FireEye

From the field

Cyber Threat Landscape

Cyber Threat Intelligence

Anca Holban
Systems Engineer – Central and Eastern Europe

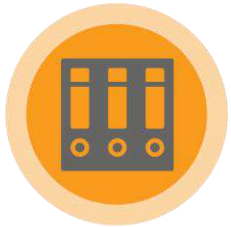
What is Mandiant Consulting… one of FireEye's souls

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

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

14+ years responding to and remediating headline breaches

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

M-Trends: Tracking our investigative experience

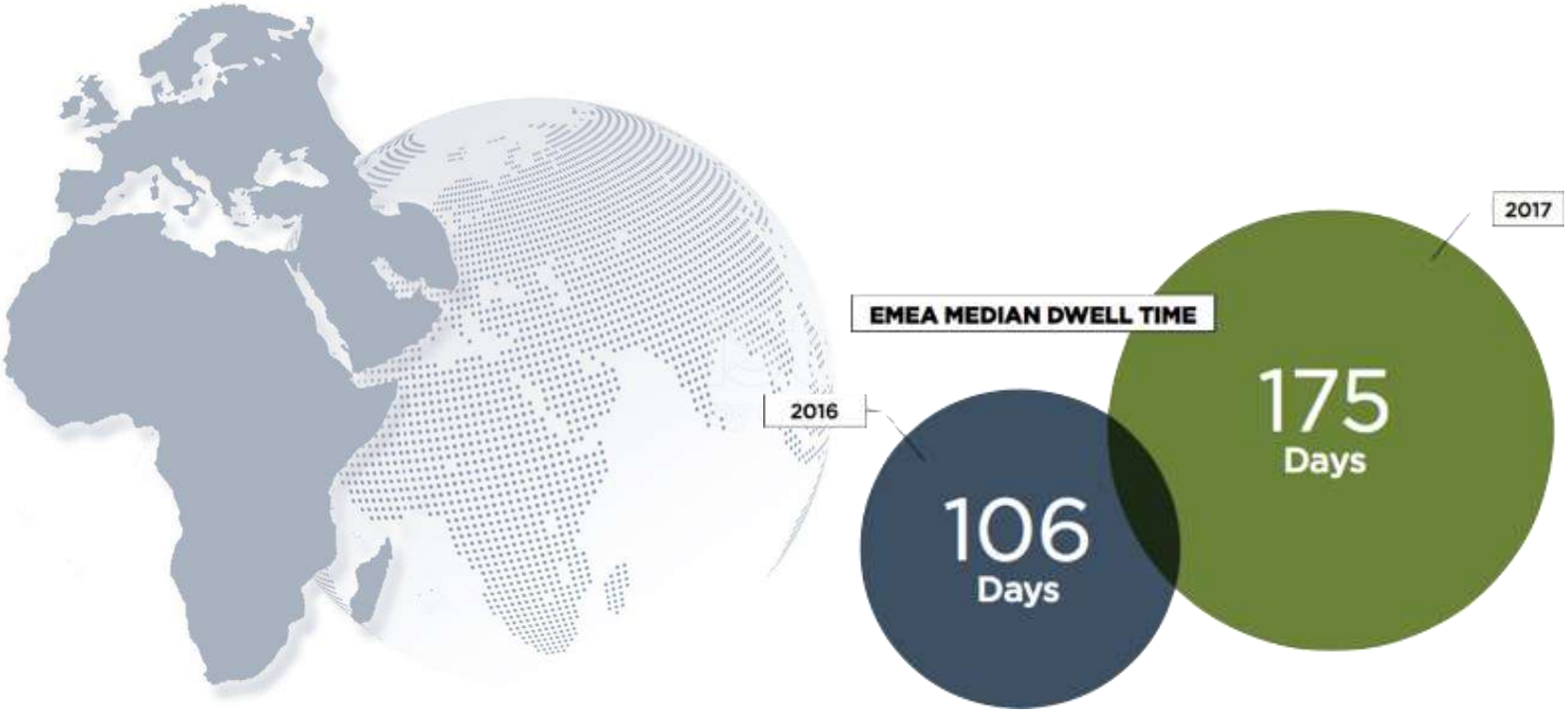
- Informing the cyber security community since 2010
- Annual publication sought after by security professionals and market analysts
- Data based on **12 months of forensic investigative findings** (10/01/16 – 09/30/17)

