

Účinná ochrana před moderními hrozbami

- Jakub Jiříček, CNSE, CISSP
- Systems Engineer, Eastern Europe



Dříve a nyní

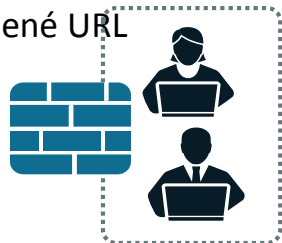
.. jak se s postupujícím časem mění pojetí bezpečnosti ..

Internetový perimetr

DŘÍVE

Blokace známých špatných portů, signatur a URL odkazů

- Ochrana sítě před známými hrozbami
- Pojetí bezpečnosti:
 - otevírají se pouze porty požadované pro business
 - pomocí IPS se signaturami blokuje známý škodlivý kód
 - známé nebezpečné nebo neschálené URL stránky se blokují
- Sada statických pravidel



NYNÍ

Zabezpečení aplikací a uživatelů zaměřené na prevenci 0-Day

- Ochrana uživatelů a aplikací před útoky
- Pojetí bezpečnosti:
 - Blacklist/Whitelist na aplikace a uživatele
 - Wildfire pro *detekci* neznámého škodlivého kódu
 - *Prevence* napadení analýzou a doručení v uzavřené smyčce
 - Integrace AV signatur pro známý i neznámý škodlivý kód
 - Zakázání známých nebezpečných URL stránek — každý den přibýde 13,500 nových
 - Jednotná pravidla spojující aplikace, signatury a URL
- Dynamické pojetí bezpečnosti

Vzdáleně připojení uživatelé

DŘÍVE

Vzdálený VPN přístup

- Pravidla obvykle předepisují:
 - vytváření zabezpečených tunelů od vzdálených uživatelů pro přístup k síťovému koncentrátoru
 - Po úvodním ověření jsou přidělena plná přístupová oprávnění
 - Pro vzdálené uživatele se nastavují jen mírná, případně vůbec žádná omezení

NYNÍ

Vzdálený VPN přístup s ochranou proti škodlivým kódům

- Pojetí bezpečnosti spoléhá na:
 - ověření zařízení pro možnost rozhodnutí o úrovni jejich stavu zabezpečení
 - ochrana zařízení před škodlivým kódem, izolace nakažených
 - šifrovaný přístup pro veškerý provoz
 - integrace User-ID do pravidel, bez ohledu na způsob připojení a umístění v síti
 - plná kontrola všech spojení – hledání škodlivého kódu přicházejícího ze vzdálených zařízení

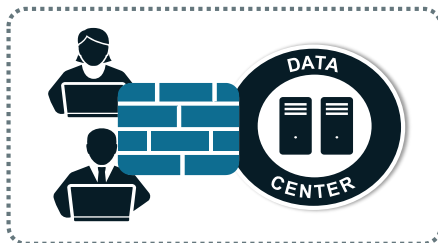
Segmentační strategie

DŘÍVE

Omezit provoz mezi různými segmenty sítě

Rozlišit oprávnění pro různé skupiny uživatelů

- Typicky se používají firewallová pravidla, která povolí průchod určitých portů mezi segmenty



NYNÍ

Zamezit laterální pohyb škodlivého kódu v síti

Vytvořit segmentační zóny pro omezení uživatelů ve skupinách

Striktní řízení toků mezi bezpečnostními zónami

Omezení typů toků, které mohou probíhat mezi segmenty

- Pravidla se zaměřují na vyjmenování povolených uživatelů/aplikací (whitelisting), vše ostatní se zakazuje
- Pasivní detekce škodlivého kódu a útočníků

Perimetr datového centra (provoz N/S)

DŘÍVE

Ochránit datové centrum před nepovoleným provozem

- Pravidla se typicky vytváří pro:
 - otevírání portů dovnitř a ven pro povolené aplikace
 - obvykle žádné nebo jen malé používání IPS
 - menší důraz na kontrolu odchozího provozu z DC
- Často je důležitější shoda s předpisy než bezpečnost



