Integrácia s kľúčovými komponentami

Stanislav Smolár, SOITRON, s.r.o. (stanislav.smolar@soitron.com)

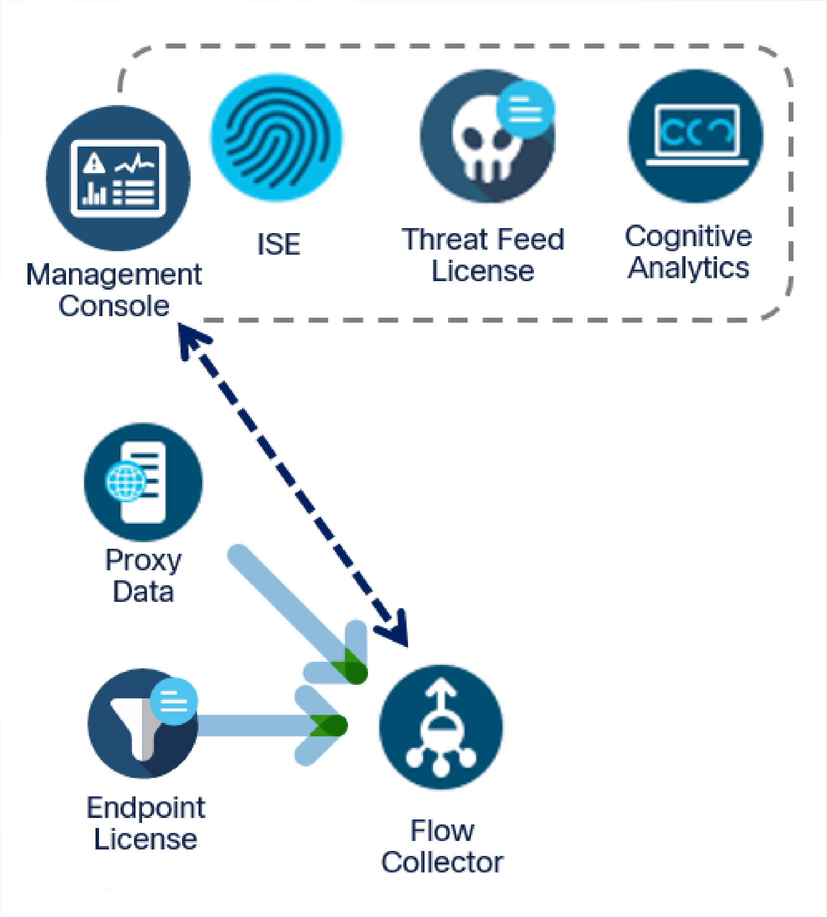
Martin Vozár, SOITRON, s.r.o. (martin.vozar@soitron.com)

SOITRON*

Contextual Feeds

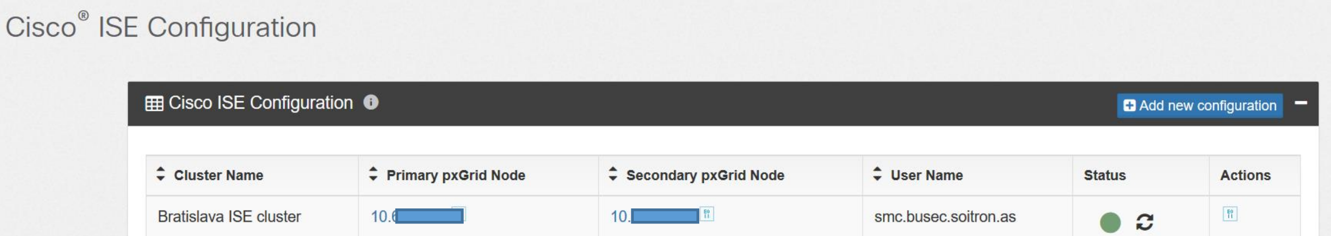
Doplnenie ďalších prepojení a zdroj pre lepšiu viditeľnosť

- **Cisco ISE (pxGrid)**
  - **Authentication (User <-> IP)**
  - TrustSec Tags (SGT/DGT)
  - Quarantine Capability
- **Proxy Ingest**
- **Endpoint License**
- **Threat Feed**
- **Cognitive Analytics**
- **Encrypted Traffic Analytics**
- Cisco ASA (Neflow Secutity Event Logging)
  - Flow create/teardown/deny udalosti
  - NAT udalosti



SOITRON*

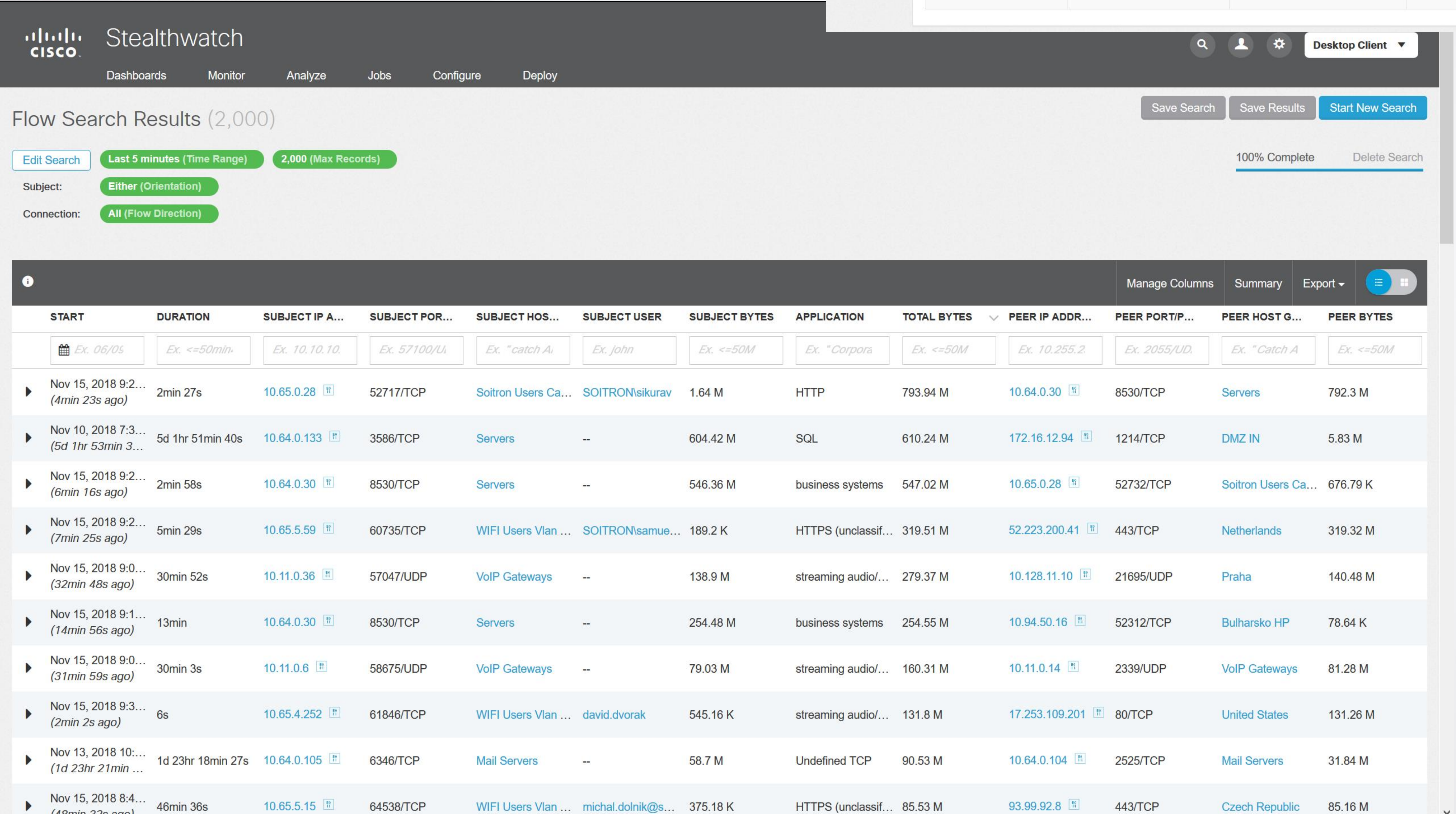
ISE integrácia



Cisco® ISE Configuration

Cisco ISE Configuration

Cluster Name	Primary pxGrid Node	Secondary pxGrid Node	User Name	Status	Actions
Bratislava ISE cluster	10.[redacted]	10.[redacted]	smc.busec.soitron.as	●	



Flow Search Results (2,000)

Edit Search | Last 5 minutes (Time Range) | 2,000 (Max Records)

