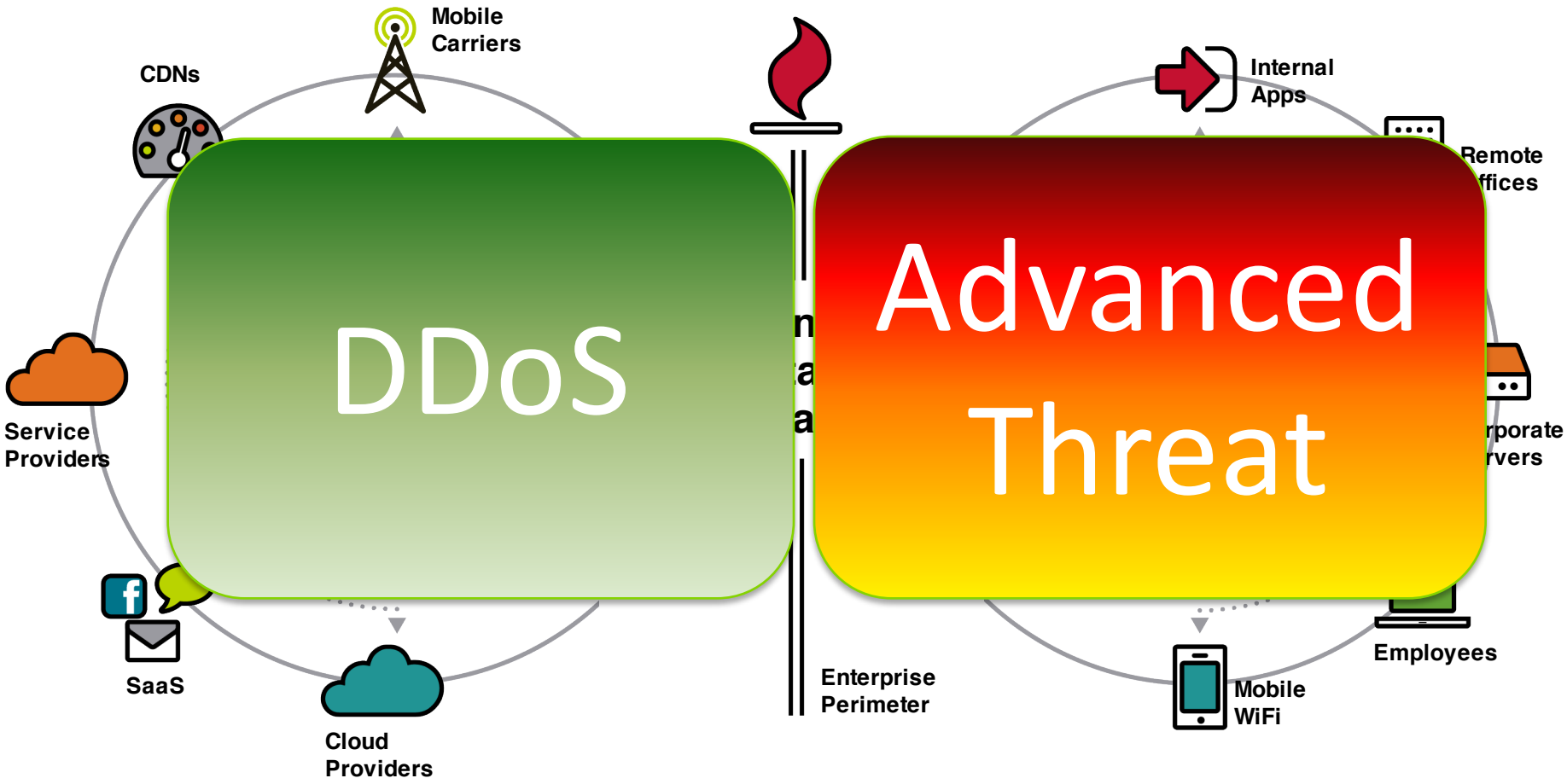
DDoS & APT威脅趨勢, 關聯性, 及因應解決之道

Tony Teo
Director Sales Engineering, APAC
Arbor Networks

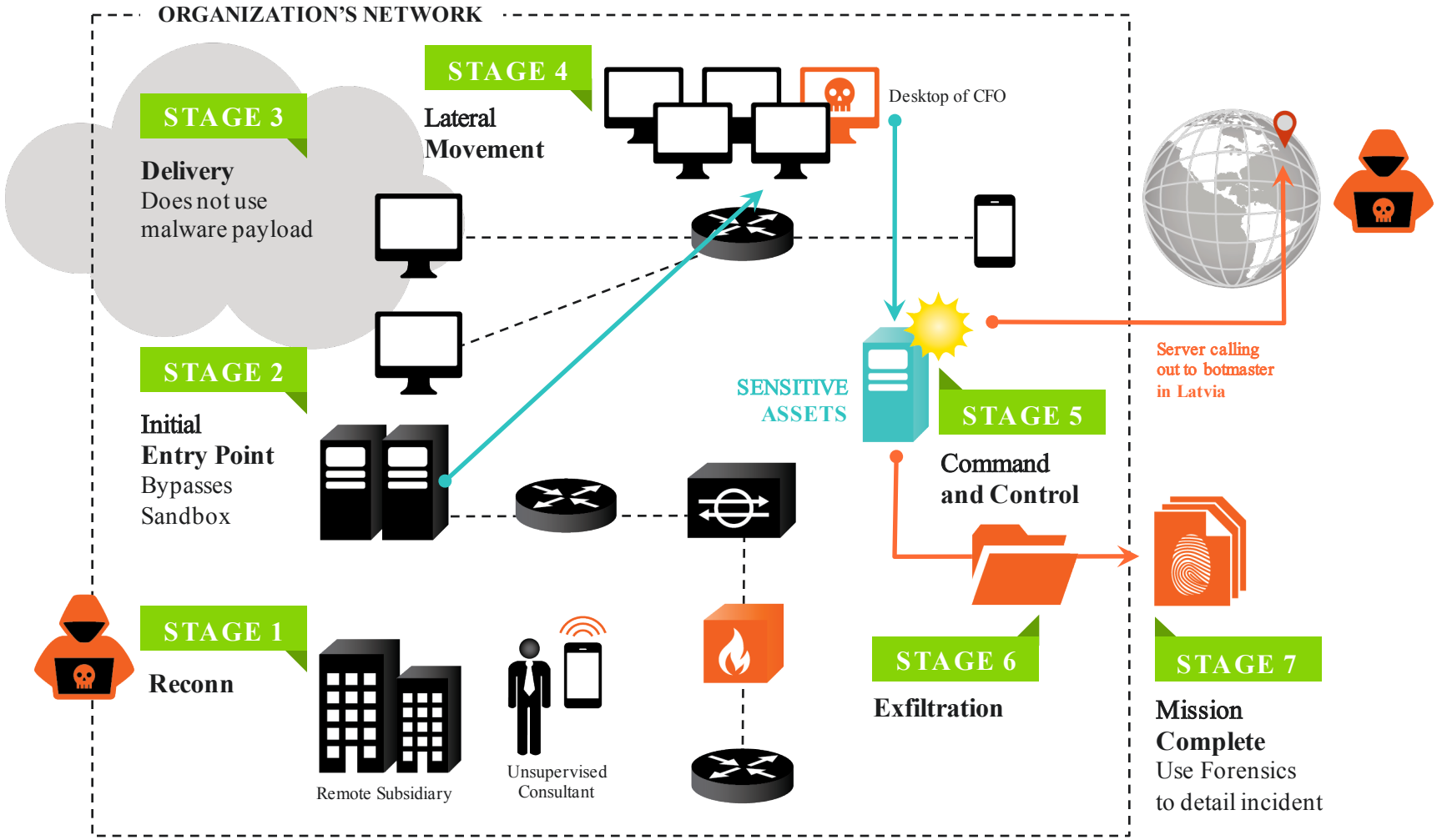
ARBOR® NETWORKS

Today's Cyber Security Challenges



ARBOR NETWORKS

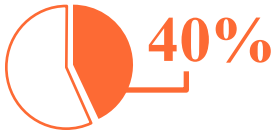
The Anatomy of an Attack Campaign (Attack Kill Chain)



Facts on Attack Campaigns

Did You Know?

Advanced attacks in 2015 used **7 or more toolkits**, less than half exploited a critical vulnerability.



…of advanced attacks in 2015 **did <u>not</u> involve malware**.

…of all Advanced threat attacks **involved DDoS** 2014-2015

Average dwell time of breaches is greater than 200 days.

ARBOR NETWORKS

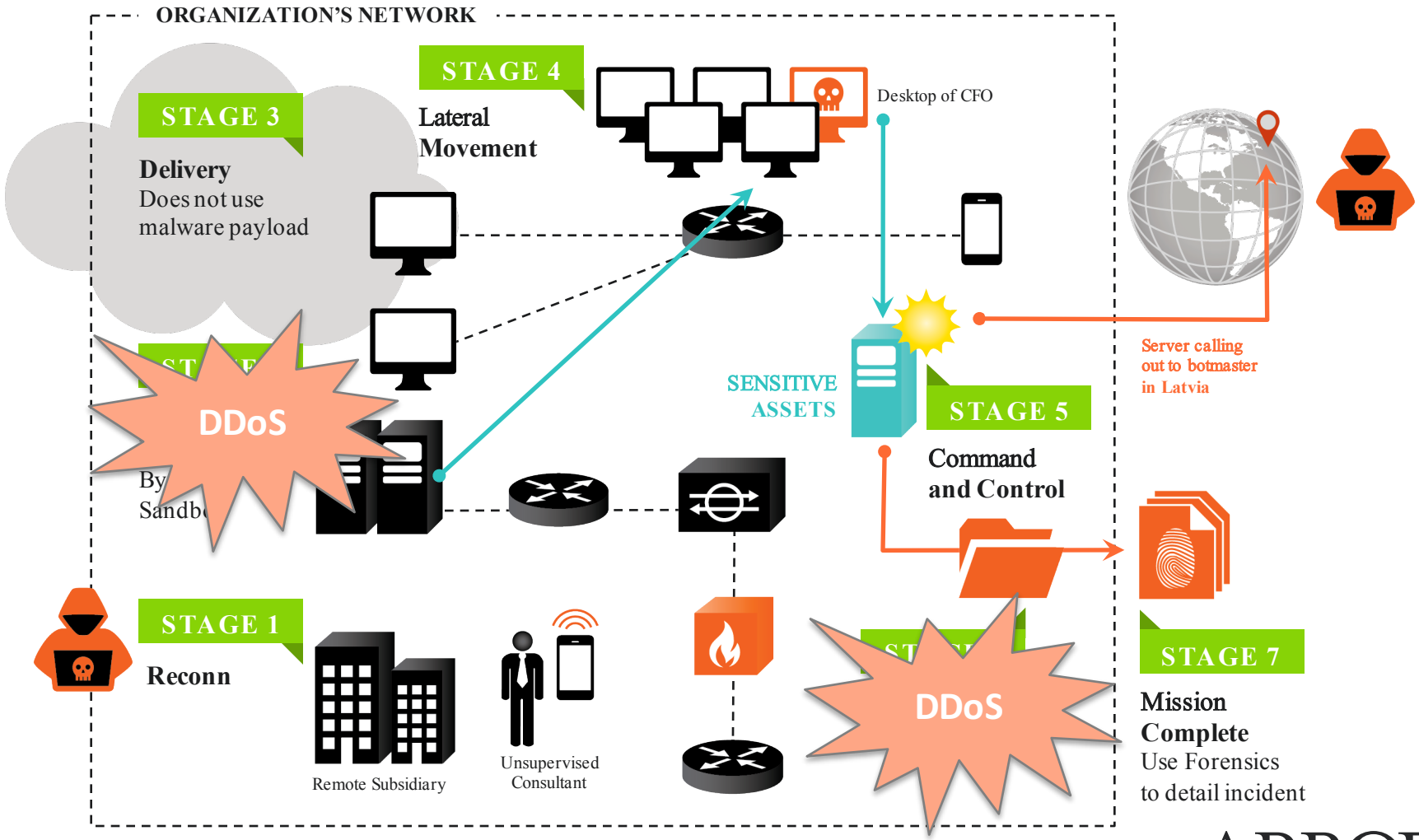
DDoS and APT Partnership

DDoS attacks: a perfect smoke screen for APTs and silent data breaches

- While this chaos is happening, who will keep an eye on web security alerts and incidents? Quite probably nobody

- Log rotation to delete previous records
  - A DDoS attack can overwrite the same volume of log data in several days, deleting all previous records that quite probably contain information about a sophisticated data breach.

