



Behavior-Based Intrusion Detection - Theory and Implementation

Trinh Ngoc Minh

Ph.D, CISSP

Security Solution Consultant – Cisco Systems Vietnam

Hanoi July 2017



Agenda

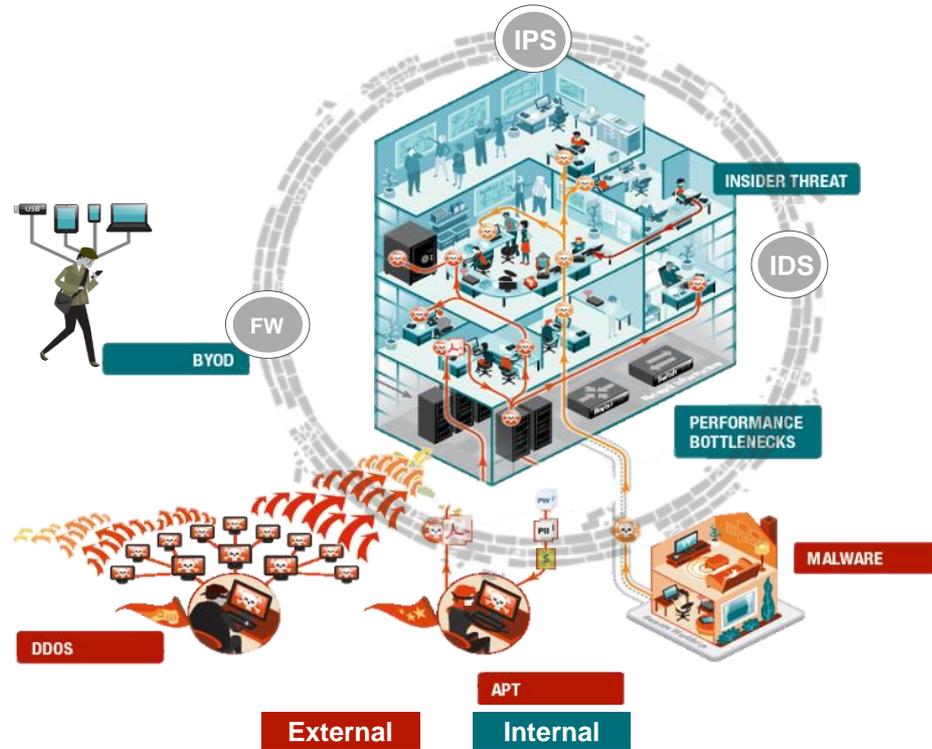
1. Threat Landscape and Today's Security Challenges
2. Behavior-based Intrusion Detection Approach
3. StealthWatch: Behavior-based Intrusion Detection System basing on Network Communication Data

Threat Landscape and Today's Security Challenges

APT's

- Written by professional engineering teams
- Not released until they are guaranteed to circumvent your protection systems
- Backed by nation-states that have a large enough budget to circumvent your commercial anti-virus

Realities of Modern Threats



Highlights

One in four breaches are caused by malicious insiders

95% of all cybercrime is triggered by a user clicking on a malicious link disguised to be legitimate

Two in three breaches exploit weak or stolen passwords

With lateral movement of advanced persistent threats, even external attacks eventually become internal threats

Source: 2014 Verizon Data Breach Investigations Report and Forrester research.

Three Kinds of Insider Threats

Negligent Insiders:

- Employees who accidentally expose data

Malicious Insiders:

- Employees who intentionally expose data



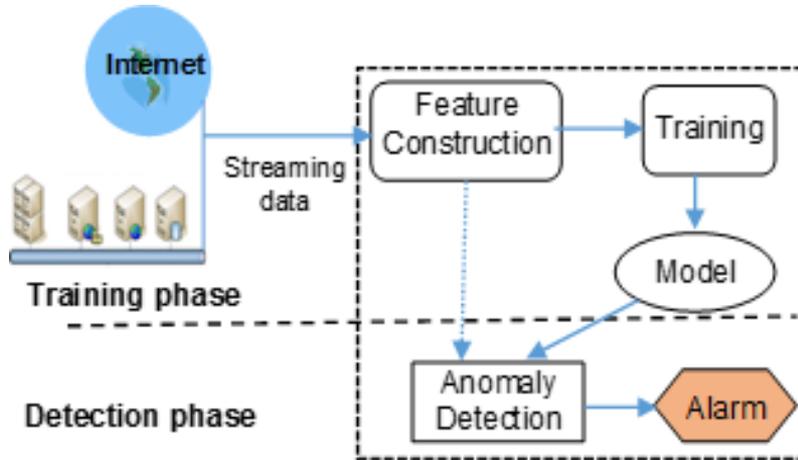
Compromised Insiders:

- Employees whose access credentials or devices have been compromised by an outside attacker

Behavior-based Intrusion Detection Approach

Anomaly-based IDS Architecture

Technologies



Statistical

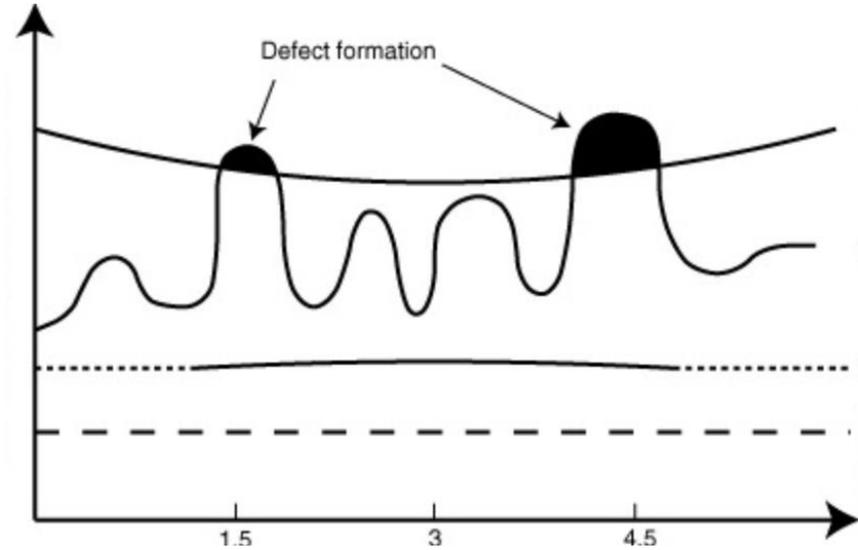
Information theory

Clustering

Classification

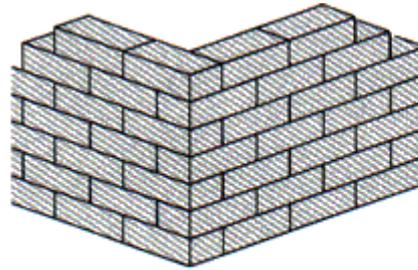
Statistical

- Regression, correlation, chi-square...
- Threshold used for alert

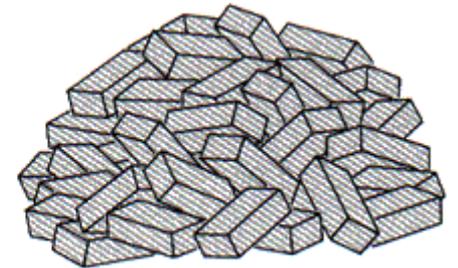


Information Theory

- Level of Entropy (Packet content, IP addresses, DNS domain name...)



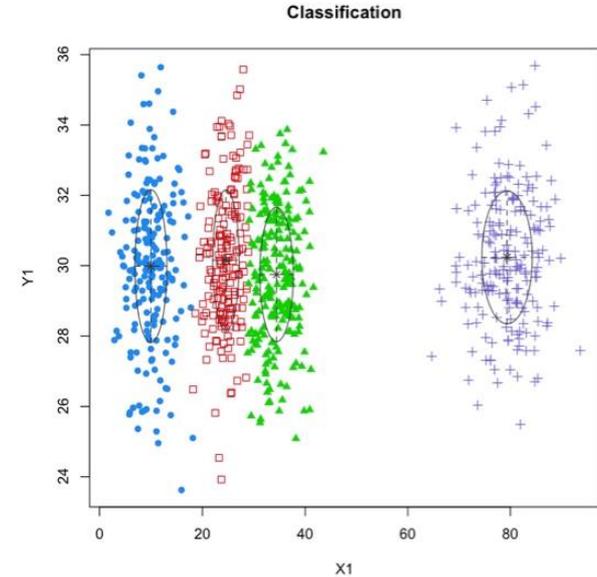
(a)



(b)

