


Behavior-Based Intrusion Detection - Theory and Implementation

Trinh Ngoc Minh
Ph.D, CISSP
Security Solution Consultant – Cisco Systems Vietnam
Hanoi July 2017

REQUIRED

Agenda

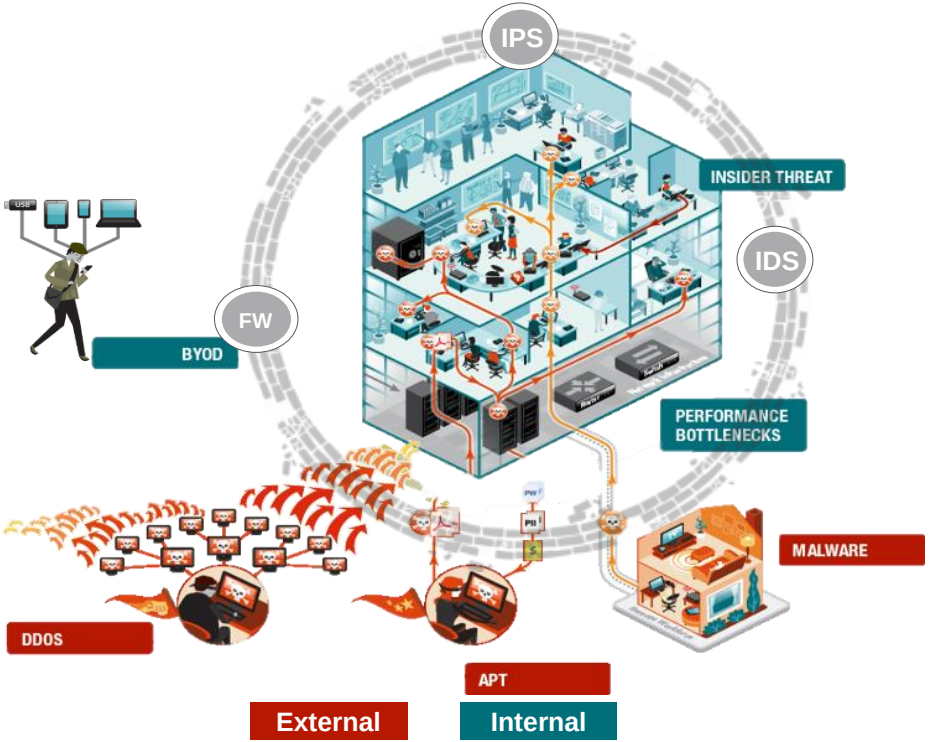
1. Threat Landscape and Today's Security Challenges
2. Behavior-based Intrusion Detection Approach
3. StealthWatch: Behavior-based Intrusion Detection System basing on Network Communication Data

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:

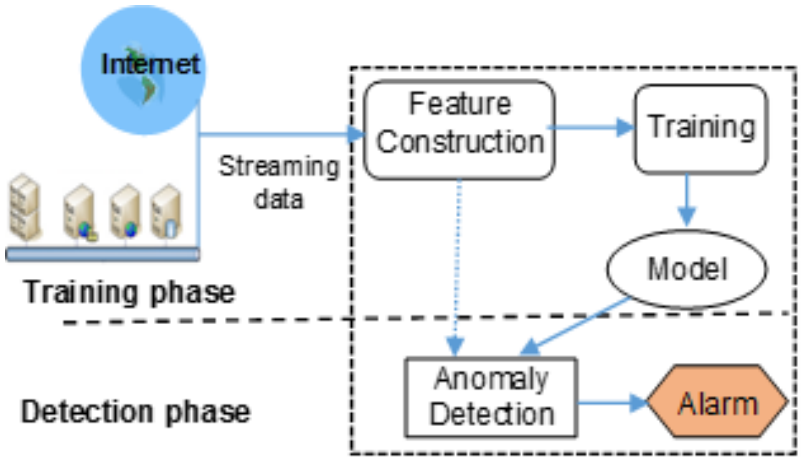
- Employees who intentionally expose data

