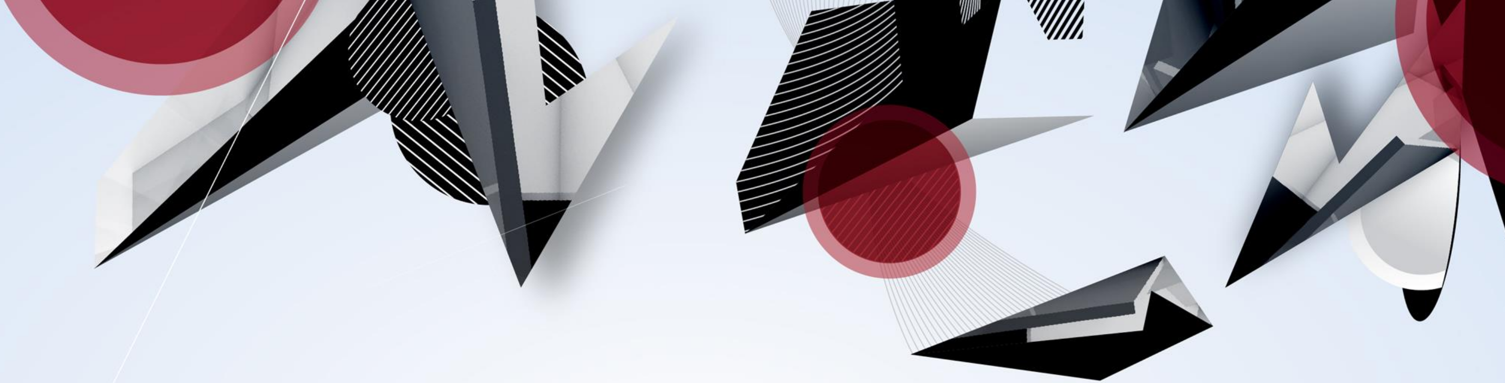


Commercial Practices for Cybersecurity

Understanding Today’s Cyber Security Trends

Presented by: Lyle Sudin, Manager, Security Consulting Services
lyle.sudin@mandiant.com

May 15, 2018

Lyle Sudin

- Manager of Security Consulting Services at Mandiant, a FireEye company
- First security job for Akamai starting in 2000
- 12 years in government funded R&D at BBN Technologies, now part of Raytheon
  - Developed cutting edge security technologies
  - Roles included Principal Investigator, manager, software developer, architect, integration engineer, and systems administrator
- 2.5 years as Senior Manager at HERE Technologies
  - Application security reviews, creation of a Security SDLC, and ISO 27001 certification
- 2+ years at Mandiant
  - Consulting manager for the North Central region
  - Focus is on strategic, proactive, and transformational activities

Mandiant Consulting, a FireEye company

Prevent, detect, & respond to advanced cyber-security events and protect your organization's critical assets.

40%

Trusted by organizations worldwide – **Over 40%** of Fortune 100 companies[1]

14+

14+ years responding to and remediating headline breaches

Mandiant DNA

Mandiant DNA – Pioneers in sophisticated incident response

Portfolio of services to **assess, enhance and transform** security posture and upskill internal security staff

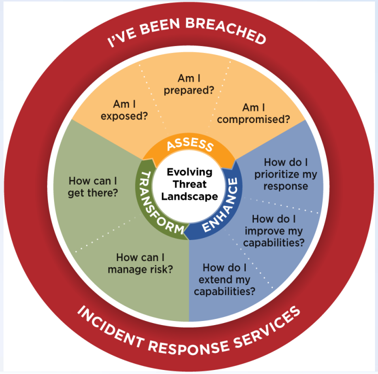
Cutting-edge threat intelligence informed by frontline adversary exposure

Cyber security services enabled by purpose-built technology

Global workforce of over 300 consultants in 20+ countries

[1] 2017 Fortune list

So What? Who Cares?


