RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

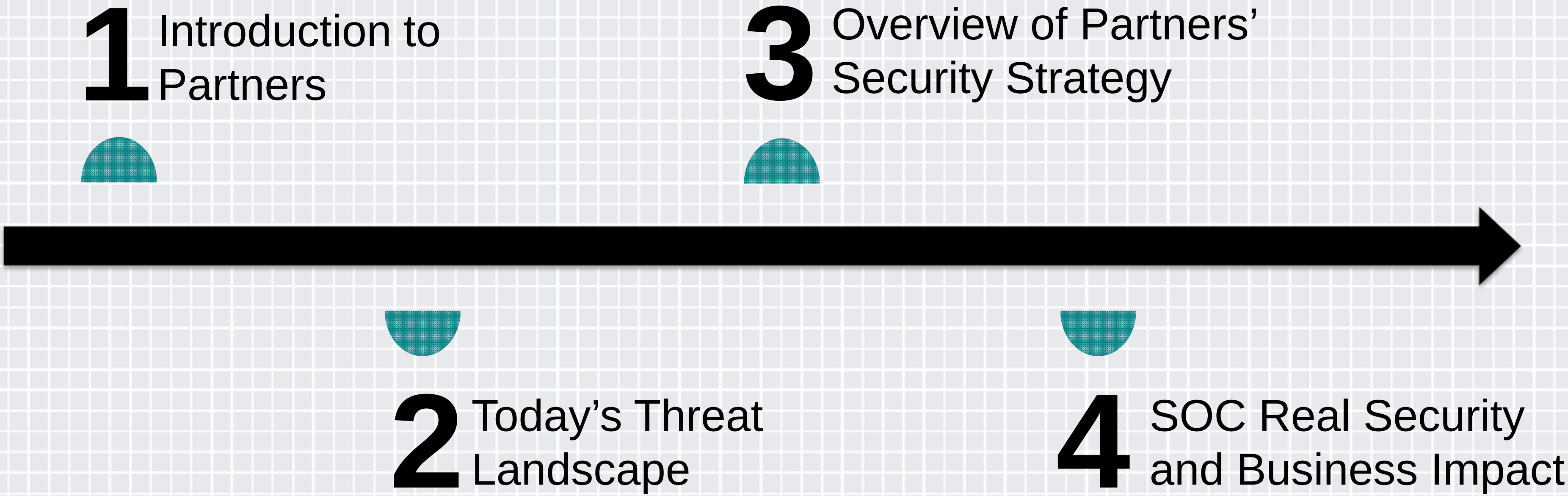
SESSION ID: SPO2-W03

Healthcare Case Study: Beating Cybercrime, Nation-states & Insider Threats

Jigar Kadakia

Chief Information Security and Privacy Officer
Partners HealthCare

Agenda



1 Introduction to Partners

2 Today’s Threat Landscape

3 Overview of Partners’ Security Strategy

4 SOC Real Security and Business Impact

Learning Objectives

- Gain insight on healthcare-specific cyber security concerns
- Discover methods of how to gain more visibility and control in your network
- Understand the technology components behind Partners' SOC strategy
- Learn the best practices for a successful security program deployment

What comes to mind when you think of…..?

‘Wicked good’ sports…Ha’vahhd…and everybody’s favorite brand of coffee.

The next thing that comes to mind is healthcare…

Partners = Integrated Healthcare Network

MGH
1811

BWH

Connectivity To Different Medical Entities

RSAConference2015
San Francisco | April 20-24 | Moscone Center

- Two academic, research oriented medical centers
- Home health & long-term care services
- Community & specialty hospitals
- Physician network
- Managed care organization
- Community health centers

RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

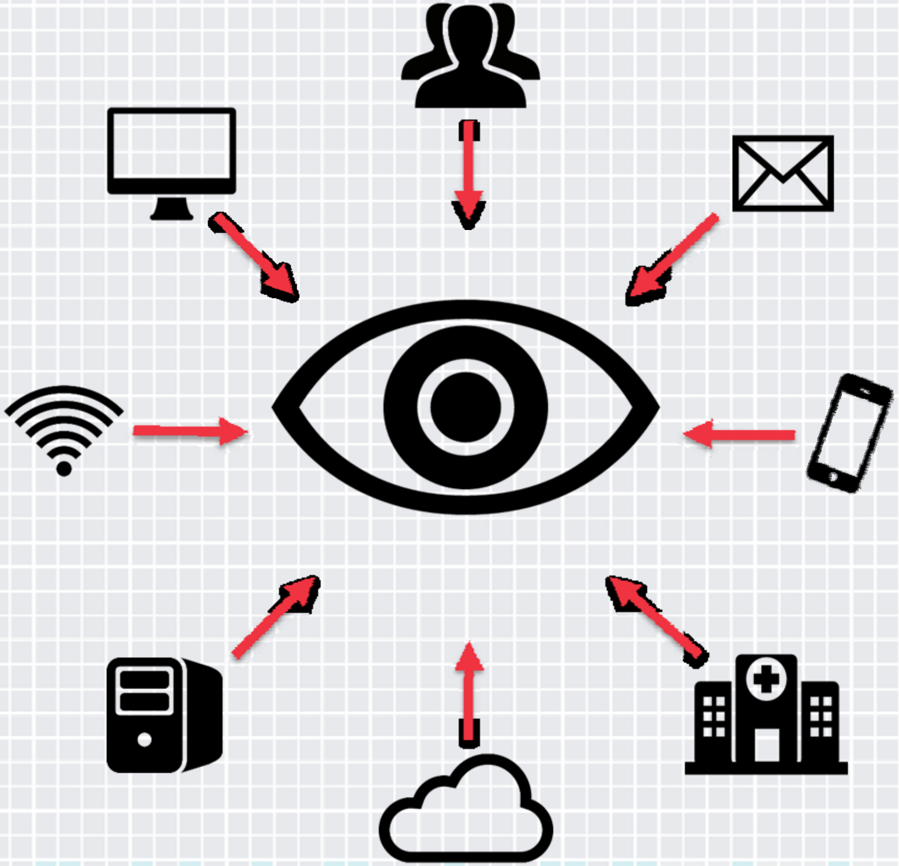
What Attracts Cyber Criminals to Healthcare?

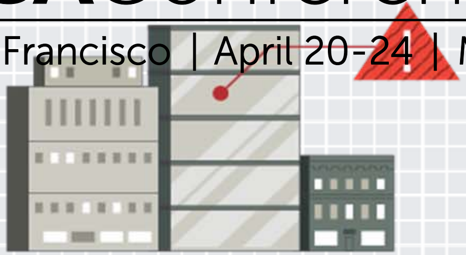
PARTNERS HEALTHCARE

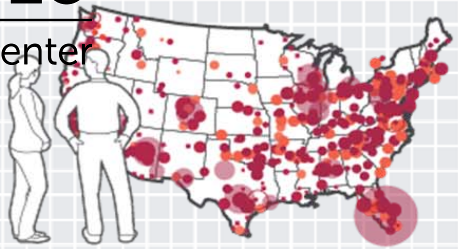
Abundance of Highly Valuable Data

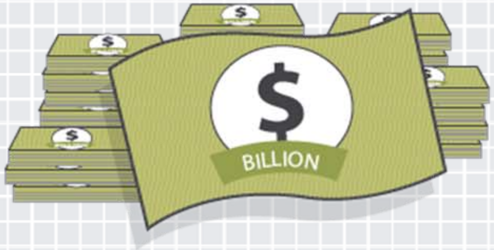
- Protected health information
- Research data
- Employee data

Numerous Points Of Entry









$150-$250
Average cost per breached medical record.

