FireEye
SECURITY REIMAGINED

FireEye: Cloud Security Re-Imagined

Adam Palmer, Director International Government Affairs

Malaysia September 10, 2015

SECURITY
REIMAGINED

FireEye™
MANDIANT®

FireEye
SECURITY REIMAGINED

Who am I?

- FireEye Director of International Government Affairs
- Former US Government JAG Cybercrime Prosecutor
- Former Manager of UN Global Program against Cybercrime
- Lead Cybersecurity Advisor at Symantec for 3 years

GOAL

Support Good Cyber Policy

Be a Trusted Partner

My support is ALWAYS FREE

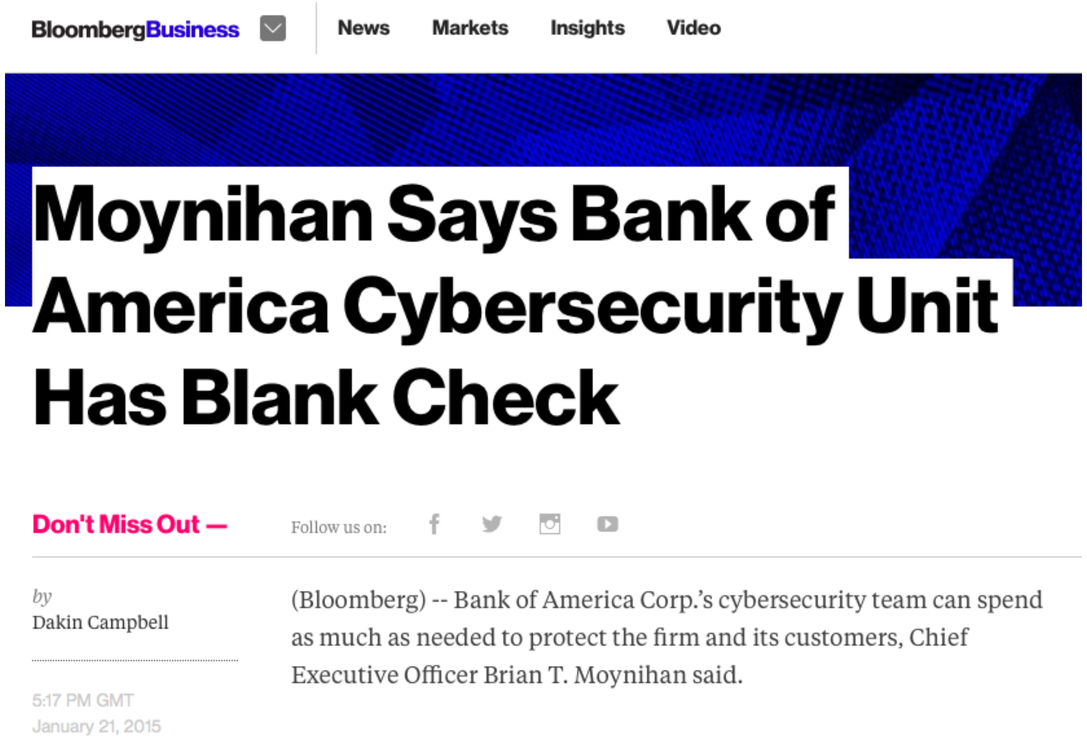
Recent Cyber Media Coverage

Dear Fellow Shareholders,

CYBER SECURITY UPDATE: POST BREACH

“By the end of 2014, we will have spent more than $250 million annually

We’re making good progress on these and other efforts, but cyberattacks are growing every day in strength and velocity across the globe. It is going to be a continual and likely never-ending battle to stay ahead of it — ***and, unfortunately, not every battle will be won****.*