DDoS role in Advanced Threat



Advanced Threat Challenges

ARBOR® NETWORKS

Traditional Solutions Challenges – Network Firewall, IPS, Sandbox

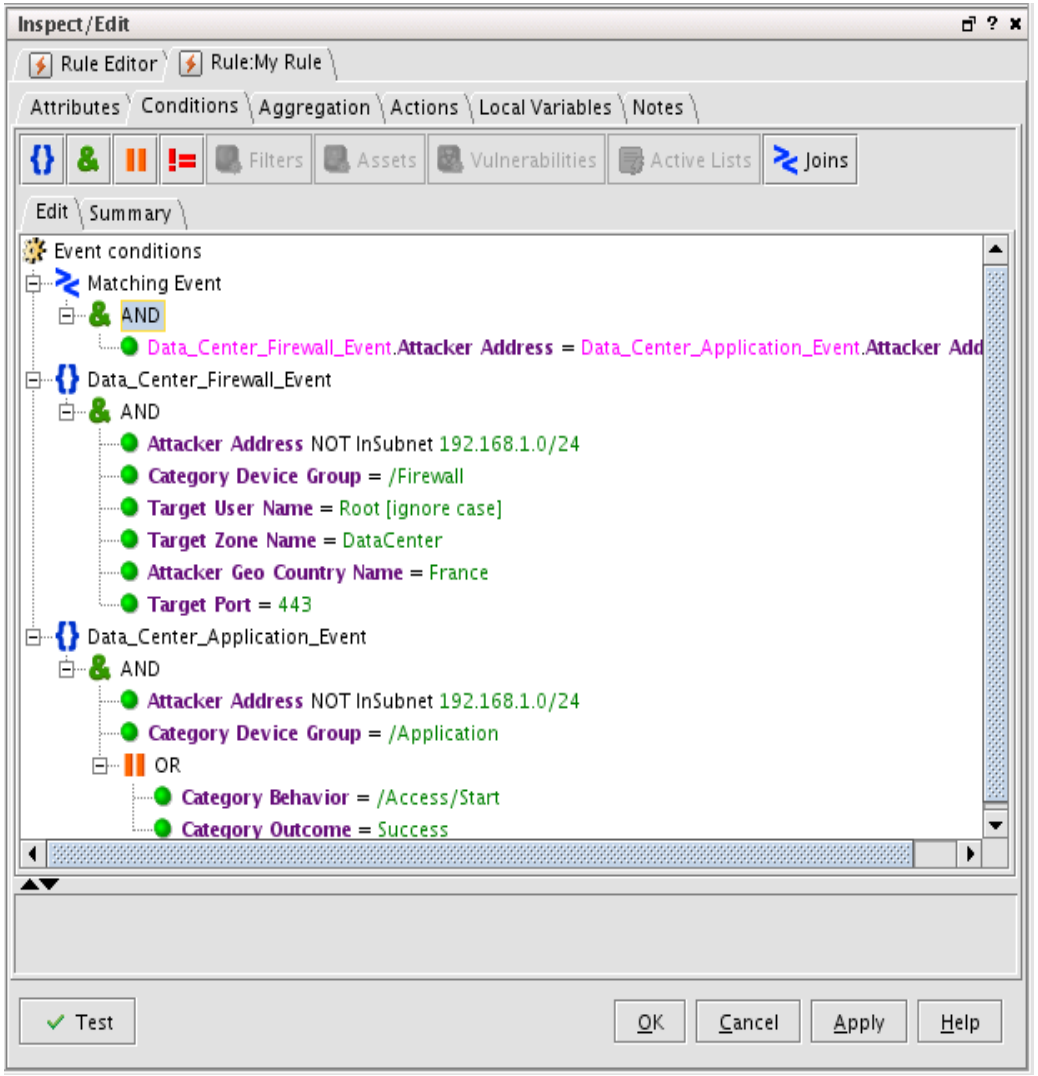
- Overly dependent on in-line deployments **at the edge** with focus blocking based on simple rules
- When deciding to block a session/packet, **no context** to previous sessions, exploits and risk
- Sandboxes overly focus on malware as point of infection => no insight to host behavior
- Often no preserved evidence to help user **ID false positives**

McAfee Intrushield-IPS attack detail report

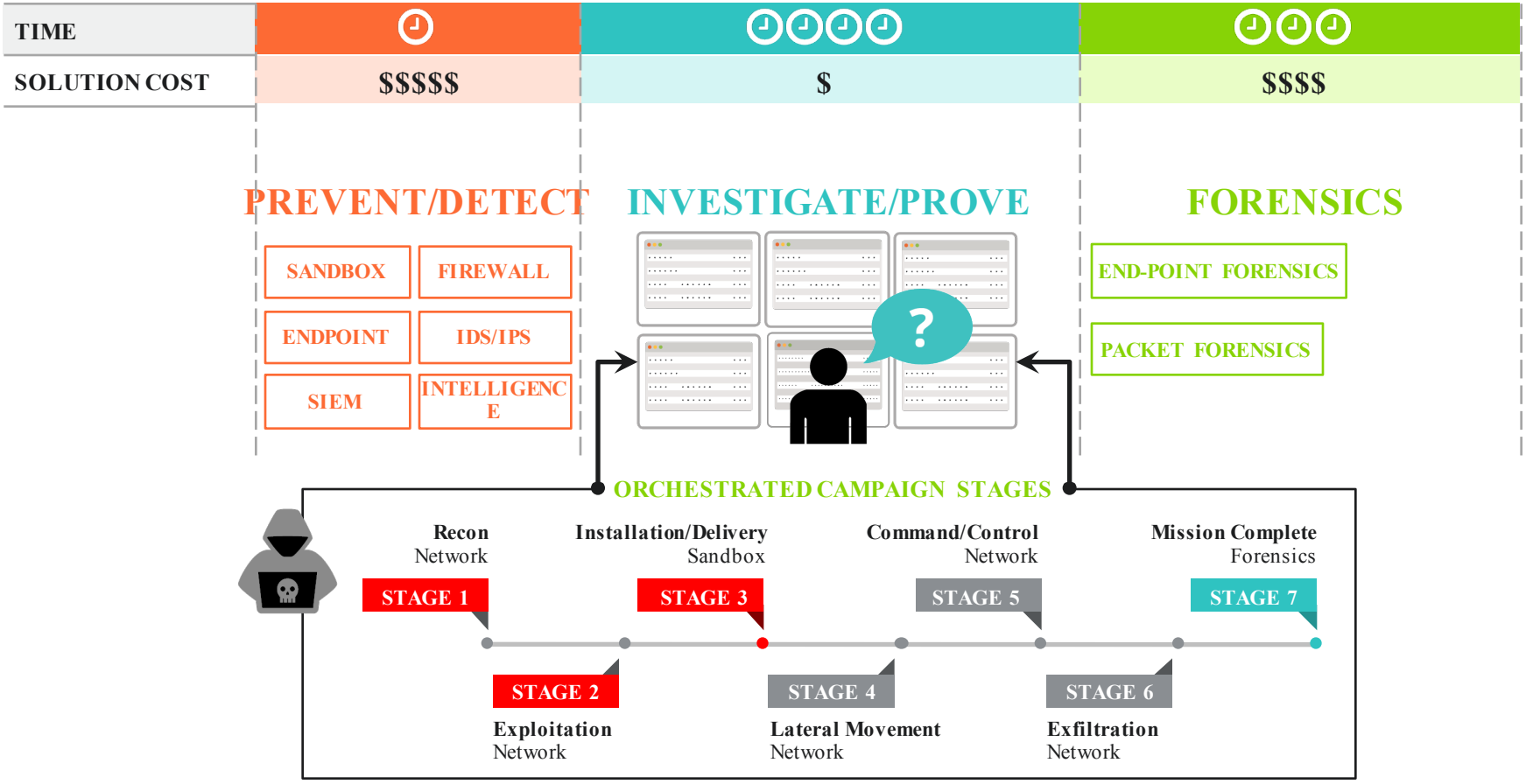
Attack Time	Attack Name	Attack Source	Attack Destination	Attack Category	Attack Sub Category	Attack Severity	Attack Status
1/25/2015 16:05	TCP: Fingerprinting NMAP	192.164.1.77	192.165.7.3	OS Finger	OS Finger Printing	High	Blocked
1/25/2015 17:31	TCP: FIN Port Scan	59.13.12.80	192.165.7.12	port-scan	port-scan	High	Blocked
1/25/2015 18:56	BACKDOOR: Dagger Trojan	1.0.193.27	192.165.7.21	Exploit	Exploit	High	Blocked
1/25/2015 20:22	BACKDOOR: Injector Trojan	59.13.12.10	192.165.7.30	Exploit	Exploit	High	Blocked
1/25/2015 21:47	RADIUS: Access Denied	1.0.193.142	192.165.7.39	Brute Force	Brute Force	High	Blocked
1/25/2015 23:13	SMTP: Worm Spread via Attachment	85.125.23.44	192.165.7.48	Exploit	Exploit	High	Blocked
1/26/2015 00:38	FTP: Login Failed	12.22.124.36	192.165.7.57	Brute Force	Brute Force	High	Blocked
1/26/2015 02:04	TELNET: Login Brute Force	85.125.23.127	192.165.7.66	Brute Force	Brute Force	High	Blocked
1/26/2015 03:29	BACKDOOR: Back orifice Trojan	12.22.124.75	192.165.7.75	Exploit	Exploit	High	Blocked
1/26/2015 04:55	FTP: SITE EXEC Exploit	85.125.23.46	192.165.7.84	Exploit	Exploit	High	Blocked
1/26/2015 06:20	RLOGIN: Password Brute Force	12.22.124.38	192.165.7.93	Brute Force	Brute Force	High	Blocked
1/26/2015 07:46	RADIUS: Authentication Brute Force	59.13.12.85	192.165.7.102	Brute Force	Brute Force	High	Blocked
1/26/2015 09:11	NETBIOS-SS: Virus/Worm File Share Spread	1.0.193.32	192.165.7.111	Service Sweep	Service Sweep	High	Blocked
1/26/2015 10:37	NETBIOS-NS: NBTSTAT Scan	59.13.15.23	192.165.7.120	Service Sweep	Service Sweep	High	Blocked
1/26/2015 12:02	MSSQL: Password Brute Force	1.0.13.23	192.165.7.129	Brute Force	Brute Force	High	Blocked
1/26/2015 13:28	IMAP: Password Brute Force	59.13.12.87	192.165.7.138	Brute Force	Brute Force	High	Blocked
1/26/2015 14:53	ICMP: Host Sweep	1.0.193.34	192.165.7.147	Host sweep	Host sweep	High	Blocked
1/26/2015 16:19	FTP: Login Brute Force	59.13.12.88	192.165.7.156	Brute Force	Brute Force	High	Blocked
1/26/2015 17:44	Over Threshold	1.0.45.253	192.165.7.165	DDos	DDos	High	Blocked

Traditional solutions challenges – SIEM

- Threat detection based on correlated rules that are painful (expensive) to write, prone to false positives & **require you to know how you'll be attacked**
- Visibility limited to logs => **no insights to activity that doesn't produce a log**, such as network connections
- Are your intelligence sources accurate and current?



Gap In Existing Approach



ARBOR NETWORKS

Introducing Arbor Networks Spectrum™

See global attack campaigns in real-time across your entire network.

- Arbor's real-time global threat intelligence harvested from its service provider network is now connected to an organization's internal traffic patterns to detect the most damaging threats, those representing the highest form of risk.

Search and surface anything within the network.

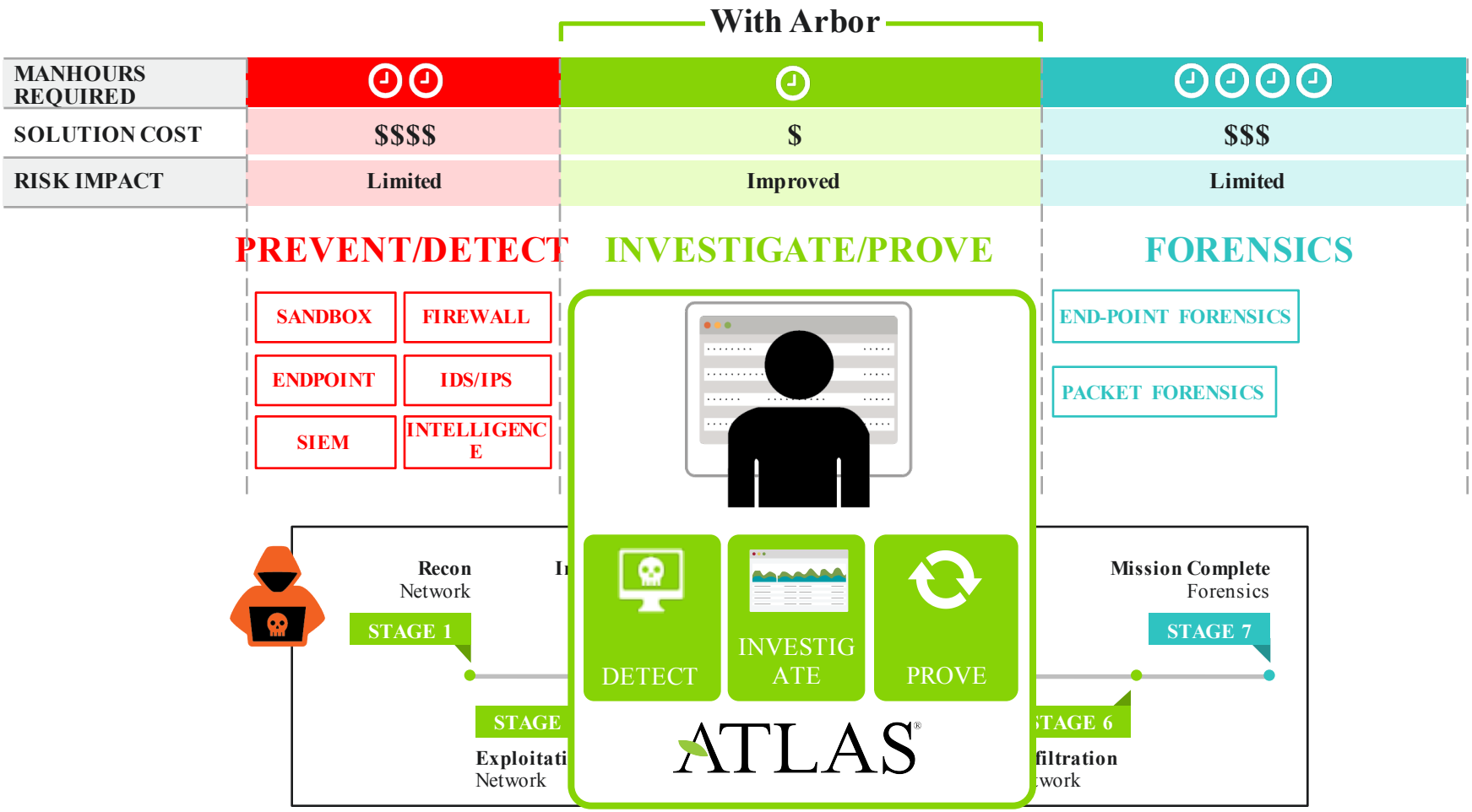
- Disruptive security forensics with complete visibility into all past and present network activity at a fraction of the cost & complexity.

Prove threats on your network faster.