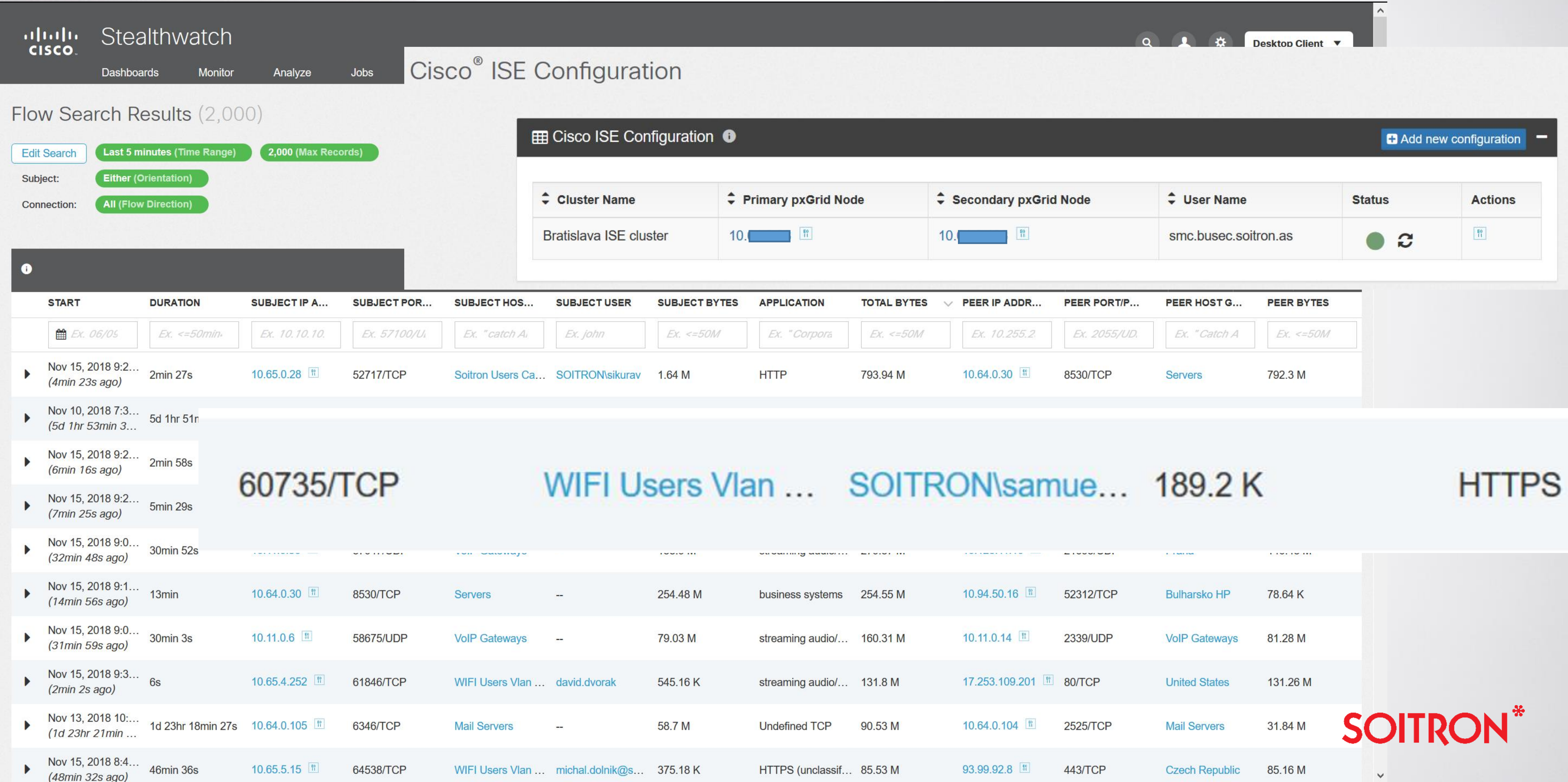
100% Complete | Delete Search

Subject: Either (Orientation)

Connection: All (Flow Direction)

START	DURATION	SUBJECT IP A...	SUBJECT POR...	SUBJECT HOS...	SUBJECT USER	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT/P...	PEER HOST G...	PEER BYTES
Ex. 06/05	Ex. <=50min	Ex. 10.10.10.	Ex. 57100/U	Ex. "catch A	Ex. john	Ex. <=50M	Ex. "Corpora	Ex. <=50M	Ex. 10.255.2	Ex. 2055/UD	Ex. "Catch A	Ex. <=50M
Nov 15, 2018 9:2... (4min 23s ago)	2min 27s	10.65.0.28	52717/TCP	Soitron Users Ca...	SOITRON\sikurav	1.64 M	HTTP	793.94 M	10.64.0.30	8530/TCP	Servers	792.3 M
Nov 10, 2018 7:3... (5d 1hr 53min 3...	5d 1hr 51min 40s	10.64.0.133	3586/TCP	Servers	--	604.42 M	SQL	610.24 M	172.16.12.94	1214/TCP	DMZ IN	5.83 M
Nov 15, 2018 9:2... (6min 16s ago)	2min 58s	10.64.0.30	8530/TCP	Servers	--	546.36 M	business systems	547.02 M	10.65.0.28	52732/TCP	Soitron Users Ca...	676.79 K
Nov 15, 2018 9:2... (7min 25s ago)	5min 29s	10.65.5.59	60735/TCP	WIFI Users Vlan ...	SOITRON\samue...	189.2 K	HTTPS (unclassif...	319.51 M	52.223.200.41	443/TCP	Netherlands	319.32 M
Nov 15, 2018 9:0... (32min 48s ago)	30min 52s	10.11.0.36	57047/UDP	VoIP Gateways	--	138.9 M	streaming audio/...	279.37 M	10.128.11.10	21695/UDP	Praha	140.48 M
Nov 15, 2018 9:1... (14min 56s ago)	13min	10.64.0.30	8530/TCP	Servers	--	254.48 M	business systems	254.55 M	10.94.50.16	52312/TCP	Bulharsko HP	78.64 K
Nov 15, 2018 9:0... (31min 59s ago)	30min 3s	10.11.0.6	58675/UDP	VoIP Gateways	--	79.03 M	streaming audio/...	160.31 M	10.11.0.14	2339/UDP	VoIP Gateways	81.28 M
Nov 15, 2018 9:3... (2min 2s ago)	6s	10.65.4.252	61846/TCP	WIFI Users Vlan ...	david.dvorak	545.16 K	streaming audio/...	131.8 M	17.253.109.201	80/TCP	United States	131.26 M
Nov 13, 2018 10:... (1d 23hr 21min ...	1d 23hr 18min 27s	10.64.0.105	6346/TCP	Mail Servers	--	58.7 M	Undefined TCP	90.53 M	10.64.0.104	2525/TCP	Mail Servers	31.84 M
Nov 15, 2018 8:4... (48min 32s ago)	46min 36s	10.65.5.15	64538/TCP	WIFI Users Vlan ...	michal.dolnik@s...	375.18 K	HTTPS (unclassif...	85.53 M	93.99.92.8	443/TCP	Czech Republic	85.16 M

ISE integrácia



Cisco® ISE Configuration

Flow Search Results (2,000)

Edit Search | Last 5 minutes (Time Range) | 2,000 (Max Records)

Subject: Either (Orientation)

Connection: All (Flow Direction)

Cisco ISE Configuration

Add new configuration

Cluster Name	Primary pxGrid Node	Secondary pxGrid Node	User Name	Status	Actions
Bratislava ISE cluster	10.[redacted]	10.[redacted]	smc.busec.soitron.as	●	

START	DURATION	SUBJECT IP A...	SUBJECT POR...	SUBJECT HOS...	SUBJECT USER	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT/P...	PEER HOST G...	PEER BYTES
Ex. 06/05	Ex. <=50min	Ex. 10.10.10.	Ex. 57100/U	Ex. "catch A	Ex. john	Ex. <=50M	Ex. "Corpora	Ex. <=50M	Ex. 10.255.2	Ex. 2055/UD	Ex. "Catch A	Ex. <=50M
Nov 15, 2018 9:2... *(4min 23s ago)*	2min 27s	10.65.0.28	52717/TCP	Soitron Users Ca...	SOITRON\sikurav	1.64 M	HTTP	793.94 M	10.64.0.30	8530/TCP	Servers	792.3 M
Nov 10, 2018 7:3... *(5d 1hr 53min 3...*	5d 1hr 51r											
Nov 15, 2018 9:2... *(6min 16s ago)*	2min 58s											
Nov 15, 2018 9:2... *(7min 25s ago)*	5min 29s											
Nov 15, 2018 9:0... *(32min 48s ago)*	30min 52s											
Nov 15, 2018 9:1... *(14min 56s ago)*	13min	10.64.0.30	8530/TCP	Servers	--	254.48 M	business systems	254.55 M	10.94.50.16	52312/TCP	Bulharsko HP	78.64 K
Nov 15, 2018 9:0... *(31min 59s ago)*	30min 3s	10.11.0.6	58675/UDP	VoIP Gateways	--	79.03 M	streaming audio/...	160.31 M	10.11.0.14	2339/UDP	VoIP Gateways	81.28 M
Nov 15, 2018 9:3... *(2min 2s ago)*	6s	10.65.4.252	61846/TCP	WIFI Users Vlan ...	david.dvorak	545.16 K	streaming audio/...	131.8 M	17.253.109.201	80/TCP	United States	131.26 M
Nov 13, 2018 10:... *(1d 23hr 21min ...*	1d 23hr 18min 27s	10.64.0.105	6346/TCP	Mail Servers	--	58.7 M	Undefined TCP	90.53 M	10.64.0.104	2525/TCP	Mail Servers	31.84 M
Nov 15, 2018 8:4... *(48min 32s ago)*	46min 36s	10.65.5.15	64538/TCP	WIFI Users Vlan ...	michal.dolnik@s...	375.18 K	HTTPS (unclassif...	85.53 M	93.99.92.8	443/TCP	Czech Republic	85.16 M

