



# Ako otestovať Stealthwatch?

**Stanislav Smolár, SOITRON, s.r.o. ([stanislav.smolar@soitron.com](mailto:stanislav.smolar@soitron.com))**

**SOITRON\***

# Ako to začalo?

### SECURITY MANAGEMENT AND COMPLIANCE

**Managed Security Service Providers**  
IBM, at&t, Verizon, Raytheon, hp, NTT, CSC, BT, Trustwave, CenturyLink, Symantec

**SIEM**  
hp, EMC, RSA, McAfee, Splunk, TIBCO, LogRhythm, Tenable, NetIQ, Acronis, Trustwave, SolarWinds

**Security Training**  
Security Mentor, Popcorn Training, HE ONE, SANS, wombat, SCIPP, AUJAS, KnowBe4, Security Innovation, Safelight, Fishnet Security, PhishME, PhishLine

**Governance, Risk and Compliance**  
SAP, IBM, CMO, SWORD, CYBERARK, Protiviti, SAS, Enablon, Mega, SAI GLOBAL, RESOLVER, EMC, RSA, BWISE, MetricStream, Thomson Reuters, Winward

### ENDPOINT SECURITY

**Secure Email Gateways**  
SOPHOS, DELL, CLEAR SWIFT, Mimecast, Barracuda, Trustwave, Fortinet, Websense, Proofpoint, Symantec, WatchGuard, Trend Micro, SilverSky

**Data Loss Prevention**  
Absolute Software, Websense, Symantec, Verimetric, McAfee, Zecurion, Digital Guardian, Symantec

**Endpoint Protection & Anti-virus**  
IBM, Lumension, Webroot, Sophos, F-Secure, Arkon, Panda, Check Point, Threat Stack, Trend Micro, Microsoft, BeyondTrust, Symantec, Kaspersky, BitDefender, McAfee, Eset, Landesk

**Endpoint Threat Detection & Response**  
Avira, EMC, RSA, Zonefox, Trend Micro, DTEX, Promisec, Tanium, ForeScout, Guidance, Invincea, Nextthink, Rylands, Cylance, Bit9, Bromium, Ziften

### IDENTITY AND ACCESS MANAGEMENT

**User Authentication**  
HID, EMC, RSA, Entrust, Equifax, Gemalto, DeepNet Security, mi-token, Vasco, TeleSign, SecureEnvoy, Microsoft, Swivel, Symantec, SecureAuth, Duo, Authentify, Duo, SafeNet, OnePass

**Identity Governance and Administration**  
SAP, Evident, Omada, Onelogin, Caradigm, SailPoint, IBM, Courion, Fischer, Simeio, AlertEnterprise, Dell, AtoS, Aveksa, Okta, Hitachi ID Systems, Welcome, Covisint, NetIQ, Centrify, Exostar, PingIdentity

### INFRASTRUCTURE SECURITY

**Data Masking**  
IBM, GreenSight, Informatica, Solix, MENTIS, Axis, Voltage, Oracle

**Enterprise Network Firewalls**  
Hillstone, Juniper, Cisco, Sophos, AhnLab, Palo Alto, Fortinet, McAfee

**Intrusion Prevention Systems**  
Stonesoft, McAfee, NSFOCUS, IBM, Enterasys, Cisco, HP, Radware, Sourcefire, Core Security

**Network Access Control**  
ForeScout, Cisco, Juniper, IXIA, N-Station, StillSecure

**Unified Threat Management**  
Hillstone, Cyberoam, Arbor, Aker, Lancope, Sophos, Fortinet, Check Point, Rapid7, Barracuda, Juniper, WatchGuard, Cisco, Dell

### APPLICATION SECURITY

**Application Security Testing**  
Qualium, Veracode, HP, Trend Micro, IBM, Coverity, Acunetix, N-Stalker, Pradeo, Ntobjectives, Appharity

**Web Application Firewalls**  
Imperva, Trustwave, Pentasecurity, Denyall, Barracuda, ADNovum, Fortinet, Akamai, NSFOCUS, Radware, BEE WARE, Ergon, Citrix

