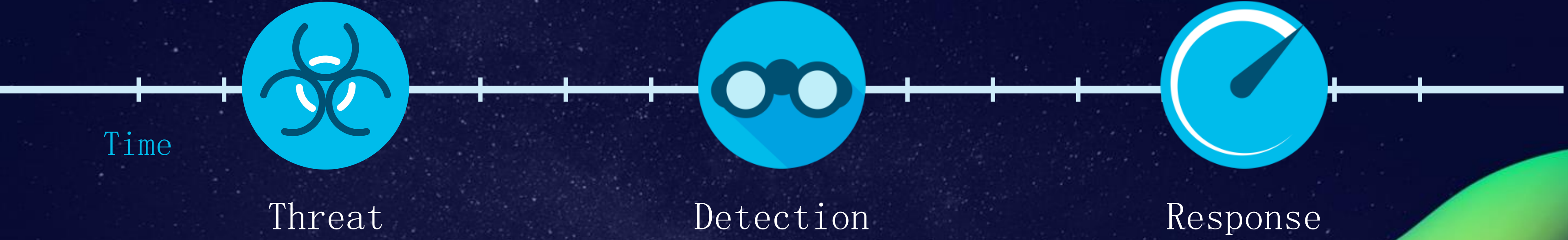
Security for the 21st Century

Jeff Reed JeffReed415 | Cisco Senior Vice President, Security Business

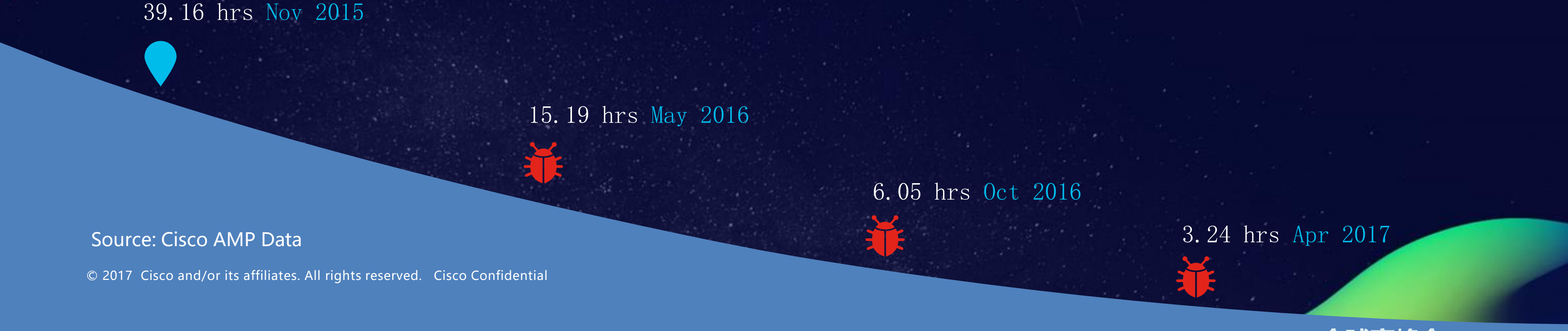
Are we secure?

Do you have an effective security posture?



Going in the right direction: TTD decreasing

TTD declined 11.95 hours from May 2016 through April 2017



39.16 hrs Nov 2015

15.19 hrs May 2016

6.05 hrs Oct 2016

3.24 hrs Apr 2017

Source: Cisco AMP Data

Key concerns for an effective security posture

How do you stop threats at the edge?

How do you control who gets onto your network?

How do you find and contain problems fast?

How do you protect users wherever they work?

How do you simplify network segmentation?

Secure Multicloud

How do you find and contain problems fast?

Stealthwatch + Stealthwatch Cloud

Encrypted Traffic Analytics (ETA)