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

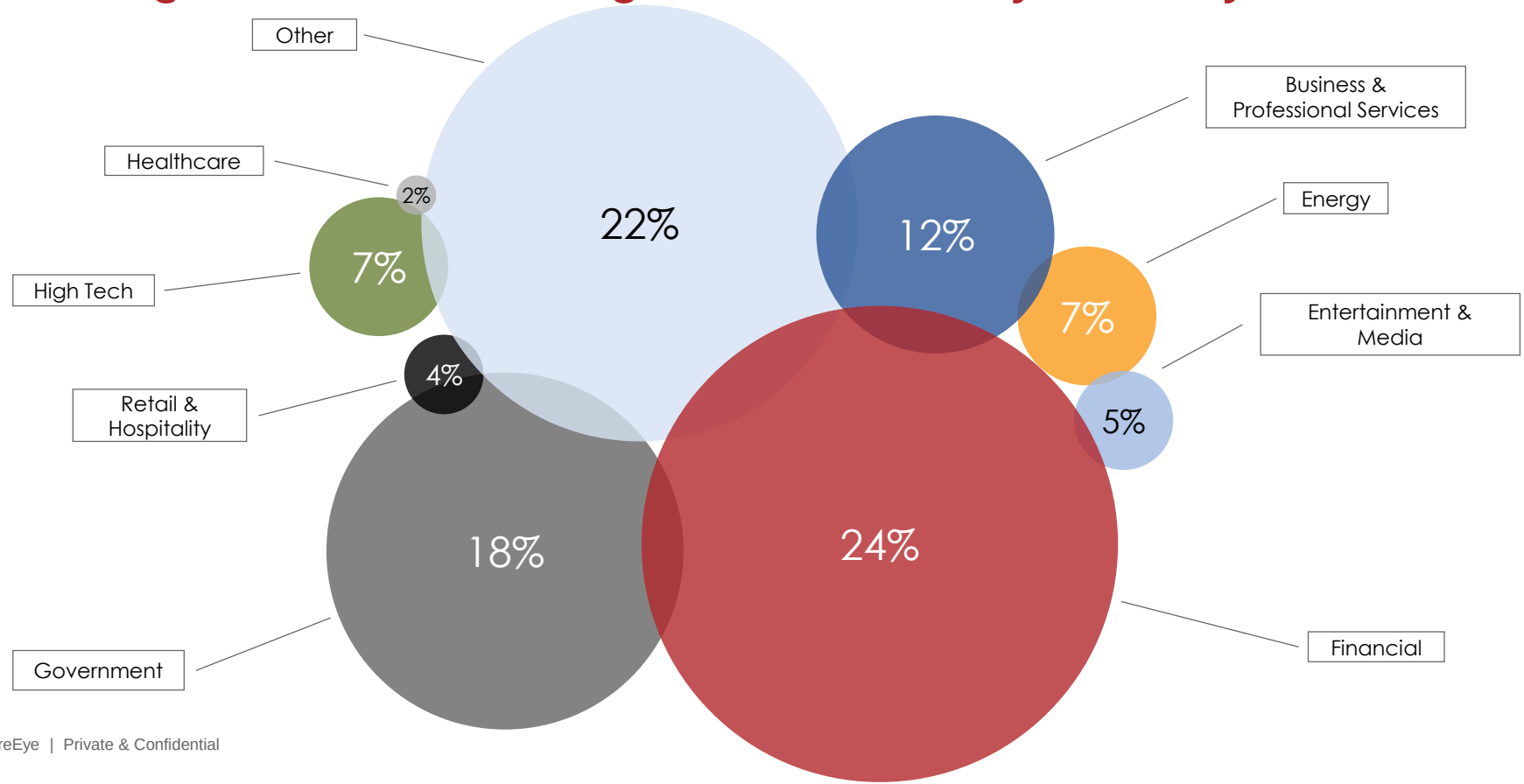
FireEye

What would you do if you had 101 days of time?

