Inteligentní NGFW aneb když obyčejné NGFW již ve světě ISP nestačí

Ing. Martin Ťupa

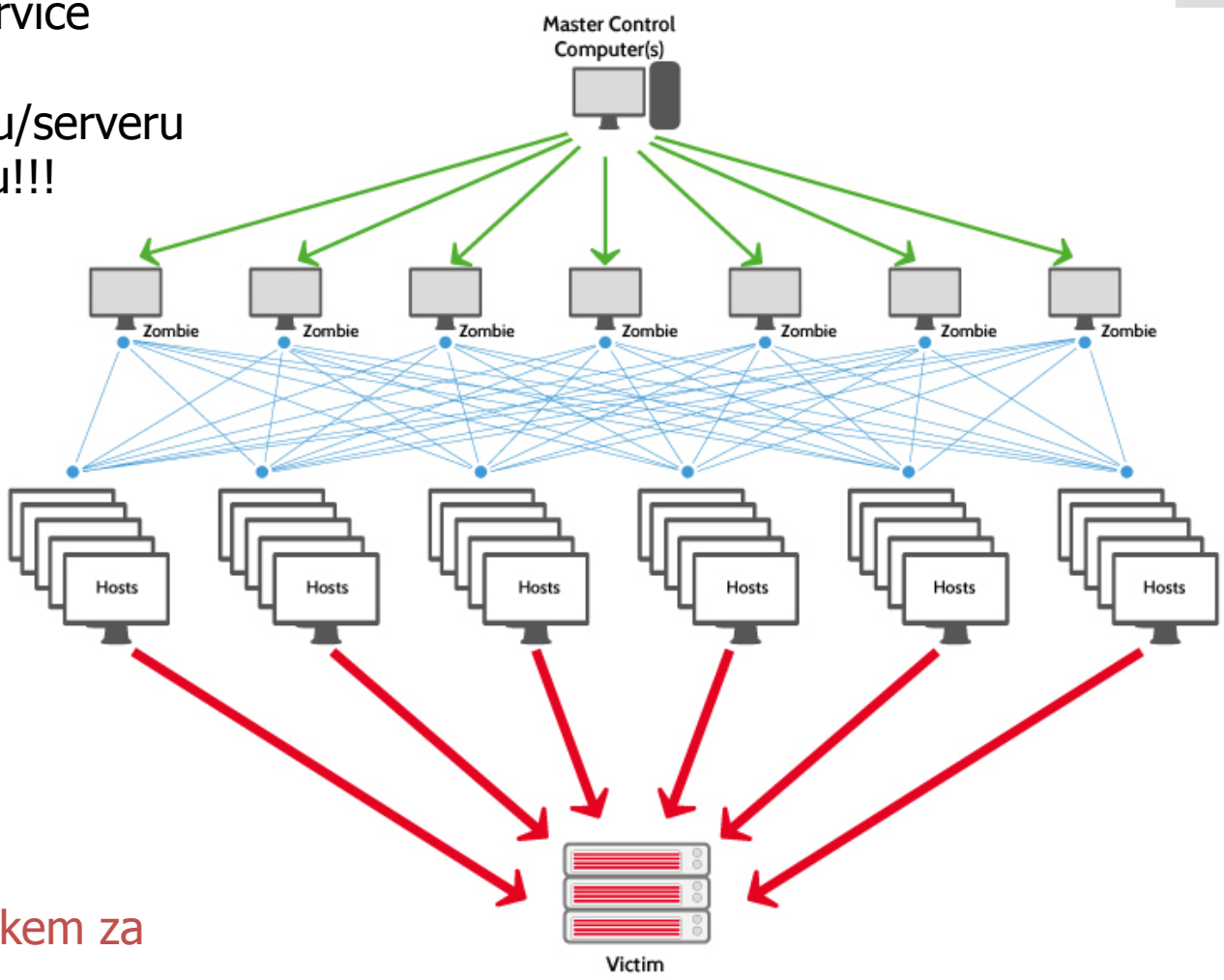
KKTS 2016 - Sk

13.10.2016 Demanovská Dolina - Jasná

Hrozby v ICT dnešních dnů
a
Jak ohrožuje ekonomiku firem
a
Proč klást velký důraz na bezpečnost

Reálná zkušenost s DDoS útokem

- Distributed Denial of Service
- Nedostupnost služeb
- Saturace aktivního prvku/serveru
- Objednávka DDoS útoku!!!
- Jaká je obrana?



- 28% on-line firem v ČR
- 32% v EU
- 38% ve světě
  se potkalo s DDoS útokem za posledních 12 měsíců

Zdroj: B2B International

Další možné Hrozby

- Botnetem infikovaná stanice z lokální sítě zavlečená do DDoS útoků
  - Neobvyklé komunikace
  - Odchylky od standardního chování stanic a celé sítě
- Změna používaného DNS serveru na stanici
  - Možnost manipulace s DNS záznamy a přístupem na webové servery, Geolokace
- Útok na autentizaci http služeb
  - Pokusy o uhodnutí hesla pro phpMyAdmin
- Internet of Things botnety
  - Většina zařízení není vyvíjena s ohledem na bezpečnost
- Kyberkriminalita jako služba
  - Konkurenční boj
- Zero Day útoky

Spojení se silným partnerem jehož technologie řeší bezpečnost na vysoké úrovni

Představení Hillstone

Hillstone NETWORKS

World Class Team

- Experienced leadership from Netscreen, Cisco, Juniper, Intel

- Founded in *2006* by founding engineers from Netscreen
- *10,000+* customers in *27* countries: financial, telecom, education
- *500+* employees globally, *>50%* in engineering

Gartner

IDC Analyze the Future

FROST & SULLIVAN 2014 BEST PRACTICES AWARD

RED HERRING GLOBAL 100 WINNER
2012 Red Herring 100 Global Winner

PROFICOMMS value added distributor

www.proficomms.cz

- ***Americká*** společnost založená v roce ***2006*** lidmi z Netscreen
  - Vedoucí zkušenosti z Cisco, Juniper, Intel
- ***10,000+*** zákazníků z ***27*** zemí: finančnictví, telekomunikace, vzdělání
- ***500+*** zaměstnanců celosvětově, ***>50%*** technických inženýrů

CZ

Řešení pro ISP, malé a střední podnikové sítě, Enterprise

S série – Network Intrusion Prevention System

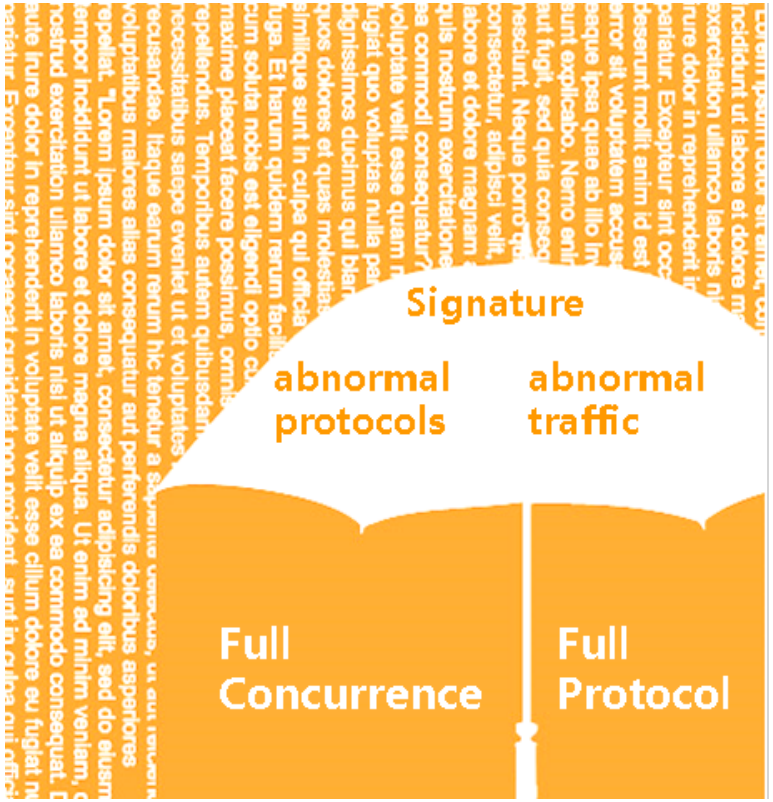
- Systém prevence průniků IPS
- Velmi podrobný a uživatelsky nastavitelný reporting
- Centrální management a jednoduchá instalace

E série – Next Generation FireWall

- Komplexní síťová ochrana s přidanou hodnotou
- Granulární řízení aplikací
- Proaktivní ochrana proti hrozbám

L2-L7 komplexní bezpečnostní ochrana

Vysoká výkonost a vysoce účinné IPS, AV, detekce-URL nástroje k identifikaci a filtrování všech aplikací a provozu včetně SSL šifrovaného provozu

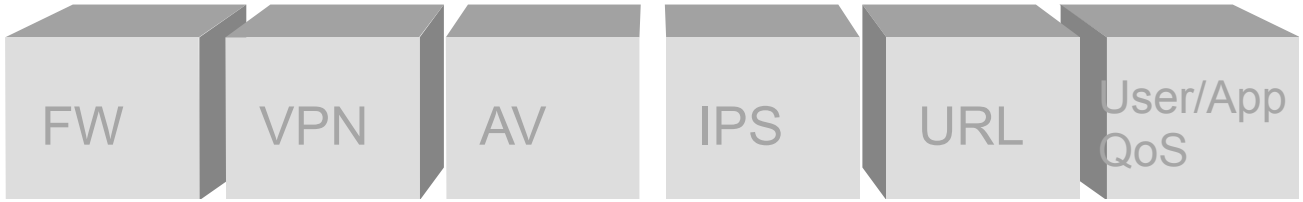


- Prevence SQL insertion, XSS cross-site scripts.
- Prevence DoS/DDoS network-layer útoky.
- Profesionální Botnet filtering a izolace.
- Two-way attack detection, and full traffic protection.
- Firewall linkage. Rapidly blocks attacks.