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

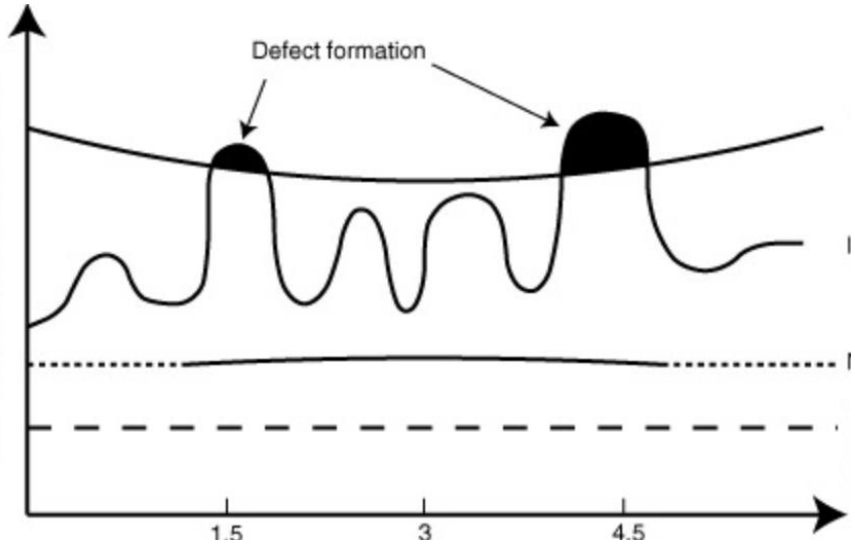
Information theory

Clustering

Classification

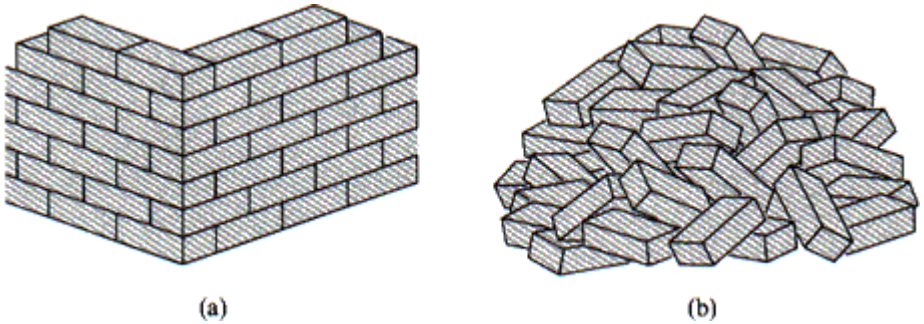
Statistical

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



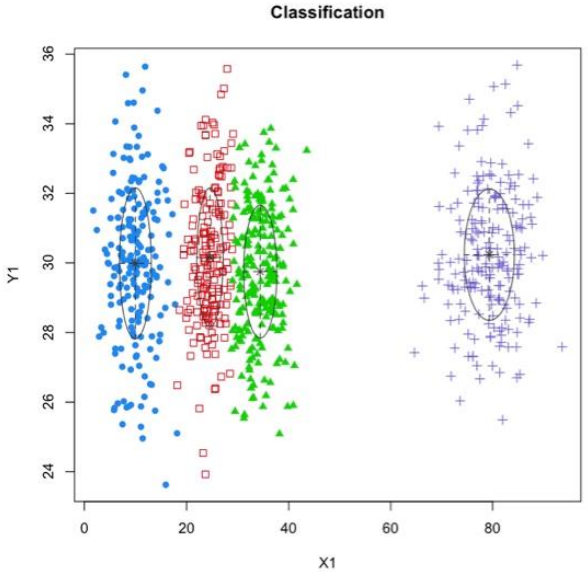
Information Theory

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



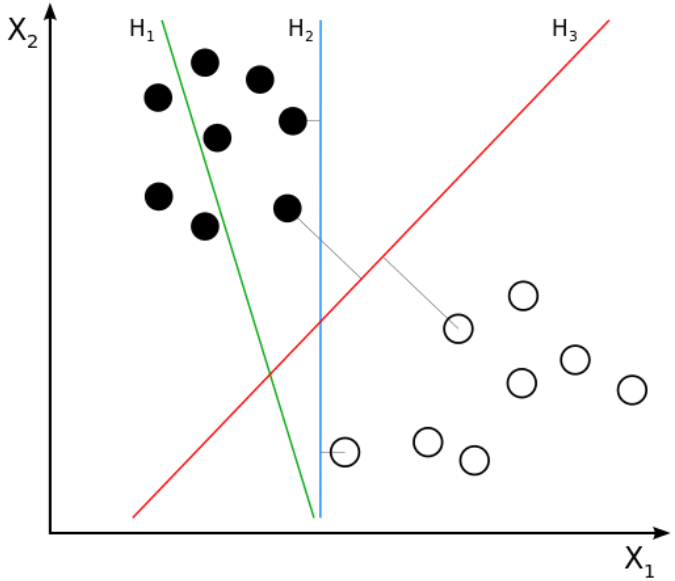
Clustering

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.

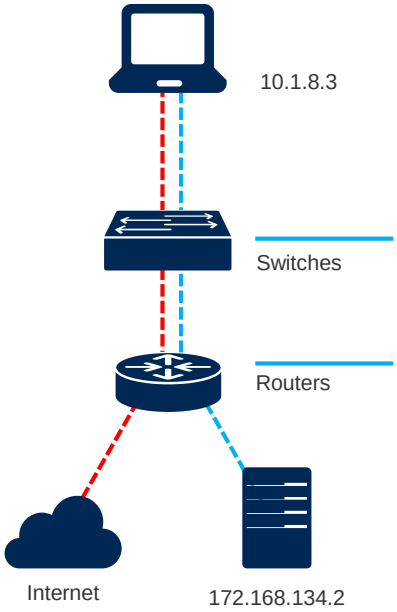
Behavior-based IDS basing on Network Communication Data

