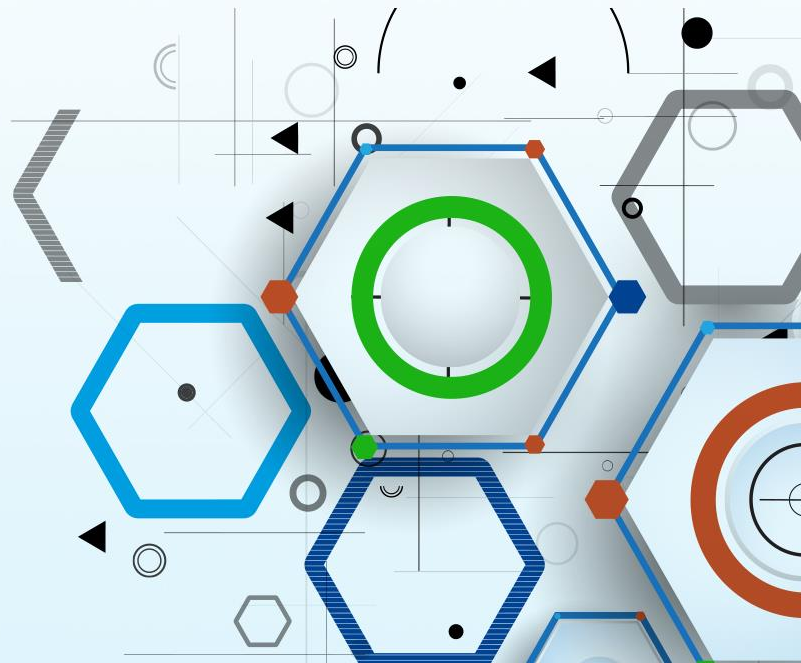




Monitorování chování sítě a detekce bezpečnostních incidentů

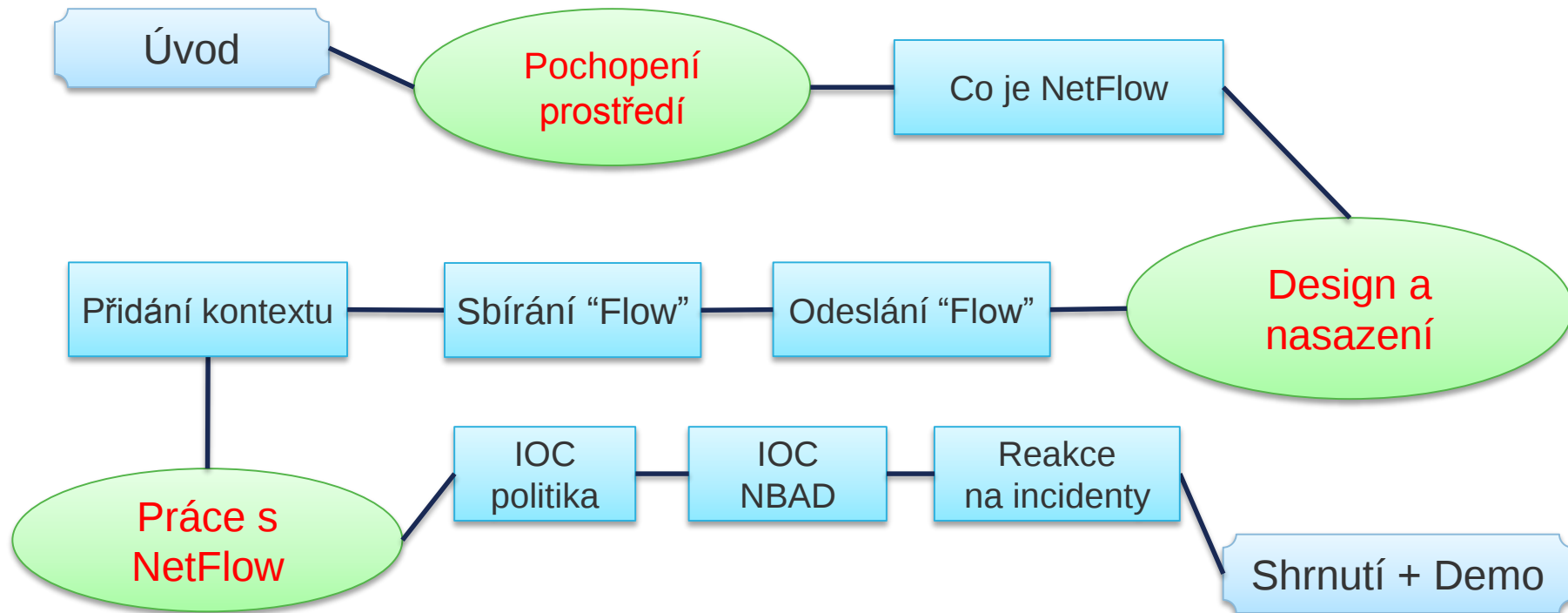
- SEC4 DETAIL/L2

Andrej Jeleník - Systems Engineer



Agenda

1. Prostředí a co je NetFlow?
2. Jak získat údaje / důkazy (D & D)
3. Hodnota dat / důkazů (analýza NetFlow)



Na co se zaměříme?



Hrozby uvnitř sítě

Zvládnutí hrozeb uvnitř sítě

Kontrola přístupu

- Kdo a co se snaží dostat do sítě



Jste kdo tvrdíte že jste, a to jsou zdroje, ke kterým máte povolen přístup na základě Vašich přihlašovacích údajů.



Segmentace

- Definuj co mohou dělat



Zvládnutí hrozeb uvnitř sítě

Kontrola pohybu škodlivého obsahu prostřednictvím kontrolních bodů



To je to, co je dovoleno vnášet do bezpečné zóny / sítě.



Kontrola obsahu

- Hluboká viditelnost obsahu na kontrolních bodech

Zvládnutí hrozeb uvnitř sítě

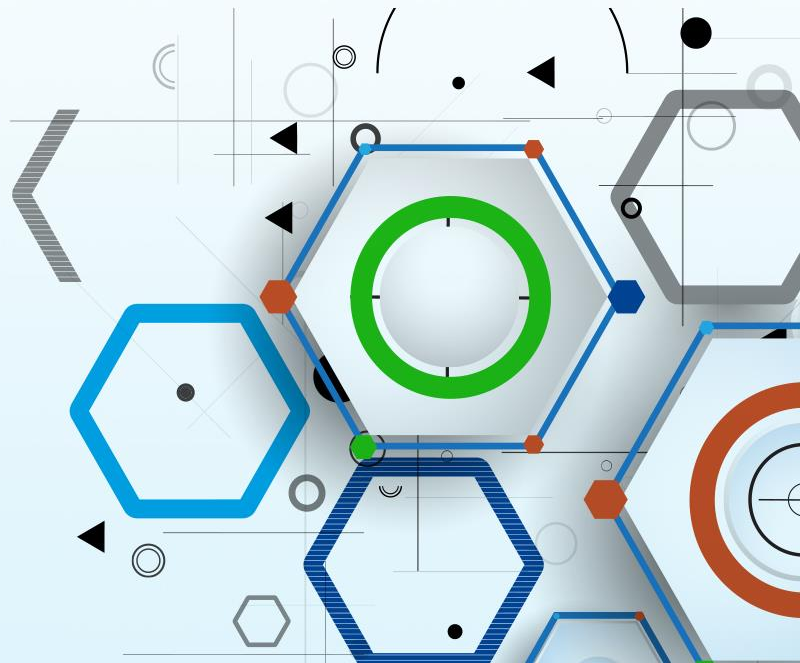
A teď sledovat činnost uvnitř
kontrolované a zabezpečené zóny.



Monitorovaný prostor poskytuje
viditelnost a vyšší bezpečnost.