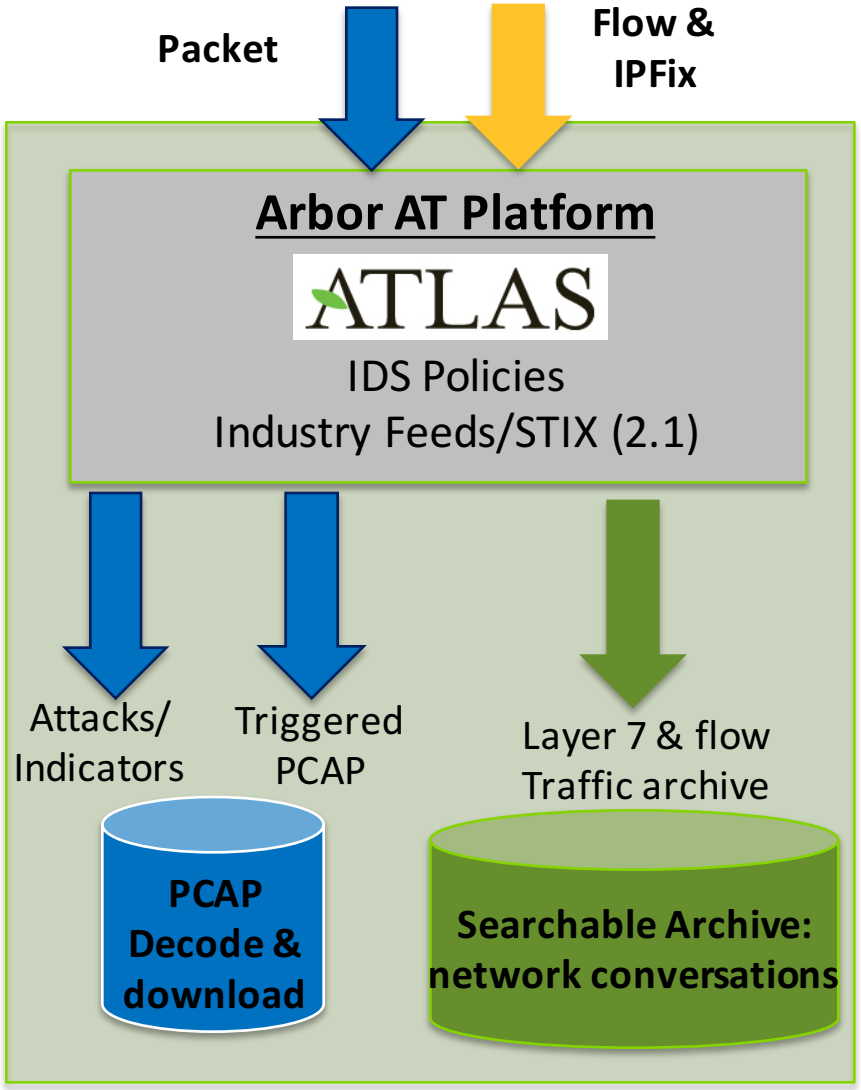
- Designed with the security user in mind, real-time workflows and analytics to empower & scale security teams to investigate and prove threats 10x more efficiently than existing solutions today.

ARBOR® NETWORKS

Why Arbor Spectrum Fills The Gap



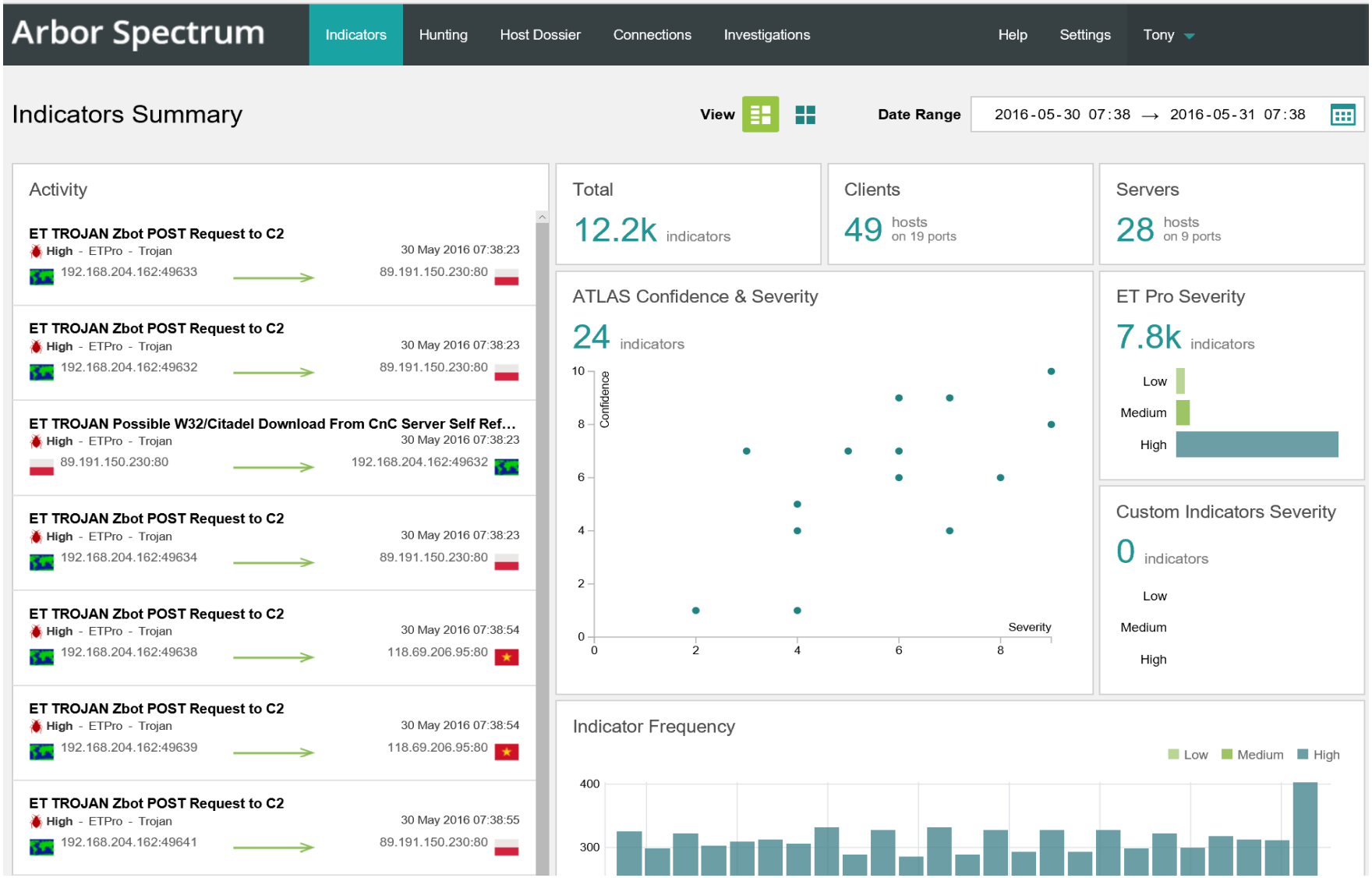
Architecture: Robust Network Archive of Packets & Flow



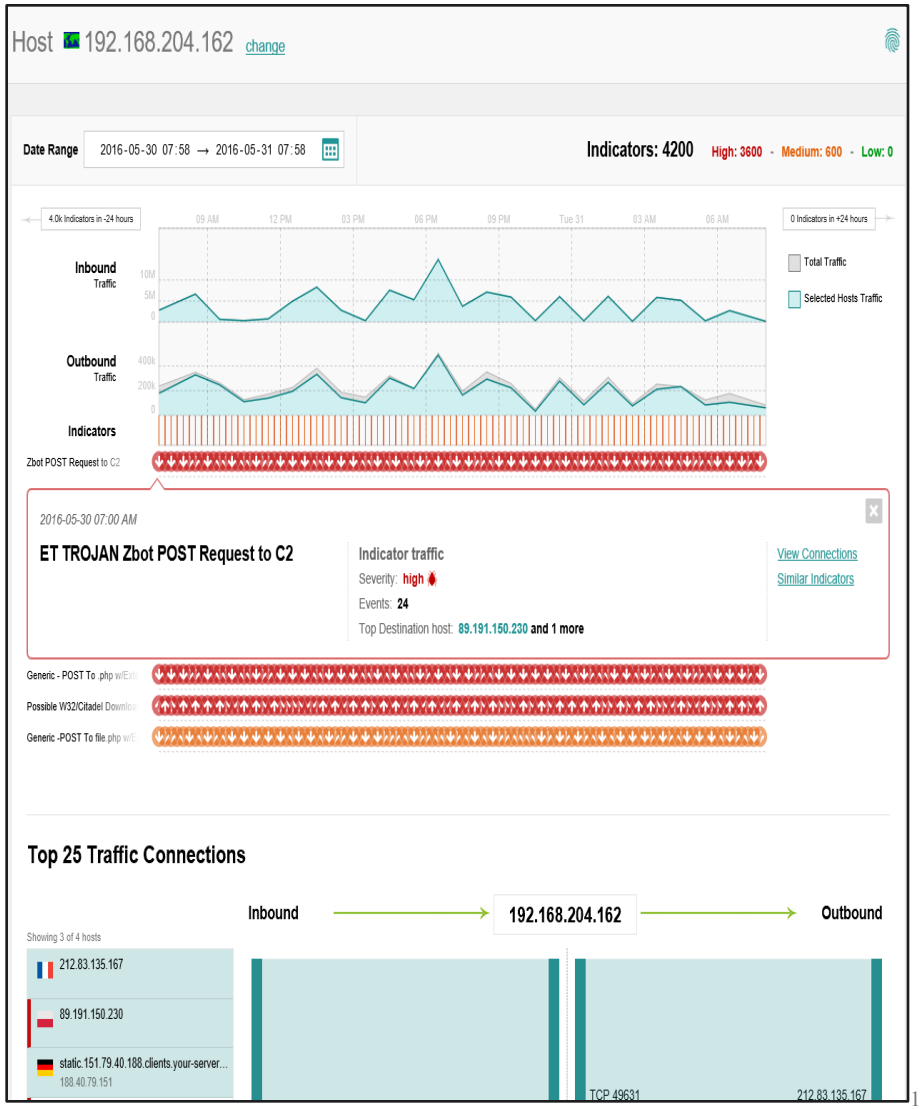
- Incoming packets & flows analyzed for security events
- Attacks/Indicators identified and sent to the controller
- Packet archive
  - Attack/Indicator traffic
  - Triggered packet captures (v2.1)
- Searchable archive: network conversation details
  - URLs, DNS names
  - L3/L4 network header fields (flags)
  - HTTP headers
  - DNS decoded data
  - SSL handshake information (future)
  - File hashes (future)
  - Stream entropy (future)