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

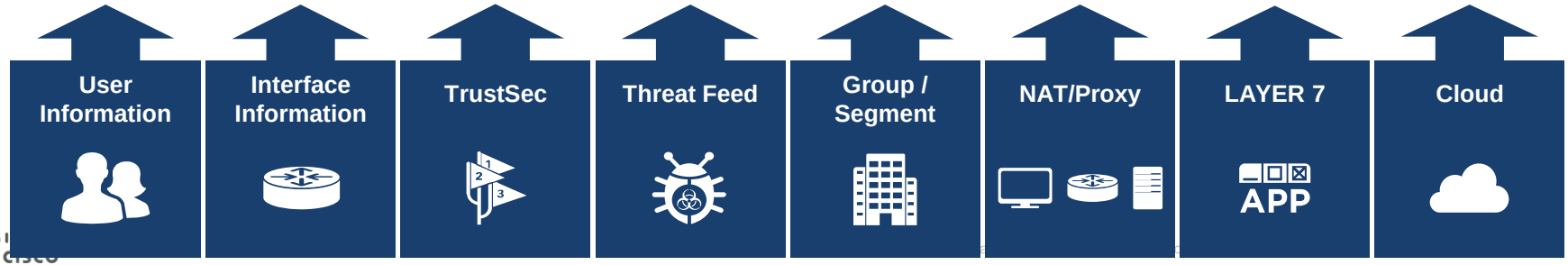
Event Data

Security Events Behavioral Analytics

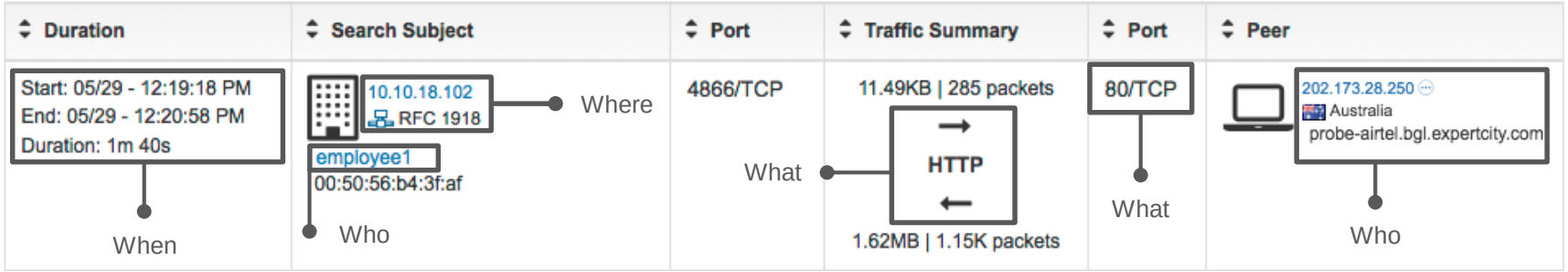
Session Data | *100% network accountability*

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

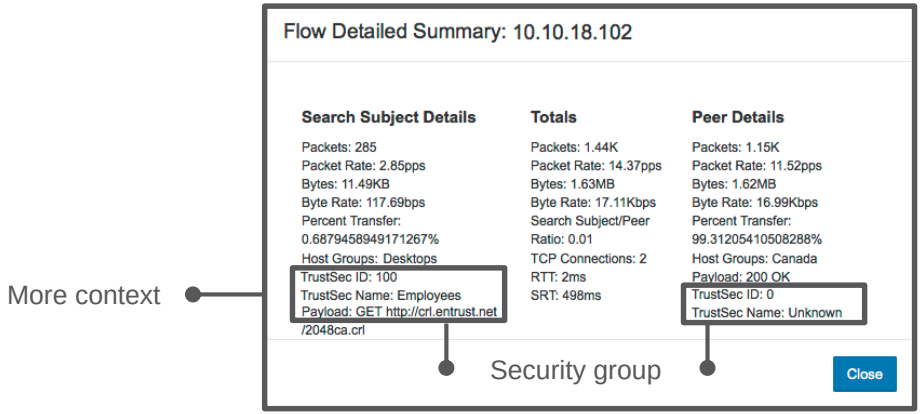
Visibility



The General Ledger



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



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

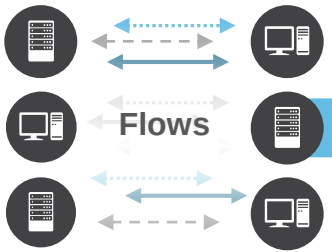
- Accelerate network troubleshooting and threat mitigation
- Respond quickly to threats
- Continuously improve enterprise security posture

Detect Threats

Behavioral and Anomaly Detection Model

Behavioral Algorithms are Applied to Build “Security Events”

Collect and Analyze Flows



Security Events (94+)

Addr_Scan/tcp
Addr_Scan/udp
Bad_Flag_ACK**
Beaconing Host
Bot Command Control Server
Bot Infected Host - Attempted
Bot Infected Host - Successful
Flow_Denied
.
.
ICMP Flood
.
.
Max Flows Initiated
Max Flows Served
.
Suspect Long Flow
Suspect UDP Activity
SYN Flood

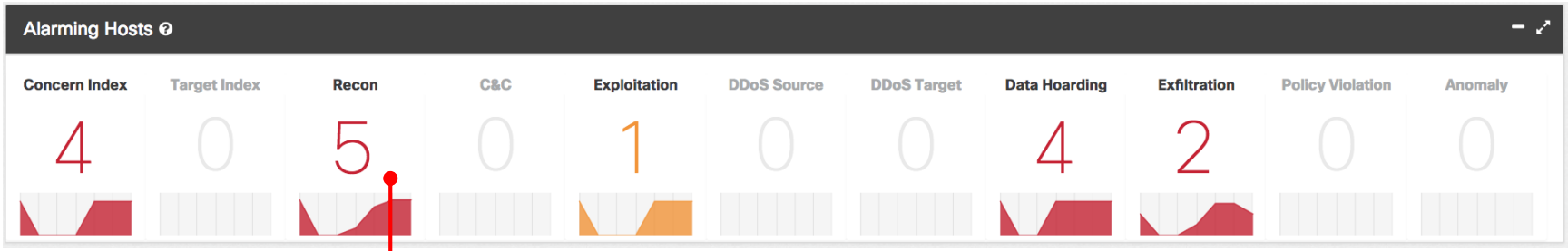
Alarm Category

- Concern
- Recon
- C&C
- Exploitation
- Data hoarding
- Exfiltration
- DDoS target