The power of Cisco networking + security unleashed

Malware in Encrypted Traffic

ETA algorithms analyze multiple network data sources

Security AND Privacy

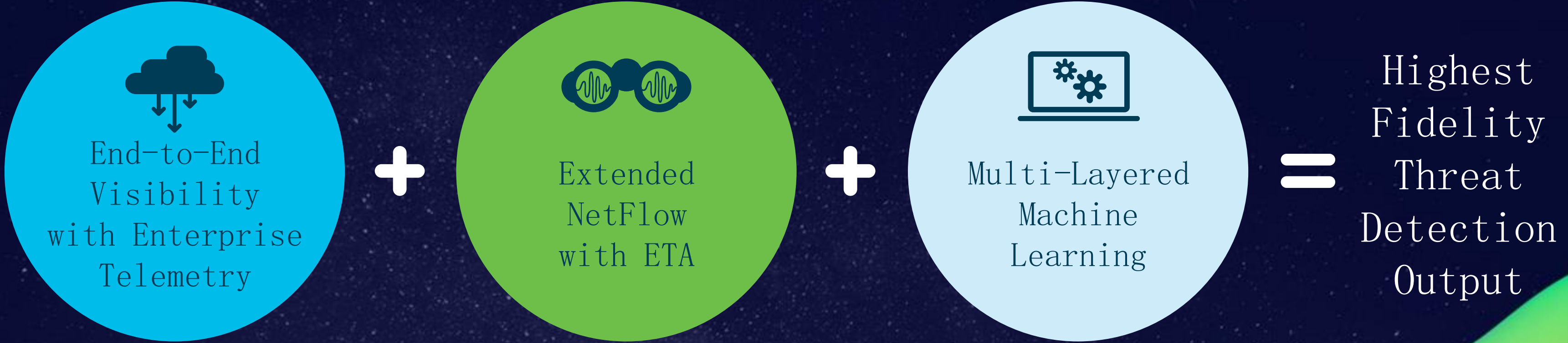
No information is decrypted

Detection Accuracy

Prioritized high accuracy findings

How do you find and contain problems fast?

The role of AI and Analytics in Advanced Threat Detection



End-to-End Visibility with Enterprise Telemetry

+

Extended NetFlow with ETA

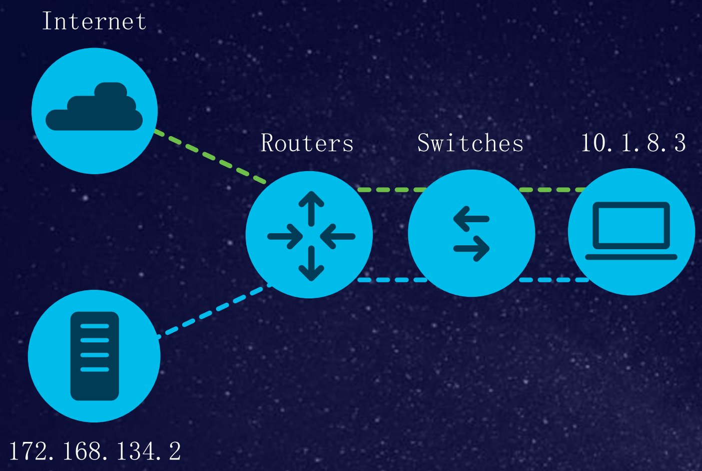
+

Multi-Layered Machine Learning

=

Highest Fidelity Threat Detection Output

Visibility through NetFlow

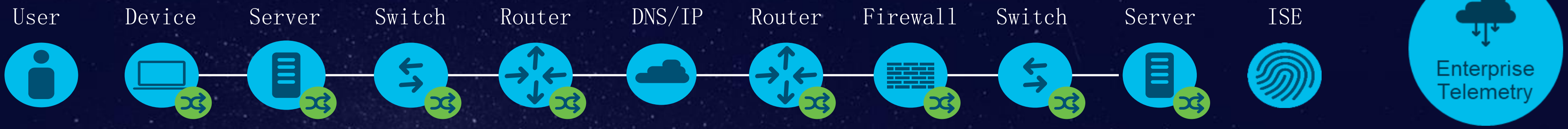


Flow Information	Packets
SOURCE ADDRESS	10. 1. 8. 3
DESTINATION ADDRESS	172. 168. 134. 2
SOURCE PORT	47321
DESTINATION PORT	443
INTERFACE	Gi0/0/0
IP TOS	0x00
IP PROTOCOL	6
NEXT HOP	172. 168. 25. 1
TCP FLAGS	0x1A
SOURCE SGT	100
:	:
APPLICATION NAME	NBAR SECURE-HTTP

Enterprise Telemetry

全球高峰会

End-to-end visibility



User Device Server Switch Router DNS/IP Router Firewall Switch Server ISE

Enterprise Telemetry

Web	Web Security Appliance (WSA)	
Endpoint	AnyConnect	
Data Center	Nexus switch	Tetration
Policy and User Info	Cisco Identity Services Engine (ISE), Cloudlock	

Router	ISR	CSR	ASR	WLC
Switch	Catalyst	IE	ETA enabled catalyst	
Firewall	ASA	FTD	Meraki	
Other	Stealthwatch Flow Sensor, Umbrella			

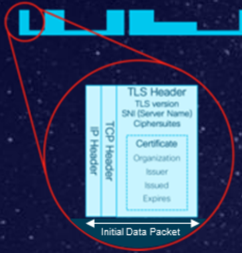
Stealthwatch Enterprise also enables telemetry ingestion from many third-party exporters

How can we inspect encrypted traffic?