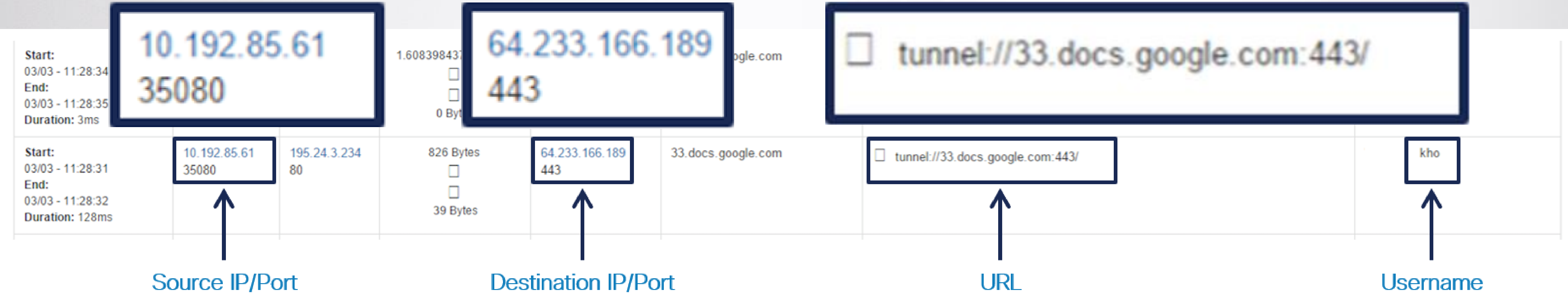
60735/TCP WIFI Users Vlan ... SOITRON\samue... 189.2 K HTTPS

SOITRON*

Proxy viditeľnosť

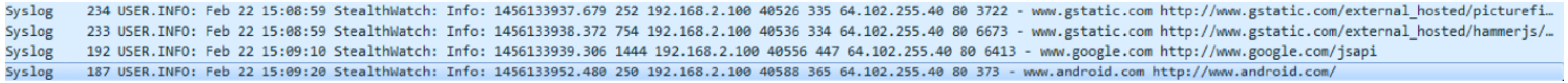
- Proxy posiela do kolektora logy prostredníctvom **syslog** protokolu
- Kolektor asociuje logy s flow dátami
- Podporované: Cisco WSA, Bluacoat, Squid, McAfee Web Gateway, ...

- Získané dáta
  - User Name, URL, URL Host, Byte Summary, Session Duration, Source IP/Port, Destination IP/Port

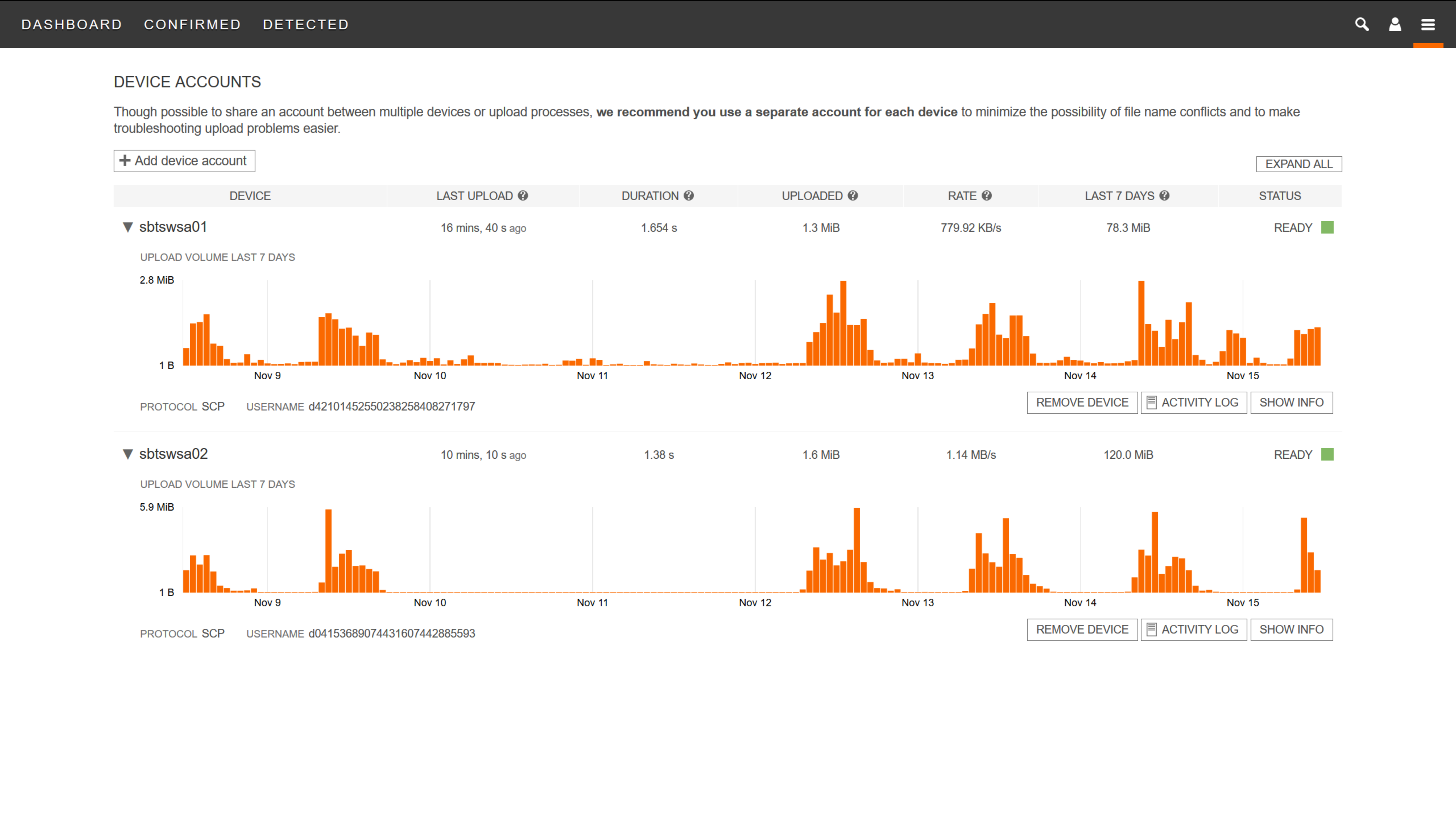


Start: 03/03 - 11:28:34 **End:** 03/03 - 11:28:35 **Duration:** 3ms | 10.192.85.61 35080 | 1.608398437 □ □ 0 Byt | 64.233.166.189 443 | ogle.com | □ tunnel://33.docs.google.com:443/

Start: 03/03 - 11:28:31 **End:** 03/03 - 11:28:32 **Duration:** 128ms | 10.192.85.61 35080 | 195.24.3.234 80 | 826 Bytes □ □ 39 Bytes | 64.233.166.189 443 | 33.docs.google.com | □ tunnel://33.docs.google.com:443/ | kho



```
Syslog    234 USER.INFO: Feb 22 15:08:59 StealthWatch: Info: 1456133937.679 252 192.168.2.100 40526 335 64.102.255.40 80 3722 - www.gstatic.com http://www.gstatic.com/external_hosted/picturefi…
Syslog    233 USER.INFO: Feb 22 15:08:59 StealthWatch: Info: 1456133938.372 754 192.168.2.100 40536 334 64.102.255.40 80 6673 - www.gstatic.com http://www.gstatic.com/external_hosted/hammerjs/…
Syslog    192 USER.INFO: Feb 22 15:09:10 StealthWatch: Info: 1456133939.306 1444 192.168.2.100 40556 447 64.102.255.40 80 6413 - www.google.com http://www.google.com/jsapi
Syslog    187 USER.INFO: Feb 22 15:09:20 StealthWatch: Info: 1456133952.480 250 192.168.2.100 40588 365 64.102.255.40 80 373 - www.android.com http://www.android.com/
```



DEVICE ACCOUNTS

Though possible to share an account between multiple devices or upload processes, **we recommend you use a separate account for each device** to minimize the possibility of file name conflicts and to make troubleshooting upload problems easier.