Moynihan Says Bank of America Cybersecurity Unit Has Blank Check

by
Dakin Campbell

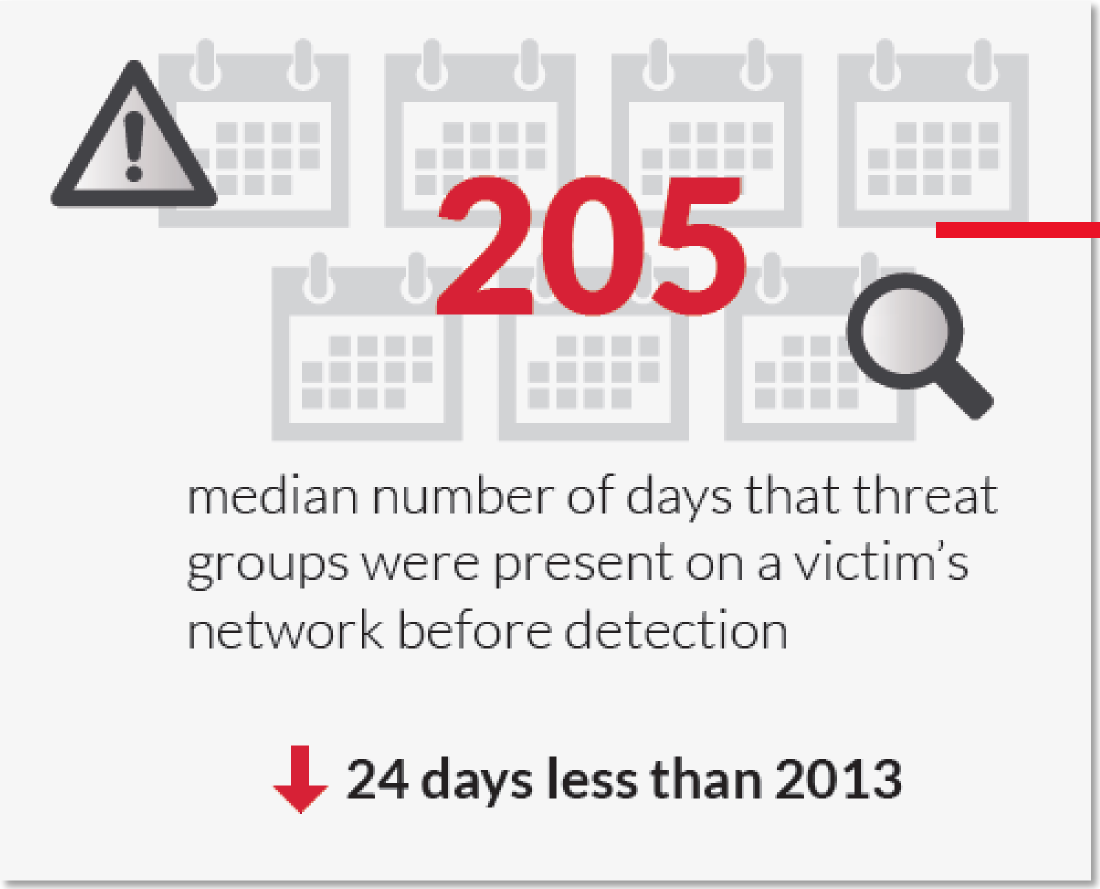
5:17 PM GMT
January 21, 2015

(Bloomberg) -- Bank of America Corp.’s cybersecurity team can spend as much as needed to protect the firm and its customers, Chief Executive Officer Brian T. Moynihan said.

M TRENDS THREAT REPORT 2015 HIGHLIGHTS

SECURITY REIMAGINED

Time for Earliest Evidence to Discovery of Compromise



205

median number of days that threat groups were present on a victim's network before detection

↓ 24 days less than 2013

Longest Presence:

2,882

Days

That's over 8 YEARS!

STUDY: KPMG SWEDEN 2014

Case Study: KPMG Sweden – May 2014

93% Of organisations were breached

79% were exfiltrating data

49% of the detected malware was unknown

- 14 Organisations across retail, government, banking & manufacturing
- 30 day assessment of network traffic

POLICY TRENDS

Australia: **CRITICAL Strategies for Cybersecurity:**

“Automated dynamic analysis of email and web content run in a sandbox to detect suspicious behavior including network traffic, new or modified files, or other configuration changes”

Japan: Toughening and adding more advanced cybersecurity measures after large governemtn breach. Advanced security is now “essential” security.

