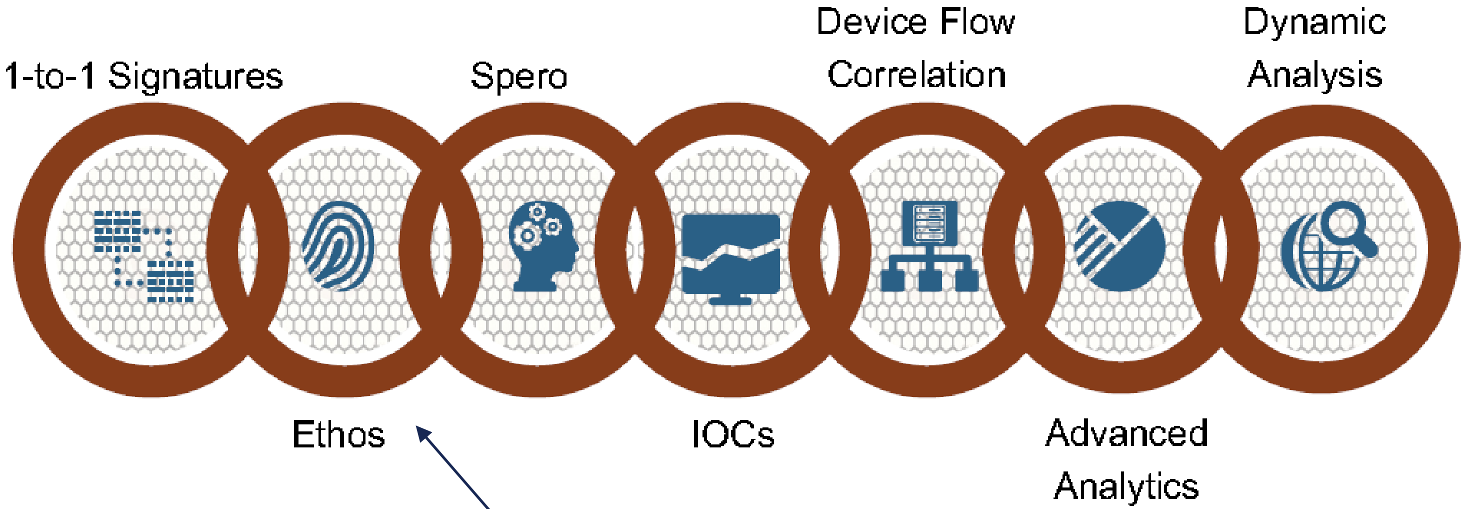
Managed Security Services

Active Threat Analytics

Cisco Security Solutions

Milan Habrcetl
Security Account Manager CZ+SK
23. 3. 2017

AMP4E – prevention analysis



Polymorphic modifications

The results speak for themselves

6.5 hours

Average time to detection with Cisco security

100 days

Industry average time to detection

Source: Cisco Annual Security Report 2017

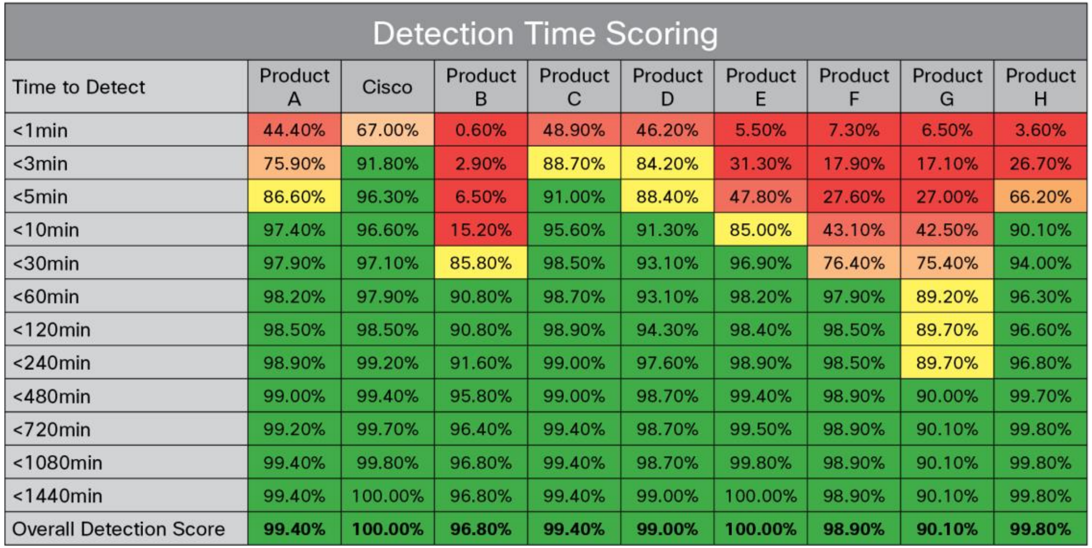
cisco

Competitive Threat Intelligence Comparison

	TaLOS	Palo Alto Networks (AutoFocus)	Check Point (ThreatCloud)	Fortinet (FortiGuard)
Unique Malware Samples/Daily	1.5M per day	10s of Thousands per day	10s of Thousands per day	10s of Thousands per day
Email Messages Analyzed/Daily	93B per day (86% are SPAM)	none	Not reported	6M SPAM Signatures/day
Total Threats Blocked Daily	19.6B per day	Not reported: Likely 1000s	700K per day	Not Reported
Categorized Web Blocks	4.3B per day	Millions per day	Not reported	35M per day
Threat Data Processed	120TB/day - 3.6PB per month (CWS)	Not reported	Not reported	31TB/Day/900TB per month
Contributing Users/Sensors	150M (AC/AMP)/1.6M (IPS)	1000s	1000s of Gateways	Not Reported
Cost	Free with Product	$35K per Seat	Free with Product	FortiGuard Subscription

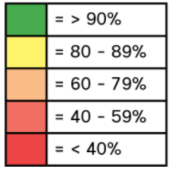
Fastest Time to Detection

Faster time to detection means less time and space for attackers to operate – closing the protection gap and providing more effective security.



Detection Time Scoring									
Time to Detect	Product A	Cisco	Product B	Product C	Product D	Product E	Product F	Product G	Product H
<1min	44.40%	67.00%	0.60%	48.90%	46.20%	5.50%	7.30%	6.50%	3.60%
<3min	75.90%	91.80%	2.90%	88.70%	84.20%	31.30%	17.90%	17.10%	26.70%
<5min	86.60%	96.30%	6.50%	91.00%	88.40%	47.80%	27.60%	27.00%	66.20%
<10min	97.40%	96.60%	15.20%	95.60%	91.30%	85.00%	43.10%	42.50%	90.10%
<30min	97.90%	97.10%	85.80%	98.50%	93.10%	96.90%	76.40%	75.40%	94.00%
<60min	98.20%	97.90%	90.80%	98.70%	93.10%	98.20%	97.90%	89.20%	96.30%
<120min	98.50%	98.50%	90.80%	98.90%	94.30%	98.40%	98.50%	89.70%	96.60%
<240min	98.90%	99.20%	91.60%	99.00%	97.60%	98.90%	98.50%	89.70%	96.80%
<480min	99.00%	99.40%	95.80%	99.00%	98.70%	99.40%	98.90%	90.00%	99.70%
<720min	99.20%	99.70%	96.40%	99.40%	98.70%	99.50%	98.90%	90.10%	99.80%
<1080min	99.40%	99.80%	96.80%	99.40%	98.70%	99.80%	98.90%	90.10%	99.80%
<1440min	99.40%	100.00%	96.80%	99.40%	99.00%	100.00%	98.90%	90.10%	99.80%
Overall Detection Score	**99.40%**	**100.00%**	**96.80%**	**99.40%**	**99.00%**	**100.00%**	**98.90%**	**90.10%**	**99.80%**

