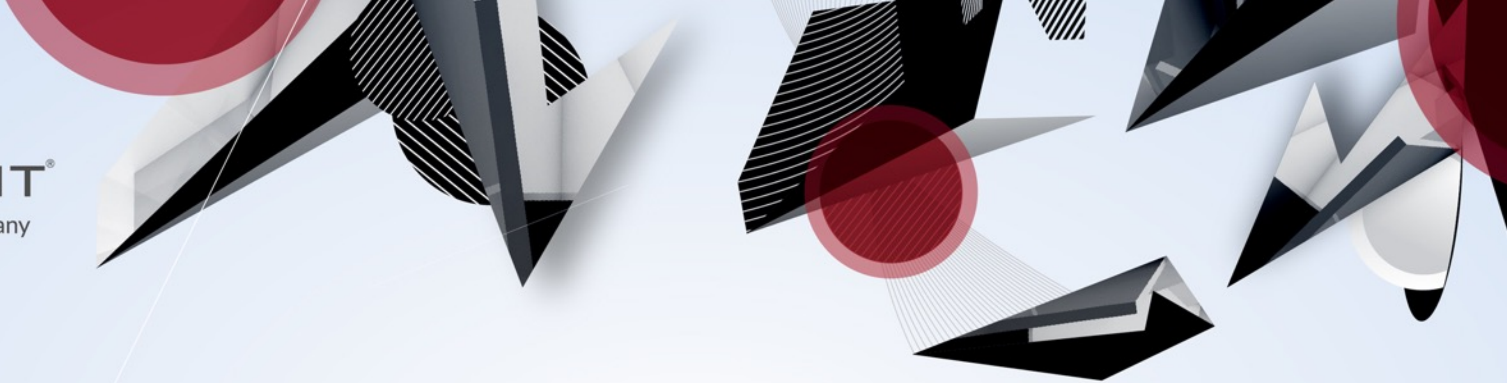
MANDIANT®
A FireEye® Company



Cyber Threat Trends and Strategies

A U.S. and Global Perspective

Presented by: Ron Bushar, CTO and VP – Government Solutions

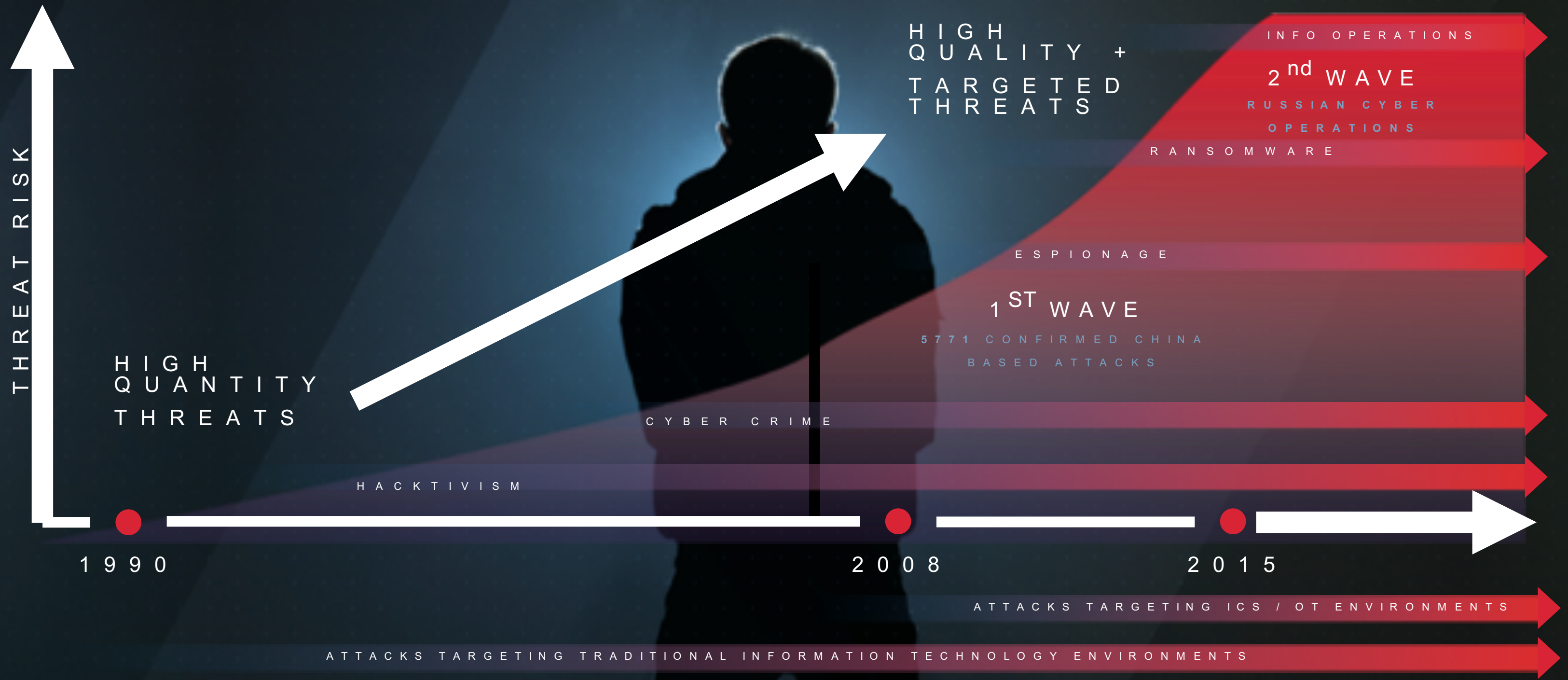
June 14, 2018

MANDIANT®
A FireEye® Company

Today’s Threat Landscape:

What has changed, what hasn’t

THE EVOLUTION OF THE THREAT



THREAT RISK

HIGH QUANTITY THREATS

HIGH QUALITY + TARGETED THREATS

INFO OPERATIONS

2nd WAVE

RUSSIAN CYBER OPERATIONS

RANSOMWARE

ESPIONAGE

1ST WAVE

5771 CONFIRMED CHINA BASED ATTACKS

CYBER CRIME

HACKTIVISM

1990

2008

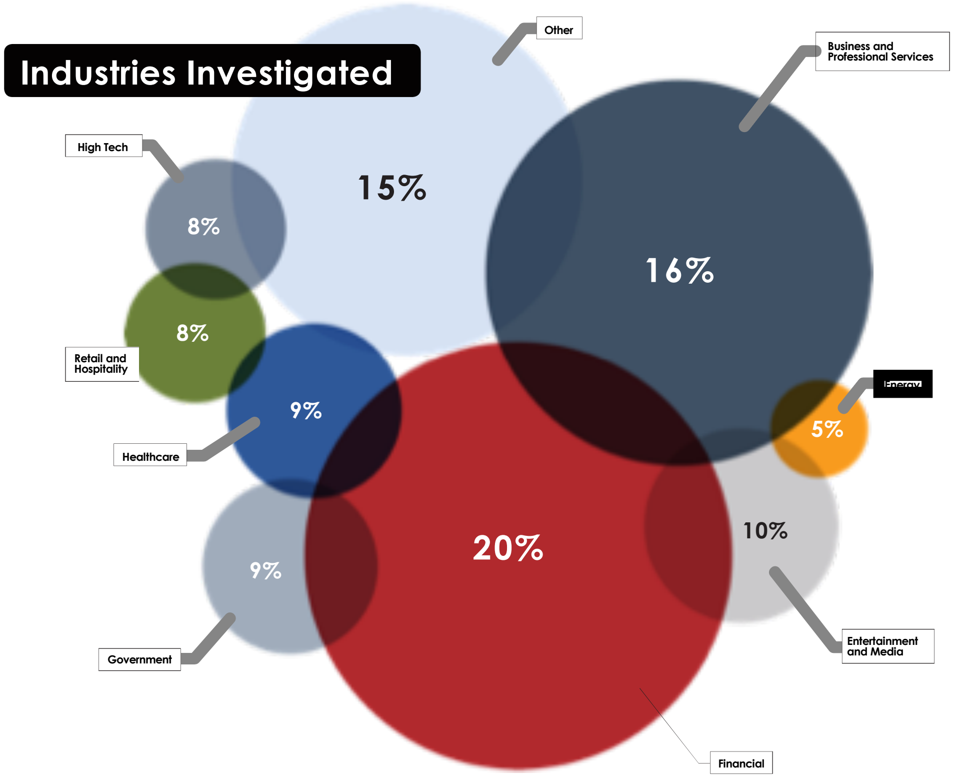
2015

ATTACKS TARGETING ICS / OT ENVIRONMENTS

ATTACKS TARGETING TRADITIONAL INFORMATION TECHNOLOGY ENVIRONMENTS

Who’s a Target

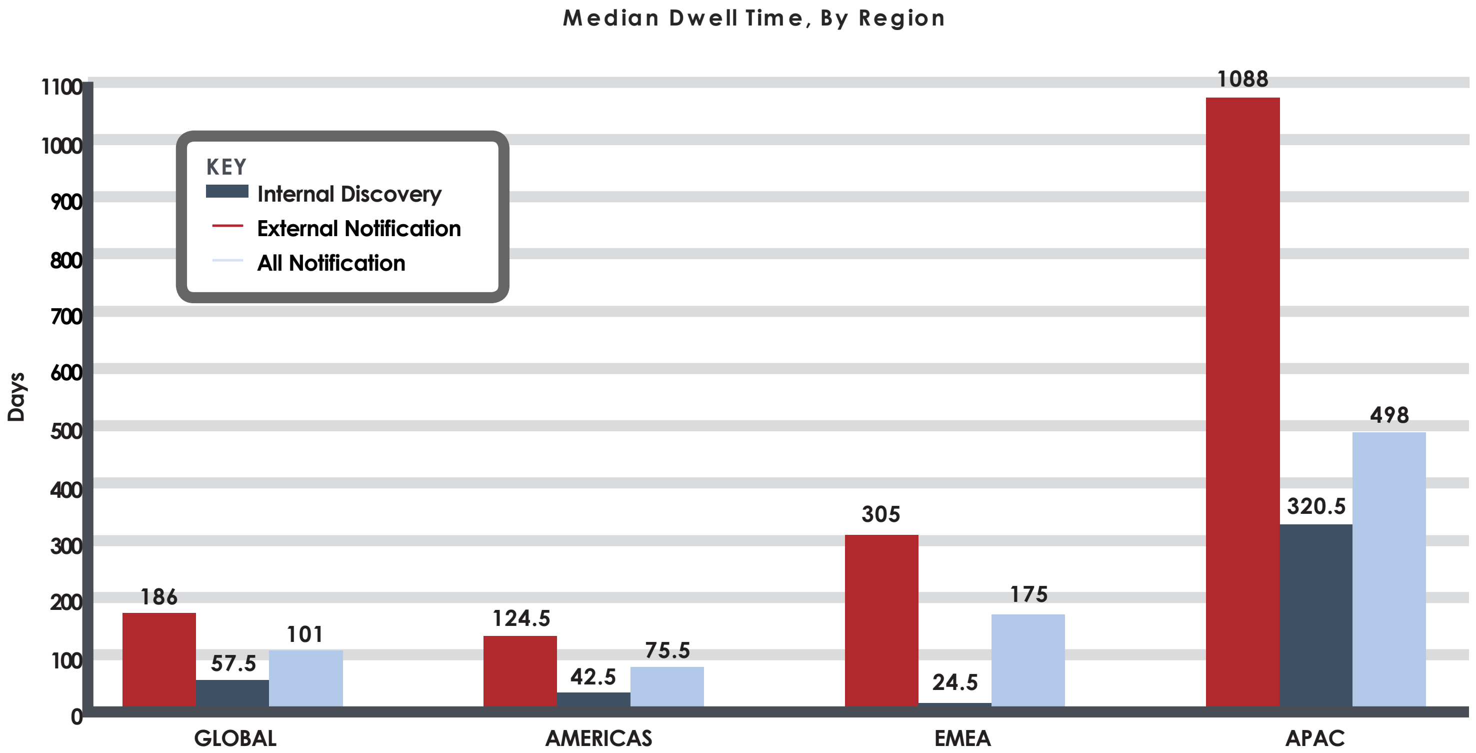
Industries Investigated



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%