Klíčové požadavky moderních firewallů

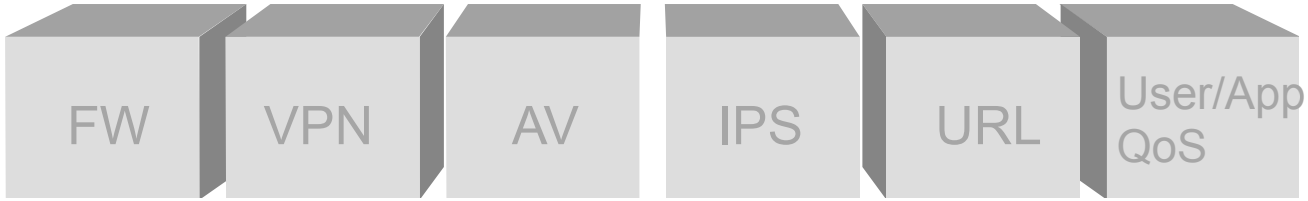
- Identifikace aplikací nikoliv portu
  - Možnost tvorby vlastních signatur pro aplikační detekci
- Identifikace uživatelů jménem nikoliv jen dle IP adresy
  - Forenzní vyhledávání
- Identifikace obsahu komunikace
  - Analýza šifrované komunikace v reálném čase
- Blokování hrozeb v reálném čase
  - Chrání síť před zranitelnostmi
- Zjednodušení správy bezpečnostních politik
  - Jednoduchá editace bezpečnostních politik
- Využití multi-gigabitové propustnosti
  - Nízká latence
- Virtualizace
  - V rámci jednoho fyzického boxu více virtuálních firewallů

