2016 THREAT BRIEFING

“GOOD ENOUGH” IS NOT GOOD ENOUGH

FireEye
CYBER DEFENSE LIVE
SEOUL | 2016

GRADY SUMMERS
CHIEF TECHNOLOGY OFFICER

FireEye
SECURITY REIMAGINED

AGENDA

M-TRENDS BY THE NUMBERS

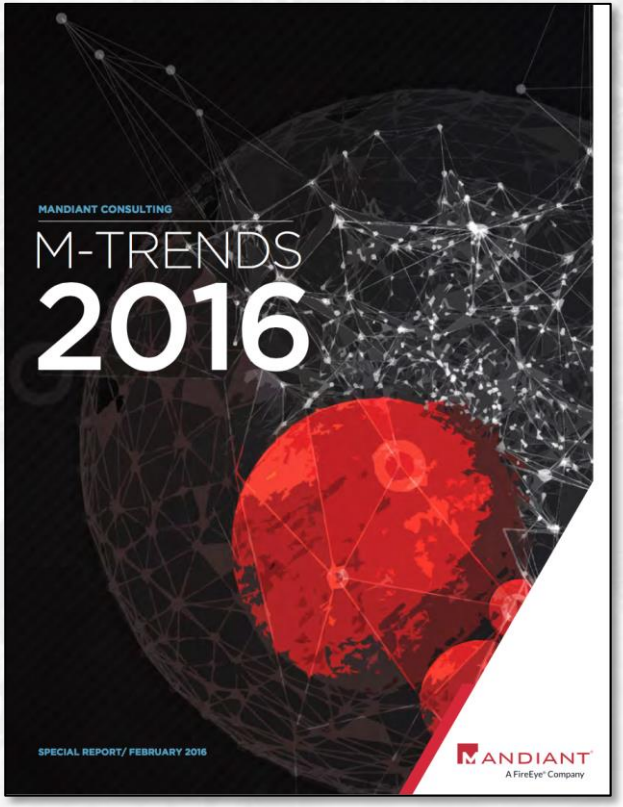
WHAT WE'VE LEARNED

CASE STUDIES

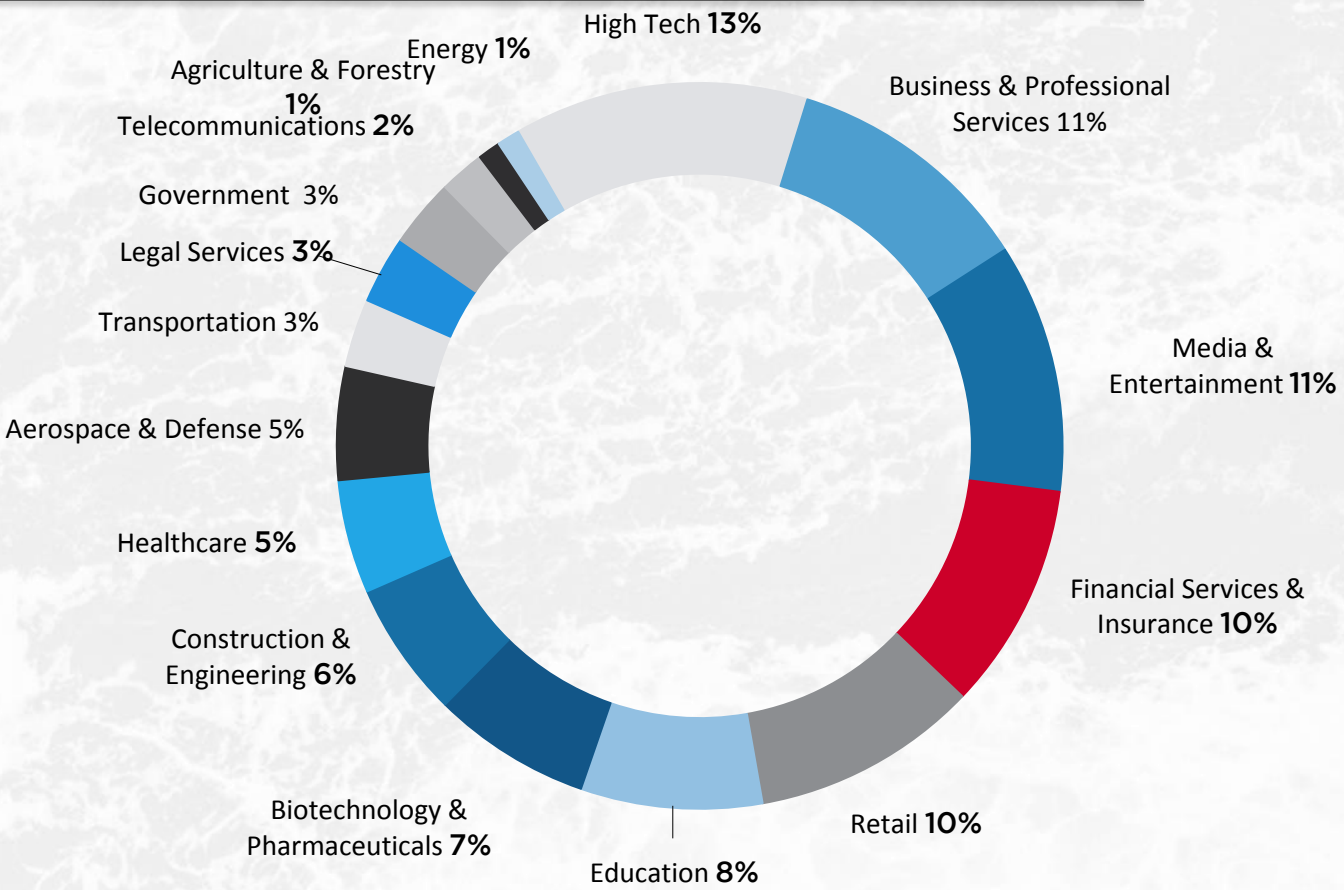