ETA

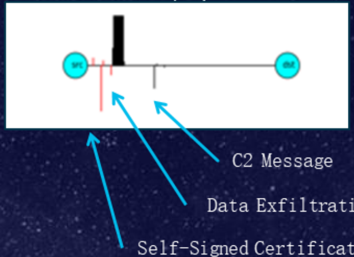
Initial Data Packet

Make the most of
the unencrypted fields



Sequence of Packet Lengths and Times

Identify the content type
through the size and timing of



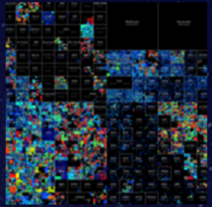
C2 Message

Data Exfiltration

Self-Signed Certificate

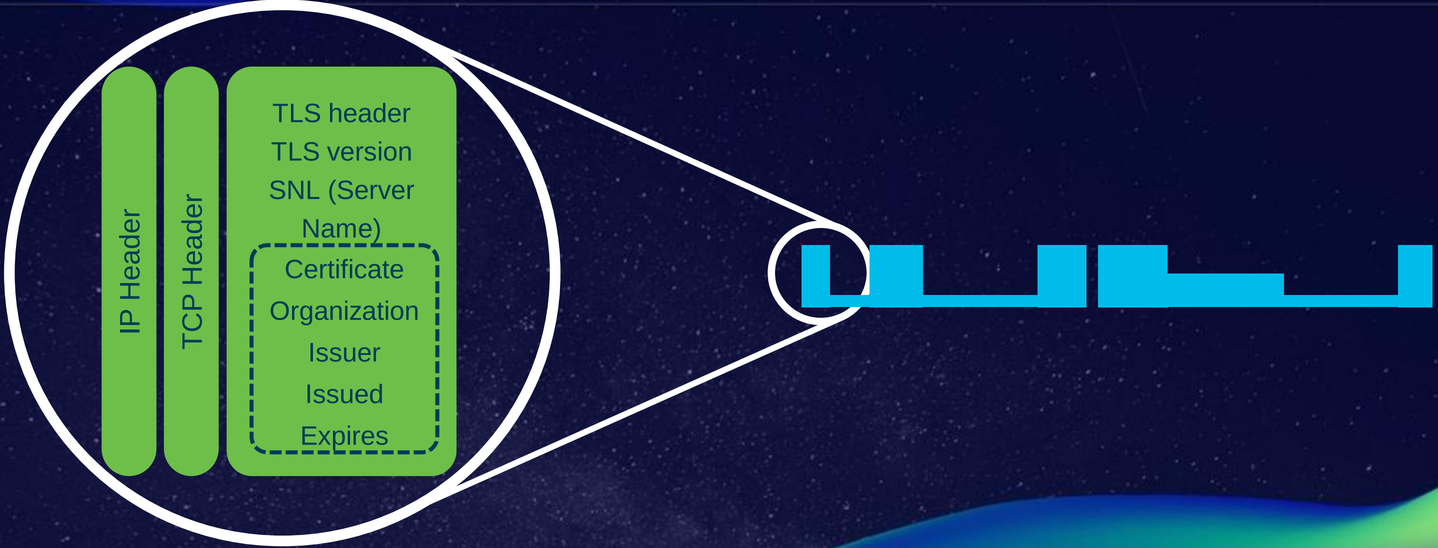
Global Risk Map

Who’s who of the
Internet’s dark side



Broad behavioral information
about the servers on the
Internet.

Initial Data Packet (IDP)



IP Header

TCP Header

TLS header

TLS version

SNL (Server Name)