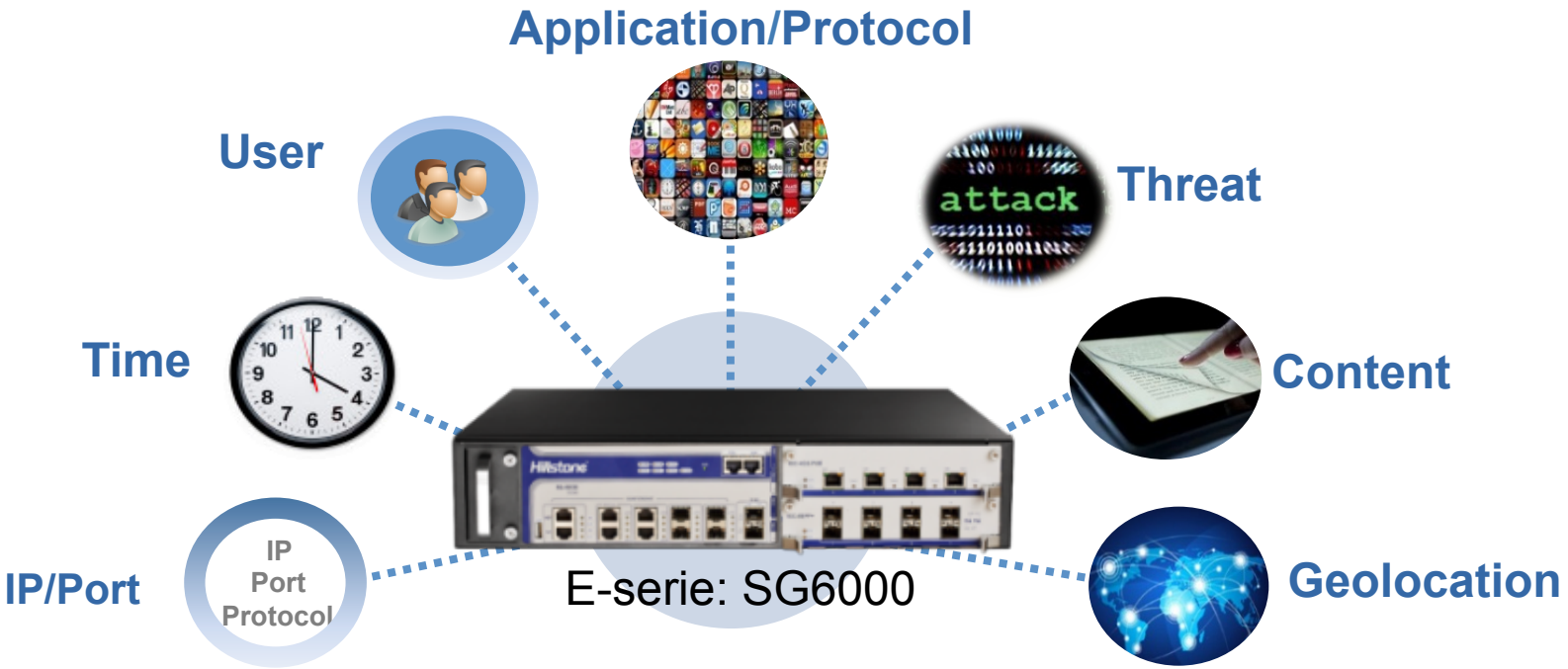
Řešení Hillstone - NGFW



Next Generation FireWall

FireWall nové generace NGFW

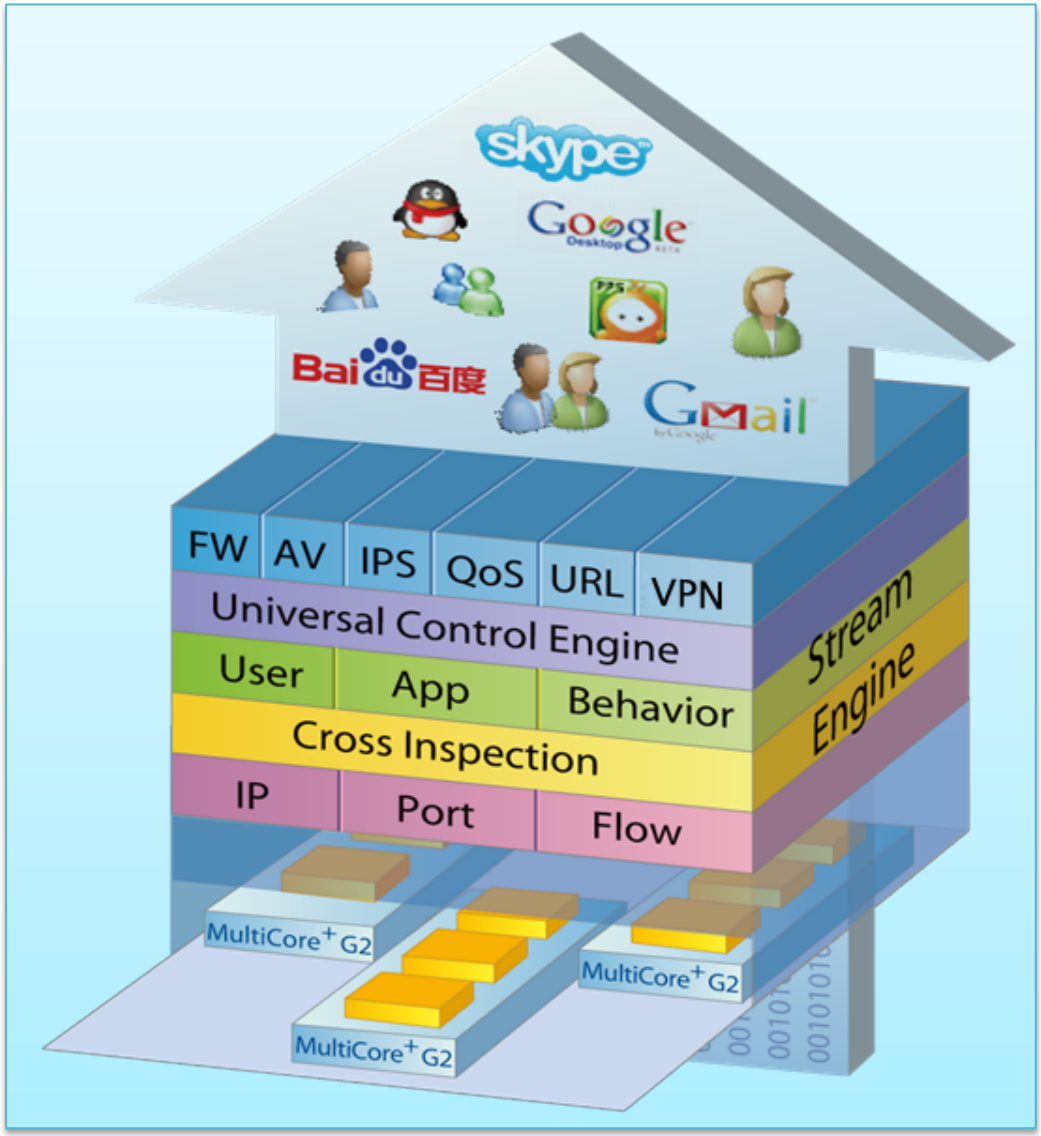




PROFICOMMS value added distributor

Hillstone® NETWORKS

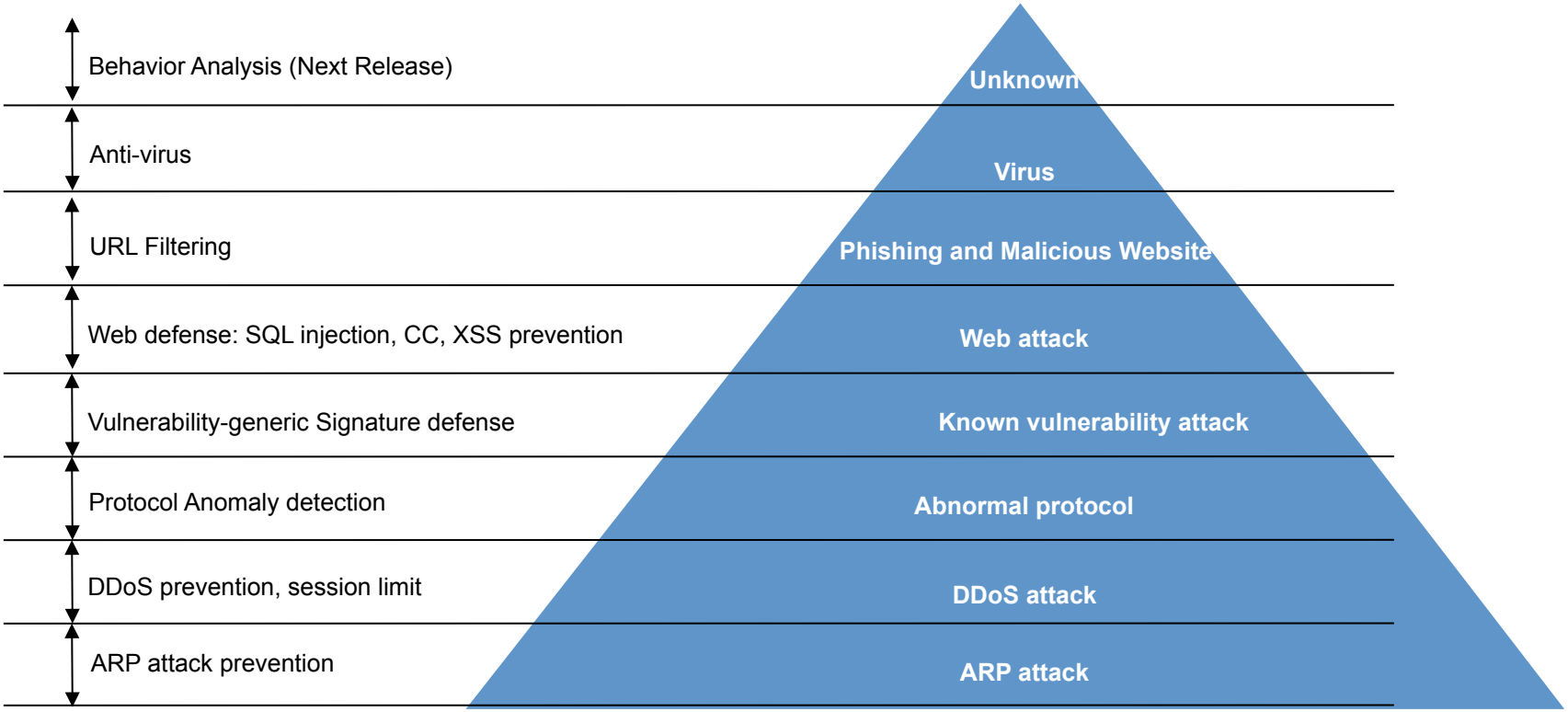
Parallel Architecture Delivers High Performance



- Multi-core and multi-CPU architecture provides high performance
- Each core provides security functions independently of each other
- Same-session can be handled on all cores concurrently
- Unified security engine provides security processing once, thereby reducing latency

Comprehensive L2-L7 Protection

The best defense is always full protection!

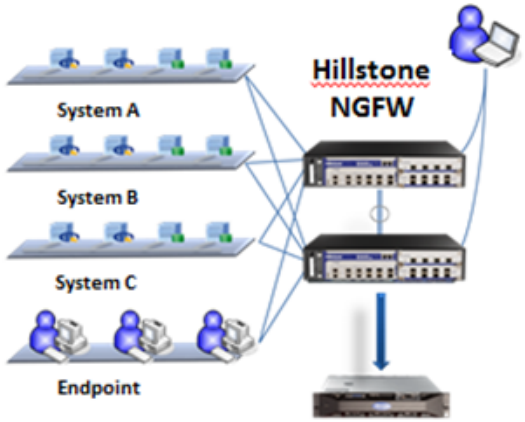


Možnosti nasazení – Hillstone NGFW

Internet Access

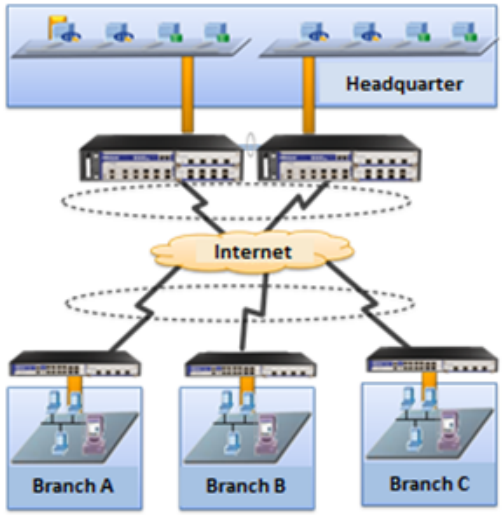
- Granulární a výkonný management – aplikace, uživatel, ..
- Komplexní ochrana internetových hrozeb
- Podpora více nezávislých ISP operátorů a silný aplikační routing s QoS prioritizací

Server Protection



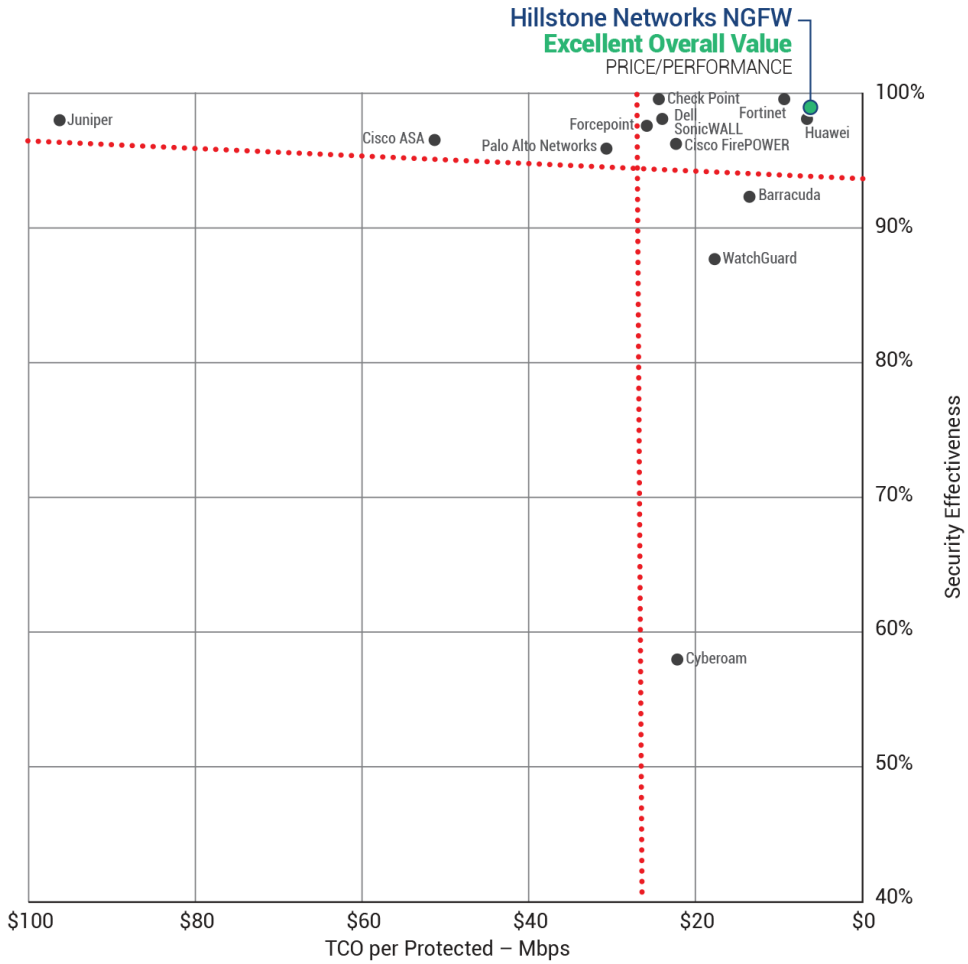
- Flexibilní řízení přístupových politik
- Profesionální ochrana WEB serverů
- Bezpečnostní ochrana Virtuálních obchodů
- Vysoká Dostupnost - redundance