GOOD ENOUGH IS NOT GOOD ENOUGH

THE FIREEYE PLATFORM

M-TRENDS 2016



INCIDENTS BY INDUSTRY



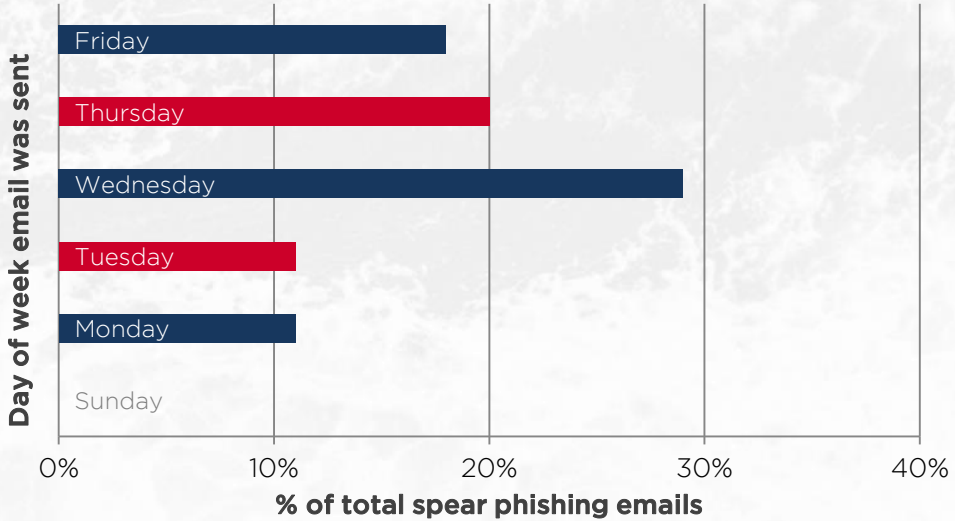
BY THE NUMBERS

Median Days from Compromise to Discovery

All Mandiant Investigation in 2015	External Notification	Internal Discovery
146 days	320 days	56 days