NYNÍ

Ochránit datové centrum před hacknutými uživateli a škodlivým kódem (nevěříme uživatelům) na úrovni aplikací

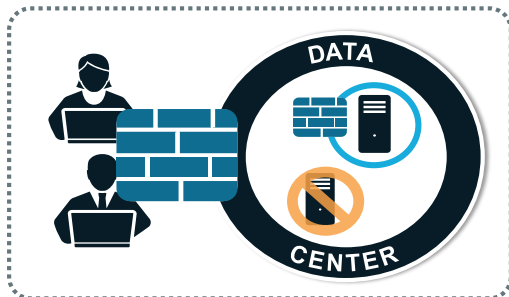
- Pravidla jsou založená na:
 - principu whitelisting-u: uživatelé a aplikace spolu mohou komunikovat pouze konkrétním povoleným způsobem
- Pro povolená pravidla se využívá Wildfire/WF-500 pro kontrolu souborů a hledání škodlivého kódu v přenášených souborech
- Prosazení odchozích pravidel pro odchozí směr – zamezení úniku dat

Uvnitř datového centra (provoz E/W)

DŘÍVE

Ochránit virtuální stroje v datovém centru prosazením pouze povolených portů pro komunikaci aplikací

- Pravidla:
 - otevírají povolené porty mezi virtuálními počítači
 - obvykle bez IPS kontrol, nebo jen s velmi mírnou



NYNÍ

Ochránit datové centrum před hacknutými uživateli a škodlivým kódem (nevěříme našim virtuálním strojům) na úrovni aplikací

- Pravidla:
 - pravidla pro whitelisting: komunikovat spolu mohou pouze aplikace konkrétními povolenými způsoby (omezení nejsou založená na portech)
- Pro povolená pravidla se využívá Wildfire/WF-500 pro kontrolu souborů a hledání škodlivého kódu v přenášených souborech

Dříve a nyní

.. a co s tím lze dělat?

Výzkum hrozeb a útoků – unit42



Poslání: analýzou dostupných informací zjišťovat útočníky, jejich motivaci a možnosti pro lepší porozumění hrozbám, kterým jsou naši zákazníci vystaveni