Response

- Alarm table
- Host snapshot
- Email
- Syslog / SIEM
- Mitigation

Stealthwatch Alarm Categories

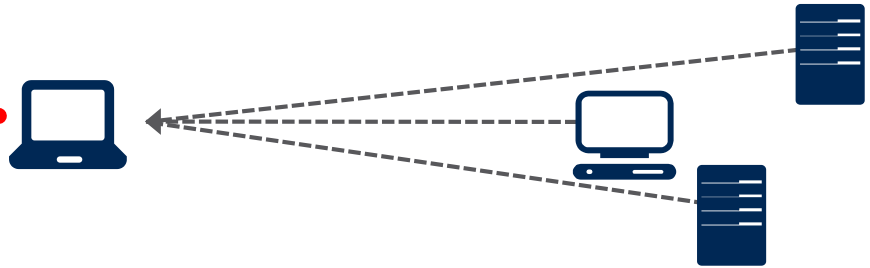


Each category accrues points

Example Algorithm: Data Hoarding

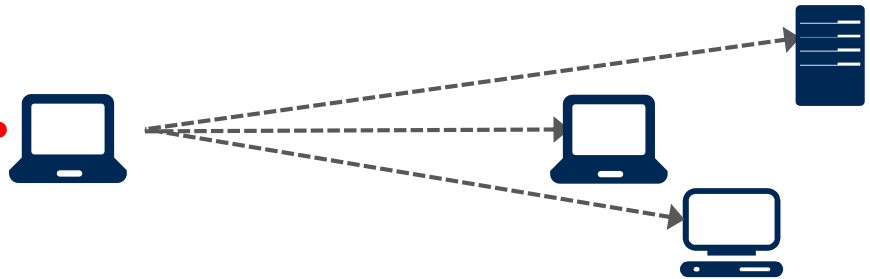
Suspect Data Hoarding

- **Unusually large amount** of data inbound from other hosts

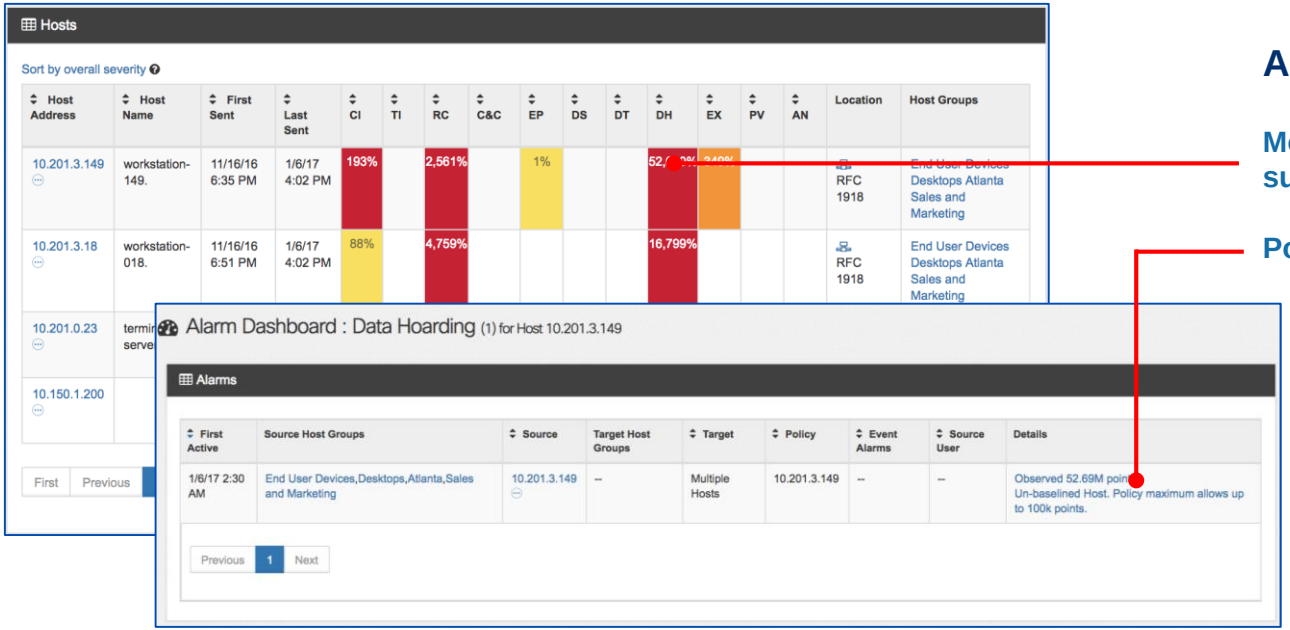


Target Data Hoarding

