RSAConference2015
San Francisco | April 20-24 | Moscone Center

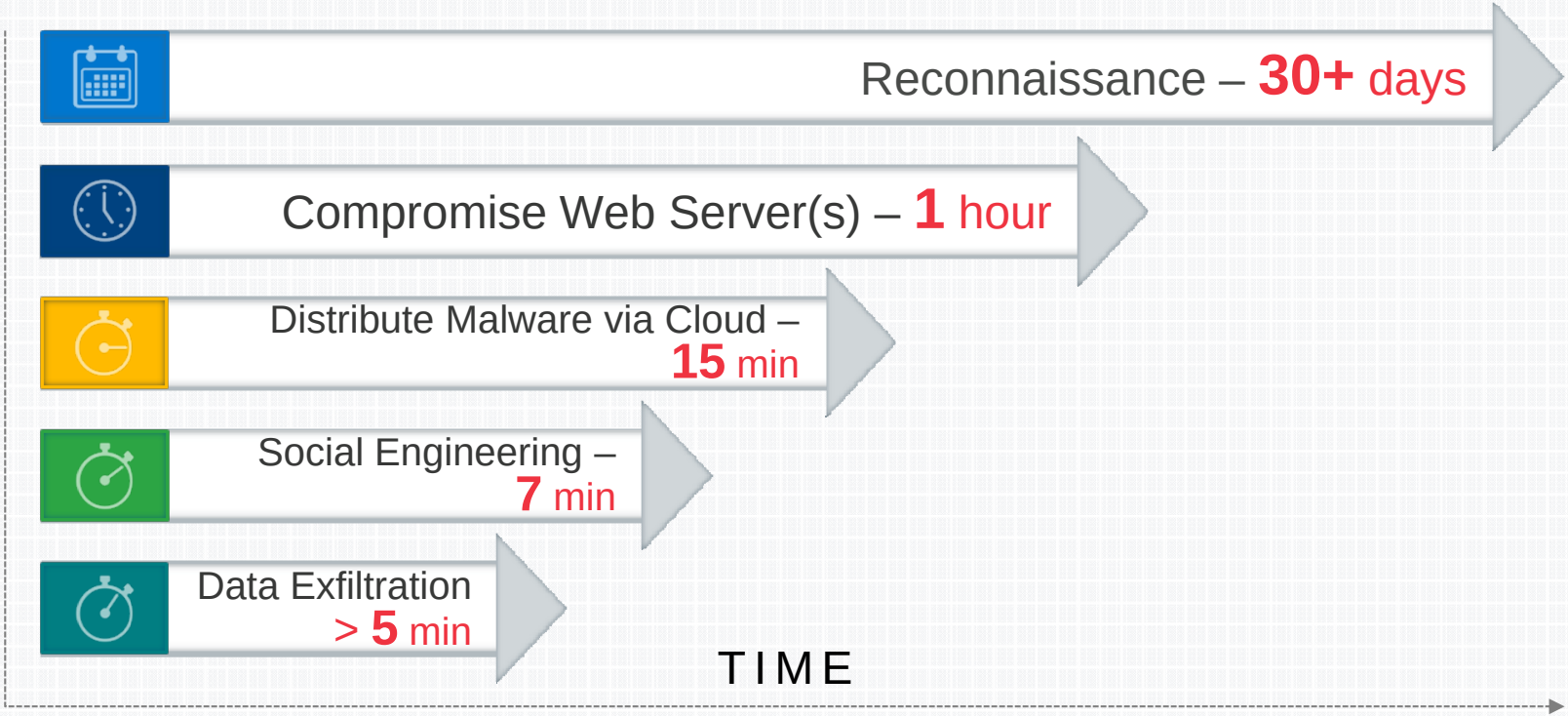
SESSION ID: SPO1-W03

Incident Response Agility: Leverage the Past and Present into the Future

Torry Campbell

CTO, Endpoint and Management Technologies
Intel Security

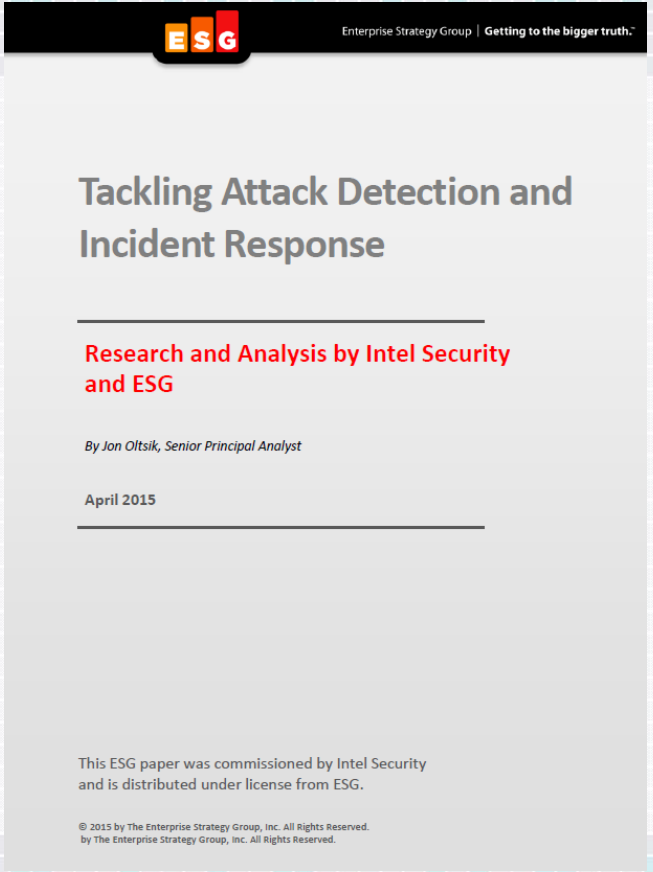
The Reality we Face



Incident Response Survey

Released April 13, 2015

http://mcaf.ee/r7ei8



Why Agility?