USA-: “The information system implements nonsignature-based malicious code detection

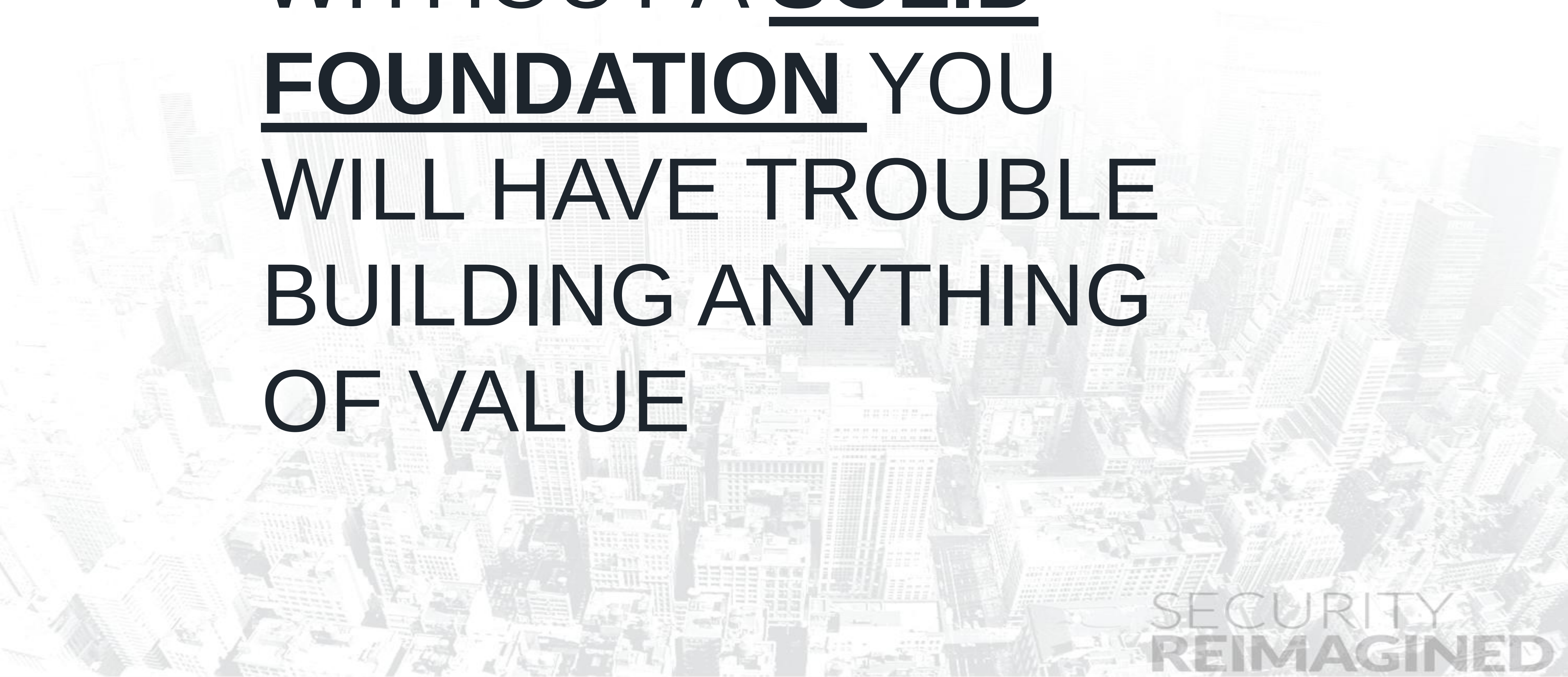
“Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems. . . and the organization employs a detonation chamber capability

Global Council on Cybersecurity: “Ensure that automated monitoring tools use behavior based anomaly detection to complement traditional signature based detection.”

Europe / Germany: “state of the art security”

- **Data Breach Reporting & Auditing**
- **National Strategy**

A “Roadmap” for Success!



WITHOUT A **SOLID FOUNDATION** YOU WILL HAVE TROUBLE BUILDING ANYTHING OF VALUE

POLICY STANDARDS ANSWER:

- WHY?
- WHAT?
- WHEN?

What are the basic goals to achieve?

- Improve security of your nation and the Internet

- Harmonize and level (uplift) the playing field between LE, Military, & Private

- Provide incentives to invest in security.