Day of Week of Spearphishing Frequency

DAY	SUM OF PERCENTAGE
Sunday	0%
Monday	11%
Tuesday	11%
Wednesday	29%
Thursday	20%
Friday	18%
Saturday	10%



WHAT WE'VE LEARNED

2015 - 2016

PII TARGETED BY STATE-SPONSORED ATTACKERS

A SHIFT IN STRATEGY


BUSINESS DISRUPTION ATTACKS
MORE COMMON THAN EVER


ENTERPRISE NETWORK DEVICES
ARE NOW A TARGET


SERVICE PROVIDER
COMPROMISES
AN ALTERNATE PATH TO VICTIMS


Passwo
KEY WEAKNESSES
AUTHENTICATION, DETECTION, EGRESS POINTS


RED TEAMING
TEST YOURSELF LIKE AN ATTACKER

CASE STUDIES

APT30 APT3 APT5 APT10 FIN1 APT4 APT14 APT17

APT3

- Attackers sent spear phishing e-mails to multiple targets
  - Targets included two key financial organizations
- Malicious links dropped backdoor onto victim's system.
- Actors targeted employees with expertise in:
  - Fixed income
  - Mortgage sales
  - Macroeconomic trends & analysis

International Bank

- Multiple China-based threat actors gained access for 730 days
- Conducted aggressive reconnaissance on the network
  - Compromised 9 key systems, accessed another three
  - Compromised about 7 accounts overall, some possessed administrator privileges
- Intruders likely looking for insights into infrastructure investments
  - Intrusions occurred during the contentious debate between the U.S. and China on international development banks

APT10

- Activity over the last year, compromising an east Asian manufacturer and two Japanese public policy organizations
- Have used video game themed phishing emails, which install an actual (trojanized) video game; primarily Angry Birds and Block
  - Other phishing emails are poorly worded and minimally researched
- Uses KABOB backdoor to maintain persistence
- Other APT10 malware is commonly self-signed and suffers from high detection rates by commercial AV

WHAT IS WORKING?

Move sensitive data to its own network

Ensures that attackers cannot easily move from one segment of the network to another.

Improve control over powerful accounts

Requires the most powerful accounts to be checked in / out prior to usage, usually protected by two-factor authentication.

Promote a "Security Culture"

Senior executives set the tone in any successful initiative. Security orgs often need increased support for new controls like two-factor access, incident response plan testing, etc.

Focus on phishing prevention

Phishing (luring users to click on malicious e-mail attachments) is still the #1 method that attackers use to compromise organizations. Most orgs are not well-protected.

Require two-factor authentication for remote access

Prevents attackers from using stolen passwords to access resources. Most companies prioritize remote access to e-mail and networks (virtual provide networks).

Only permit pre-authorized programs to run on servers

Critical systems like servers generally only need to run a small set of software--yet they are often allowed to run arbitrary programs. "Whitelisting" technology can prevent this.

Test the incident response plan

Fewer than 20% of organizations test response plans with a cross-functional team on an annual basis.

Use new technology to block advanced malware

New technologies can proactively execute and test web downloads in a secure environment (known as a "sandbox") to find malware that traditional signature-based models miss.

