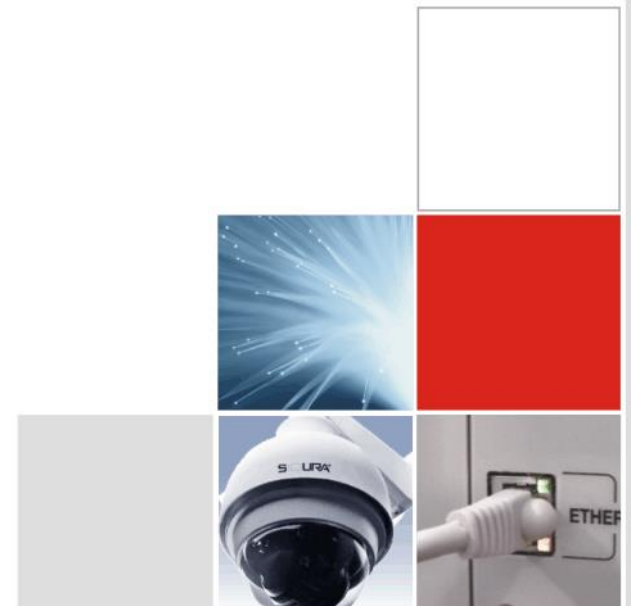


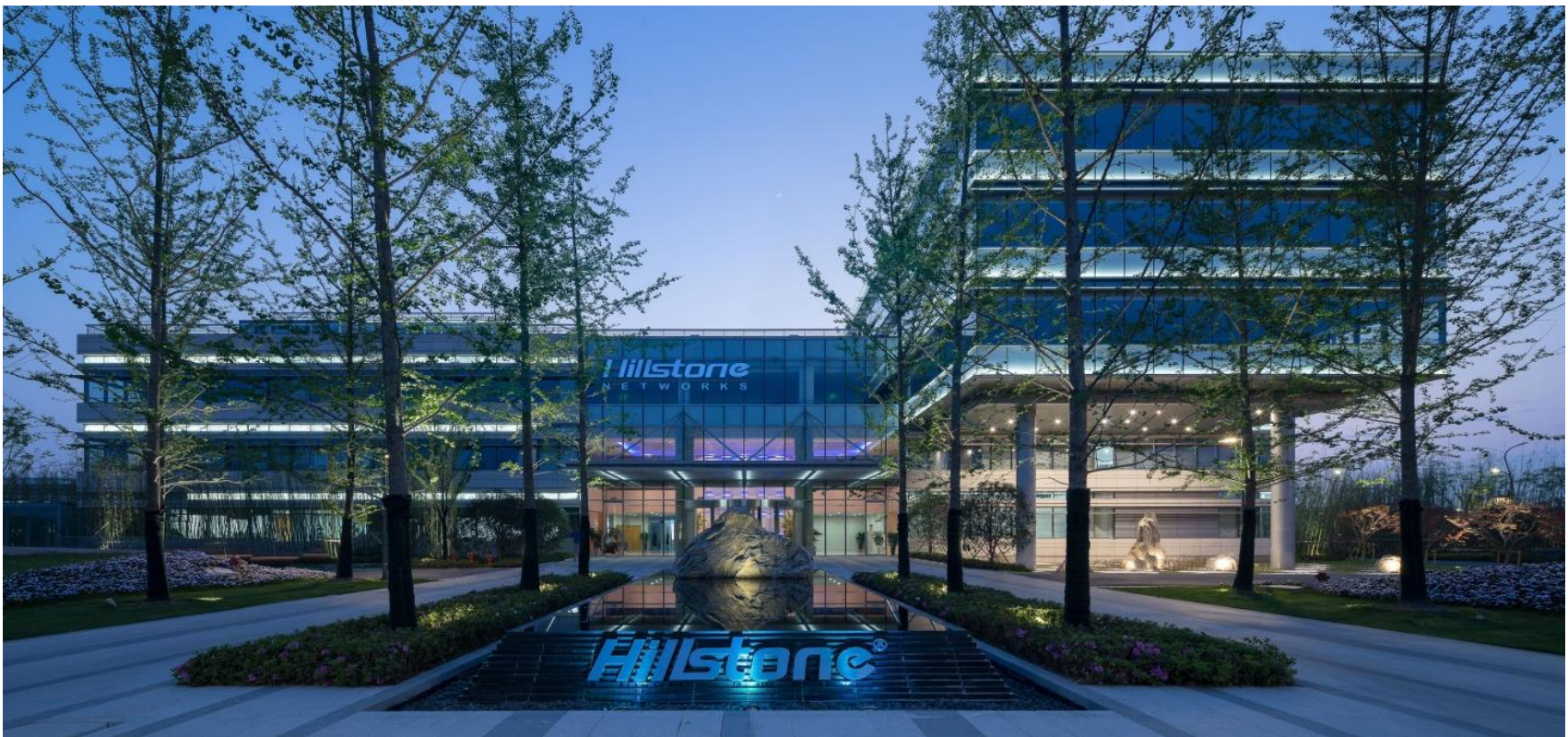
iNGFW – účinná automatizovaná ochrana proti aktuálním kybernetickým hrozbám