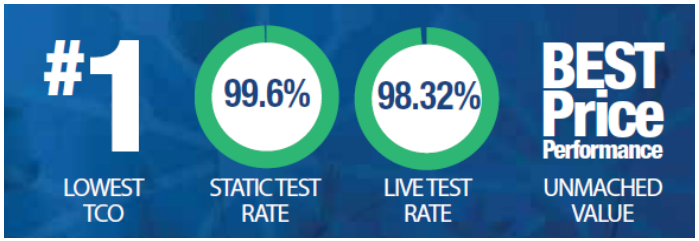
Branch VPN Connection



- Malé zpoždění, vysoká výkonost VPN přístupů
- Jednoduché nasazení IPsec VPN
- Centrální management a monitoring
- Dvoufaktorová autentizace

NSS Labs Recommended NGFW - The Best TCO!





NSS LABS RECOMMENDED

99.60%
Block Rate in Static test

98.32%
Block Rate in Live Test

iNGFW
Unikátní a inteligentní technologie

iNGFW
Unikátní a inteligentní technologie

T série – Inteligentní Next Generation Firewall

- Kontinuální monitoring Vaší sítě a statistický clustering
- Behaviorální a forenzní analýza, Kill Chain - grafické zobrazení průběhu útoku
- Mittigace - automatické zablokování datového toku při útoku

Behavior Learning & Modeling

Abnormal behavior Analysis

Threat & Risk Identification

iNGFW
Unikátní a inteligentní technologie

T série – Inteligentní Next Generation Firewall

- Kontinuální monitoring Vaší sítě a statistický clustering
- Behaviorální a forenzní analýza, Kill Chain - grafické zobrazení průběhu útoku
- Mittigace - automatické zablokování datového toku při útoku

- Host/server behavior modeling by adaptive machine learning
- Layer 4-7, hundreds of behavior dimensions

Abnormal behavior Analysis

- Real time Behavior Model and rules
- Identify abnormal dimensions by behavior partnering

Threat & Risk Identification

- Quantitate risk severity and certainty by correlation analysis
- Threat forensics including suspicious and relevant PCAP

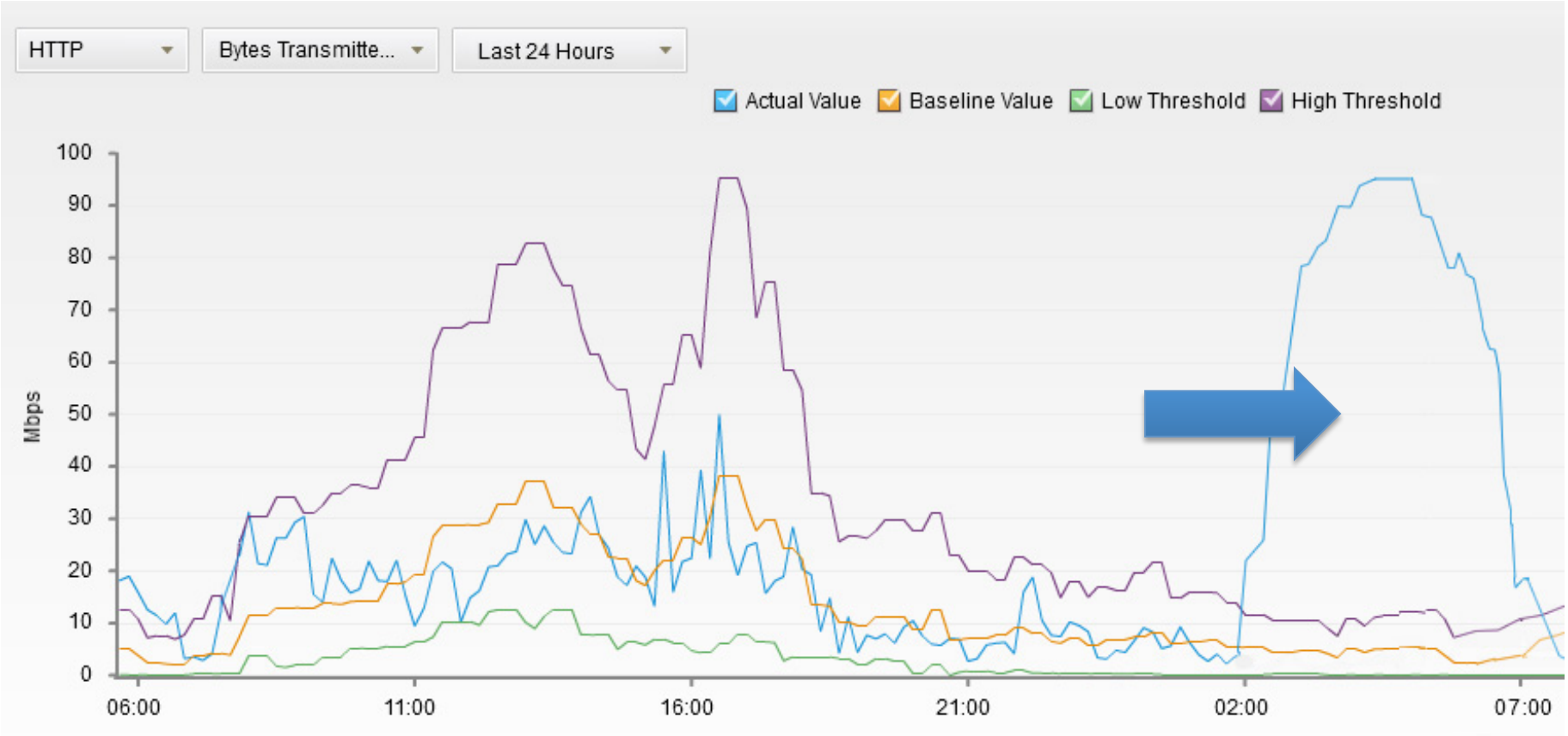
iNGFW
Unikátní a inteligentní technologie

- ABA
- ATD
- Mitigation
- Kill Chain
- Risk Index
- Forenzní analýza
- Statistical Clustering

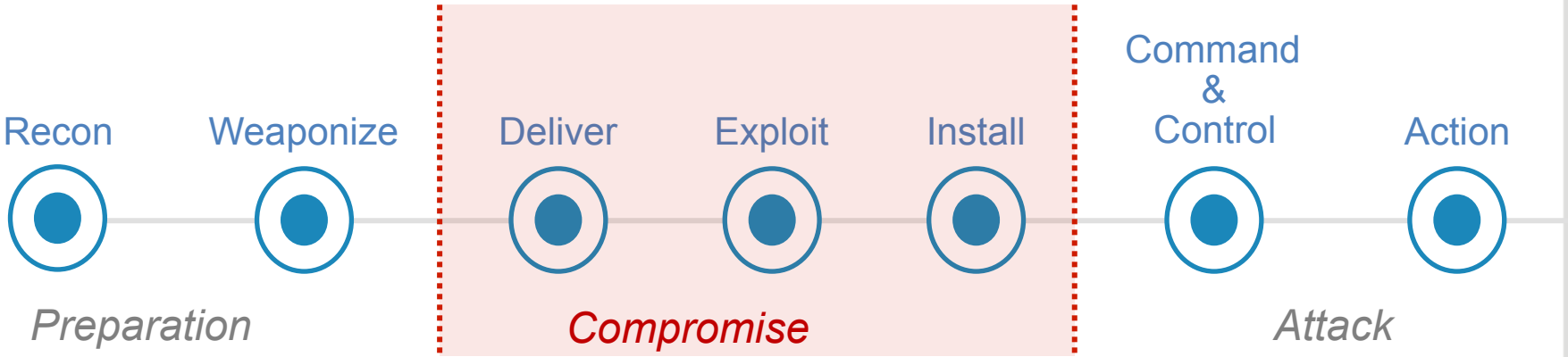
Bezpečnostní nástroje iNGFW

- ABA
- ATD
- Mitigation
- Kill Chain
- Risk Index
- Forenzní analýza
- Statistical Clustering

