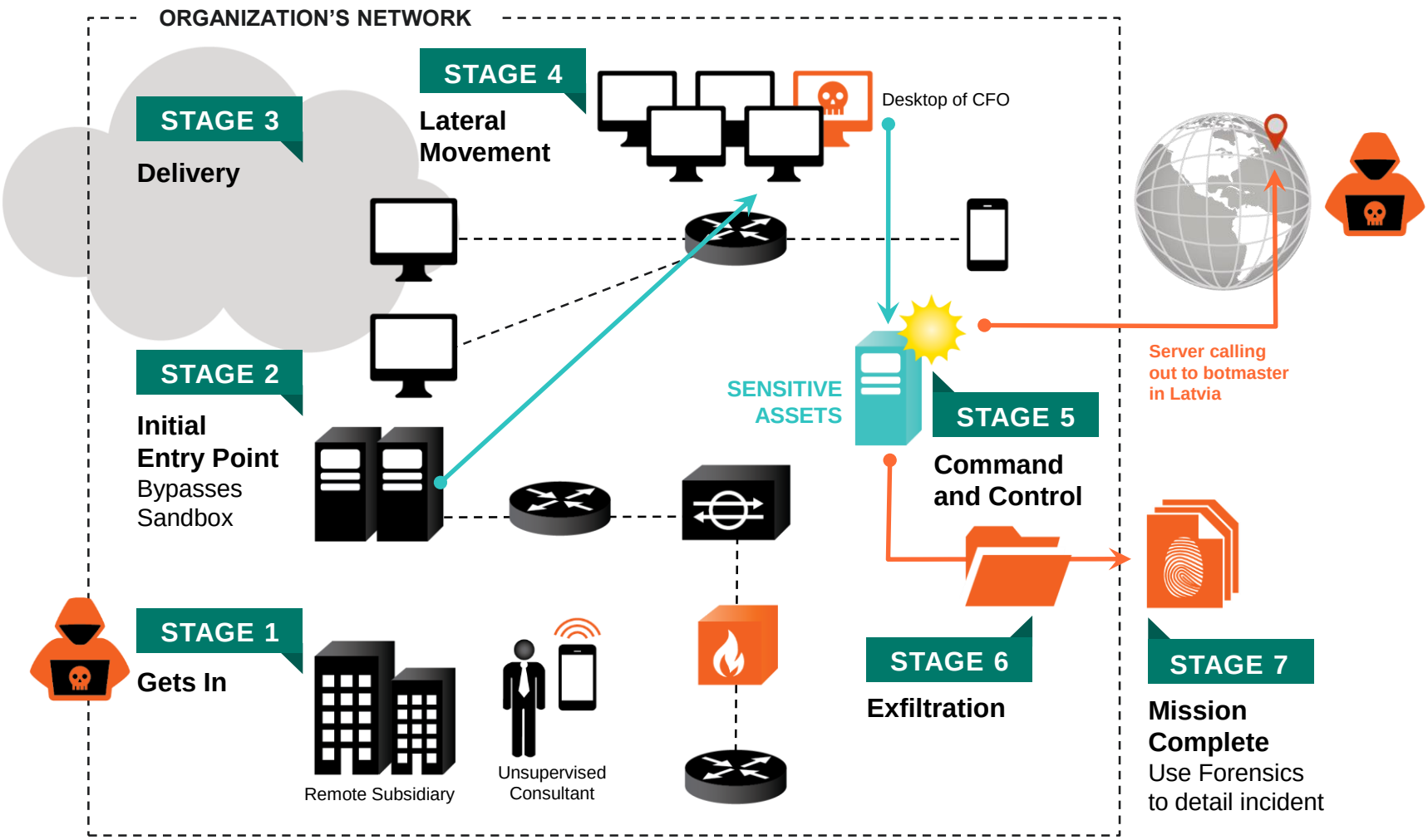
ARBOR SPECTRUM™

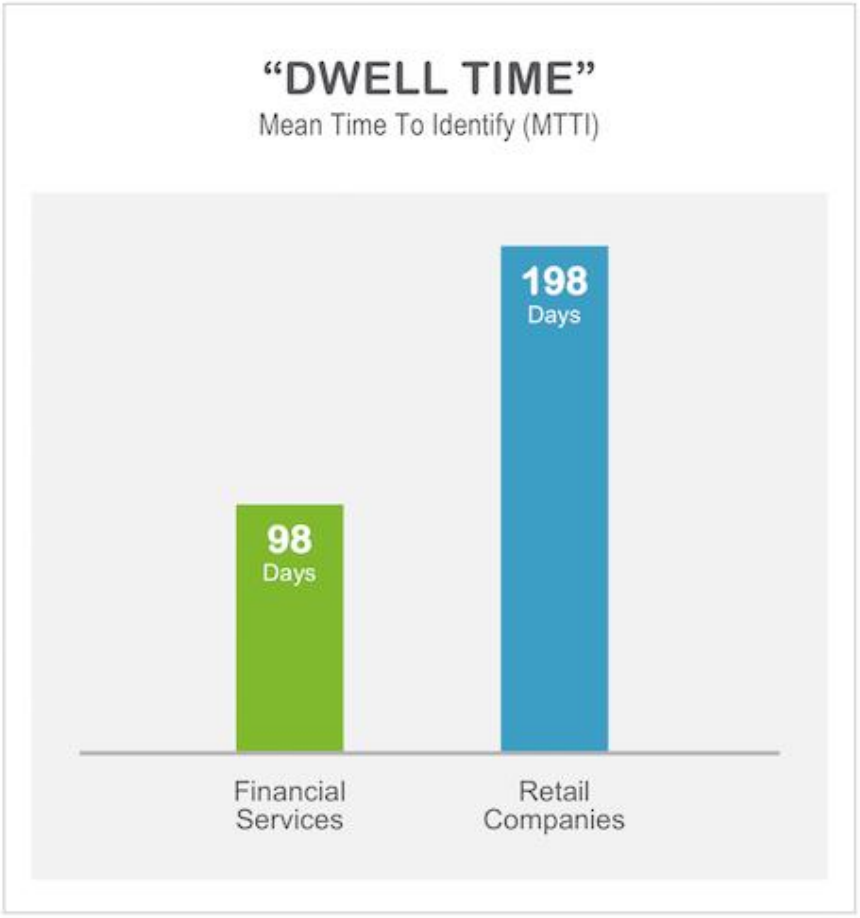
Epic Range, Faster Proof

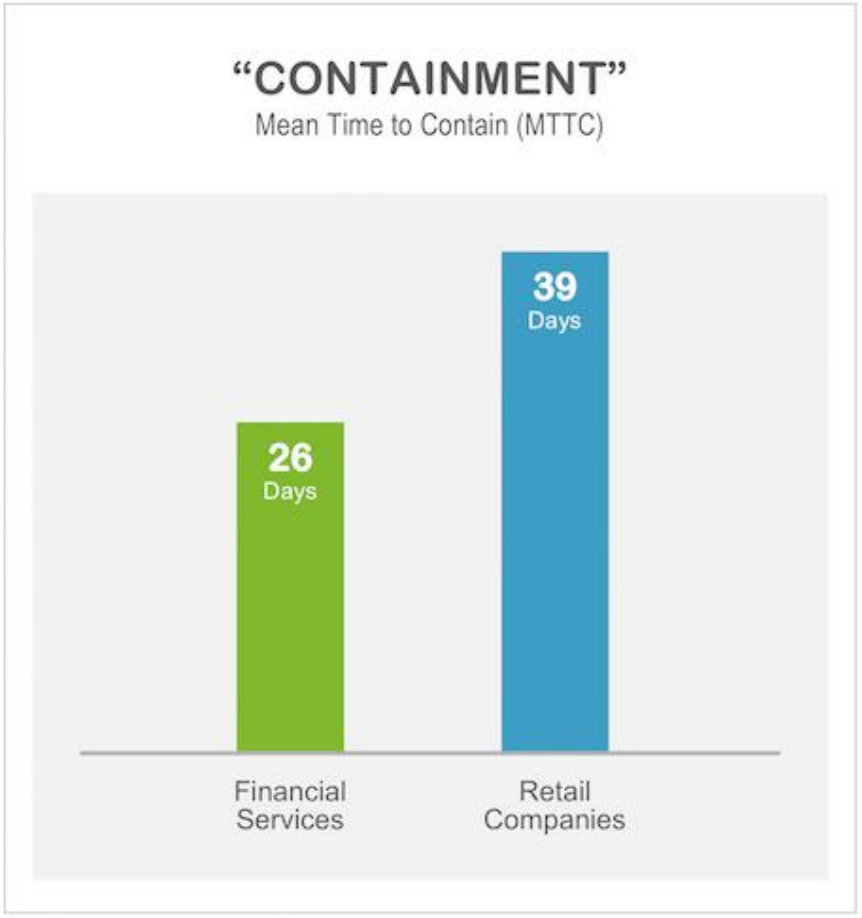