Average number of incidents investigated in 2014

Total (n= 700)	500 to 999 employees	1,000 to 4999 employees	More than 5,000 employees
78	31	41	150

Intel Security Data via Vanson Bourne, March 2015. http://www.mcafee.com/us/resources/reports/rp-esg-tackling-attack-detection-incident-response.pdf

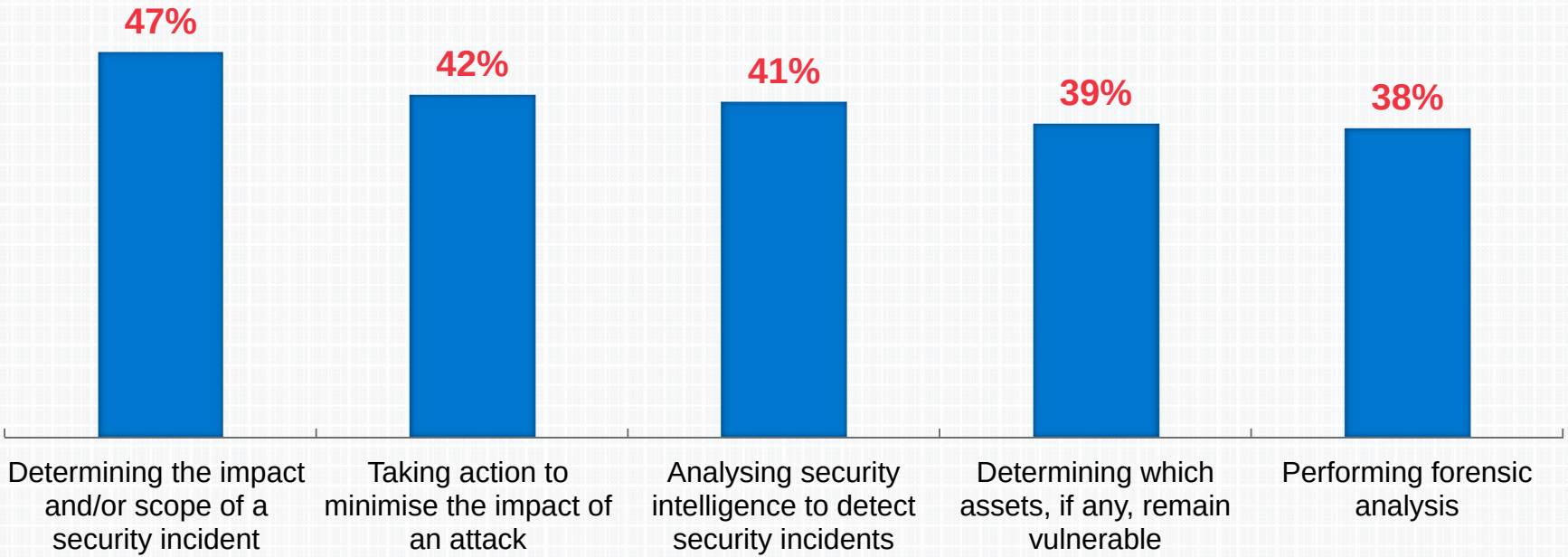
High Proportion of Targeted Attacks

Average percentage of investigations in 2014 associated with targeted attacks

Total (n= 700)	500 to 999 employees	1,000 to 4999 employees	More than 5,000 employees
28%	24%	30%	28%

Intel Security Data via Vanson Bourne, March 2015. http://www.mcafee.com/us/resources/reports/rp-esg-tackling-attack-detection-incident-response.pdf