**Adapted from NIS Directive

How do you define scope?

NIS example:

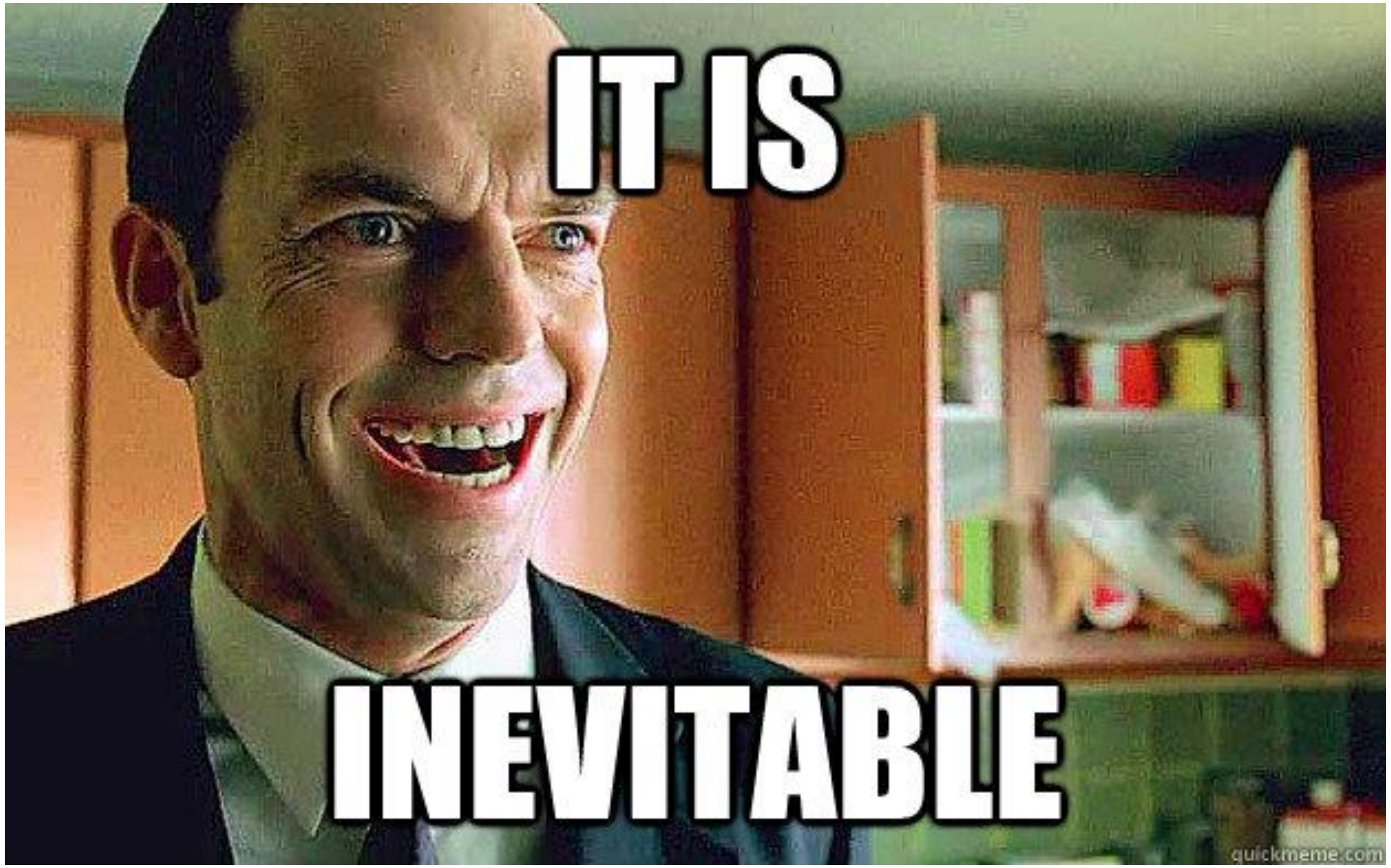
- All Member State Governments
- (binding/non-binding) duty of care?

