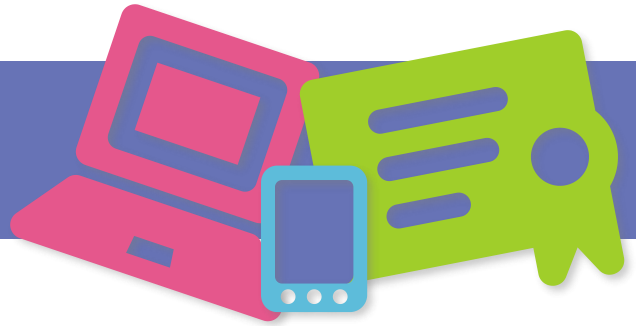
SECURITY 2015

23. ročník konference o bezpečnosti v ICT



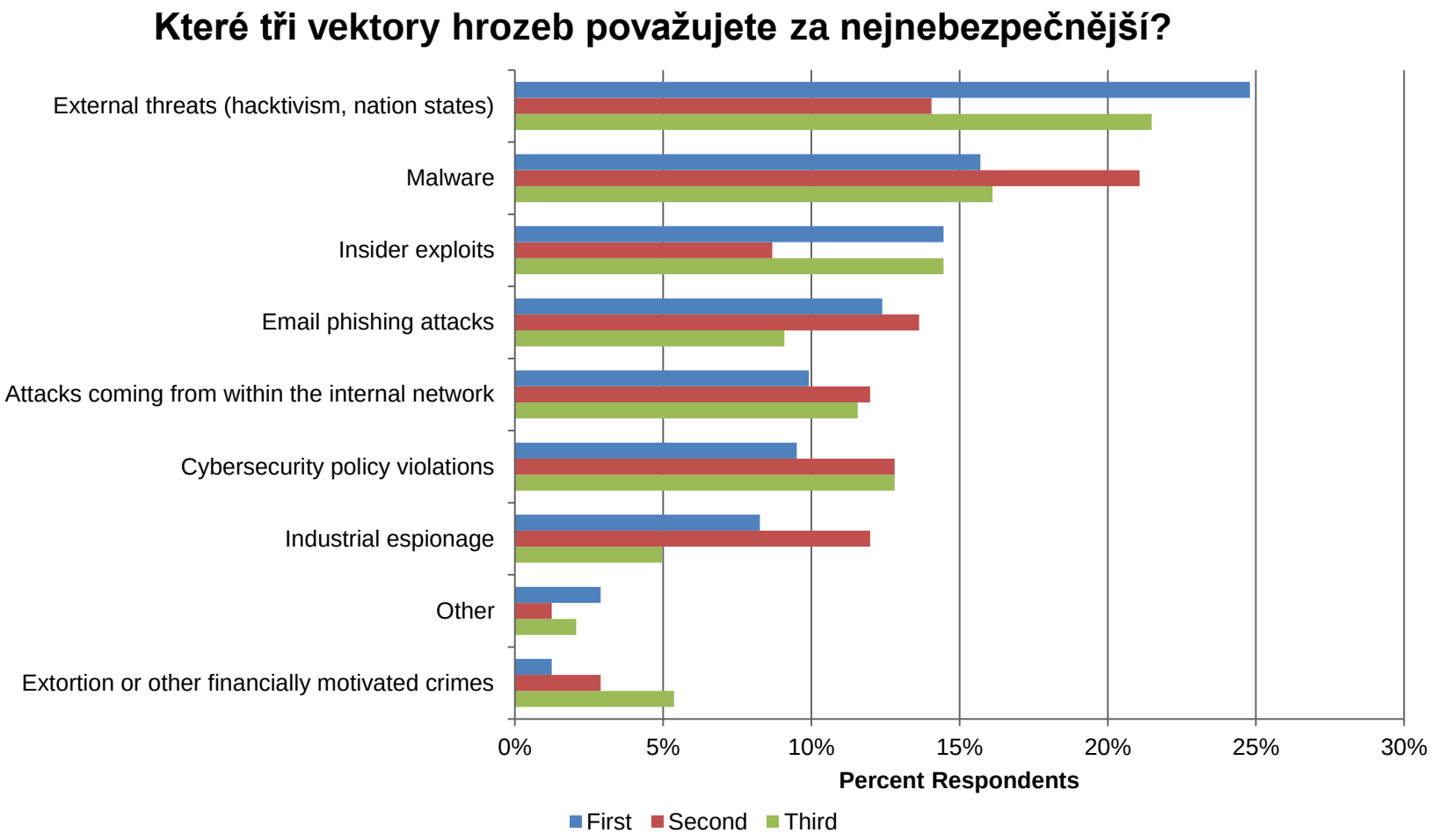
Nová generace ochrany pro prostředí SCADA

Jakub Jiříček

Palo Alto Networks

Čím se v noci budí CISO?

Průzkum SANS 2014 pro průmyslová IT prostředí (ICS)



SECURITY 2015

Pokročilé cílené hrozby (APT)

Norway Oil & Gas Attacks

- Sociální inženýrství: spearphishing, watering hole
- Cíl: krádež duševního vlastnictví ???

STUXNET

- Sociální inženýrství: výměnná média
- Zneužití zero-day zranitelností (Windows, Siemens)
- Šíření/zkoumání běžných aplikací a typů souborů
- Cíl: narušit program obohacování uranu

Energetic Bear

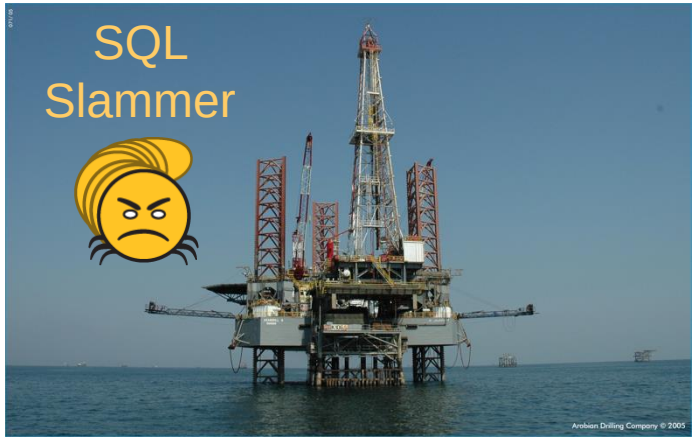
- Sociální inženýrství: spearphishing, watering hole, trojský kůň v ICS Software
- Zjištění OPC assets (ICS protokol!)
- Cíl: krádež duševního vlastnictví a zřejmě i proof of concept útoku na ICS