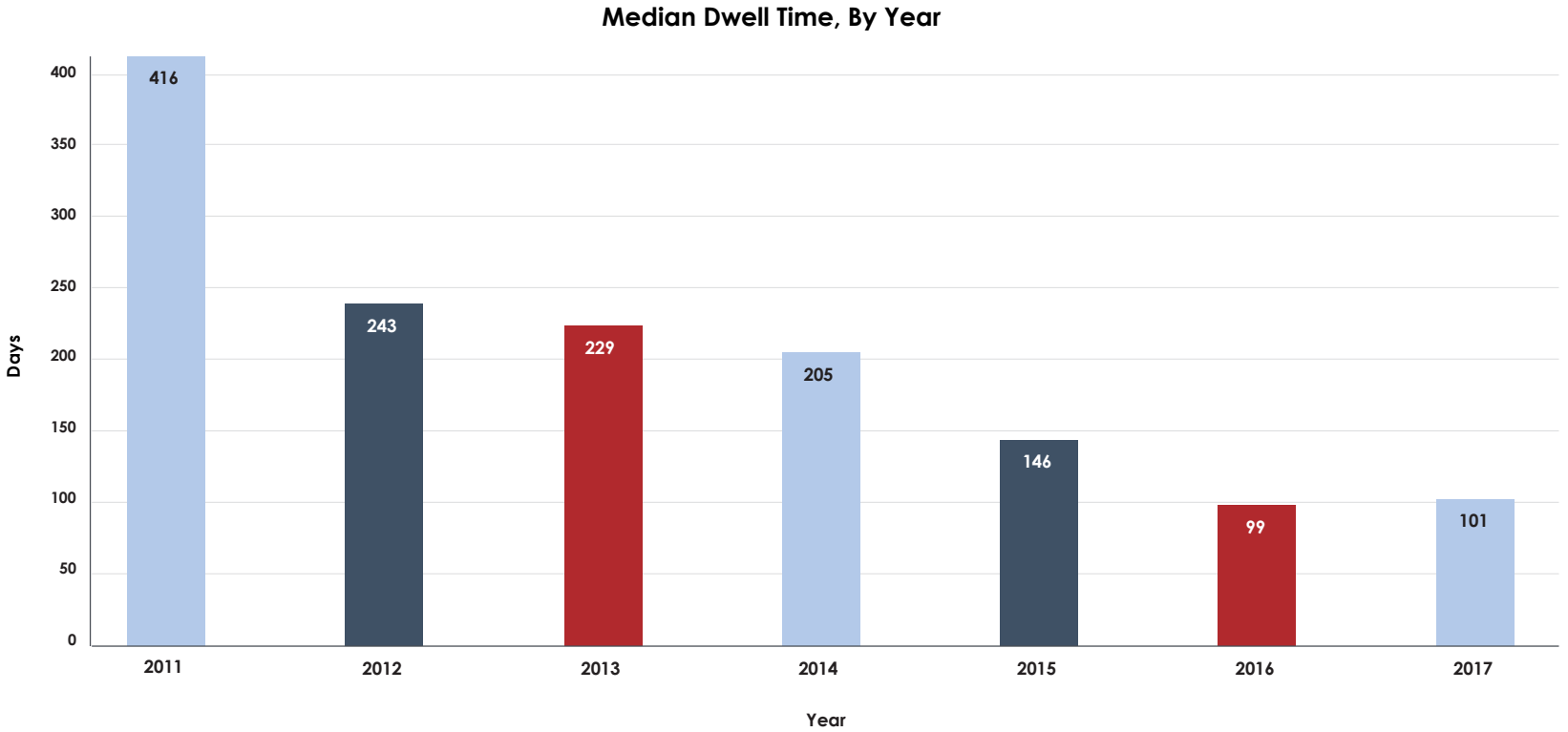
Zoom in to EMEA



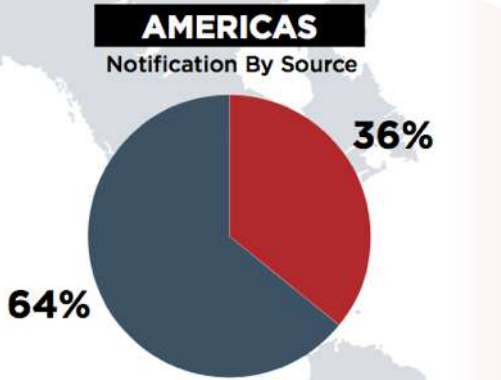
EMEA organizations investigated in 2017, by industry

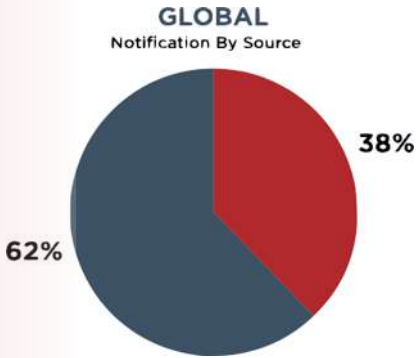


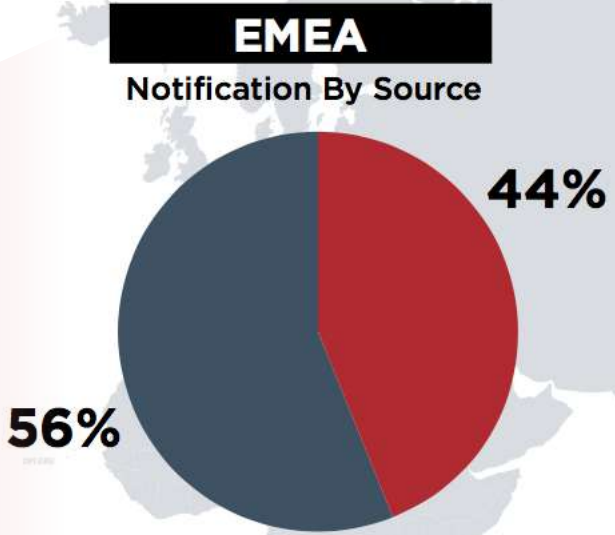
Median Dwell Time Trending



Notification by Source







External Notification

Internal Notification

FireEye

Cyber Security Skills Gap – The Invisible Risk

The Gap, according to Mandiant CDC Engagements

LACK OF EXPERTISE
- CYBER DEFENDERS
- INVESTIGATORS
- THREAT ANALYSTS

LACK OF PROCESSES
- ACTIONABLE THREAT INTEL
- TELEMETRY PRIORITIZATION
- ORCHESTRATION

LACK OF PEOPLE
- NUMERIC (9/12 PER CDC)
- 24/7 AVAILABILITY
- EXTENSIBLE IN EMERGENCY

Enduring Trends in Security Fundamentals

Security Risk Management

Identity and Access Mgmt

Data Protection

Network, Cloud & DC Protection

Incident Response

Host and Endpoint Protection

Expertise at your fingertips: Global view, local perspectives

1000+ global security experts | 24x7x365 visibility:
7 Global SOCs | 100K IR hours/year | Track 16K threats
300+ consultants | 26 countries
150+ intelligence personnel | 30+ languages | 22 countries

Newly Named APT Groups

ATTRIBUTION – relate activity to a specific sponsoring nation

Identify TTPs

Targeting specific VERTICAL or GEO

Specific MOTIVATION – hacktivism, financial etc.

APT32

APT 32
March 20, 2017

- Known as OceanLotus Group
- Vietnamese threat group
- Primary targets:
  - Journalists
  - Dissidents
  - Foreign corporations
- Leveraged social engineering emails with Microsoft ActiveMime file attachments to deliver malicious macros

APT33

APT 33
August 21, 2017

- Iranian threat group
- Targets
  - Defense
  - Aerospace
  - Petrochemical
  - Western companies who support Saudi Arabia's military
- Uses public and non-public tools
  - DROPSHOT -> TURNEDUP
  - DROPSHOT -> SHAPESHIFT?