By The Numbers, Americas

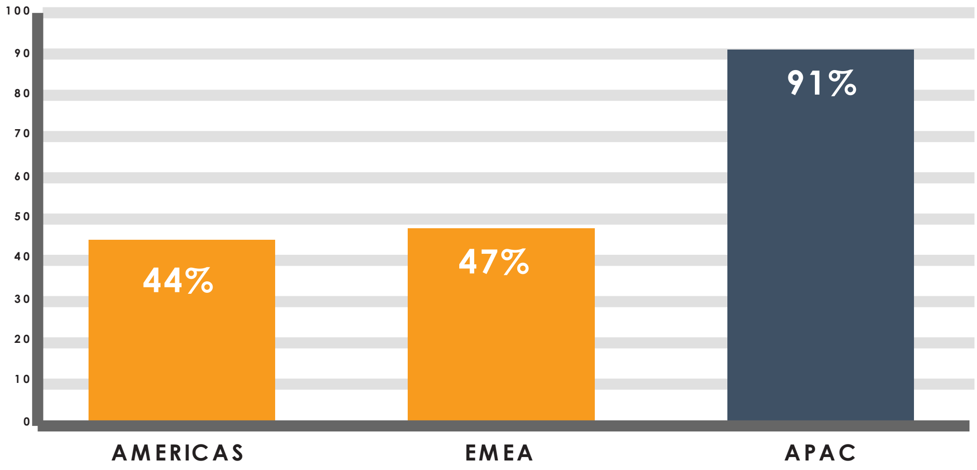


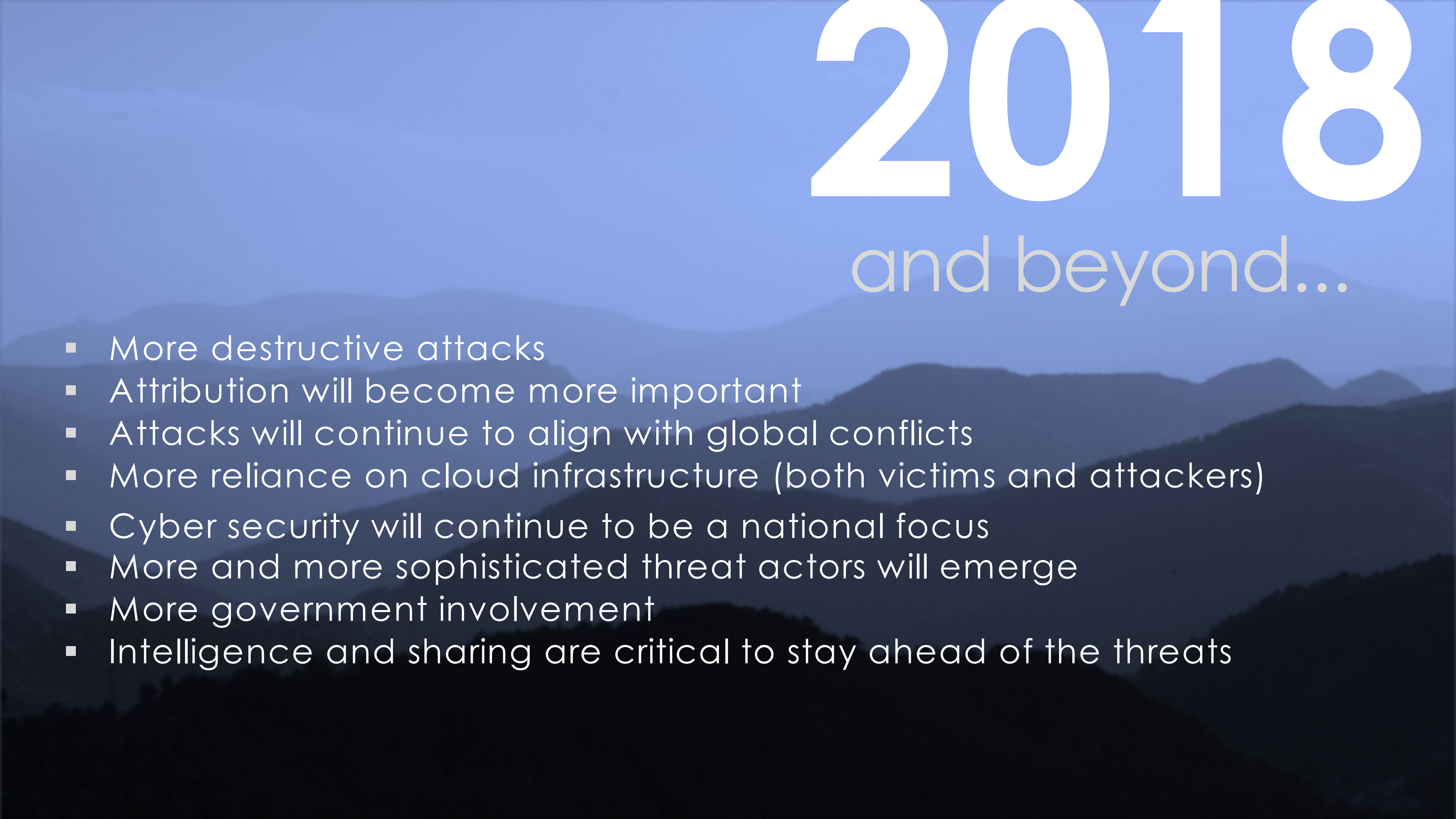
Once a Target, Always a Target

56%

victims subsequently retargeted

Victims subsequently retargeted by region





2018 and beyond...

- More destructive attacks
- Attribution will become more important
- Attacks will continue to align with global conflicts
- More reliance on cloud infrastructure (both victims and attackers)
- Cyber security will continue to be a national focus
- More and more sophisticated threat actors will emerge