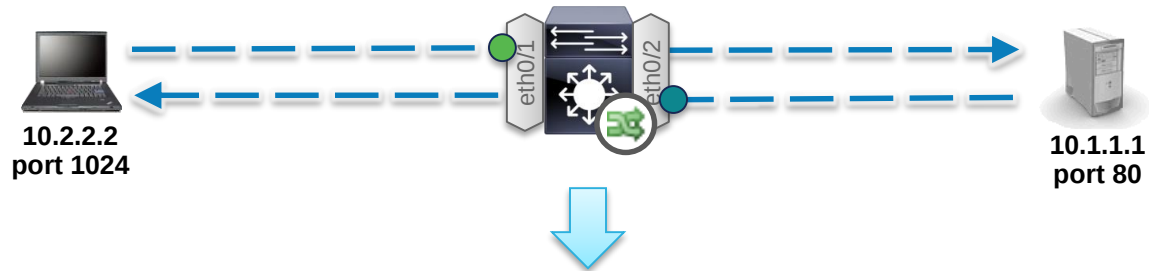
NetFlow



Introduction to NetFlow

- Developed by Cisco in 1996 as a packet forwarding mechanism
 - Uses a fixed seven tuples of IP information to identify a flow
 - Reporting is based on Flow and not necessarily per-packet
- Various versions exist version 1 through 9, with 5 being the most popular and 9 being the most functional
 - Traditional NetFlow (TNF) – fixed info to identify a flow
 - Flexible Netflow (FNF) – user defines how to identify a flow
- NetFlow will let you understand who, what, when, where, and how network traffic is flowing
- Flexible NetFlow fully supported in IOS 15.0 and up & IOS XE 3.1S and up

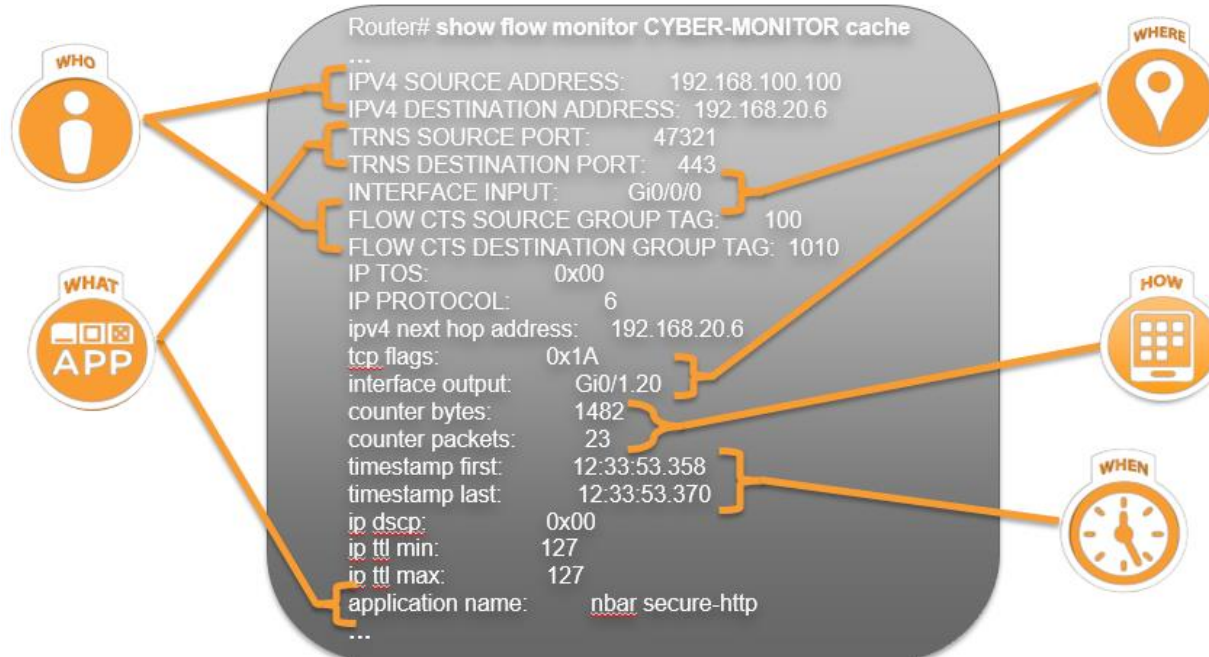
NetFlow



Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent	SGT	DGT	TCP Flags
10:20:12.221	eth0/1	10.2.2.2	1024	10.1.1.1	80	TCP	5	1025	100	1010	SYN,ACK,PSH
10:20:12.871	eth0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712	1010	100	SYN,ACK,FIN

NetFlow = Visibility

A single NetFlow Record provides a wealth of information



NetFlow - The Network Phone Bill

Telephone Bill

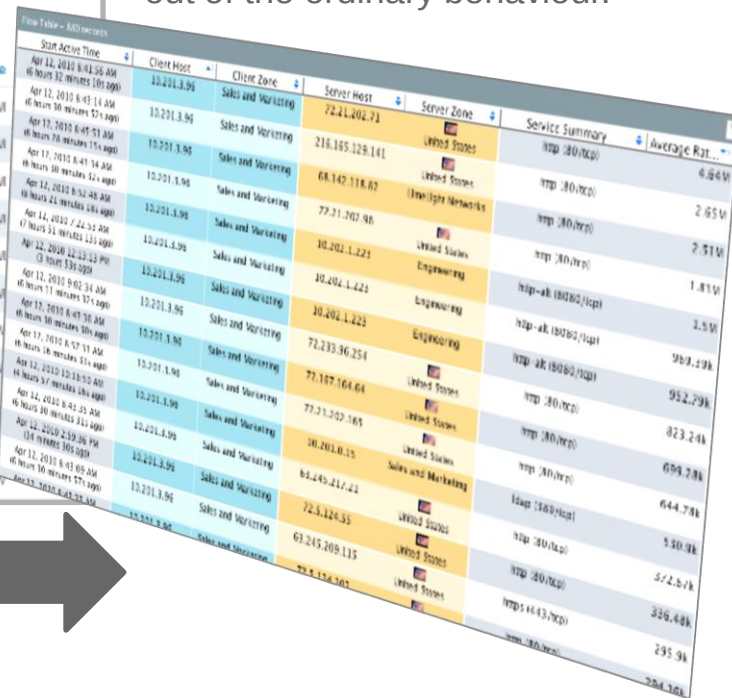


Monthly Statement
Bill At-A-Glance

#	Date	Time	Number Called	Min	Airtime Charge	LD/Add'l Charge	Feature
1	01/09/2013	02:05PM	678-936-2247	7	0.00	0.00	M2AM
2	01/08/2013	02:13PM	678-617-8151	1	0.00	0.00	M2AM
3	01/06/2013	02:14PM	678-617-7783	1	0.00	0.00	M2AM
4	01/08/2013	02:18PM	678-617-7783	7	0.00	0.00	M2AM
5	01/06/2013	02:35PM	678-997-8365	2	0.00	0.00	M2AM
6	01/06/2013	03:58PM	678-617-6151	2	0.00	0.00	M2AM
7	01/08/2013	04:00PM	678-617-8151	15	0.00	0.00	CN
8	01/06/2013	05:45PM	678-617-6151	36	0.00	0.00	M2AM
9	01/06/2013	05:23PM	678-997-8365	2	0.00	0.00	M2AM
10	01/06/2013	07:42PM	678-617-6151	6	0.00	0.00	M2AM
11	01/06/2013	07:47PM	678-617-7783	4	0.00	0.00	CN

NetFlow = shows you the **who, what, where and when**. It's a phone bill, which we use to look for out of the ordinary behaviour.