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



Network Behavior and Anomaly Detection



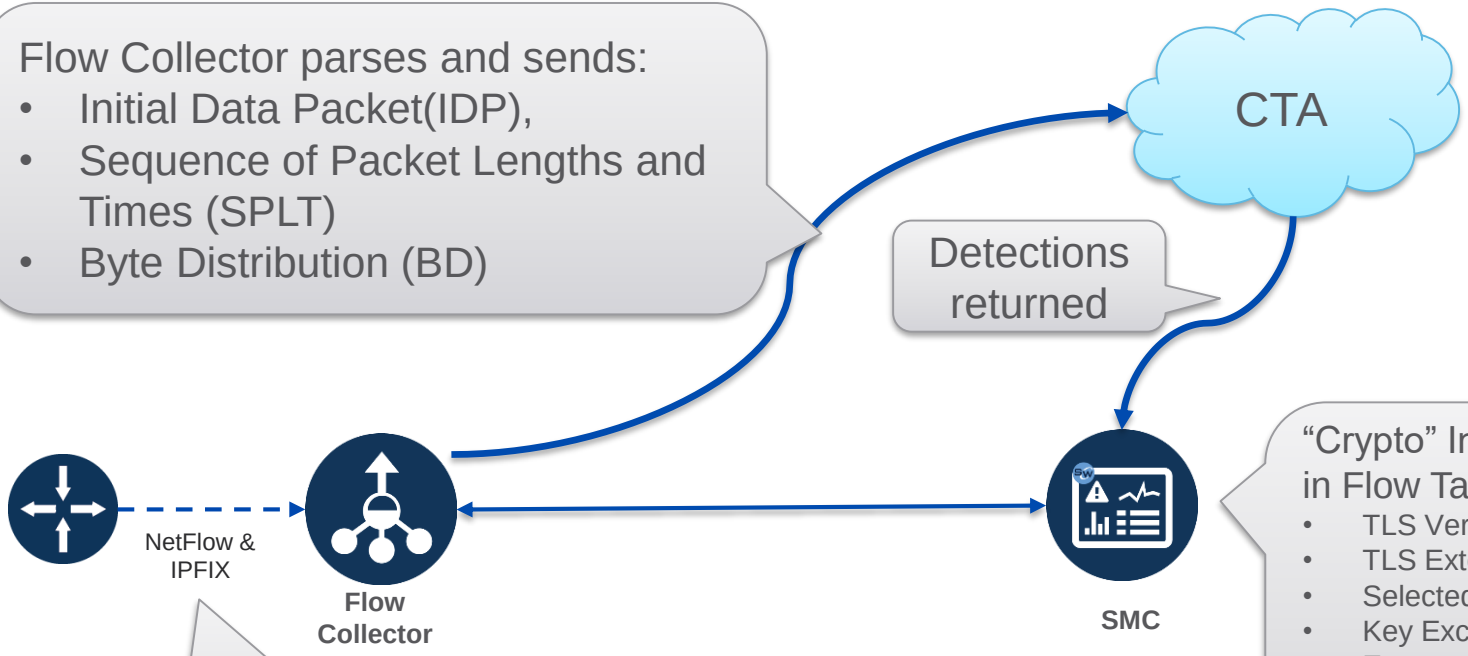
Alarm Model

Monitor activity and alarm on suspicious conditions

Policy and behavioral

What does ETA Mean to Stealthwatch

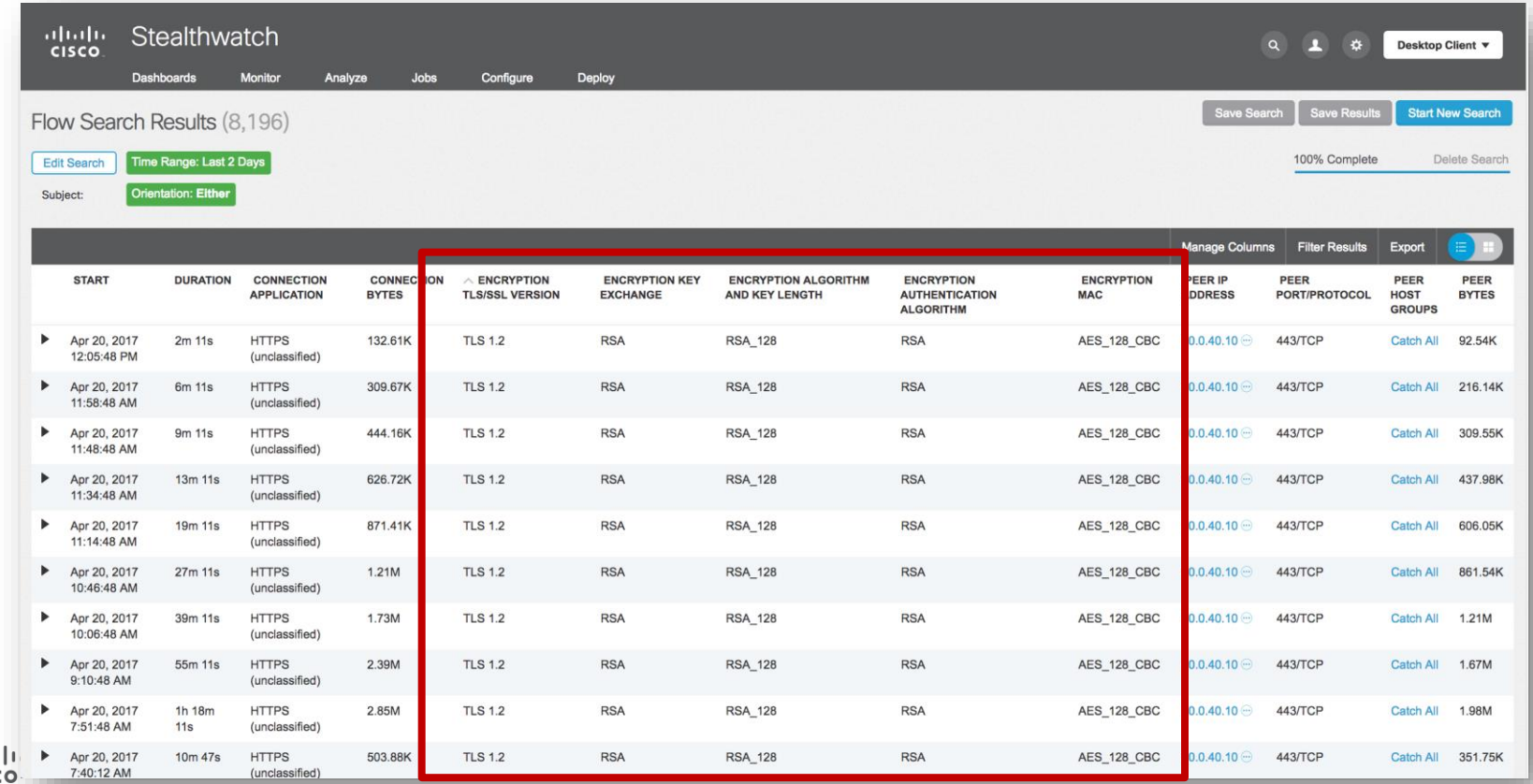
Flow Collector parses and sends:
- Initial Data Packet(IDP),
- Sequence of Packet Lengths and Times (SPLT)
- Byte Distribution (BD)