APT34

- Iranian threat group
- Targets Middle Eastern
  - Financial
  - Government
  - Energy
  - Chemical
  - Telco
- Public and non-public tools

APT35

- Also known as Newscaster Team
- Iranian
- Targets
  - U.S. and Middle Eastern government personnel
  - Military
  - Diplomatic
  - Media
  - Energy and engineering
  - Business services and telecommunications
- Complex social engineering campaigns
- Broadening scope targets and toolsets

APT36 (Lapis)

- Pakistani espionage group
- supports Pakistani military and diplomatic interests
- Targets
  - Indian Military and government
- Operations also seen in US, Europe, Central Asia
- Social engineering emails, multiple open-source and custom malware tools

APT 36
January 2018

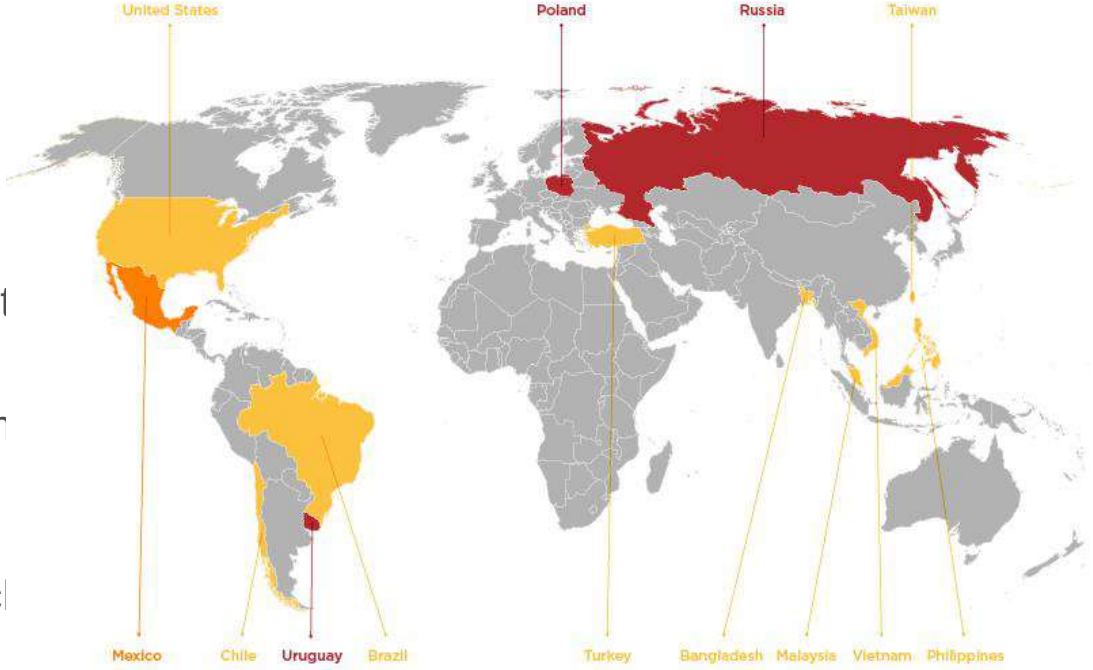
APT37 (Reaper)

- North Korea espionage group
- In 2012 targeted South Korea
- In 2017 expanded to Japan, Vietnam, Middle East
- Intelligence gathering for government
- Toolsets includes access to zero-day vulnerabilities and wiper malware

APT 37
February 2018

APT38

- North Korea threat group
- Financially motivated, backed by Nort Korean regime
- Since 2014 compromised more than 16 organizations in at least 13 different countries
- Very well planned sophisticated attac against banks



APT 38
October 2018

APT Groups

- APT0-27, 30/31 = China (APT0 was a very short lived one)
- APT28/29 = Russia
- APT32 = Vietnam
- APT33/34/35 = Iran
- APT36 = Pakistan
- APT37 = North Korea
- APT38 = North Korea

Cyber Threat Intelligence

Most people confuse

with Intelligence

Information versus Intelligence

INFORMATION	INTELLIGENCE
Raw, unfiltered data	Processed, sorted, and distilled information

Information versus Intelligence

INFORMATION	INTELLIGENCE
Raw, unfiltered data	Processed, sorted, and distilled information
Unevaluated when delivered	Evaluated and interpreted by trained expert analysts

Information versus Intelligence

INFORMATION	INTELLIGENCE
Raw, unfiltered data	Processed, sorted, and distilled information
Unevaluated when delivered	Evaluated and interpreted by trained expert analysts
Aggregated from virtually every source	Aggregated from reliable sources and cross correlated for accuracy

Information versus Intelligence

INFORMATION	INTELLIGENCE
Raw, unfiltered data	Processed, sorted, and distilled information
Unevaluated when delivered	Evaluated and interpreted by trained expert analysts
Aggregated from virtually every source	Aggregated from reliable sources and cross correlated for accuracy
May be true, false, misleading, incomplete, relevant, or irrelevant	Accurate, timely, complete (as possible), assessed for relevancy

Information versus Intelligence

INFORMATION	INTELLIGENCE
Raw, unfiltered data	Processed, sorted, and distilled information
Unevaluated when delivered	Evaluated and interpreted by trained expert analysts
Aggregated from virtually every source	Aggregated from reliable sources and cross correlated for accuracy
May be true, false, misleading, incomplete, relevant, or irrelevant	Accurate, timely, complete (as possible), assessed for relevancy