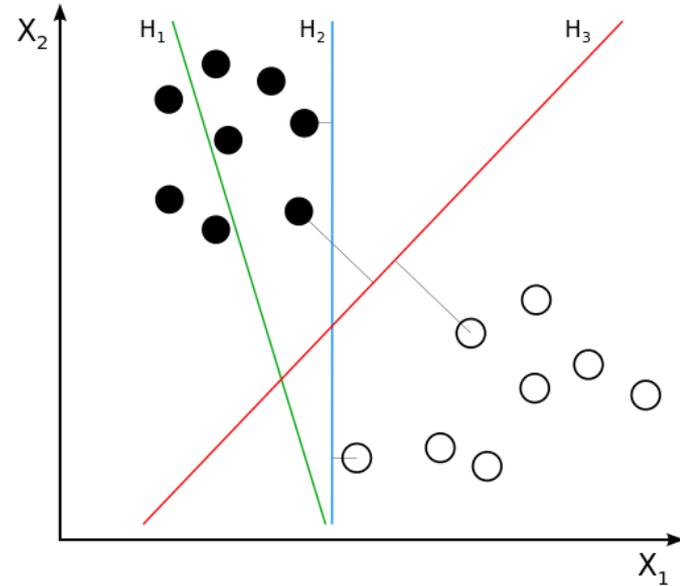
Clustering

1. Self-Organizing Map (SOM):
Unsupervised learning
2. Hierarchical Clustering:
clustering based on distance
3. *k*-means clustering:
partitioning n object into k sets
with minimum overall distance
in each set.
4. ...



Classification

- ~ Supervised (labeled training data) learning.
- Algorithms: Support Vector Machine, Neuron Network, Bayesian, Decision tree...



Note

- No the best model!
- Fault positive problem, so learning and continuous learning are key factors.
- Big data, high performance are required.

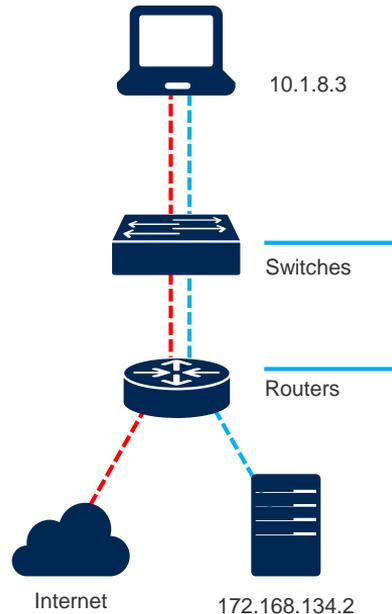
Behavior-based IDS basing on Network Communication Data

StealthWatch

Visibility Through Netflow

Netflow Provides

- A trace of every conversation in your network
- An ability to collect records everywhere in your network (switch, router, or firewall)
- Network usage measurements
- An ability to find north-south as well as east-west communication
- Lightweight visibility compared to Switched Port Analyzer (SPAN)-based traffic analysis
- Indications of compromise (IOC)
- Security group information



Flow Information	Packets
SOURCE ADDRESS	10.1.8.3
DESTINATION ADDRESS	172.168.134.2
SOURCE PORT	47321
DESTINATION PORT	443
INTERFACE	Gi0/0/0
IP TOS	0x00
IP PROTOCOL	6
NEXT HOP	172.168.25.1
TCP FLAGS	0x1A
SOURCE SGT	100
:	:
APPLICATION NAME	NBAR SECURE-HTTP

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

The General Use cases

Use Cases

Insider Threat	Internal User Monitoring	Firewall Planning	Segmentation	Network Operations	Network Visualization	TrustSec
----------------	--------------------------	-------------------	--------------	--------------------	-----------------------	----------

Event Data

Security Events

Behavioral Analytics

Session Data | *100% network accountability*

Client	Server	Translation	Service	User	Application	Traffic	Group	Mac	SGT
1.1.1.1	2.2.2.2	3.3.3.3	80/tcp	Doug	http	20M	location	00:2b:1f	10

Visibility



The General Ledger

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 What	11.49KB 285 packets HTTP 1.62MB 1.15K packets	80/TCP What	202.173.28.250 Australia probe-airtel.bgl.expertcity.com Who

- Stitched and de-duplicated
- Conversational representation
- Highly scalable data collection and compression
 - Enables months of data retention

Flow Detailed Summary: 10.10.18.102

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

More context

Close

See and detect more in your network with Stealthwatch



Monitor

- Obtain comprehensive, scalable enterprise visibility and security context
- Gain real-time situational awareness of traffic



Detect

- Detect and analyze network behavior anomalies
- Easily detect behaviors linked to advanced persistent threats (APTs), insider threats, distributed denial-of-service (DDoS) attacks, and malware