Útok typu Malicious Insider

- Čistírna odpadních vod v Maroochy Shire, Queensland, Austrálie
- Nespokojený zaměstnanec dodavatele ICS se pomstil na zákazníkovi a zaměstnavateli
- Svých znalostí prostředí zneužil k získání přístupu a způsobil škodu
- Dopad
  - Do místních parků, řeky a na pozemky hotelu se rozlilo 800,000 litrů splašků
  - Poškození životního prostředí, zdravotní rizika, úhyn mořských živočichů

Zdroj: Applied Control Solutions

Kybernetické incidenty z nedbalosti



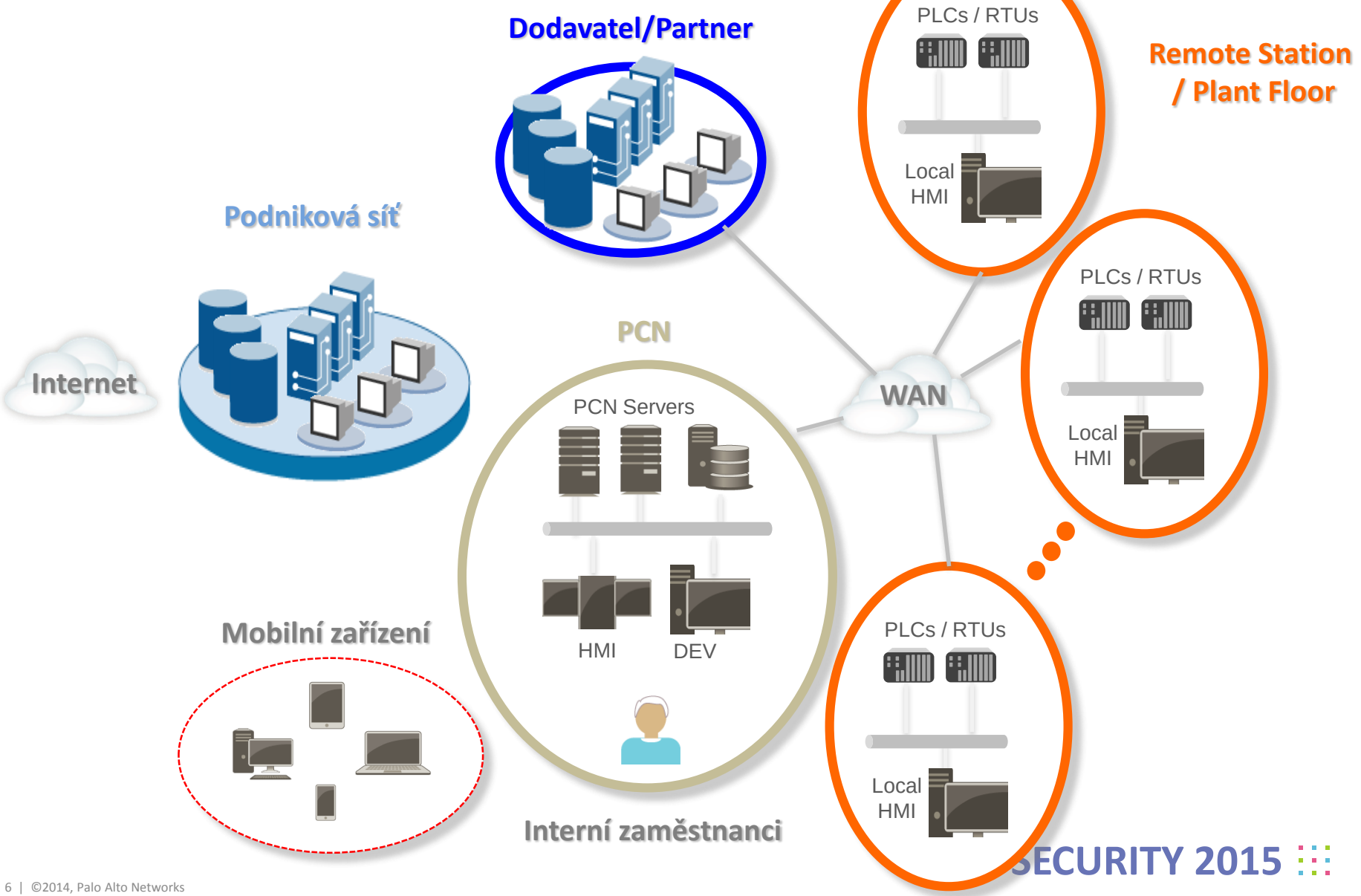
- Těžařskou platformu sdílí hlavní provozovatel a partnerské firmy
- Přes jednu partnerskou síť se celá plošina nakazila červem SQL Slammer
- Havárie pracovních stanic a SCADA serverů
  - Po restartu se nespustily OS
  - Obnova prostředí SCADA a návrat k produkci trval 8 hodin
- Důsledky
  - Okamžitá ztráta informací o vrtech
  - Výpadek v produkci všech 4 hlavních vrtů
  - Celkové ztráty > $1.2M

Zdroj: Red Tiger Security

- Application Visibility and Risk Report provedený v energetické společnosti ve východní Evropě
- Vedení společnosti bylo přesvědčené o izolaci od internetu
- V síti prostředí SCADA byl objevený neschválený přístupový bod s internetem a rizikové webové aplikace
  - Wuala (storage), eMule (P2P), DAV (Collaboration)
- Otazníky okolo možného úniku informací, dostupnosti sítě a zanesení škodlivého kódu