I'VE BEEN BREACHED
Am I prepared?
Am I exposed?
Am I compromised?
ASSESS
Evolving Threat Landscape
TRANSFORM
ENHANCE
How can I get there?
How do I prioritize my response
How do I improve my capabilities?
How can I manage risk?
How do I extend my capabilities?
INCIDENT RESPONSE SERVICES

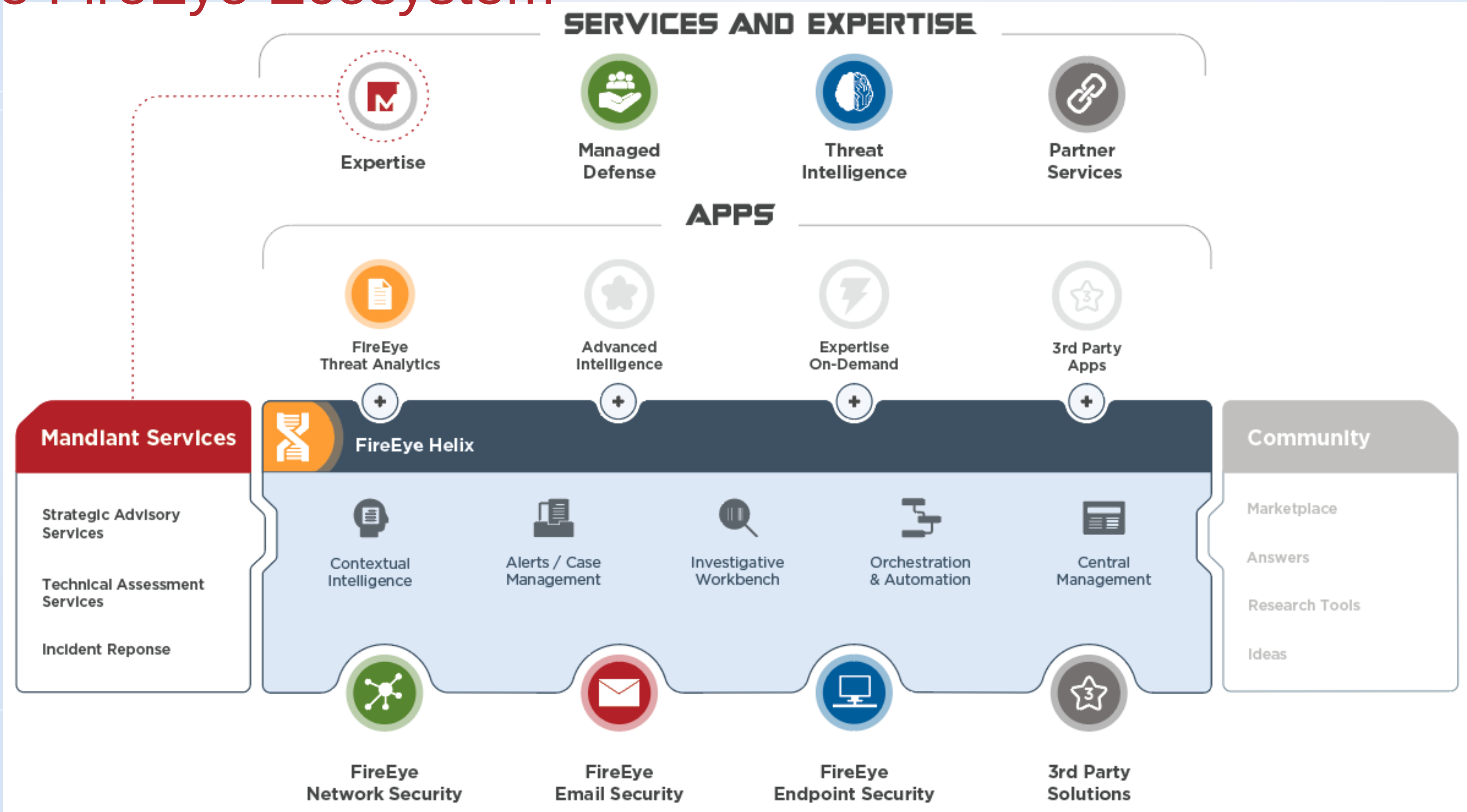
- You will be hacked, what are you going to do about it?
  - Adversaries are professionals, organized, and well funded
  - Mandiant can help prepare you to deal with the incident
    - Identify and reduce security risks at all levels of the organization
- Best practice is to focus on detection and response
  - Create an investigation ready environment
  - Leverage threat intelligence
  - Develop layers of controls proportional to the data
  - People, processes, and technology are all required to mount an effective defense

Questions?