- More government involvement
- Intelligence and sharing are critical to stay ahead of the threats

FireEye

Looking Ahead

Lessons Learned and Key Cyber Strategies

Spectrum of Nation State Capabilities

Aspiring

- Azerbaijan
- Bahrain
- Bangladesh
- Belgium
- Bosnia and Herzegovina
- Bulgaria
- Chile
- Cyprus
- Czech Republic
- Ecuador
- Egypt
- Estonia
- Ethiopia
- Honduras
- Hungary
- Kazakhstan
- Luxembourg
- Malaysia
- Mexico
- Mongolia
- Morocco
- Nigeria
- Oman
- Panama
- Qatar
- Saudi Arabia
- Singapore
- Sudan
- Thailand
- Turkmenistan
- United Arab Emirates
- Uzbekistan

Developing

- Argentina
- Belarus
- Brazil
- Colombia
- Denmark
- Finland
- India
- Italy
- Iran
- Lebanon
- Myanmar
- Netherlands
- North Korea
- Norway
- Pakistan
- Philippines
- Poland
- South Africa
- Spain
- Syria
- Switzerland
- Turkey
- Ukraine
- Vietnam

Mature

- Russia
- Israel
- China
- United States
- UK
- France
- Germany
- South Korea
- Canada
- Australia
- New Zealand

“More than 60 countries have or are developing tools for computer espionage and attacks.” –WSJ

WHAT HAVE WE LEARNED?