The Anatomy of an Attack Campaign



ARBOR® NETWORKS

Time Is The Currency That Matters





SOURCE: Ponemon Institute LLC, Sponsored by Arbor Networks

1.) Advanced Threats in Financial Services: A study of North America & EMEA (May 2015)

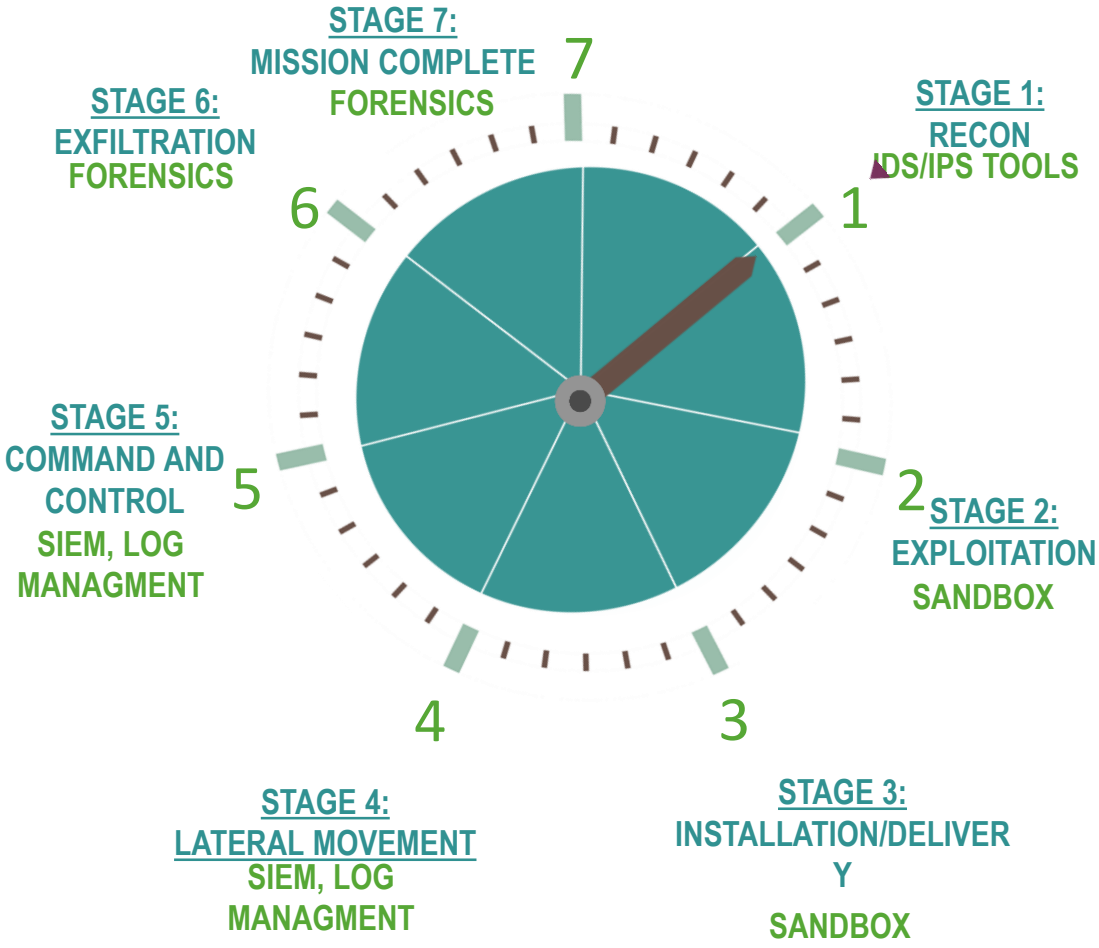
2.) Advanced Threats in Retail Companies: A study of North America & EMEA (May 2015)