FireEye

Thank You

The FireEye Ecosystem



FireEye

Additional Material

Evolving Threat Landscape

It's a "who," not a "what"

- There is a human at a keyboard
- Performing highly tailored and customized attacks
- Targeted specifically at you

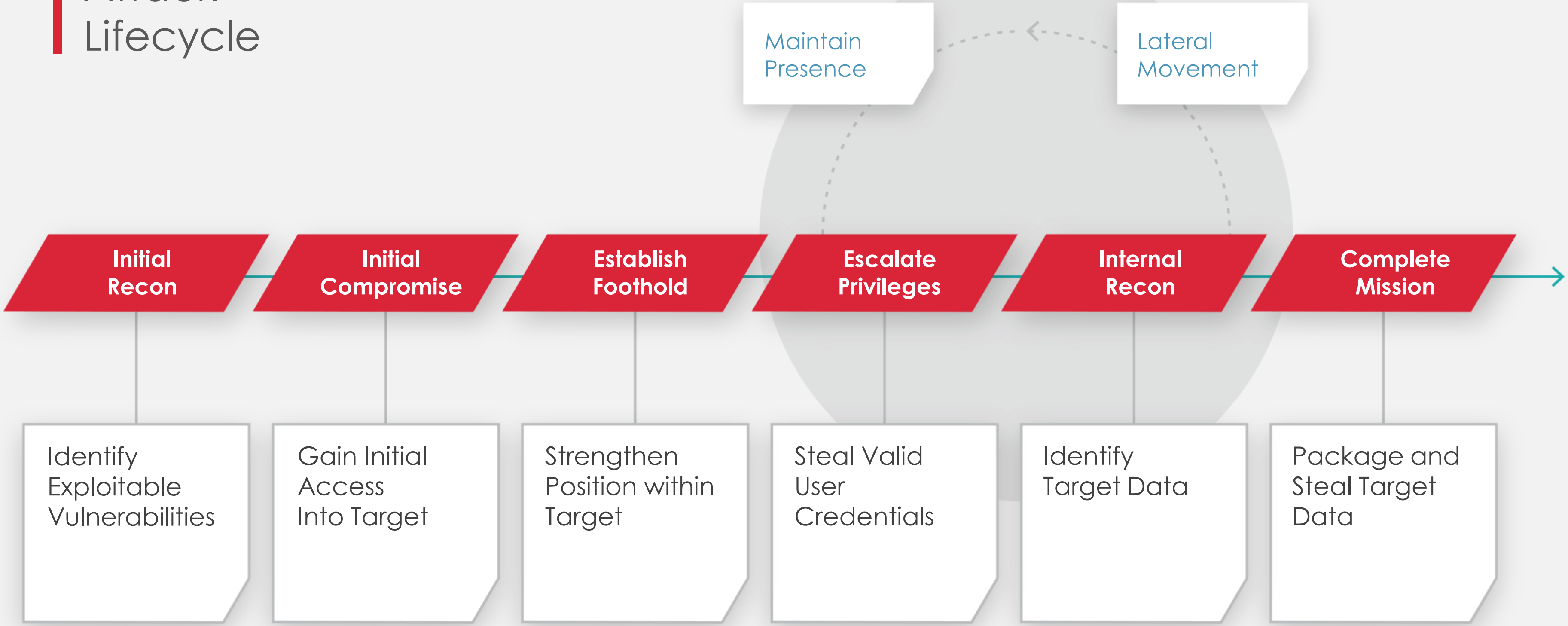
Professional, organized and well funded

- Attackers escalate sophistication of their tactics as needed
- They remain relentlessly focused on their objective

If you kick them out they will return

- They have specific objectives
- Their goal can be long-term occupation or short term destruction
- Their utilization of persistence tools and tactics ensure ongoing access