- Critical National Infrastructure (CNI)
  - Depends on Country
  - Differentiates levels of security controls necessary for certain groups(ex. social networks)

Minimum “essential” standards: The Sinking Boat

FOUNDATIONAL TRUTHS

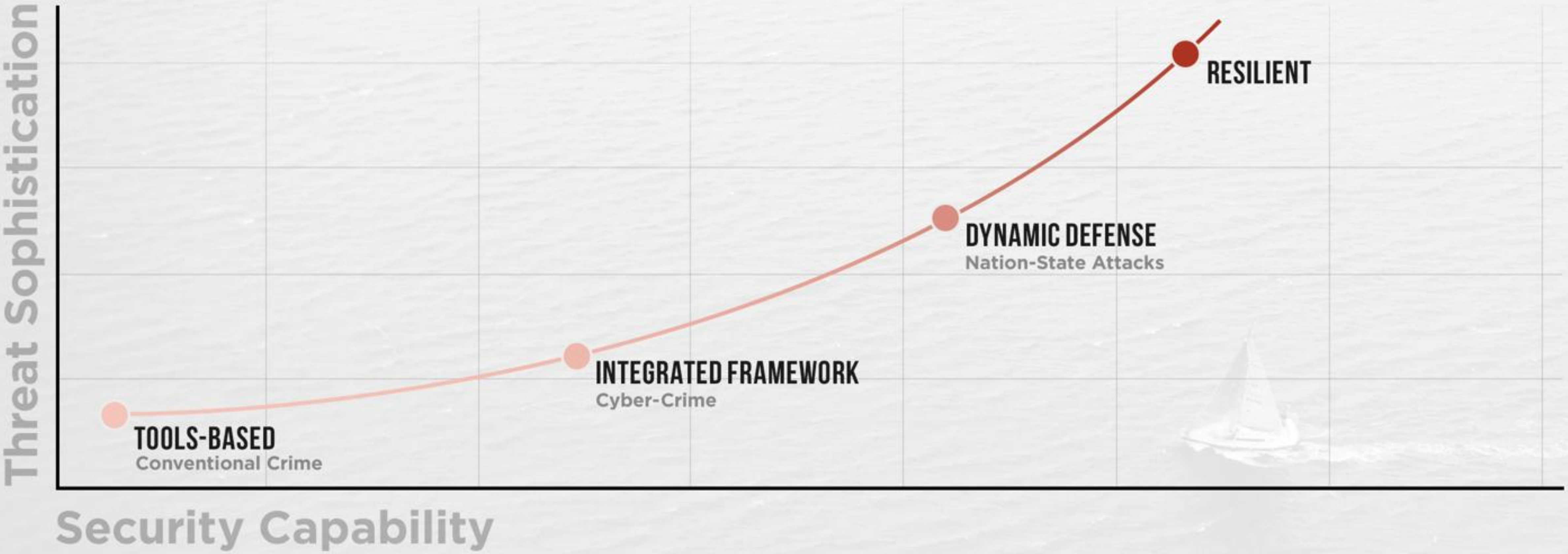
Foundational Truths #1



Foundational Truths #2

Foundational Truths #3

HOW GOOD DO YOU WANT TO BE?



FireEye
SECURITY REIMAGINED

DO NOT FEAR THE CLOUD

Moving to the cloud is a security BENEFIT:

More resources to security than the typical company that uses these services

Example: Amazon Web Services has hundreds of people focused on the security of its platform

SECURITY REIMAGINED

This is Very Helpful in Malaysia

But isn’t it better for me to see my own Data Center?

Most commercial Cloud providers have really robust logging options—better than corporate servers!

Example: Amazon Web Services has CloudTrail, a service that will enable 40+ different sub-services (access logs, usage data, file system, etc) to stream logs with the flip of a switch…

How To REALLY Secure the CLOUD

Combining AWS type robust logging with:

a service like **FireEye Threat Analytics Platform (TAP)**

Natively ingests CloudTrail--- you can **gain** superior visibility into your cloud infrastructure.

THE GOOD
THE BAD
AND THE UGLY

Predicting Rain Does Not Count, Building a Boat Does
Good policy = a strong boat

THANK YOU!

Adam Palmer
Director, International Government Affairs

adam.palmer@fireeye.com

+49-151-275-04814
Munich, Germany