**Application Control**  
Lumension, McAfee, Faronics, Bit9, Veeva, Trend Micro, Arellia, Kaspersky

### SECURITY PARTNERS

UNISYS, Fishnet Security, Nexum, AtoS, AccessIT, GuidePoint, AccuVant, Thundercat, Fujitsu, Adre, BT, Dimension Data, ForeSight, NTT, Gotham Technology Group, Denim Group

### CYBER SECURITY

**Secure Web Gateways**  
Blue Coat, Zscaler, Sophos, Barracuda, Cisco, Symantec, Intel Security, Trustwave, Websense, Sangfor, Trend Micro, Iboss

**Network Forensics**  
IBM, EMC, RSA, Blue Coat, WildPackets, Narus, AccessData, Cyphort, Riverbed, Netscout, Novetta, Glimmerglass, DocuSign

**Threat Intelligence Services**  
EMC, RSA, Team Cymru, Symantec, ThreatStream, NORSE, Fox IT, Malwarebytes, IID, Cyveillance, SenseCy, Csis, IBM, FreeEye, One World Lab, VeriSign, Webroot

### CLOUD SECURITY

Blue Coat, Barracuda, Skyhigh, CloudPassage, Trustwave, Sophos, Zscaler, SafeNet, McAfee, BitDefender, CloudLock, Websense, CipherCloud, Symantec, Trend Micro, Cisco

### SECURITY ORGANIZATIONS

**Education & Academic**  
SANS, OWASP, IANS, IST, Mississippi State University, CSA, UTSA, CIAC, UMUC

**Professional Associations & Certification**  
ISC, GIAC, CompTIA, EC-Council, ISACA, Financial Services, SANS, IANS, ISSA, IACRS, OWASP

**Government**  
CESG, NIST, US-CERT, EURPOL

### MOBILE SECURITY

**Mobile Data Protection**  
Dell, Intel, CenterTools, Wave, Check Point, Symantec, Microsoft, WinMagic, Trend Micro, Digital Guardian, Sophos, Kaspersky

**Mobile Device Management**  
SAP, Soti, Absolute Software, Citrix, Good, IBM, Rwatch, Symantec, GLOBE, BlackBerry, MobileIron, Sophos, Landesk, Tangoe, Mocana