TOO MANY ALERTS

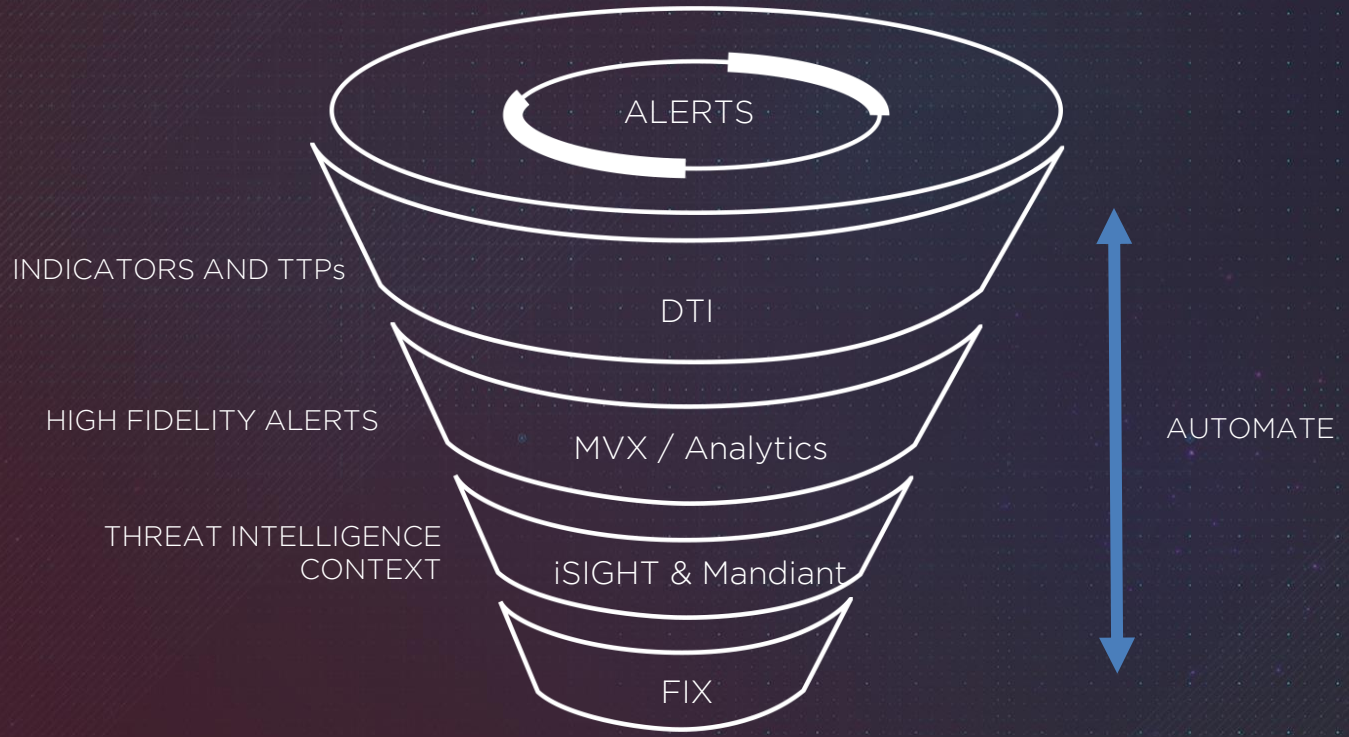
OF ALL ALERTS GENERATED IN THE ENTERPRISE,