Ing. Martin Ťupa

Seminář FTTx

09.03.2017 Brno





- **Americká** společnost založená v roce **2006** lidmi z Netscreen
 - Vedoucí zkušenosti z Cisco, Juniper, Intel
- **12,000+** zákazníků z **27** zemí: finančnictví, telekomunikace, vzdělání
- **500+** zaměstnanců celosvětově, **>50%** technických inženýrů



Základní filozofie prevence



ÚPLNÁ
VIDITELNOST

MENŠÍ PLOCHA
PRO ÚTOK

ZASTAVENÍ VŠECH
ZNÁMÝCH HROZEB

ODHALENÍ A ZASTAVENÍ
NOVÝCH HROZEB

- Síť i koncové body
- Všechny aplikace, cloud a SaaS
- Všichni uživatelé a zařízení
- Šifrovaná komunikace

- Povolení schválených aplikací
- Zastavení nežádoucích aplikací
- Omezení funkcí aplikací
- Omezení rizikového obsahu

- Zneužití zranitelnosti
- Škodlivý kód
- Command & control
- Škodlivé a phishingové weby
- Nakažené domény

- Neznámí škodlivý kód
- Zero-day zneužití zranitelnosti
- Nové chování útoků

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
- Mitigace - automatické zablokování datového toku při útoku