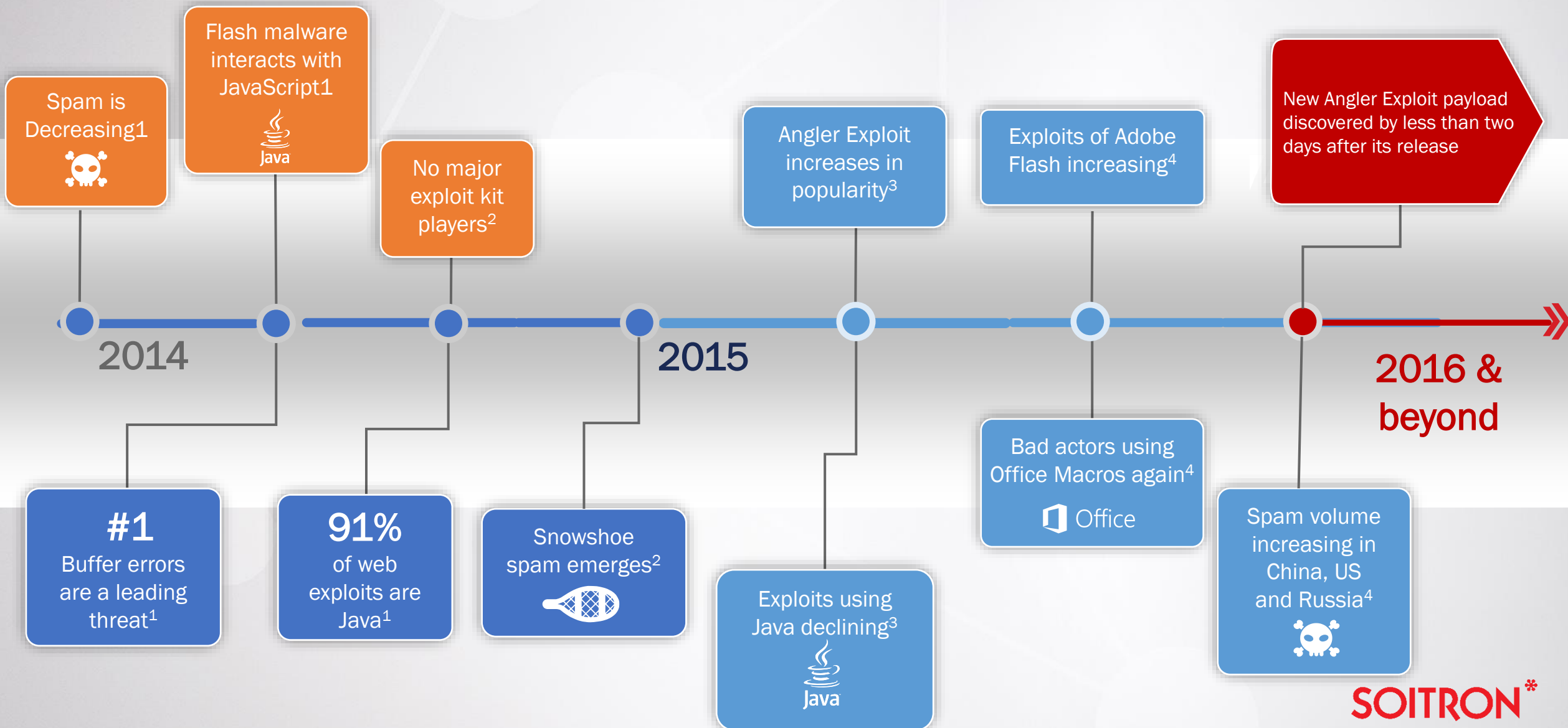
### SECURITY CONFERENCES

Gartner, Blackhat, RSA, Ten

