FROM A REACTIVE SECURITY TO PROACTIVE HUNTING

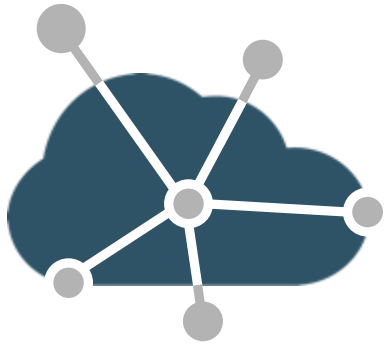
– Endpoint & Intelligence the new security pillars

FireEye
SECURITY REIMAGINED

Evolving Challenges

Macro trends imply a shifting and complex environment for enterprise security teams

**New surface,
new usage to monitor and protect**



+

**Lack of qualified
talent, Retention**

+

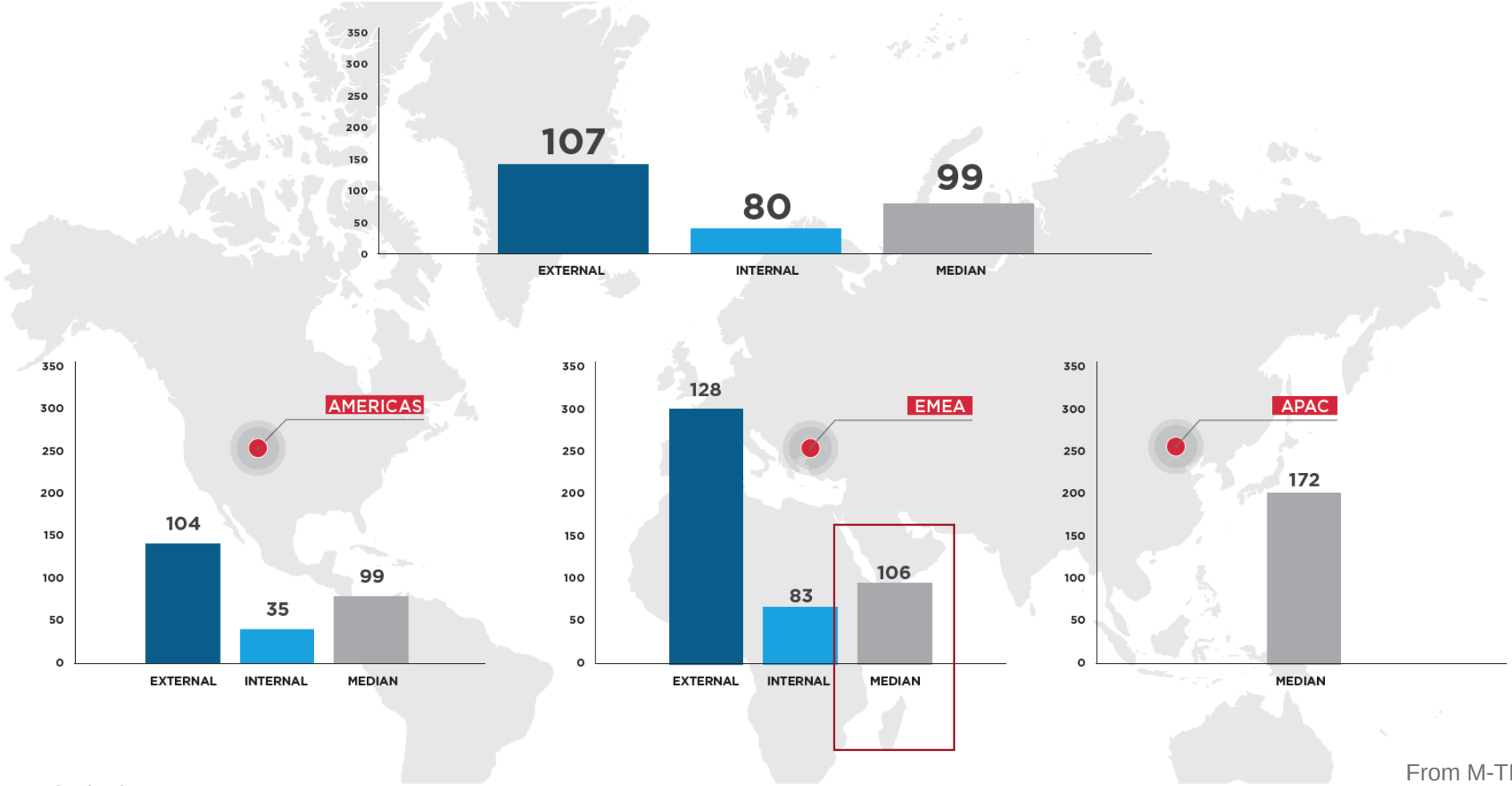
**Increasing number
of sources creating
huge volumes of data**