Where Incident Responders Spend Their Time

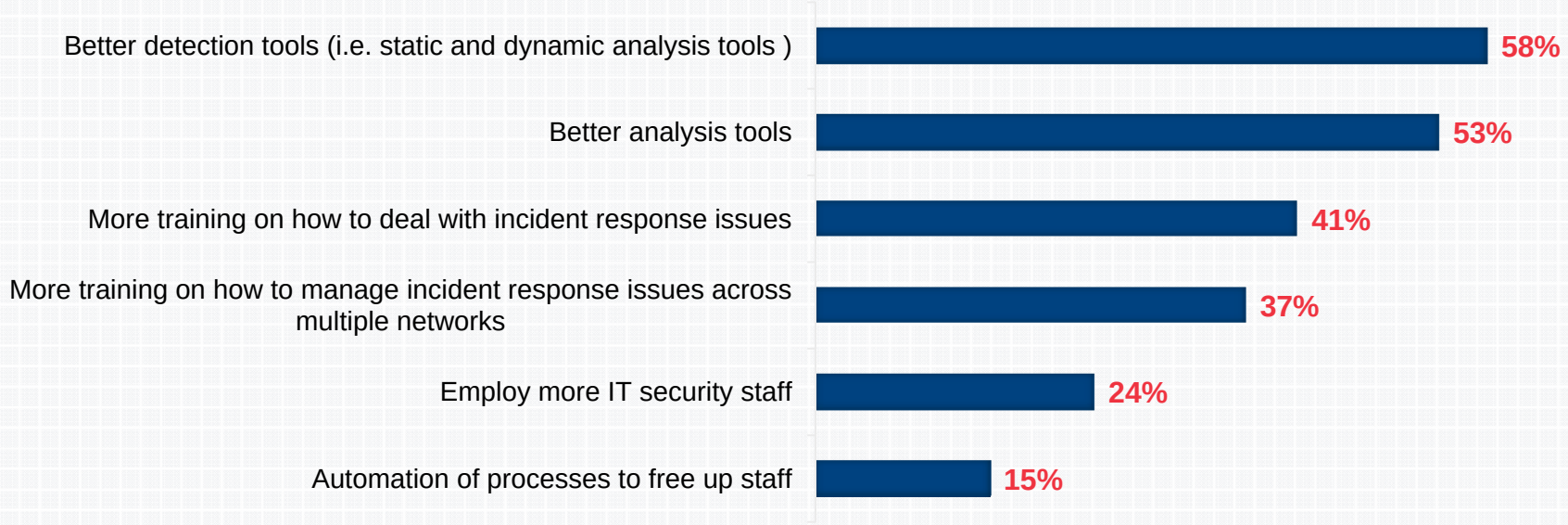


Intel Security Data via Vanson Bourne, March 2015. http://www.mcafee.com/us/resources/reports/rp-esg-tackling-attack-detection-incident-response.pdf

Best Boost for Efficiency and Effectiveness

#RSAC

Detection, analytics, training

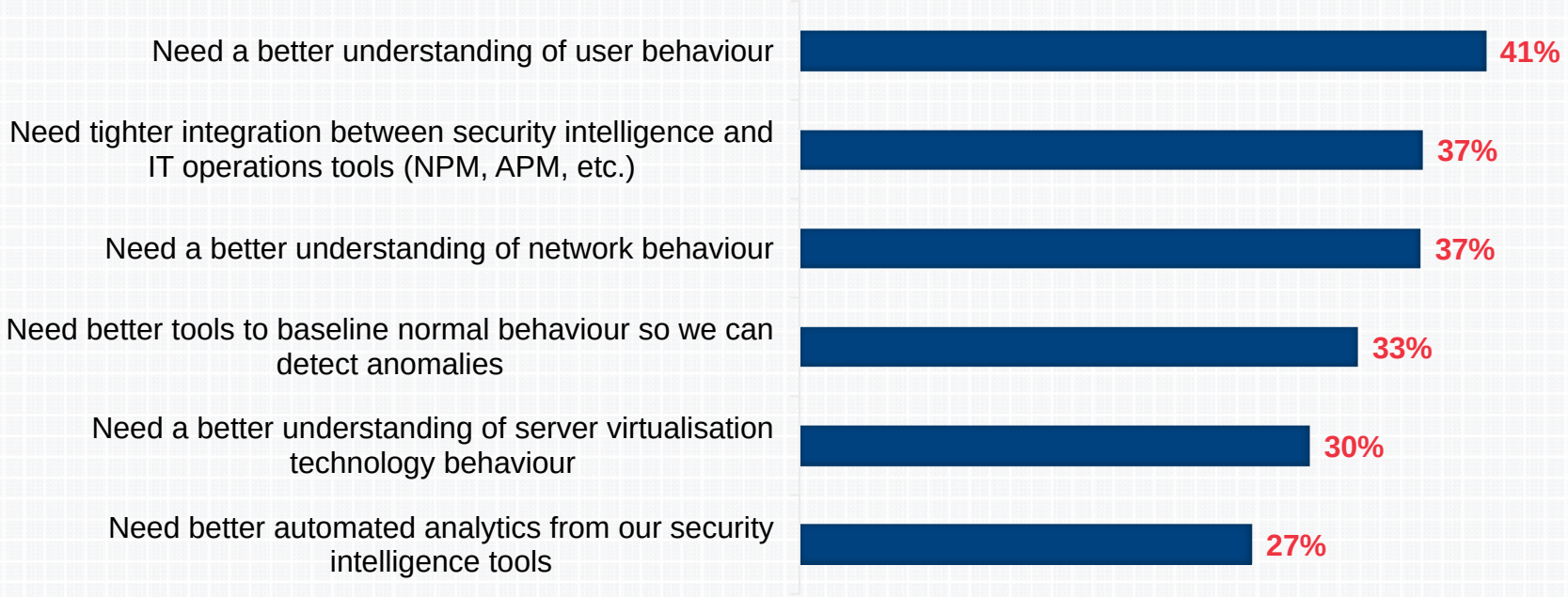


Intel Security Data via Vanson Bourne, March 2015. http://www.mcafee.com/us/resources/reports/rp-esg-tackling-attack-detection-incident-response.pdf