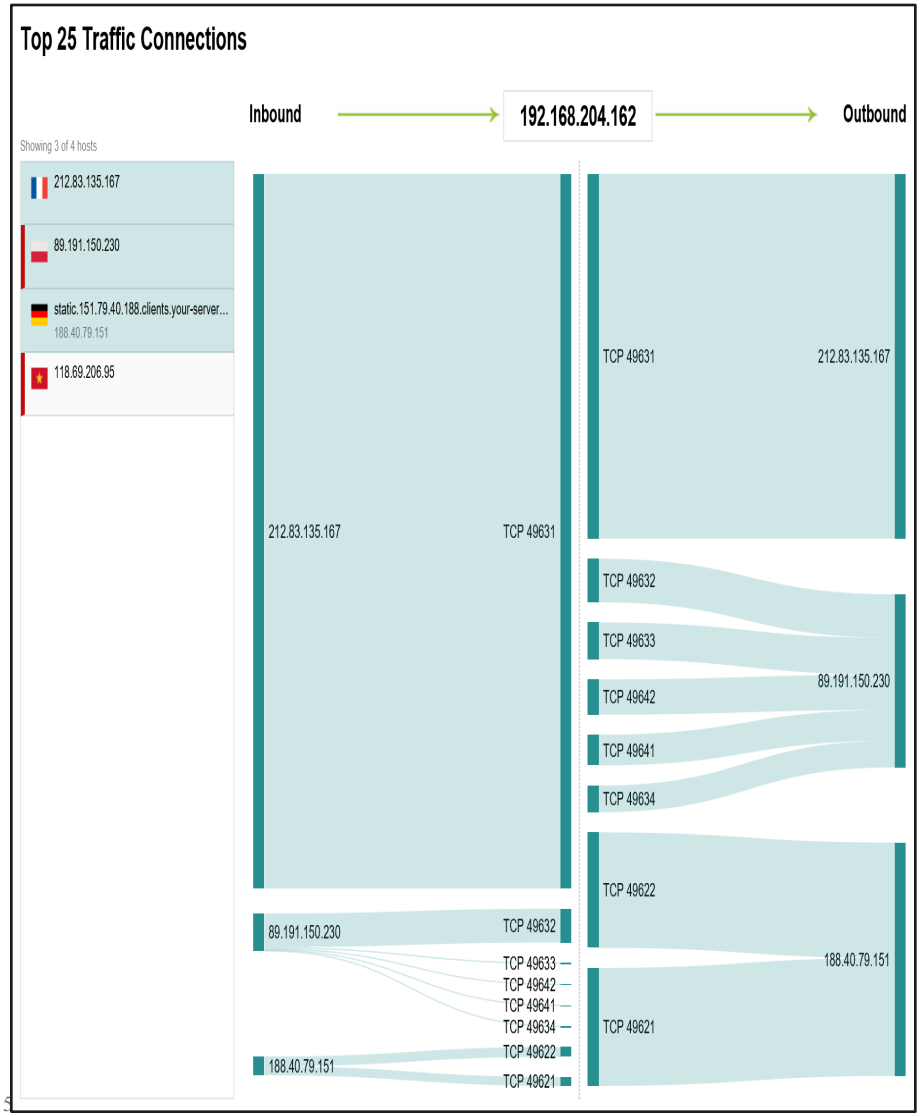
ARBOR NETWORKS

Attack Indicator Summary



Host Dossier: Speed of analysis & context of conversations





Firewall / IPS / SIEM Log

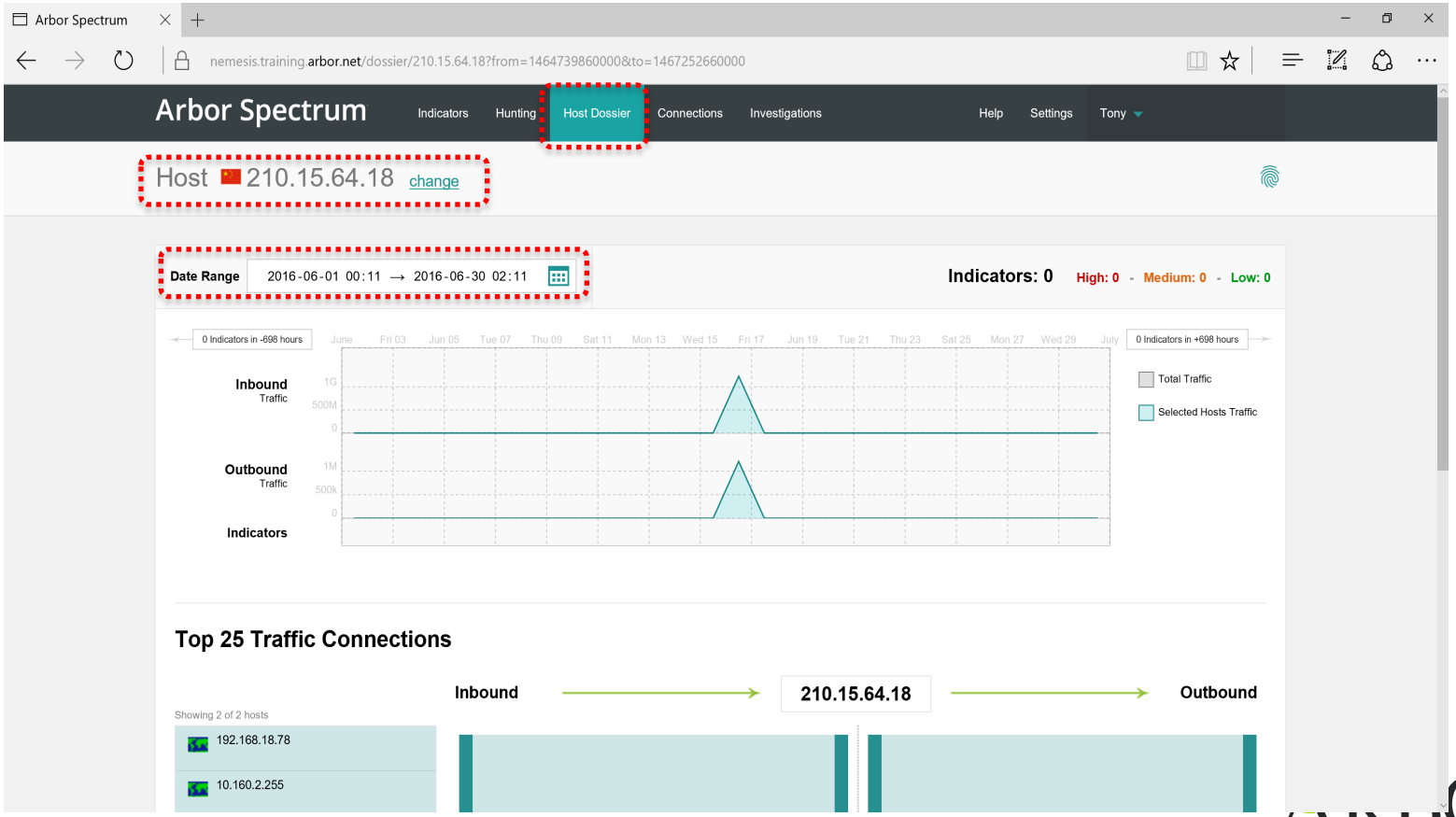
Timestamp	Src IP	Src Port	Dst IP	Dst Port	Protocol	Bytes	Action
Jun 16, 2016 5:25:02	192.168.15.50	2123	10.88.123.8	99	TCP	2K	Drop
Jun 16, 2016 5:26:13	192.168.17.22	4563	202.16.8.11	80	TCP	1K	Permit
Jun 16, 2016 5:28:07	192.168.18.78		210.15.64.18	21	TCP	1G	Permit
Jun 16, 2016 5:29:02	192.168.17.100	5534	10.88.123.8	5533	TCP	200 bytes	Drop
Jun 16, 2016 5:30:50	192.168.22.30	6668	10.88.123.8	5545	TCP	1K	Drop
Jun 16, 2016 5:31:18	192.168.15.51	3112	10.88.123.8	2000	TCP	3K	Drop

How Spectrum can help !?