"Crypto" Information Displayed in Flow Table:
- TLS Version
- TLS Extension
- Selected Cipher Suite
- Key Exchange Algorithm
- Encrypted Algorithm & Key Length
- Authentication
- MAC Algorithm

New fields being sent in NetFlow

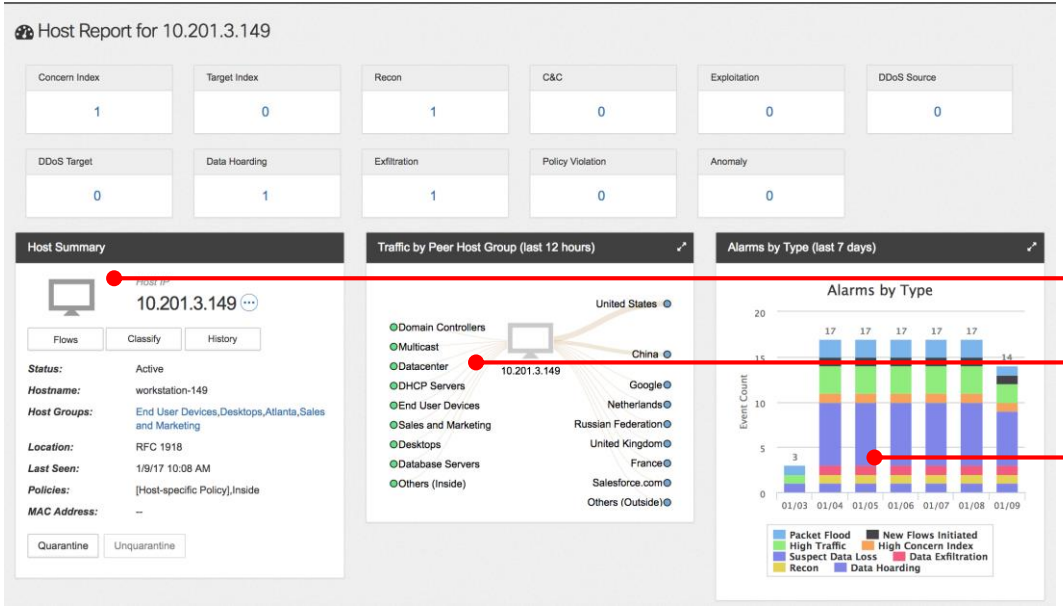
Example “Crypto” Information in Flow Table



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	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