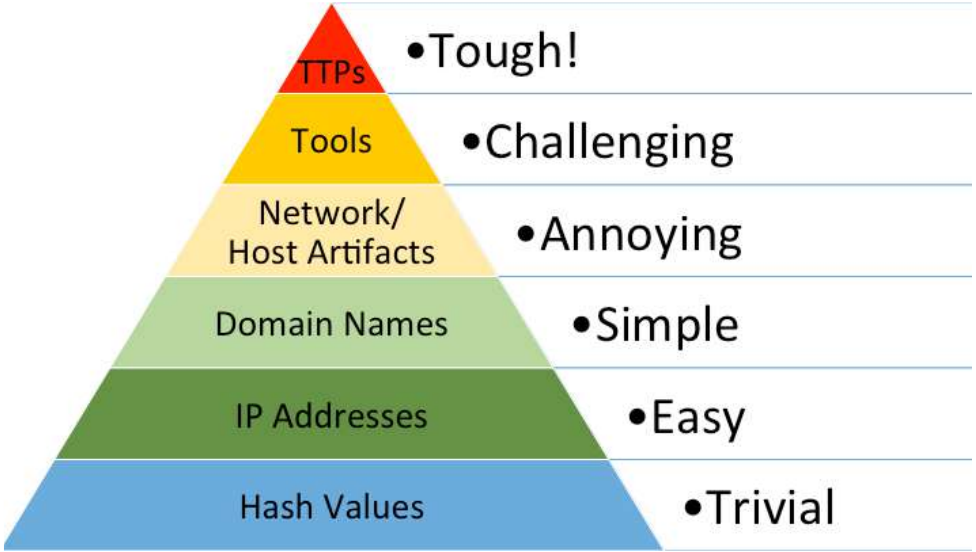
Or as the FBI put it: *"simply defined, intelligence is information that has been analyzed and refined so that it is useful to policymakers in making decisions – specifically, decisions about potential threats to our national security."*

Cyber Threat Intelligence

Purpose of Intelligence

- To **reduce the degree of uncertainty** about an adversary, or potential adversary, situation or threat which may be experienced by decision makers.
- To convey the truth to decision makers and **provide managers with accurate information** so they can **make informed, reasoned, and timely decisions**.

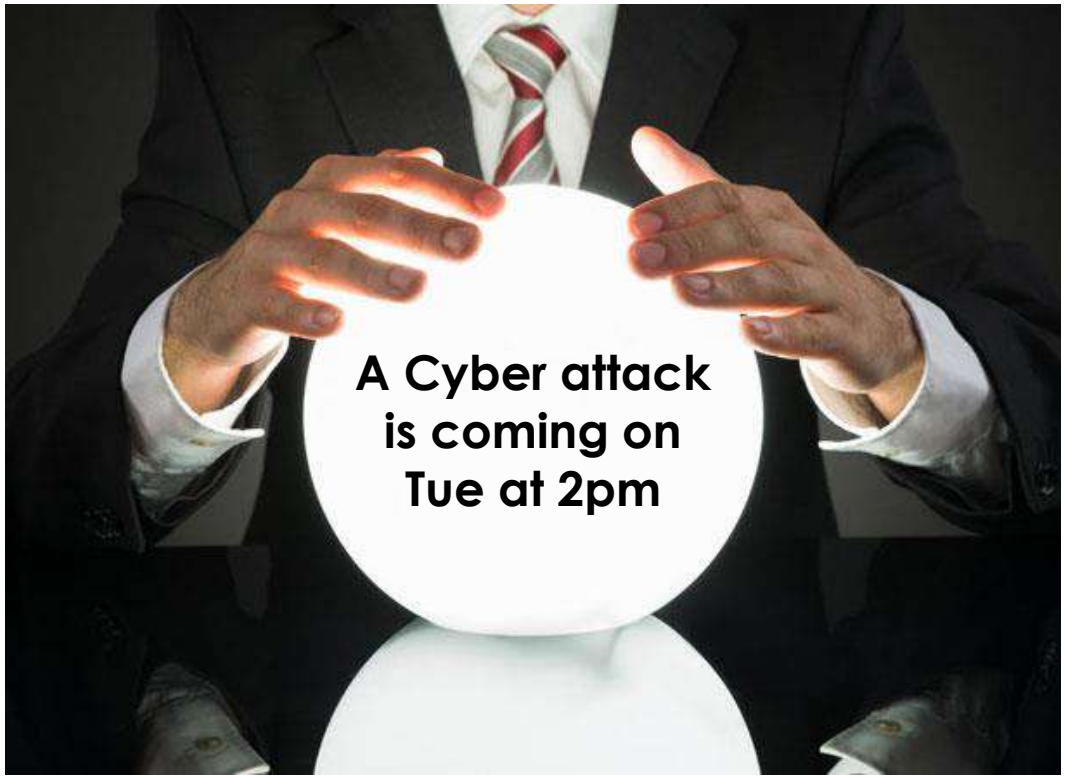
The Pyramid of Pain



FireEye

How To Think about Threat Intelligence

How NOT To Think About Threat Intelligence



How To Think About Threat Intelligence

Strategic

Future oriented

- Use emerging trends and patterns to make long-term decisions
- Helping business decision makers to reduce risk

Executives

Intel Analysts

How To Think About Threat Intelligence

Strategic

Future oriented

- Use emerging trends and patterns to make long-term decisions
- Helping business decision makers to reduce risk

Operational

Prioritize Resources for "real" versus "perceived" threats

- Consider historical capabilities, affiliations, and motivations of actors
- Factor business outcomes of threats into detection, mitigation strategies and priorities

Executives

Intel Analysts

Incident Response

Security Operations

How To Think About Threat Intelligence

Strategic

Future oriented

- Use emerging trends and patterns to make long-term decisions
- Helping business decision makers to reduce risk

Operational

Prioritize Resources for "real" versus "perceived" threats

- Consider historical capabilities, affiliations, and motivations of actors
- Factor business outcomes of threats into detection, mitigation strategies and priorities