Analyze

- Collect and analyze holistic network audit trails
- Achieve faster root cause analysis
- Conduct thorough forensic investigations



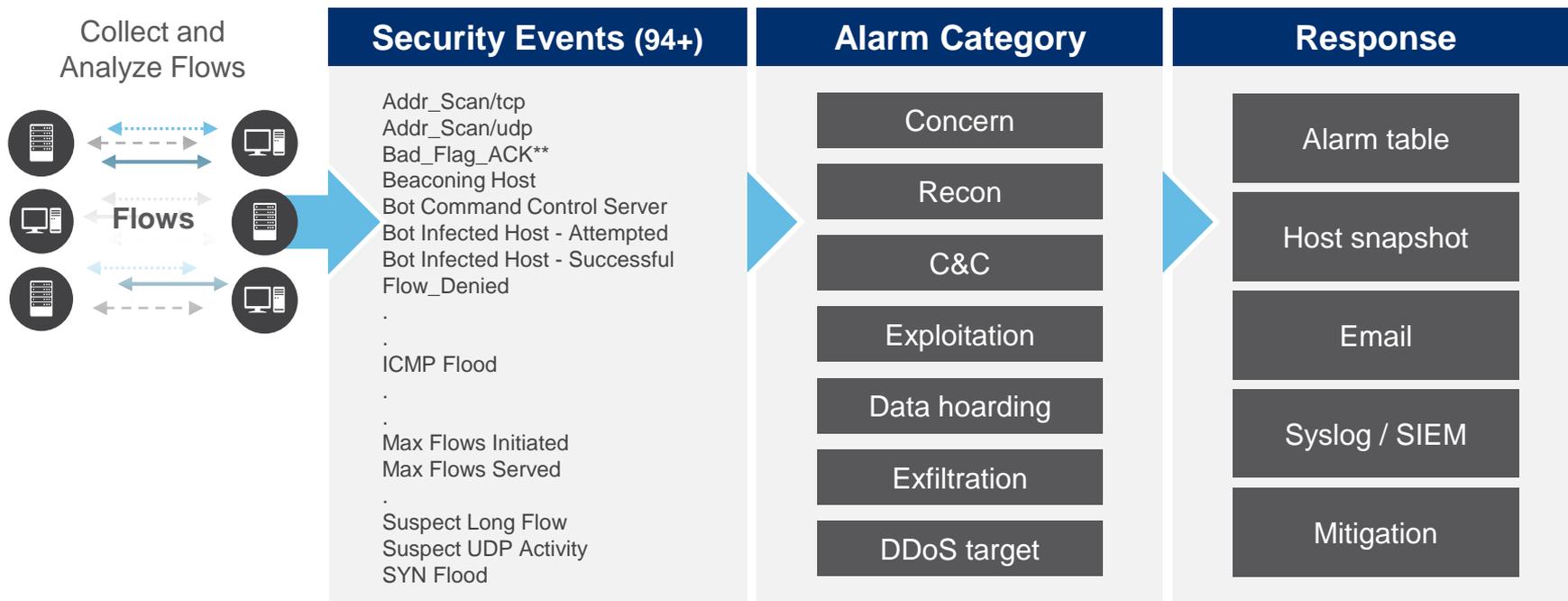
Respond

- Accelerate network troubleshooting and threat mitigation
- Respond quickly to threats
- Continuously improve enterprise security posture

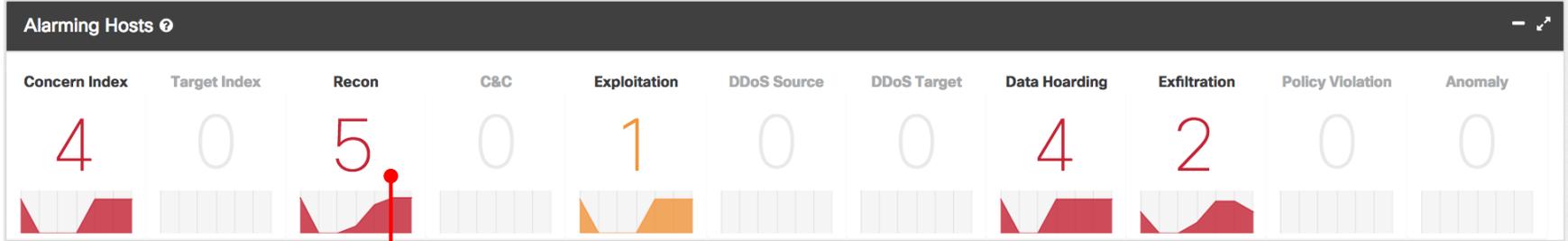
Detect Threats

Behavioral and Anomaly Detection Model

Behavioral Algorithms are Applied to Build “Security Events”