Attack Lifecycle



Maintain Presence

Lateral Movement

Initial Recon: Identify Exploitable Vulnerabilities

Initial Compromise: Gain Initial Access Into Target

Establish Foothold: Strengthen Position within Target

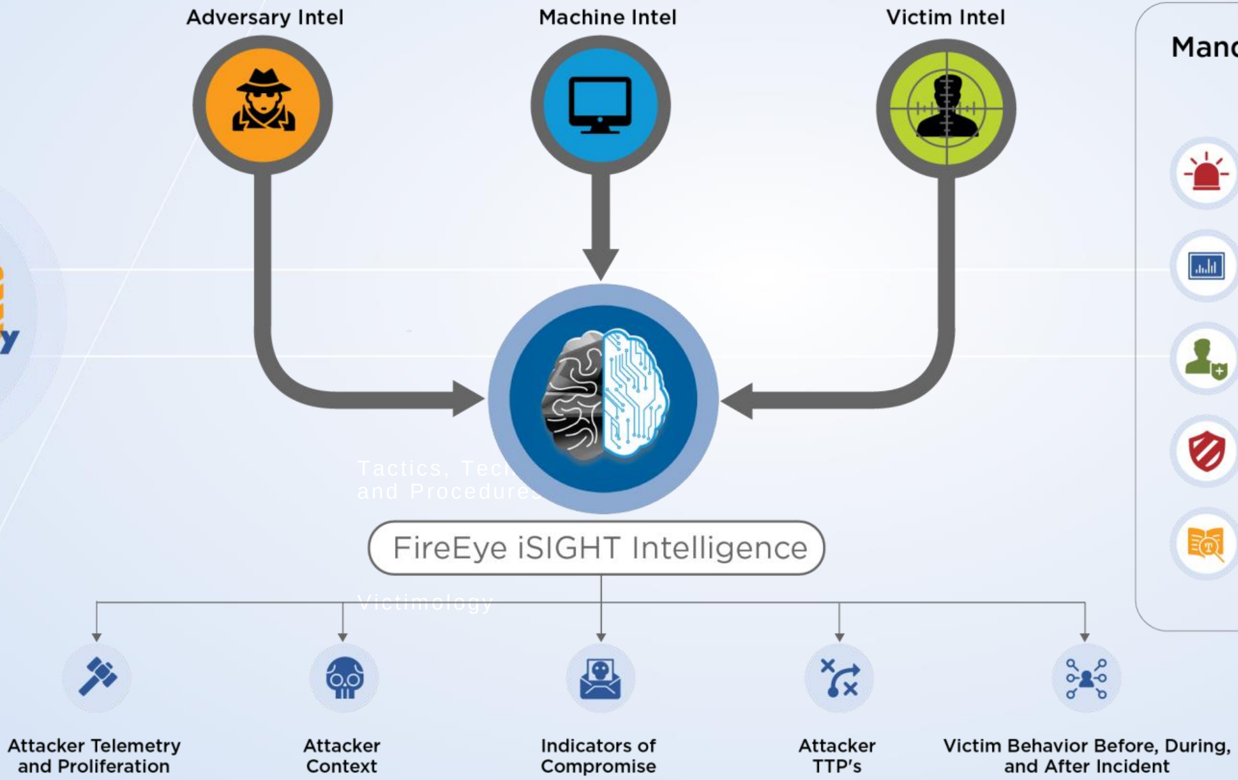
Escalate Privileges: Steal Valid User Credentials