Flow Record

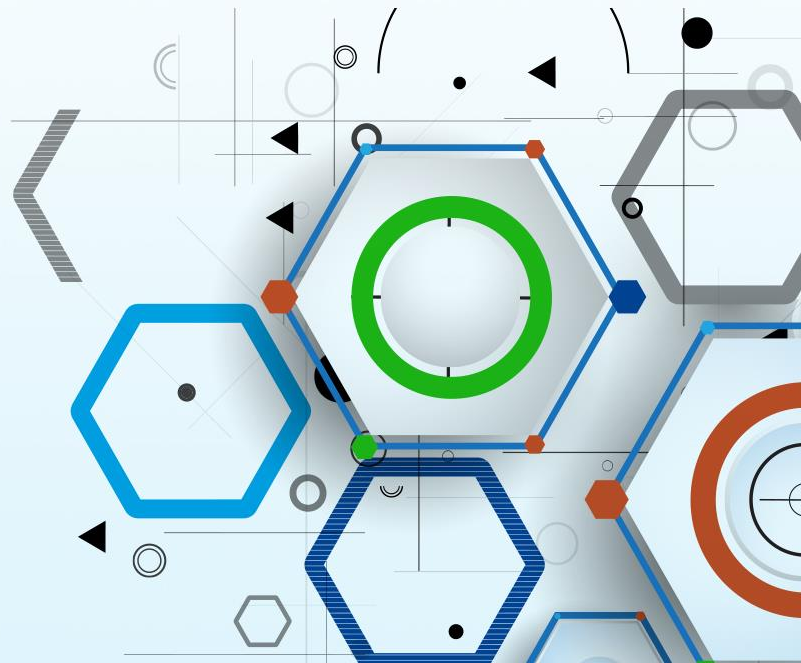


Start Active Time	Client Host	Client Zone	Server Host	Server Zone	Service Summary	Average RST...
Apr 12, 2010 8:41:36 AM 6 hours 32 minutes 101 ago	10.201.3.96	Sales and Marketing	72.21.202.71	United States	http://80/tcp	6.864M
Apr 12, 2010 8:43:14 AM 6 hours 30 minutes 571 ago	10.201.3.96	Sales and Marketing	216.185.128.141	United States	http://80/tcp	2.65M
Apr 17, 2010 8:45:51 AM 6 hours 28 minutes 171 ago	10.201.3.96	Sales and Marketing	68.142.118.67	United States	http://80/tcp	2.51M
Apr 17, 2010 8:41:14 AM 6 hours 30 minutes 521 ago	10.201.3.96	Sales and Marketing	77.21.202.98	United States	http://80/tcp	1.81M
Apr 12, 2010 8:52:48 AM 6 hours 21 minutes 541 ago	10.201.3.96	Sales and Marketing	10.202.1.223	Engineering	http://80/tcp	1.5M
Apr 14, 2010 7:42:22 AM 6 hours 51 minutes 121 ago	10.201.3.96	Sales and Marketing	10.202.1.223	Engineering	http://80/tcp	989.39K
Apr 12, 2010 12:13:22 PM 3 hours 536 ago	10.201.3.96	Sales and Marketing	10.202.1.223	Engineering	http://80/tcp	952.29K
Apr 12, 2010 9:02:34 AM 6 hours 11 minutes 321 ago	10.201.3.96	Sales and Marketing	72.233.36.254	United States	http://80/tcp	823.24K
Apr 17, 2010 8:45:36 AM 6 hours 30 minutes 501 ago	10.201.3.96	Sales and Marketing	77.187.164.64	United States	http://80/tcp	694.28K
Apr 17, 2010 8:57:11 AM 6 hours 18 minutes 511 ago	10.201.3.96	Sales and Marketing	77.21.202.165	United States	http://80/tcp	550.9K
Apr 12, 2010 10:18:52 AM 6 hours 17 minutes 481 ago	10.201.3.96	Sales and Marketing	10.201.0.15	United States	http://80/tcp	342.84K
Apr 14, 2010 8:42:25 AM 6 hours 34 minutes 211 ago	10.201.3.96	Sales and Marketing	68.245.217.21	United States	http://80/tcp	286.48K
Apr 12, 2010 2:59:36 PM 104 minutes 185 ago	10.201.3.96	Sales and Marketing	72.5.124.55	United States	http://80/tcp	295.9K
Apr 12, 2010 8:43:09 AM 6 hours 30 minutes 571 ago	10.201.3.96	Sales and Marketing	69.245.209.115	United States	http://80/tcp	286.48K
Apr 12, 2010 8:43:09 AM 6 hours 30 minutes 571 ago	10.201.3.96	Sales and Marketing	72.5.124.55	United States	http://80/tcp	295.9K

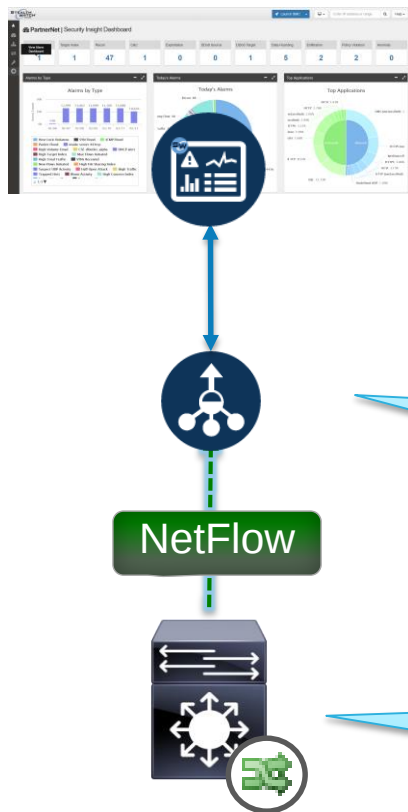


Viditelnost

Design a nasazení



NetFlow Deployment Architecture



Management/Reporting Layer:

- Run queries on flow data
- Centralize management and reporting

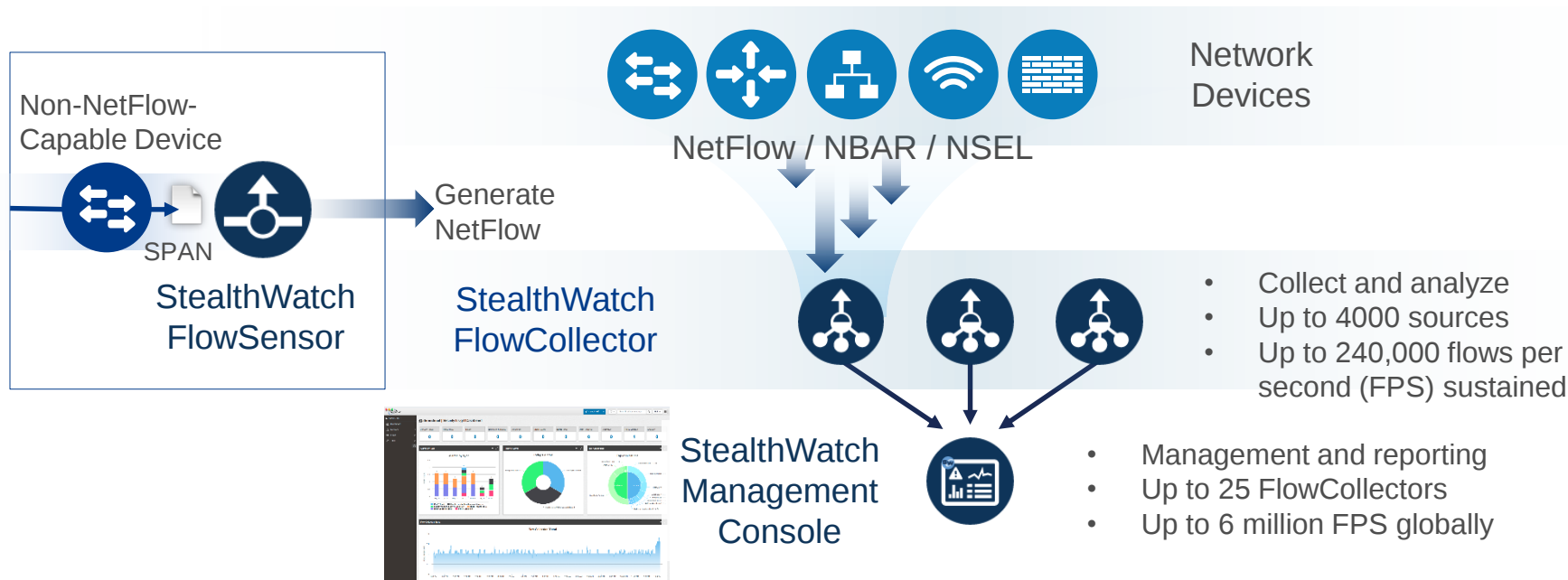
Flow Collection Layer:

- Collection, storage and analysis of flow records

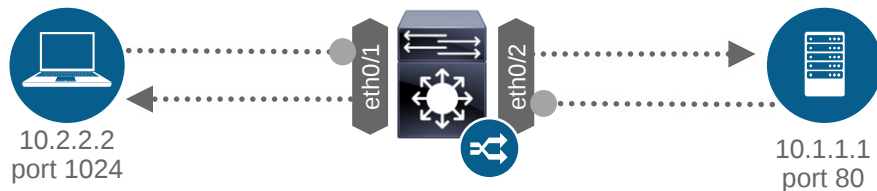
Flow Exporting Layer:

- Enables telemetry export
- As close to the traffic source as possible

StealthWatch System Overview



Scaling Visibility: Flow Stitching



Unidirectional Flow Records

Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent
10:20:12.221	eth0/1	10.2.2.2	1024	10.1.1.1	80	TCP	5	1025
10:20:12.871	eth0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712