Behavior Analysis



Hillstone Stops Attacks at Every Step in the Kill Chain



Traditional FW

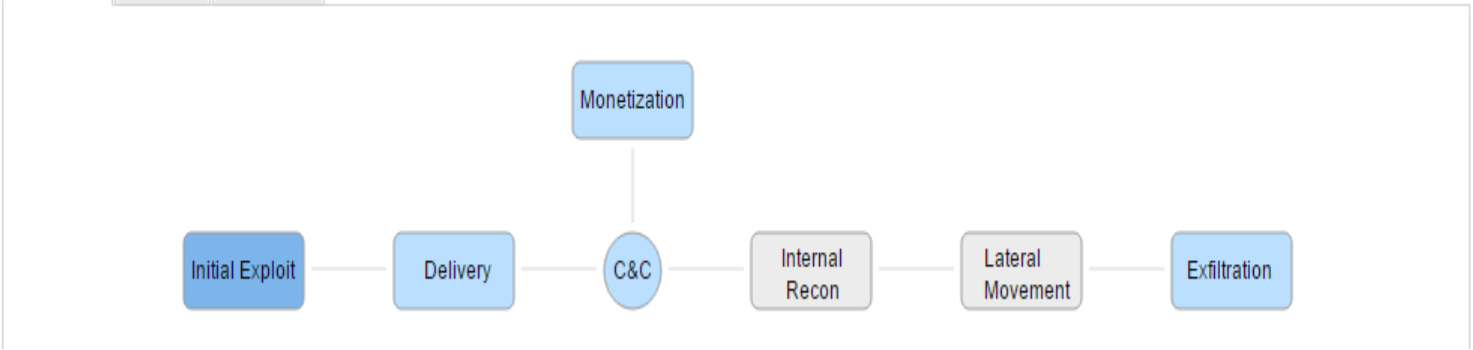
NGFW

Malware Detection Software

Hillstone **Intelligent** NGFW (i+NGFW)

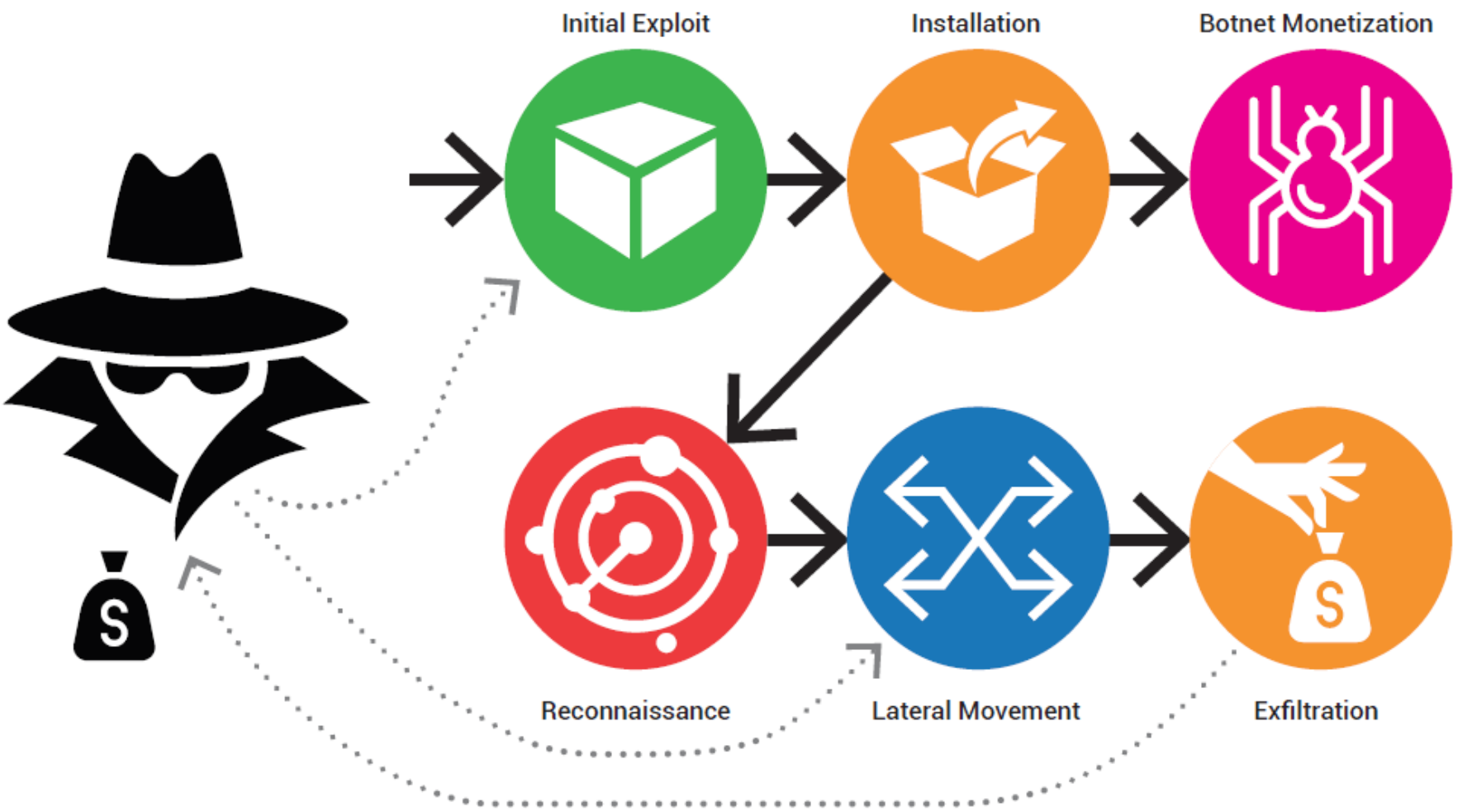
What is kill chain?