Figure 2. NSS Time to Detection Test Results



🟩	= > 90%
🟨	= 80 - 89%
🟧	= 60 - 79%
🟥	= 40 - 59%
🟥	= < 40%

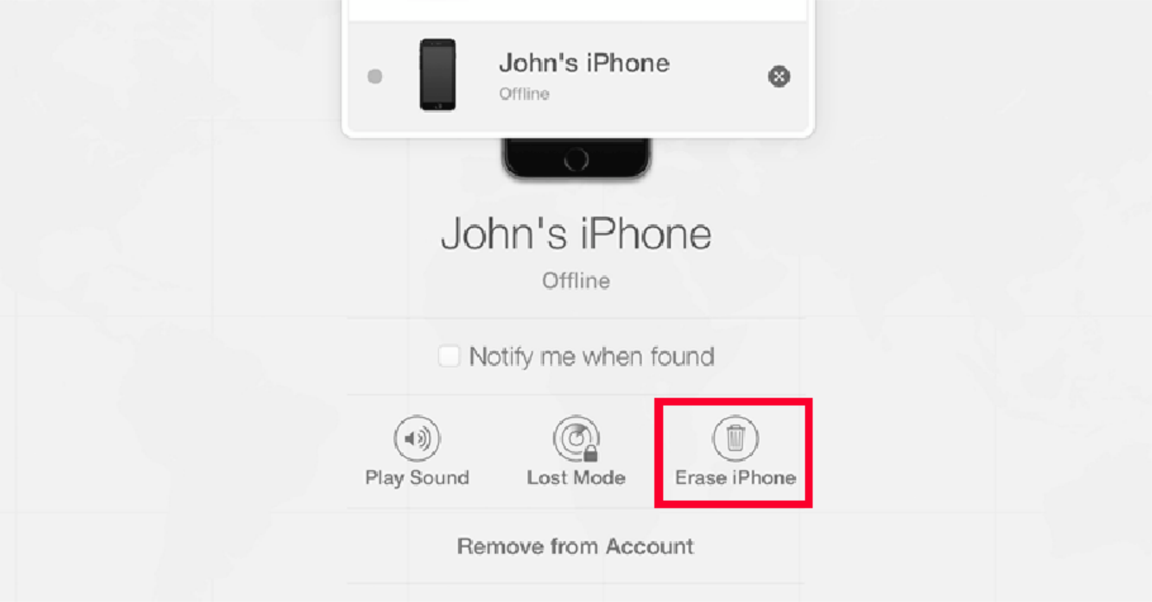
- We block attacks fastest - blocking 91.8% of attacks in < 3 minutes
- Products with faster detection rates get to green numbers faster moving from top to bottom.
- Products may have the same Overall Detection Score at the bottom, but those with the faster time to detection are more effective – giving attackers less time and space to operate.

Welcome in SOC

Hackers Threaten to Remotely Wipe 300 Million iPhones Unless Apple Pays Ransom

Tuesday, March 21, 2017 Mohit Kumar

G+1 82 Like 5.4K Share 17.7K Tweet 1770 in Share 983 Share 28.9K



If you use iCloud to sync your Apple devices, your private data may be at risk of getting exposed or deleted by April 7th.

It has been found that a mischievous group of hackers claiming to have access to over 300 million iCloud accounts is threatening Apple to remotely wipe data from those millions of Apple devices unless Apple pays it $75,000 in crypto-currency or $100,000 worth of iTunes gift cards.

Security Challenges

Changing Business Models

Dynamic Threat Landscape

Complexity and Fragmentation

Security Challenges

Changing Business Models

IOE

25%
increase in an organization’s cybersecurity risk due to IoE

CLOUD

5-10
times more cloud services are being used than known by IT

Dynamic Threat Landscape

60% data in breaches is stolen in hours

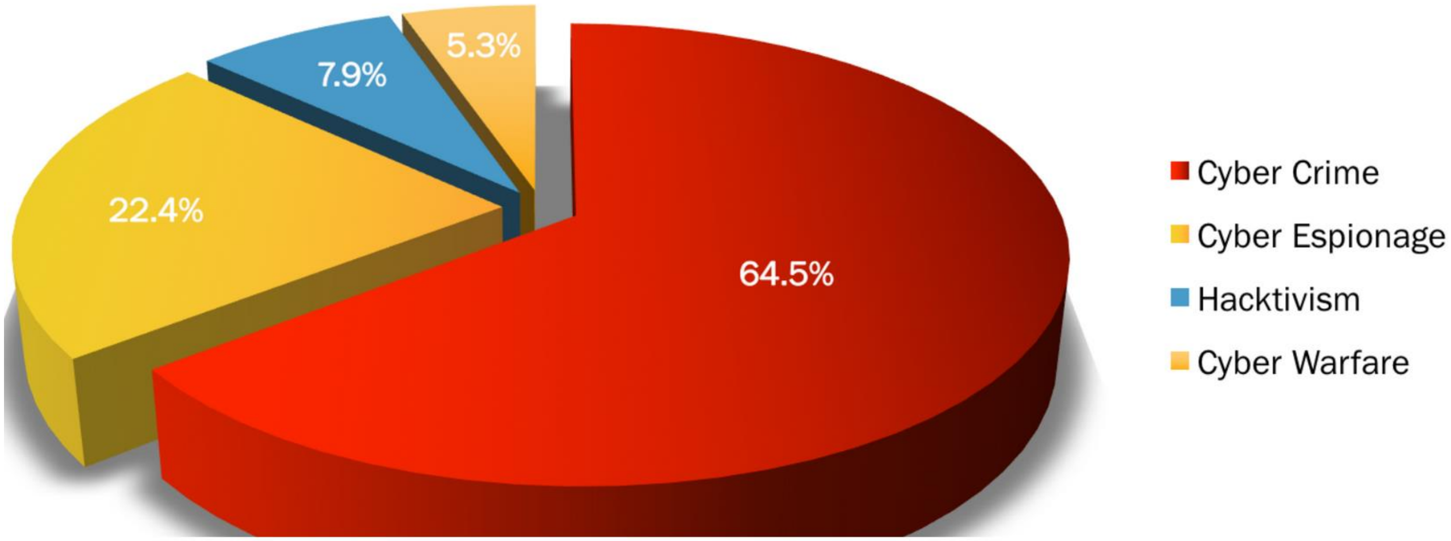
54% of breaches remain undiscovered for months