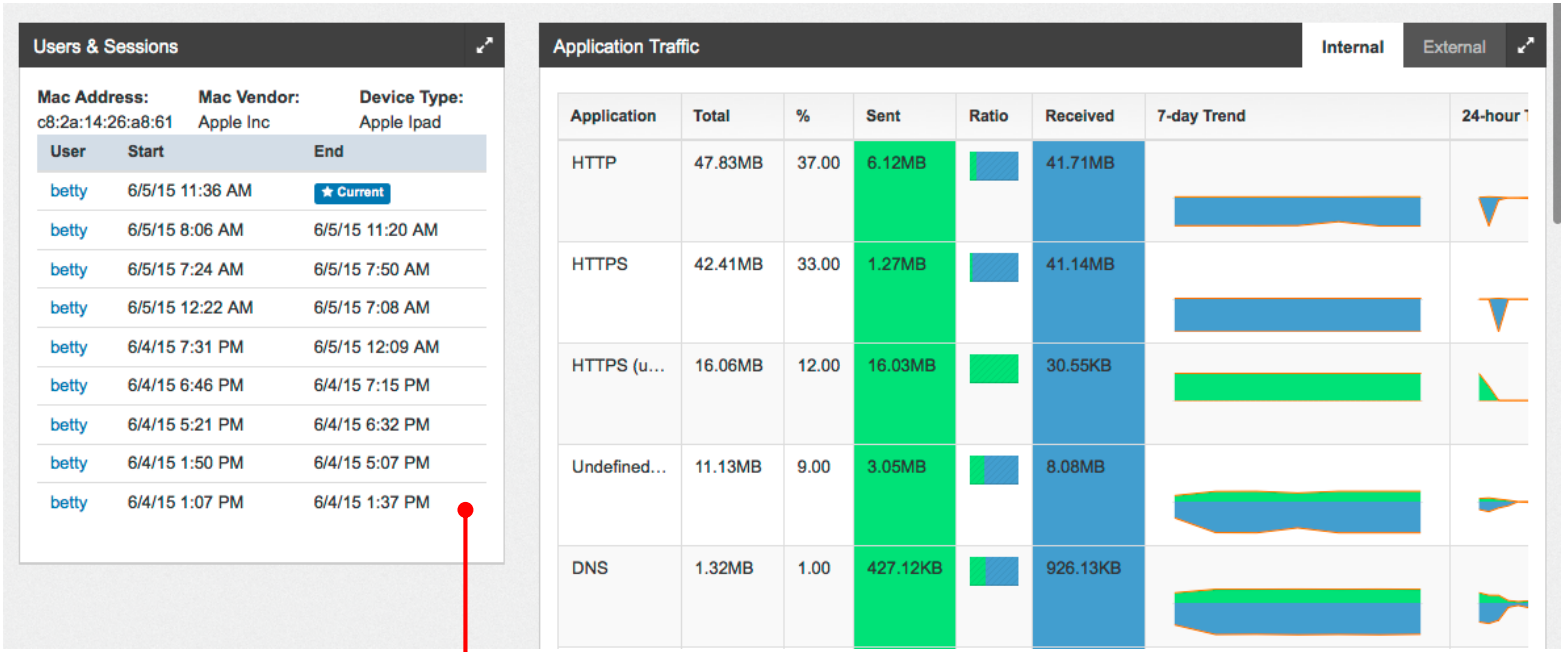


Summary of aggregated host information

Observed communication patterns

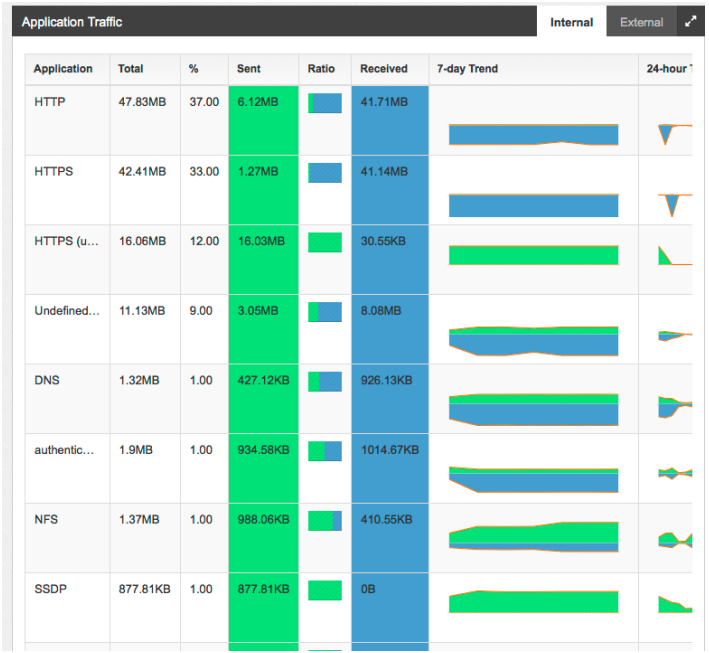
Historical alarming behavior

Investigating: Host Drill-Down

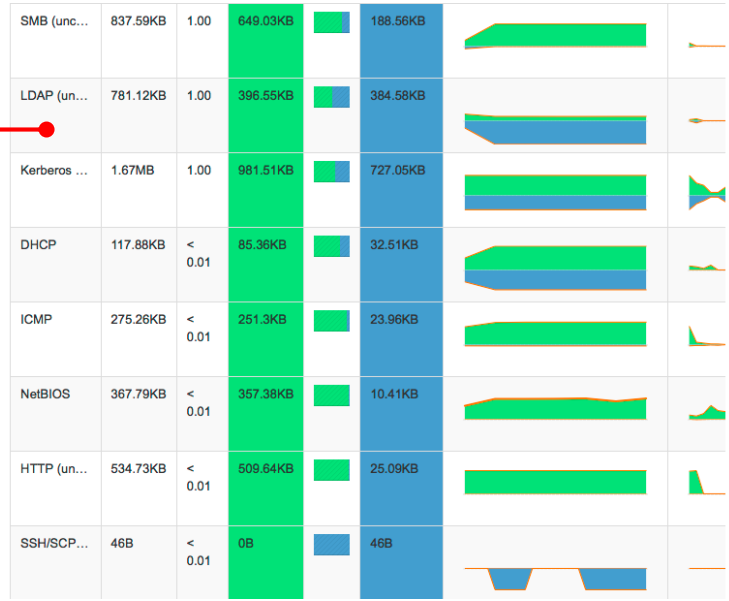


User information

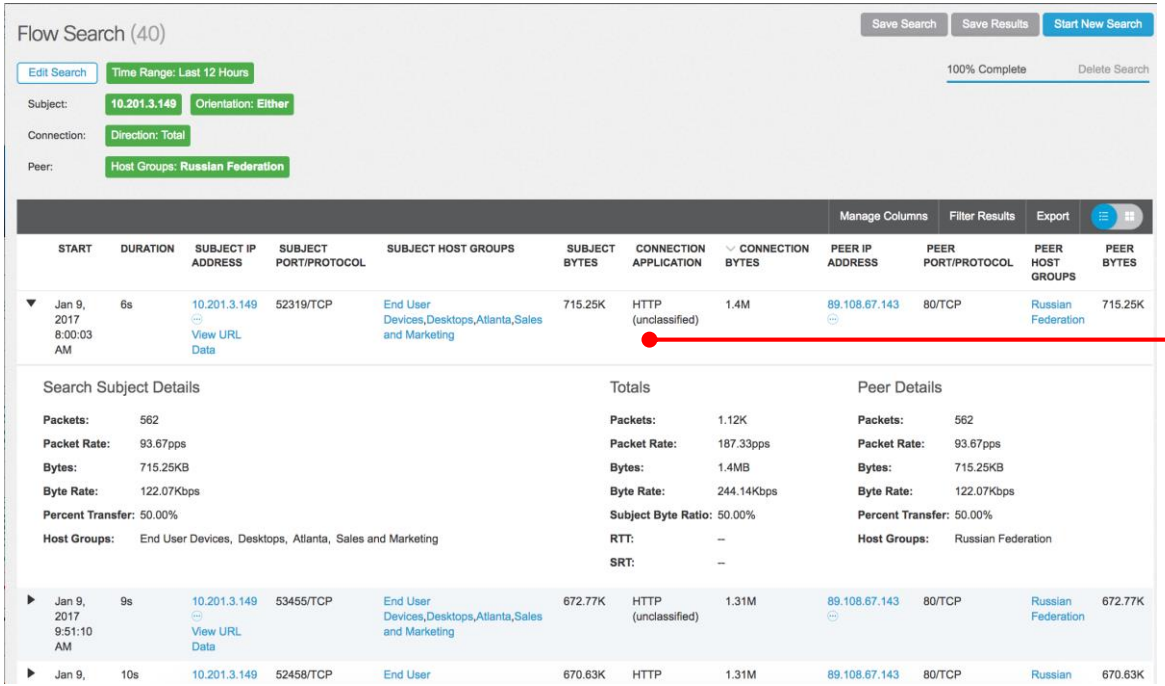
Investigating: Applications