DEVICE	LAST UPLOAD ❓	DURATION ❓	UPLOADED ❓	RATE ❓	LAST 7 DAYS ❓	STATUS
▼ sbtswsa01	16 mins, 40 s ago	1.654 s	1.3 MiB	779.92 KB/s	78.3 MiB	READY 🟩
▼ sbtswsa02	10 mins, 10 s ago	1.38 s	1.6 MiB	1.14 MB/s	120.0 MiB	READY 🟩

UPLOAD VOLUME LAST 7 DAYS

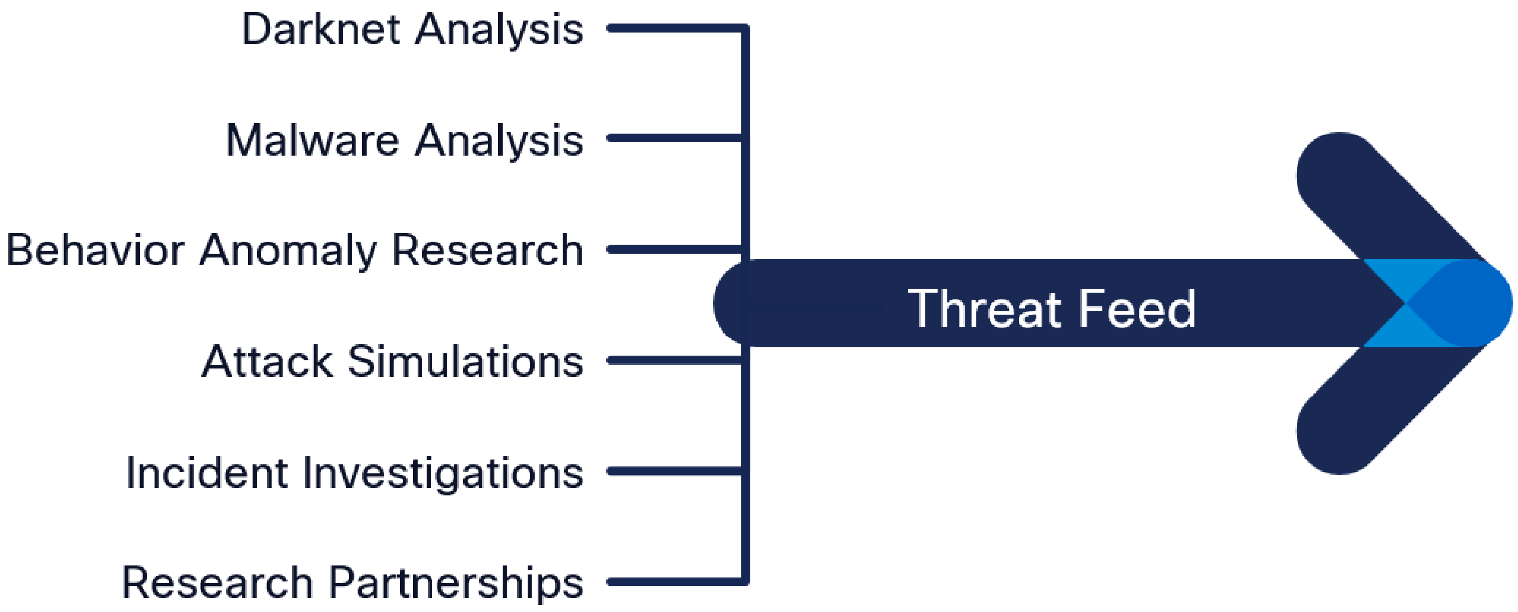
PROTOCOL SCP USERNAME d42101452550238258408271797

UPLOAD VOLUME LAST 7 DAYS

PROTOCOL SCP USERNAME d04153689074431607442885593

Threat Intelligence License

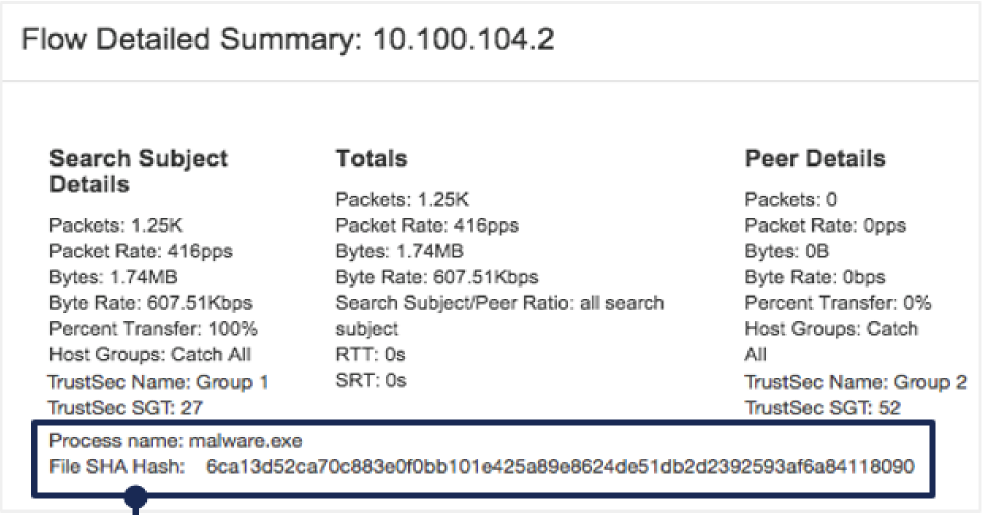
- Voliteľná licencia pre kolektory (odhaľovanie komunikácie na „nevhodné“ ciele)



- Team performs feed validation and independent research and analytics
- Threat research influences continued algorithm development
- Works with Proxy License
- Ideally deployed with Flow Sensor(s)
- Enables alarming within Stealthwatch around:
  - Host interaction with known bad URLs
  - Host interaction with C&C servers

Endpoint Visibility

- Integrácia do Cisco Anyconnect – **Network Visibility Module**; Endpoint Concentrator



Flow Detailed Summary: 10.100.104.2

Search Subject Details

Packets: 1.25K
Packet Rate: 416pps
Bytes: 1.74MB
Byte Rate: 607.51Kbps
Percent Transfer: 100%
Host Groups: Catch All
TrustSec Name: Group 1
TrustSec SGT: 27

Totals

Packets: 1.25K
Packet Rate: 416pps
Bytes: 1.74MB
Byte Rate: 607.51Kbps
Search Subject/Peer Ratio: all search subject
RTT: 0s
SRT: 0s

Peer Details

Packets: 0
Packet Rate: 0pps
Bytes: 0B
Byte Rate: 0bps
Percent Transfer: 0%
Host Groups: Catch All
TrustSec Name: Group 2
TrustSec SGT: 52

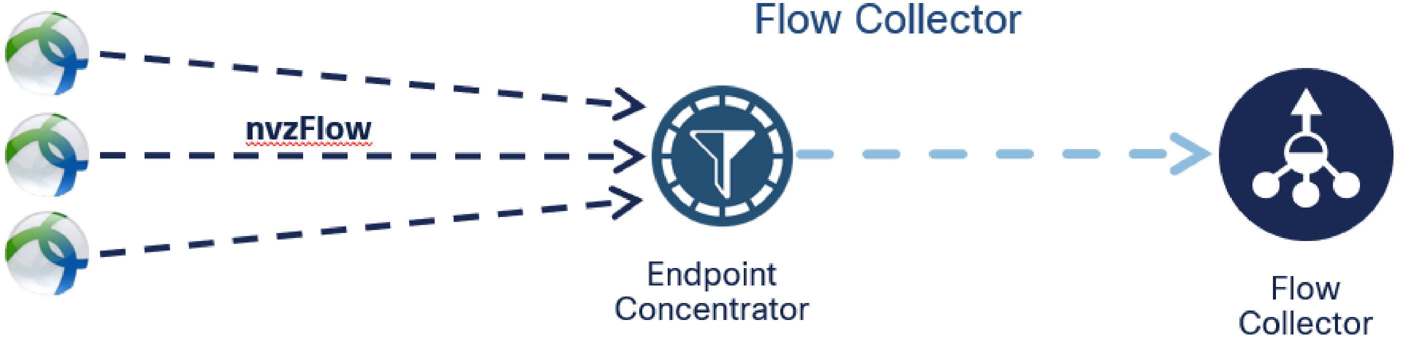
Process name: malware.exe
File SHA Hash: 6ca13d52ca70c883e0f0bb101e425a89e8624de51db2d2392593af6a84118090

Attributing a flow to:

- Process name
- Process hash
- Process account
- Parent process name
- Parent process hash
- Parent process account