CRYPTOWALL v3 Ransomware

 **\$325M** in estimated damages across the globe



839
command and control URLs



5
second-tier IP addresses used for command and control



49
campaign code identifiers



406,887
attempted infections of CryptoWall version 3

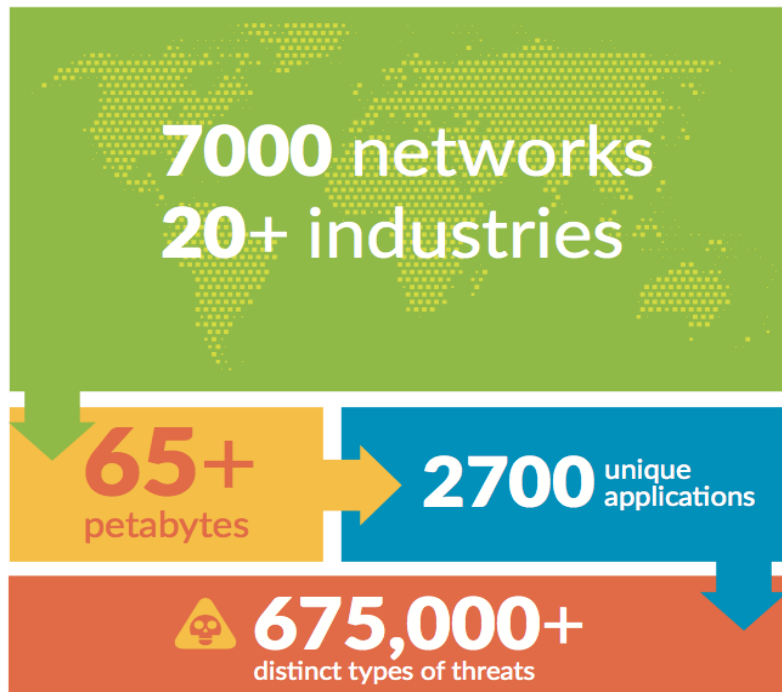


4,046
malware samples

<https://www.paloaltonetworks.com/threat-research.html>



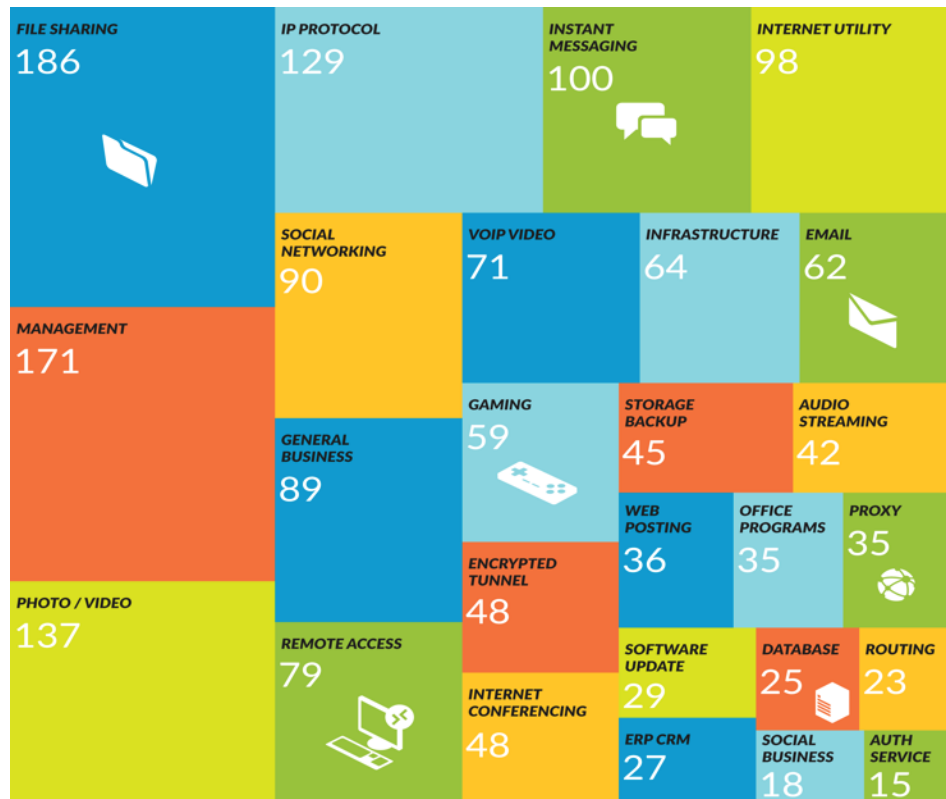
Application Usage and Threat Report



go.paloaltonetworks.com/autr

Globální přehled podkategorií používaných aplikací

Celkový počet aplikací v podkategorii



Zjištění

- 10% používaných aplikací je určených ke sdílení souborů, což může být pro data organizace bezpečnostní riziko – celkem jde o 186 aplikací.
- 137 aplikací z kategorie foto-video znamená, že uživatelé z firemních zařízení nejen pracují – možný dopad na produktivitu a také případnou nákazu malware – jde o téměř 8% všech aplikací.
- 4.5% všech aplikací jsou aplikace pro vzdálený přístup - mohou představovat významné bezpečnostní riziko, celkem jde o 79 typů.

Angler EK: vynalézavé ukrývání se

- Cookies – náказа se pošle jen jednou
- Šíří se z napadených webů
- Domain Shadowing
- Geo-location
- User-Agent Checks

Spear Phish + Decoy



Sudetenland
1938
"Legitima"

INVITATION TO A SPECIAL SCREENING OF THE NORWEGIAN

In celebration of the 100th anniversary of the birth of the Norwegian explorer Heyerdahl, the Norwegian Embassy has the pleasure of inviting you and a guest featuring the 2012 Norwegian historical drama "Kon-Tiki". The film was nominated for the category "Best Foreign Film" and tells the story of Thor Heyerdahl and his 2 (see attached flyer). The screening will be preceded by a reception.