Why Is It Taking So Long?

ATTACK DETECTED

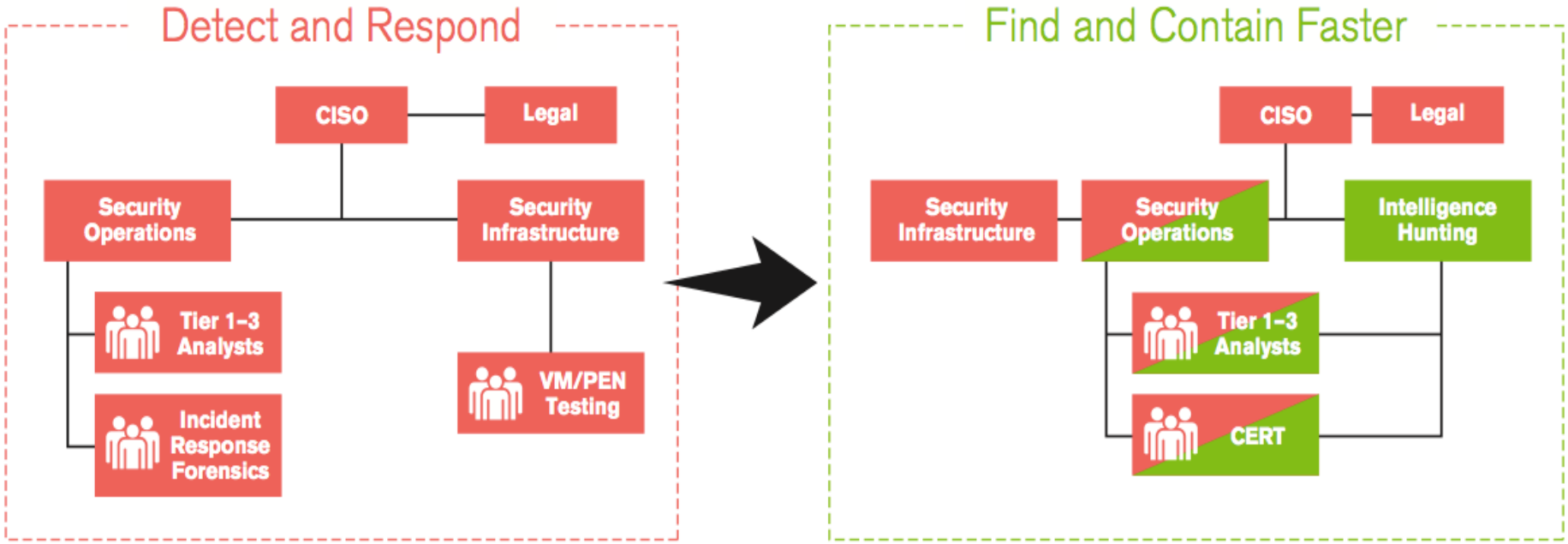
198

DAYS



ARBOR® NETWORKS

Moving Beyond Detect And Respond



- Use Better Indicators of Attack
- See Inside Your Entire Network
- Threat Hunting to Find Attacks That Matter, Detect Unknowns.
- Contain Attacks Faster By Seeing Compromised Infrastructure