Stealthwatch Alarm Categories

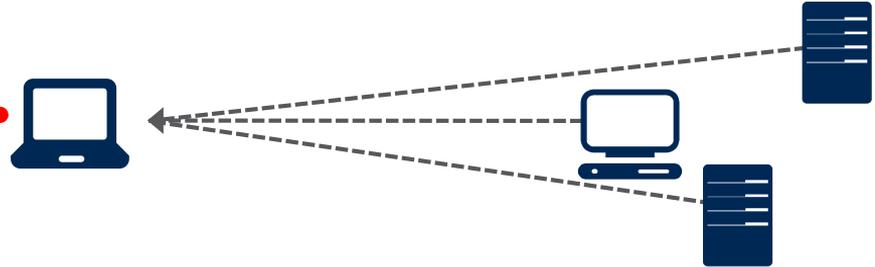


Each category accrues points

Example Algorithm: Data Hoarding

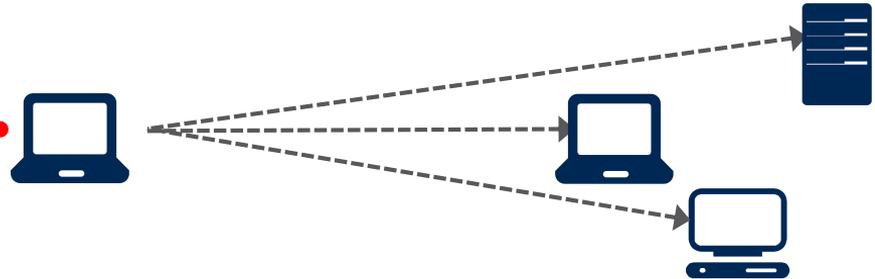
Suspect Data Hoarding

- 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

The screenshot displays a network monitoring interface with two main sections: Hosts and Alarms.

Hosts Table:

Host Address	Host Name	First Sent	Last Sent	CI	TI	RC	C&C	EP	DS	DT	DH	EX	PV	AN	Location	Host Groups
10.201.3.149	workstation-149.	11/16/16 6:35 PM	1/6/17 4:02 PM	193%		2,561%		1%			52,799%	5,499%			RFC 1918	End User Devices Desktops Atlanta Sales and Marketing
10.201.3.18	workstation-018.	11/16/16 6:51 PM	1/6/17 4:02 PM	88%		4,759%					16,799%				RFC 1918	End User Devices Desktops Atlanta Sales and Marketing

Alarm Dashboard: Data Hoarding (1) for Host 10.201.3.149

Alarms Table:

First Active	Source Host Groups	Source	Target Host Groups	Target	Policy	Event Alarms	Source User	Details
1/6/17 2:30 AM	End User Devices, Desktops, Atlanta, Sales and Marketing	10.201.3.149	--	Multiple Hosts	10.201.3.149	--	--	Observed 52,69M points. Un-baselined Host. Policy maximum allows up to 100k points.

Navigation: Previous | 1 | Next

Alarm Model

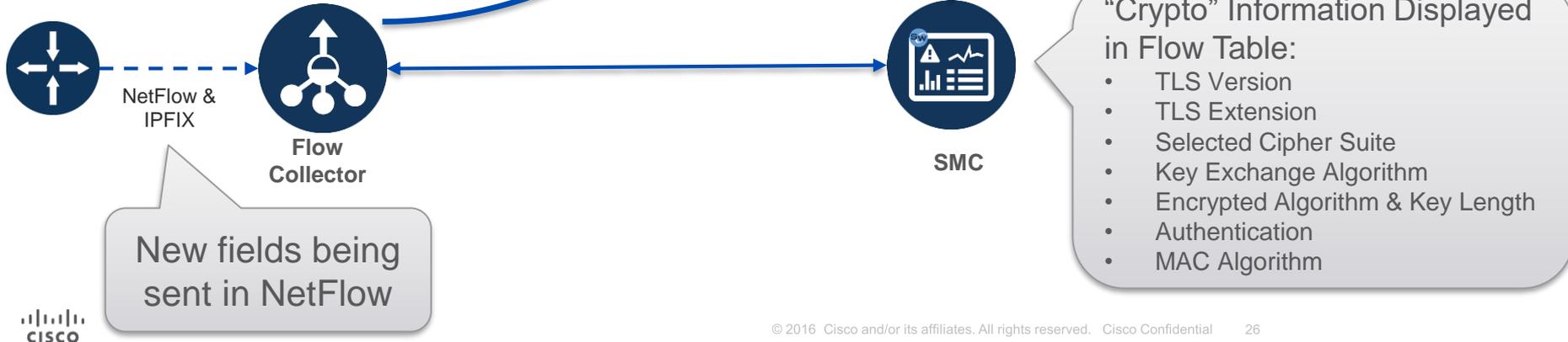
Monitor activity and alarm on suspicious conditions