THERE EXIST **FEW RISKS** OR **REPERCUSSIONS** FOR ATTACKERS

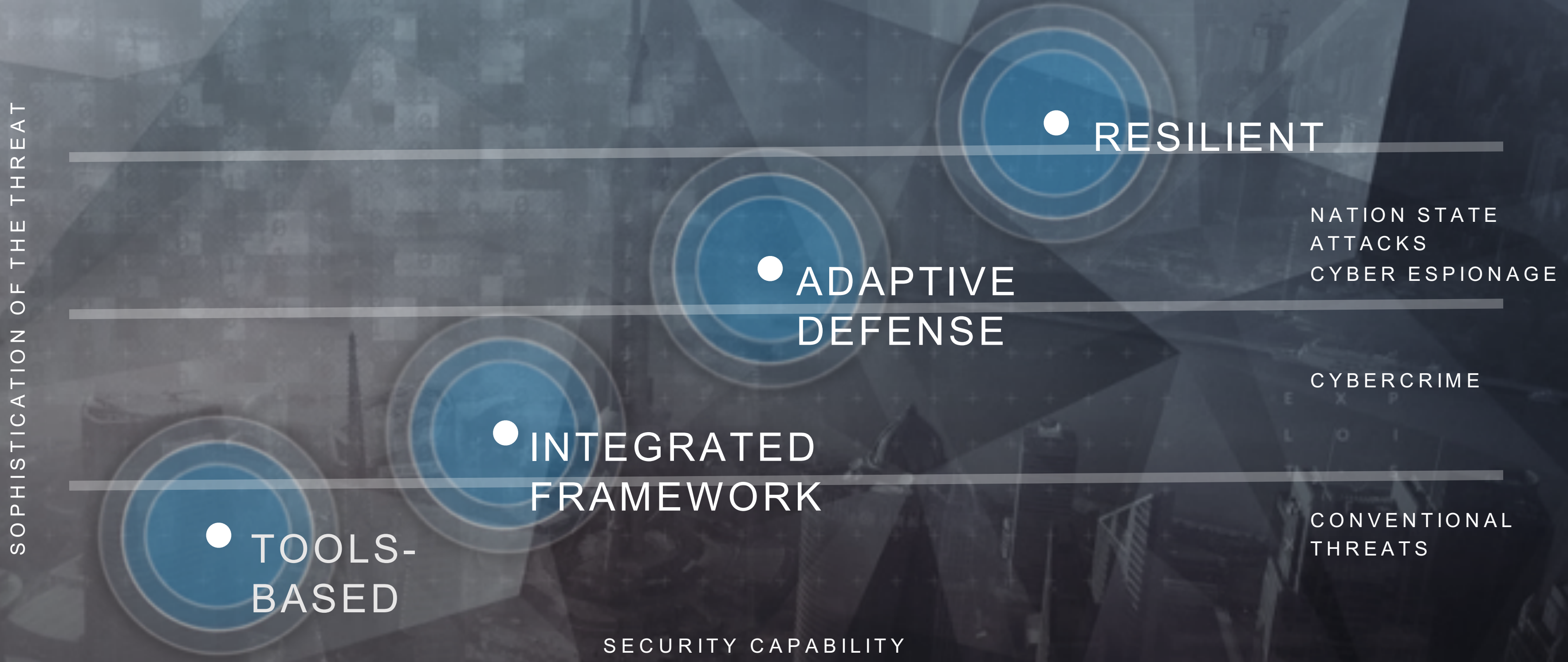
CYBER CRIME TRADECRAFT HAS IMPROVED DRASTICALLY

ATTRIBUTION AND THREAT INTELLIGENCE ARE MORE IMPORTANT

DISCLOSURE IS MORE PROBABLE AND NOT ON YOUR TERMS

THE GOAL IS NOT TO ELIMINATE BREACHES BUT…
ELIMINATE THE CONSEQUENCES OF A CYBER SECURITY BREACH

CYBER MATURITY MODEL



SOPHISTICATION OF THE THREAT

RESILIENT

ADAPTIVE DEFENSE

INTEGRATED FRAMEWORK

TOOLS-BASED

NATION STATE ATTACKS
CYBER ESPIONAGE

CYBERCRIME

CONVENTIONAL THREATS

SECURITY CAPABILITY

WHAT’S WORKING?