Behavior Learning & Modeling



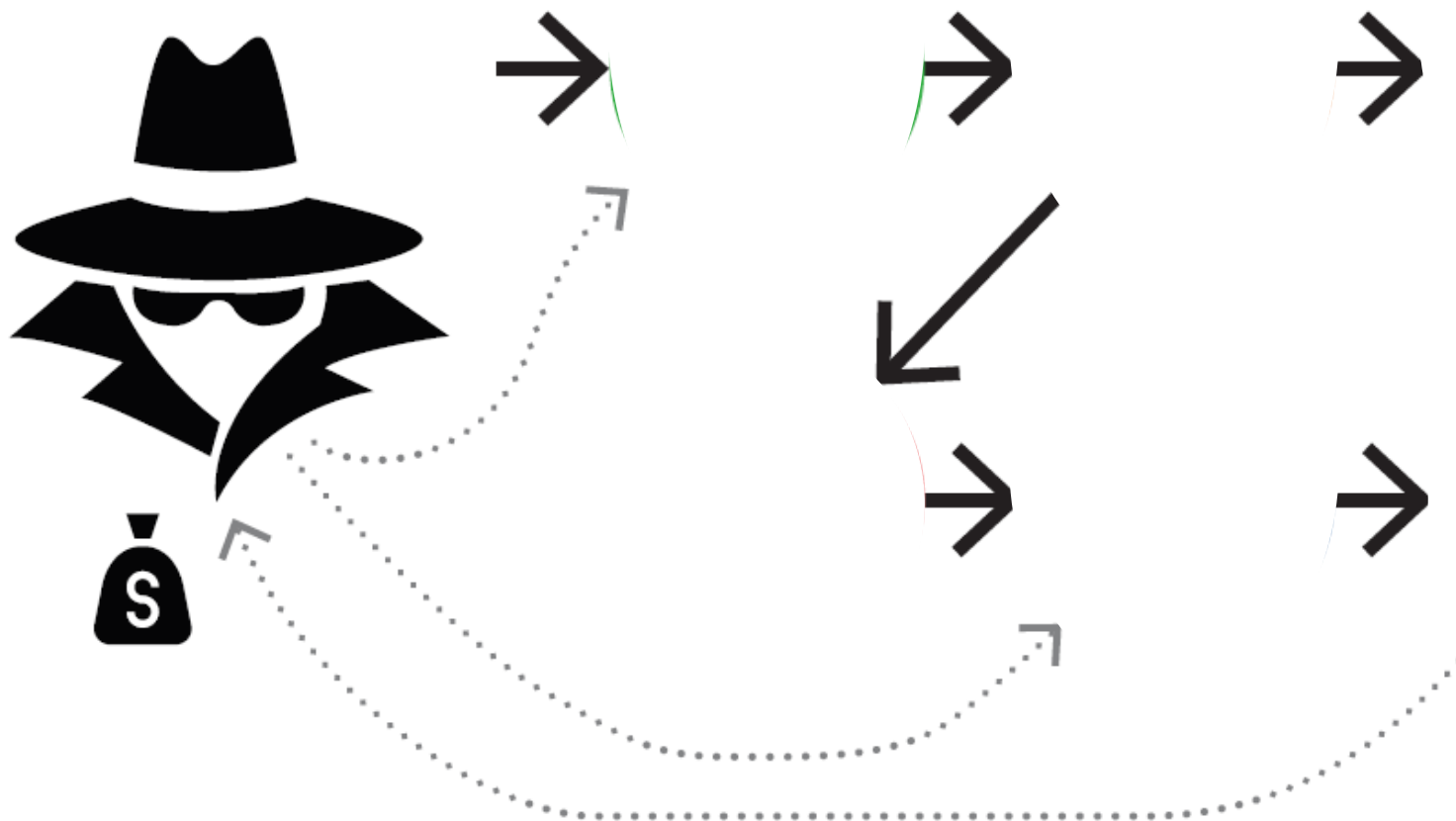
Abnormal behavior Analysis



Threat & Risk Identification



Co je Kill Chain Mapping?



Hillstone Kill Chain nám ukáže – Kdo, Jak, Co

Risky Hosts

Host Name/IP: 10.210.3.189
Operating System:
Active: Inactive
Zone: vpn

Risk Level: Medium
Certainty: 75%

Kill Chain | Threats | Mitigation

```
graph LR; IE[Initial Exploit] --> D[Delivery]; D --> C[C&C]; C --> IR[Internal Recon]; IR --> LM[Lateral Movement]; LM --> E[Exfiltration]; M[Monetization] --- C;
```

Name	Certainty	Source	Destination	Detected at	Status
1 The Do	100%	208.201.224.11	10.210.3.189	2017/01/26 08:42:10	Detected
2 The Do	100%	8.8.8.8	10.210.3.189	2017/01/26 08:42:06	Detected
3 High Frequency DNS Query	70%	YUEZHANG-SZ(10...	119.28.48.212	2016/06/15 04:03:00	Detected
4 Hidden DNS T...	50%	10.210.3.189	10.210.3.189	2016/05/14 10:10:00	Detected
5 Hidden					
6 High F					
7 Suspicious					
8 The TTL of DNS Response Is 0	90%	8.8.8.8	YZSONG-PC(10.21...	2016/07/13 22:17:21	Detected