Complexity and Fragmentation

12x Demand for security talent

45 Security vendors for some customers

Cyber Attacks motivation



February 2017 Cyber Attacks Statistics

Cisco Security Hypothesis

Security Challenges + Operational Focus + Talent Shortage

Requires Improved Outcomes

Visibility

Threat-centric

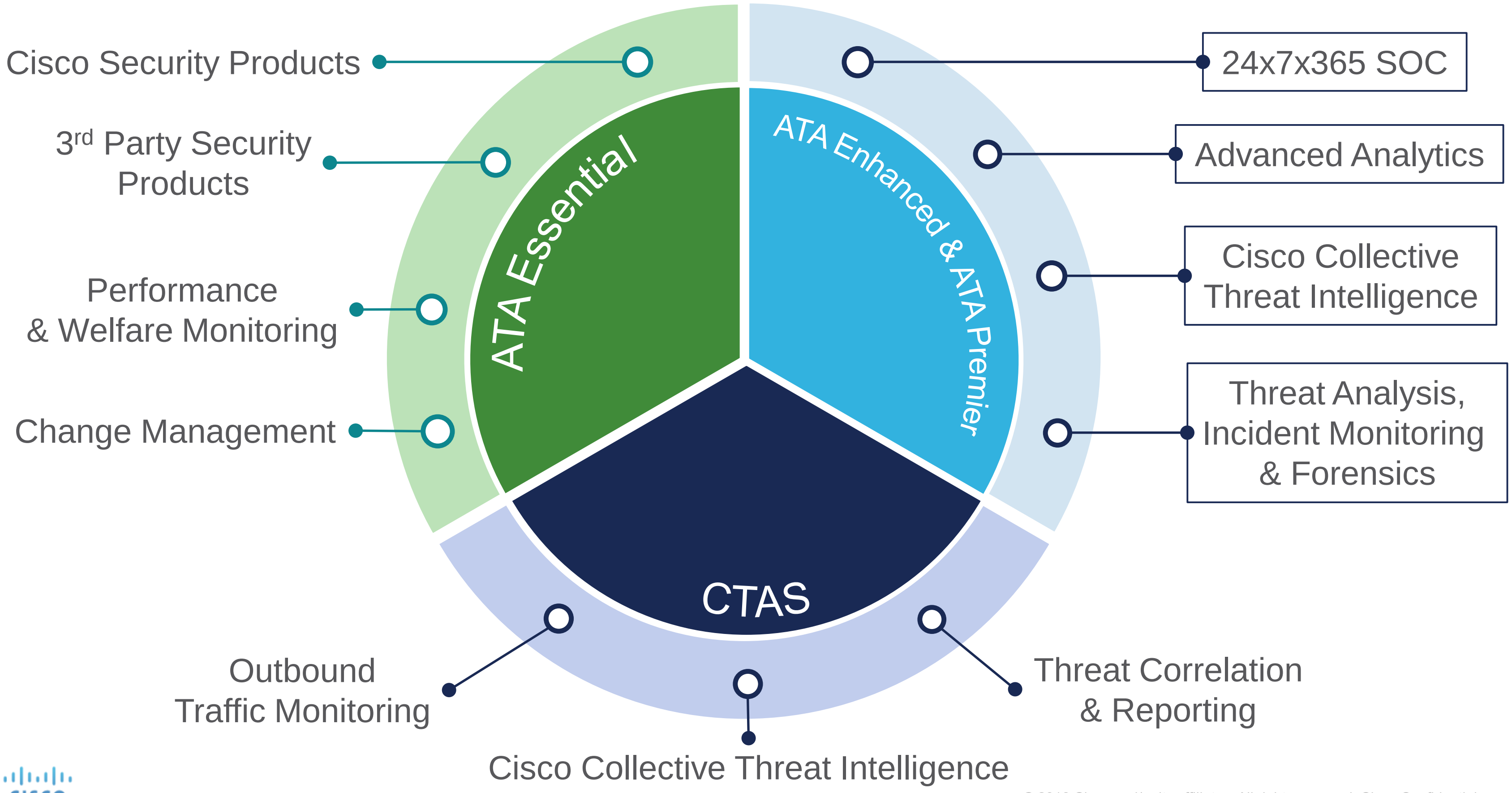
Platform-based

Advisory

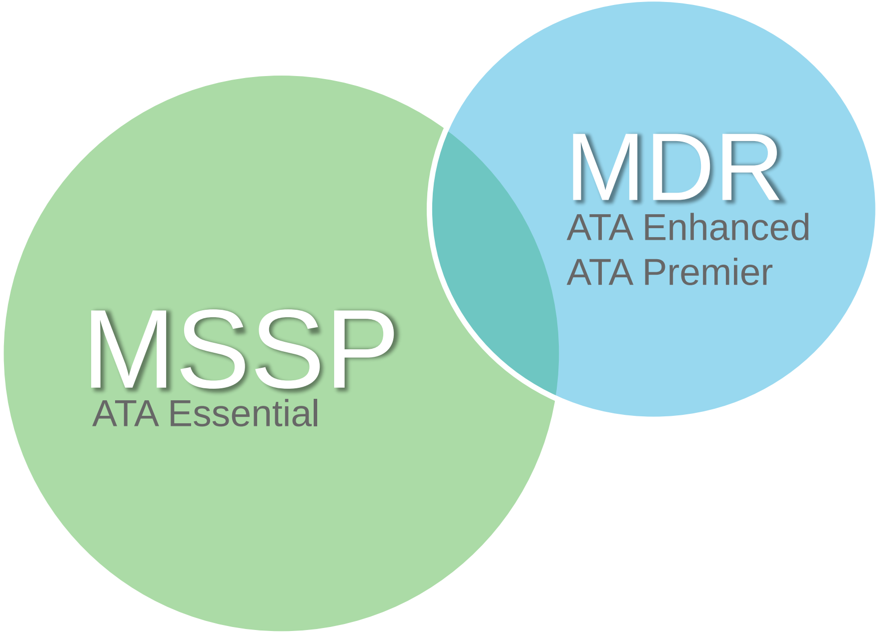
Integration

Managed

Cisco Managed Security Services


Cisco Security Products
3rd Party Security Products
Performance & Welfare Monitoring
Change Management
ATA Essential
ATA Enhanced & ATA Premier
CTAS
24x7x365 SOC
Advanced Analytics
Cisco Collective Threat Intelligence
Threat Analysis, Incident Monitoring & Forensics
Outbound Traffic Monitoring
Threat Correlation & Reporting
Cisco Collective Threat Intelligence

Gartner: Managed Detection and Response (MDR)



What is MDR?

It is a new category focused on improving threat detection and incident response.

It generally relies on threat intelligence and advanced analytics, with several offerings leveraging big data platforms for advanced detection.

It is an emerging market:

- By 2020, Gartner expects 15% of organizations will be using MDR and 50% of MSSP's will offer MDR services

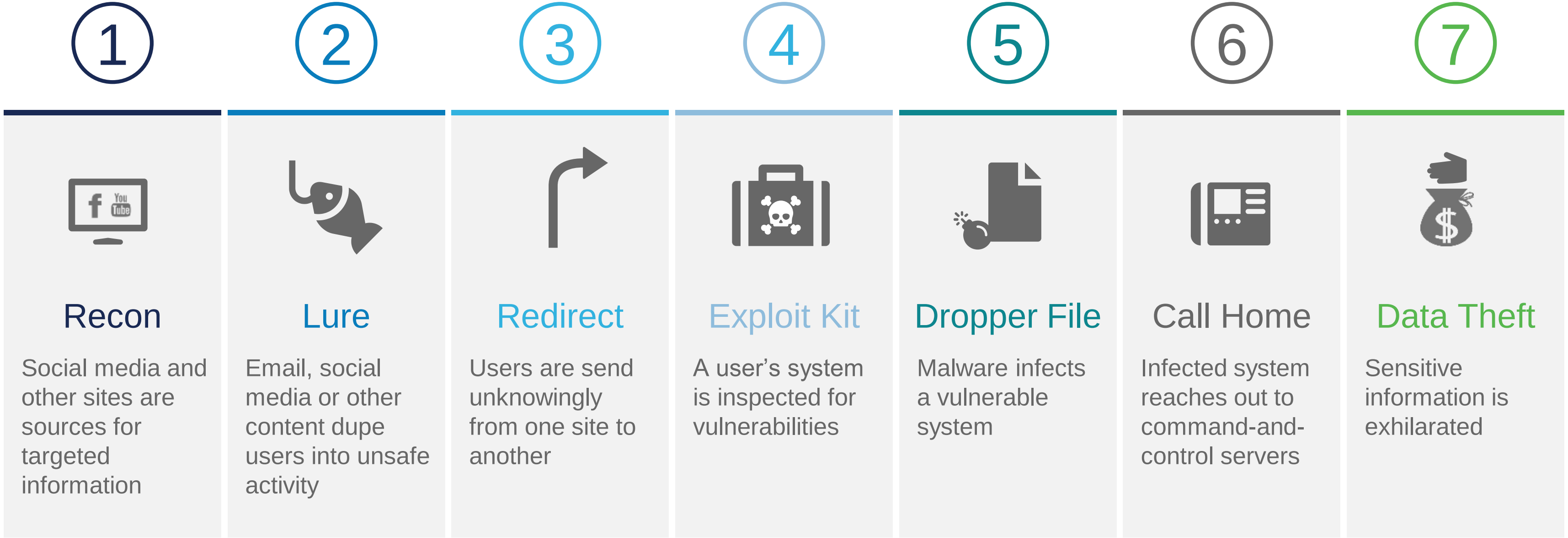
Gartner: MSSP vs MDR

MSSP	MDR
Addresses compliance, remote monitoring and management, and basic threat detection	Focus is primarily on advanced threat detection.
Generally focuses on monitoring of perimeter devices or devices managed by the provider	Addresses attacks that bypass perimeter defenses.
Collects limited contextual information, which results in insufficient detail for the customer to properly analyze incident and take action	Aims to offer as much information and context as possible for targeted recommendations based on concrete information

“Clients should be wary of claims from traditional MSSPs on their ability to deliver MDR-like services. Delivering these services requires technologies not traditionally in scope for MSS”

Active Threat Analytics (ATA) Overview

Cyber Kill Chain



1 Recon
Social media and other sites are sources for targeted information

2 Lure
Email, social media or other content dupe users into unsafe activity

3 Redirect
Users are send unknowingly from one site to another

4 Exploit Kit
A user’s system is inspected for vulnerabilities

5 Dropper File
Malware infects a vulnerable system

6 Call Home
Infected system reaches out to command-and-control servers

7 Data Theft
Sensitive information is exhilarated

Stage 2 (Lure) – ATA has detection for the compromised websites

Stage 3 (Redirect) – ATA has detection for the injected code that redirects the user to the exploit page

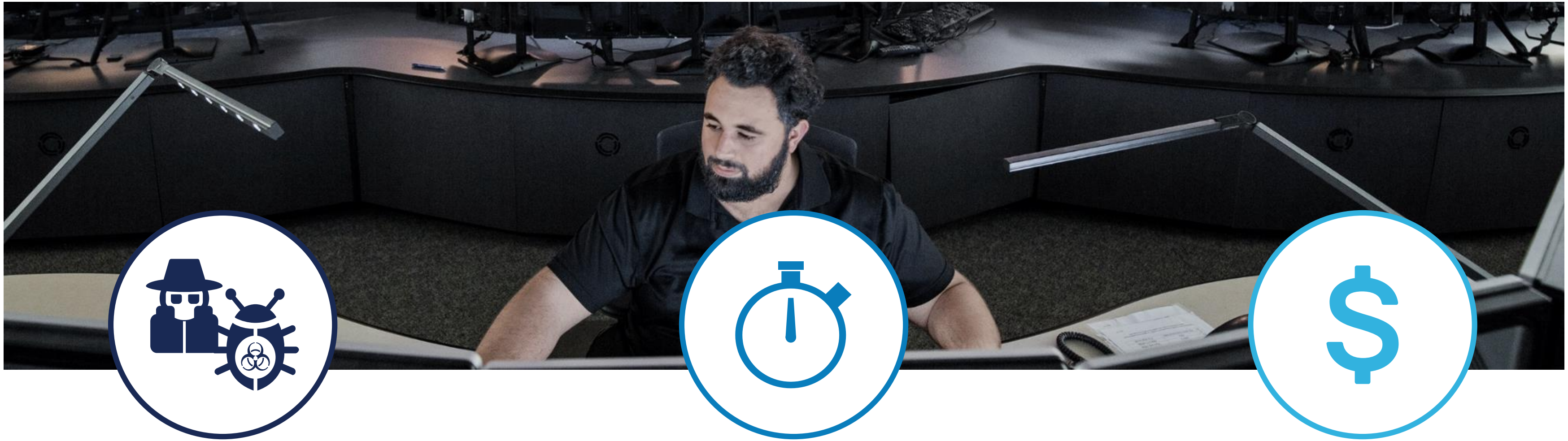
Stage 4 (Exploit Kit) – ATA has detection for the malicious code that attempts to execute this cyber attack

Stage 5 (Dropper Files) – ATA has detection for the binary files associated with this attack

Google is testing a way to log into devices with a challenge
sent to your Android or iOS phone, rather than a password.
Internet Explorer 11 – now the only way to
2

Why Active Threat Analytics?