Internal Recon: Identify Target Data

Complete Mission: Package and Steal Target Data

An Intelligence-Led Approach to Services

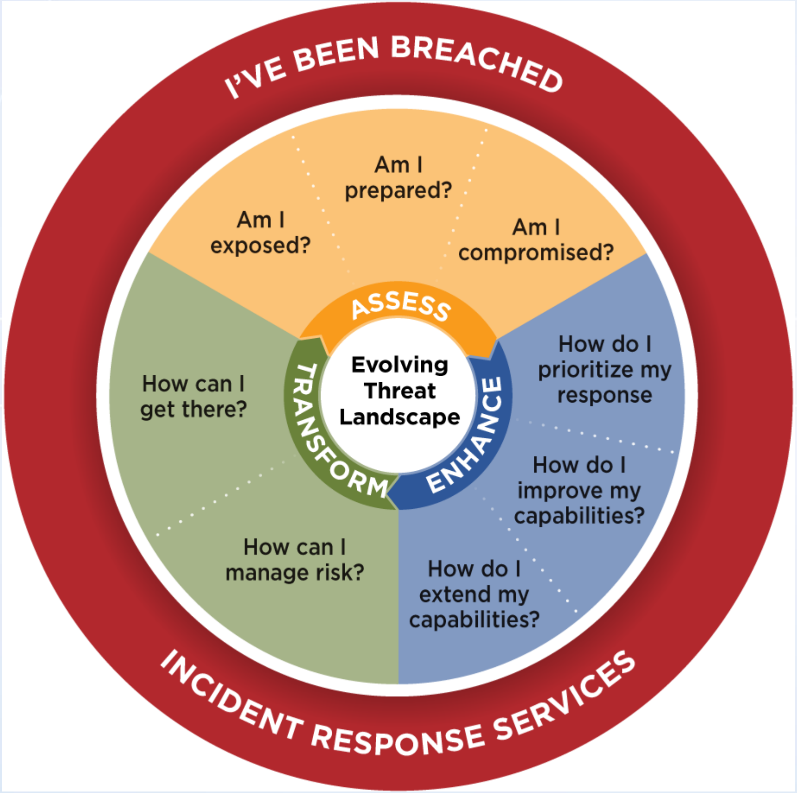
FireEye TECHNOLOGY STACK



Mandiant Consulting Services

- Incident Response
- Technical Assessments
- Strategic Services
- Security Transformation
- Training

Security Needs Framework


I'VE BEEN BREACHED
Am I exposed?
Am I prepared?
Am I compromised?
ASSESS
How do I prioritize my response
How do I improve my capabilities?
How do I extend my capabilities?
ENHANCE
How can I get there?
How can I manage risk?
TRANSFORM
Evolving Threat Landscape
INCIDENT RESPONSE SERVICES

7 Reasons to Have Mandiant on Speed Dial

1 INVESTIGATIVE EXPERTISE

2 SPEED AND SCALE

3 WORLD CLASS THREAT INTELLIGENCE

4 CUSTOM TECHNOLOGY OPTIONS

5 GLOBAL FOOTPRINT

6 CRISIS MANAGEMENT EXPERTISE

7 EXPERT STAFF AND INNOVATIVE RESEARCH

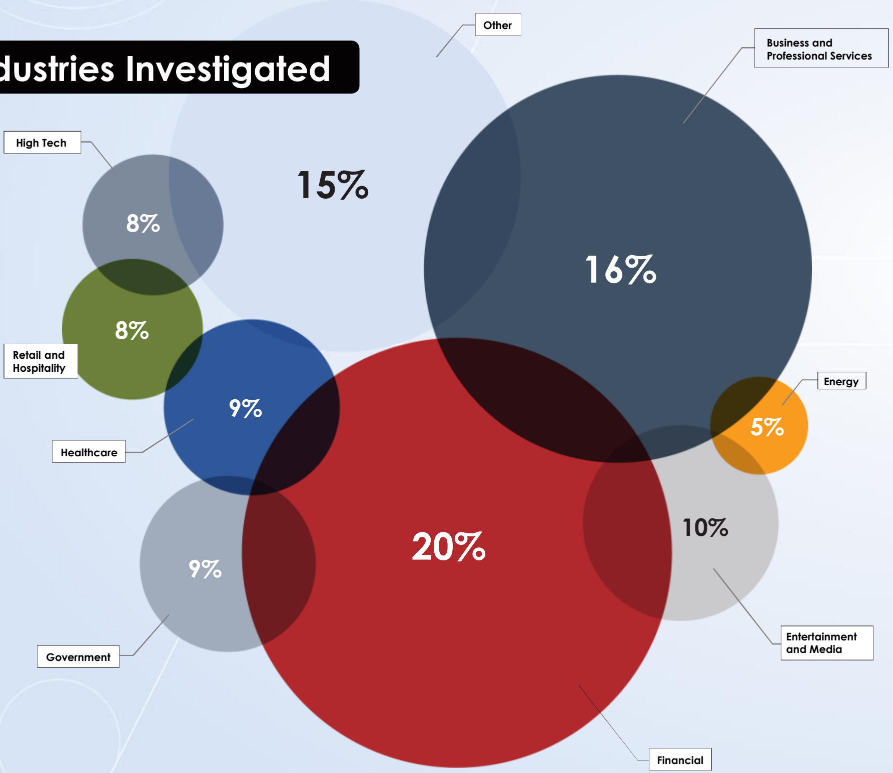
M-Trends: Tracking our investigative experience

- Informing the cyber security community since 2010
- Annual publication sought after by security professionals and market analysts
- Data based on **12 months of forensic investigative findings** (10/01/16 – 09/30/17)

[2] Ponemon Institute (2017). *Cost of Data Breach Study*.