Displaying 1 - 9 of 9

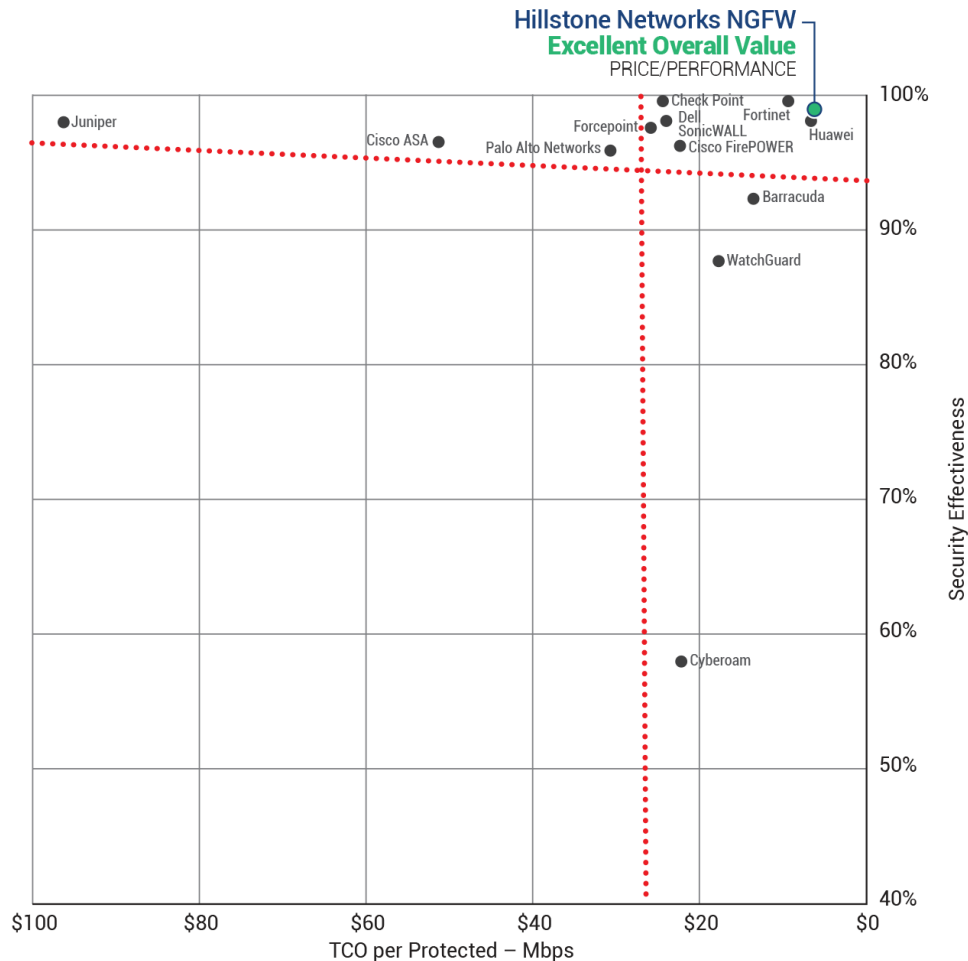
Page 1 / 1 | 20 Per Page

Close

NGFW

Hillstone Intelligent NGFW (i+NGFW)

NSS Labs Recommended NGFW - The Best TCO!



#1
LOWEST TCO

99.6%
STATIC TEST RATE

98.32%
LIVE TEST RATE

BEST Price
Performance
UNMACHED VALUE



99.60%

Block Rate in Static test

98.32%

Block Rate in Live Test

Hillstone Networks v Brně otevřel vzdělávací a výzkumnou laboratoř



Reference CZ a SK

Edge-Core:

- prodáno od roku 2006 **více jak 29 000 switchů**
 - RIO Media a.s.
 - Infos Art, s.r.o.
 - Faster CZ spol. s r.o.
 - OpavaNet a.s.
 - WIA spol. s r.o.



Brocade:

- ISP Alliance a.s.
- Družstvo OFX
- Bankovní sektor (SR)
- Energetika (ČR,SR)
- Datové centrum Rondel (ČR)



RAISECOM:

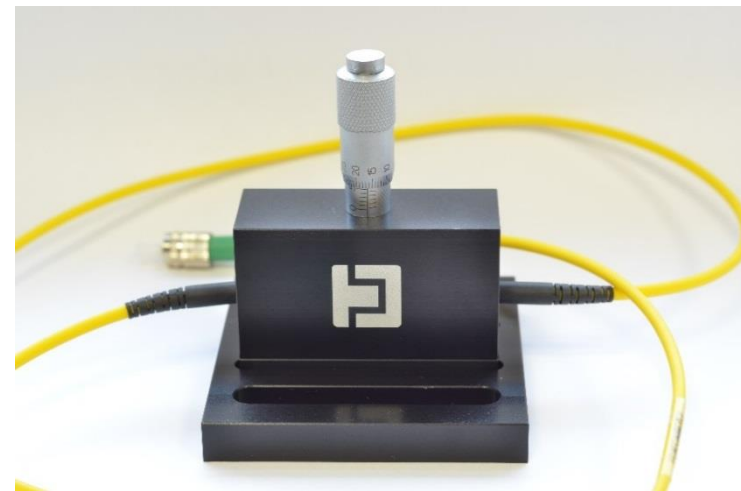
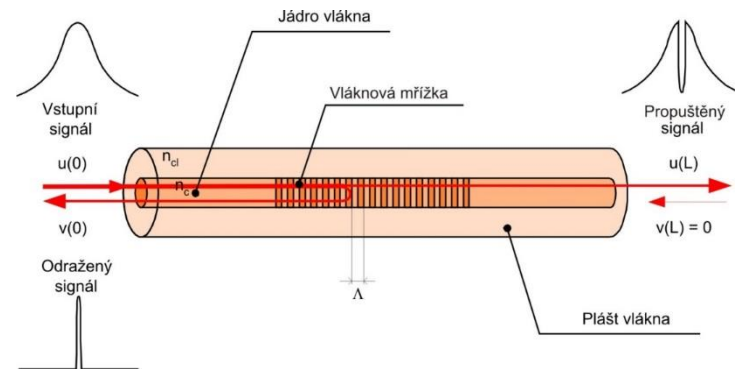
- Internet4you.cz, spol. s r.o.
- OMEGA tech s.r.o.



NETWORK GROUP, s.r.o.

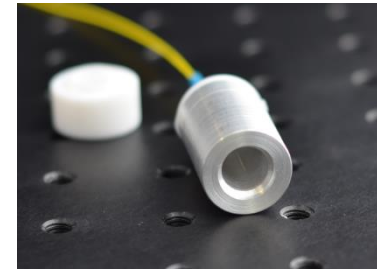
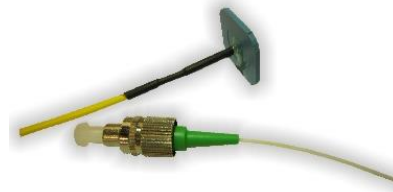
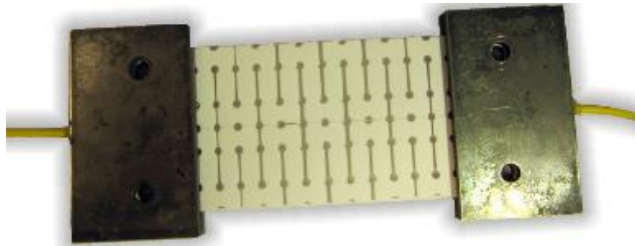
SPECIAL FIBER OPTICS

- *Návrh, vývoj a výroba pokročilých optických vláknových prvků*
- *OEM výrobce FBG mřížek a FP rezonátorů v ČR*
- *Laditelné a fixní optické FBG filtry*



Optovláknové senzory na bázi FBG a FP

- *Senzory teploty, tlaku, tahu, mechanických deformací, náklonu, vibrací, tenzometry aj.*

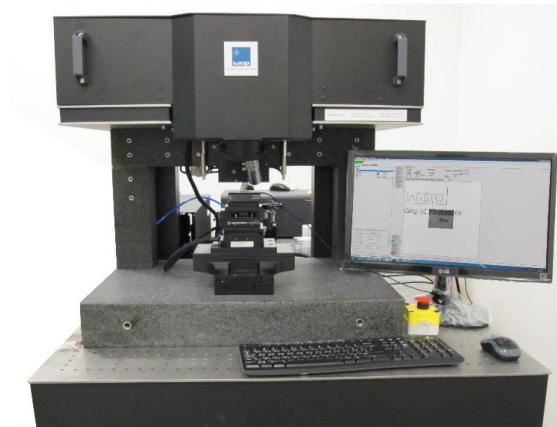


- *Vyhodnocovací elektronika, FBG interogátory*



High-end technologie

- *Mikro-oblábění femto-sekundovým laserem*
- *LDS splicing system*



sfo.nwg.cz