Building the Story Requires Comprehension

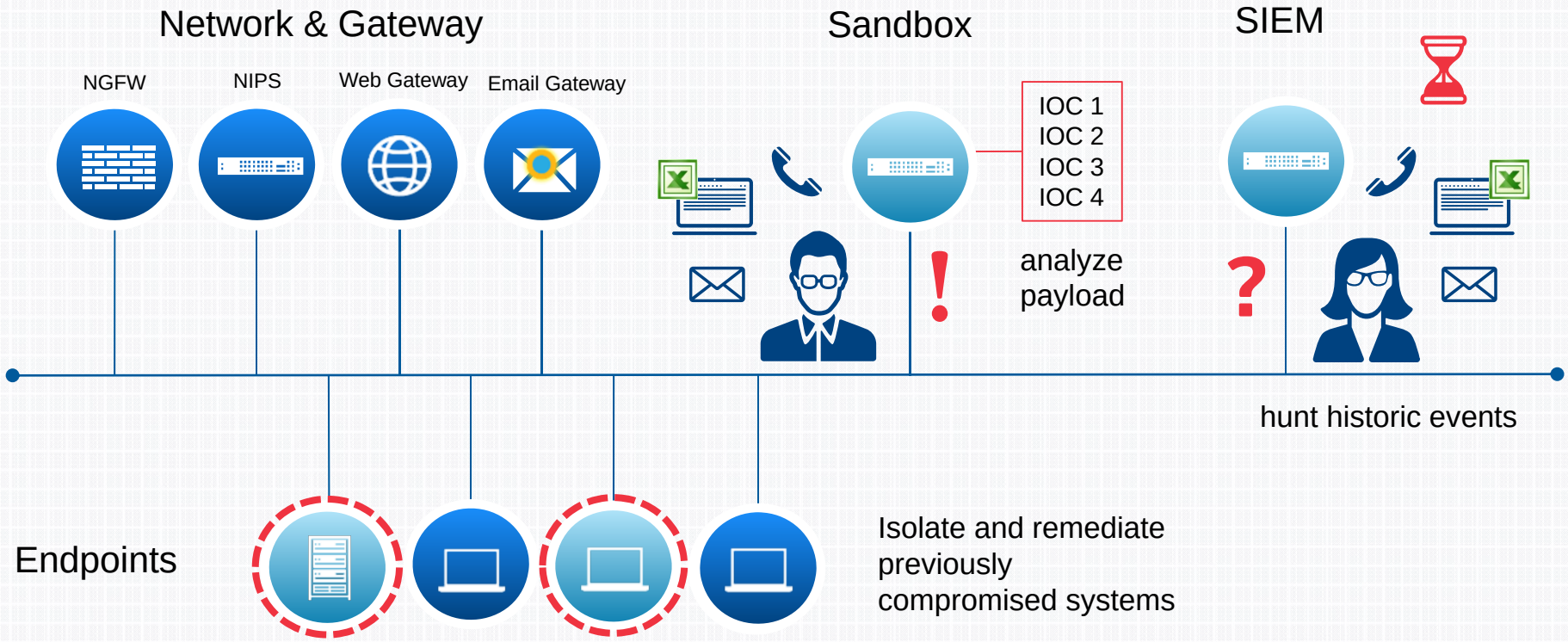
Inhibitors to Real-time Awareness

Understanding behavior, operational integration, analytics

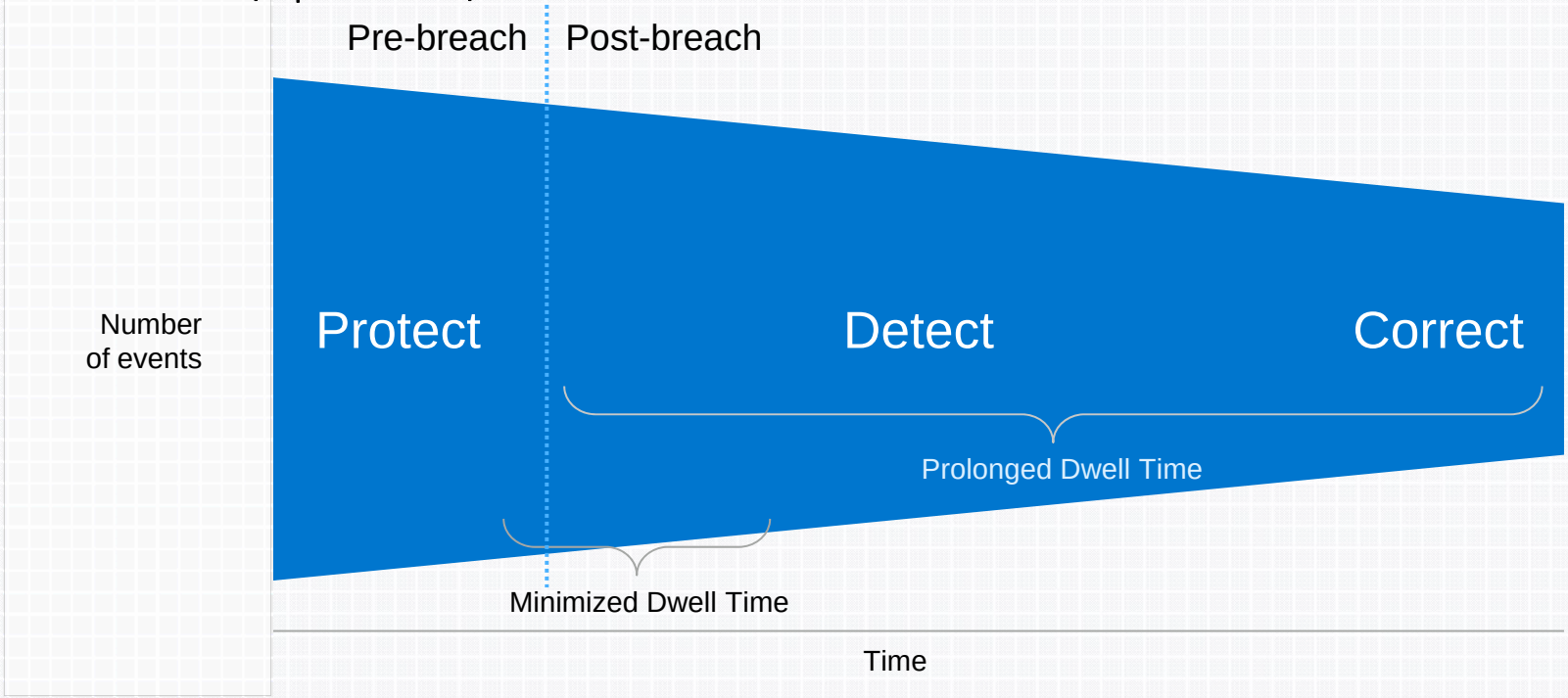


Intel Security Data via Vanson Bourne, March 