+

**Rapid threat evolution
creating complex and
diverse threats**

As a result

Dwell time is too long …



From M-TREND 2017

OUR ANSWERS:

How to reduce DWELL time ?
Intelligence – to focus & prioritize
Endpoint – to validate & react
Orchestration - to speed up reaction

GIVING THE ADVANTAGE BACK TO THE DEFENDERS - INTELLIGENCE

INTELLIGENCE

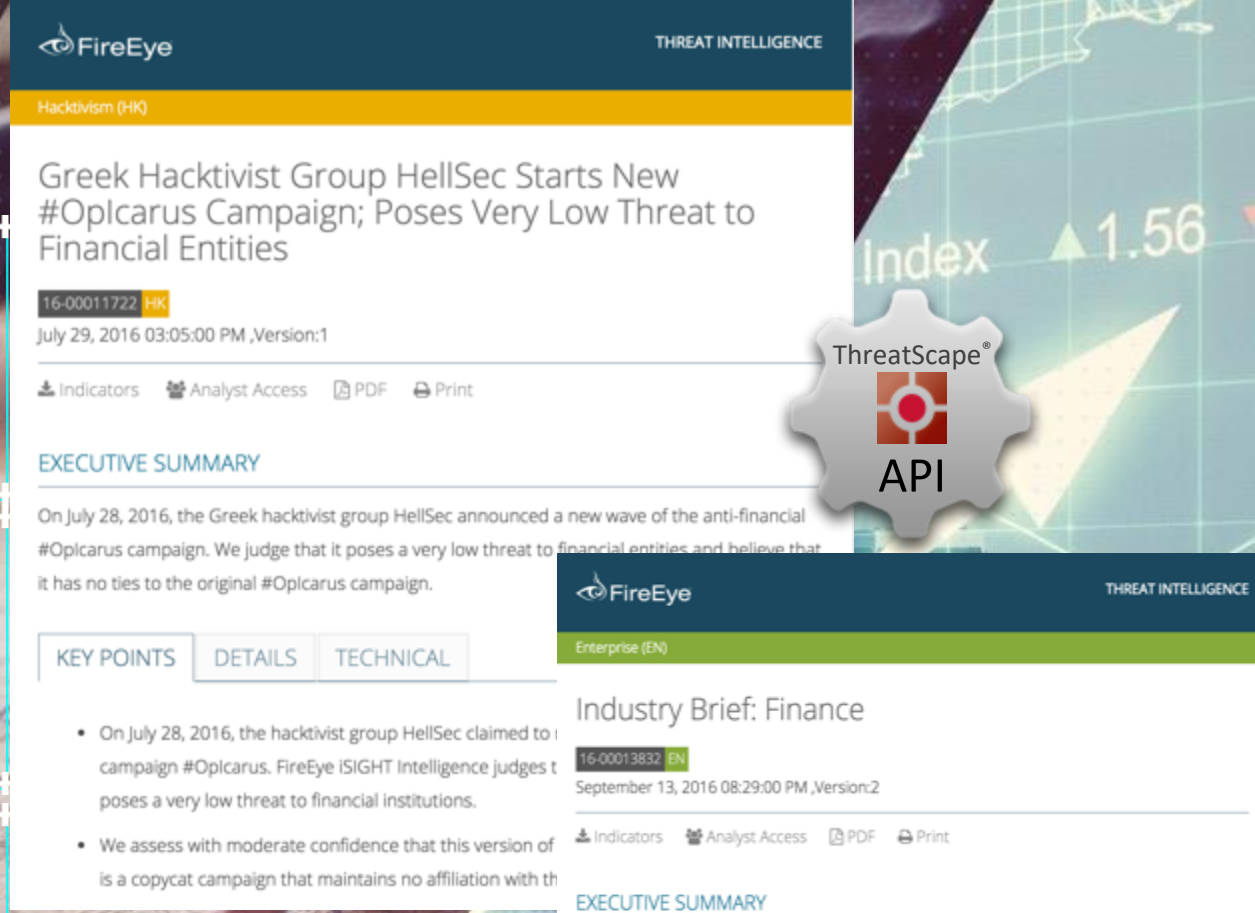
SOME NUMBERS

250 Analysts

19 countries, 29 languages

100 Millions invested

17 000 groups