Bidirectional Flow Record

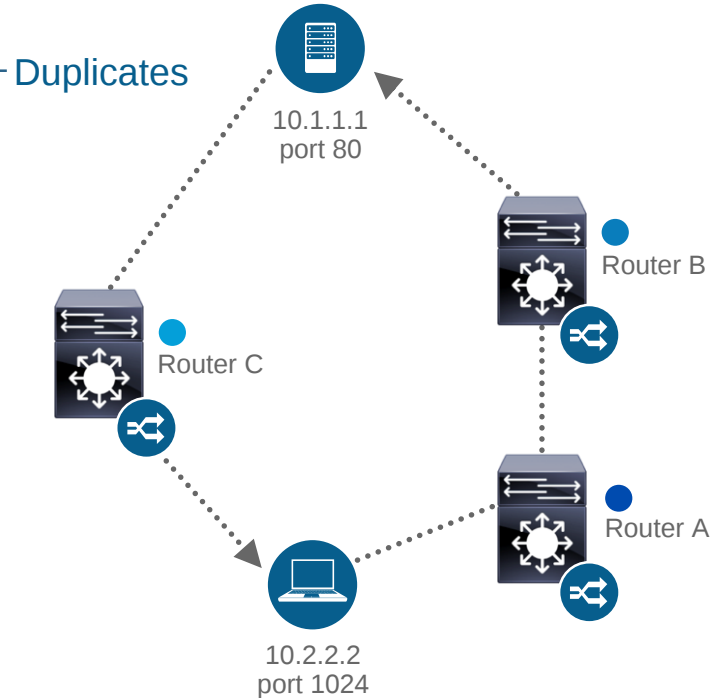
- Conversation flow record
- Allows easy visualization and analysis

Start Time	Client IP	Client Port	Server IP	Server Port	Proto	Client Bytes	Client Pkts	Server Bytes	Server Pkts	Interfaces
10:20:12.221	10.2.2.2	1024	10.1.1.1	80	TCP	1025	5	28712	17	eth0/1 eth0/2

Scaling Visibility: NetFlow Deduplication

- Router A: 10.2.2.2:1024 -> 10.1.1.1:80
- Router B: 10.2.2.2:1024 -> 10.1.1.1:80
- Router C: 10.1.1.1:80 -> 10.2.2.2:1024

- Without deduplication
 - Traffic volume can be misreported
 - False positives would occur
- Allows for efficient storage of flow data
- Necessary for accurate host-level reporting
- Does not discard data



Conversational Flow Record

Duration	Search Subject	Port	Traffic Summary	Port	Peer
Start: 05/29 - 12:19:18 PM End: 05/29 - 12:20:58 PM Duration: 1m 40s When	 10.10.18.102 RFC 1918 Where employee1 00:50:56:b4:3f:af Who	4866/TCP	11.49KB 285 packets  HTTP 1.62MB 1.15K packets	80/TCP What	 216.191.247.145 Canada crl.entrust.net Who

- Highly scalable (enterprise-class) collection
- High compression => long-term storage
 - Months of data retention

More context

Flow Detailed Summary: 10.10.18.102

Search Subject Details	Totals	Peer Details
Packets: 285	Packets: 1.44K	Packets: 1.15K
Packet Rate: 2.85pps	Packet Rate: 14.37pps	Packet Rate: 11.52pps
Bytes: 11.49KB	Bytes: 1.63MB	Bytes: 1.62MB
Byte Rate: 117.69bps	Byte Rate: 17.11Kbps	Byte Rate: 16.99Kbps
Percent Transfer: 0.6879458949171267%	Search Subject/Peer Ratio: 0.01	Percent Transfer: 99.31205410508288%
Host Groups: Desktops	TCP Connections: 2	Host Groups: Canada
TrustSec ID: 100	RTT: 2ms	Payload: 200_OK
TrustSec Name: Employees	SRT: 498ms	TrustSec ID: 0
Payload: GET http://crl.entrust.net/2048ca.crl		TrustSec Name: Unknown

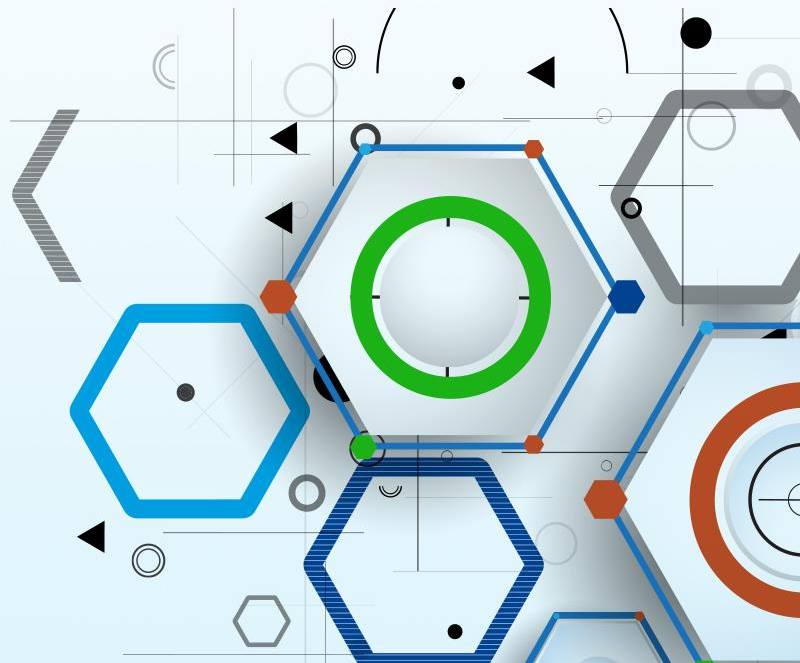
Security group

Close



Zjišťování

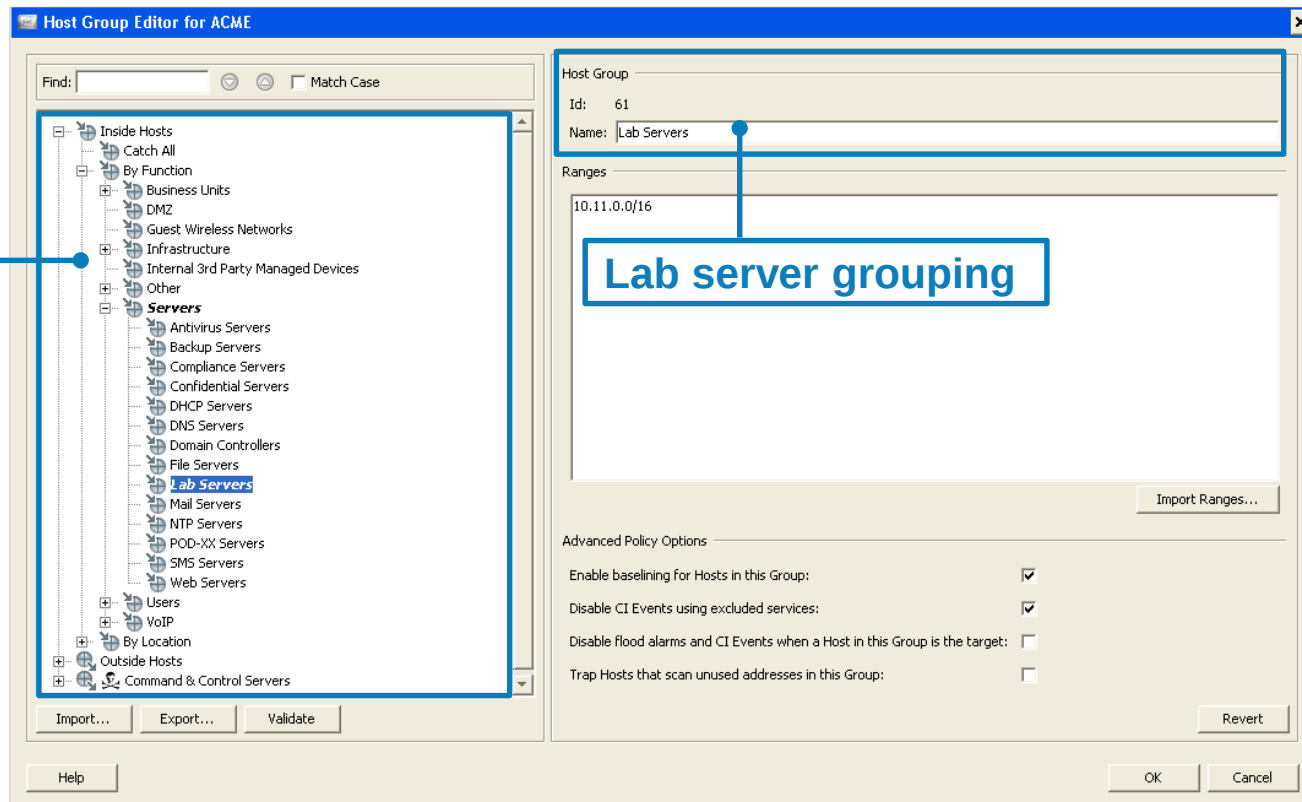
Design a nasazení



Host Groups: Applied Situational Awareness

Virtual container of multiple IP addresses/ranges that have similar attributes

Best practice:
Classify all known IP addresses into one or more host groups



Locating Services and Applications

Query Builder Standard Advanced

Range: Last 24 Hours -- OR -- From:
To:

☒ Search Subject

Host: +
User: +
Devices: +
Port/Protocol: includes 80/TCP +
TrustSec ID: +
TrustSec Name: +
Orientation: either

☒ Peer

Host: +
User: +
Devices: +
Port/Protocol: +
TrustSec ID: +
TrustSec Name: +

Search for assets based on transactional data — for example, protocol (HTTP servers, FTP server, etc.)