Zdroj: Palo Alto Networks

Nový pohled na důvěru v ICS



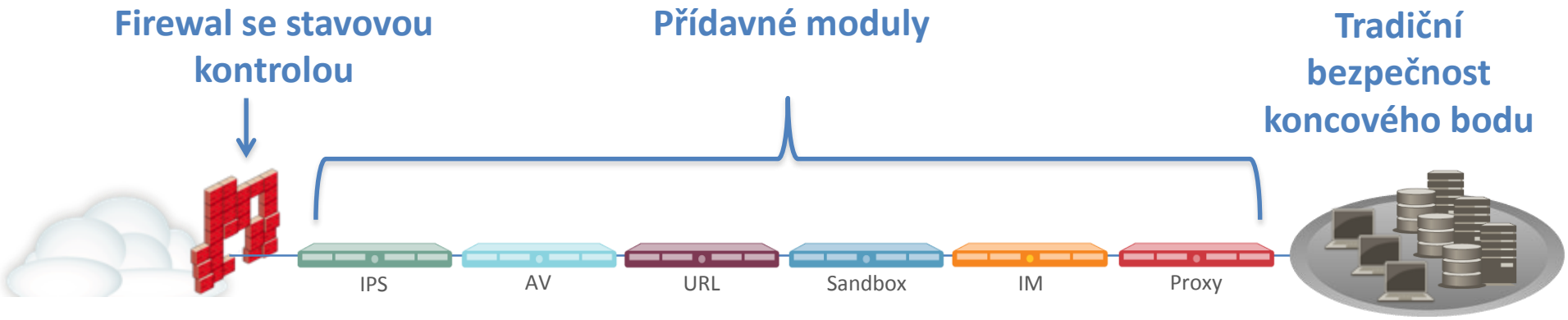
Standardy ISA99 a ISA/IEC

- ISA/IEC 62443 je sada standardů
- Na vývoji se podílí 3 skupiny
  - ISA99 → ANSI/ISA-62443
  - IEC TC65/WG10 → IEC 62443
  - ISO/IEC JTC1/SC27 → ISO/IEC 2700x

Nejdůležitější zjištění

- Nikomu se nedá věřit
  - Kritické je nasazení mikrosegmentace
- Je důležité detailně rozumět provozu
  - Aplikace, uživatelé, obsah
  - Sdílení kontextů
- Bez bezpečnosti na koncových bodech to nejde
  - Hrozby startují z koncových bodů a šíří se sítí
- Skutečná a potenciálně vysoká rizika spojená s kybernetickými incidenty
  - Samotná detekce nestačí, útoky je nutné okamžitě zastavovat (detekce vs. prevence)
- Pokročilé útoky použijí “zero-day” zranitelnosti
  - Je třeba rychle nacházet a zastavit neznámé hrozby
  - Pomůže automatická analýza hrozeb a sdílení informacíl

Limity tradiční architektury



Princip fungování

- Základem je kontrola stavu spojení
  - Pravidla na čísla portů a IP adresy
  - Bez rozlišení typu provozu

Související omezení

- Omezený přehled o provozu a rizicích v ICS
- Hrubé možnosti nastavení přístupu; bez uživatelských rolí

- Firewal je doplněný o přídavné moduly pro zvýšení bezpečnosti

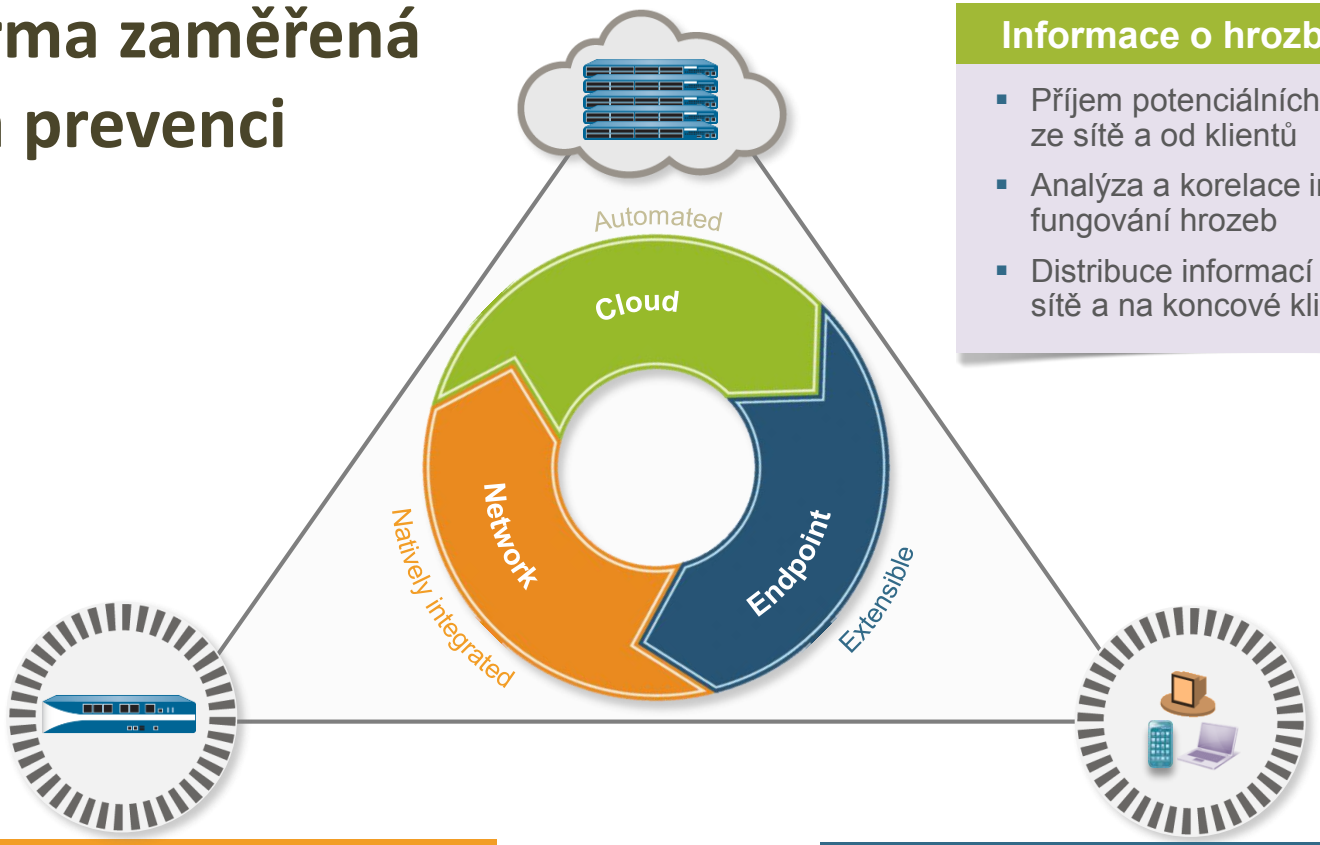
- Oddělená sila nekorelovaných informací, pomalé vyšetřování
- Náročná správa; pokles výkonu při zapojení bezpečnostních funkcí

- Nalezení a zastavení hrozeb se omezuje na již známé hrozby (ne ty zero-day)

- Snadno podlehne cíleným útokům
- Ochrany sítě a konc. bodů nespolupracují

Jaké to má řešení?