Certificate

Organization

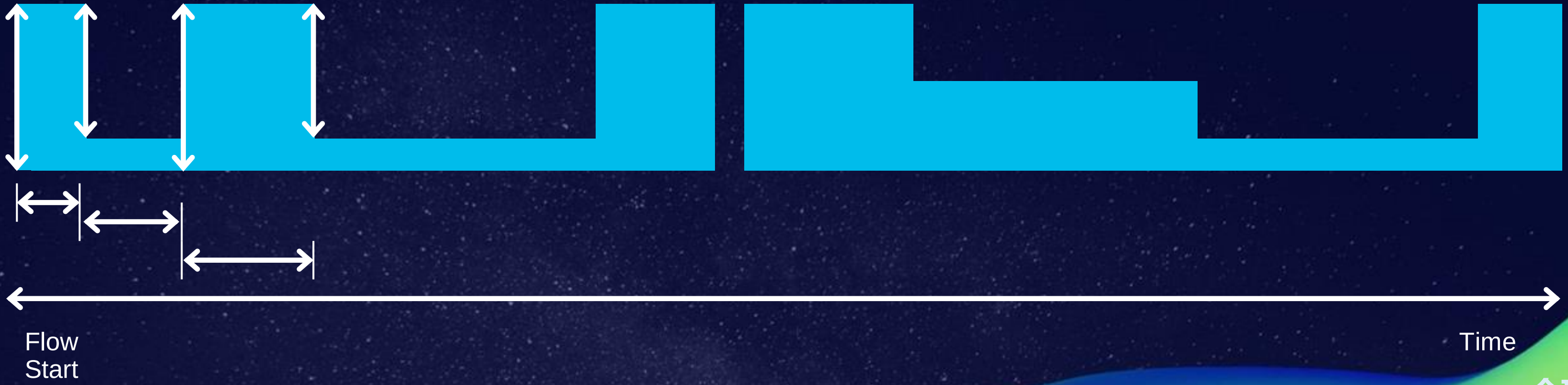
Issuer

Issued

Expires

ETA

Sequence of Packet Lengths and Time (SPLT)

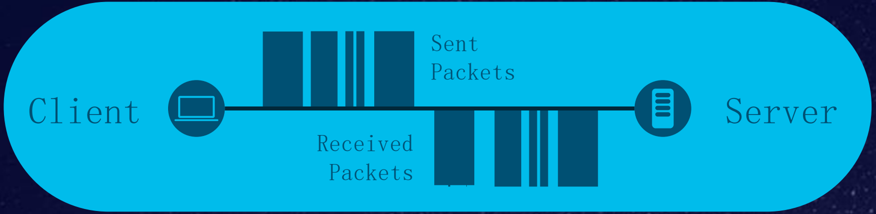


ETA

全球高峰会

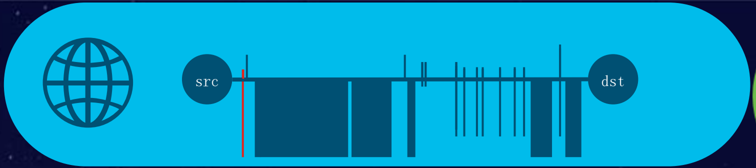
SPLT shows TLS metadata differences

Model



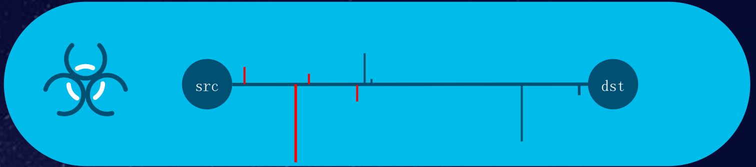
Packet lengths, arrival times and durations tend to be inherently different for malware than benign traffic.

Google Search Page Download

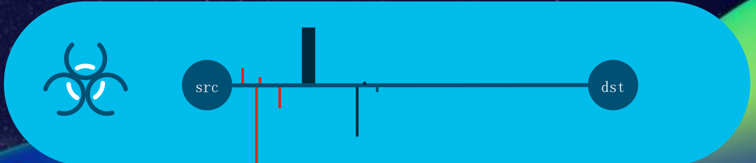


ETA

Initiate Command and Control



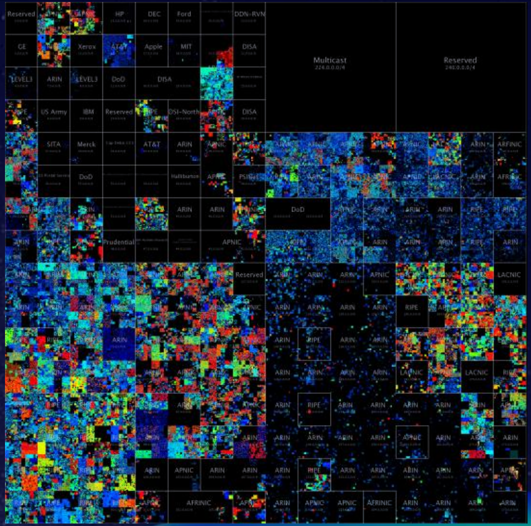
Exfiltration and Keylogging



Global Risk Map

- Behavioral statistics for millions of servers on the Internet
- Tracking servers likely becoming part of an attack
- Risk profiling