Threats Find Safety in Numbers



70,000

average number of security events an enterprise generates per week[1]

395

hours lost investigating false-positives each week[2]

$1.3M

cost per year of time lost investigating false-positives[2]

*Derived from Ponemon Institute Cost of Cyber Crime Study 2015

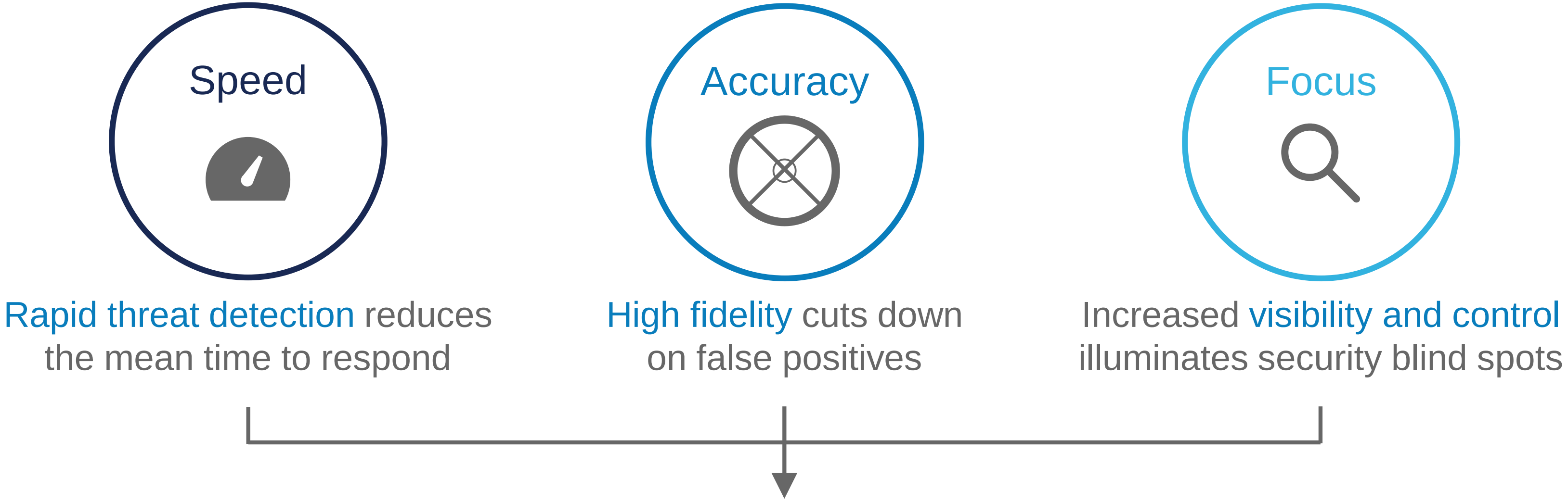
[1] 2014 State of Infections Report. Damballa. May 2014. https://www.damballa.com/downloads/r_pubs/Damballa_Q114_State_of_Infections_Report.pdf

[2] The Cost of Malware Containment. Ponemon Institute. January 2015. http://www.ponemon.org/local/upload/file/Damballa%20Malware%20Containment%20FINAL%203.pdf

The Challenges of False-Positives

- Too many alerts to investigate
- Hard to know which alerts to prioritize
- Frustration of redundant efforts
- Risk of a real threat slipping through the cracks
- Opportunity cost of investigating false-positives

Active Threat Analytics Enables:



Speed

Rapid threat detection reduces the mean time to respond

Accuracy

High fidelity cuts down on false positives

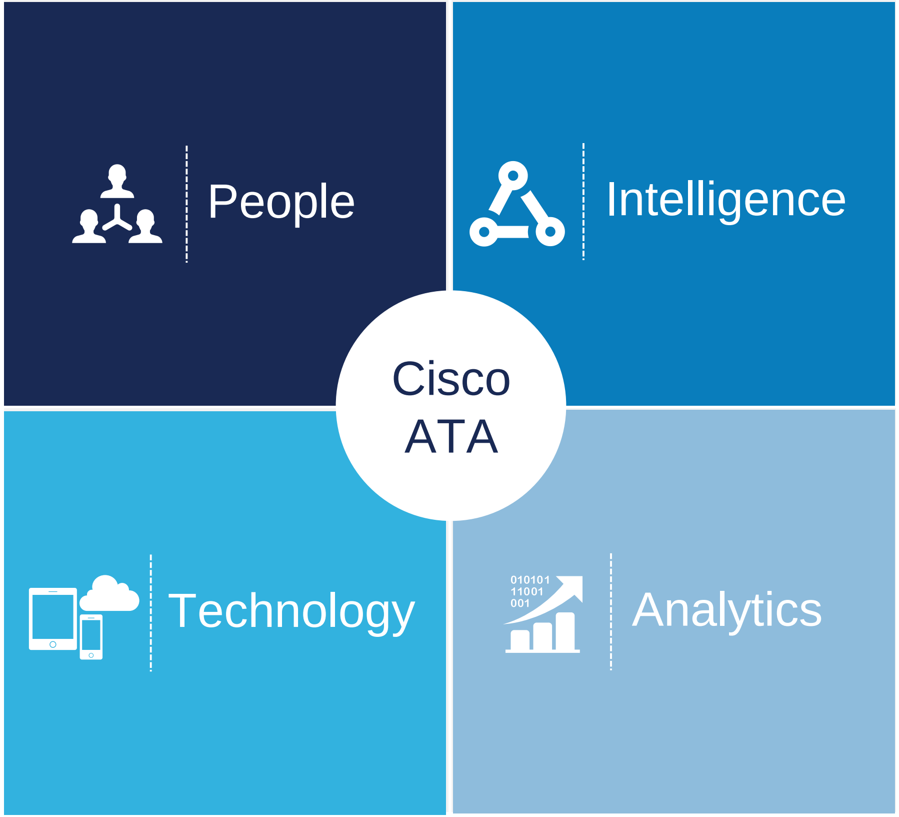
Focus

Increased visibility and control illuminates security blind spots

Customer Benefits

Risk Mitigation	Proactive Security	Operational Efficiency	Strategic Focus	Comprehensive Coverage

Active Threat Analytics



People

Intelligence

Cisco ATA

Technology

Analytics

Cisco Collective Security Intelligence

Built on unmatched collective security telemetry that gets better every 5 minutes

Cisco Talos

101 1110011 0110011 101000 0110 00
1000 0110 00 0111000 111010011 101 1100001 110
001110 1001 1101 1110011 0110011 101000 0110 00

1001 1101 1110011 0110011 101000 0110 00
101000 0110 00 0111000
1100001110001110 1001

Cisco Collective Security Intelligence

Email
Endpoints
WWW Web
Networks
IPS
Devices

1.6M
global sensors

100TB
of data received per day

150M+
deployed endpoints

600+
engineers, technicians, and researchers

35%
worldwide email traffic

13B
web requests

24x7x365
operations

40+
languages

180,000+ File Samples per Day

FireAMP Community

Advanced Microsoft and Industry Disclosures

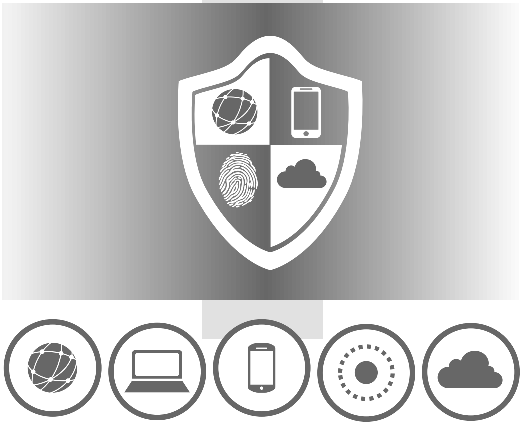
Snort and ClamAV Open Source Communities