Platforma zaměřená na prevenci



Informace o hrozbách v cloud-u

- Příjem potenciálních nových hrozeb ze sítě a od klientů
- Analýza a korelace informací o fungování hrozeb
- Distribuce informací o hrozbách do sítě a na koncové klienty/servery

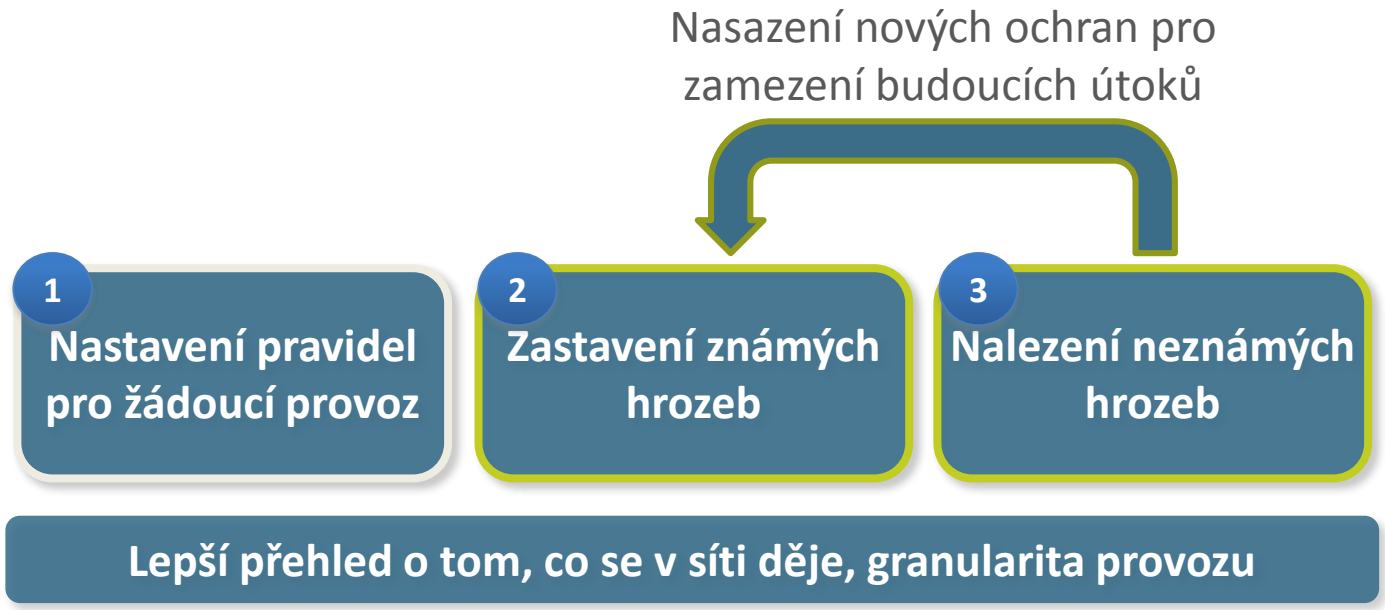
Next-Generation bezpečnost sítě

- Kontrola veškerého provozu
- Zastavení známých hrozeb
- Odesílání neznámého do cloud-u
- Rozšíření i pro mobilní a virtuální sítě

Pokročilá ochrana konc. bodů

- Inspects all processes and files
- Prevents both known & unknown exploits
- Integrates with cloud to prevent known & unknown malware

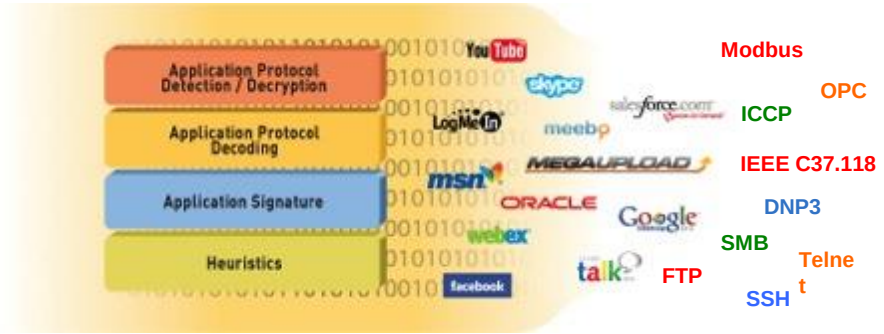
Systematický přístup k bezpečnosti



Klasifikační technologie

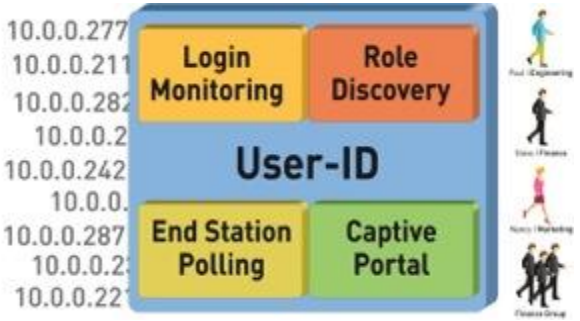
App-ID

Identifikace aplikací a protokolů



User-ID

Identifikace uživatelů



Content-ID

Prohledávání obsahu

SECURITY 2015

Identifikace pro SCADA a ICS

Protokol / aplikace	Protokol / aplikace	Protokol / aplikace
Modbus base	ICCP (IEC 60870-6 / TASE.2)	CIP Ethernet/IP
Modbus function control	Cygnet	Synchrophasor (IEEE C.37.118)
DNP3	Elcom 90	Foundation Fieldbus
IEC 60870-5-104 base	FactoryLink	Profinet IO
IEC 60870-5-104 function control	MQTT	OPC
OSIsoft PI Systems	BACnet	

Identifikace funkcí aplikace

Funkční varianty aplikace (celkem 15)
Modbus-base
Modbus-write-multiple-coils
Modbus-write-file-record
Modbus-read-write-register
Modbus-write-single-coil
Modbus-write-single-register
Modbus-write-multiple-registers
Modbus-read-input-registers
Modbus-encapsulated-transport
Modbus-read-coils
Modbus-read-discrete-inputs
Modbus-mask-write-registers
Modbus-read-fifo-queue
Modbus-read-file-record
Modbus-read-holding-registers

Záznam v Applipedia pro App-ID Modbus-base

modbus-base

Description

Modbus is a serial communications protocol published by Modicon in 1979 for use with its programmable logic controllers (PLCs). It has become a de facto standard communications protocol in industry, and is now the most commonly available means of connecting industrial electronic devices.