- Kill Chain is the classical APT process including seven stages

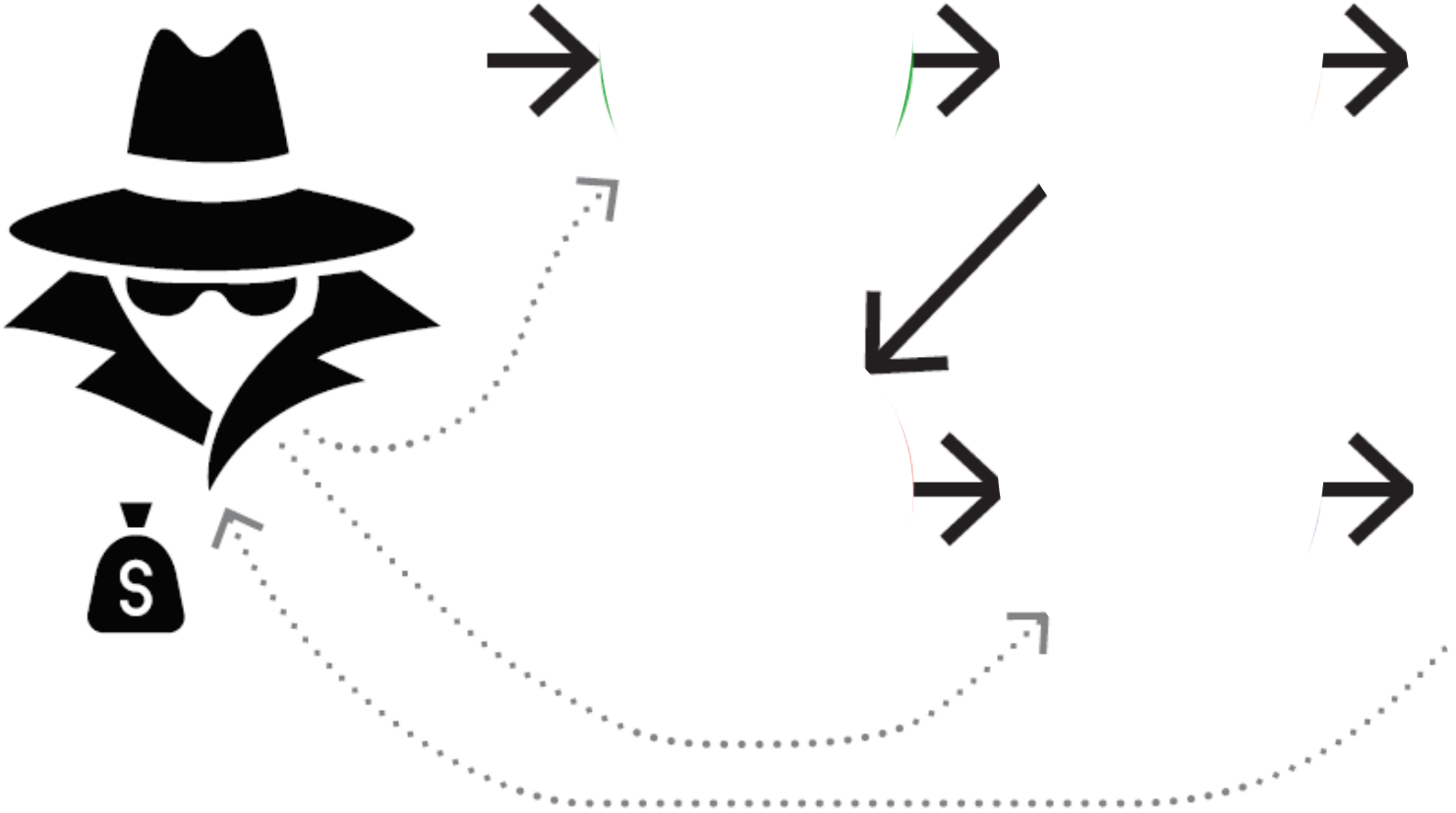


- Kill Chain can show us
  - Who
  - How
  - What

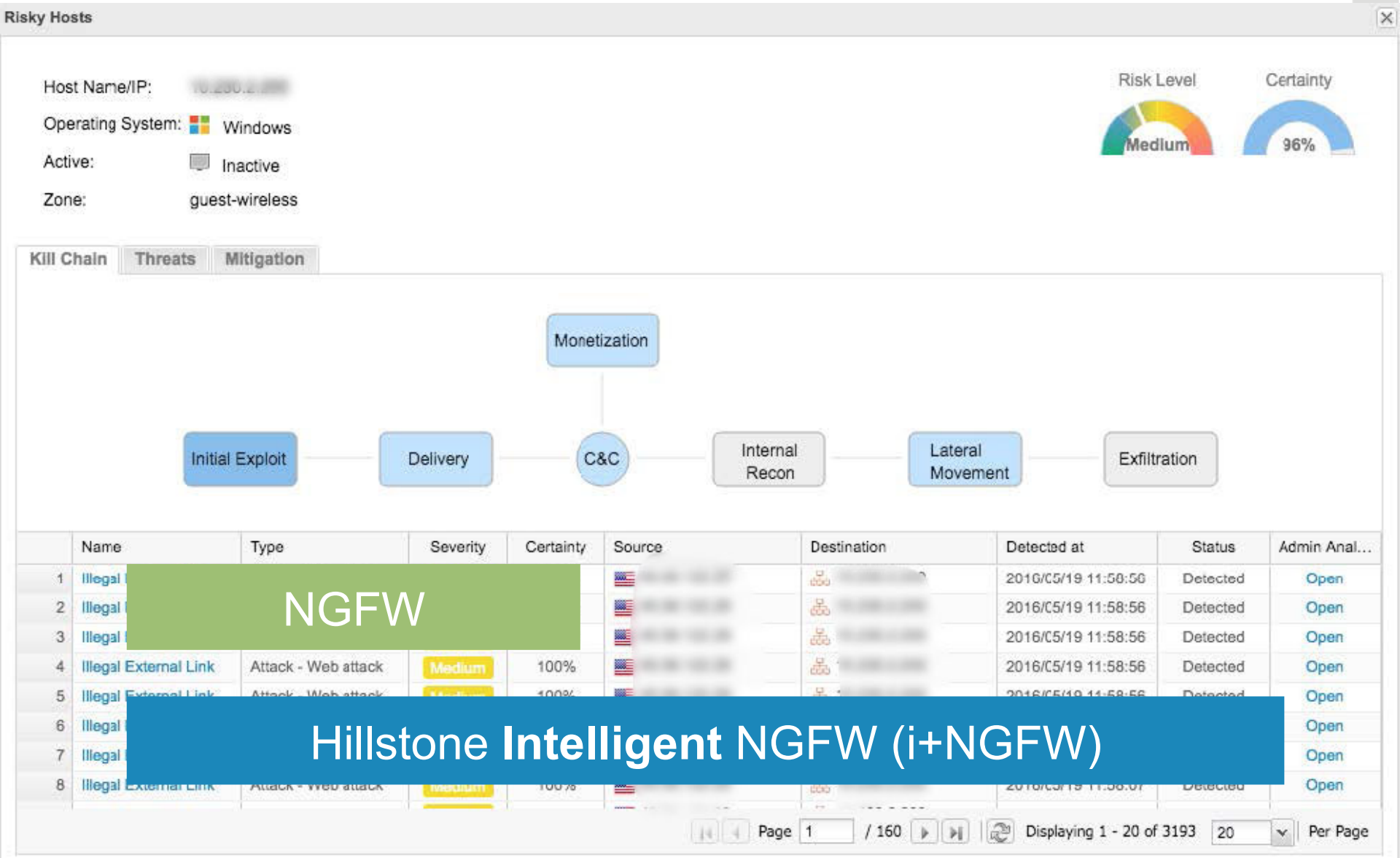
Co je Kill Chain Mapping?



Co je Kill Chain Mapping?



Kill Chain nám ukáže – Kdo, Jak, Co

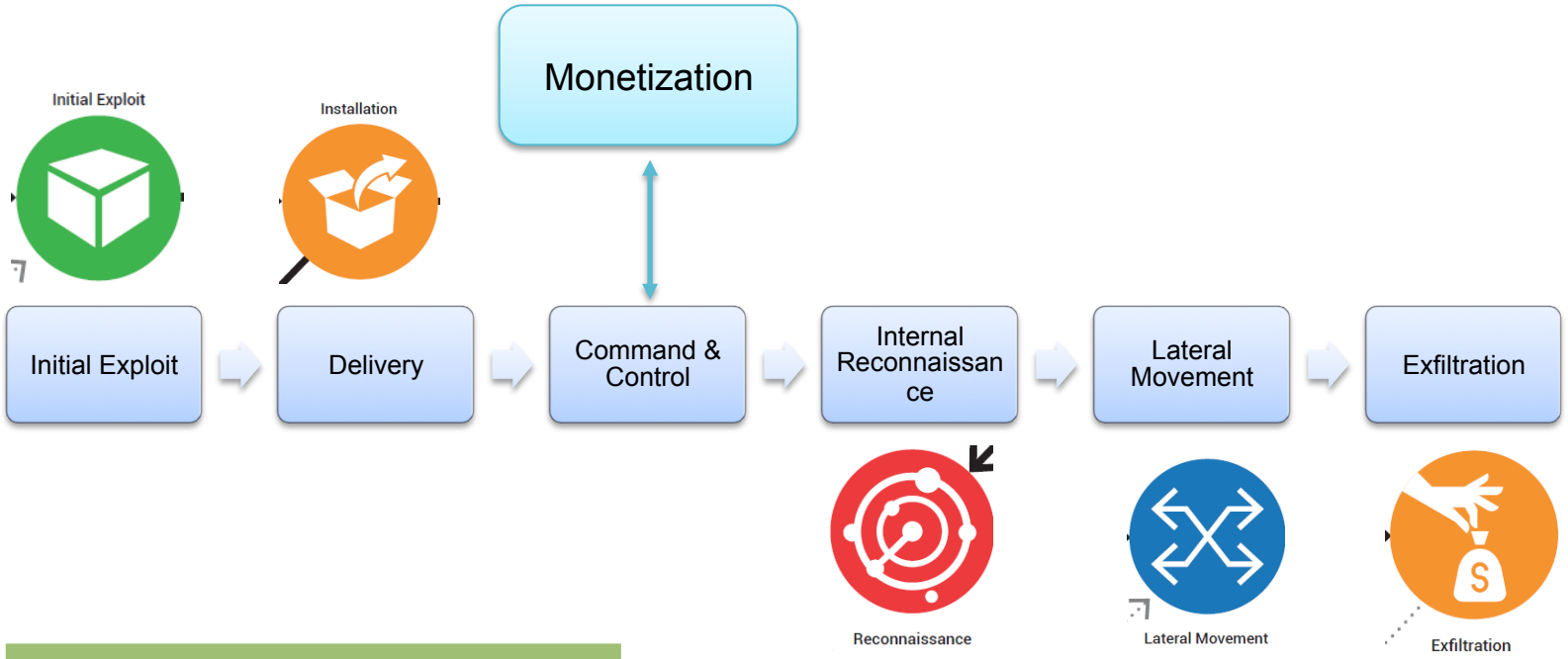


NGFW

Hillstone **Intelligent** NGFW (i+NGFW)

Hillstone Kill Chain nám ukáže – Kdo, Jak, Co

Co je Kill Chain Mapping?



NGFW

Malware Detection Software

Hillstone **Intelligent** NGFW (i+NGFW)

Není to jen o ”technologiích”, ale i o lidech

S kým poletíte raději?