Honeypots

Sourcefire AEGIS Program

Private and Public Threat Feeds

Dynamic Analysis

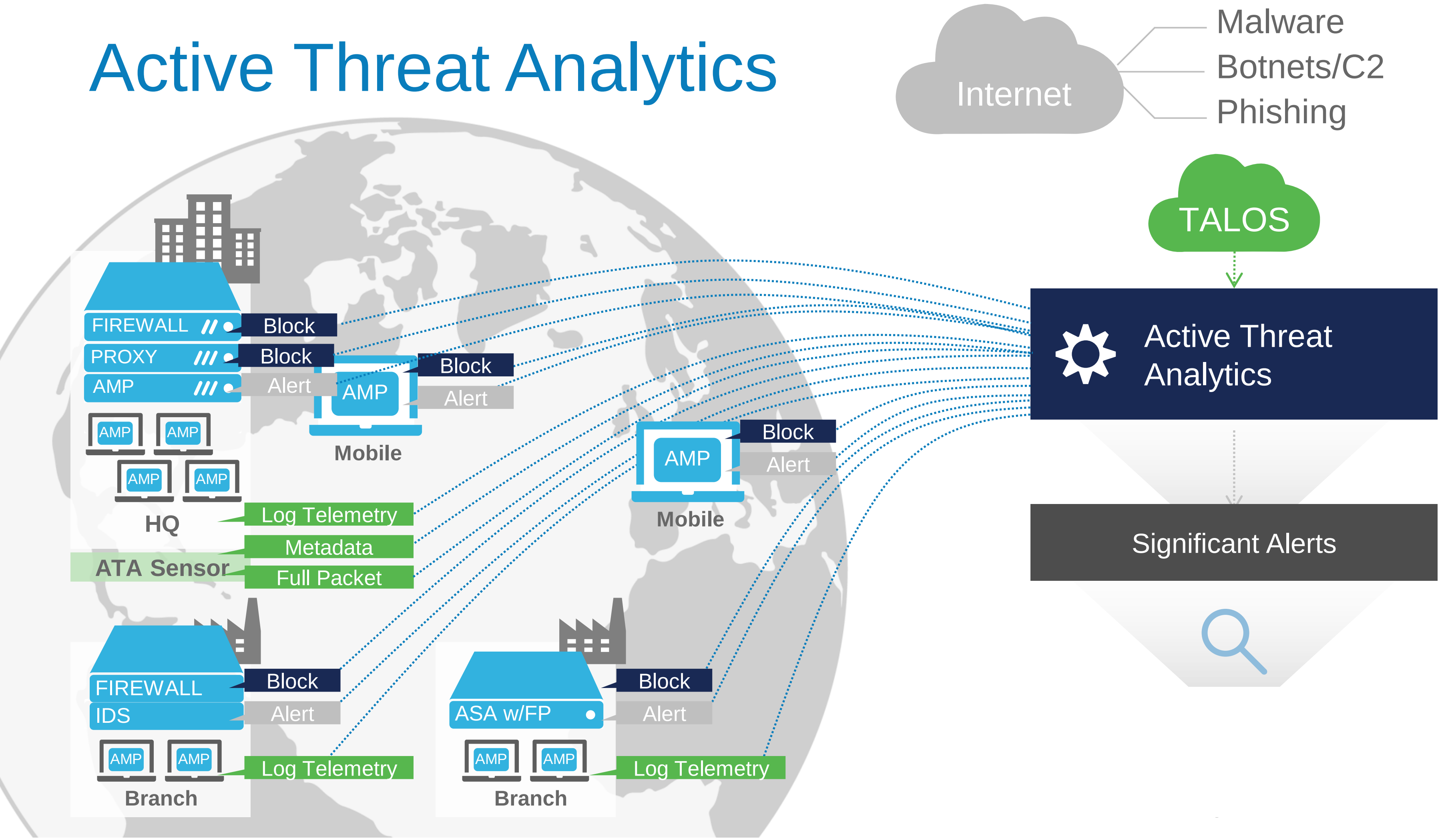


Analytics Methods

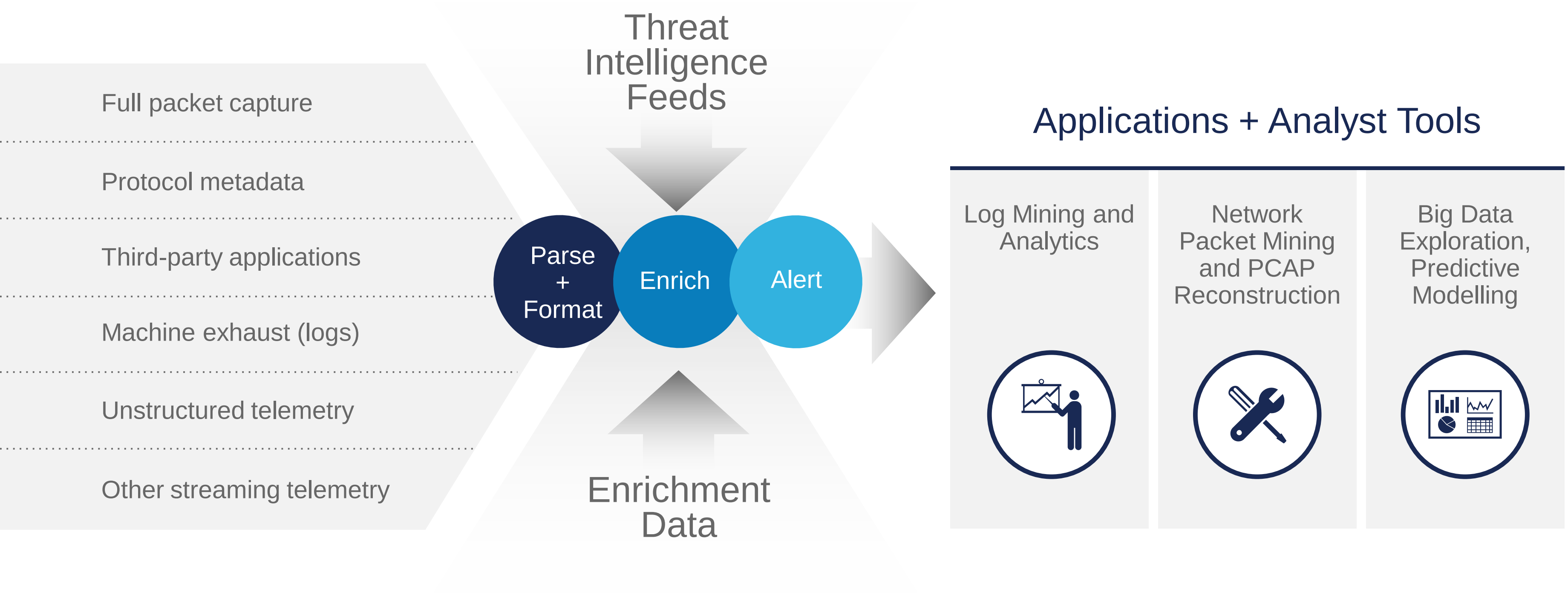
Service Differentiator

	Deterministic Rules-Based Analytics (DRB)	Statistical Rules-Based Analytics (SRB)	Data Science-Centric Analytics (DSC)
Examples	• Signature based detection • Alerting when predefined thresholds are exceeded • Identification of outbound communication to known C&C domains or IPs	• Unusual system changes such as from non-standard administrator accounts or bulk changes at unexpected times • Highlight abnormal levels of data export from critical systems	• Automated categorization of data, such identifying classified documents • Alert on suspicious activity gathering around a high value asset. For example, a classified asset is injected with malware, then logged into from a foreign IP, then proceeds to port scan the internal network
Characteristics	• Mature method of analysis • Covers a majority of known threats • Fast detection	• Anomaly detection based on historical context (i.e. highlighting atypical behavior) • Dynamic outlier detection independent of predefined thresholds	• Adaptive learning to automatically tune system for useful alerts • Clustering information around specific attributes to identify behavioral anomalies • Extrapolation of future threat behavior to reduce time to detect
Effort Required	• Creation of rules library based on current known threats • Ongoing maintenance and tuning of rules library	• Manual tuning of statistical parameters to reduce false positives and false negatives • Intimate knowledge of use cases and environmental data to create statistical models	• Automated tuning of model parameters to reduce false positives and false negatives • Broad understanding of use cases and intimate understanding of environmental data

Active Threat Analytics



ATA Flow Framework



Full packet capture

Protocol metadata

Third-party applications

Machine exhaust (logs)