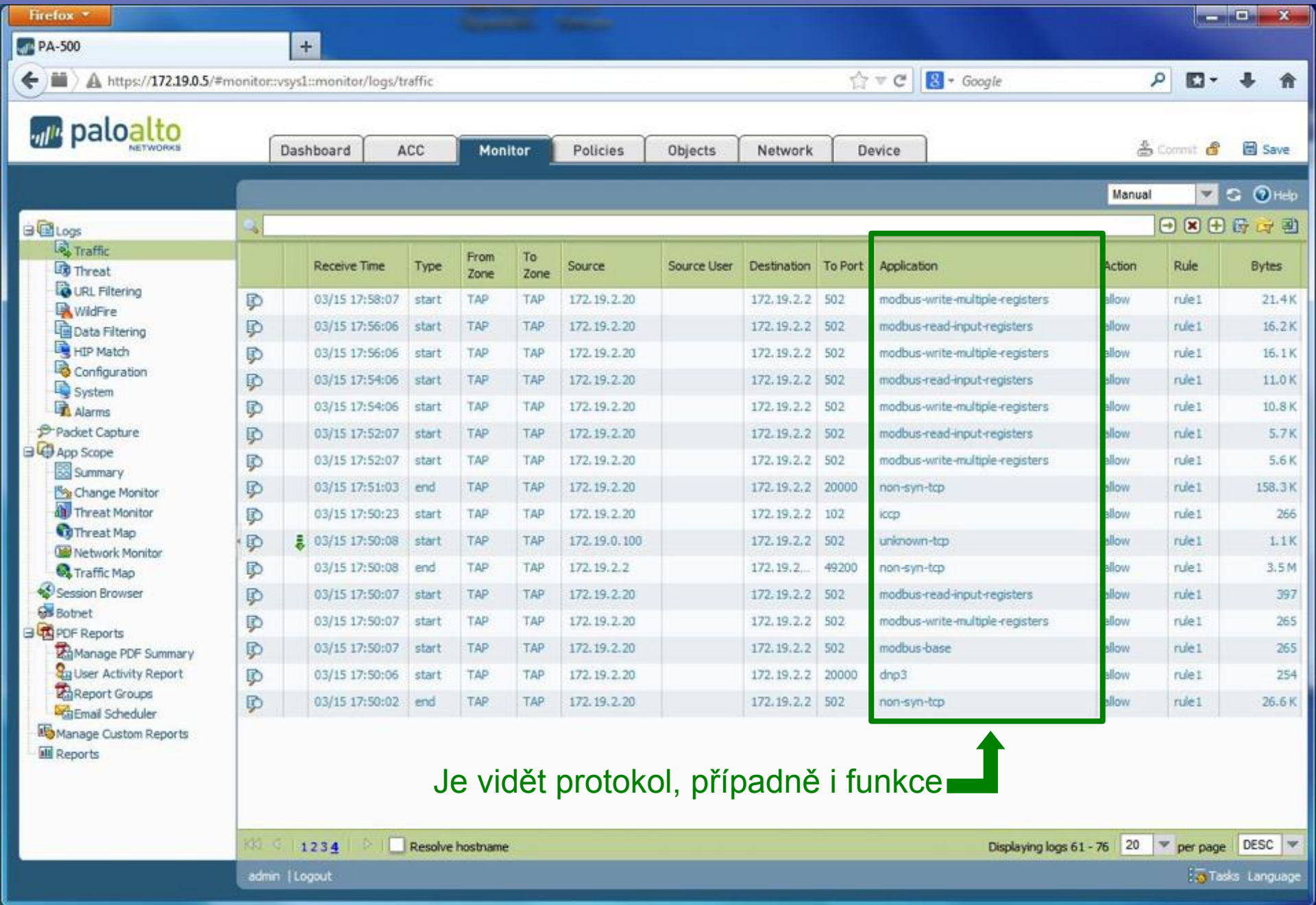
Reference

Wikipedia Google Yahoo!

Characteristics

Category	business-systems	Evasive	no
Subcategory	management	Excessive Bandwidth	no
Risk	2	Prone to Misuse	no
Standard Ports	tcp/502	Capable of File Transfer	no
Technology	network-protocol	Tunnels Other Applications	yes
		Used by Malware	no
		Has Known Vulnerabilities	yes
		Widely Used	no