Venue: Cinémathèque, 22A Hai Ba Trung Street, Hoan Kiem, Hanoi

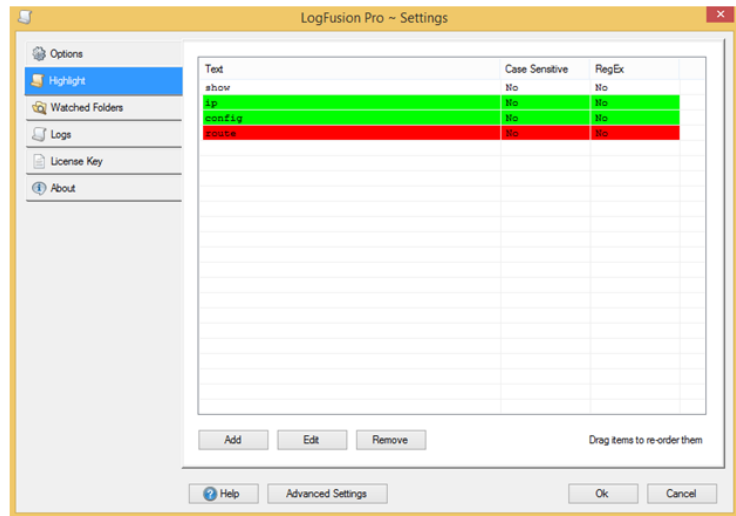
Date: 13 December, 2014

Time: Reception 19:00-20:00, Screening at 20:00

Seating is limited and based on a "first come, first served" basis. Reservations should be sent by email to officer.norwegian@yahoo.com.vn, no later than 12 December. In your email, please indicate if you will bring a guest. If you are unable to attend, please forward this invitation to a colleague.

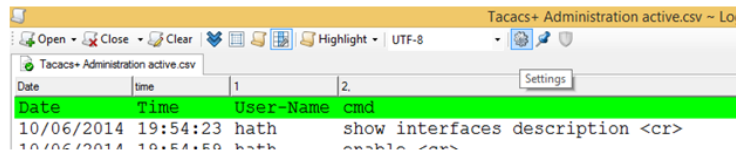


Các màu hiển thị theo thứ tự ưu tiên từ trên xuống dưới, màu nào đặt trên sẽ ưu tiên hiển thị. Thông thường thứ tự ưu tiên là: trắng > lục > đỏ. VD: với câu lệnh show ip route, sẽ hiển thị màu trắng



Lại chọn mục Highlight, tick vào lệnh config vừa tạo

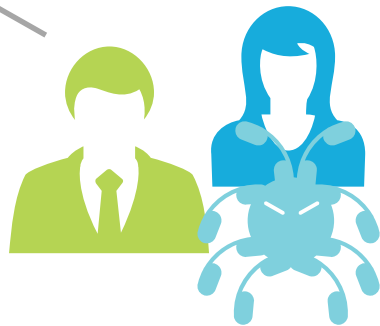
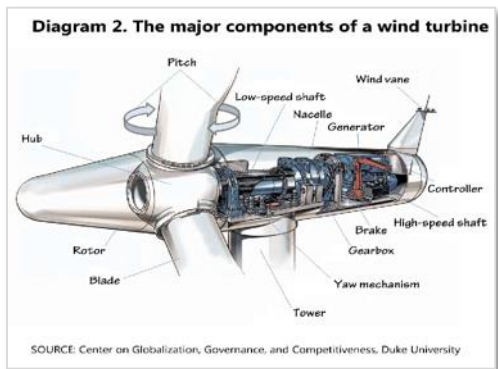
5. Click vào Setting để thay đổi kích thước, font chữ hiển thị.