Move sensitive data to its enclave network

Require two-factor authentication for remote access

Improve controls for privileged accounts

Only permit authorized programs to run on servers

Promote a “Security First Culture”

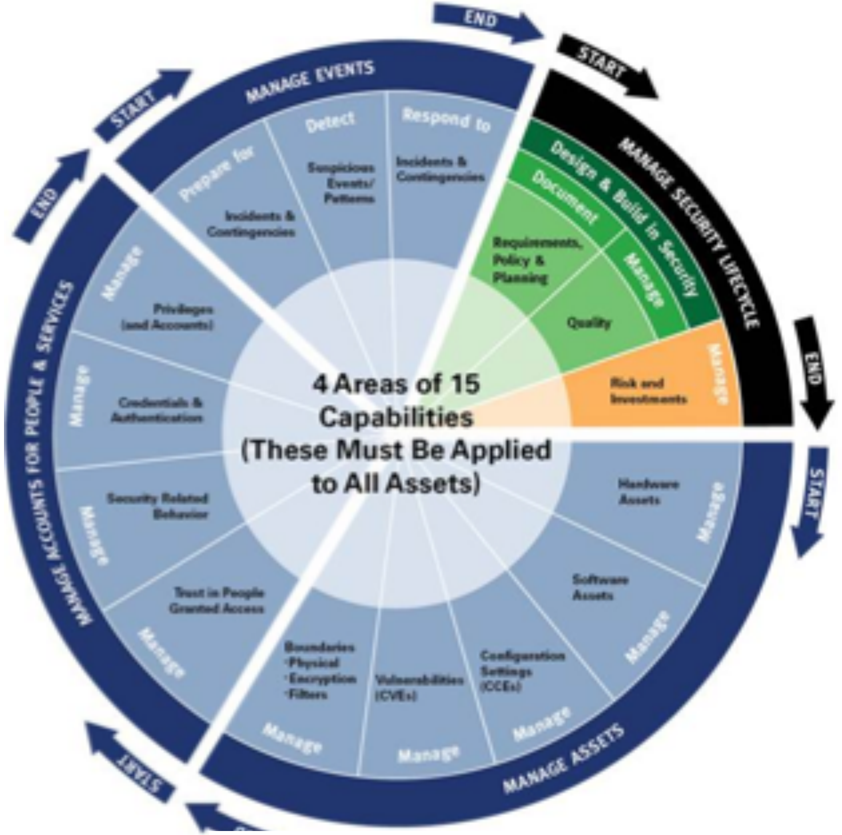
Test the incident response plan

Focus on phishing prevention

Use new technology to block advanced malware

National Framework

- Manage Assets
  - **Hardware** Asset Management
  - **Software** Asset Management
  - **Configuration** Baseline Management
  - **Vulnerability** Management
- Manage Accounts
  - Manage **Trust** in People Granted Access
  - Mange Security Related **Behavior**
  - Manage **Credentials** and **Authentication**
  - Manage **Privileges**
- Manage Events
  - **Boundary** Protection
  - **Prepare** for Incidents and Contingencies
  - **Detect** Suspicious Events
  - **Respond** to Incidents and Contingencies



4 Areas of 15 Capabilities (These Must Be Applied to All Assets)
MANAGE EVENTS
Prepare for
Incidents & Contingencies
Detect
Suspicious Events/ Patterns
Respond to
Incidents & Contingencies
MANAGE SECURITY LIFECYCLE
Design & Build in Security
Document
Requirements, Policy & Planning
Manage
Quality
Manage
Risk and Investments
MANAGE ASSETS
Hardware Assets
Manage
Software Assets
Manage
Configuration Settings (CCEs)
Manage
Vulnerabilities (CVEs)
Manage
Boundaries ·Physical ·Encryption ·Filters
Manage
MANAGE ACCOUNTS FOR PEOPLE & SERVICES
Trust in People Granted Access
Manage
Security Related Behavior
Manage
Credentials & Authentication
Manage
Privileges (and Accounts)
Manage
START
END
START
END
START
END
START

FireEye

Thank You

Ron Bushar – ron.bushar@fireeye.com