Ukázka provozu v GUI firewallu



Systematický přístup k bezpečnosti

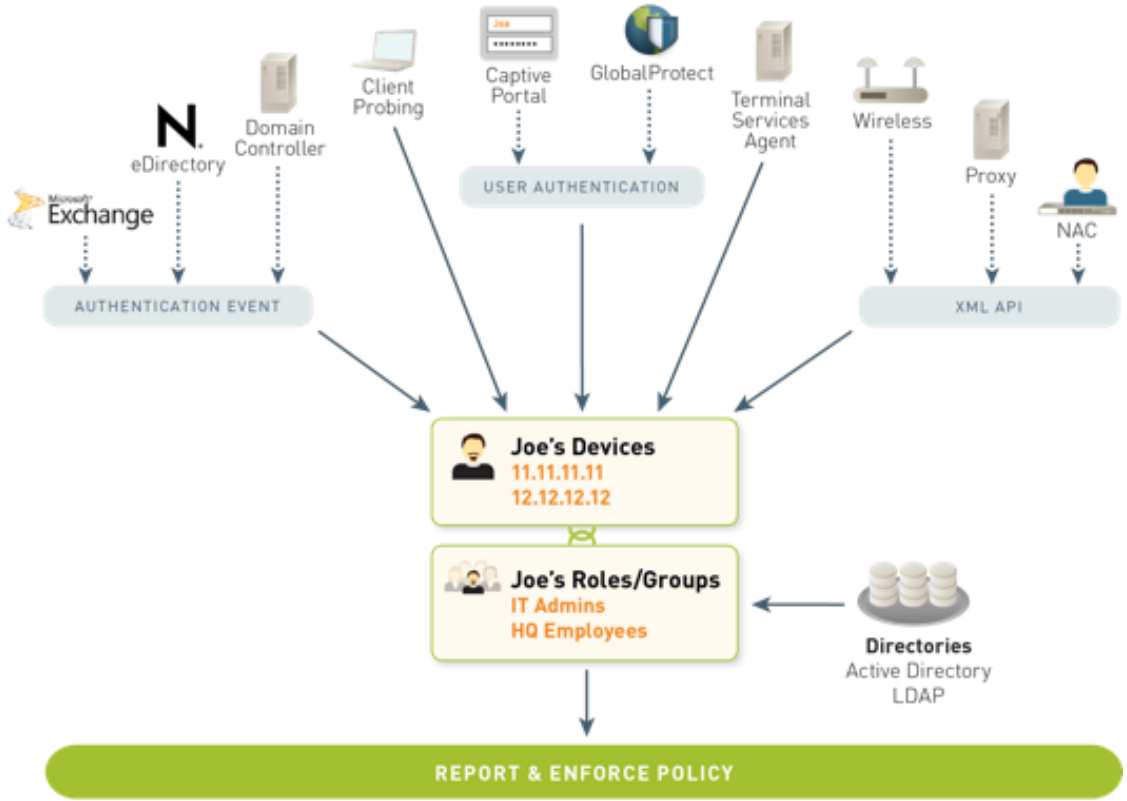
Možnosti segmentace

HW zařízení pracující s různými zónami, v souladu s doporučeními rámce IEC 62443

- Protocol (Modbus)
- Protocol Functions (Modbus Write Coil)
- Applications (OsiSoft Pi)
- SSL / SSH
- Unknown Traffic
- User
- User Group
- Content
- URL
- Country
- Physical / VWIRE
- Layer 2
- Layer 3
- VLAN
- VPN
- Temporal
- Virtual Machines
- Virtual Systems
- Port/Service
- IP Address

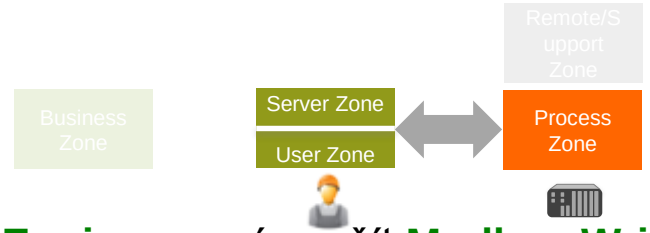
Řízení přístupu pomocí rolí

- Klíčová je identifikace uživatelů
- Prosazení pravidel na základě uživatelů a skupin

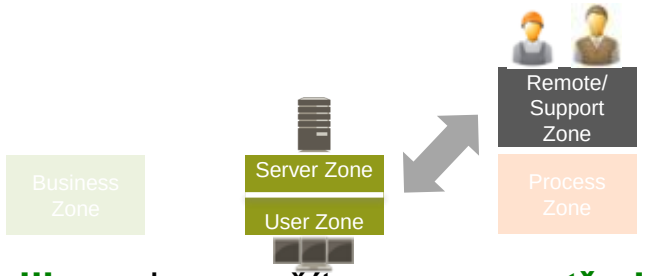


Segmentace aplikací a uživatelů

Uživatel s přístupem k aplikaci **Historian, např. Pi**



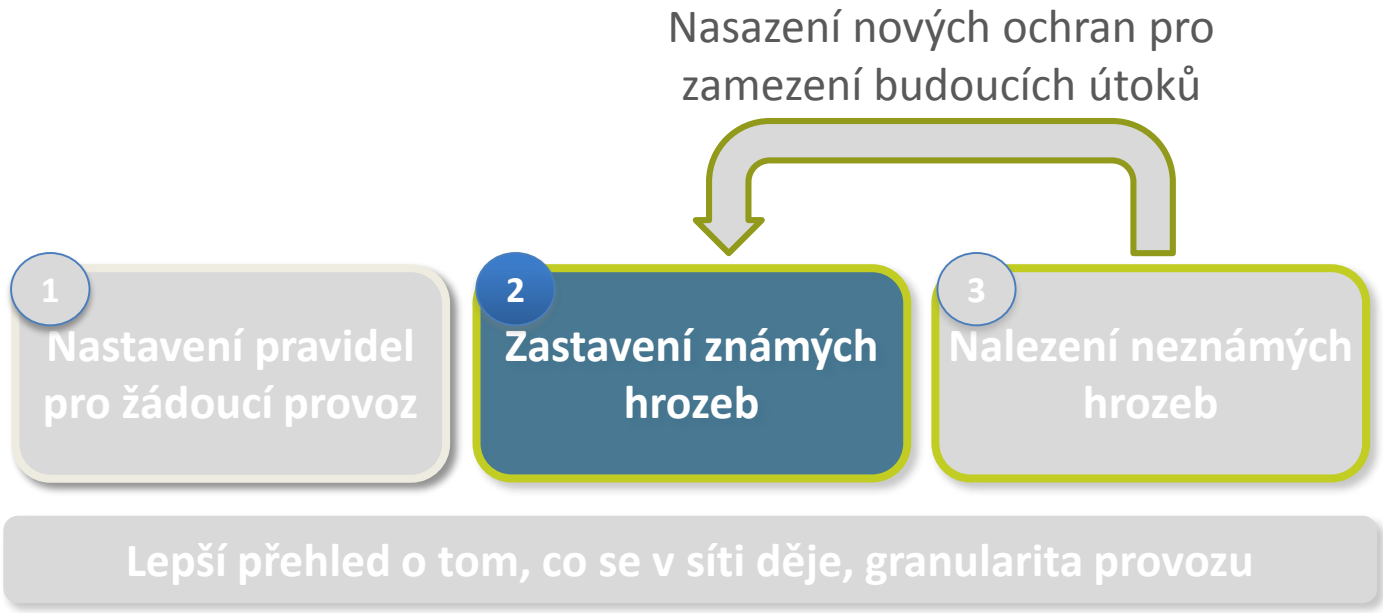
Sr. Engineer smí použít **Modbus Write, SSH**



Cizí aplikace lze použít pouze **prostřednictvím serveru**

SECURITY 2015

Systematický přístup k bezpečnosti



IPS signatury specifické pro ICS

- Speciální SW produkty

ID	Name	Severity	CVE
35908	Scadatec Limited Procyon Buffer Overflow Vulnerability	High	CVE-2011-3322
35907	Interactive Graphical SCADA System Directory Traversal Vulnerability	Low	CVE-2011-1565
35868	ScadaTEC ModbusTagServer and ScadaPhone Buffer Overflow Vulnerability	High	CVE-2011-4535
35789	Advantech WebAccess HMI and SCADA Software Cross-Site Scripting Vulnerability	High	CVE-2012-0233
35650	Schneider Electric Interactive Graphical SCADA Buffer Overflow Vulnerability	High	CVE-2013-0657
35262	DATAC RealWin SCADA Server SCPC_INITIALIZE Buffer Overflow Vulnerability	High	CVE-2010-4142