Unstructured telemetry

Other streaming telemetry

Threat Intelligence Feeds

Parse + Format

Enrich

Alert

Enrichment Data

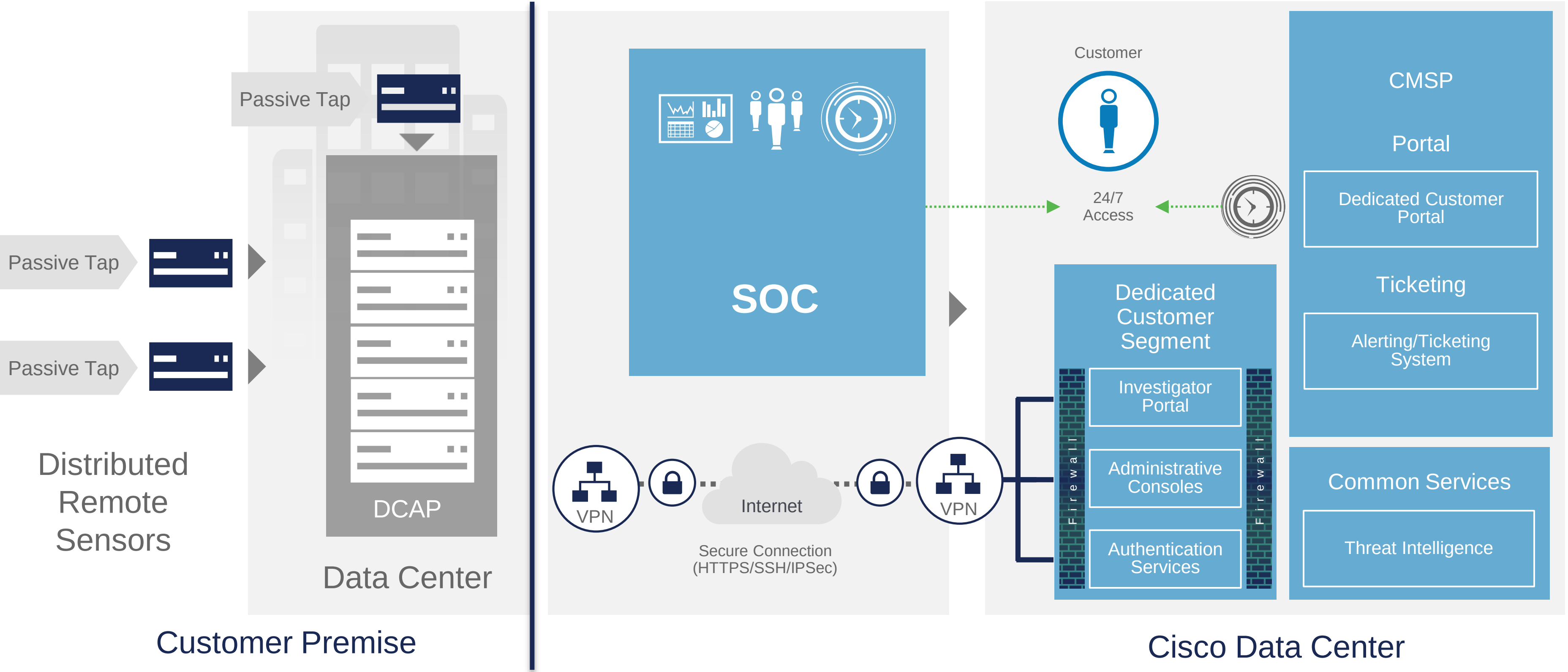
Applications + Analyst Tools

Log Mining and Analytics

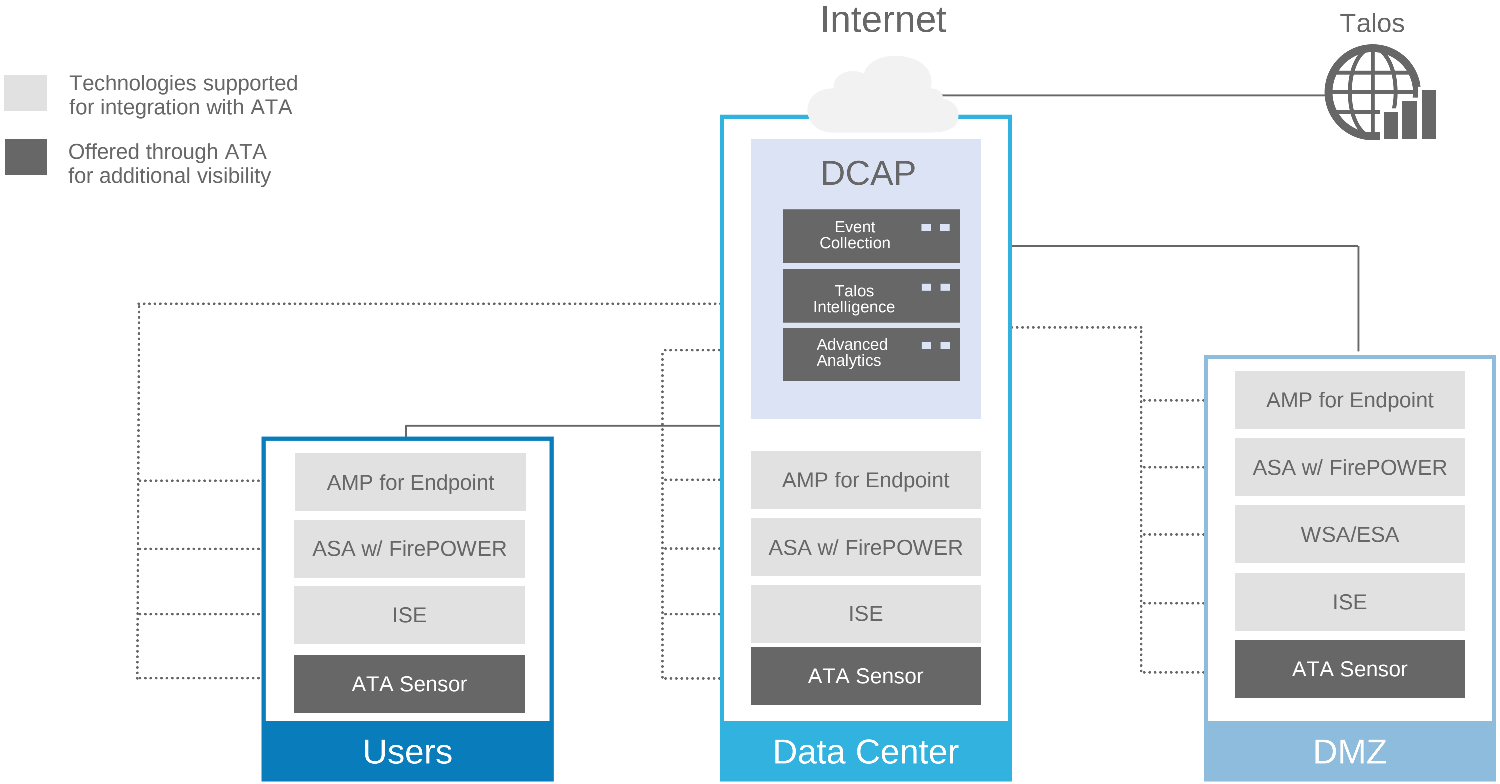
Network Packet Mining and PCAP Reconstruction