Policy and behavioral

What does ETA Mean to Stealthwatch

Flow Collector parses and sends:

- Initial Data Packet(IDP),
- Sequence of Packet Lengths and Times (SPLT)
- Byte Distribution (BD)



Example “Crypto” Information in Flow Table

Stealthwatch

Search, User, Settings, Desktop Client

Dashboards Monitor Analyze Jobs Configure Deploy

Flow Search Results (8,196)

Save Search Save Results Start New Search

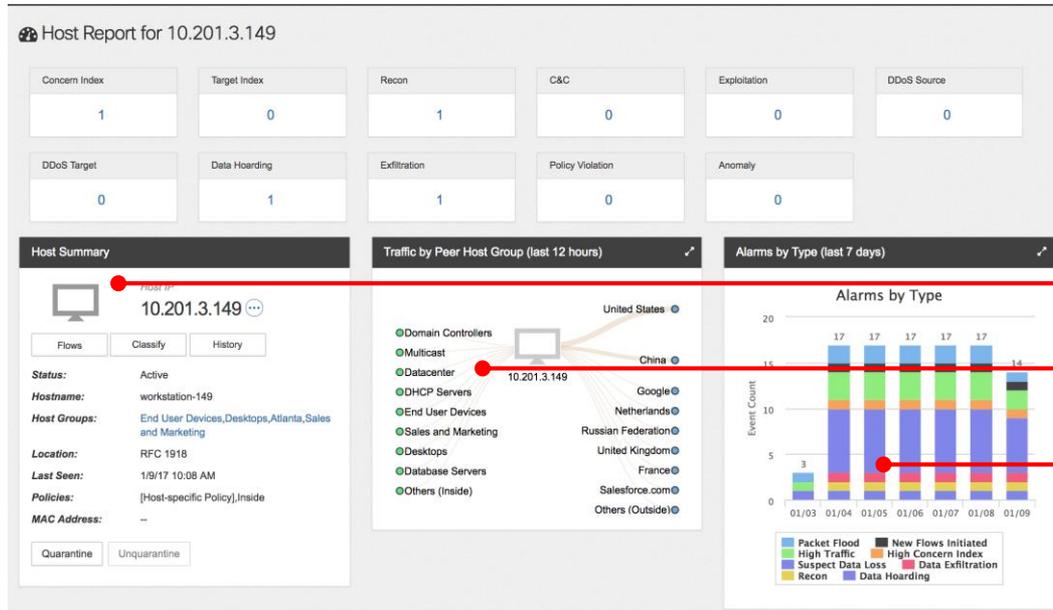
Edit Search Time Range: Last 2 Days 100% Complete Delete Search

Subject: Orientation: Either

START	DURATION	CONNECTION APPLICATION	CONNECTION BYTES	CONNECTION	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	0.0.40.10	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	0.0.40.10	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	0.0.40.10	443/TCP	Catch All	309.55K
▶ Apr 20, 2017 11:34:48 AM	13m 11s	HTTPS (unclassified)	626.72K		TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	0.0.40.10	443/TCP	Catch All	437.98K
▶ Apr 20, 2017 11:14:48 AM	19m 11s	HTTPS (unclassified)	871.41K		TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	0.0.40.10	443/TCP	Catch All	606.05K
▶ Apr 20, 2017 10:46:48 AM	27m 11s	HTTPS (unclassified)	1.21M		TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	0.0.40.10	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	0.0.40.10	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	0.0.40.10	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	0.0.40.10	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	0.0.40.10	443/TCP	Catch All	351.75K