AnyConnect with
Network Visibility Module

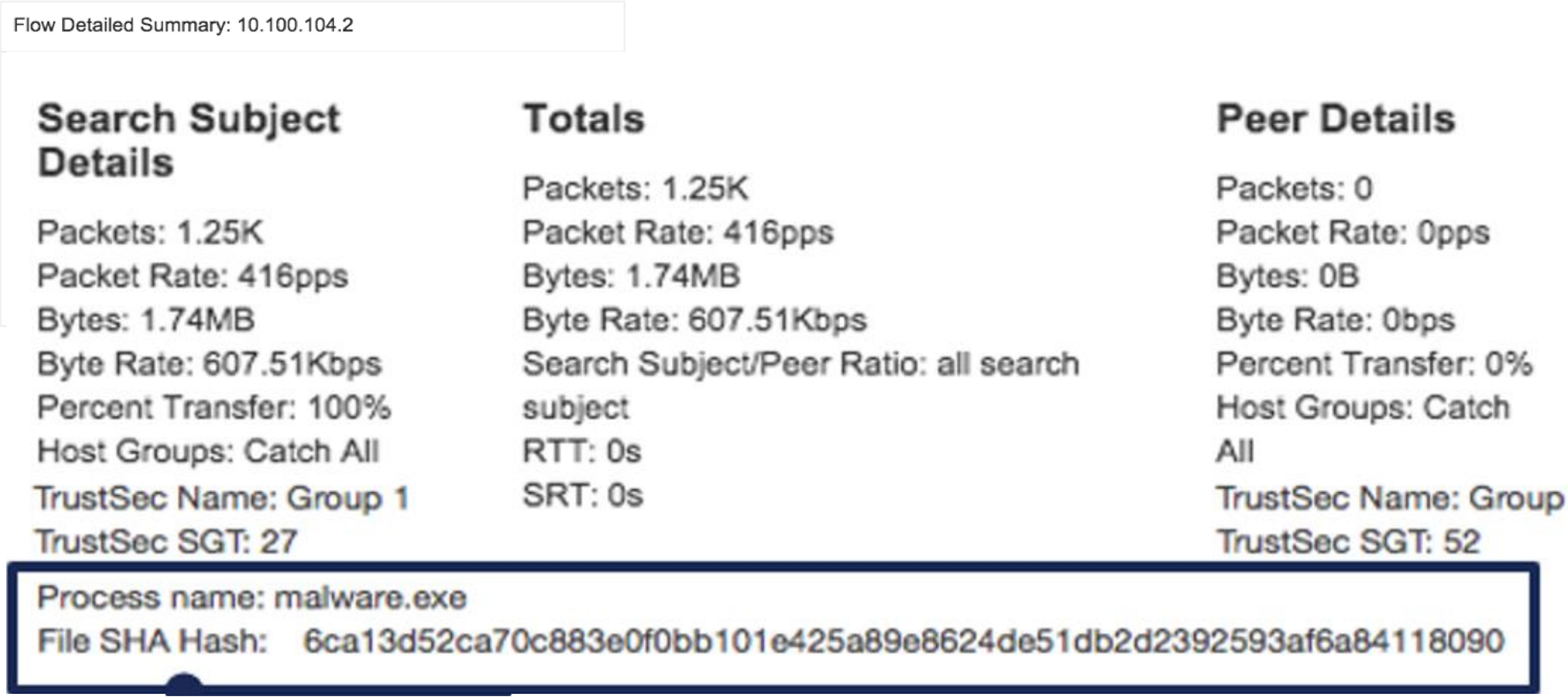
- Global destination for nvzFlow records
- Forward flow records to the Flow Collector



- Appears as a single exporter in the Flow Collector
- Required in order to collect endpoint flow records
- Endpoint fields are stitched into flow records

Endpoint Visibility

- Detail toku



Flow Detailed Summary: 10.100.104.2

Search Subject Details

Packets: 1.25K
Packet Rate: 416pps
Bytes: 1.74MB
Byte Rate: 607.51Kbps
Percent Transfer: 100%
Host Groups: Catch All
TrustSec Name: Group 1
TrustSec SGT: 27

Totals

Packets: 1.25K
Packet Rate: 416pps
Bytes: 1.74MB
Byte Rate: 607.51Kbps
Search Subject/Peer Ratio: all search subject
RTT: 0s
SRT: 0s

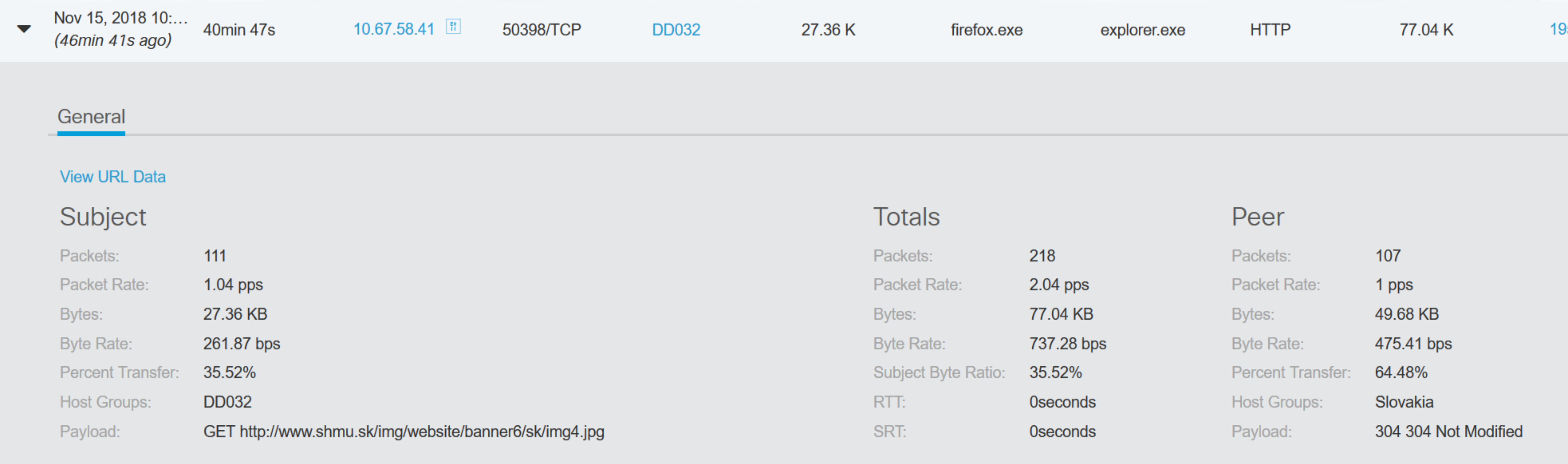
Peer Details

Packets: 0
Packet Rate: 0pps
Bytes: 0B
Byte Rate: 0bps
Percent Transfer: 0%
Host Groups: Catch All
TrustSec Name: Group 2
TrustSec SGT: 52

Process name: malware.exe
File SHA Hash: 6ca13d52ca70c883e0f0bb101e425a89e8624de51db2d2392593af6a84118090

Endpoint Visibility

- Detail toku #2



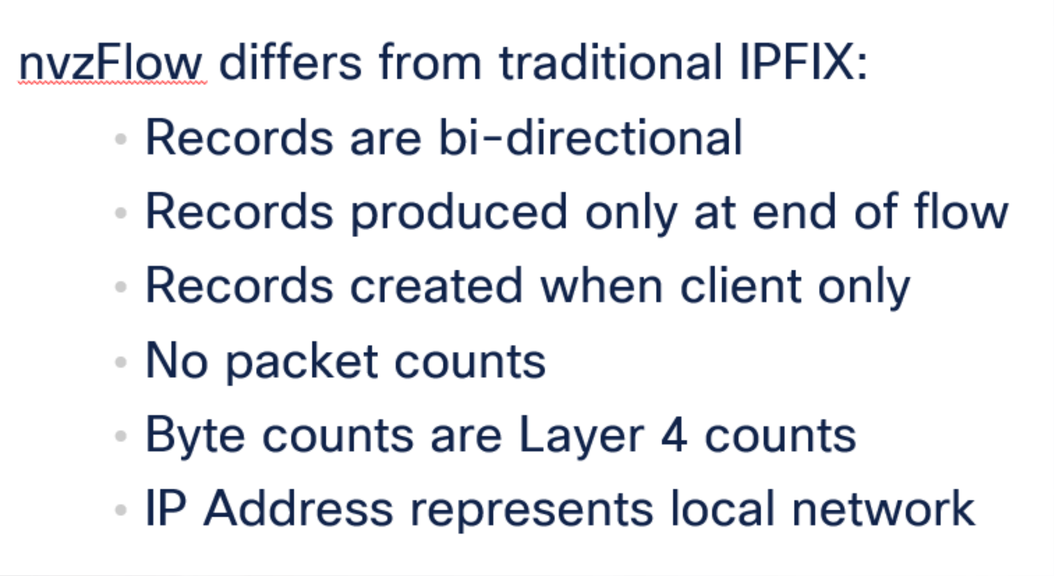
▾	Nov 15, 2018 10:... *(46min 41s ago)*	40min 47s	10.67.58.41	50398/TCP	DD032	27.36 K	firefox.exe	explorer.exe	HTTP	77.04 K	19

View URL Data

Subject		Totals		Peer	
Packets:	111	Packets:	218	Packets:	107
Packet Rate:	1.04 pps	Packet Rate:	2.04 pps	Packet Rate:	1 pps
Bytes:	27.36 KB	Bytes:	77.04 KB	Bytes:	49.68 KB
Byte Rate:	261.87 bps	Byte Rate:	737.28 bps	Byte Rate:	475.41 bps
Percent Transfer:	35.52%	Subject Byte Ratio:	35.52%	Percent Transfer:	64.48%
Host Groups:	DD032	RTT:	0seconds	Host Groups:	Slovakia
Payload:	GET http://www.shmu.sk/img/website/banner6/sk/img4.jpg	SRT:	0seconds	Payload:	304 304 Not Modified