FORENSICS AS A BEHAVIOR

ENDPOINT

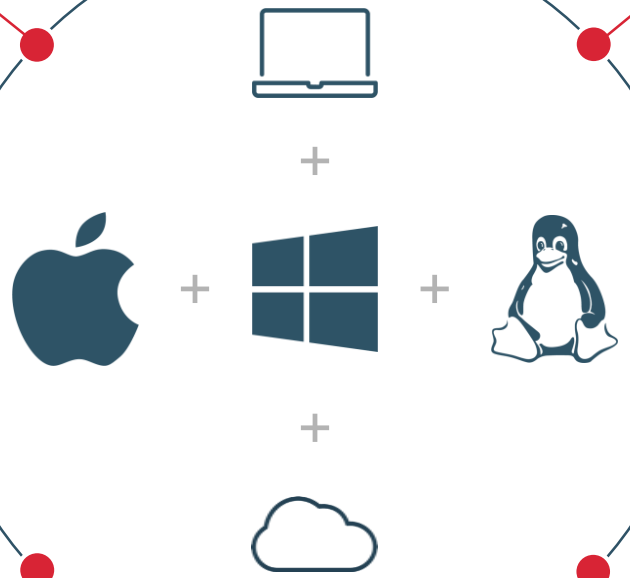
Endpoint Security Overview

Assess & Prepare

Ongoing intelligence gathering, application along with in depth endpoint status awareness

Detect & Prevent

Exploit Guard
Indicator Hunting
Network Validation
Containment
Multi engine Detection



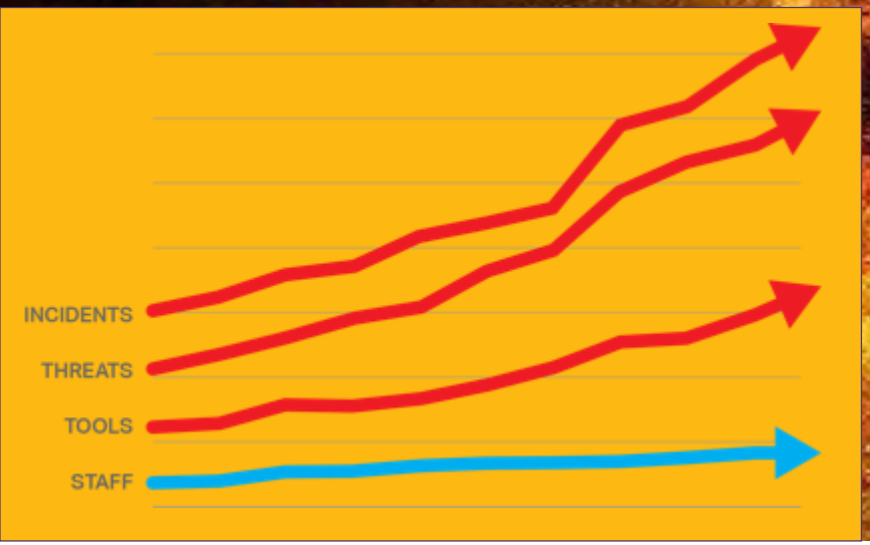
Enterprise Security Search to rapidly scan for and contain threats. Data Acquisition for in-depth endpoint inspection and analysis