6. Cuối cùng, click vào Auto-Scroll to Bottom để luôn hiển thị thời gian thực.

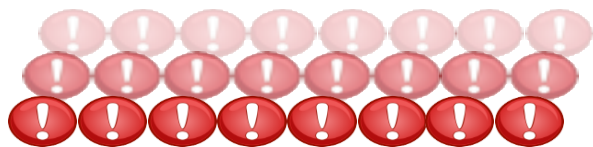
Watering hole

AKA: Strategic Web Compromise



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

Strategie ochrany proti moderním hrozbám



Všechno musí projít trychtýřem



Co nejmenší plocha pro útok

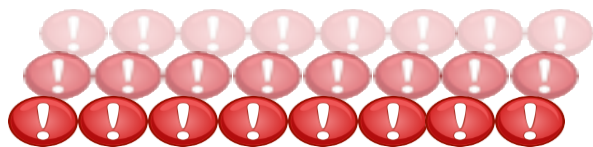
Zastavení známých hrozeb

Zjištění a zastavení neznámého

Vyšetřování a odezva

- Ne jen HTTP a SMTP, ale všechny protokoly, všechny aplikace
- ~10% malware přichází jinudy než přes Web & Email
- ~40% webového malware přichází šifrovaně

Strategie ochrany proti moderním hrozbám



Všechno musí projít trychtýřem

Co nejmenší plocha pro útok

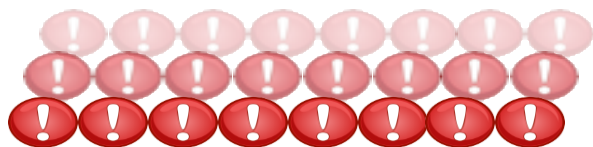
Zastavení známých hrozeb

Zjištění a zastavení neznámého

Vyšetřování a odezva

- Rizikové aplikace a funkce
- Blokace typů souborů s dlouhodobě špatnou pověstí
- Blokace spustitelných souborů z neznámých URL adres

Strategie ochrany proti moderním hrozbám



Všechno musí projít trychtýřem

Co nejmenší plocha pro útok

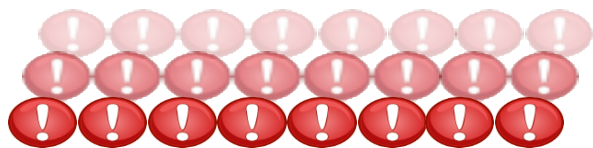
Zastavení známých hrozeb

Zjištění a zastavení neznámého

Vyšetřování a odezva

- Exploity, malware, C2
- Varianty a polymorfní hrozby
- DNS, URL odkazy, zdroje škodlivého obsahu

Strategie ochrany proti moderním hrozbám



Všechno musí projít trychtýřem

Co nejmenší plocha pro útok

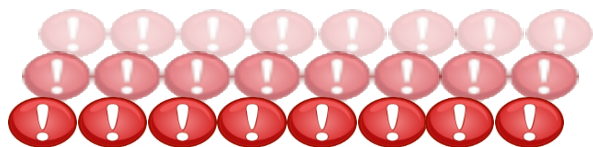
Zastavení známých hrozeb

Zjištění a zastavení neznámého

Vyšetřování a odezva

- Analýza chování a hledání anomálií
- Automatické vytvoření a doručení ochrany
- Globální sdílení