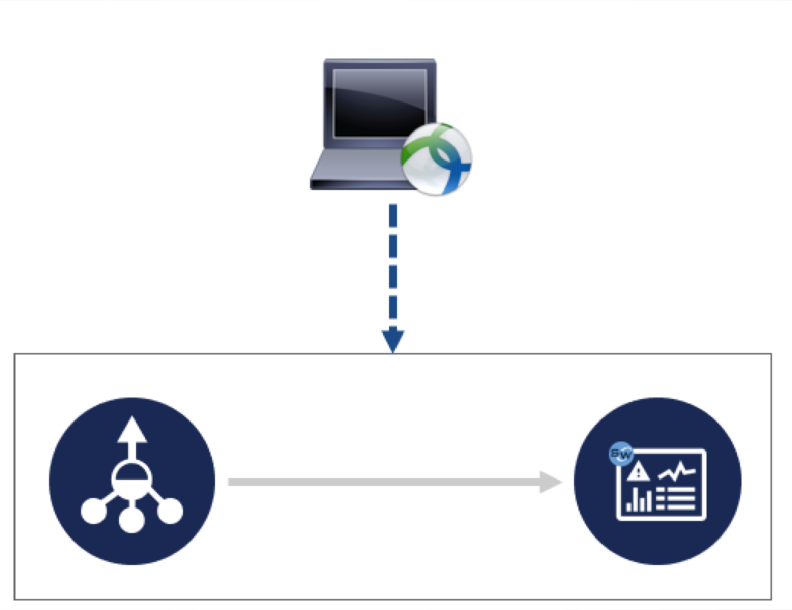
Endpoint Visibility

- Odlišnosti nvzFlow



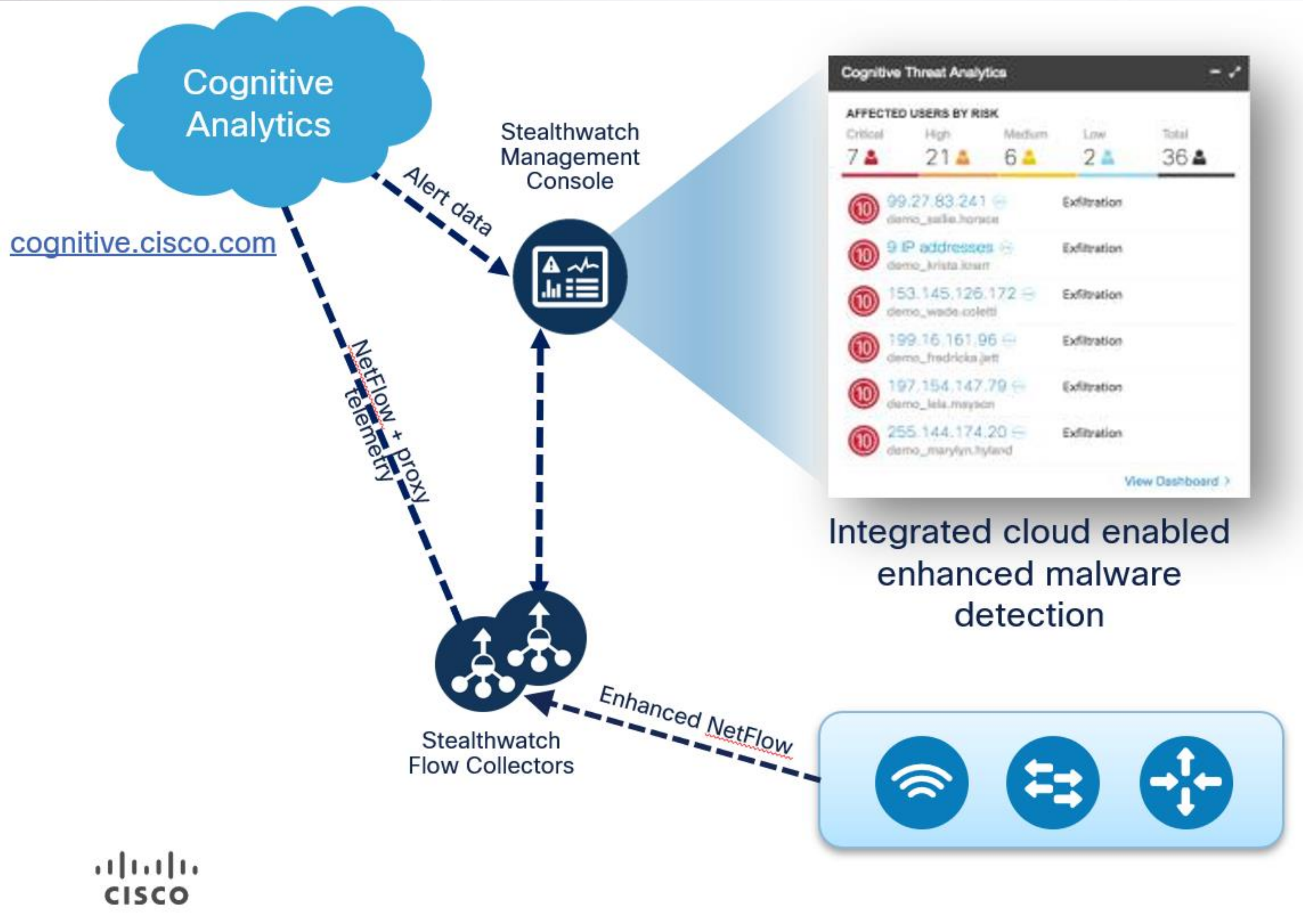
nvzFlow differs from traditional IPFIX:

- Records are bi-directional
- Records produced only at end of flow
- Records created when client only
- No packet counts
- Byte counts are Layer 4 counts
- IP Address represents local network



Cognitive Analytics

- Výhoda - cloud inteligencia nad našimi dátami


Cognitive Analytics
cognitive.cisco.com
Alert data
Stealthwatch Management Console
NetFlow + proxy telemetry
Stealthwatch Flow Collectors
Enhanced NetFlow
cisco

Cognitive Threat Analytics

AFFECTED USERS BY RISK

Critical	High	Medium	Low	Total
7	21	6	2	36

10	99.27.83.241 demo_sallie.horace	Exfiltration
10	9 IP addresses demo_krista.kran	Exfiltration
10	153.145.126.172 demo_wade.coletti	Exfiltration
10	199.16.161.96 demo_fredricka.jett	Exfiltration
10	197.154.147.79 demo_lela.mayson	Exfiltration
10	255.144.174.20 demo_marylyn.hyland	Exfiltration

View Dashboard >

Integrated cloud enabled enhanced malware detection

Global <=>local correlation
Higher precision of threat findings

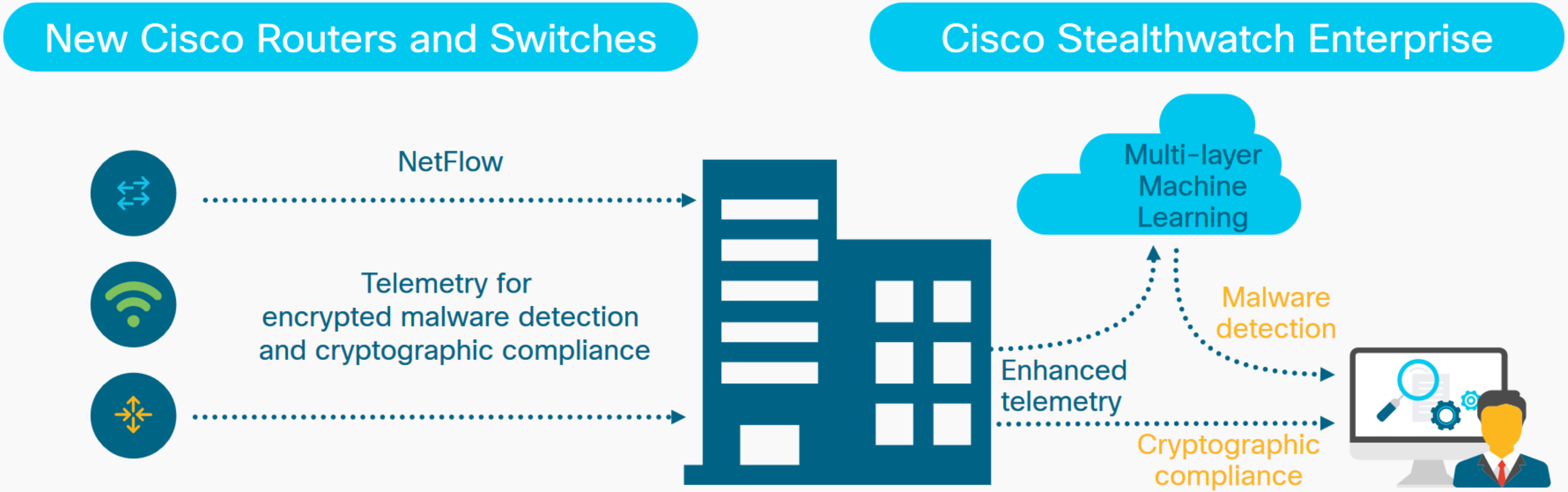
Machine learning analytics
Reduces threat investigation time

Encrypted Traffic Analytics
Enhanced NetFlow from Cisco's newest switches and routers

SOITRON*

Encrypted Traffic Analytics

- Vyhodnocovanie správania SSL „obálky“ + crypto compliance (TLS verzie, šifry)