### ANALYST HOUSES

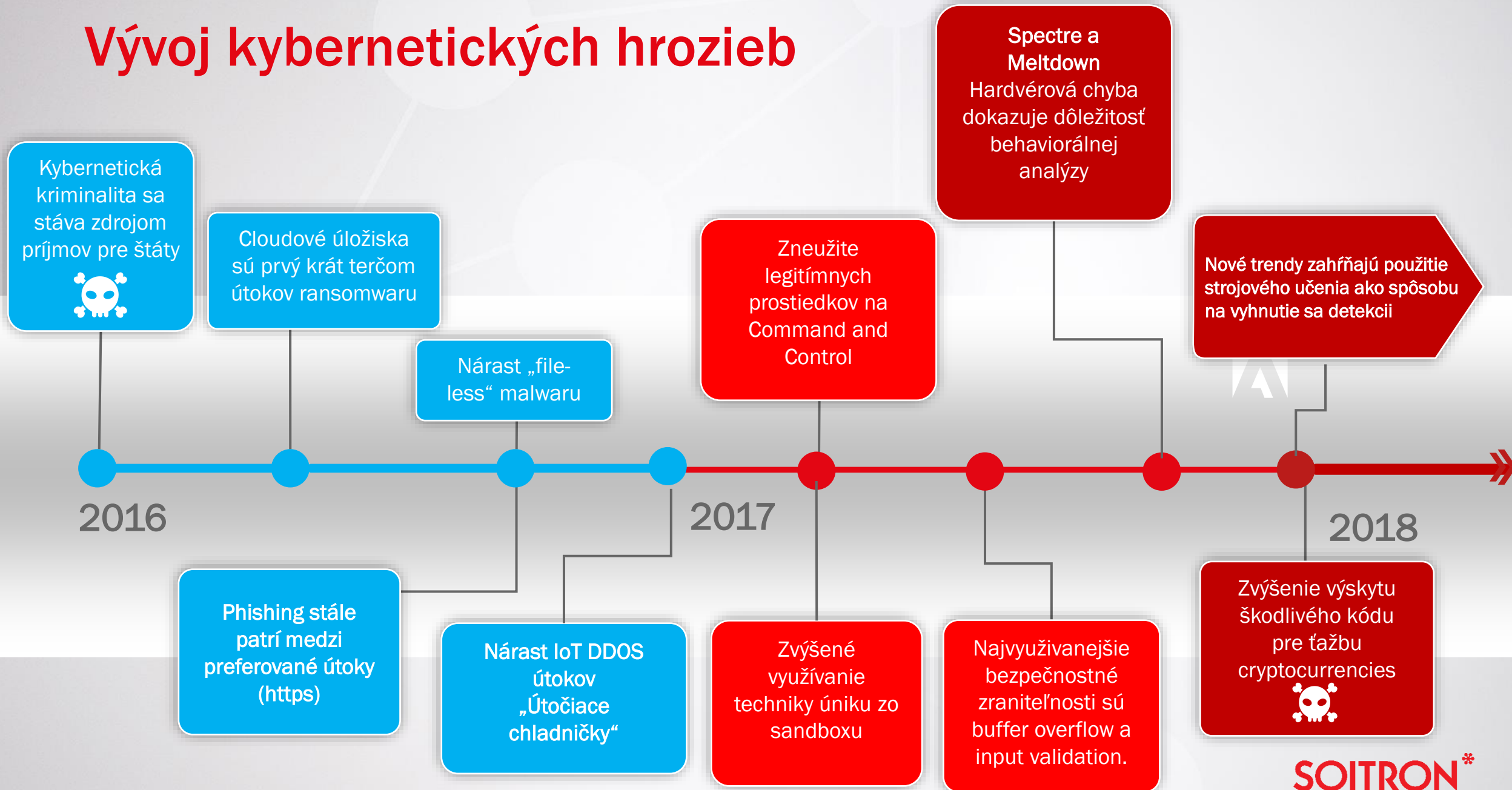
MSI Research, Gartner, Quocirca, Ovum, ESG, IDC, Forrester

