**



**internetová  
brána**



**datové centrum/  
privátní cloud**



**veřejný cloud**



**SaaS**



**mobilní uživatelé**



**koncové body**



**IoT**

# ***Jaké jsou doporučené další kroky?***

1. Začněte hned!
2. Další informace - <http://go.paloaltonetworks.com/regulation>
3. Vlastníkem je top management
4. Gap Analysis vyhodnocení rizik – dokážete rizika popisovaná v GDPR dnes měřit?
  - Ve spolupráci s auditními a poradenskými partnery jasně definujte vyhodnocení rizik
5. Vypracujte právní postupy a směrnice, zohledněte i ochranu soukromí (interní i externí)
6. **Vytvořte plán jak zajistit a udržet technologický status „state of the Art”**
7. Vytvořte jasný plán, co dělat v případě, dojde-li k incidentu

# Ultimate Test Drive – pozvánka na Tesla drive

Půldenní praktický seminář s nastavením a laděním skutečného NGFW zařízení



- Pro zájemce o NGFW řešení – koncové zákazníky
- Praktický workshop – virtuální lab v cloudu, příklady z praxe
- Možnost vyzkoušet si nejen firewall 😊
- Registrace zde:
  - [www.paloaltonetworks.com/events/tes-t-drive.html](http://www.paloaltonetworks.com/events/tes-t-drive.html)





# ***Otázky, odpovědi..***

- Jakub Jiříček, CISSP, CNSE

- Systems Engineer, Eastern Europe

- [jjiricek@paloaltonetworks.com](mailto:jjiricek@paloaltonetworks.com)

# Rozsáhlý partnerský ekosystém

Virtualization	Networking	Mobility	Security Analytics	Enterprise Security