Who’s a Target

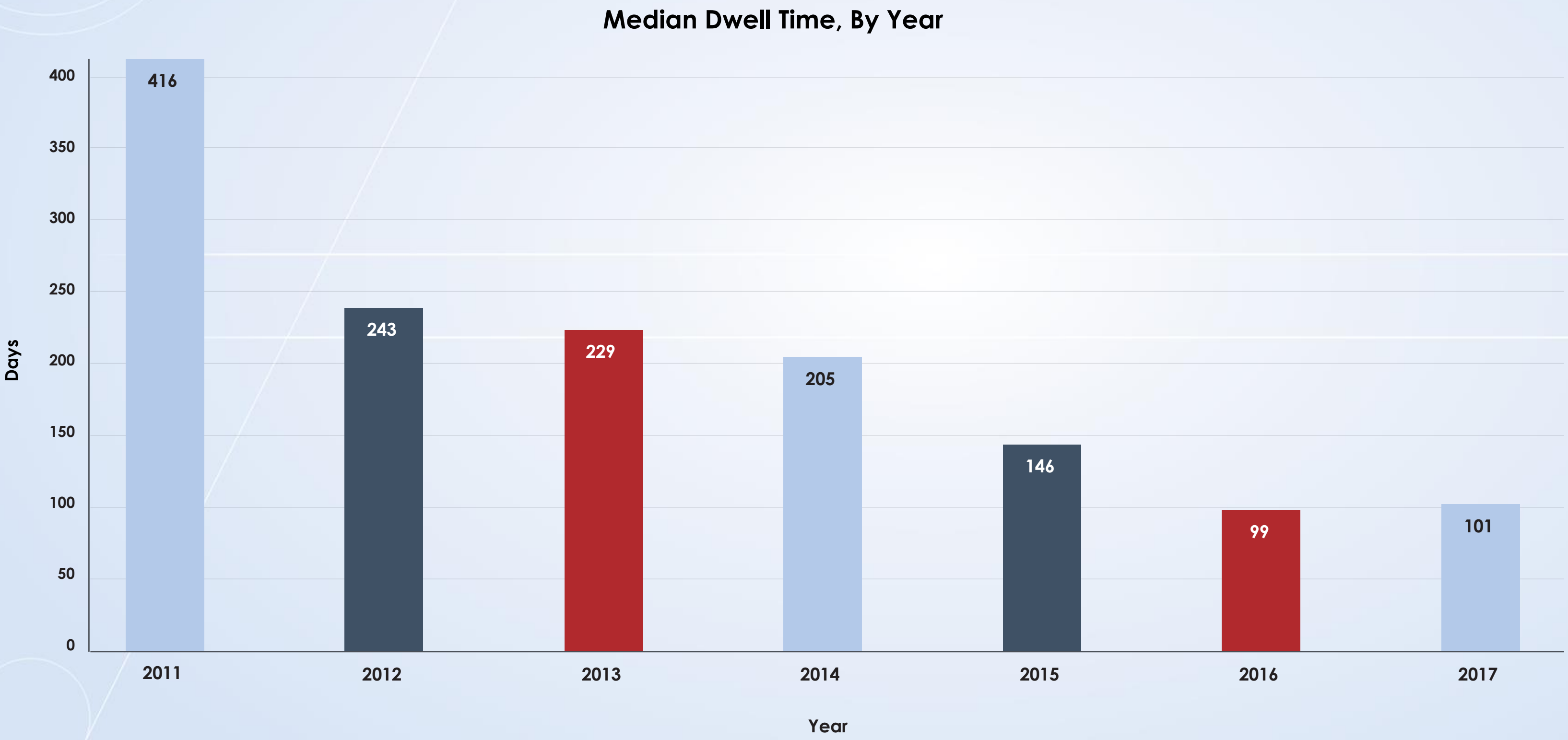
Industries Investigated



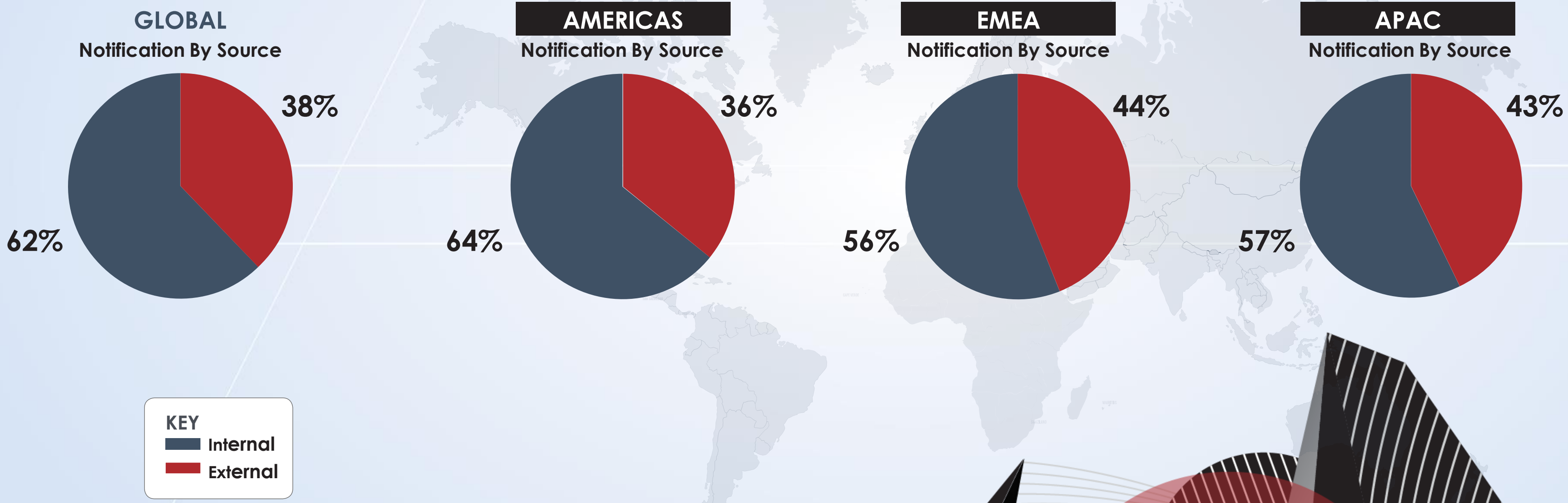
Organizations Investigated By Mandiant in 2017, By Industry

Industry	Americas	APAC	EMEA	Global
Business and Professional Services	18%	10%	12%	16%
Energy	5%	2%	7%	5%
Entertainment and Media	11%	7%	5%	10%
Financial	17%	39%	24%	20%
Government	6%	7%	18%	8%
Healthcare	12%	2%	2%	9%
High Tech	9%	10%	7%	8%
Retail and Hospitality	10%	2%	4%	8%
Other	12%	20%	22%	15%