Strategie ochrany proti moderním hrozbám



Všechno musí projít trychtýřem

Co nejmenší plocha pro útok

Zastavení známých hrozeb

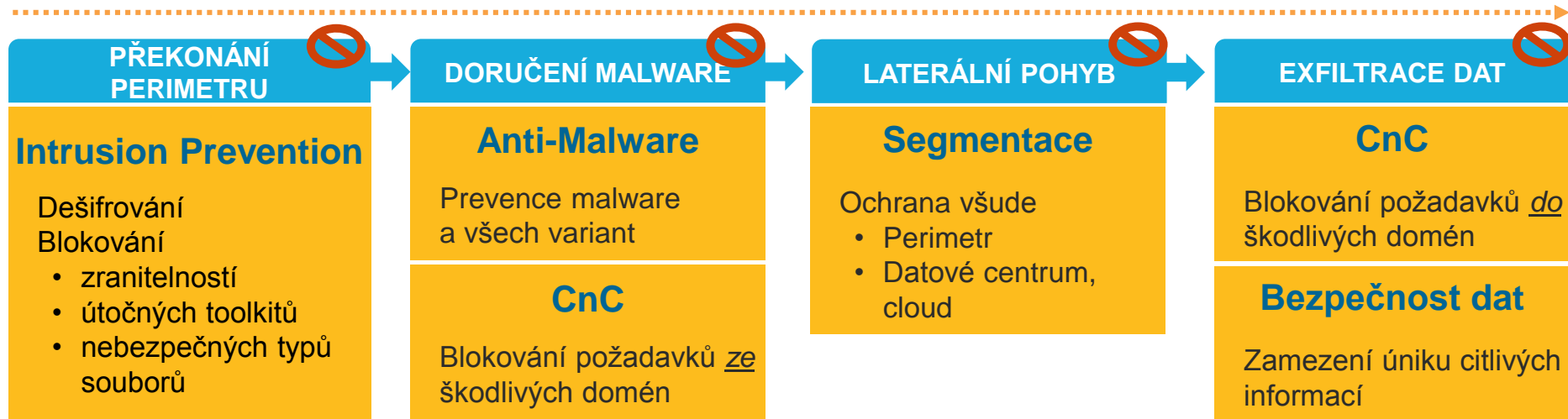
Zjištění a zastavení neznámého

Vyšetřování a odezva

- Nalezení ukazatelů nákazy (IOC)
- Doplnění kontextu

Zero Trust: bezpečnost ve všech vrstvách

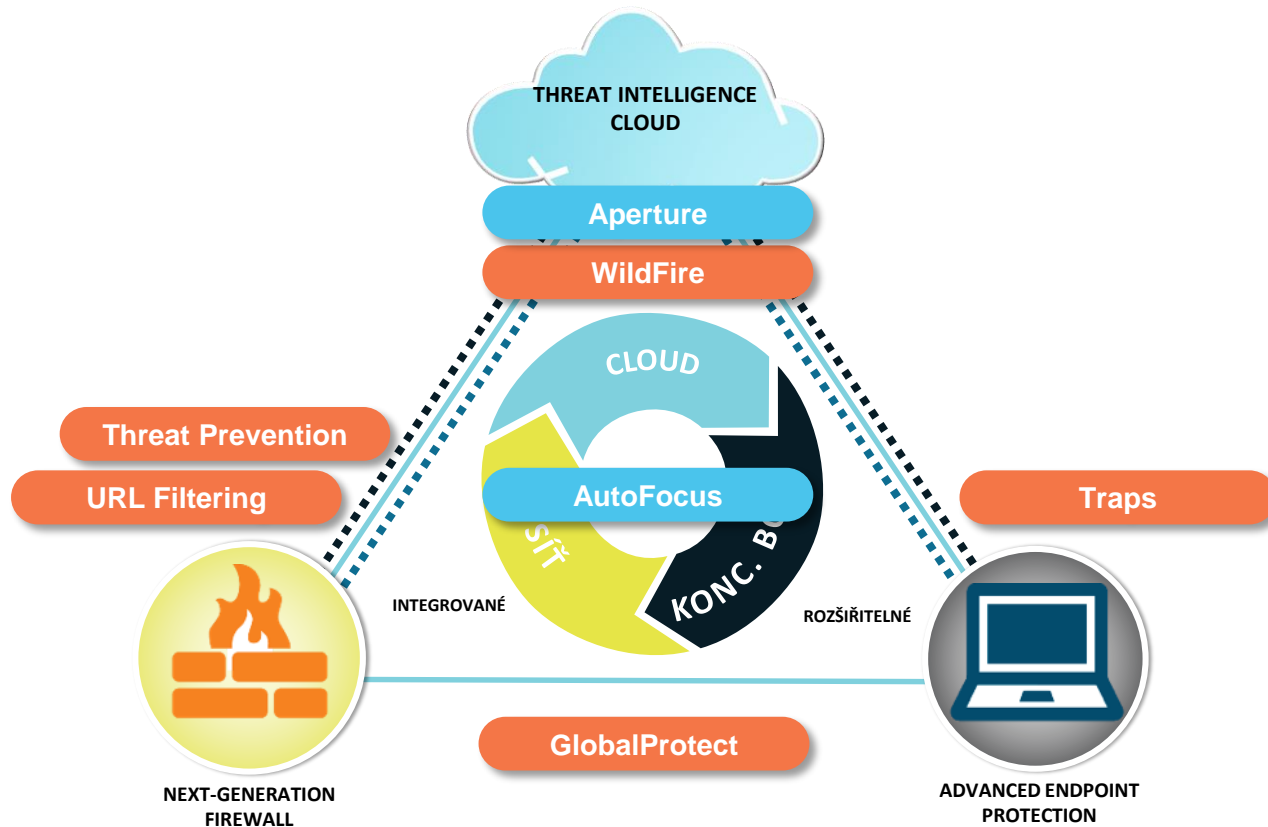
ZABRÁNĚNÍ HROZBÁM V KAŽDÉ FÁZI KYBERNETICKÉHO ÚTOKU