ARBOR NETWORKS

IR Workflow - Mapping Attack Kill Chain

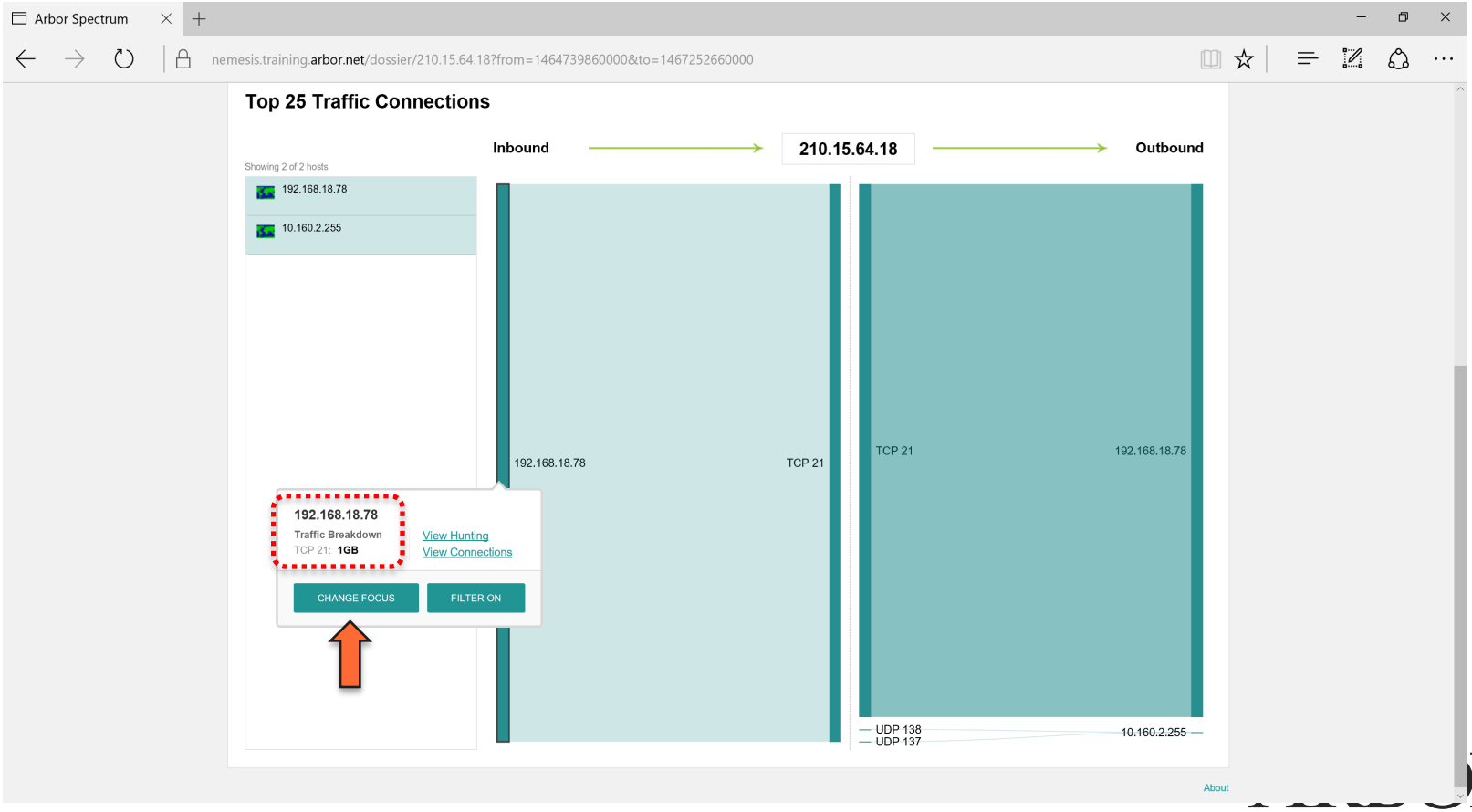
210.15.64.18



IR Workflow - Mapping Attack Kill Chain

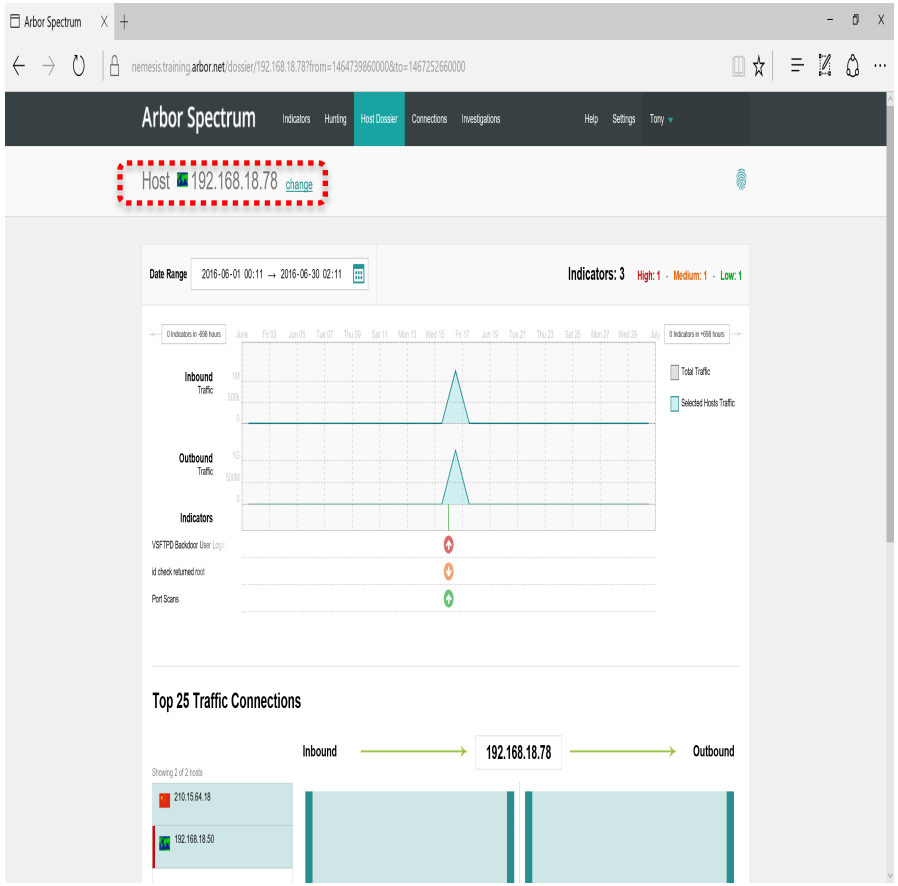
FTP
1Gbps

192.168.18.78 ⟷ 210.15.64.18

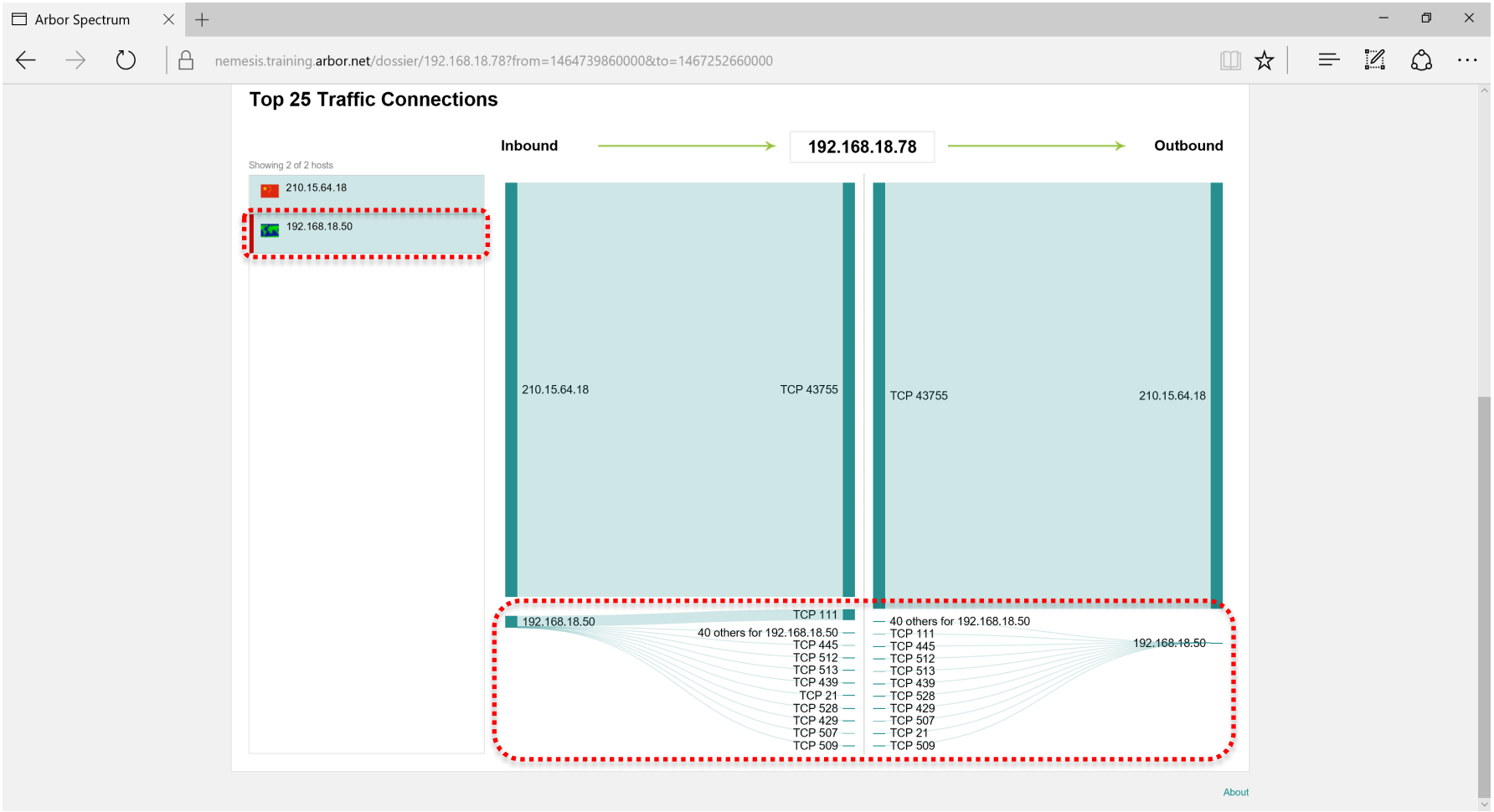


IR Workflow - Mapping Attack Kill Chain

192.168.18.50 <— Port Scans —> 192.168.18.78 <— FTP 1Gbps —> 210.15.64.18

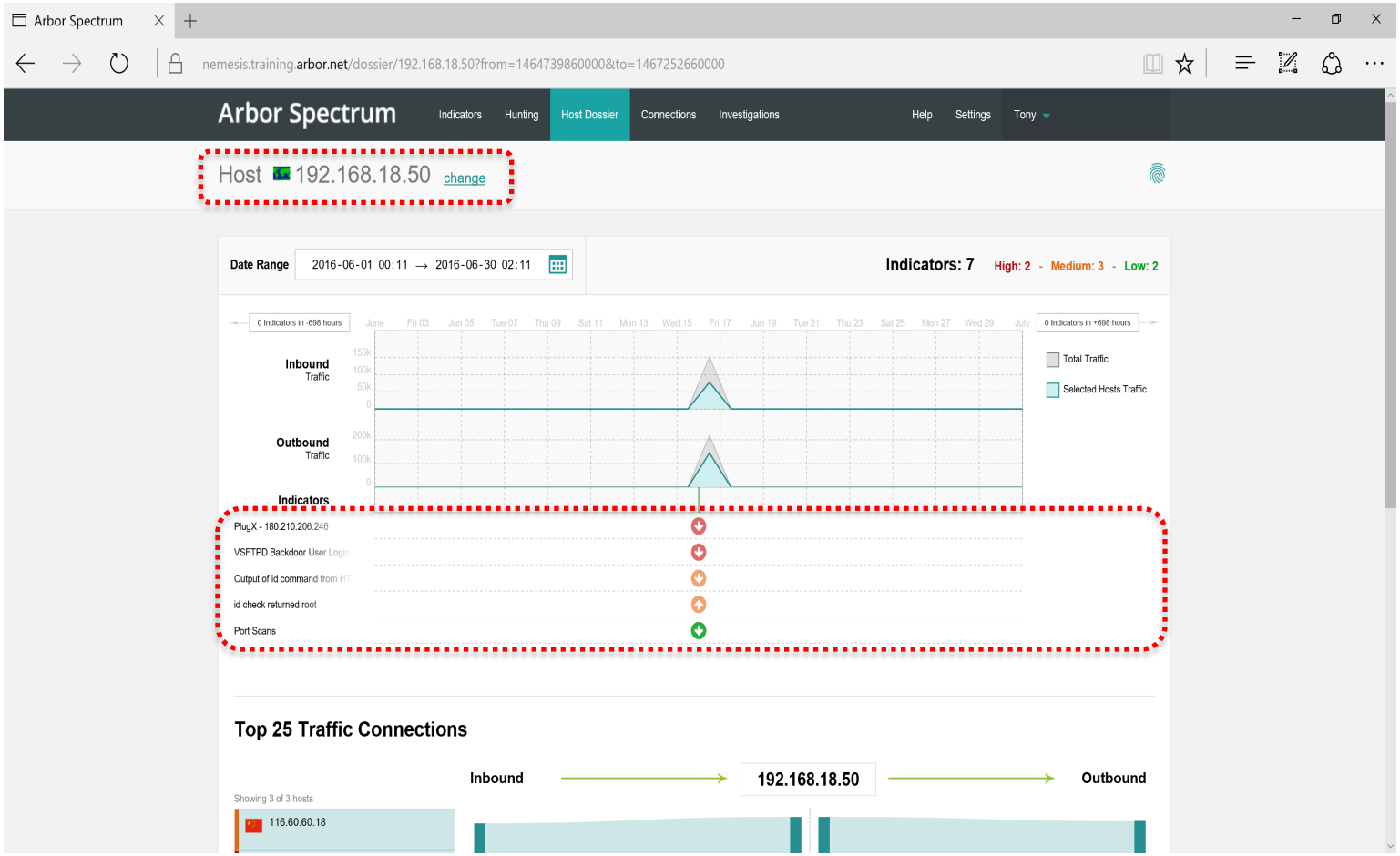


IR Workflow - Mapping Attack Kill Chain



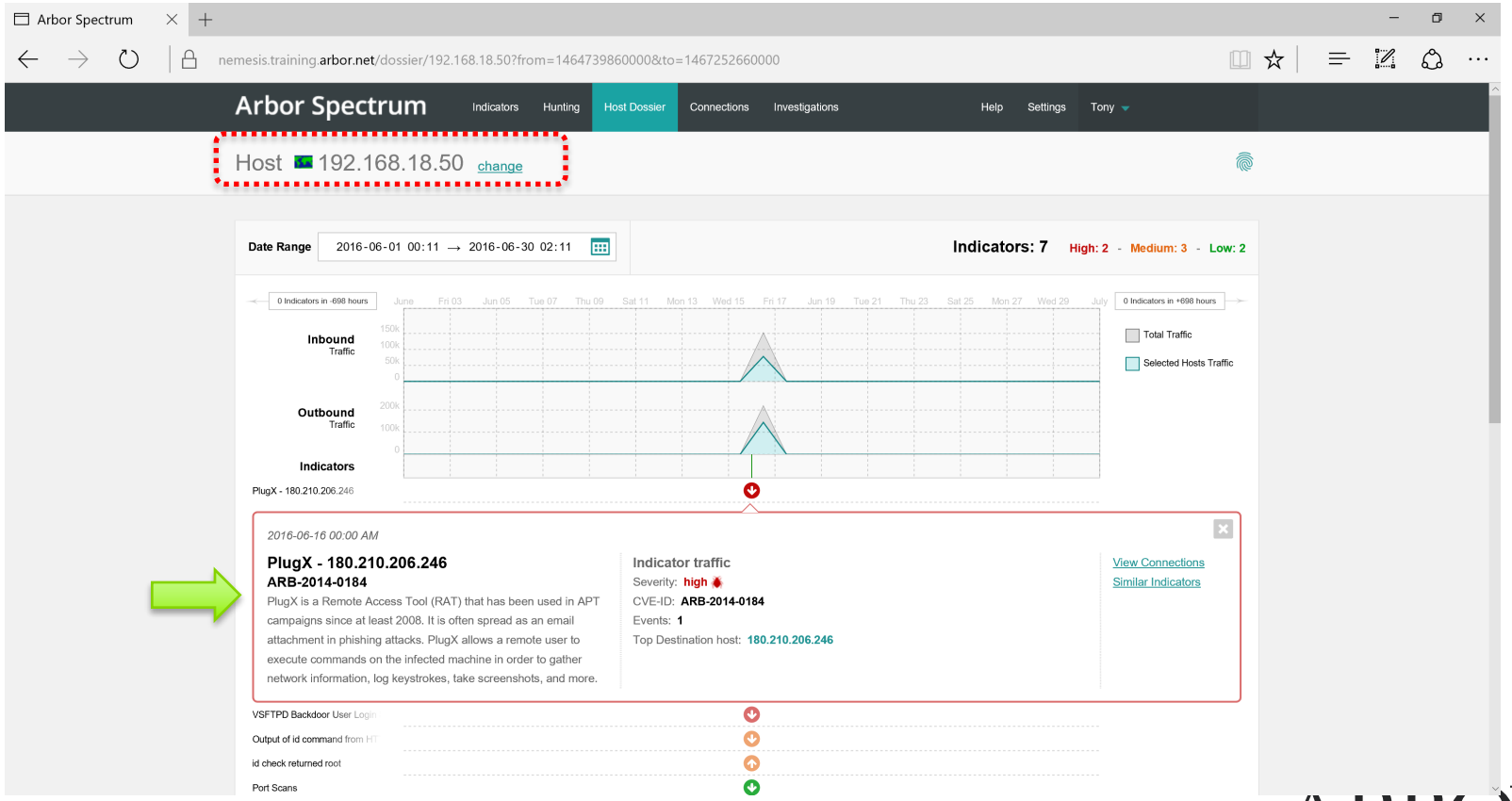
ARBOR NETWORKS

IR Workflow - Mapping Attack Kill Chain

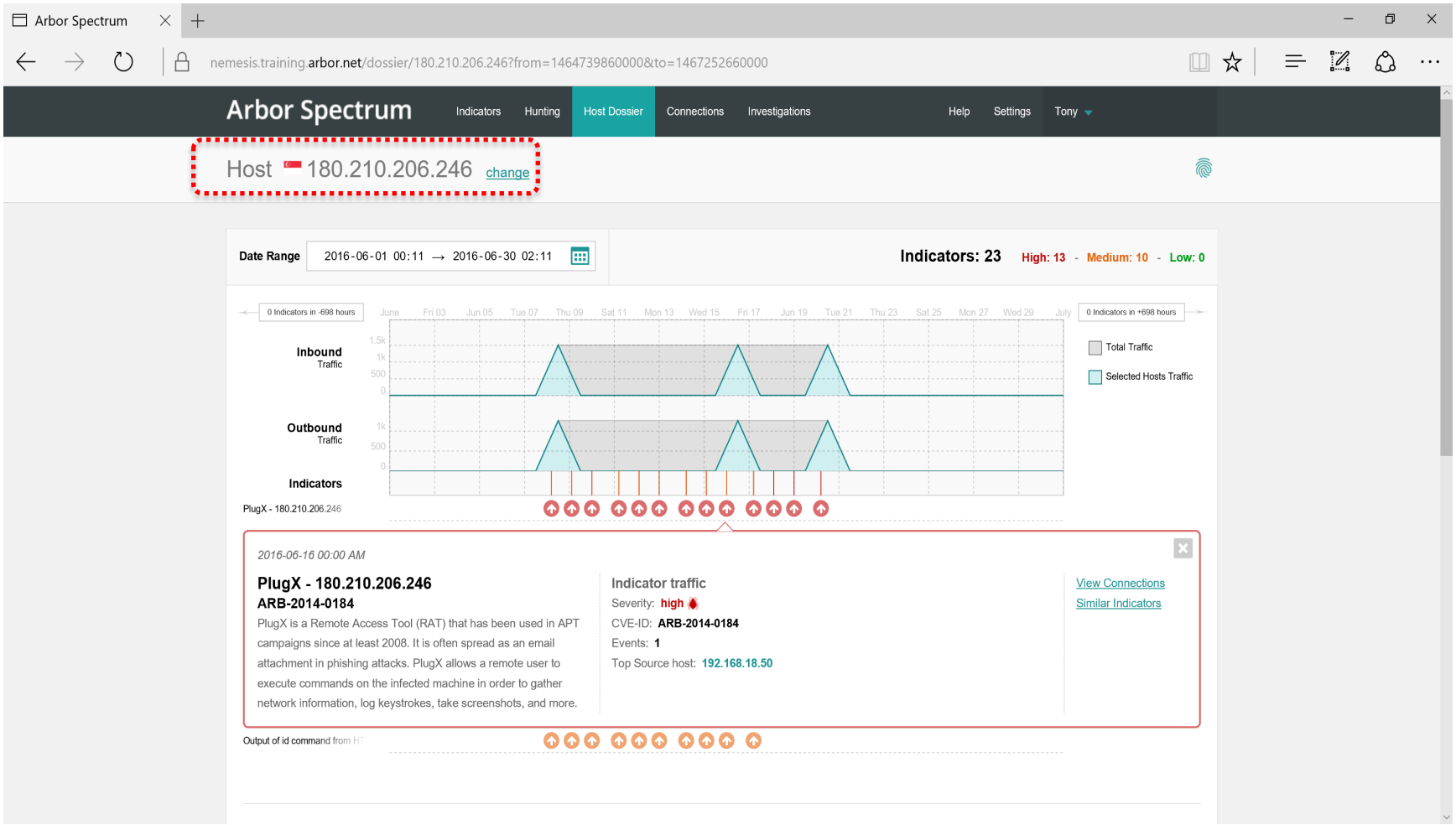


IR Workflow - Mapping Attack Kill Chain

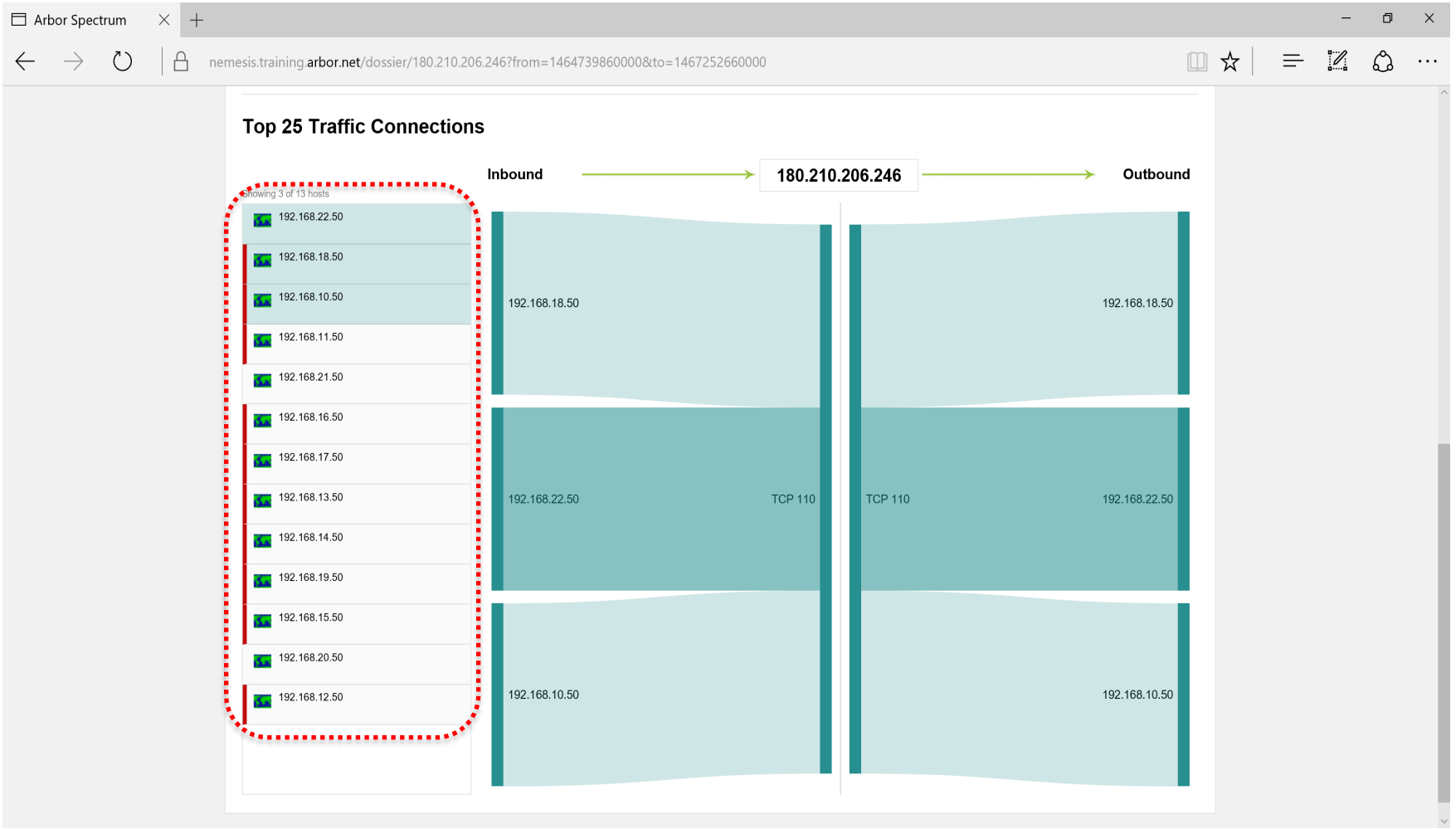
180.210.206.246 —PlugX RAT→ 192.168.18.50 ←Port Scans→ 192.168.18.78 ←FTP 1Gbps→ 210.15.64.18



IR Workflow - Mapping Attack Kill Chain



IR Workflow - Mapping Attack Kill Chain



ARBOR NETWORKS

IR Workflow - Mapping Attack Kill Chain

180.210.206.246 (Internet)