PROFIcomms s.r.o. nabízí svým partnerům k produktům Hillstone přidanou hodnotu v podobě dalších služeb:

- technická podpora (dálková i přímo u zákazníka)
- Pick up file - možnost analýzy logu
- certifikovaní technici – HCSA a HCSP certification

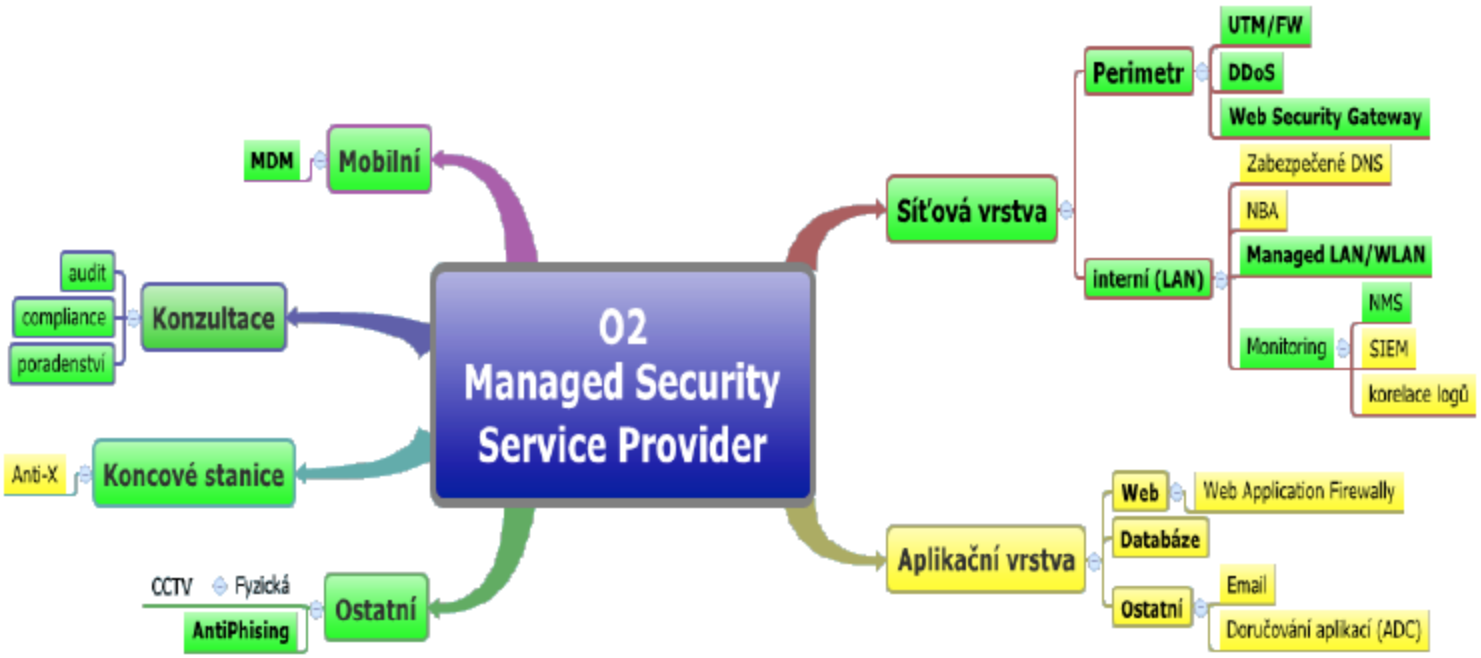
Máte pokryty všechny možnosti?

Ing. Martin Ťupa

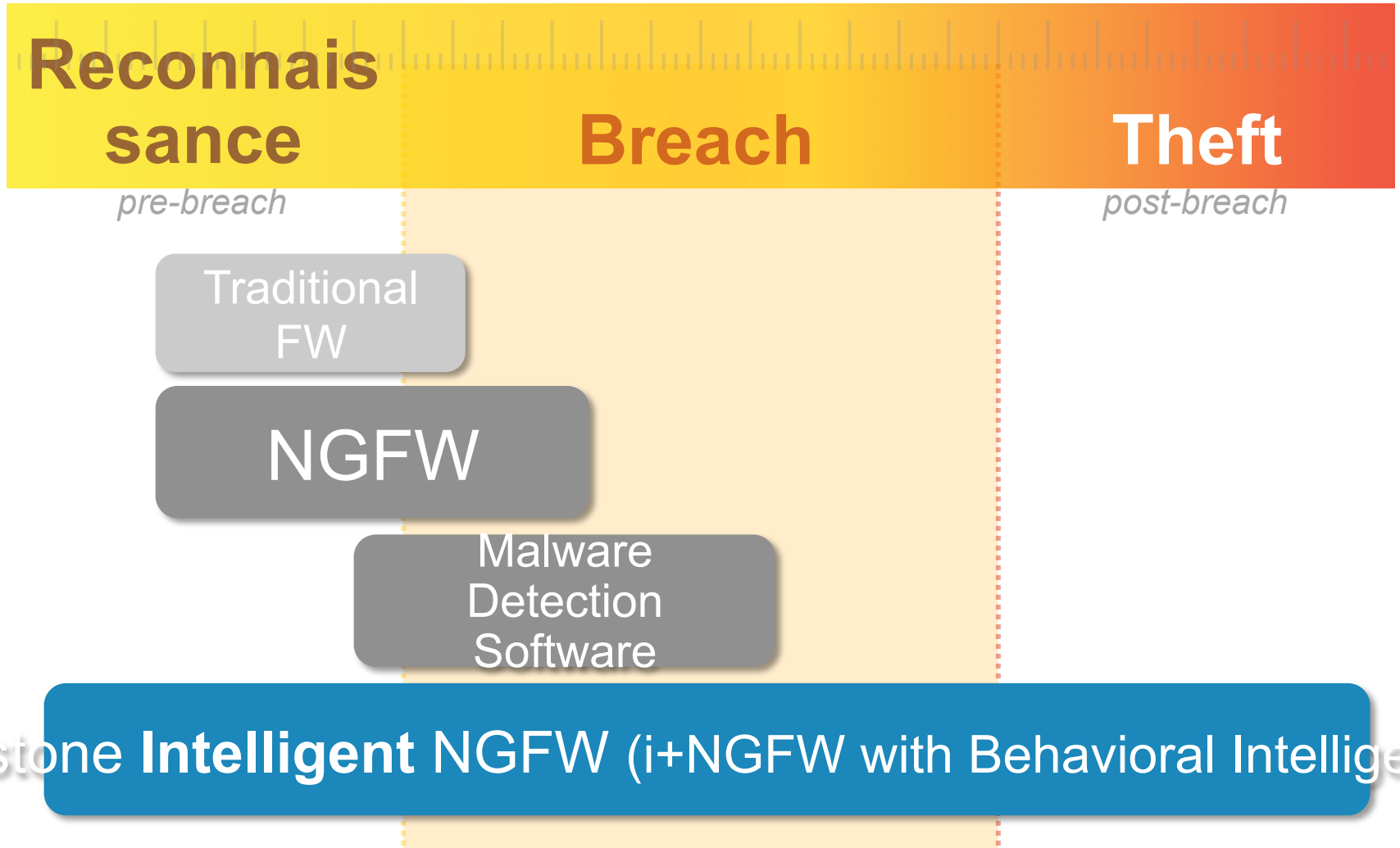
tupa@proficomms.cz

+420 736 625 811

Bezpečnost vyžaduje mnoho vrstev



Hillstone Protects Across the Cyber Kill Chain

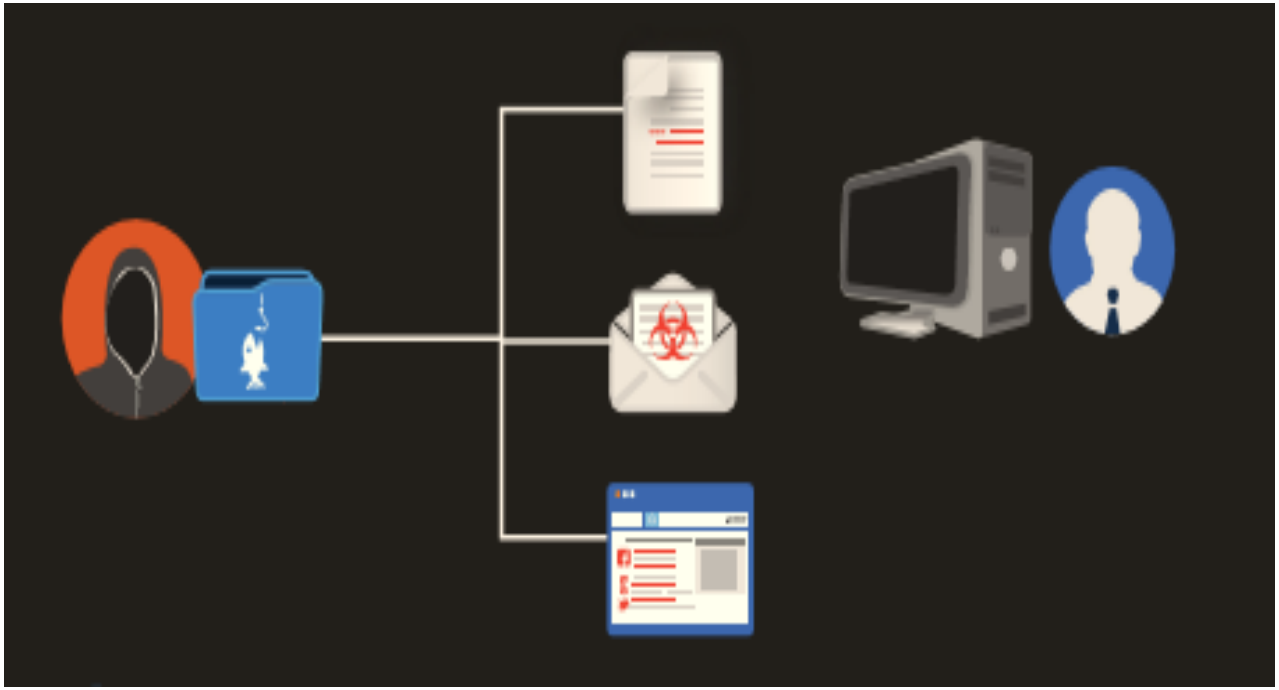


Stage1: Initial Exploit

The attacker identifies and gathers information of the targeted victim hosts. This can be done using means like social networking and publicly available information on the internet or by performing vulnerability and service scanning.