19% ARE CONSIDERED RELIABLE

but ONLY 4% ARE INVESTIGATED

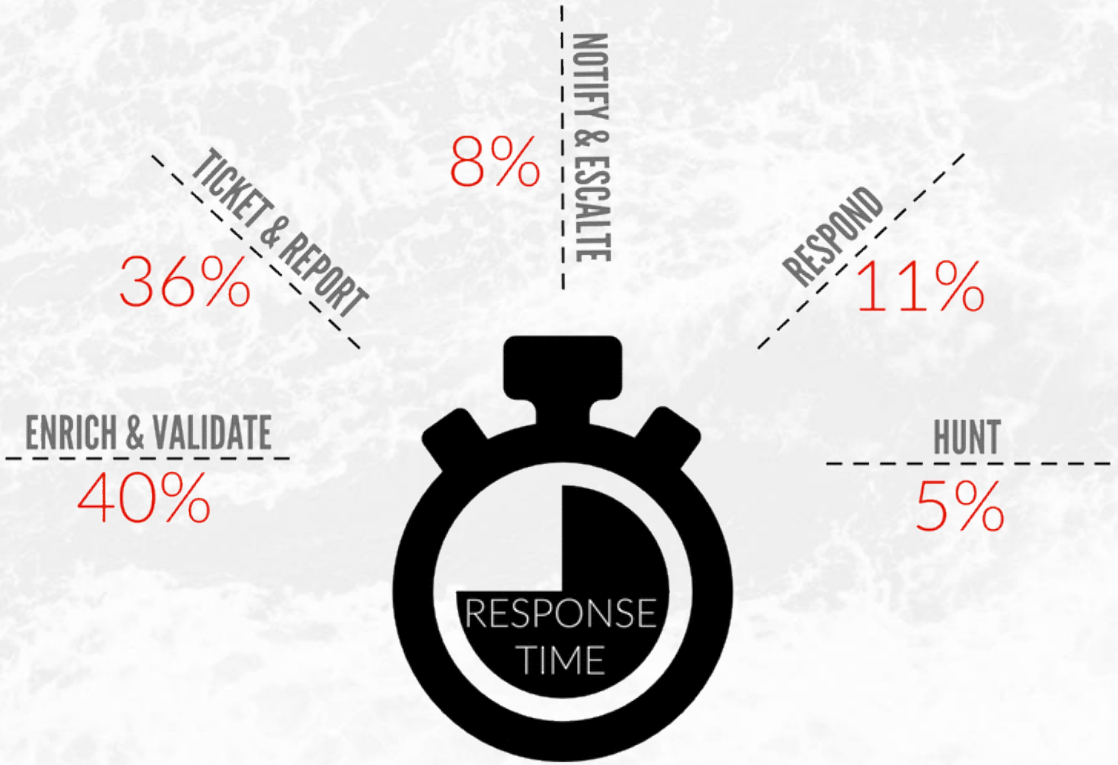
Source: The Cost of Malware Containment http://www.ponemon.org/blog/the-cost-of-malware-containment