↓ **Delivery/Installation (PlugX RAT)**

192.168.10.50 , 192.168.11.50, 192.168.12.50, 192.168.13.50, 192.168.14.50, 192.168.15.50, 192.168.16.50, 192.168.17.50, 192.168.19.50, 192.168.20.50, 192.168.21.50, 192.168.22.50, 192.168.18.50 **Jump server**

↓ **lateral movement**

192.168.18.78

↓ **data transfer – Kill Chain completed**

210.15.64.18 (Internet)

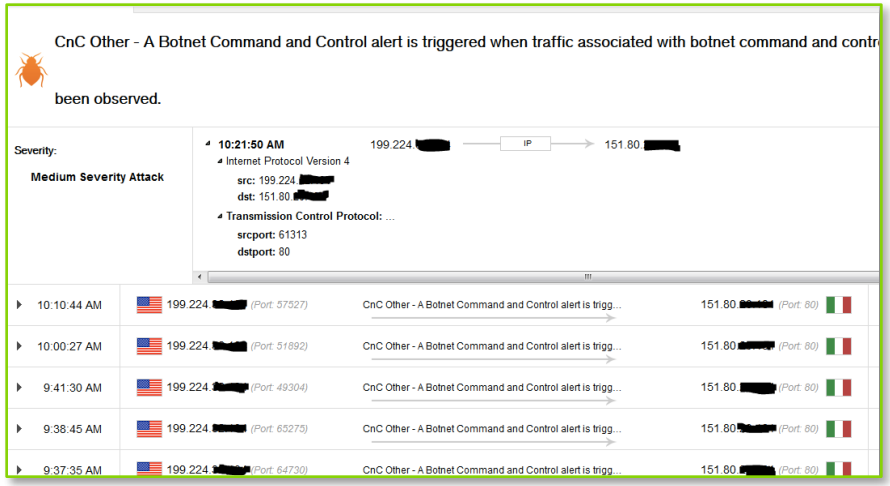
Case Study: Detection & Proof of an Attack Campaign in Minutes

Challenge:

- Small Security Operations function responsible for managing events and incidents across a large, distributed network with global data centers.
- Deployed SIEM, Security forensics and used 3 open source and other tools to detect and investigate incidents.

Arbor:

- Deployed Arbor within a day and received one hour of training. Within the same day the team was using the solution to find and investigate potential threats.
- Almost immediately a threat indicator was detected using Arbor Intelligence.
- Further analysis of the traffic, and subsequent hosts implicated.
- Investigation took minutes whereas the team would normally take 3-4 days to perform a similiar analysis.
- Their SIEM and existing threat infrastructure had not identified the initial threat indicator.



"The best thing about Arbor Spectrum is that you really don't even need a novice skill level of network forensics to use it. The interface is straightforward, and it's simple to extract important information relevant to an investigation."

– Security Operations Lead F500 Multinational

ARBOR NETWORKS

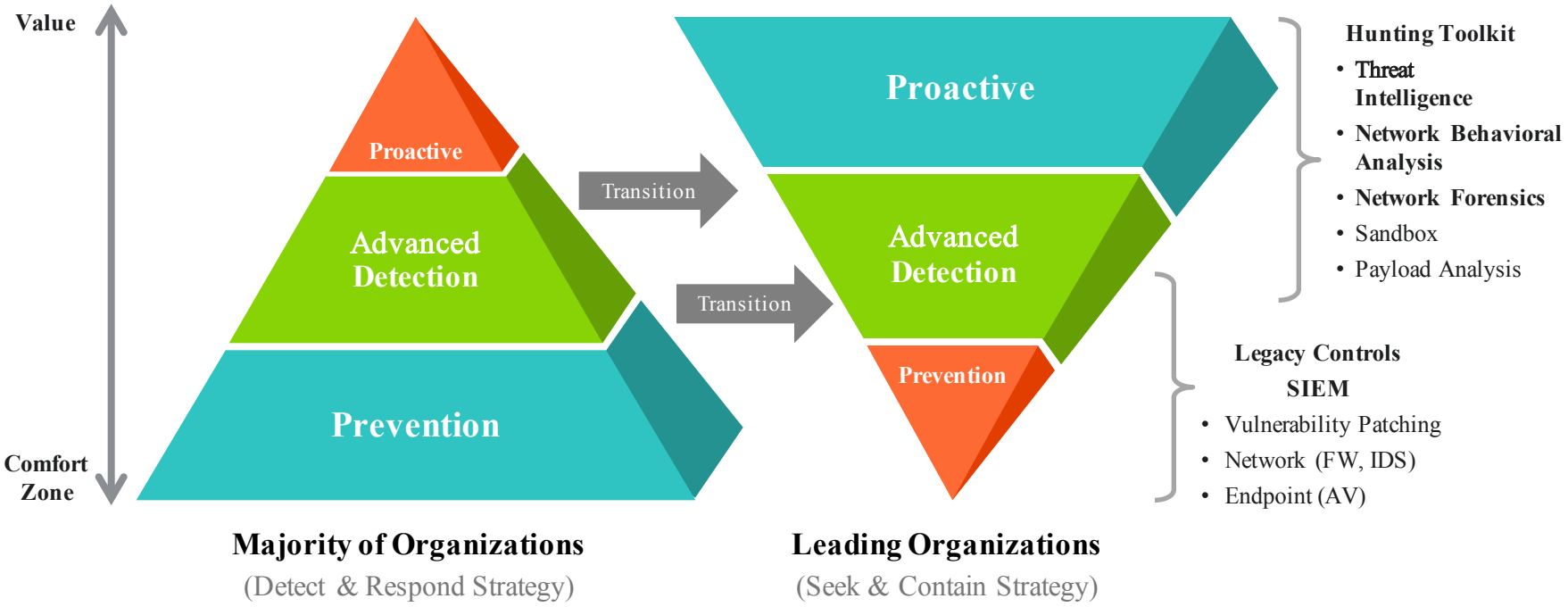
The Numbers:
Investigations per 8-Hour Shift

	Today	With Arbor Spectrum
Senior Incident Responder	3	30+
Mid-level Analyst	0	10-20
Junior Analyst	0	5-10
Network Engineer	0	3-5

ARBOR NETWORKS

Compromise is Inevitable, Data Loss is Not

Attackers only Need to Win <u>ONCE</u>, We Need to Win <u>EVERY TIME!</u>



ARBOR NETWORKS

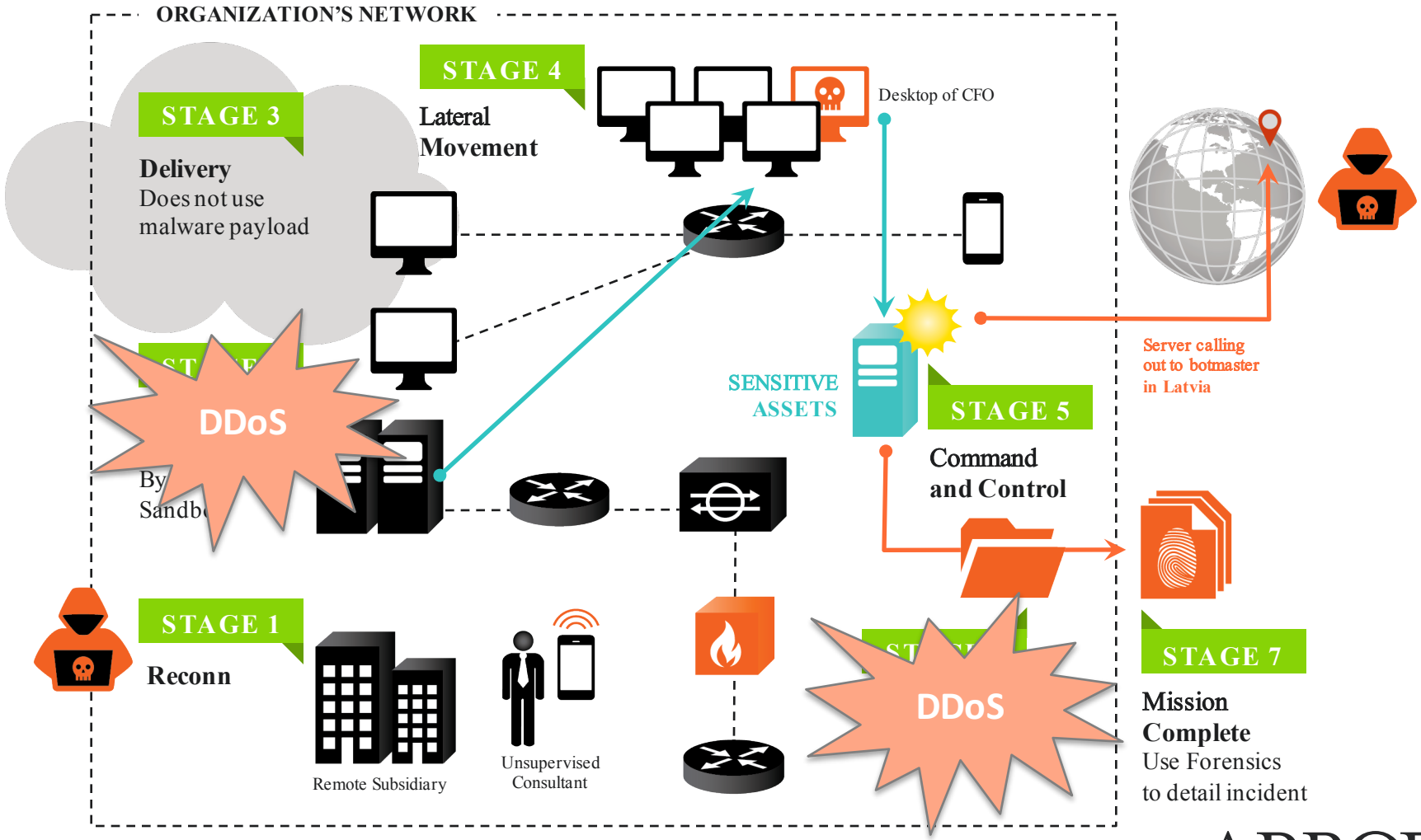
Do you want to be
The Hunter

Or do you want to be
The Hunted

Distribute Denial of Service

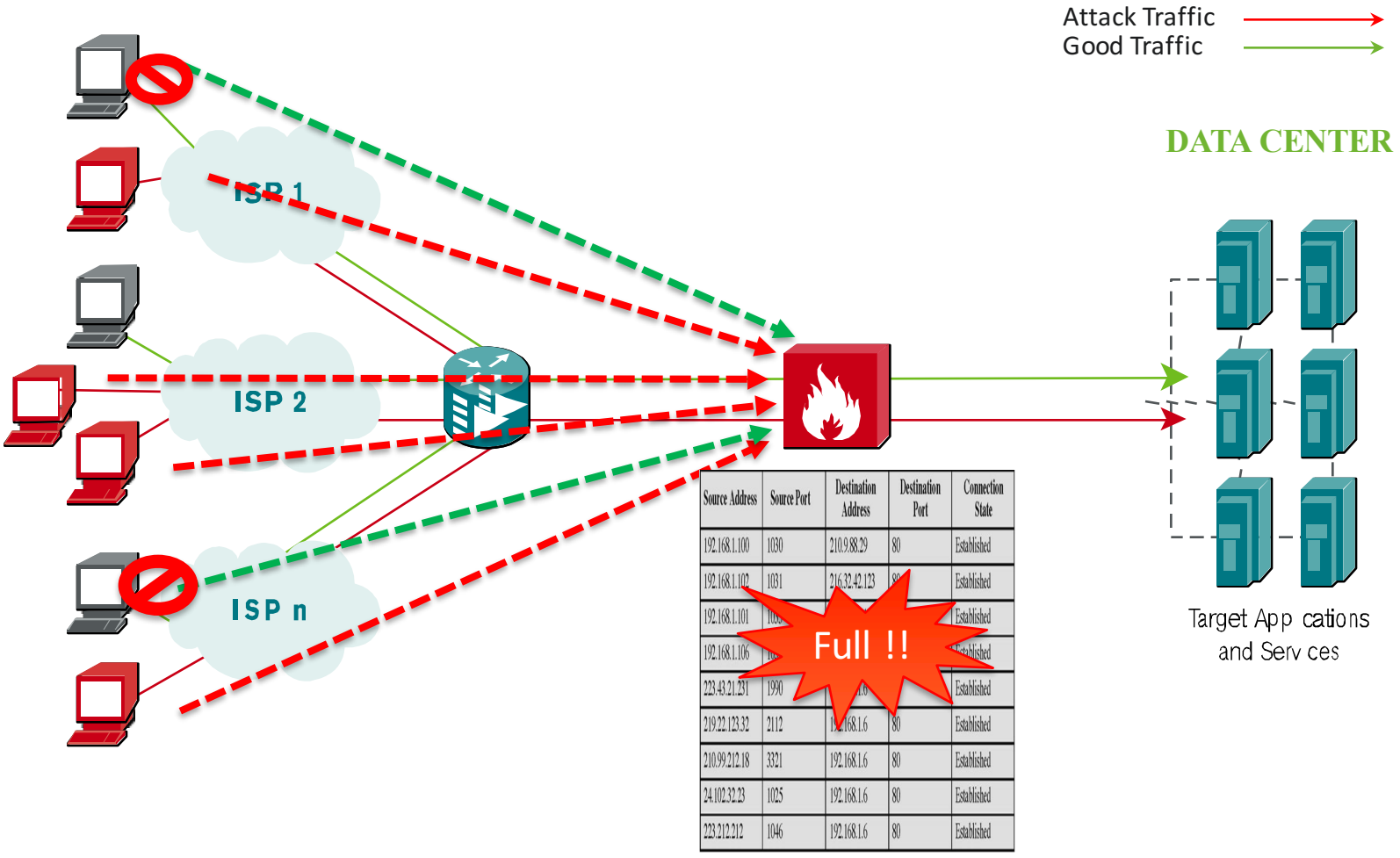
ARBOR NETWORKS

DDoS role in Advanced Threat



ARBOR NETWORKS

STATE EXHAUSTION DDOS ATTACK



Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033			Established
192.168.1.106	1035			Established
223.43.21.231	1990			Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.212.212	1046	192.168.1.6	80	Established

ARBOR NETWORKS

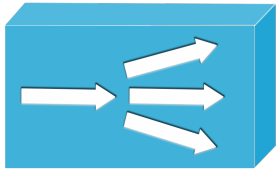
STATEFUL DEVICE ?

Firewall

WAF

IPS

Anti-DDoS



Load Balancer

ARBOR NETWORKS

STATEFUL DEVICE ?