2015. http://www.mcafee.com/us/resources/reports/rp-esg-tackling-attack-detection-incident-response.pdf

A Series of Unintegrated Events



Agile Incident Response



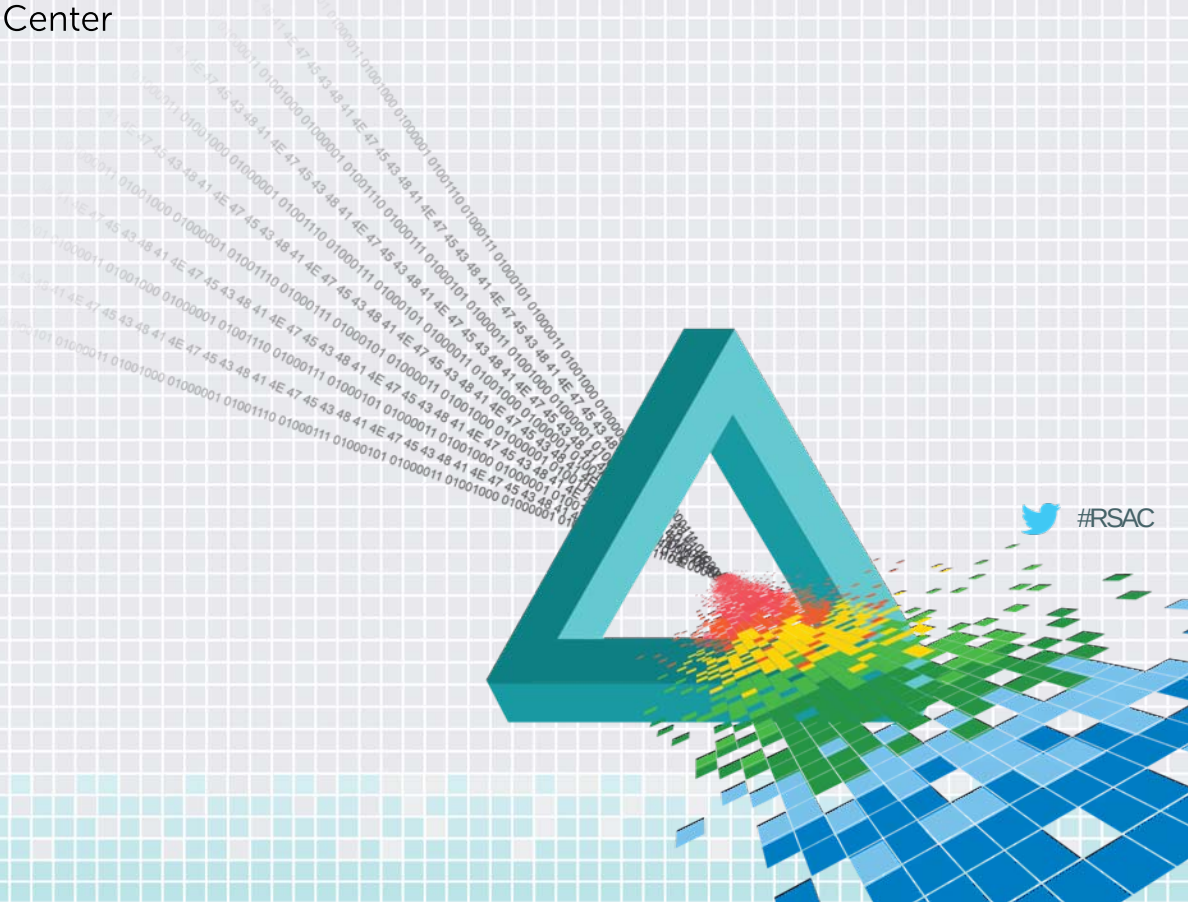
SESSION ID: SPO1-W03

Protecting the Future by Studying the Past and Present

Josh Thurston

Manager, WW Technical Operations

“Omaha”