New Cisco Routers and Switches

Cisco Stealthwatch Enterprise

NetFlow

Telemetry for encrypted malware detection and cryptographic compliance

Multi-layer Machine Learning

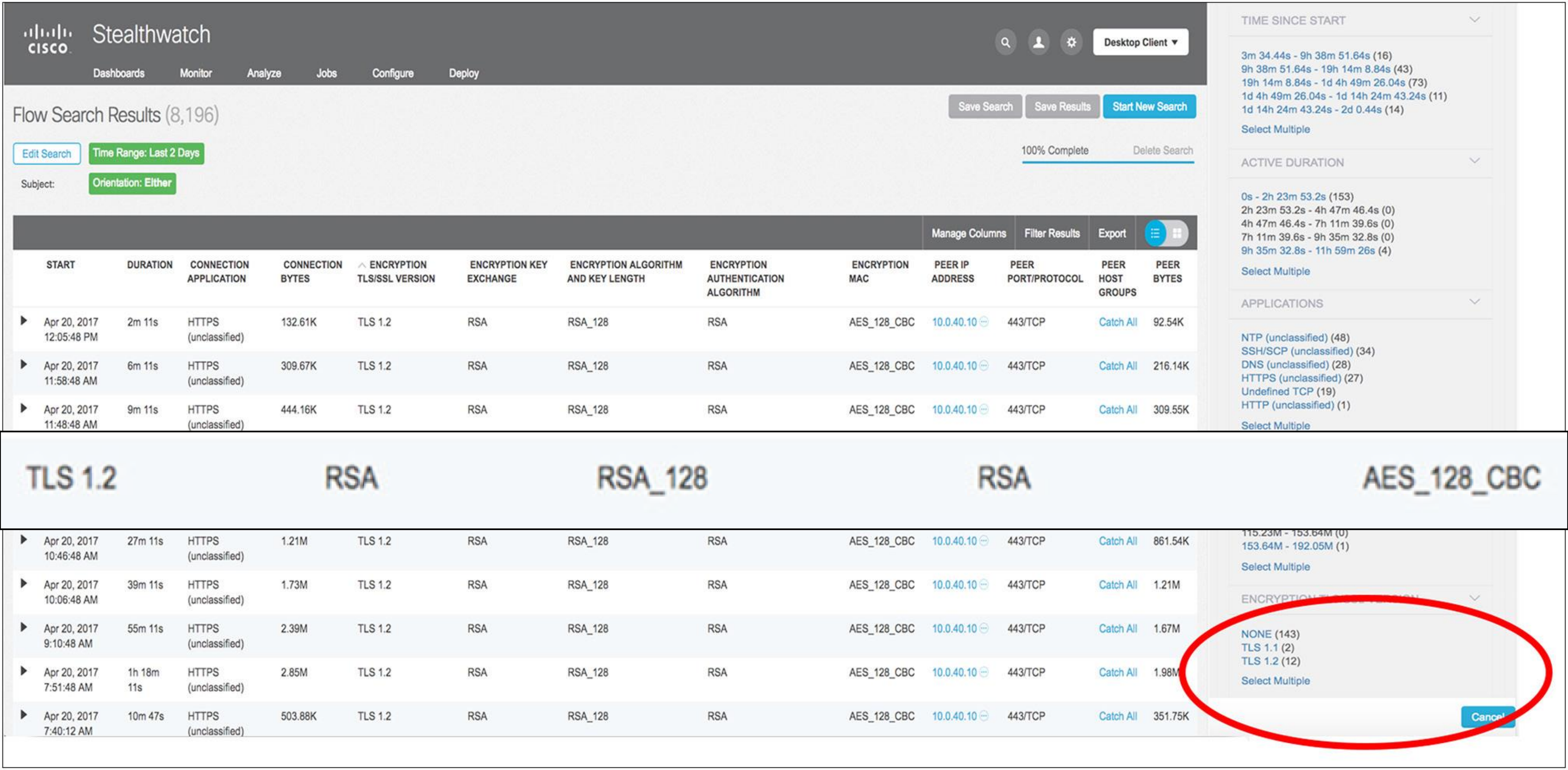
Enhanced telemetry

Malware detection

Cryptographic compliance

Leveraged network	Faster investigation	Higher precision	Stronger protection
Enhanced telemetry from Cisco’s newest switches and routers	Advanced analytics and machine learning	Global-to-local knowledge correlation	Continuous Enterprise-wide compliance

Encrypted Traffic Analytics



Flow Search Results (8,196)

Time Range: Last 2 Days

Subject: Orientation: Either

100% Complete

START	DURATION	CONNECTION APPLICATION	CONNECTION BYTES	ENCRYPTION TLS/SSL VERSION	ENCRYPTION KEY EXCHANGE	ENCRYPTION ALGORITHM AND KEY LENGTH	ENCRYPTION AUTHENTICATION ALGORITHM	ENCRYPTION MAC	PEER IP ADDRESS	PEER PORT/PROTOCOL	PEER HOST GROUPS	PEER BYTES
Apr 20, 2017 12:05:48 PM	2m 11s	HTTPS (unclassified)	132.61K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	92.54K
Apr 20, 2017 11:58:48 AM	6m 11s	HTTPS (unclassified)	309.67K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	216.14K
Apr 20, 2017 11:48:48 AM	9m 11s	HTTPS (unclassified)	444.16K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	309.55K
Apr 20, 2017 10:46:48 AM	27m 11s	HTTPS (unclassified)	1.21M	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	861.54K
Apr 20, 2017 10:06:48 AM	39m 11s	HTTPS (unclassified)	1.73M	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	1.21M
Apr 20, 2017 9:10:48 AM	55m 11s	HTTPS (unclassified)	2.39M	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	1.67M
Apr 20, 2017 7:51:48 AM	1h 18m 11s	HTTPS (unclassified)	2.85M	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	1.98M
Apr 20, 2017 7:40:12 AM	10m 47s	HTTPS (unclassified)	503.88K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	351.75K

TLS 1.2 RSA RSA_128 RSA AES_128_CBC

TIME SINCE START

3m 34.44s - 9h 38m 51.64s (16)
9h 38m 51.64s - 19h 14m 8.84s (43)
19h 14m 8.84s - 1d 4h 49m 26.04s (73)
1d 4h 49m 26.04s - 1d 14h 24m 43.24s (11)
1d 14h 24m 43.24s - 2d 0.44s (14)
Select Multiple

ACTIVE DURATION

0s - 2h 23m 53.2s (153)
2h 23m 53.2s - 4h 47m 46.4s (0)
4h 47m 46.4s - 7h 11m 39.6s (0)
7h 11m 39.6s - 9h 35m 32.8s (0)
9h 35m 32.8s - 11h 59m 26s (4)
Select Multiple