PERFORMANCE AND CAPACITIES[1]	PA-5060	PA-5050	PA-5020
Firewall throughput (App-ID enabled)	20 Gbps	10 Gbps	5 Gbps
Threat prevention throughput	10 Gbps	5 Gbps	2 Gbps
IPSec VPN throughput	4 Gbps	4 Gbps	2 Gbps
Max sessions	4,000,000	2,000,000	1,000,000
New sessions per second	120,000	120,000	120,000
IPSec VPN tunnels/tunnel interfaces	8,000	4,000	2,000
GlobalProtect (SSL VPN) concurrent users	20,000	10,000	5,000
SSL decrypt sessions	90,000	45,000	15,000
SSL inbound certificates	1,000	300	100
Virtual routers	225	125	20
Virtual systems (base/max2)	25/225*	25/125*	10/20*
Security zones	900	500	80
Max. number of policies	40,000	20,000	10,000

Scale and Performance	BIG-IP 10050s/10250v	BIG-IP 7050s/7250v	BIG-IP 5050s/5250v
Maximum firewall throughput	80 Gbps	40 Gbps	30 Gbps
Connections per second	850,000	370,000/ 750,000	670,000/ 330,000
Maximum concurrent connections	36 million	22 million	22 million

Scale and Performance	BIG-IP 4000s/4200v	BIG-IP 2200s/2000s
Maximum firewall throughput	10 Gbps	5 Gbps
Connections per second	130,000/ 250,000	135,000/ 67,000
Maximum concurrent connections	9 million/ 10 million	5 million/ 4.5 Million

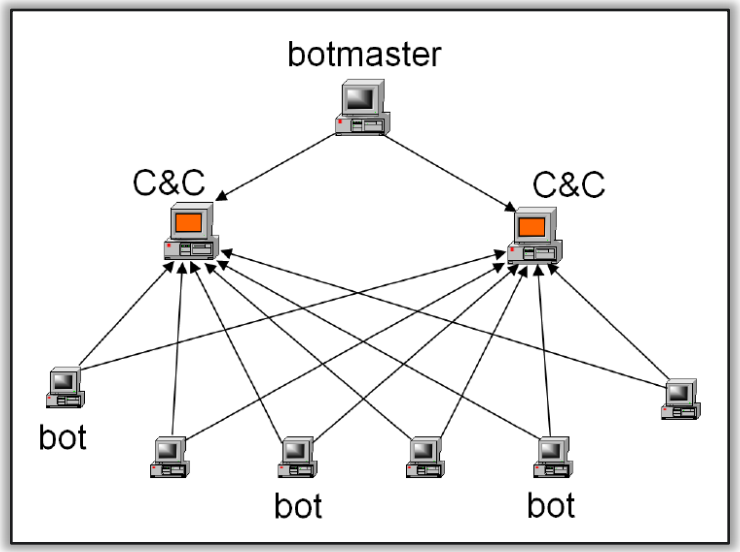
10 Gigabit Ethernet Connectivity

Sensor Hardware Components	M-8000	M-6050	M-4050	M-3050	M-2950	M-2850	M-1450	M-1250
Performance								
Real-World Throughput	10 Gbps	5 Gbps	3 Gbps	1.5 Gbps	1 Gbps	600 Mbps	200 Mbps	100 Mbps
Maximum Throughput (UDP 1512 Byte Packets)	Up to 20 Gbps	Up to 10 Gbps	Up to 4 Gbps	Up to 2.5 Gbps	Up to 1.5 Gbps	Up to 1 Gbps	Up to 300 Mbps	Up to 150 Mbps
Maximum Concurrent Connections	4,000,000	2,000,000	1,500,000	750,000	750,000	750,000	80,000	40,000
TCP Connections per Second	250,000	125,000	75,000	38,000	31,500	20,800	8,300	4,150
HTTP Connections per Second	120,000	60,000	36,000	18,000	15,000	10,000	4,000	2,000

ARBOR NETWORKS

BOTNET SIZES

Marina – 6 million Bots
Mariposa – 12 million Bots
ZeroAccess – 1.9 million Bots
Storm – up to 50 million Bots
Cutwail – 1.5 million Bots
Conficker – 10.5 million Bots
BredoLab – 30 million Bots
TDL4 – 4.5 million Bots
Ramnit – 3 million Bots
Akbot – 1.3 million Bots
Grum – 560,000 Bots
Mega-D – 509,000 Bots
Kraken – 500,000 Bots
Srizbi – 450,000 Bots



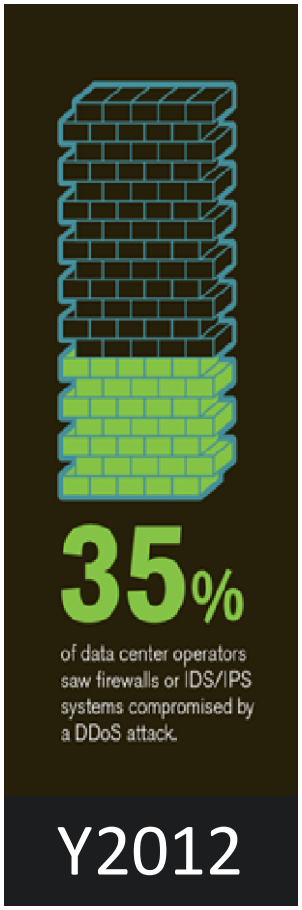
10 x 3 = 30

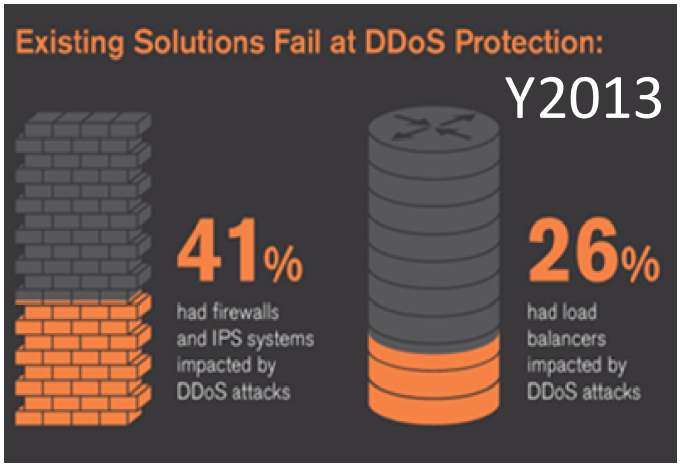
Connection **million** **million**

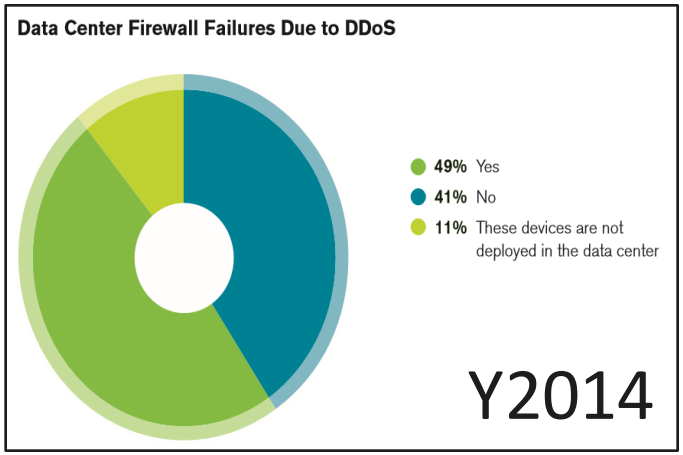
ARBOR NETWORKS

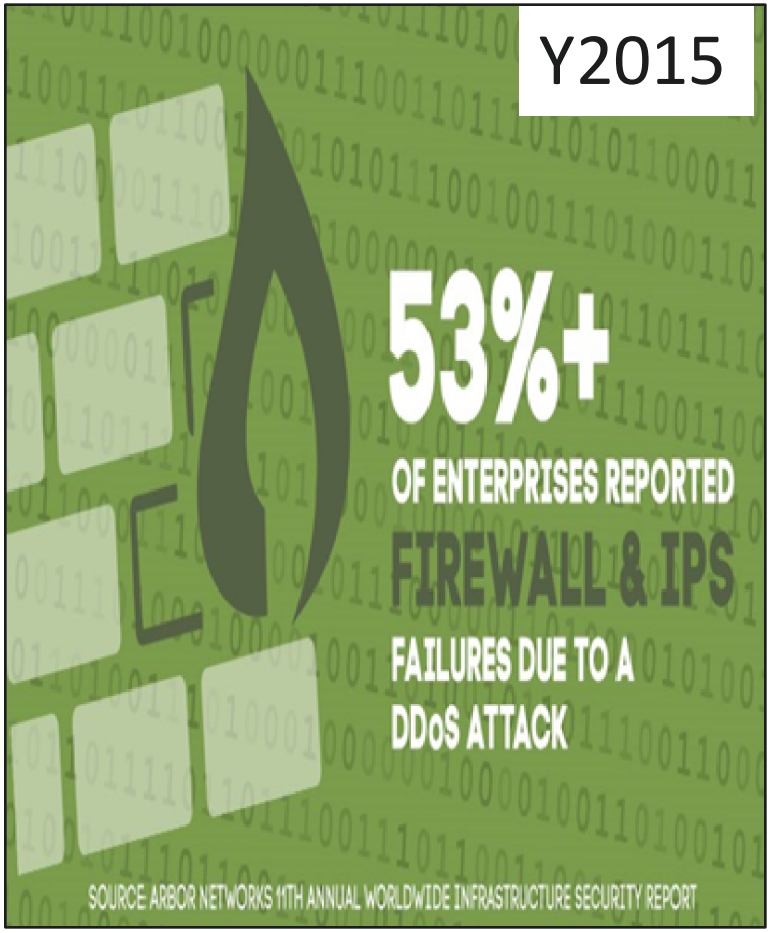
ARBOR WISR STATISTICS

Firewall, IPS FAILED during DDoS Attacks









Source: Arbor Networks Annual Worldwide Infrastructure Security Report

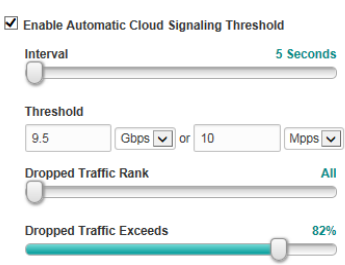
ARBOR NETWORKS

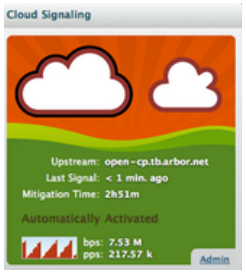
ON-PREMISE: ARBOR AVAILABILITY PROTECTION SYSTEM (APS)

- **Always On, In-Line Protection** from network & application layer DDS attacks and advanced threats
- **In-bound and Out-bound** threat identification and mitigation
- **Mitigation platforms and capacities** ranging from 2U appliances (1Gbps-40Gbps) to virtual (sub 1Gbps)
- **One-Box SSL Inspection** to protect against malicious attacks embedded into encrypted traffic with SSL Card
- **Intelligent communication through Cloud Signaling**[SM] between APS and Arbor Cloud for comprehensive DDoS protection
- **ATLAS Intelligence Feed (AIF)** continuously arms APS with global, actionable threat intelligence
- **Managed APS (mAPS)** for optimized DDoS protection

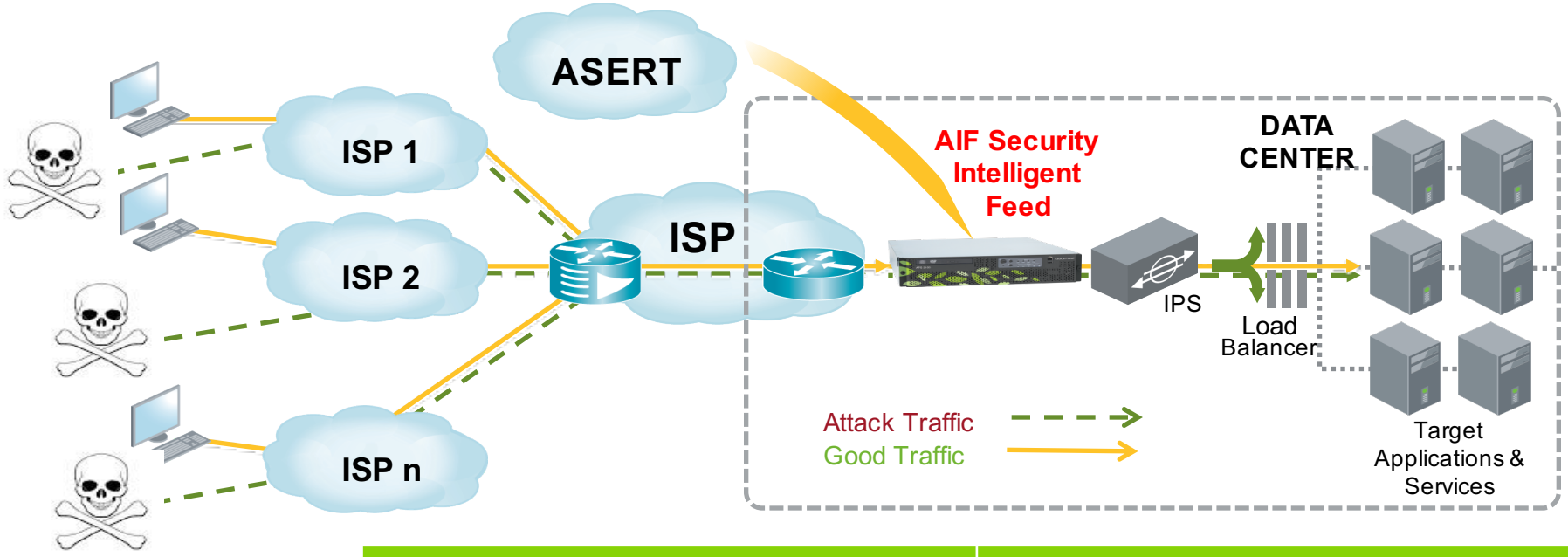
Appliances

Virtual



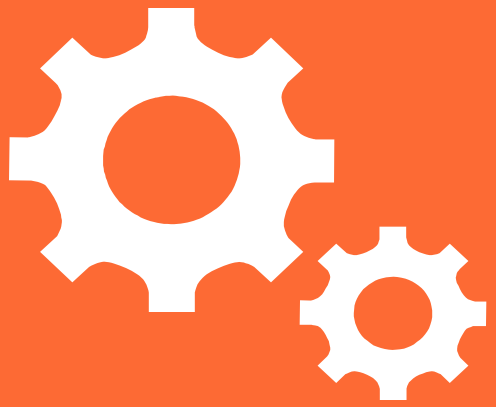


DDoS Campaigns & Advanced Threats



AIF BASIC	AIF ADVANCED
DDoS Threats	Location Based Threats
IP Geo-Location	Email Threats
Web Crawler Identification	Targeted Attacks / Campaigns
Command and Control	Mobile
Malware	

ARBOR ADVANTAGE



PROVEN, TRUSTED DDoS PROTECTION

107 countries

Where Arbor Networks solutions are deployed

15 years

Delivering security and network visibility innovation

Global traffic visibility

Hundreds of terabits of global Internet traffic intelligence

55% of revenue

From Global Customers in Asia, Europe and Latin America.