Image: http://census2012.sourceforge.net/images.html



The power of multi-layer machine learning

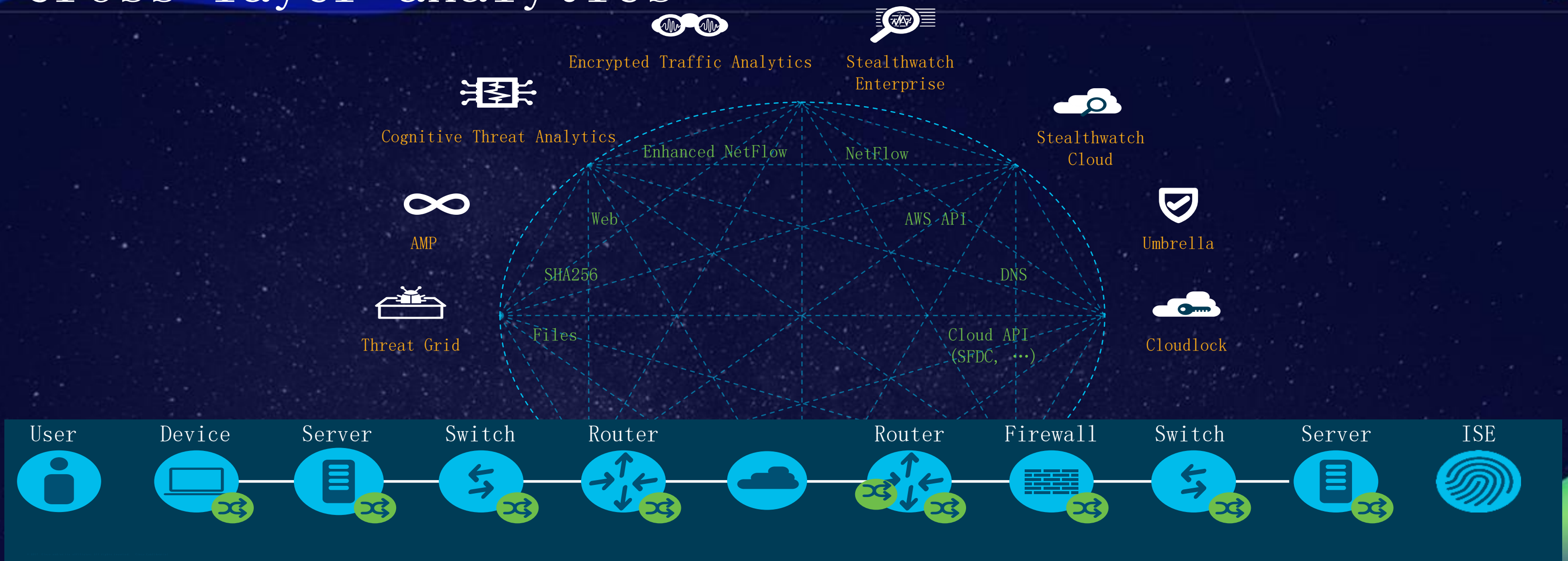
Machine Learning

Extended Visibility and Behavioral Analytics

Advanced Threat Detection

Encrypted Traffic Analytics

Cross-layer analytics



Encrypted Traffic Analytics

Stealthwatch Enterprise

Cognitive Threat Analytics

Enhanced NetFlow

NetFlow

Stealthwatch Cloud

AMP

Web

AWS API

Umbrella

SHA256

DNS

Threat Grid

Files

Cloud API (SFDC, …)