Flow Query Results

Duration	Search Subject	Port	Traffic Summary	Port	Peer
Start: 05/24 - 02:33:38 PM End: 05/24 - 02:36:59 PM Duration: 3m 21s	 10.3.200.10 RFC 1918	80/TCP	71.84KB 160 packets → HTTP ← 44.44KB 324 packets	52171/TCP	 10.10.18.102 RFC 1918 w7-client-3850.cts.local employee1, pciuser1 00:50:56:b4:3f:af

Identify servers and assets

Profile Applications

+

 Custom Application: Production Payment Processing

Name:

Production Payment Processing

Description:

Payment processing application on production server

 Add Rule

Enter criteria to define the custom application below. Criteria within each block is "AND-ed" together. Subsequent blocks are "OR-ed" together.

Port/Protocol: ⓘ

80/TCP

Server: ⓘ

IP Address

10.3.200.10

DPI Classification: ⓘ

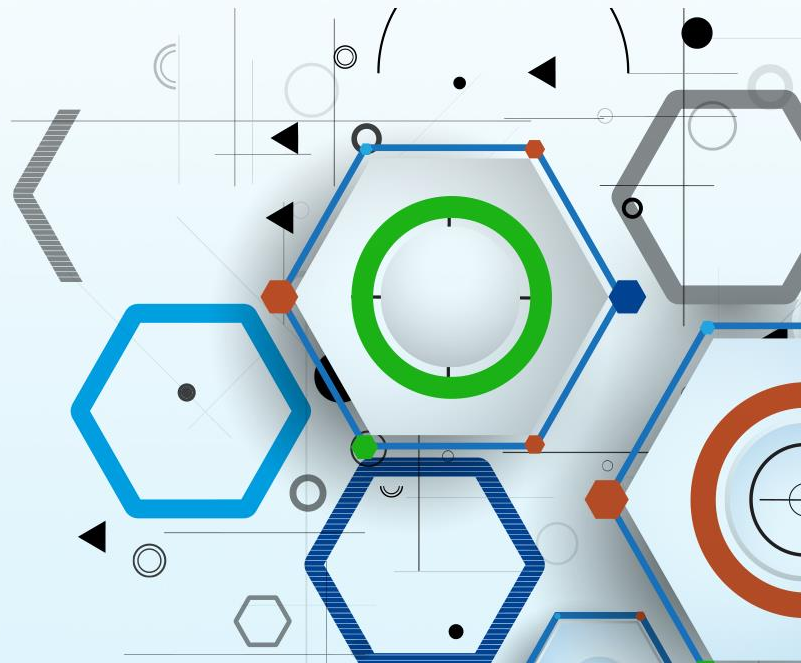
HTTP

+ Add to Rules

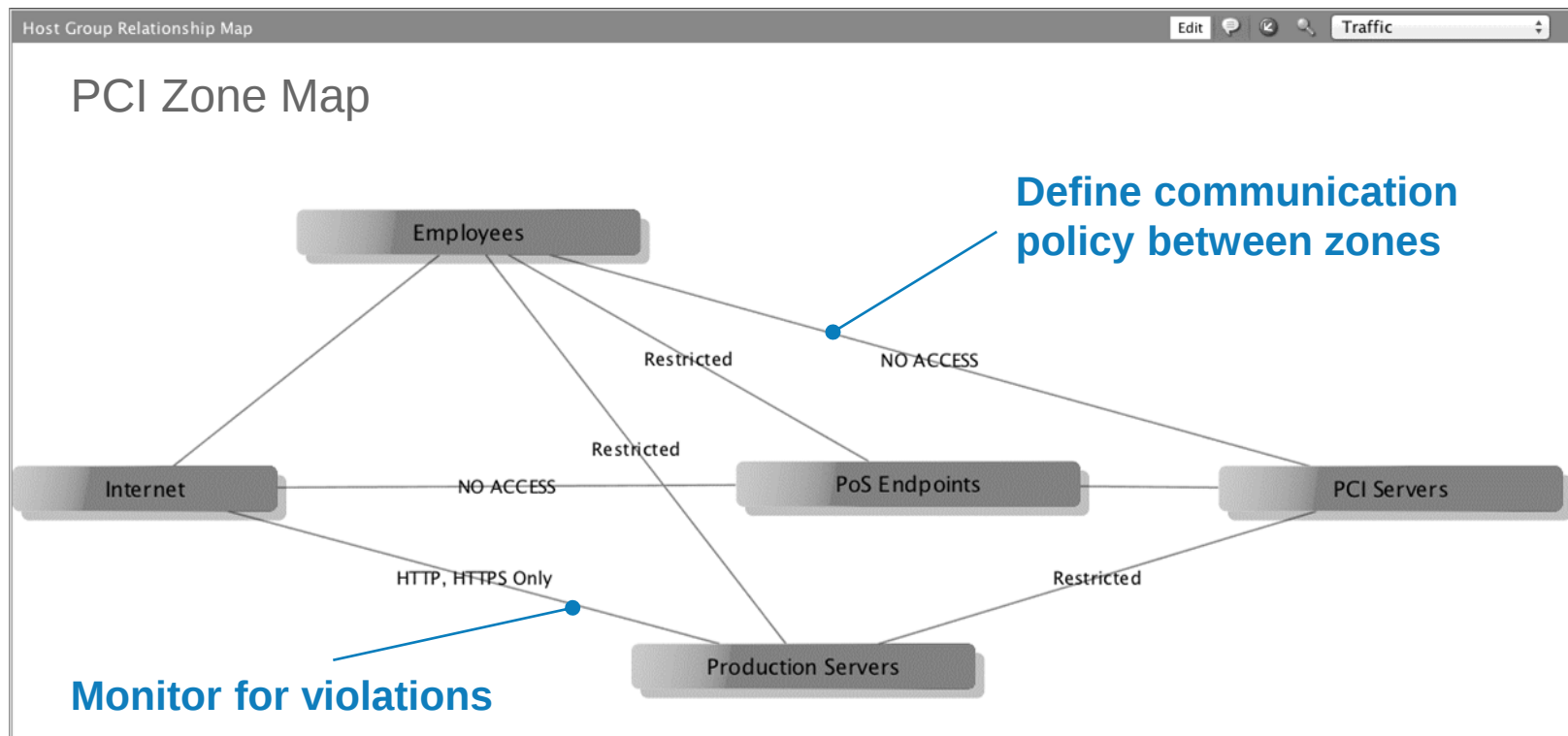
Classify business-critical applications



Indication of Compromise: Politika a segmentace



Segmentation Monitoring with StealthWatch



Policy Modeling and Monitoring

Custom Event: Employee to PCI Servers

Custom event triggers on traffic condition

Rule/Event Name:

Employee to PCI Servers

Description:

Violation of Security Group Policy

Rule name and description

Object

Host: +

User: +

Devices: +

Port/Protocol: +

TrustSec ID:

includes

100

SGT

+

-

TrustSec Name:

+

Application:

+

Orientation:

either

Trigger on traffic in both directions, successful or unsuccessful

Peer

Host: +

User: +

Devices: +

Port/Protocol: +

TrustSec ID:

includes

2000

DGT

+

-

TrustSec Name:

+

Application:

+

Modeling Policy in StealthWatch

Create flow-based rules for all proposed policy elements

demo.local | Custom Security Events

Custom Security Events ? [Add Custom Event](#)

Event Name	Date Modified	Description	Edit	Delete	Enabled
Employee to Production Servers	5/1/15 5:03 PM	Violation of Security Group Policy.			ENABLED
Employee to PCI Servers	5/1/15 2:15 PM	Violation of Security Group Policy			ENABLED

Policy violation alarm will trigger if condition is met.