#1 provider

DDoS mitigation to Carrier, Enterprise and Mobile, IHS Infonetics, June 2015

5 Olympic games

Protected by Arbor Networks

90%+ of the world's

Tier 1 service providers

8 of the 10 largest

Cloud service providers

9 of the 10 Largest

Managed security service providers

3 of the 5 Largest

Social media networks

5 of the 6 Largest

U.S. cable broadband providers

4 of the Top 6

U.S. banks based on assets under management

ARBOR NETWORKS

PROVEN, TRUSTED DDoS PROTECTION

1 of 10 Most Brilliant DARPA Inventions

Alongside the Internet itself

PC PRO MAGAZINE

Best Example of DDoS Protection

Praised by U.S. Department of Homeland Security's Doug Maughan, Director, Cyber Security Division

2014 CENTRE FOR SECURE INFORMATION TECHNOLOGIES CONFERENCE

Recognized Authority

Arbor was one of two companies to testify before the European Union on the subject of "Protecting Europe Against Large-Scale Cyber-Attacks."

Arbor Networks Secures Three New Patents for DDoS Detection & Mitigation

June 30, 2015 09:00 AM Eastern Daylight Time

BURLINGTON, Mass.--(BUSINESS WIRE)--Arbor Networks, Inc., a leading provider of DDoS and advanced threat protection solutions for enterprise and service provider networks, today announced three additional patents for different aspects of distributed denial-of-service (DDoS) attack detection and mitigation. Arbor has now secured 25 patents focused on DDoS defense.

Since Arbor's founding, research and innovation has been at the heart of what the company does. The Lighthouse Project was established out of the University of

"That focus on innovation and our institutional knowledge will

ARBOR NETWORKS

Release Summary

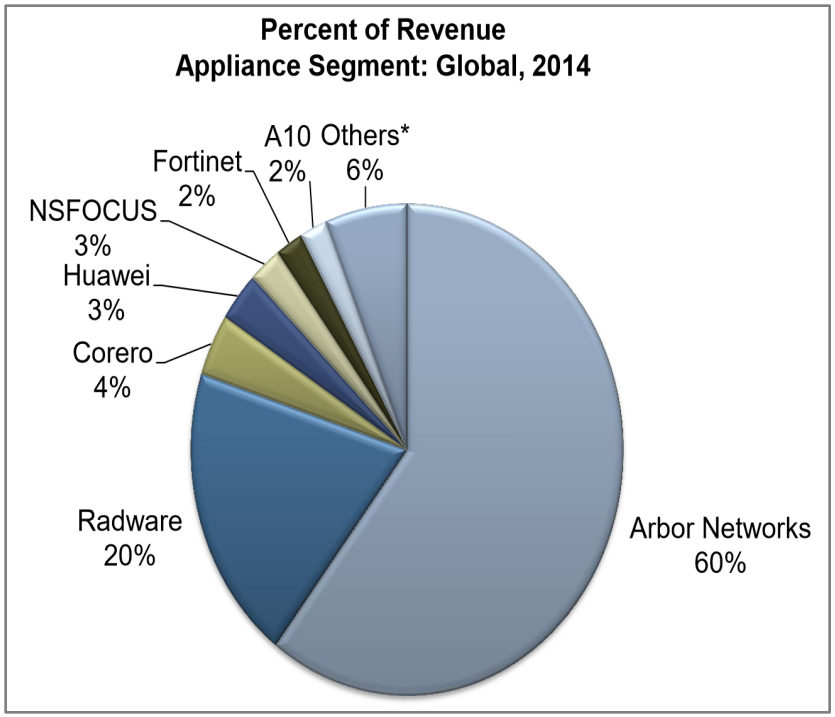
Arbor Networks today announced three additional patents for different aspects of DDoS attack detection and mitigation. Arbor has now secured 25 patents focused on DDoS

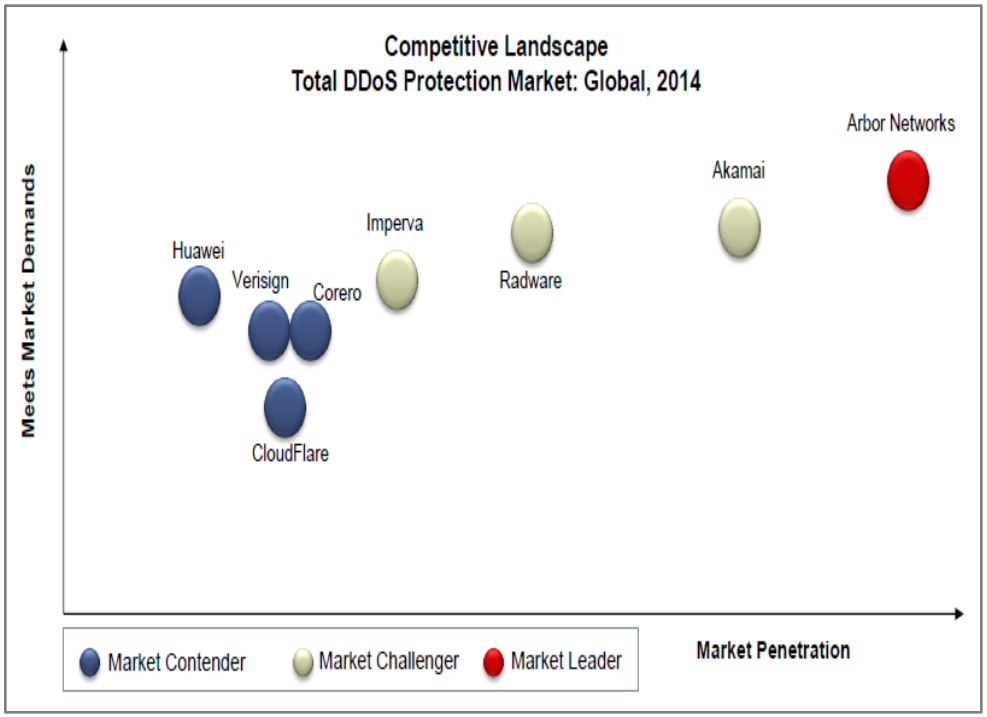
Sharing

"Arbor has now secured 25 patents focused on DDoS"

ARBOR NETWORKS

PROVEN, TRUSTED DDoS PROTECTION



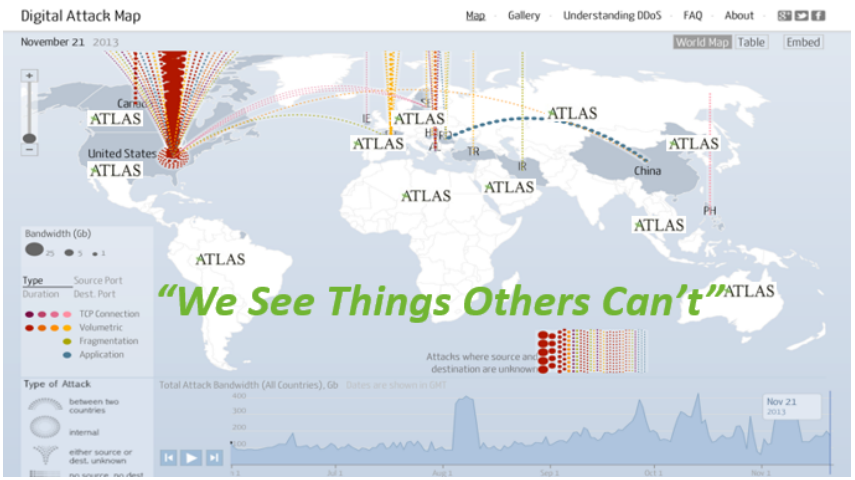


Frost & Sullivan Report
- DDoS Mitigation Global Market Analysis – Nov 2015

ARBOR NETWORKS

ATLAS & ASERT

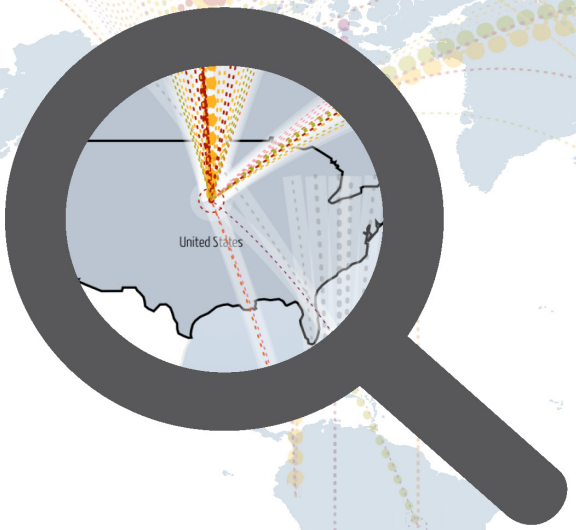
- **15 years of deployment** in a majority of world's ISPs offer unique visibility into global threats
- **Over 330 ISPs participating in ATLAS;** providing Global Visibility and Threat Intelligence
- **ASERT is a team of industry experts** who conduct threat research, help customer mitigate DDoS attacks and create ATLAS Intelligence Feeds
- **ATLAS & ASERT** continuously arm all Arbor products and services with global threat intelligence called ATLAS Intelligence Feed allowing customers to stay abreast of DDoS and advanced threats



ARBOR SERT / ATLAS / AIF
Security Engineering & Response Team

ARBOR NETWORKS

ATLAS GLOBAL THREAT ANALYSIS SYSTEM



ATLAS gathers anonymous traffic data from more than **330 ISPs** around the world

- ASERT has data of ~98% ASNs
- ~50% coverage of national CERT teams
- ASERT has seen 2.63B unique IPv4 addresses (~71% theoretical)
- ASERT monitors 1.76M "dark" IPv4 addresses

ATLAS monitors more than

120

tbps

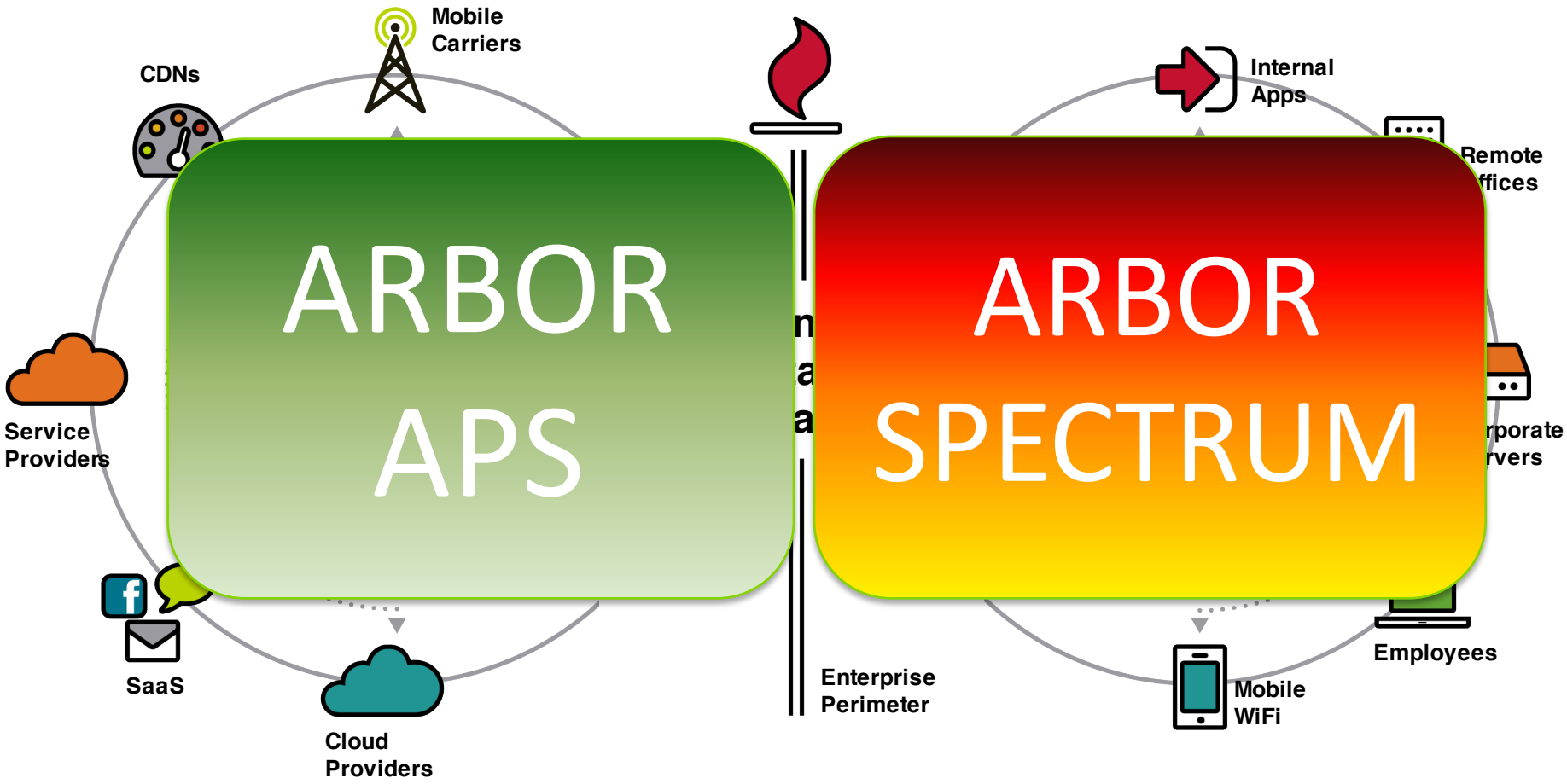
of global Internet traffic

Unique Insight

ARBOR'S security researchers use this global intelligence to develop local protection against targeted threats

SOURCE: Arbor Networks

Today's Cyber Security Challenges



ARBOR NETWORKS

Q&A / THANK YOU

For More Information, Please Contact:

Tony Teo, Director Sales Engineering, APAC

Ph: +65 9680 5133
Email: tteo@arbor.net

ARBOR® NETWORKS