Cloudlock

User

Device

Server

Switch

Router

Router

Firewall

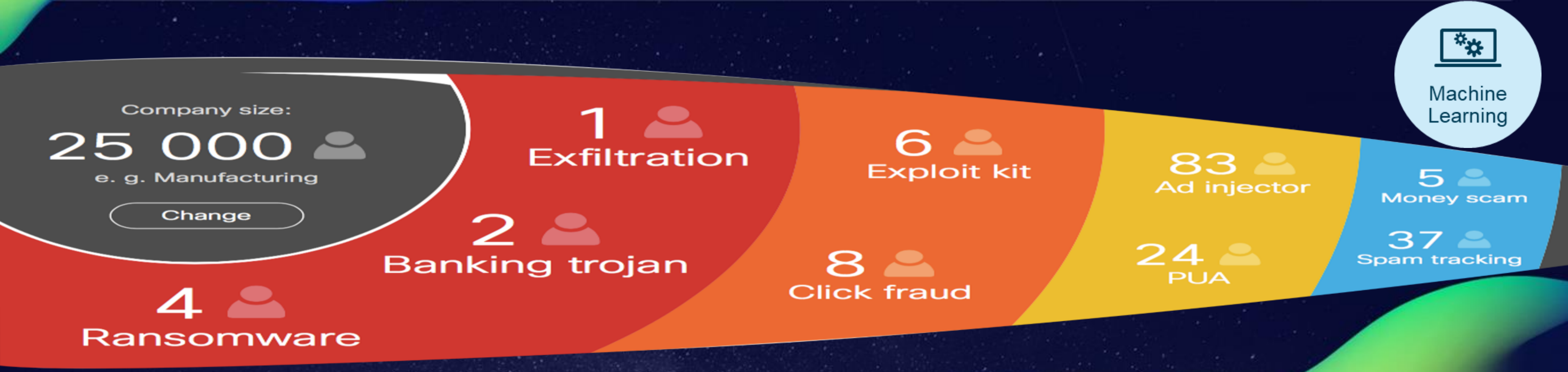
Switch

Server

ISE

Machine Learning

Threat visibility gap: 1% devices infected



Company size:

25 000

e. g. Manufacturing

Change

1 Exfiltration

2 Banking trojan

4 Ransomware

6 Exploit kit

8 Click fraud

83 Ad injector

24 PUA

5 Money scam

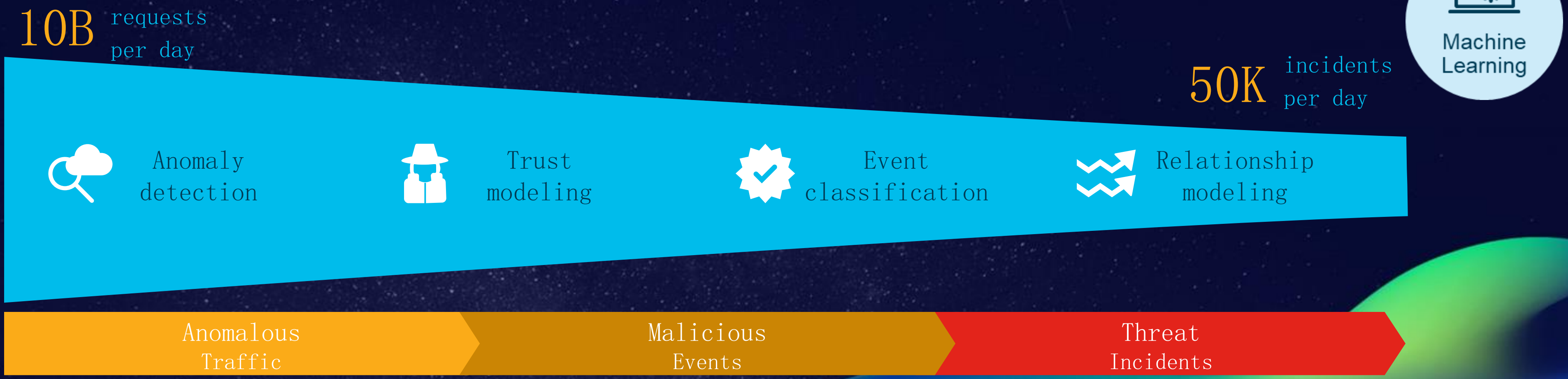
37 Spam tracking

Machine Learning

Sample report demonstrating an advanced threat visibility gap: http://cognitive.cisco.com/preview

Cognitive Threat Analytics (CTA)