Threat Intelligence Cloud

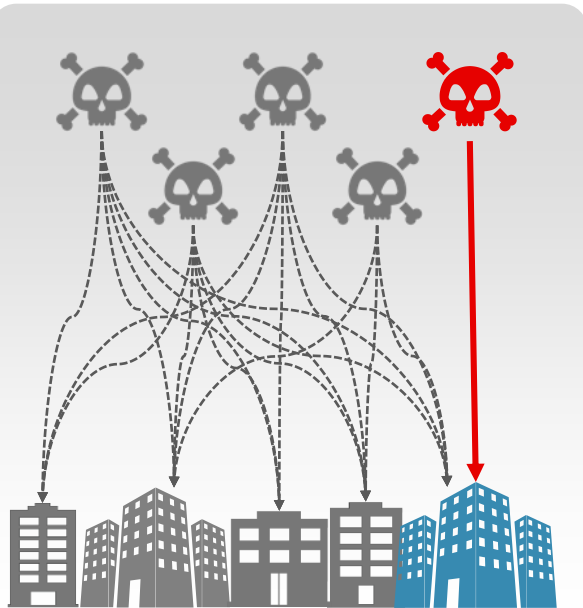
Detailní analýza, zevrubný reporting, korelace hrozeb, denní aktualizace vytvořených signatur

NEXT-GEN BEZPEČNOSTNÍ PLATFORMA

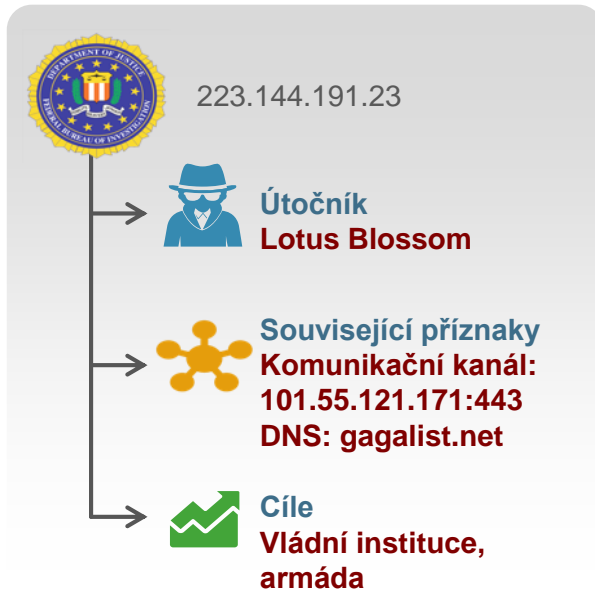


AutoFocus – vyšetřování a odezva

Prioritizace důležitých událostí




Kontext incidentů a jejich klíčových znaků



Rychlá a proaktivní reakce



Automatický export cenných příznaků útoku (IOC) do bezpečnostních prostředků

 Zamezení budoucím útokům