- Rizikové příkazy v protokolech

ID	Name
31666	SCADA DNP3 Write Request to a PLC Atetmpt
31665	SCADA DNP3 Miscellaneous Request to a PLC Atetmpt
31664	SCADA DNP3 Disable Unsolicited Response Attempt
31663	SCADA DNP3 Warm Restart Attempt
31662	SCADA DNP3 Broadcast Request Attempt
31661	SCADA DNP3 Read Request to a PLC Attempt
31660	SCADA DNP3 Stop Application Attempt
31659	SCADA DNP3 Cold Restart Attempt

DNP3

ID	Name
31668	SCADA Modbus Write Request to a PLC Attempt
31667	SCADA Modbus Read Request to a PLC Attempt
31652	SCADA Modbus Overlong Request Packet Abnormal
31651	SCADA Modbus Server Information Fetch Attempt
31650	SCADA Modbus TCP server Communications Power Cycle Attempt
31649	SCADA Modbus Device Identification Read Attempt
31648	SCADA Modbus Invalid Protocol Header
31647	SCADA Modbus Counters and Diagnostic Registers Clear Attempt
31646	SCADA Modbus PLC Force Into Listen Only Mode Attempt

Modbus

Běžné IT zranitelnosti fungují i tady

- HMI a další aplikace často využívají prohlížeče
- Zranitelnosti se objevují pořád

- V ICS se hodně používají platformy XP & Server (starší)
- Podpora pro XP a starší serverové platformy skončila

- Několik výrobců ICS vydalo doporučení v reakci na HeartBleed

Antivir a AntiSpyware

THREAT VAULT

Search

Search by id, name, CVE

Database reflects antivirus version **1370** and threats version **454**.

Type

Virus

Vulnerability
Spyware
Virus

Search

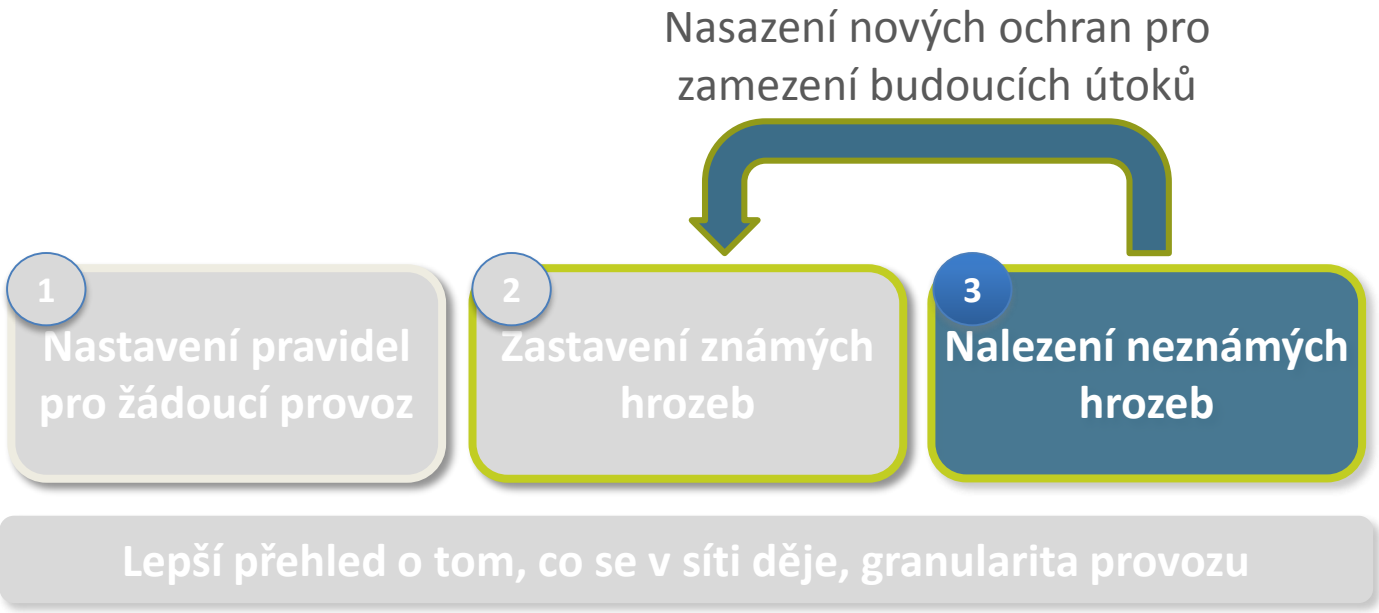
Virus(s) Listing

ID	Name
3080347	TrojanDownloader/Win32.karagany.
2095023	Trojan/Win32.stuxnet.dnf