Analyze & Respond

Triage and Audit
Viewer for thorough
Investigation and analysis
For any endpoint connected
To corporate network or not

Visibility & Access

AUTOMATION -- OPTIMIZATION



ORCHESTRATION

FireEye Security Orchestrator

Assess & Prepare

Automate repeatable tasks with drag and drop playbooks

Build powerful Course of Actions (CoAs) leveraging Mandiant mindset

Extricate time for hunting

Detect and Prevent

Accelerate prevention and remediation

Minimize the risk exposure window and persistence time of an attack

Recommended pivot actions to aid the analyst decision process

Analyze and Respond

Leverage the case workbench to remove friction from hundreds of point solutions

Eliminate “Swivel Chair” Investigations

Eliminate inconsistent processes

Optimize ROI / TCO

Increase efficiency and performance of security staff to “do more with less”

Enhance performance of SOC analysts

Flexible open plugin development

OUR MISSION:

To relentlessly protect our customers with innovative technology and expertise learned on the front lines

FireEye

UNIQUE TRIPLE THREAT ECOSYSTEM

FireEye

iSIGHTPARTNERS

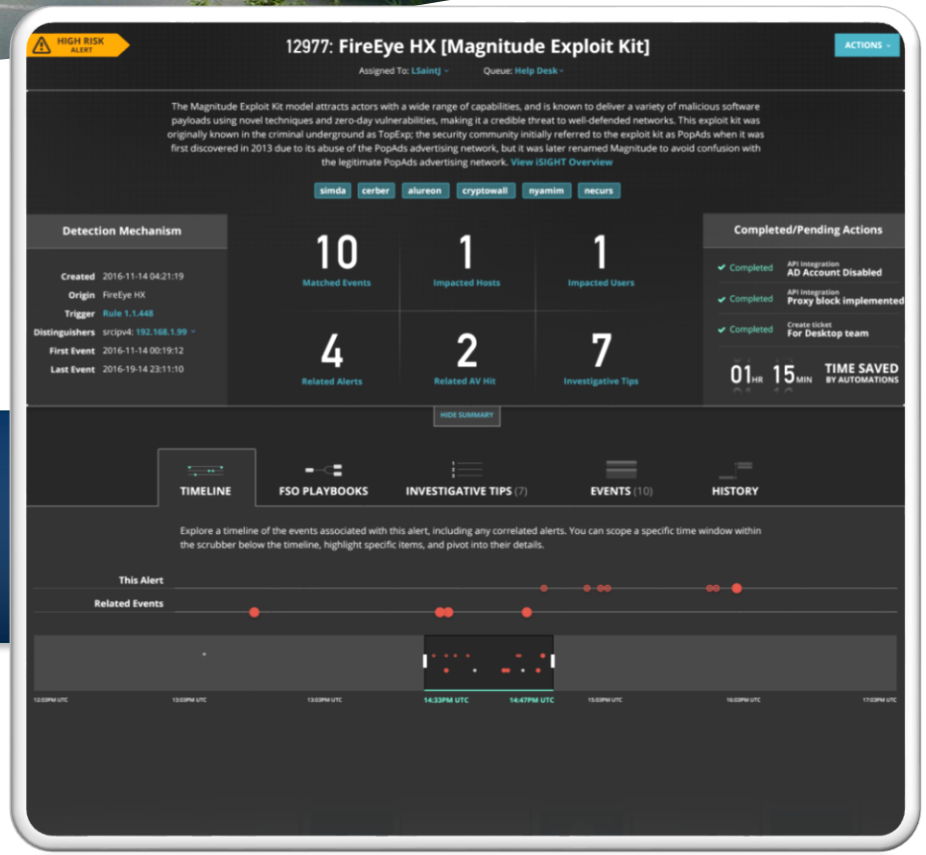
MANDIANT

HELIX- THE ANSWER

Increase expertise

Drive transformation

Protect our customers



FireEye