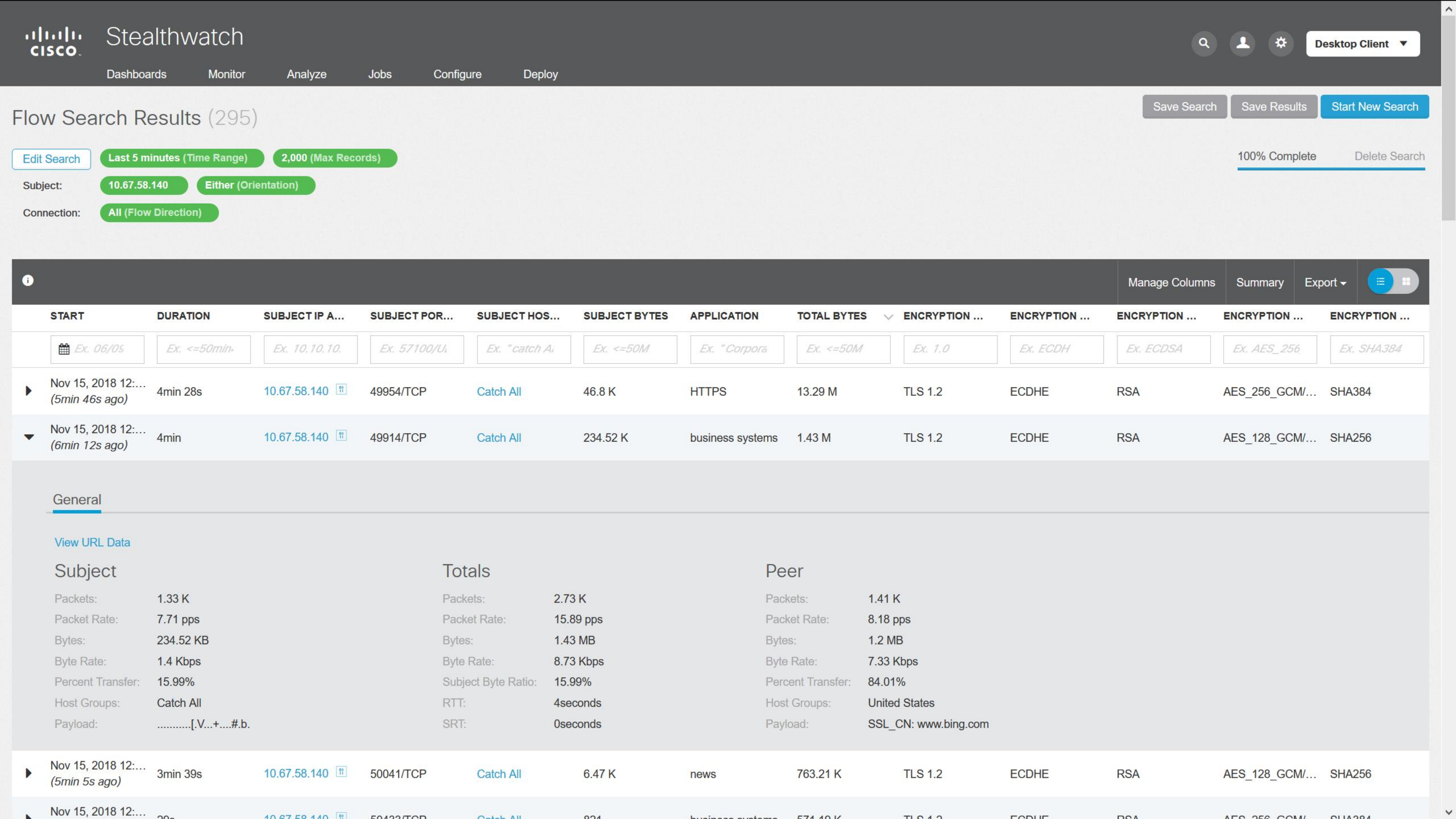
APPLICATIONS

NTP (unclassified) (48)
SSH/SCP (unclassified) (34)
DNS (unclassified) (28)
HTTPS (unclassified) (27)
Undefined TCP (19)
HTTP (unclassified) (1)
Select Multiple

115.23M - 153.64M (0)
153.64M - 192.05M (1)
Select Multiple

ENCRYPTION

NONE (143)
TLS 1.1 (2)
TLS 1.2 (12)
Select Multiple



Flow Search Results (295)

Last 5 minutes (Time Range) 2,000 (Max Records)

Subject: 10.67.58.140 Either (Orientation)

Connection: All (Flow Direction)

100% Complete Delete Search

	START	DURATION	SUBJECT IP A...	SUBJECT POR...	SUBJECT HOS...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...
	Ex. 06/05	Ex. <=50min	Ex. 10.10.10.	Ex. 57100/U	Ex. "catch A	Ex. <=50M	Ex. "Corpora	Ex. <=50M	Ex. 1.0	Ex. ECDH	Ex. ECDSA	Ex. AES_256	Ex. SHA384
▶	Nov 15, 2018 12:... *(5min 46s ago)*	4min 28s	10.67.58.140	49954/TCP	Catch All	46.8 K	HTTPS	13.29 M	TLS 1.2	ECDHE	RSA	AES_256_GCM/...	SHA384
▼	Nov 15, 2018 12:... *(6min 12s ago)*	4min	10.67.58.140	49914/TCP	Catch All	234.52 K	business systems	1.43 M	TLS 1.2	ECDHE	RSA	AES_128_GCM/...	SHA256

General

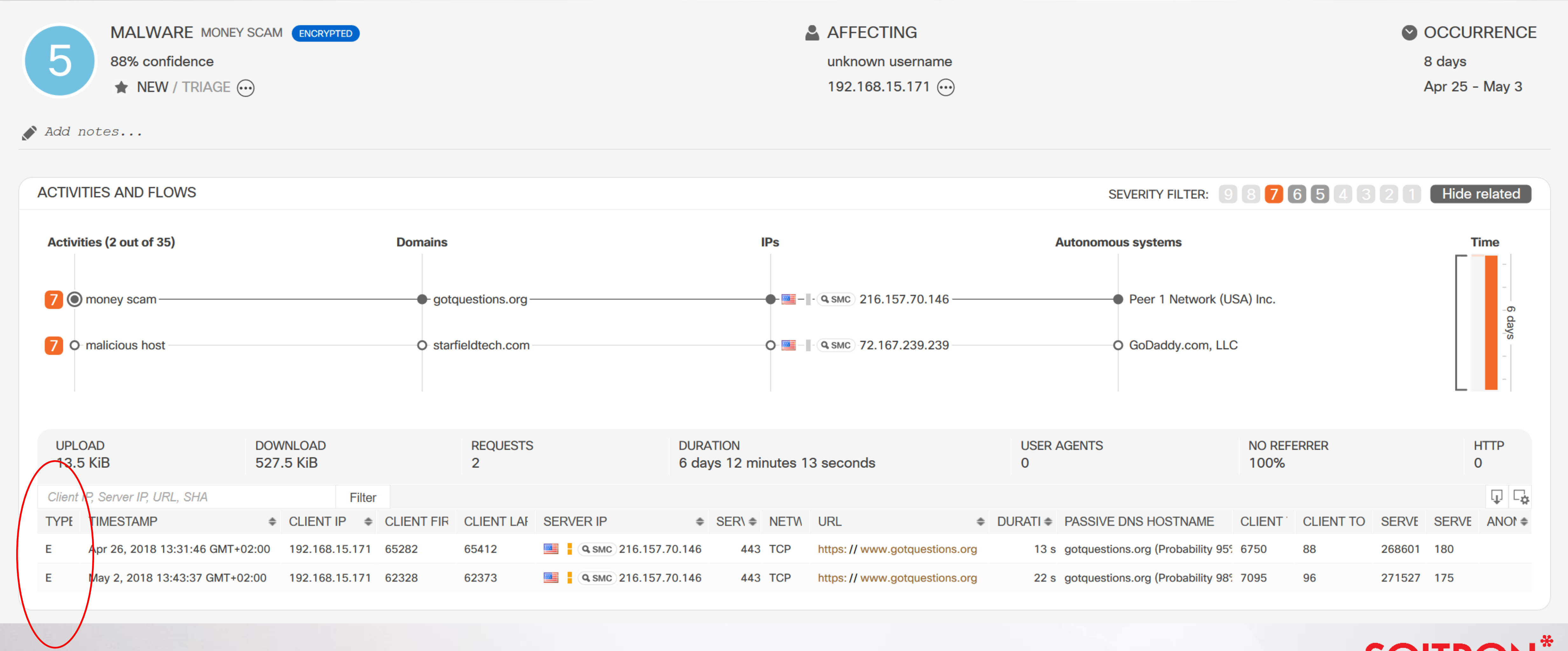
View URL Data

Subject		Totals		Peer	
Packets:	1.33 K	Packets:	2.73 K	Packets:	1.41 K
Packet Rate:	7.71 pps	Packet Rate:	15.89 pps	Packet Rate:	8.18 pps
Bytes:	234.52 KB	Bytes:	1.43 MB	Bytes:	1.2 MB
Byte Rate:	1.4 Kbps	Byte Rate:	8.73 Kbps	Byte Rate:	7.33 Kbps
Percent Transfer:	15.99%	Subject Byte Ratio:	15.99%	Percent Transfer:	84.01%
Host Groups:	Catch All	RTT:	4seconds	Host Groups:	United States
Payload:	...........[.V...+....#.b.	SRT:	0seconds	Payload:	SSL_CN: www.bing.com

	START	DURATION	SUBJECT IP A...	SUBJECT POR...	SUBJECT HOS...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...
▶	Nov 15, 2018 12:... *(5min 5s ago)*	3min 39s	10.67.58.140	50041/TCP	Catch All	6.47 K	news	763.21 K	TLS 1.2	ECDHE	RSA	AES_128_GCM/...	SHA256
▶	Nov 15, 2018 12:...	20s	10.67.58.140	50433/TCP	Catch All	821	business systems	571.19 K	TLS 1.2	ECDHE	RSA	AES_256_GCM/...	SHA384

Encrypted Traffic Analytics

- Type „E“



5

MALWARE MONEY SCAM ENCRYPTED

88% confidence

NEW / TRIAGE

AFFECTING

unknown username

192.168.15.171

OCCURRENCE

8 days

Apr 25 - May 3

Add notes...

ACTIVITIES AND FLOWS

SEVERITY FILTER: 9 8 7 6 5 4 3 2 1 Hide related

Activities (2 out of 35)	Domains	IPs	Autonomous systems
7 money scam	gotquestions.org	SMC 216.157.70.146	Peer 1 Network (USA) Inc.
7 malicious host	starfieldtech.com	SMC 72.167.239.239	GoDaddy.com, LLC

UPLOAD	DOWNLOAD	REQUESTS	DURATION	USER AGENTS	NO REFERRER	HTTP
13.5 KiB	527.5 KiB	2	6 days 12 minutes 13 seconds	0	100%	0

Client IP, Server IP, URL, SHA Filter

TYPE	TIMESTAMP	CLIENT IP	CLIENT FIR	CLIENT LAI	SERVER IP	SERV	NETW	URL	DURATI	PASSIVE DNS HOSTNAME	CLIENT	CLIENT TO	SERVE	SERVE	ANON
E	Apr 26, 2018 13:31:46 GMT+02:00	192.168.15.171	65282	65412	SMC 216.157.70.146	443	TCP	https: // www.gotquestions.org	13 s	gotquestions.org (Probability 95	6750	88	268601	180	
E	May 2, 2018 13:43:37 GMT+02:00	192.168.15.171	62328	62373	SMC 216.157.70.146	443	TCP	https: // www.gotquestions.org	22 s	gotquestions.org (Probability 98	7095	96	271527	175	

SOITRON*