Tactical

Interactive analysis and intelligence flow between internal and partner technology tools and threat environment

- Prioritize mitigation and triage resources leveraging intel in real time
- Factor business outcomes of the threats/vulns into mitigation actions

Executives

Intel Analysts

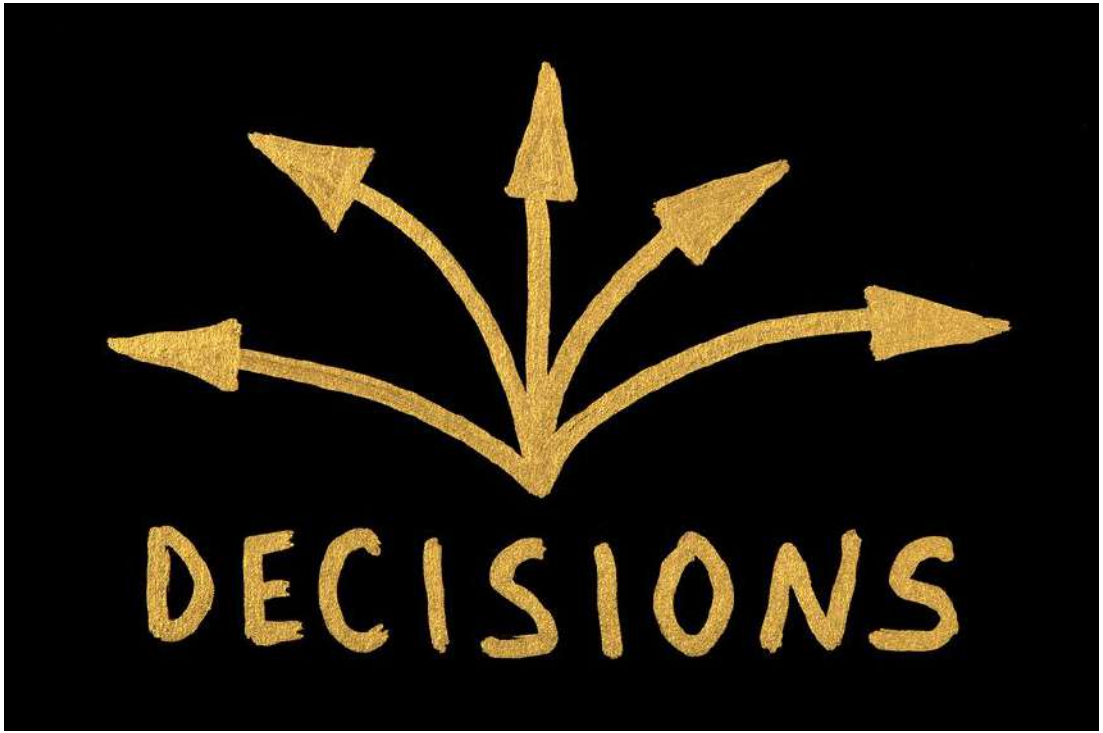