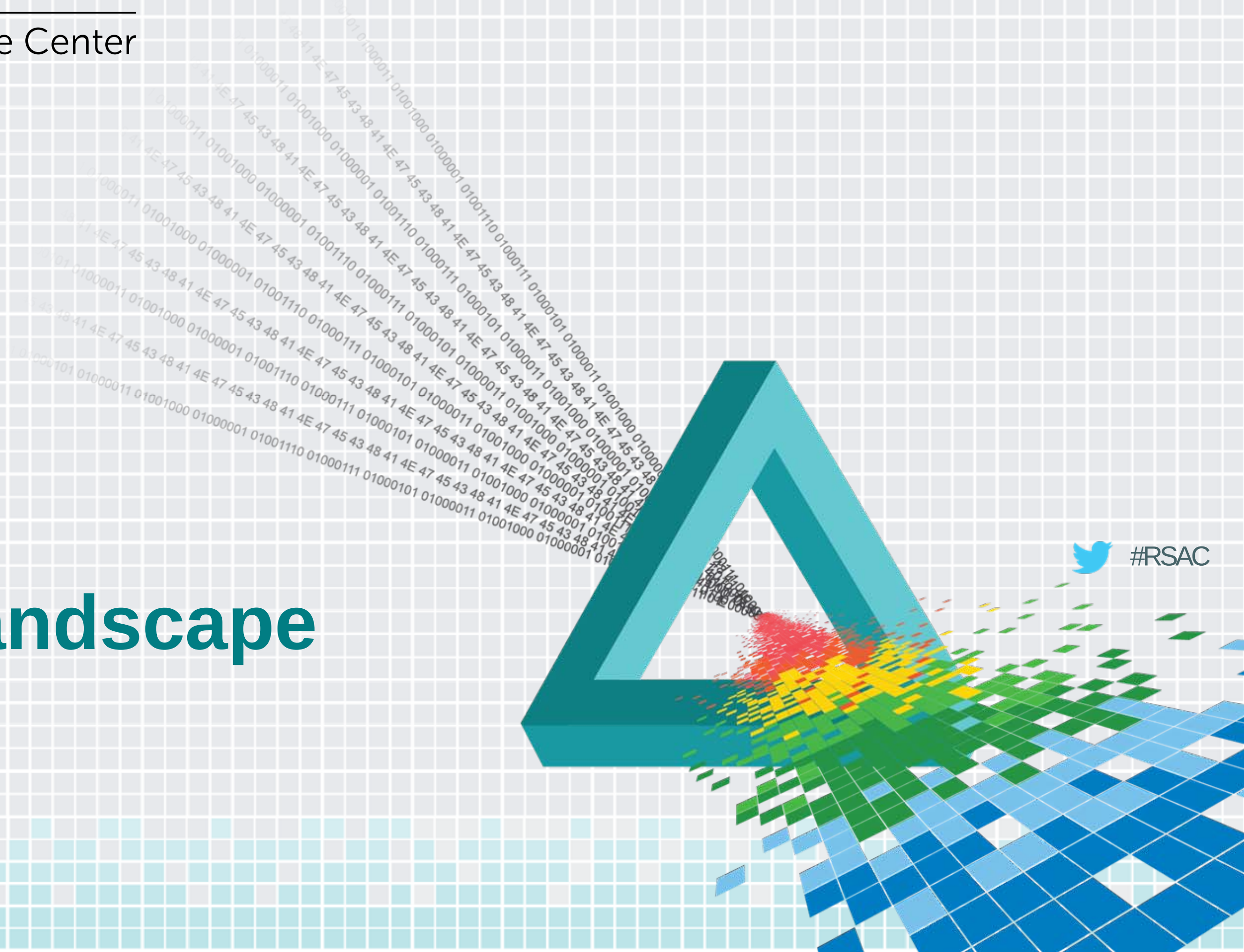
70%
Increase in reports of large data breaches from healthcare organizations since 2010.

$5.6 billon
Yearly cost to the healthcare industry, due to breaches.

94% Of healthcare organizations have reported being victims of a cyber attack.

RSAConference2015

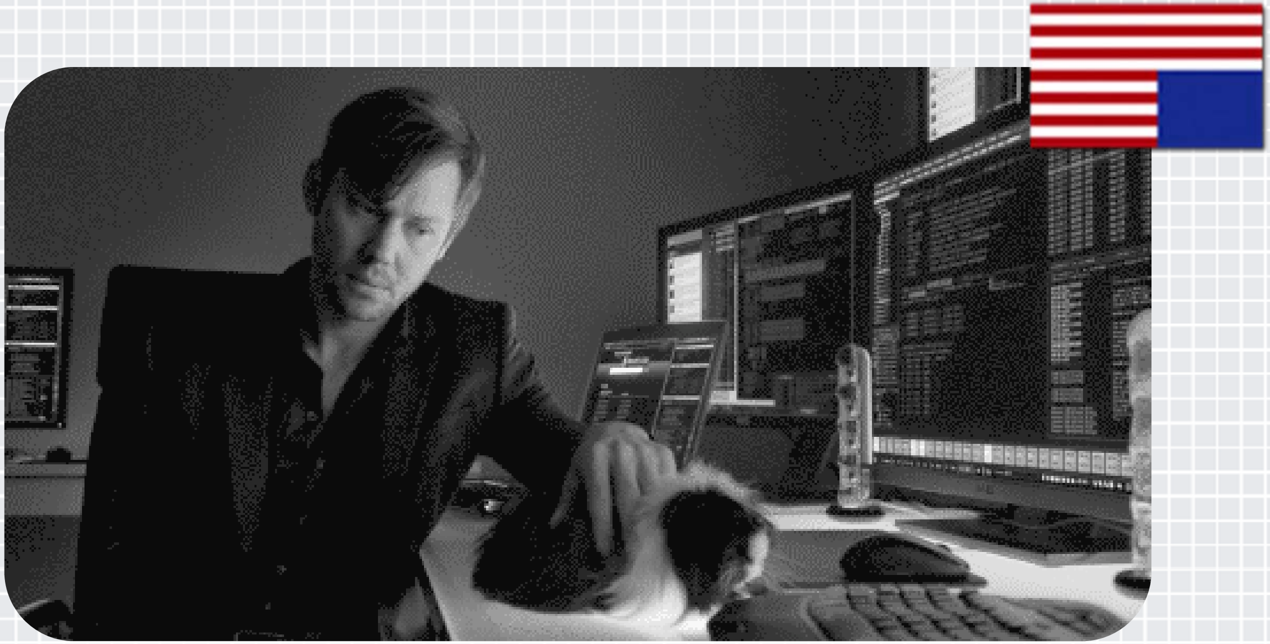
San Francisco | April 20-24 | Moscone Center