Analyze Behavior

Investigating a Host

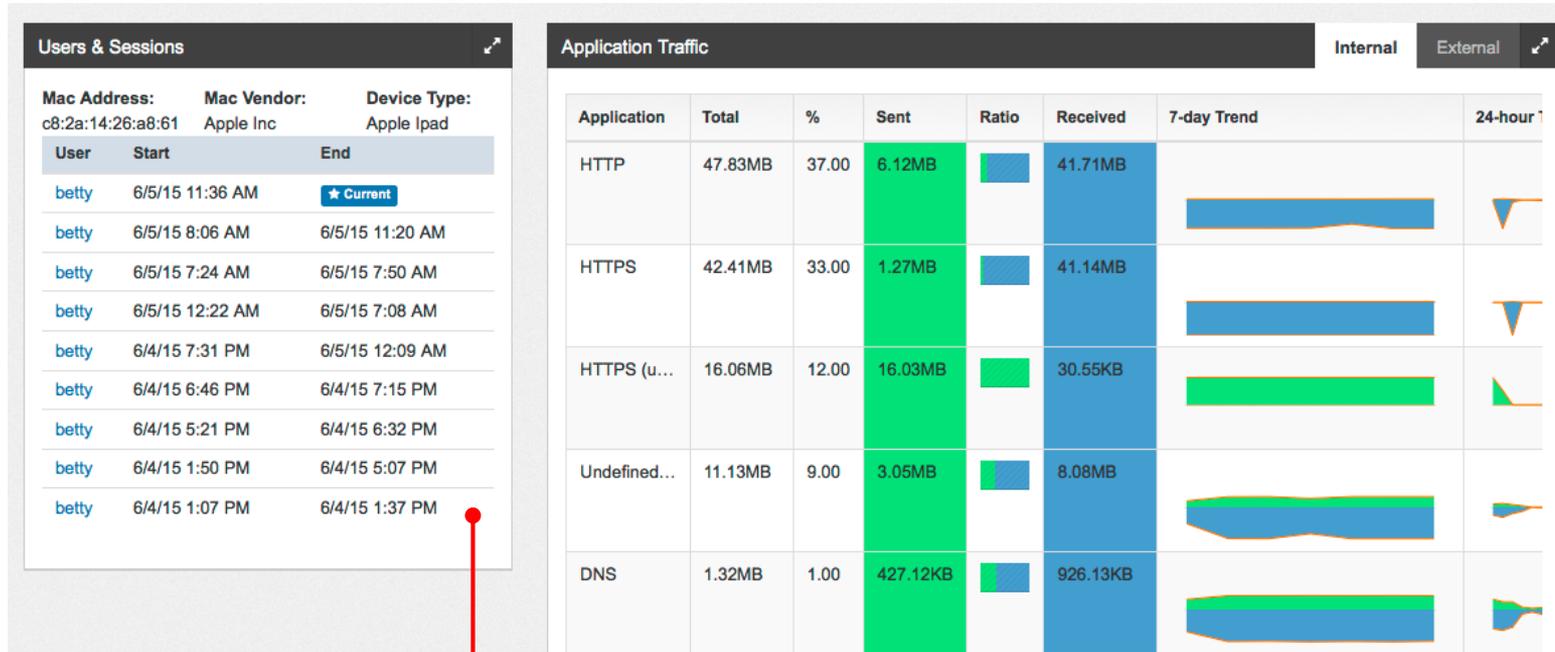


Summary of aggregated host information

Observed communication patterns

Historical alarming behavior

Investigating: Host Drill-Down



User information

Investigating: Applications

Application Traffic							
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		
authentic...	1.9MB	1.00	934.58KB		1014.67KB		
NFS	1.37MB	1.00	988.06KB		410.55KB		
SSDP	877.81KB	1.00	877.81KB		0B		

Observed applications, some suspicious

SMB (unc...	837.59KB	1.00	649.03KB		188.56KB		
LDAP (un...	781.12KB	1.00	396.55KB		384.58KB		
Kerberos ...	1.67MB	1.00	981.51KB		727.05KB		
DHCP	117.88KB	< 0.01	85.36KB		32.51KB		
ICMP	275.26KB	< 0.01	251.3KB		23.96KB		
NetBIOS	367.79KB	< 0.01	357.38KB		10.41KB		
HTTP (un...	534.73KB	< 0.01	509.64KB		25.09KB		
SSH/SCP...	46B	< 0.01	0B		46B		