# Vývoj kybernetických hrozieb zrýchľuje

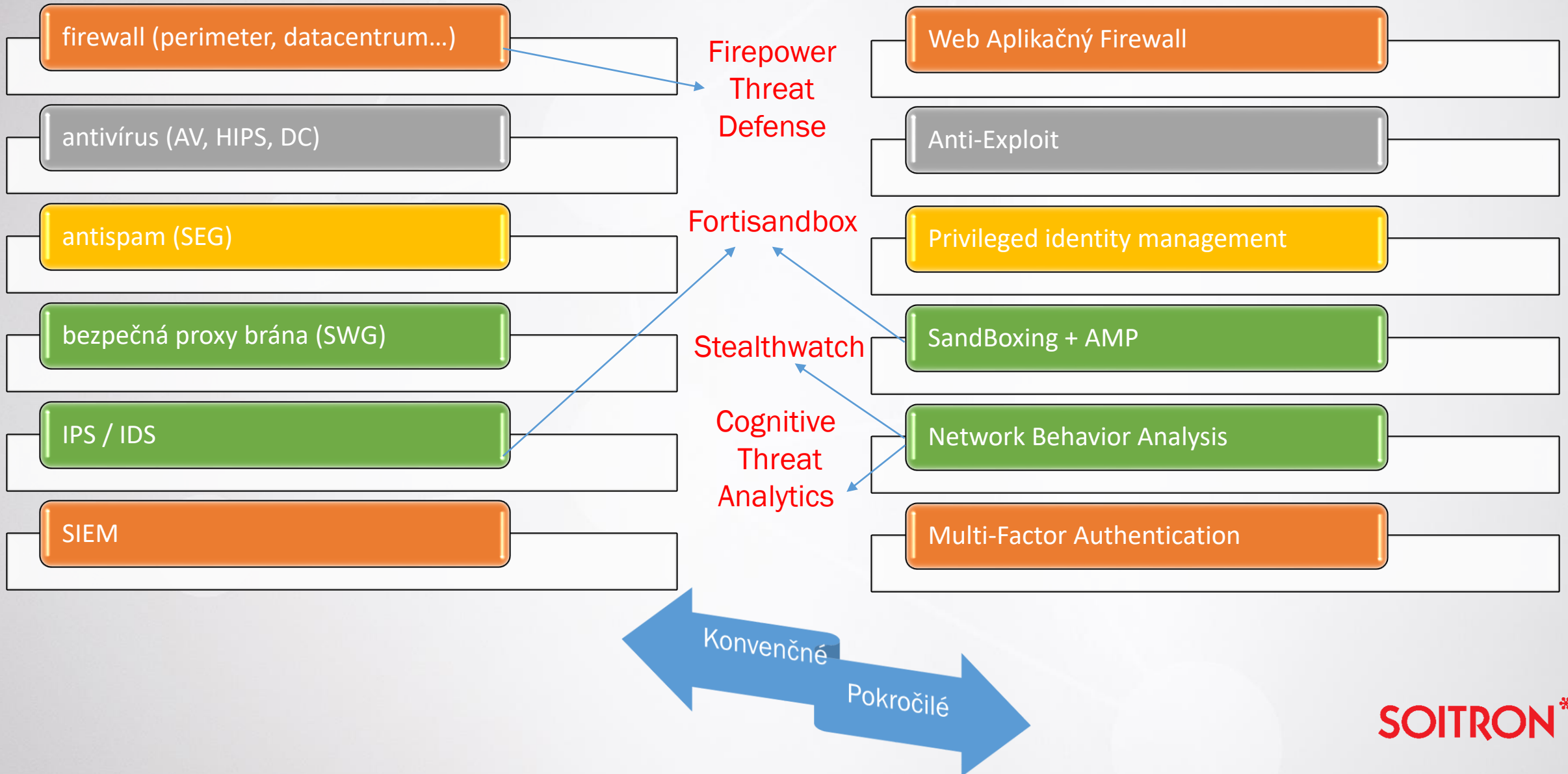




# Vývoj kybernetických hrozieb



# Vývoj kybernetických hrozieb



# Soitron Security Sensor

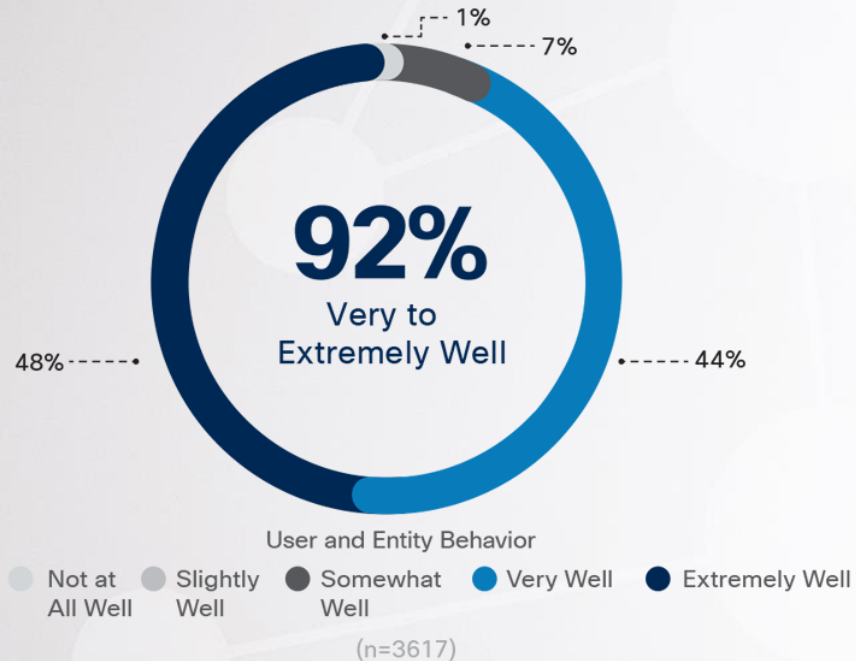
- Sonda je v pasívnom režime, iba počúva na sieti(SPAN)
- **Nemá žiaden vplyv na prevádzku zákazníka**
- **Vlastný HW, predinštalované produkty rovno nastavené na prostredie zákazníka, ku ktorým má aj zákazník prístup**
- 4 týždňový cyklus: inštalácia, nastavenia, vyhodnotenie a odprezentovanie nálezov zákazníkom formou vypracovaného reportu