Peyton Manning

The Perfectionist

- Past
  - Study Film of his team
  - Study Film of his opponent
- Present
  - Study images of plays during game
  - Analyze formations at the line
  - Reflect on data

“OMAHA”

http://goingdeep.reblog.hu/peyton-manning-a-z-vilaghaboruban

Agenda

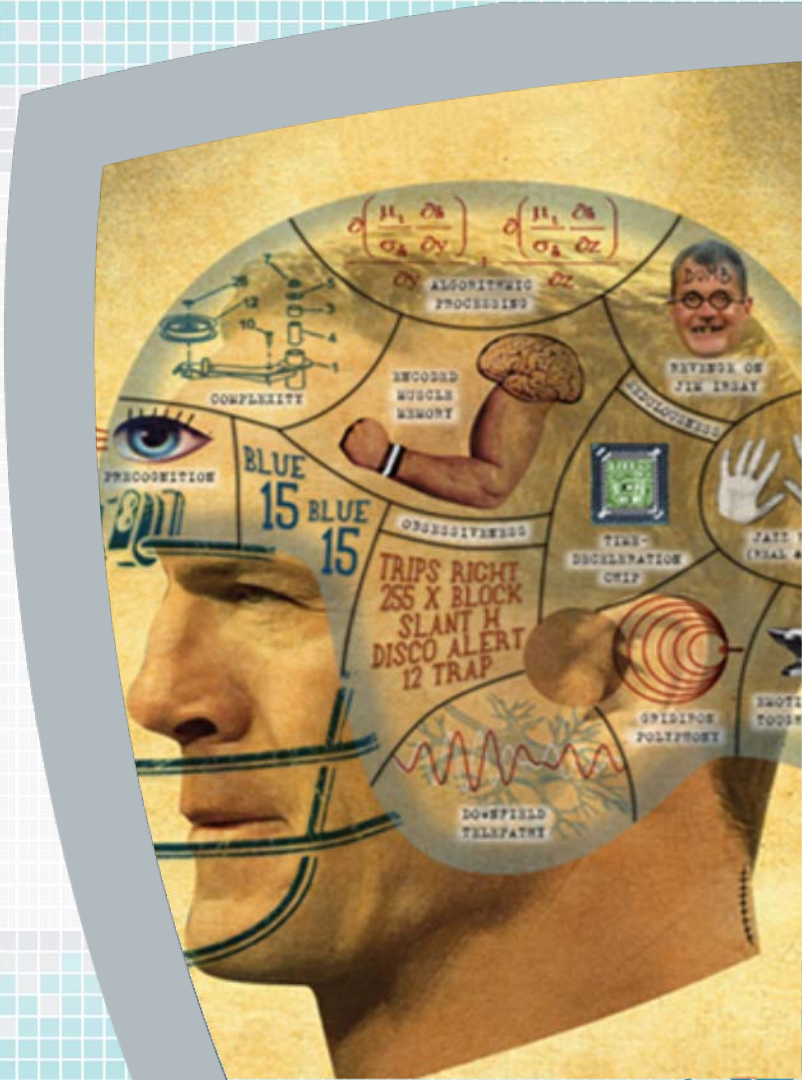
1. Pursuit of Perfection
2. Time is Against You
3. Data Collection
4. Analysis
5. Insight Through Integration

Pursuit of Perfection

The Setup

- Integrated Security Architecture
  - Ability detect and provide alerts to potential threats in as they occur
  - Adapt and improve security
  - Complete coverage:
    - Endpoint, Network, Identity, and Data
- Mature Incident Response
  - Ability to Collect Meaningful Data
  - Ability to Analyze the Data Quickly
  - Ability to Act Very Fast – Minimize Impact
  - Ability to Protect the Future

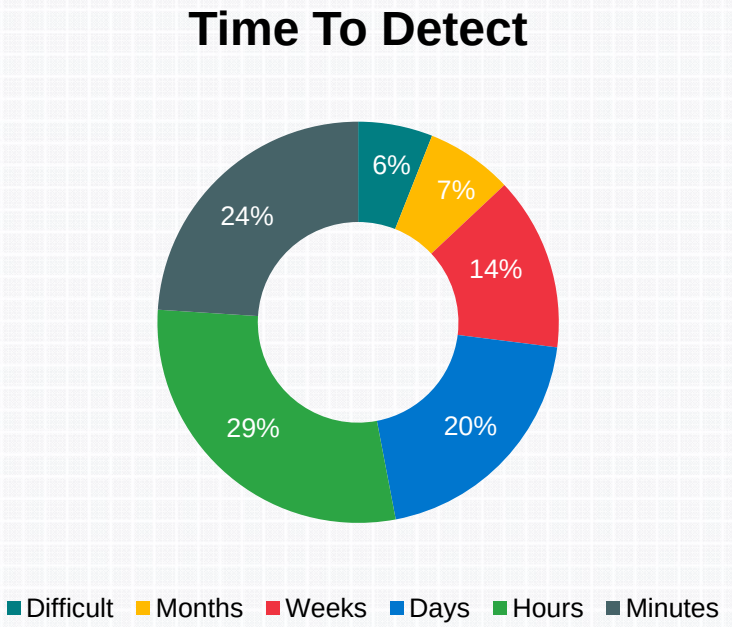
http://www.gq.com/blogs/the-feed/2013/12/peyton-manning-breaks-touchdown-record-and-other-news-a-man-needs-to-know-today.html