Early detection and response with artificial intelligence



10B requests per day

50K incidents per day

Machine Learning

Anomaly detection

Trust modeling

Event classification

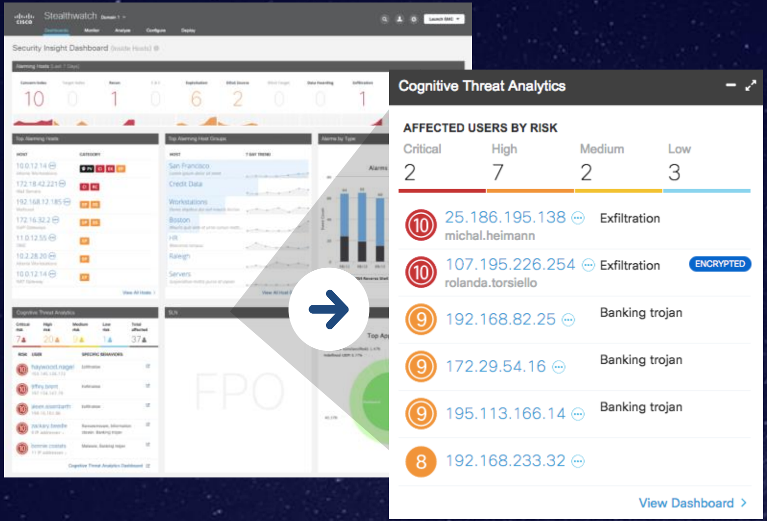
Relationship modeling

Anomalous Traffic

Malicious Events

Threat Incidents

Easily prioritize risks with relevant alarms



Stealthwatch

Security Insight Dashboard

Cognitive Threat Analytics

AFFECTED USERS BY RISK

Critical	High	Medium	Low
2	7	2	3

- 10 25.186.195.138 michal.heimann Exfiltration
- 10 107.195.226.254 rolanda.torsiello Exfiltration ENCRYPTED
- 9 192.168.82.25 Banking trojan
- 9 172.29.54.16 Banking trojan
- 9 195.113.166.14 Banking trojan
- 8 192.168.233.32

View Dashboard ›

Machine Learning

Detect malware without decryption

through **MACHINE LEARNING** and correlation of global threat behaviors

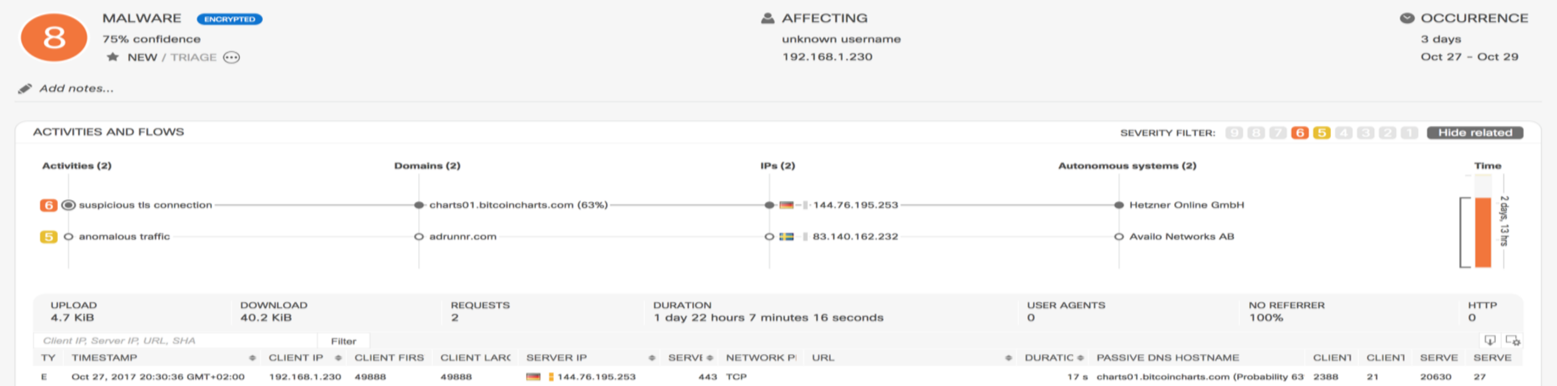
Example ETA classifier

Suspicious TLS Connections

Trained on Threat Grid samples

Features: TLS extension types, TLS cipher suite types, SPLT, GFC

Machine Learning



8 MALWARE ENCRYPTED

75% confidence

★ NEW / TRIAGE

Add notes...

AFFECTING

unknown username

192.168.1.230

OCCURRENCE

3 days

Oct 27 – Oct 29

ACTIVITIES AND FLOWS

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

Activities (2)	Domains (2)	IPs (2)	Autonomous systems (2)
6 suspicious tls connection	charts01.bitcoincharts.com (63%)	144.76.195.253	Hetzner Online GmbH
5 anomalous traffic	adrunnr.com	83.140.162.232	Availo Networks AB

Time: 2 days, 13 hrs

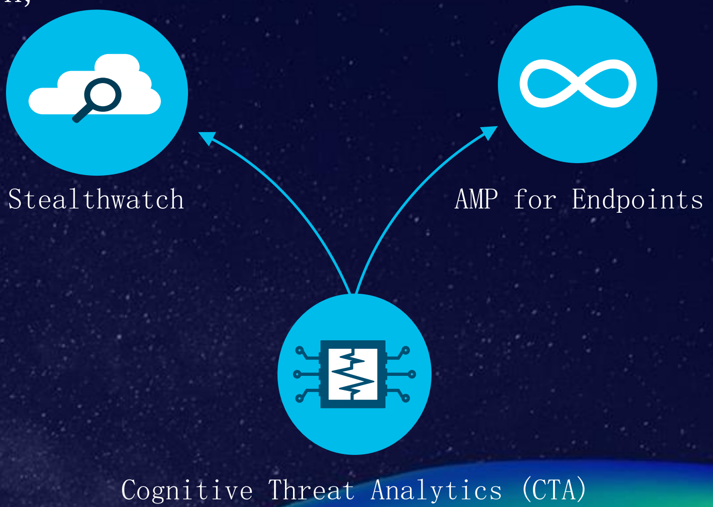
UPLOAD	DOWNLOAD	REQUESTS	DURATION	USER AGENTS	NO REFERRER	HTTP
4.7 KiB	40.2 KiB	2	1 day 22 hours 7 minutes 16 seconds	0	100%	0