Stage 2 ： Delivery

The attacker transfers exploit and malicious payload to the targeted devices using emails or other means, which can represent the command scripts or instructions that the attacker can use to stage later attacks.



Stage 3&4：C&C/Monetization

The attacker creates a communication channel between the infected host and remote command server to download additional tools and instructions

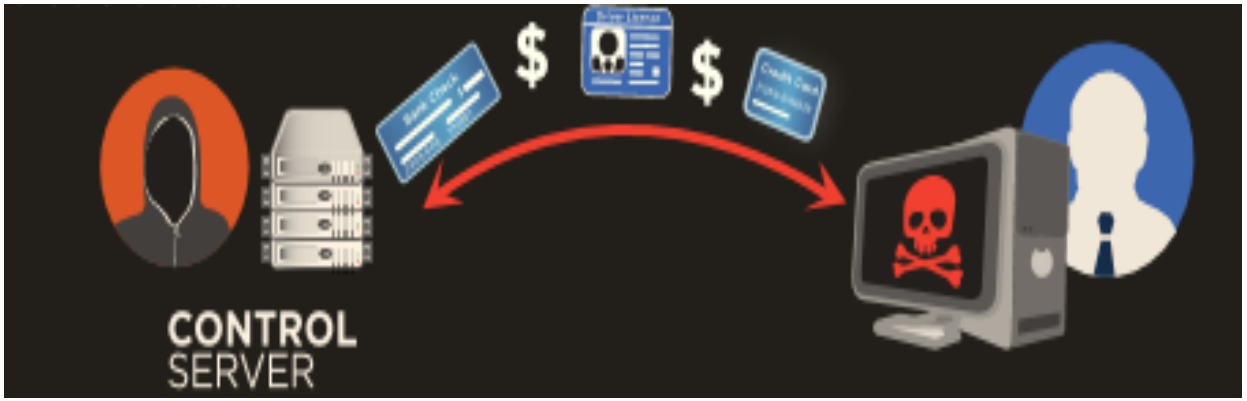
In some cases the compromised hosts are used as “bot machines” of the botnet performing activities whose main purpose is to gain profits.

Stage 5&6：Internal Recon/Laternal Movement

At this stage, the attacker can download additional tools, installing more back doors and take actions such as brute force to gain privileged credentials and access of the identified internal critical assets

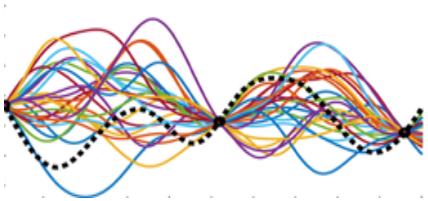
Stage 7：Exfiltration

At this stage, the attacker carries out the main purpose of the attack, to steal information on the compromised system, stolen data such as personal information, intellectual property and other valuable information are transferred of the organization.



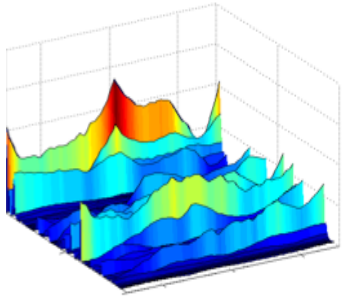
Abnormal Behavior Detection

Behavior Learning & Modeling



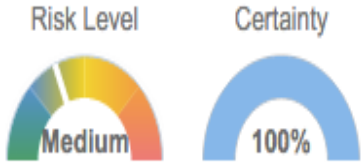
- Host/server behavior modeling by adaptive machine learning
- Layer 4-7, hundreds of behavior dimensions

Abnormal behavior Analysis



- Real time Behavior Model and rules
- Identify abnormal dimensions by behavior partnering

Threat & Risk Identification

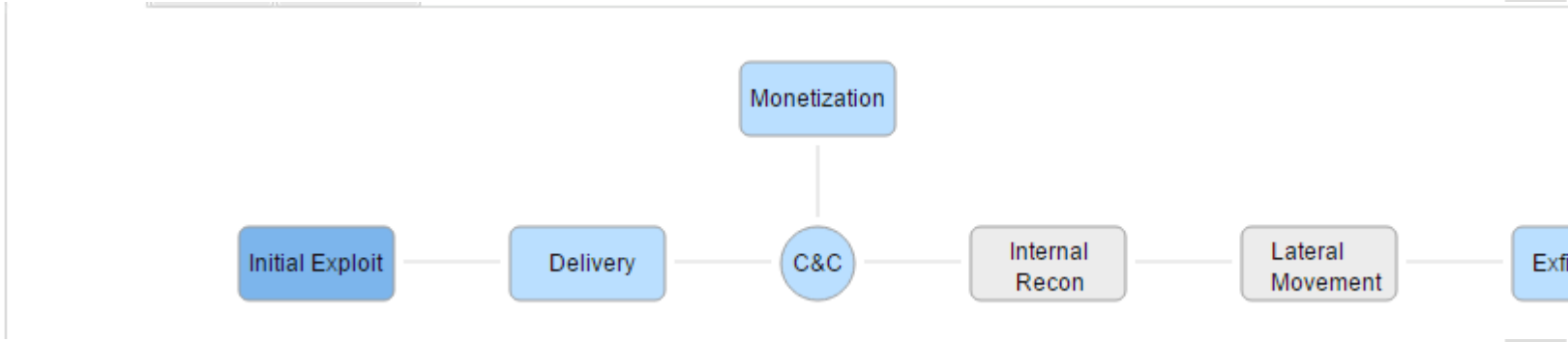


- Quantitate risk severity and certainty by correlation analysis
- Threat forensics including suspicious and relevant PCAP

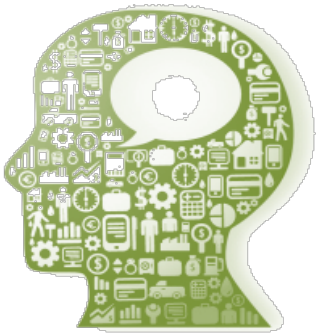
Hillstone Intelligent Next-Generation Firewall

What is kill chain?

- Kill Chain is the classical APT process including seven stages



- Kill Chain can show us
  - Who
  - How
  - What



Risky Hosts

Host Name/IP: DISKSTATION(172.18.10.10)

Operating System:

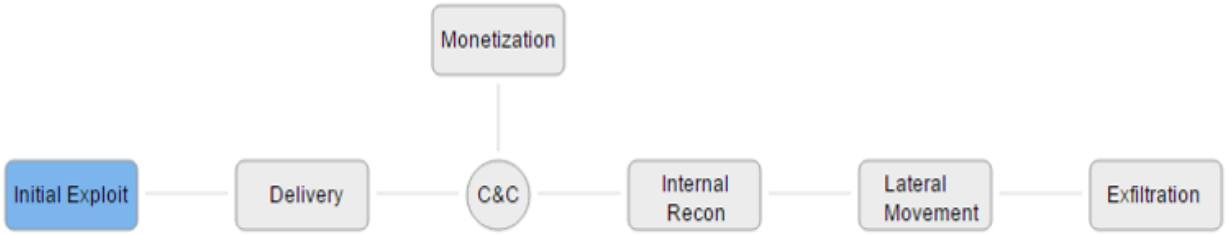
Active: active

Zone: trust

Risk Level: Low

Certainty: 10%

Kill Chain | Threats | Mitigation



	Name	Type	Severity	Certainty	Source	Destination	Detected at	Status	Admin Anal...
1	RPC ONC-RPC v2 ...	Scan - Web Applica...	Medium	100%	216.218.206.99	DISKSTATION(172...	2016/02/07 08:07:48	Detected	Open
2	RPC ONC-RPC v2 ...	Scan - Web Applica...	Medium	100%	216.218.206.123	DISKSTATION(172...	2016/02/06 06:57:13	Detected	Open
3	RPC ONC-RPC v2 ...	Scan - Web Applica...	Medium	100%	216.218.206.79	DISKSTATION(172...	2016/02/05 06:42:19	Detected	Open