Incident Response

Security Operations

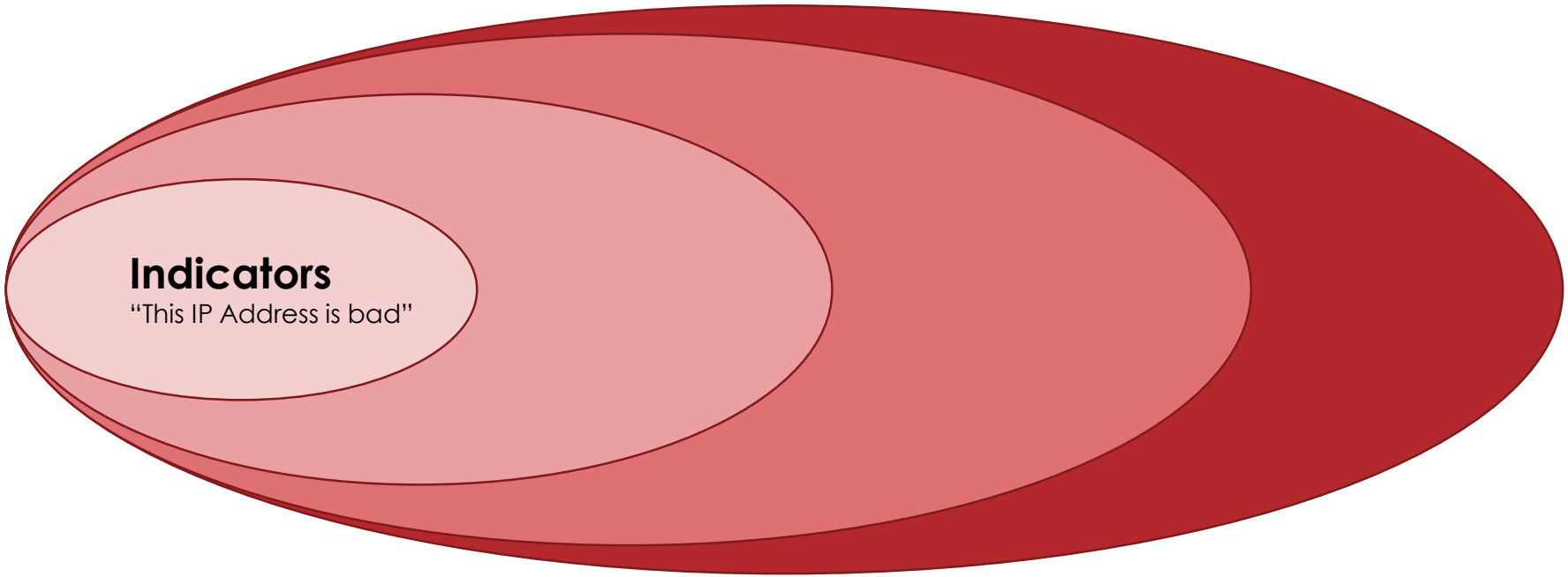
Infrastructure Operations

Vulnerability Management

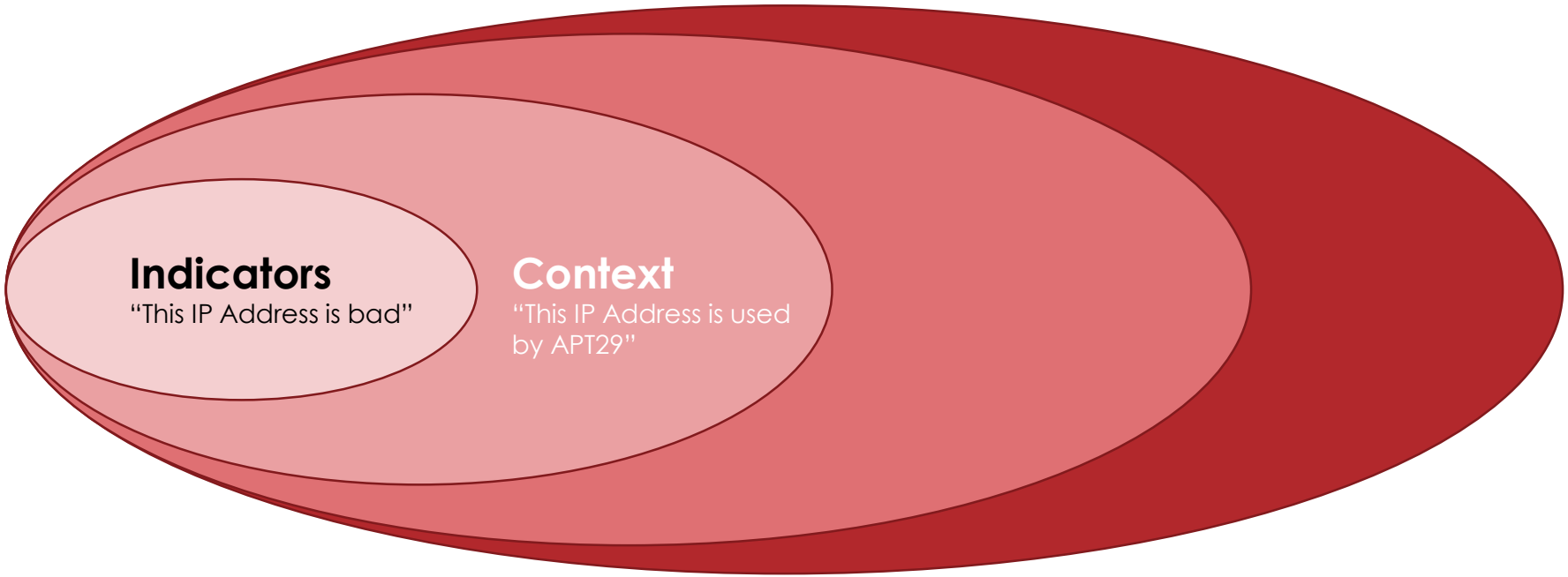
How To Think About Threat Intelligence



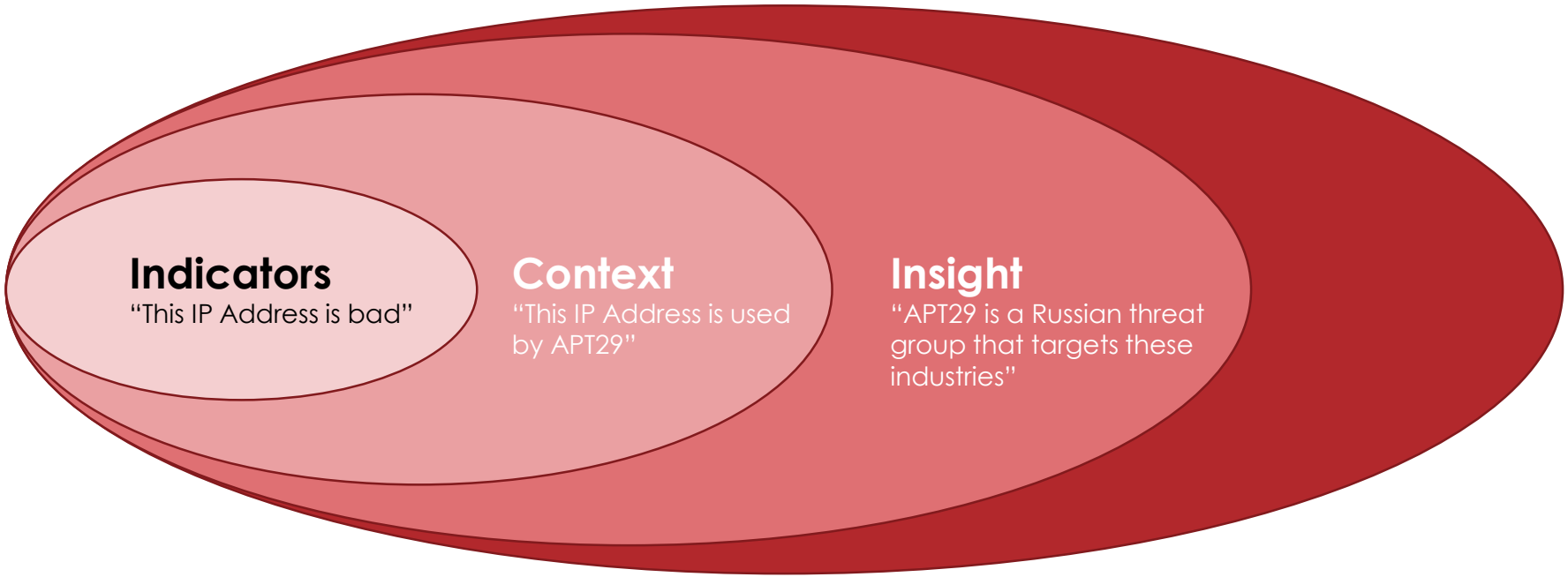
Not all Intel is created equal : From Indicators to Expertise