Modeling Policy: Alarm Occurrence

 demo.local | Alarm Dashboard : Policy Violation (1)

Alarm dashboard showing
all policy alarms

 Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Policy	Event Alarms	Source User	Details
5/25/15 4:42 PM	Catch All	10.10.18.102	--	Multiple Hosts	Inside Hosts	Employee to Production Servers	employee1	Expected 1 points, tolerance of 75 allows up to 300k points.

Details of “Employee to
Production Servers”
alarm occurrences

 demo.local | Alarms : Employee to Production Servers for 5/25/2015 (1)

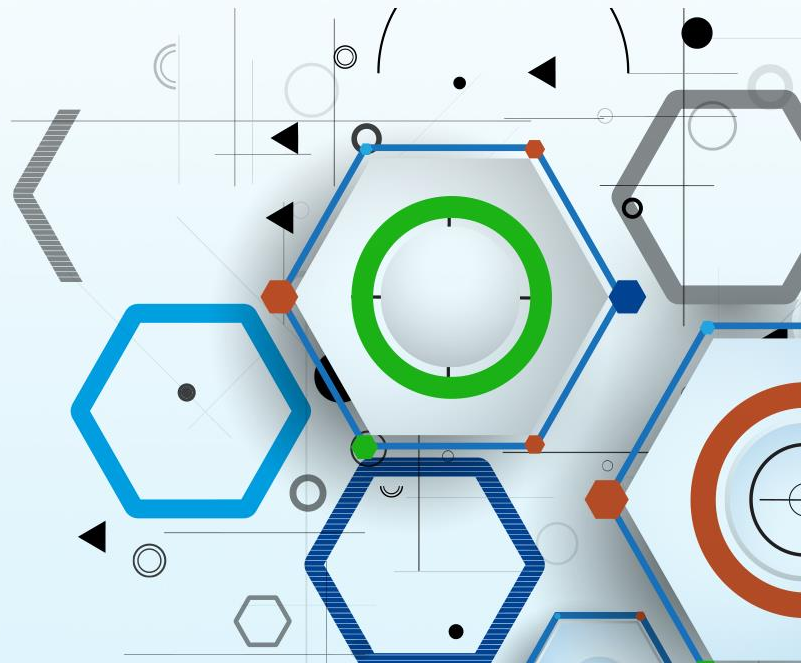
 Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Source User	Details	Last Active	Active	Acknowledged
5/25/15 4:42 PM	Catch All	10.10.18.102	Catch All	10.3.200.10	Employee to Production Servers	Inside Hosts	employee1	View Details	Current	Yes	No



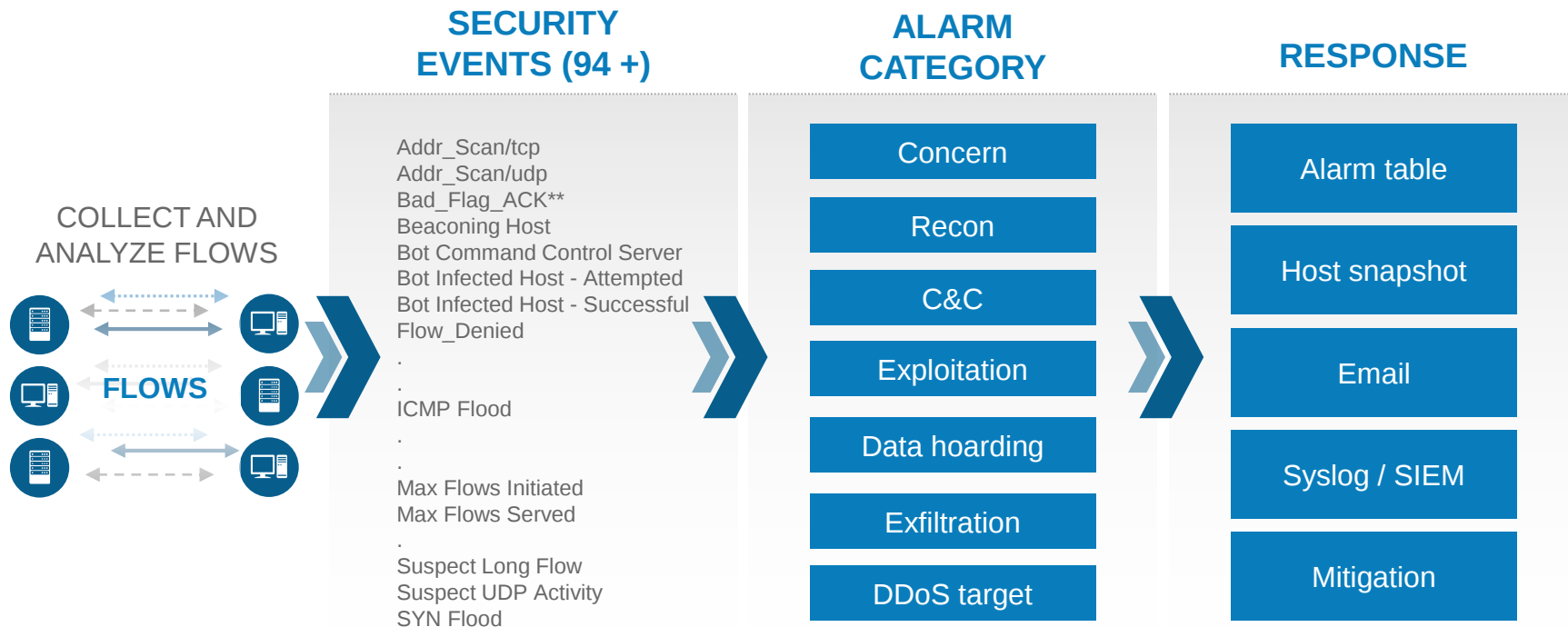
Indication of Compromise: Detekce anomálního chování v síti

Network Behavior Anomaly Detection



Behavioral and Anomaly Detection Model

Behavioral Algorithms Are Applied to Build “Security Events”