Big Data Exploration, Predictive Modelling

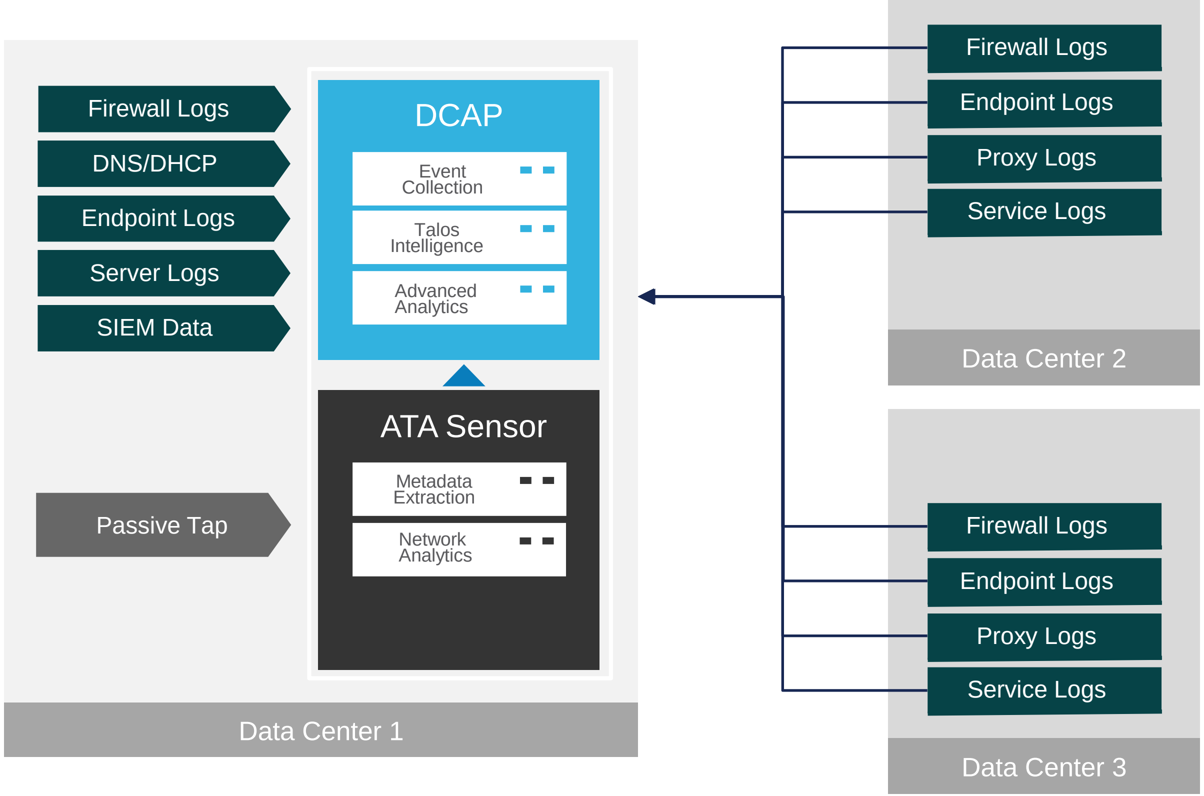
ATA 3.0 Architecture



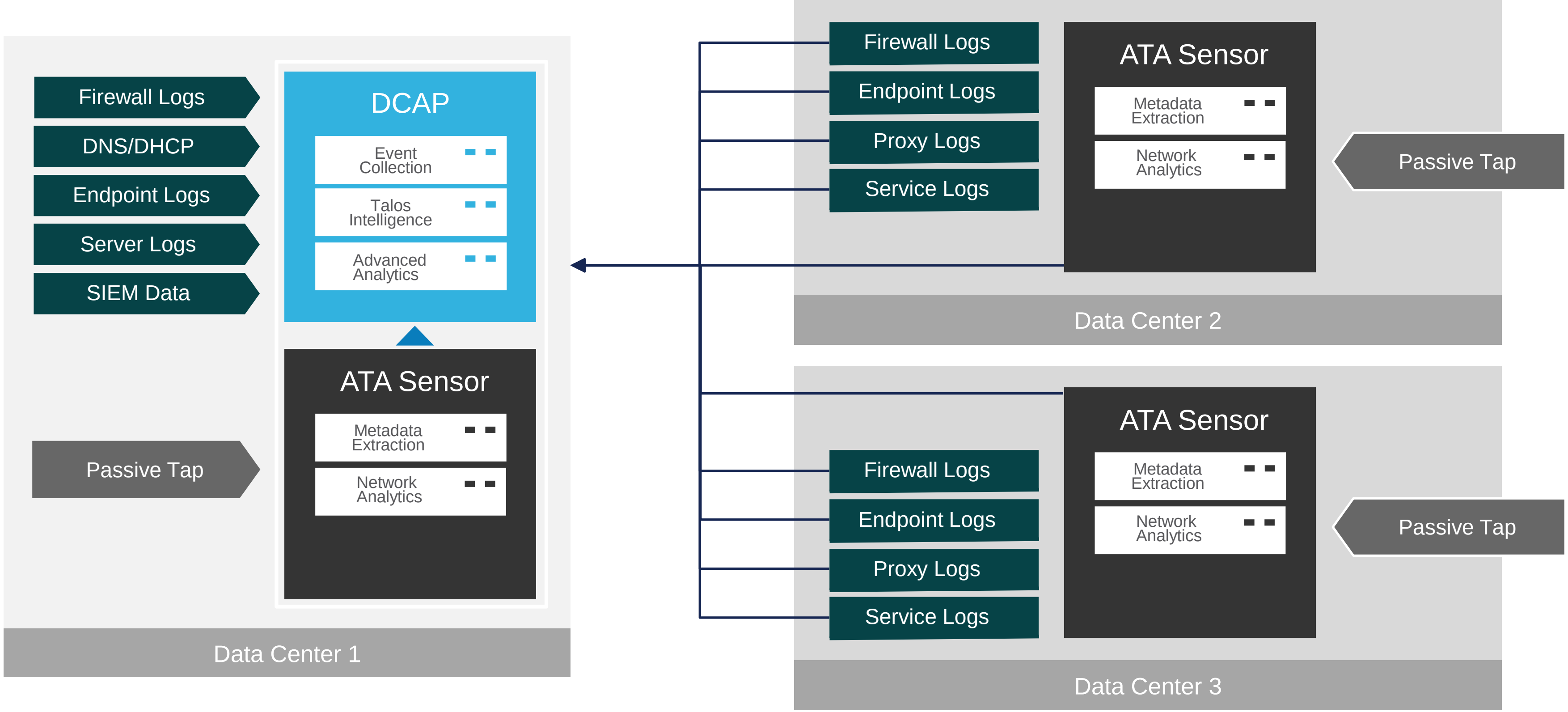
ATA Deployment



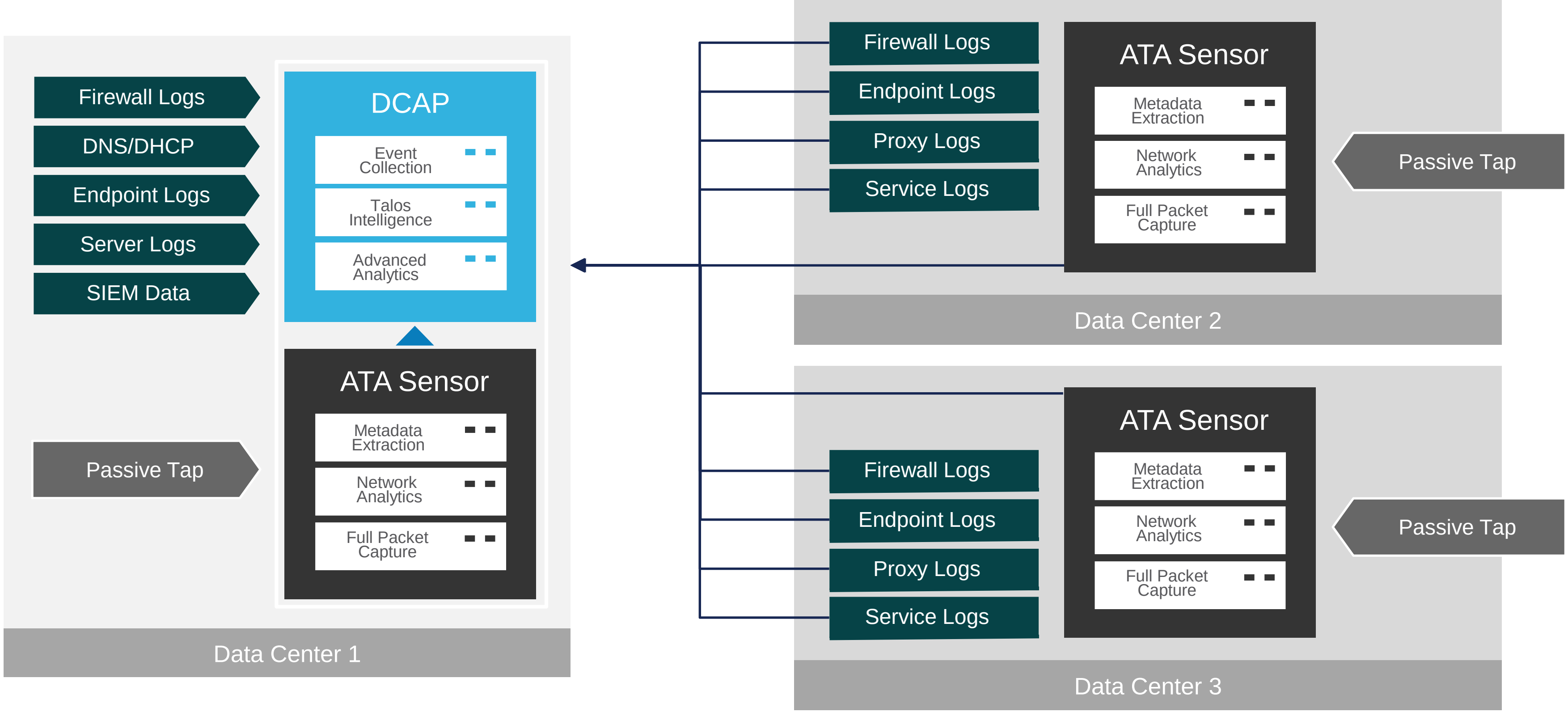
ATA Core Capabilities



ATA Additional Visibility



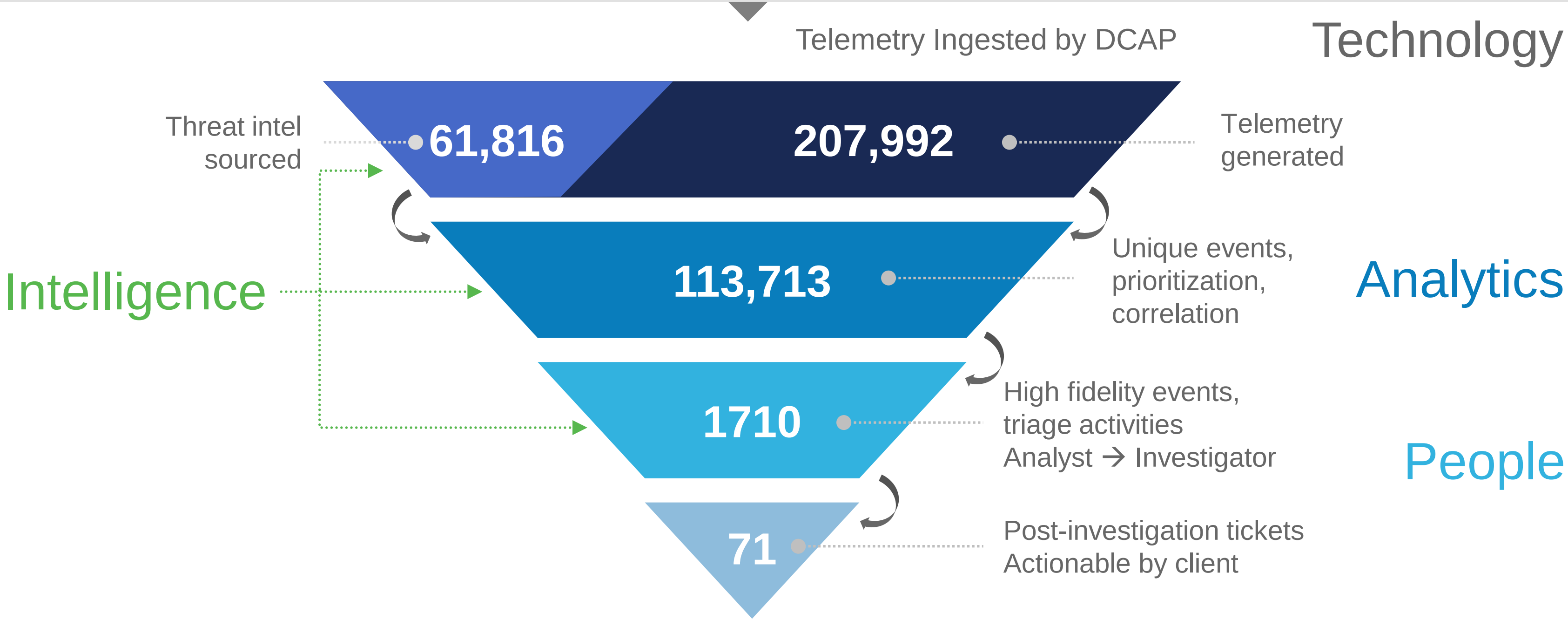
ATA Deep Forensics with Full Packet Capture