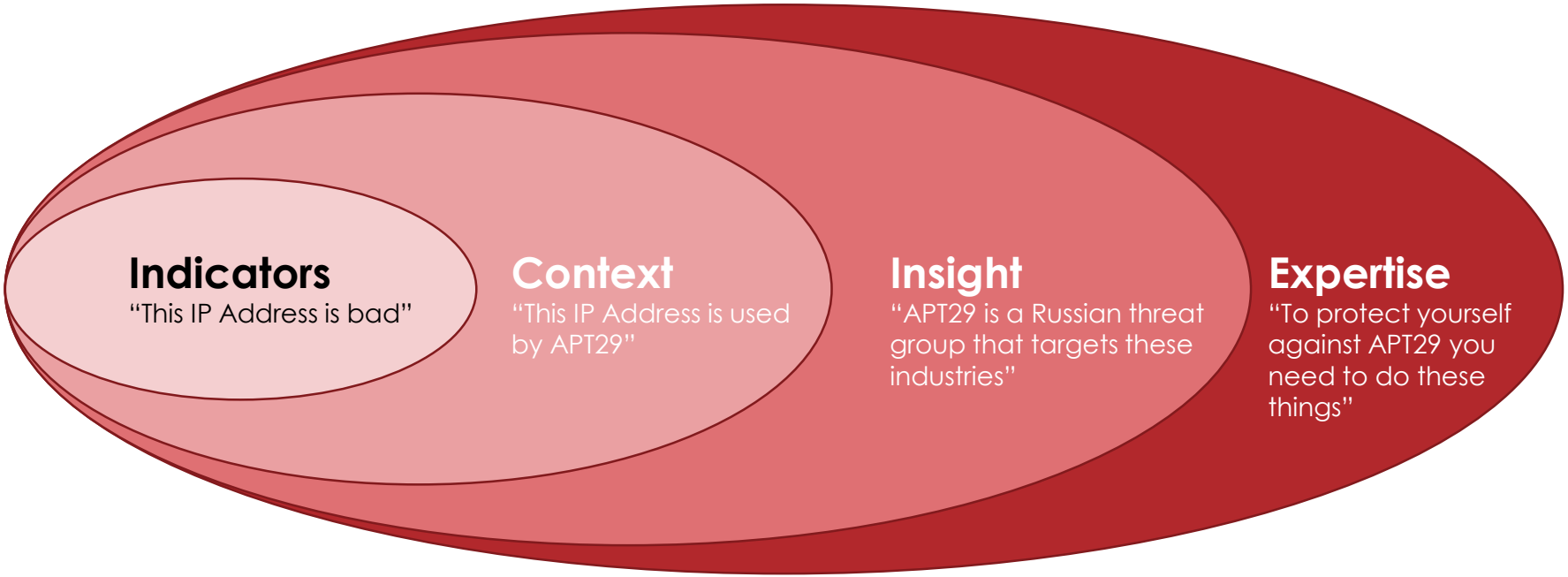
Not all Intel is created equal : From Indicators to Expertise



Not all Intel is created equal : From Indicators to Expertise

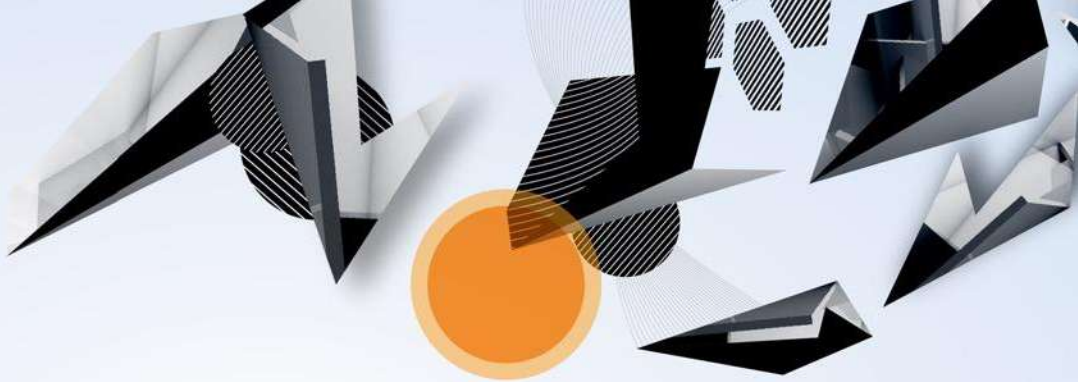


Not all Intel is created equal : From Indicators to Expertise



What Happens if You Are Breached and Do Not Utilize Threat Intelligence? Time-to-Respond Can Be Months, Not Days

FireEye



Thank you!

anca.holban@fireeye.com