Retail – Evolving To Hunt Case Study

- Security Ops Team – 90% outsourced
  - Deploy antivirus, intrusion detection,sandbox,SIEM.
- IR Team – Handful of FTEs combined with outsourcing
- Cyber Intelligence Team
  - Look for threats on the horizon, raw intel
- Reported on threats blocked, # and Time of Incidents Resolved
  - Only covering 10-20% of high interest alerts/ events surfaced.
  - Investigation <24 hours per critical event

Challenges/Benefits with Proactive Approach

- Recruited 3 analysts internally including a manager
  - Began proactive threat hunting.
- Found penetration background not sufficient to close the gap
  - Using input from the Intelligence team to guide weekly work.
  - "Where to look next" training
- Began reporting on dwell time on incidents found
  - Found attacks before they exfiltrated.
  - Identified locations and use of third- parties to gain access to sensitive assets.
  - Expanded scope of team and expanded Intel analysts.
  - Galvanized management and began quarterly reporting to Board.

Online/Consumer – Leaping To Hunt

- Security Team – Small Team Focused on Online Fraud/Web App Security
  - IP theft prompted action within Executive Team and Security Architect.
- Small Security Team, Outsourced SOC
  - Limited security operations expertise, 3 Data Centers around globe, Incident Response focus on responding to employee issues
- Borrowed 2 Security/ Network Infrastructure Analysts
  - Picked high priority alerts sent over from SOC to investigate "in house".
  - Sent to short threat hunting and intelligence training courses.

Online/Consumer – Challenges and Benefits

- Instituting a workable and consistent set of processes to begin investigation and measure progress.
  - Setting a consistent approach to team's approach and guardrails.
  - Reporting results.
- Proactively found 10 targeted attacks in < 12 months
  - Identified a number of targeted attacks that did or could have impacted business.
- Educating and Informing Management
  - Inculcating the world of threats and security risk into the culture.

Financial – Connecting Art with Science

- "Hunter" Team –4 dedicated staff
  - Solely follow hunches on where to look for attacks.
- Intelligence/Analytics Team
  - Review intel from myriad sources, input from malware research team.
- Security Operations Team – 20 people
  - Combination of insourced and outsourced to manage IDS, Sandbox and perimeter tools and alerts.
- Incident Response Team – 10 people
  - "Traditional" triage team to define and respond to incidents.
- Wanted more unstructured hunting and focus on finding "unknown unknowns"

Financial – Challenges and Benefits

- Training, Maintaining, Motivating Team
  - Building better team, more coherent picture into threat actors and risk to business.
- Staffed new "background" Team members
  - Political Science, Political Risk. Visualization and analytics expertise.
- Synthesizing output from Intel team to Inform Hunting team
  - Input and analysis still highly manual.
- Found "zero-day" attacks focused on company.
- Reporting of Dwell Time reduction by Stage of Kill Chain

Arbor Overview:15 Years of Network Excellence

Leading Network Traffic Expertise

- 15 years of understanding the worlds most complex and demanding service provider and enterprise networks.
- Deployed everywhere on the planet (107 countries).
- See more Internet traffic than any other service provider.