Median Dwell Time Trending



Notification by Source



GLOBAL
Notification By Source

AMERICAS
Notification By Source

EMEA
Notification By Source

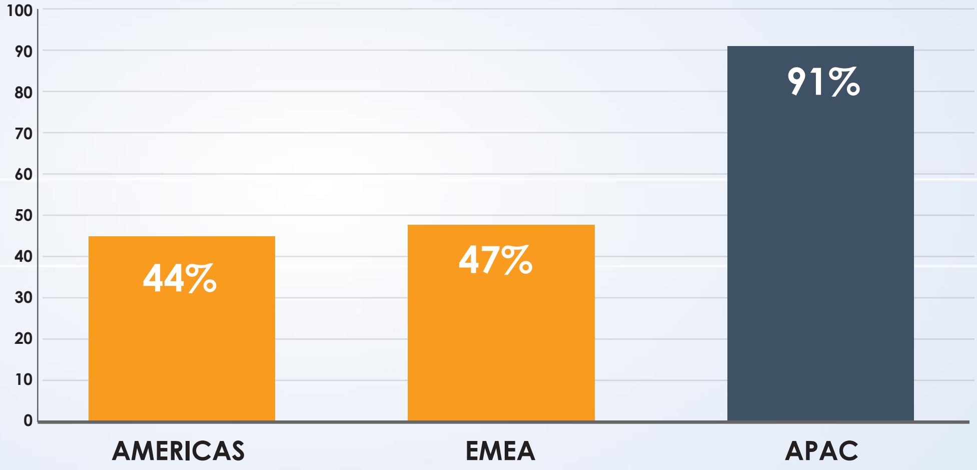
APAC
Notification By Source

Once a Target, Always a Target

56%

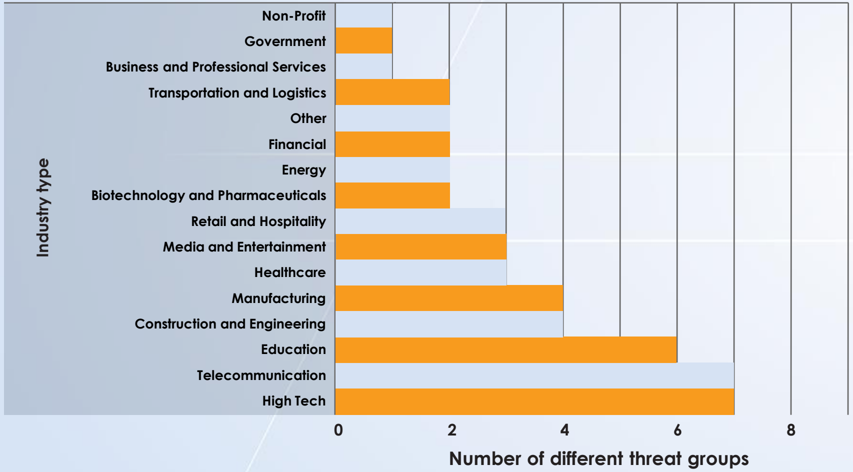
victims subsequently retargeted

Victims subsequently retargeted by region

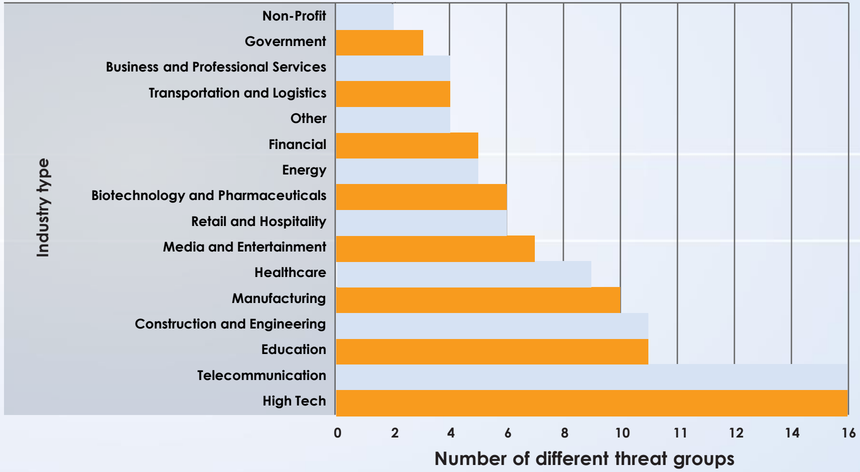


Once a Target, Always a Target, by industry

Customer industries targeted by multiple threat groups



Customer industries by number of significant attacks



Enduring Trends in Security Fundamentals

Security Risk Management

Identity and Access Mgmt

Data Protection

Network, Cloud and DC Protection

Incident Response

Host and Endpoint Protection

Cyber Security Skills Gap – The Invisible Risk

Growing skills shortage

- Demand for specialized skills rapidly outpacing supply
- Lack of visibility and detection
- Lack of specialized skill-sets

Recommendations

- Enhance current capabilities through process improvement and staff training
- Automate overhead processes
- Outsource niche functions to specialized service providers