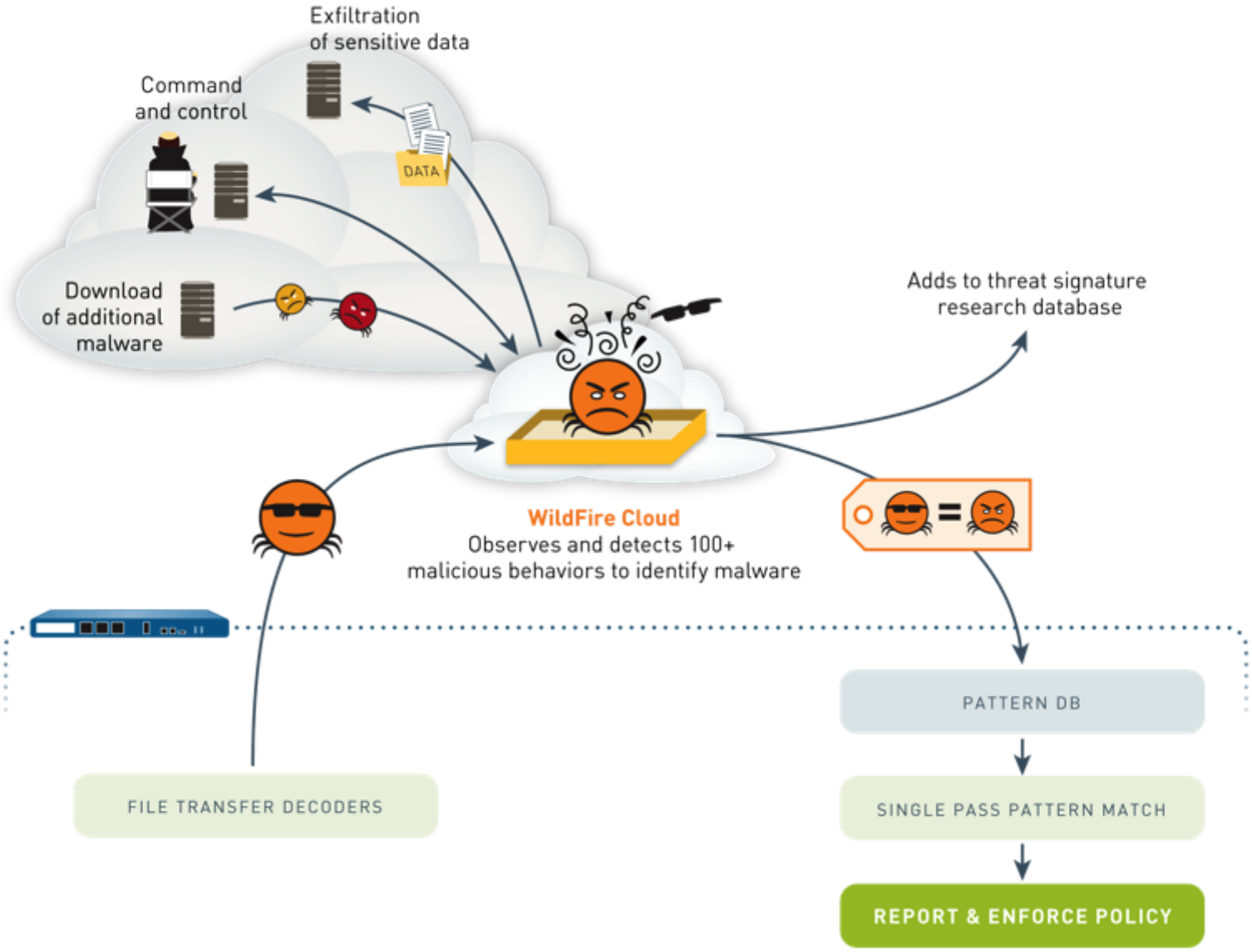
Spyware(s) Listing

13488	Havex.Gen Command And Control Traffic	Critical
13051	Stuxnet.Gen Command and Control Traffic	Critical

Systematický přístup k bezpečnosti



Detekce a prevence zero-day kódu



Zastavujeme neznámé

Zastavení hlavních útočných technik – a ne konkrétního kódu

Zneužití zranitelností software

Tisíce nových zranitelností a způsobů jejich zneužití objevené každoročně

Techniky napadení

Každý rok se objeví **maximálně 2-4** nové techniky napadení

Škodlivý kód

Milióny kusů nového škodlivého kódu každý rok

Principy fungování škodlivého kódu

Desítky až stovky nových způsobů fungování škodlivého kódu každý rok

Na prostředky nenáročný klient pro běžné OS Windows: XP SP3 a novější (i server), 25 MB RAM, 60 MB HDD, 0.1% CPU

Shrnutí

- Průmyslová IT prostředí potřebují bezpečnost nové generace
- Navrženou jako platforma…
  - Síť, koncové body, cloud
- Zaměřenou na prevenci
  - Zastaví pokročilé útoky vs. oznamení, že k útoku dochází
- Síť
  - Umožní granulární viditelnost a segmentaci
    - Viditelnost protokolů, pravidla vázaná na uživatele
  - Zastaví známé i neznámé
- Koncové body
  - Zastaví útočné techniky vs. hledání pomocí signatur
- Zjišťování hrozeb pomocí cloud-u
  - Automatická analýza a korelace
  - Spolupráce se sítí i s koncovými body

Další kroky

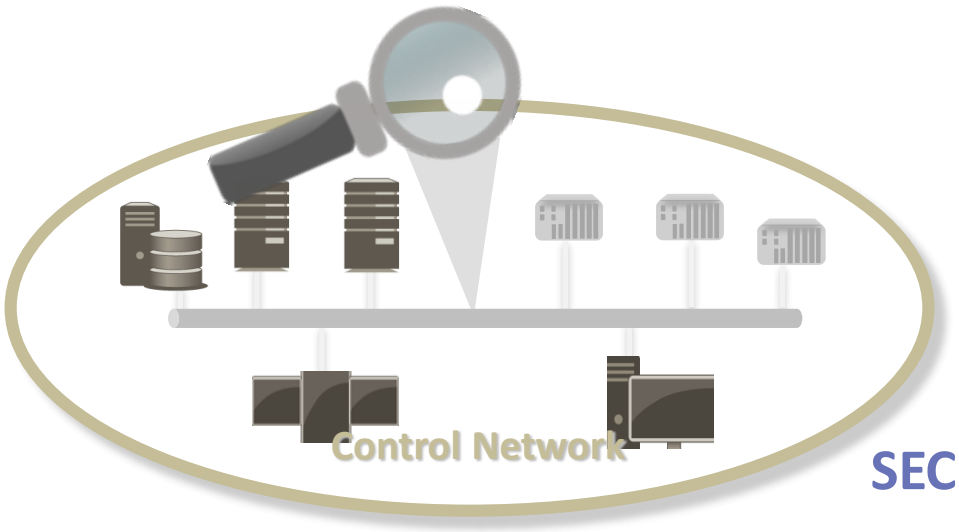
1 **Další informace o bezpečnosti pro prostředí SCADA/ICS**

Stáhněte si a přečtěte SCADA/ICS Solution Brief
go.secure.paloaltonetworks.com/secureics

Připojte se na Live Online Demo:
http://events.paloaltonetworks.com/?event_type=632

2 **Zjistěte sami, co se děje ve vaší řídící síti a jaké tam mohou být hrozby**

Požádejte o vytvoření Application Visibility and Risk Report (AVR) - zdarma:
http://connect.paloaltonetworks.com/AVR



SECURITY 2015

SECURITY 2015

23. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Jakub Jiříček, CISSP, CNSE
Palo Alto Networks
jjiricek@paloaltonetworks.com

SECURITY 2015

23. ročník konference o bezpečnosti v ICT

Panelová diskuse

SCADA security