Time is Against You

Attackers Have the Upper Hand

- Attacks take a lot of time to plan.
- You don't detect pre attack activities
- Attacks are executed quickly
- 53% of the Time it Takes More Than 1 Day to Detect a Breach



When Minutes Count: http://www.mcafee.com/us/resources/reports/rp-when-minutes-count.pdf

You Can Be Effective

Toolkit

Things to Know:

- Use the Tools You Have and Trust
- You Have The Right People
  - Only **17%** feel they need better analysis/ forensics skills.
- You Have the Data, just not integration
  - Only **26%** say they have a hard time gathering the right data for accurate situational awareness
  - A Whopping **47%** say they spend most of their time determining impact. i.e. putting the pieces together

Things To Do:

- Integrate
  - **37%** feel they need tighter integration
- Understanding and Visibility
  - **41%** Need to understand user behavior
  - **37%** Need to understand network behavior
  - **27%** Need to understand application behavior
  - **21%** Need to understand host behavior

Intel Security Data via Vanson Bourne, March 2015. http://www.mcafee.com/us/resources/reports/rp-esg-tackling-attack-detection-incident-response.pdf

Data Collection

Past and Present

- No Blind Spots
  - Endpoint
  - Network
  - Identity
  - Data

Analysis

How Fast are You

- Analyze
  - What is Normal
  - What is Abnormal
  - Filter our the white noise
  - Correlate Data between sources

Insight Through Integration

Maximize Incident Response

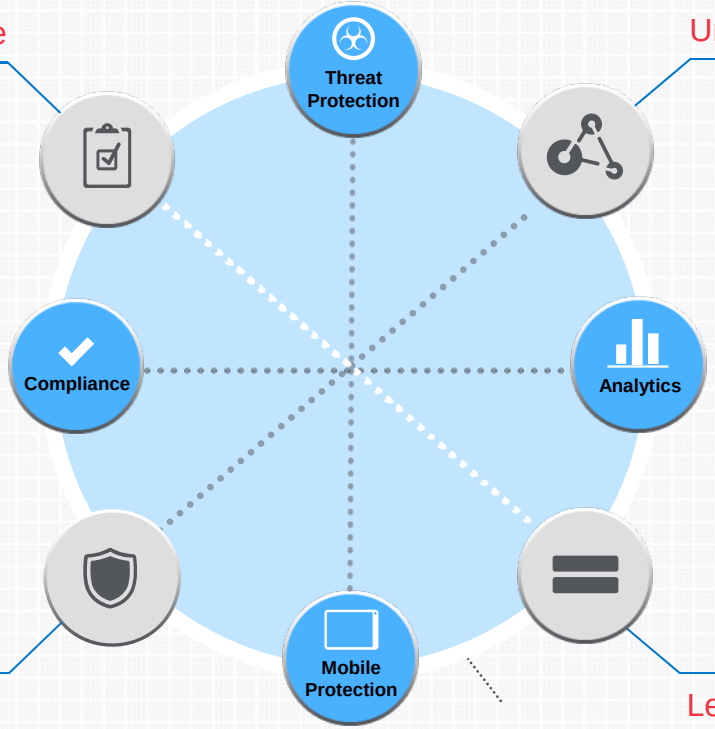
Management

Insight:
Event and Alert Correlation
Context and IOC Visibility
Breach Analysis

Understand the Infrastructure

Network

Insight:
Traffic Visibility
Lateral Movement
Network Connections



Endpoint

Insight:
Context and Posture
Malicious Activity

Protect every Endpoint

Content

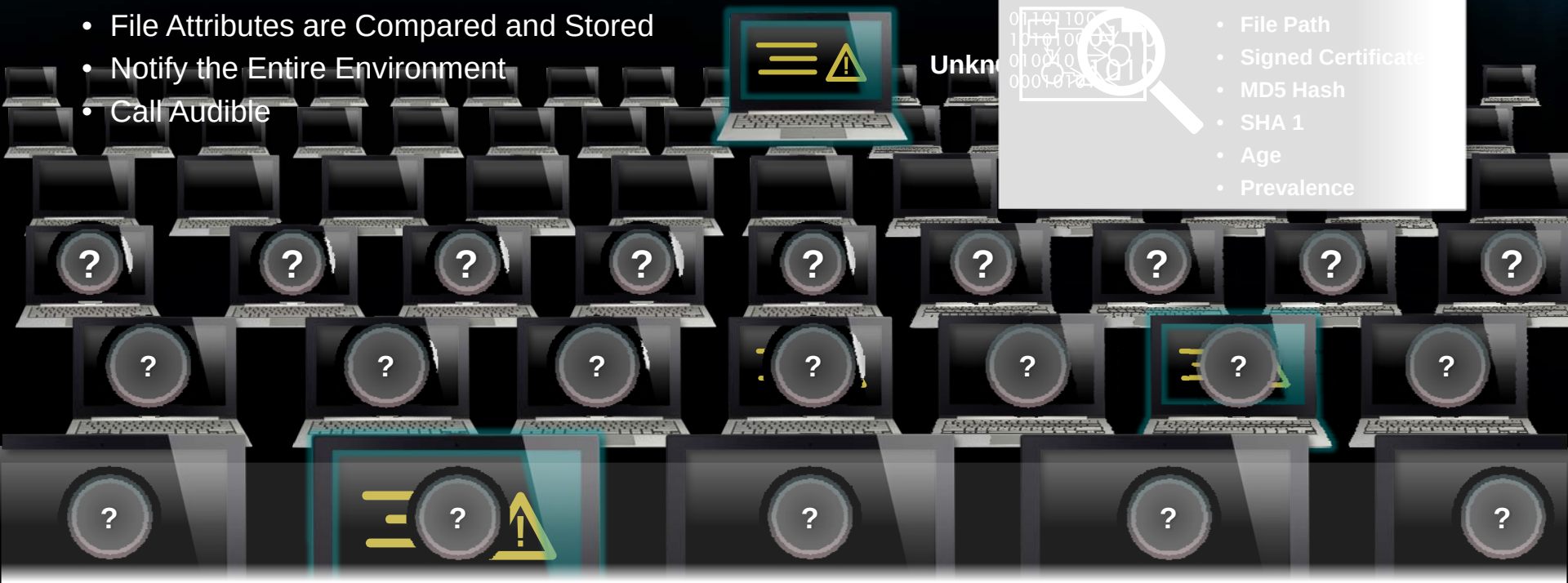
Insight:
Who is using your Data
What is accessing your Data
Suspicious Data Usage