Client IP, Server IP, URL, SHA Filter

TY	TIMESTAMP	CLIENT IP	CLIENT FIRS	CLIENT LARC	SERVER IP	SERVI	NETWORK P	URL	DURATIC	PASSIVE DNS HOSTNAME	CLIENT	CLIENT	SERVE	SERVE
E	Oct 27, 2017 20:30:36 GMT+02:00	192.168.1.230	49888	49888	144.76.195.253	443	TCP		17 s	charts01.bitcoincharts.com (Probability 63	2388	21	20630	27

Architectural advantage in action

Integrated work-flow across Stealthwatch, CTA, AMP for Endpoints



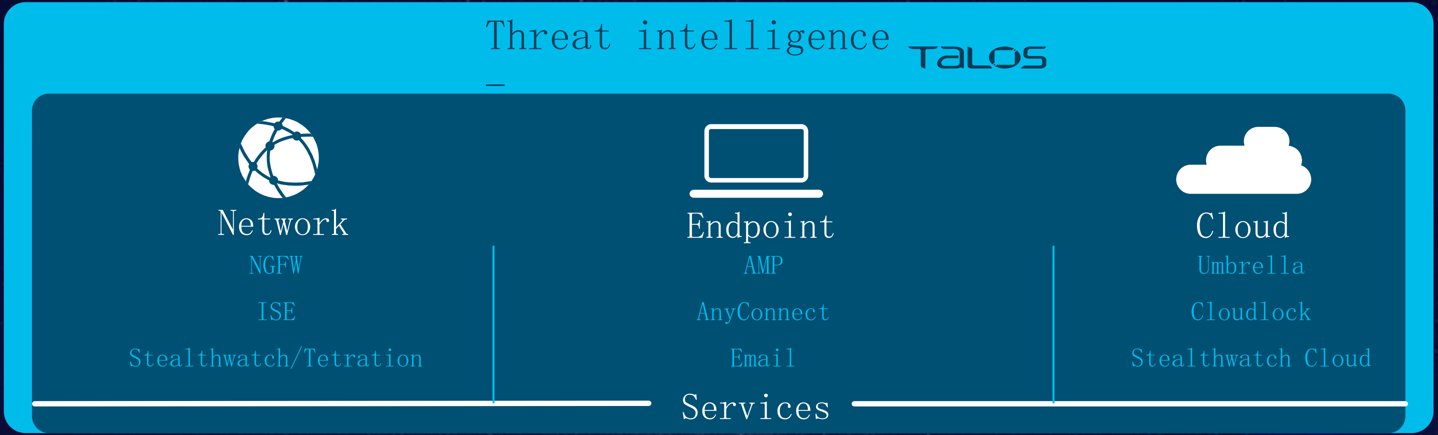
Machine Learning

Attackers may be able to evade one technique…
but not all of them

Cisco:
Security that works together

Security that works together

Cisco Security Architecture



Threat intelligence TALOS

Network
NGFW
ISE
Stealthwatch/Tetration

Endpoint
AMP
AnyConnect
Email

Cloud
Umbrella
Cloudlock
Stealthwatch Cloud

Services

Talos provides unmatched visibility, threat research, and analytics

FIT · FREEBUF

GLOBAL

Threats Across the Internet

&

LOCAL

Threats Inside Your Network

Hundreds of Thousands Customers

Tens of Millions Users

19.7B
Threats Blocked Per Day

300
Threat Researchers

Hundreds of Threat Analytic Engines

全球高峰会

Good AI is 100% dependent on accessible data

FIT · FREEBUF

We analyze massive amounts of data — 19.7 billion threats blocked daily

600 Billion
Email samples

16 Billion
Web requests

3.4 Billion
AMP queries

Our real-time datasets are diverse, global, and live

100 Billion
Internet requests

80 Million
Daily active users

12,000
Enterprise customers

160
Countries worldwide

Best of breed

Portfolio

Integrated

Architecture

扫描了解更多
思科安全方案
Cisco Cybersecurity Solution

立即下载
思科2017年中网络安全报告
2017 MCR(Midyear Cybersecurity Report)

Thank you

CISCO