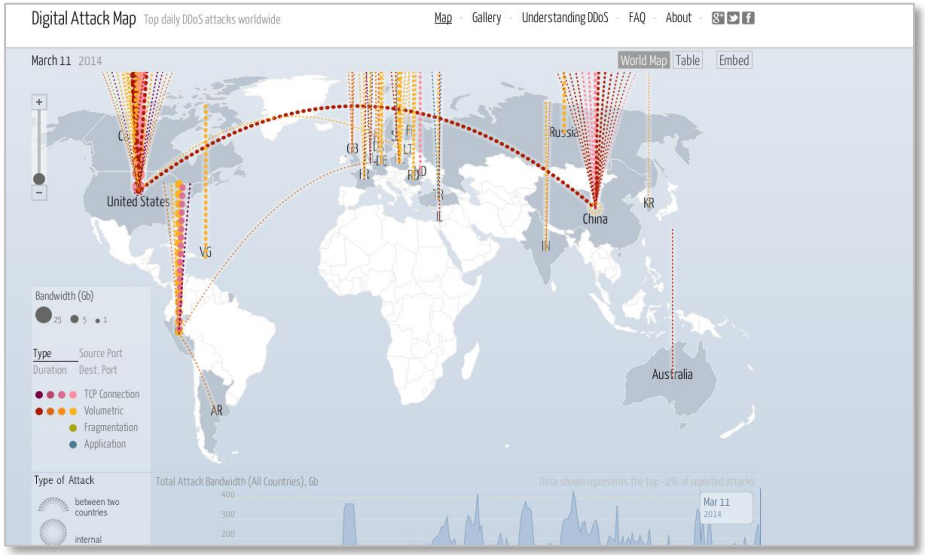
Premier Global Security Visibility

Hourly updates from 330+ providers on attack traffic across the Internet.

- World class security research team analyzing traffic patterns and reverse engineering malware and its infrastructure with ATLAS/ASERT.

Proven Scale Across Blue Chip Installed Base

- 3/5 Top Global Banks.
- Deployed largest financial institution in 28 countries.
- 9/10 of largest online brands and hosting providers.
- 100% Tier 1 Service providers.



Google ideas

Live Digital Attack Map

*Powered by: **Arbor Networks***

Arbor Networks Spectrum

Find attack campaigns in real-time across your entire network

- Automatically correlate ATLAS Intelligence with threat activity anywhere in the network to confirm an attack.

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.

Find Real Threats 10x Faster, Reduce Your Risk.

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

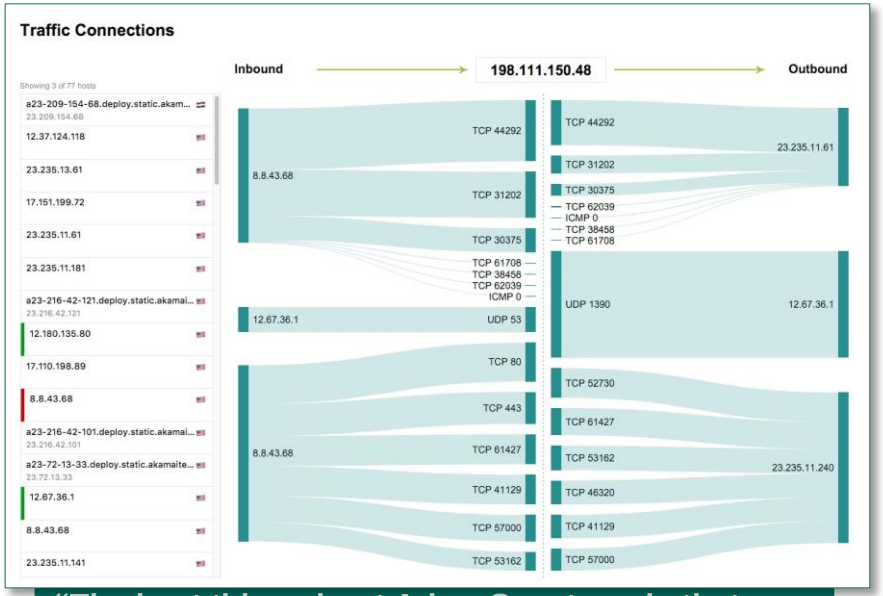
Case Study: Detection & Proof of an Attack Campaign in Minutes

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

THANK YOU