Investigating: Audit Trails

Flow Search (40) Save Search Save Results Start New Search

Edit Search Time Range: Last 12 Hours 100% Complete Delete Search

Subject: 10.201.3.149 Orientation: Either

Connection: Direction: Total

Peer: Host Groups: Russian Federation

START	DURATION	SUBJECT IP ADDRESS	SUBJECT PORT/PROTOCOL	SUBJECT HOST GROUPS	SUBJECT BYTES	CONNECTION APPLICATION	CONNECTION BYTES	PEER IP ADDRESS	PEER PORT/PROTOCOL	PEER HOST GROUPS	PEER BYTES
▼ Jan 9, 2017 8:00:03 AM	6s	10.201.3.149 View URL Data	52319/TCP	End User Devices, Desktops, Atlanta, Sales and Marketing	715.25K	HTTP (unclassified)	1.4M	89.108.67.143 View URL Data	80/TCP	Russian Federation	715.25K
▶ Jan 9, 2017 9:51:10 AM	9s	10.201.3.149 View URL Data	53455/TCP	End User Devices, Desktops, Atlanta, Sales and Marketing	672.77K	HTTP (unclassified)	1.31M	89.108.67.143 View URL Data	80/TCP	Russian Federation	672.77K
▶ Jan 9,	10s	10.201.3.149	52458/TCP	End User	670.63K	HTTP	1.31M	89.108.67.143	80/TCP	Russian	670.63K

Search Subject Details

Packets: 562
Packet Rate: 93.67pps
Bytes: 715.25KB
Byte Rate: 122.07Kbps
Percent Transfer: 50.00%
Host Groups: End User Devices, Desktops, Atlanta, Sales and Marketing

Totals

Packets: 1.12K
Packet Rate: 187.33pps
Bytes: 1.4MB
Byte Rate: 244.14Kbps
Subject Byte Ratio: 50.00%
RTT: --
SRT: --

Peer Details

Packets: 562
Packet Rate: 93.67pps
Bytes: 715.25KB
Byte Rate: 122.07Kbps
Percent Transfer: 50.00%
Host Groups: Russian Federation

Network behavior retroactively analyzed

Extrapolating to a User

The screenshot shows a user profile for 'ethel'. The page is divided into several sections:

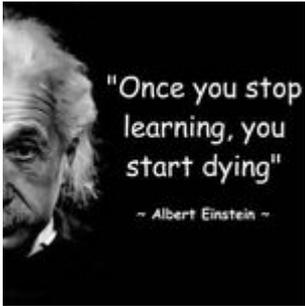
- Username:** 'ethel' is displayed at the top left.
- View flows:** A 'View Flows' button is located in the 'Actions' menu.
- Active Directory details:** A profile card shows a placeholder for a user photo and a list of icons representing Active Directory attributes.
- Devices and sessions:** A table lists active sessions for two different MAC addresses.

Annotations with red lines point to these specific elements:

- Username
- View flows
- Active Directory details
- Devices and sessions

Devices and Sessions							
Mac Address: 147d:c5:bf:34:85		Mac Vendor: Unknown		Device Type: Unknown			
Host	Name	Group	Location	Count	Start	End	
10.201.3.78	--	Sales and Marketing Atlanta Desktops	RFC 1918	5	1/11/15 10:25 PM		★ Current
Mac Address: 00:26:b0:ca:f2:a9		Mac Vendor: Unknown		Device Type: Unknown			
Host	Name	Group	Location	Count	Start	End	
10.202.1.151	--	Atlanta Sales and Marketing Desktops	RFC 1918	5	1/11/15 10:11 PM	1/11/15 10:21 PM	

Continuous Learning and Optimization



- Cisco Stealthwatch has Advanced Service for Fine-Tuning and Optimization service to protect customer's investment.



Summary

- Phát hiện tấn công theo hành vi ngày càng quan trọng, nhất là với tấn công **APT, Zero-day, nội gián**.
- Điểm yếu chính của phát hiện tấn công theo hành vi là lượng Báo động giả lớn.
- Với mỗi giải pháp thực tế, cần chú ý:
 - **Thông tin đầu vào** là gì? “Giàu” hay “nghèo”?
 - **Khả năng xử lý** nhiều hay ít, nhanh hay chậm?
 - Khả năng **hiệu chỉnh, học liên tục** để giảm báo động giả.
- **Stealthwatch** là phát hiện tấn công theo hành vi
 - Dựa vào **thông tin kết nối** do thiết bị mạng, thiết bị ATTT, đầu cuối cung cấp
 - Phương pháp **phát hiện tấn công** theo bất thường dựa trên thống kê
 - Xây dựng **hành vi “chuẩn” tự động** theo thời gian và/hoặc có trợ giúp của admin