Observed applications, some suspicious

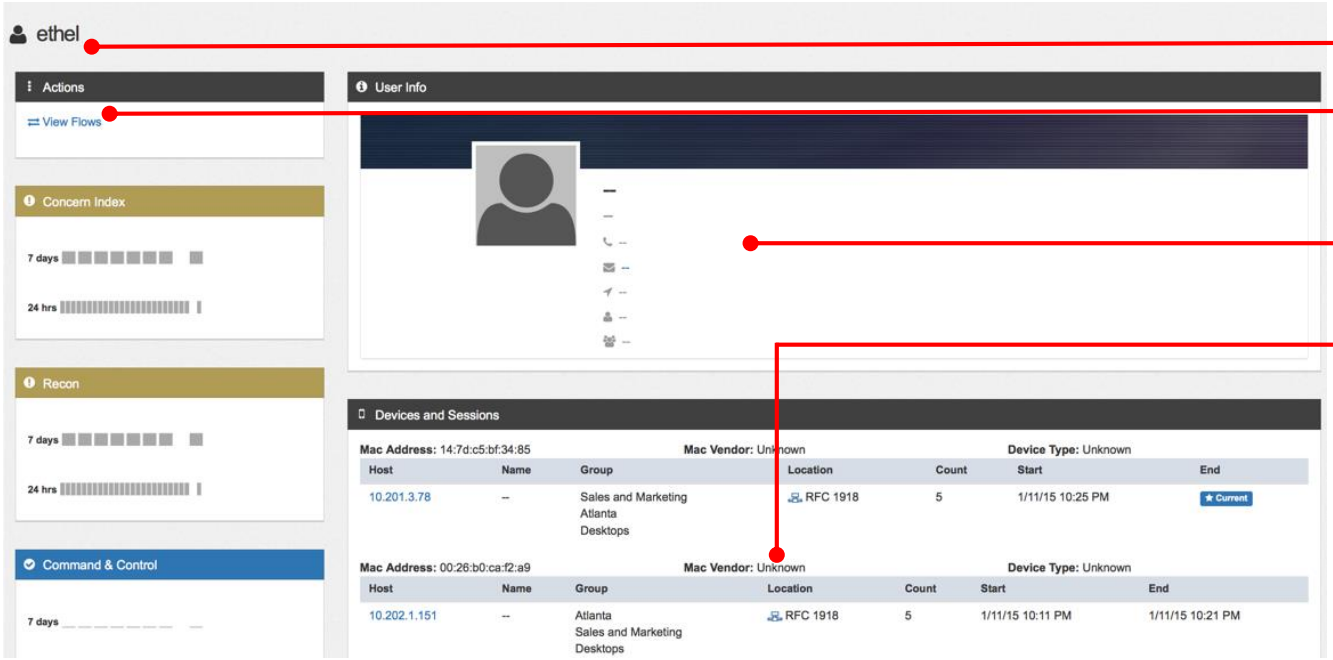


Investigating: Audit Trails



Network behavior retroactively analyzed

Extrapolating to a User



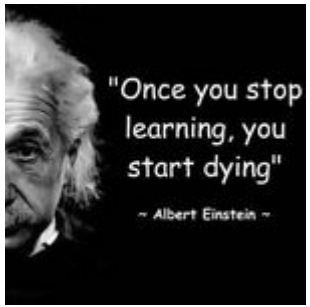
Username

View flows

Active Directory details

Devices and sessions

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