# Čo sme zistili?

Most security professionals see value in behavioral analytics tools

Source: Cisco 2018 Security Capabilities Benchmark Study



- Behaviorálna analýza sieťovej prevádzky sa zatiaľ ukazuje ako najčastejšie slabé miesto bezpečnosti a zároveň poskytuje najviac detekcií
- Každý zákazník má svoje špecifické problémy, ktoré sa zásadne líšia od vertikály-industry
- Tradičné bezpečnostné prostriedky už nie sú postačujúce

# Sensor aktivity tohto roka

- **10+ zákazníkov** u ktorých bol Soitron Security Sensor nasadený
- **Vertikály:**
  - Štátna správa
  - Zdravotníctvo
  - Výrobný sektor
  - Finančný sektor
- Stále evidujeme **d'alší záujem** zákazníkov

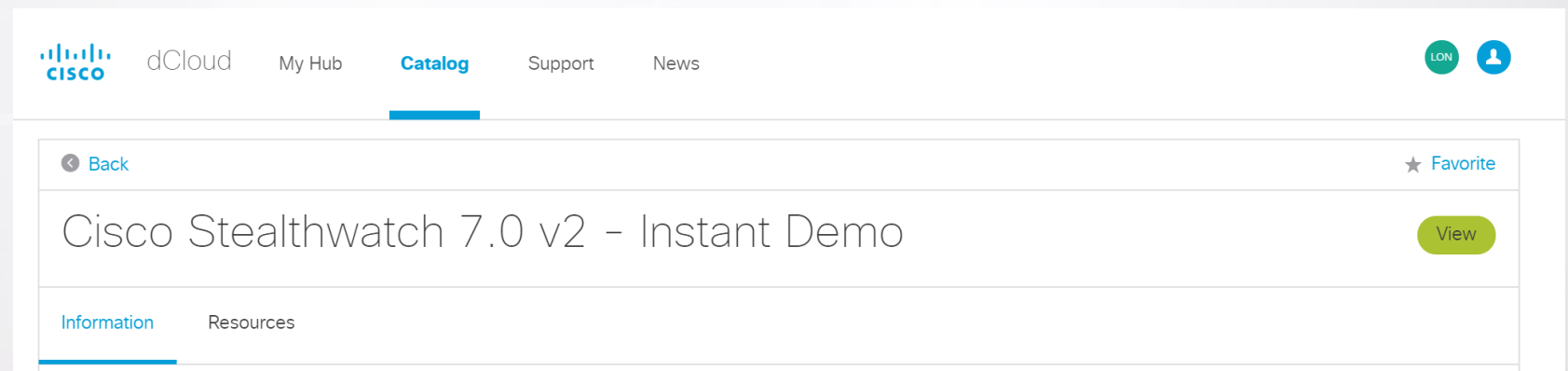


# Ale čo ak nemôžem / nechcem Sensor nasadiť?

- **Stealthwatch** má vynikajúce demo online
- **Dcloud platforma Cisco** aj z predpripravenými scenármi
- Odporúčame ako najlepší spôsob zoznámenia s web prostredím Stealthwatchu a Threat Hunting platformy
- Je tam už aj **verzia 7!**

<https://dcloud.cisco.com/>

- Spravíme s vami **online alebo živú prezentáciu**



Ak chcete **Soitron Security Sensor** vyskúšať alebo máte záujem o viac informácií, navštívte našu stránku [www.soitronsecuritysensor.sk](http://www.soitronsecuritysensor.sk)

**SOITRON\***



PLÁN  
B