Customer Example of 2-Week Timeframe (Premier)

Analytics, intelligence and people differentiators drive focus

269,808 Security Events



Customer
Use Case

Medical Technology

Protects sensitive data with real-time, cost-effective threat monitoring

Challenge

- Shortage of operational security staff
- Time and capital to invest in essential tools and security support
- An operationalized approach to detect and respond to security incidents

Solution

- Active Threat Analytics Premier provided 24/7/365 real time expert staffed SOCs
- Outsourced analysis of network data that includes leading security analytics technology
- Incident investigation and prioritization based on proven techniques and processes

Outcomes

98.6% decrease
in average monthly redundant investigations due to granular threat insight and full-packet forensic capture

93+ hours saved
monthly for customer investigators and analysts on average via reducing false positives and providing actionable recommendations for discovered incidents

42% decrease
in security costs due to migration of complex security operations to a third-party

Customer Case Study

Global Bank

Protects valuable information with real-time, centralized threat monitoring

Challenge

- Low threat visibility into IT infrastructure due to insufficient security tools
- Lack of operational security methodology
- Lack of centralized incident management

Solution

- Deployed Active Threat Analytics Premier to provide behavior-based tools, predictive big data analytics, and a deep collection of security telemetry
- 24/7/365 expert staffed SOCs utilizing a methodology for incident management
- Effectively integrated product telemetry from various sources which increased visibility and enabled usable insights

Outcomes

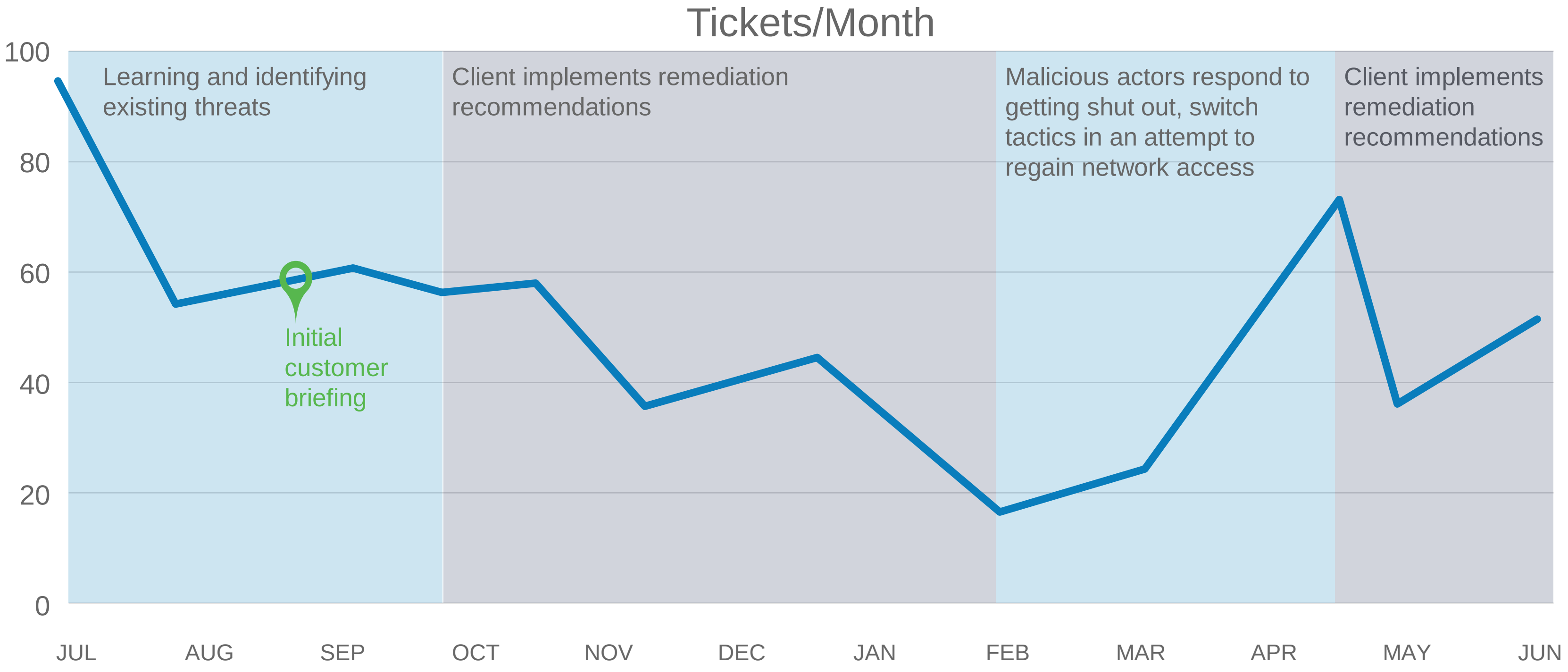
97.6% decrease in average monthly redundant investigations due to granular threat insight and full-packet forensic capture

250 hours saved monthly for customer investigators and analysts on average via reducing false positives and providing actionable recommendations for discovered incidents

Enhanced Detection by incorporating Cisco's comprehensive intelligence, expert staff, and big data technology which enabled detection of Customer unknown threats

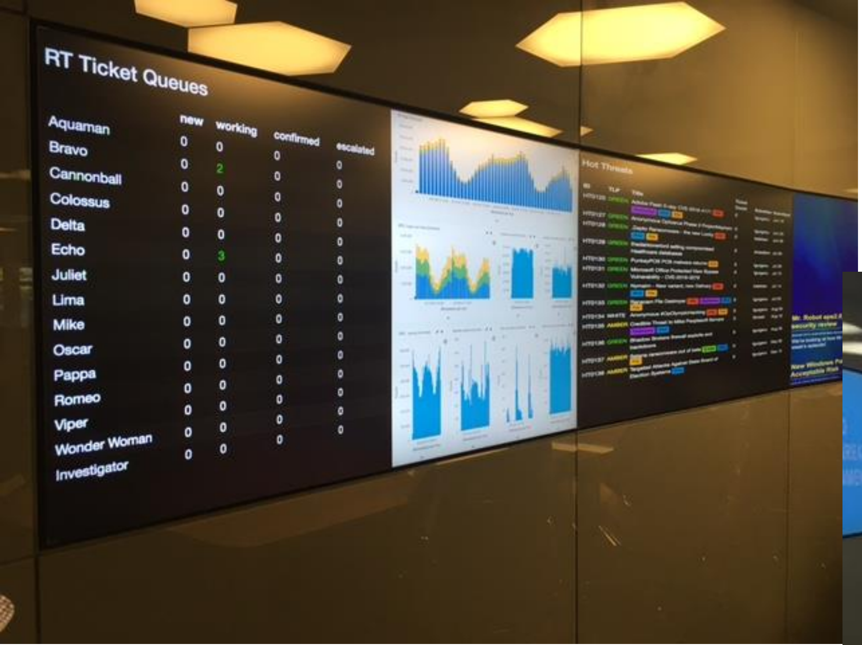
ATA

Continuous protection against evolving threats



MB

See you in Krakow again!



RT Ticket Queues

	new	working	confirmed	escalated
Aquaman	0	0	0	0
Bravo	0	2	0	0
Cannonball	0	0	0	0
Colossus	0	0	0	0
Delta	0	0	0	0
Echo	0	3	0	0
Juliet	0	0	0	0
Lima	0	0	0	0
Mike	0	0	0	0
Oscar	0	0	0	0
Pappa	0	0	0	0
Romeo	0	0	0	0
Viper	0	0	0	0
Wonder Woman	0	0	0	0
Investigator	0	0	0	0

https://www.youtube.com/watch?v=_sUBOcu0pvc www.cisco.com/go/security

https://www.youtube.com/watch?v=_sUBOcu0pvc