ALERT TO FIX IN MINUTES



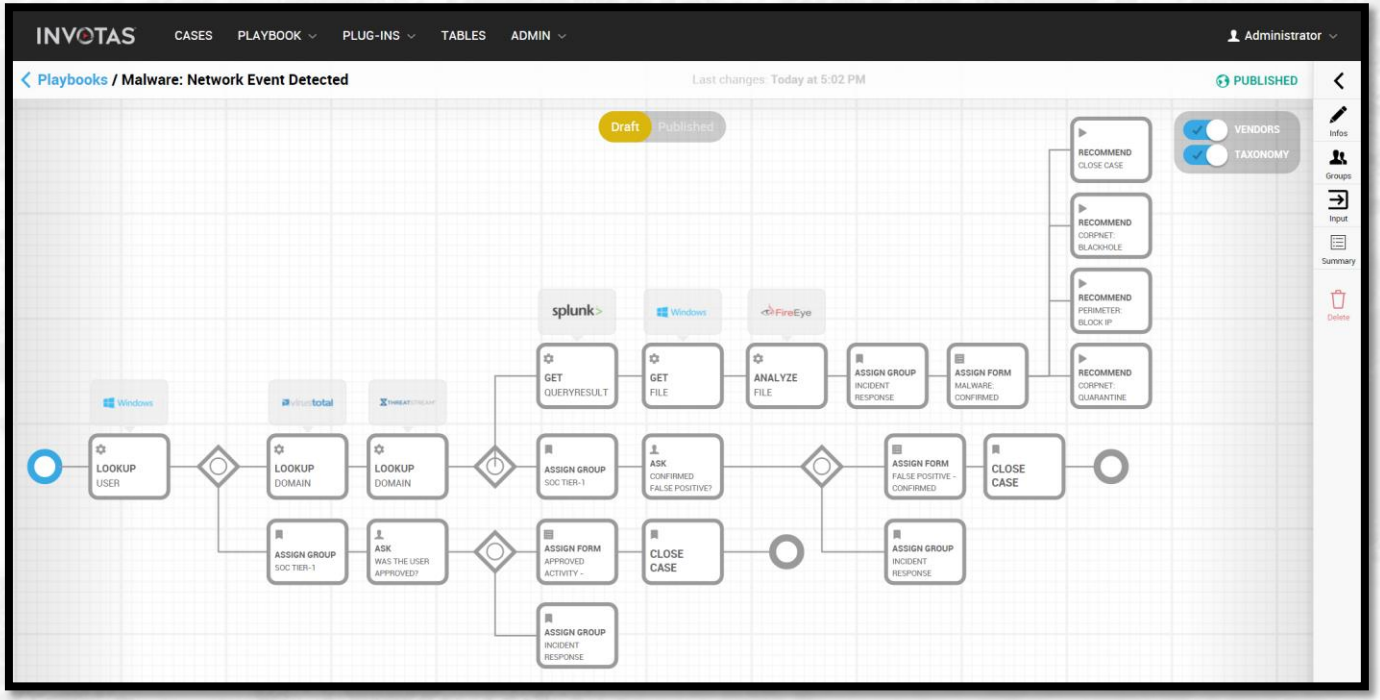
Alert to Fix: The Problem

Of all alerts generated in the enterprise, 19 percent (3,218) are considered reliable but only 4 percent (705) are investigated.



Source: The Cost of Malware Containment http://www.ponemon.org/blog/the-cost-of-malware-containment

An Answer with Automation

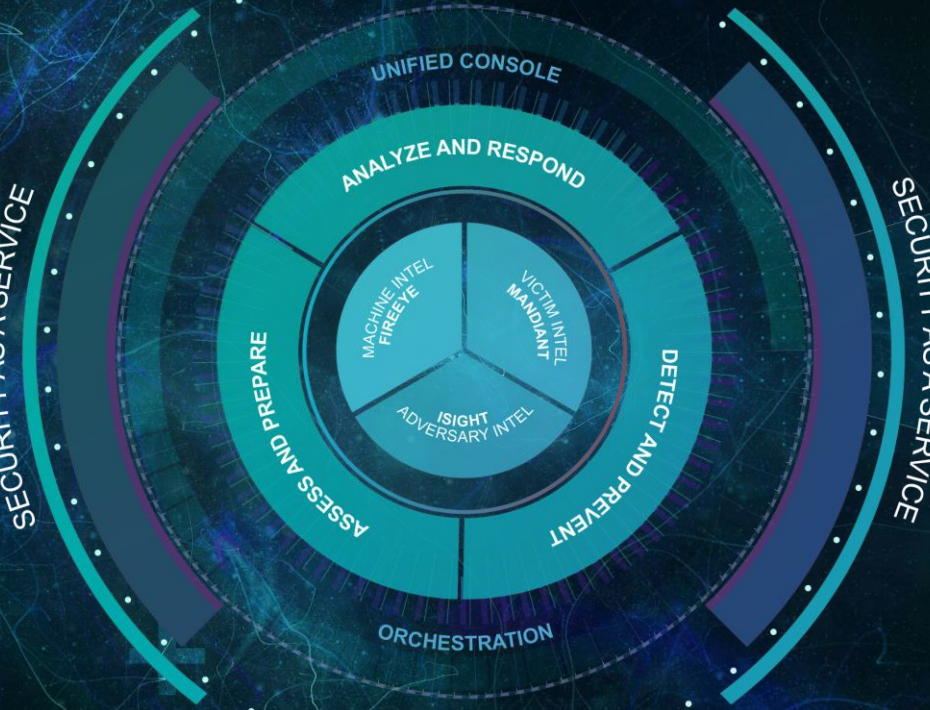


Manual

Semi Auto

Automated

GLOBAL THREAT MANAGEMENT PLATFORM



FireEye

FIREEYE TODAY

FireEye

MANDIANT

iSIGHTPARTNERS