Learn Data Trends

Omaha in Action

Live Analysis and Data Collection

- An Executable Launches
- File Attributes are Compared and Stored
- Notify the Entire Environment
- Call Audible

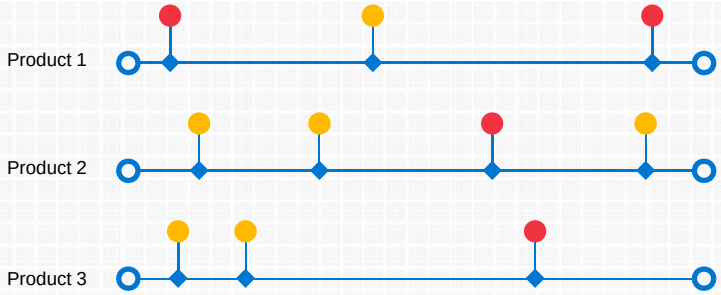


Clarity to Drive Better, Faster Decisions

Current state vs. integrated and agile

CURRENT STATE

Limited scope. Point in time context.

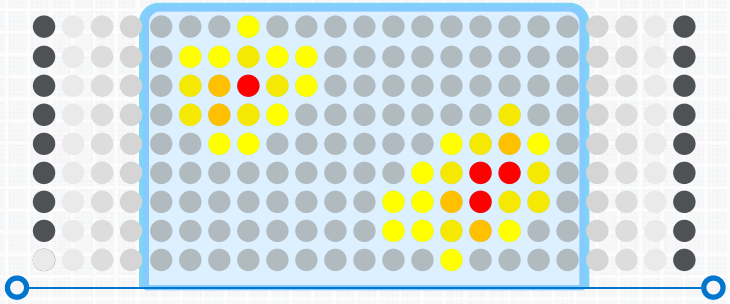


Result

Limited, reactive visibility and threat protection

AGILE APPROACH

Continuous monitoring and contextual analytics



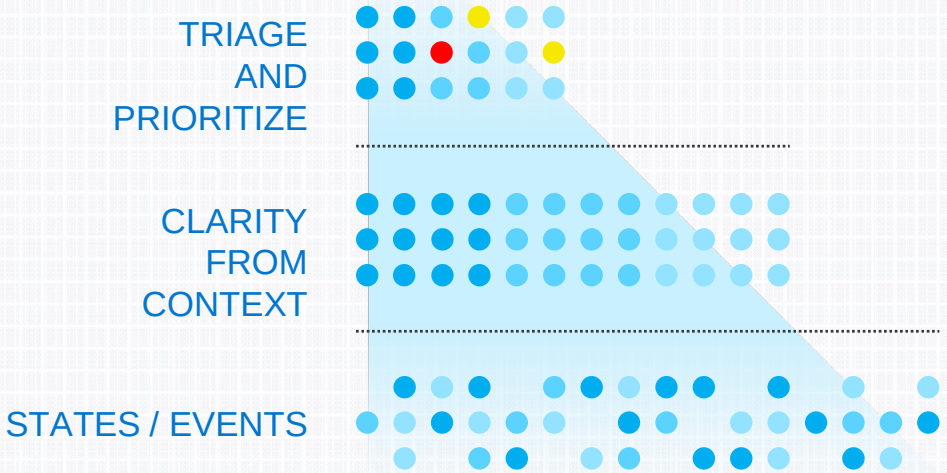
Result

Faster, more proactive awareness of threats and anomalous events

Confidence to Act

Boost confidence with risk scoring, automation, watch lists and alerting

- Gain confidence to act:
  - Distillation and prioritization
  - Risk scoring and customizable tuning
  - Increased automation
  - Focus on what matters most



IR and Forensics

Enable Your Team

1. Integrated Architecture
2. Agile Framework
3. Shared Intelligence
4. Effective SIEM Analytics Implementation
5. Clarity to Drive Better, Faster Decisions
6. Confidence to Act

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Closing

Call Omaha

Download report from
http://mcaf.ee/r7ei8