StealthWatch Alarm Categories

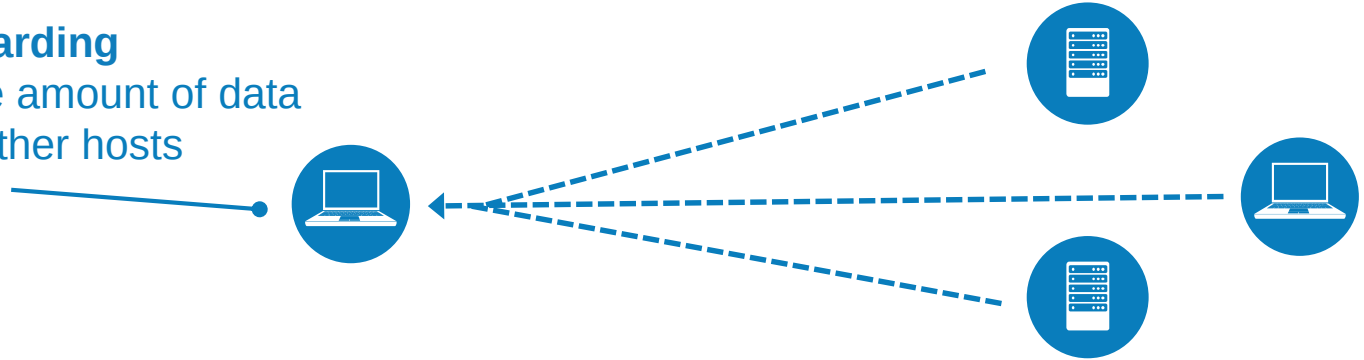


Each category accrues points

Example Algorithm: Data Hoarding

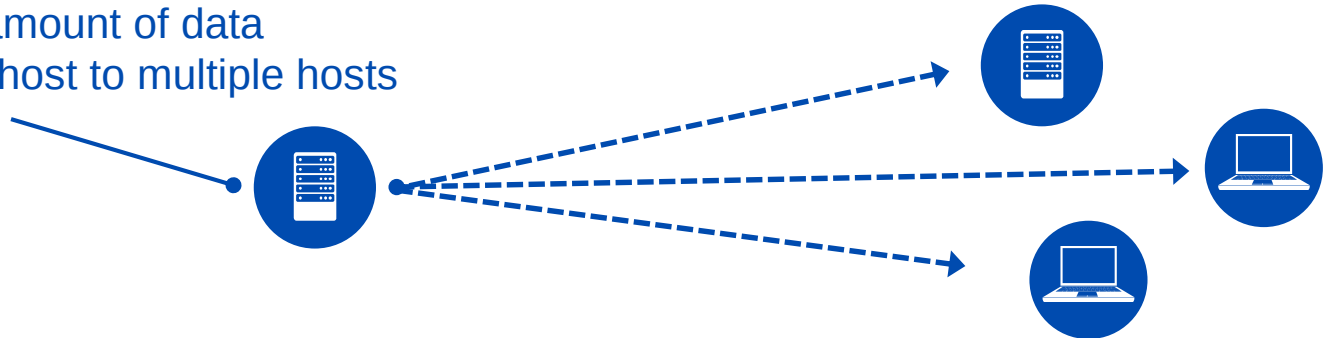
Suspect Data Hoarding

- Unusually large amount of data inbound from other hosts



Target Data Hoarding

- Unusually large amount of data outbound from a host to multiple hosts



Network Behavior and Anomaly Detection

Alarm Model

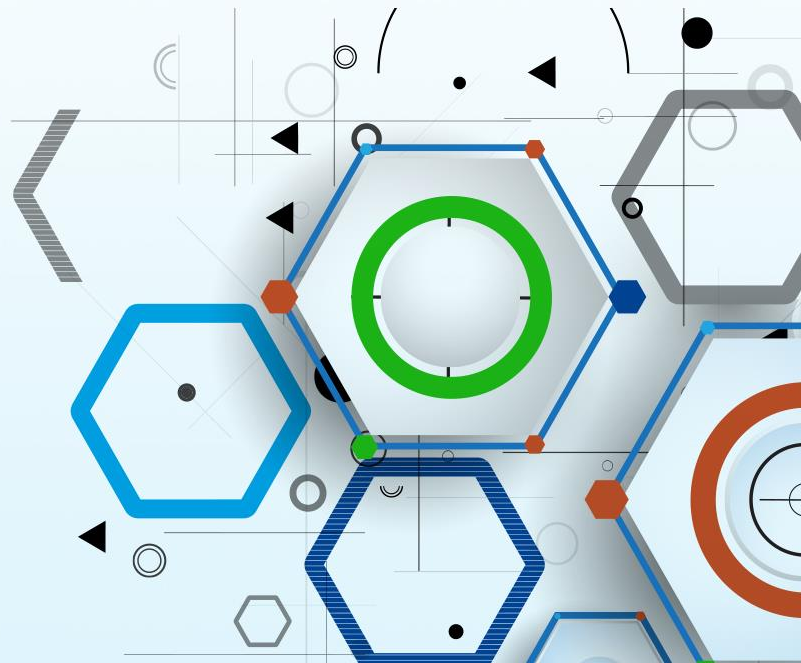
- Monitor activity and alarm on suspicious conditions
- Policy and behavioral

First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Source User	Details	Last Active
5/29/15 12:00 PM	Atlanta, Sales and Marketing, Desktops	10.201.3.18	--	Multiple Hosts	Suspect Data Hoarding	10.201.3.18	--	Observed 23.9G bytes. Policy maximum allows up to 50M bytes.	5/29/15 1:05 PM
5/29/15 11:20 AM	Terminal Server, Datacenter	10.201.0.23	--	Multiple Hosts	Suspect Data Hoarding	10.201.0.23	--	Observed 38.45G bytes. Policy maximum allows up to 50M bytes.	5/29/15 2:40 PM



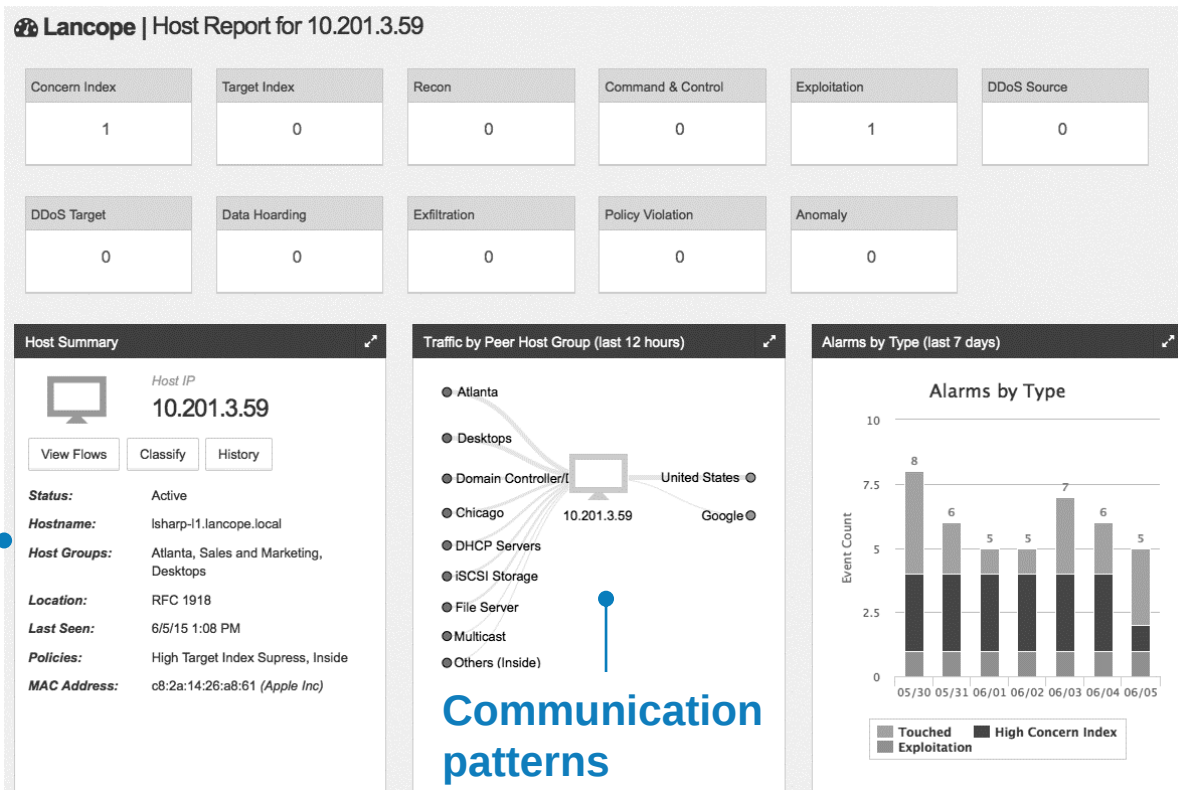
Reakce na incidenty

Incident Response



Investigating a Host

Summary



Investigating: Host Drill-Down

Users & Sessions		
Mac Address:	Mac Vendor:	Device Type:
c8:2a:14:26:a8:61	Apple Inc	Apple Ipad
User	Start	End
betty	6/5/15 11:36 AM	★ Current
betty	6/5/15 8:06 AM	6/5/15 11:20 AM
betty	6/5/15 7:24 AM	6/5/15 7:50 AM
betty	6/5/15 12:22 AM	6/5/15 7:08 AM
betty	6/4/15 7:31 PM	6/5/15 12:09 AM
betty	6/4/15 6:46 PM	6/4/15 7:15 PM
betty	6/4/15 5:21 PM	6/4/15 6:32 PM
betty	6/4/15 1:50 PM	6/4/15 5:07 PM
betty	6/4/15 1:07 PM	6/4/15 1:37 PM

User information

Application Traffic

Internal

External

Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour
HTTP	47.83MB	37.00	6.12MB		41.71MB		
HTTPS	42.41MB	33.00	1.27MB		41.14MB		
HTTPS (u...	16.06MB	12.00	16.03MB		30.55KB		
Undefined...	11.13MB	9.00	3.05MB		8.08MB		
DNS	1.32MB	1.00	427.12KB		926.13KB		
authentica...	1.9MB	1.00	934.58KB		1014.67KB		

Investigating: Audit Trails

Network behavior retroactively analyzed

Flows (20)

Actions

- Save Results
- Save Query
- Clone Query
- Export as .CSV

Current Filters

No Filters Selected

[Clear All](#)

Filter Results By:

Search Subject

Host Groups 

[Inside Hosts \(58\)](#)

Flow Query Results

Duration	Search Subject	Port	Traffic Summary	Port	Peer
Start: 01/11 - 11:54:01 PM End: 01/11 - 11:57:32 PM Duration: 3m 31s	 10.201.3.78  RFC 1918 ethel View Details	17500/UDP	17.86KB 72 packets → Undefined UDP ← 0B 0 packets	17500/UDP	 255.255.255.255  Unknown
Start: 01/11 - 11:56:15 PM End: 01/11 - 11:56:56 PM Duration: 41s	 10.201.3.78  RFC 1918 ethel View Details	54279/TCP	4.19KB 15 packets → search ← 12.99KB 16 packets	80/TCP	 74.125.137.113  United States yh-in-f113.1e100.net
Start: 01/11 - 11:54:01 PM End: 01/11 - 11:54:24 PM Duration: 23s	 10.201.3.78  RFC 1918 ethel View Details	54229/TCP	9.05KB 22 packets → HTTP (unclassified) ← 5.45KB 12 packets	80/TCP	 98.136.145.153  United States r2.ycpi.vip.ac4.yahoo.net

Extrapolating to a User

The screenshot displays the Cisco User interface for a user named 'ethel'. The interface is divided into several sections:

- Username:** 'ethel' is displayed at the top left.
- Active Directory details:** This section includes a user profile picture and a list of icons representing different user attributes or roles.
- View flows:** A button labeled 'View Flows' is located in the left sidebar.
- Concern Index:** A section showing a progress bar for '7 days' and '24 hrs'.
- Recon:** Another section showing a progress bar for '7 days' and '24 hrs'.
- Command & Control:** A section at the bottom left with a progress bar for '7 days'.
- Devices and sessions:** A table listing active sessions for the user.

The 'Devices and sessions' table contains the following data:

Mac Address	Host	Name	Group	Mac Vendor	Location	Count	Device Type	Start	End
14:7d:c5:bf:34:85	10.201.3.78	--	Sales and Marketing Atlanta Desktops	Unknown	RFC 1918	5	Unknown	1/11/15 10:25 PM	★ Current
00:26:b0:ca:f2:a9	10.202.1.151	--	Atlanta Sales and Marketing Desktops	Unknown	RFC 1918	5	Unknown	1/11/15 10:11 PM	1/11/15 10:21 PM

Adaptive Network Control



Cisco® Identity
Services Engine



StealthWatch
Management Console

Quarantine or unquarantine via pxGrid

Host Summary

 **Host IP**
192.168.100.101

[View Flows](#) [Classify](#) [History](#)

Status: Active

Hostname: sj0-i3-svr-101.cisco.com

Host Groups: PCI Servers

Location: RFC 1918

Last Seen: 1/9/15 1:56 PM

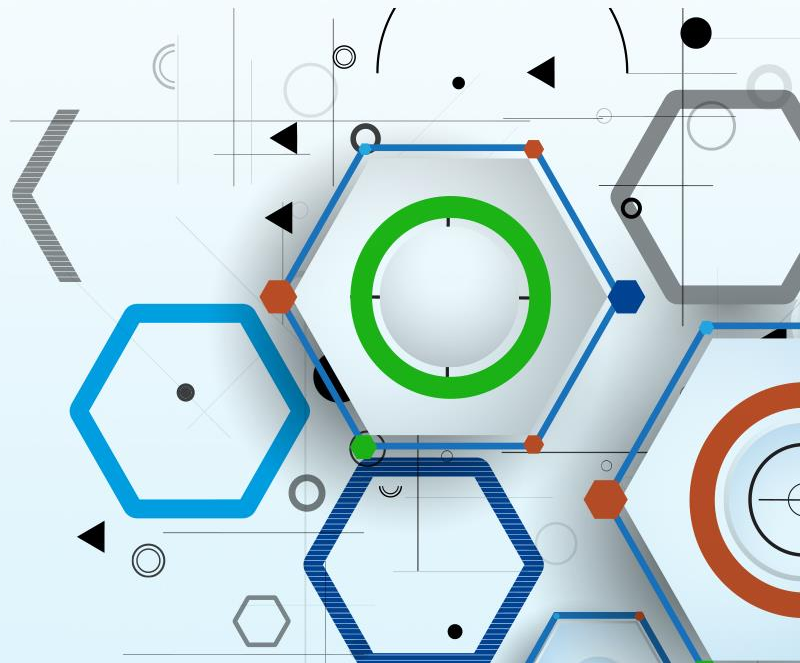
Policies: Inside, Servers

MAC Address: --

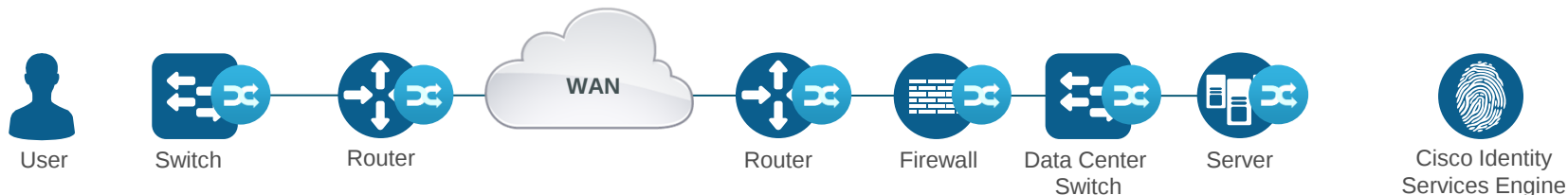
[Quarantine](#) [Unquarantine](#)



Shrnutí



NetFlow Supported Platforms



NetFlow Exporters

Cisco® Catalyst® 2960-X (NetFlow Lite) - sample only
Cisco Catalyst 3560-X (SM-10G module only)
Cisco Catalyst 3750-X (SM-10G module only)
Cisco Catalyst 3850/3650 (FNF v9 SGT support)
Cisco Catalyst 4500E (Sup7E/7LE)
Cisco Catalyst 4500E (Sup8) (FNF v9 SGT support)
Cisco Catalyst 6500E (Sup2T) (FNF v9 SGT support)
Cisco Catalyst 6800 (FNF v9 SGT support)
Cisco ISR G2 (FNF v9 SGT support)
Cisco 4000 Series ISR (FNF v9 SGT support)
Cisco ASR 1000 Series (FNF v9 SGT support)
Cisco Cloud Services Router 1000v Series (FNF v9 SGT support)

Cisco 5760 Wireless LAN Controller (WLC) (FNF v9)
Cisco 5520, 8510, 8540 WLC (v9)*
Cisco ASA 5500, 5500-X (NSEL)
Cisco Nexus® 7000 Series (M Series I/O modules – FNF v9)
Cisco Nexus 1000v (FNF v9)
Cisco NetFlow Generation Appliance (FNF v9)
Cisco UCS® Virtual Interface Card (VIC) (VIC 1224/1240/1280/1340/1380)

Lancope is now part of Cisco



StealthWatch
Management Console



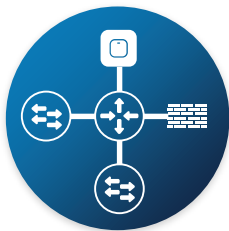
StealthWatch FlowCollector



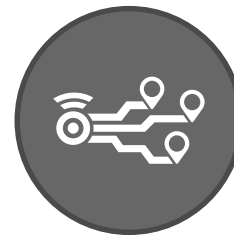
StealthWatch FlowSensor

For more information, visit: <http://www.cisco.com/c/en/us/solutions/enterprise-networks/threat-defense/index.html>

Key Takeaways



**The network is a key
asset for threat
detection and control**



**NetFlow and
StealthWatch provide
visibility and intelligence**

Reference:

Lancope is Now Part of Cisco

<https://www.lancope.com/partners/lancope-now-part-cisco>

StealthWatch Wiki

<https://www.lancope.com/wiki>

Cisco Cyber Threat Defense Solution

<http://cs.co/9004BYtJ8>

Cisco Cyber Threat Defense Solution Data Sheet

<http://cs.co/9005BYtJ3>

Cisco Identity Services Engine and Lancope StealthWatch Integration

<http://cs.co/9001BYtJT>





Děkujeme za pozornost.

DEMO

<https://dcloud-lon-web-1.cisco.com/dCloud/drn.jsp>