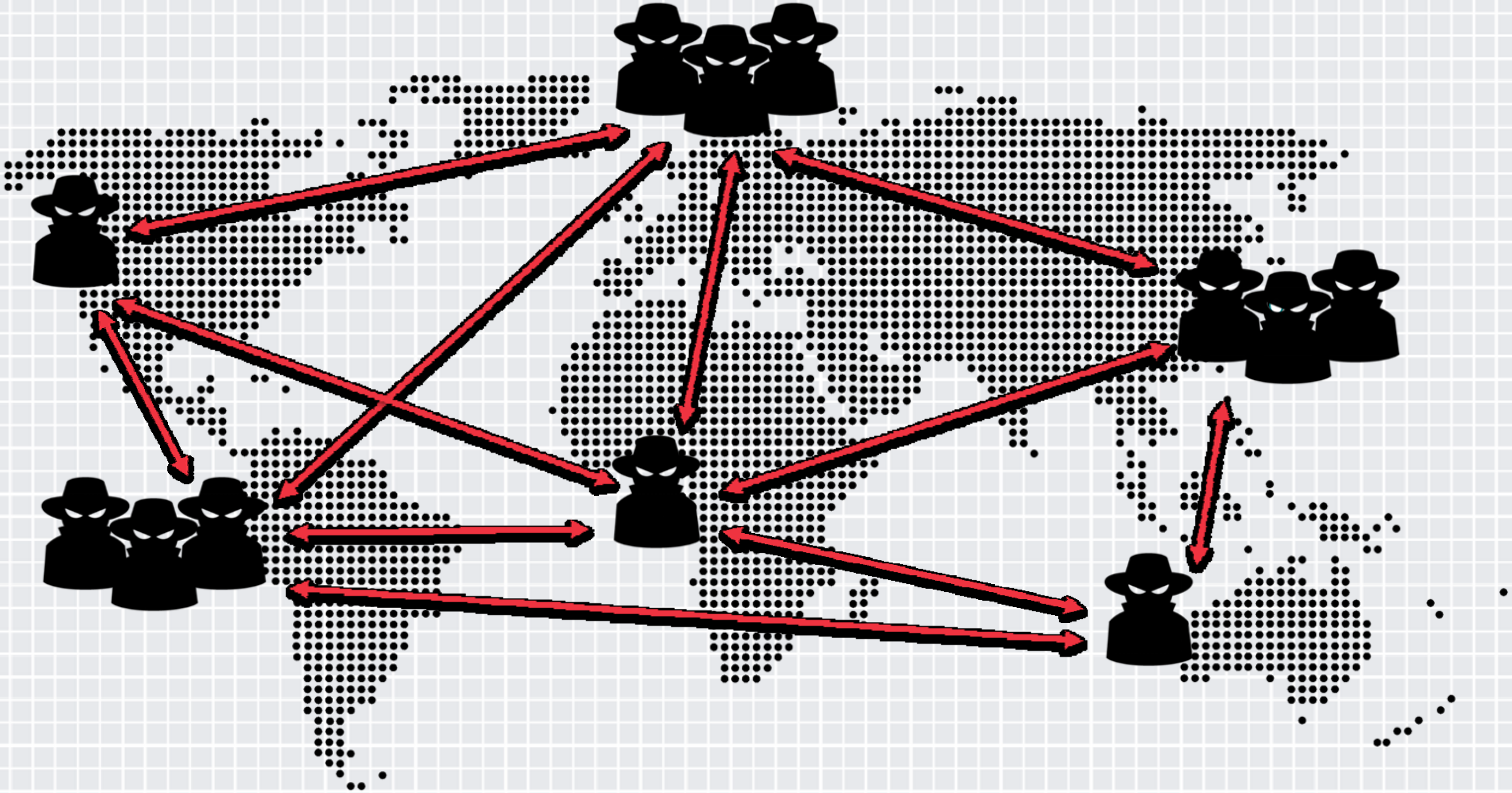
#RSAC

Today’s Threat Landscape

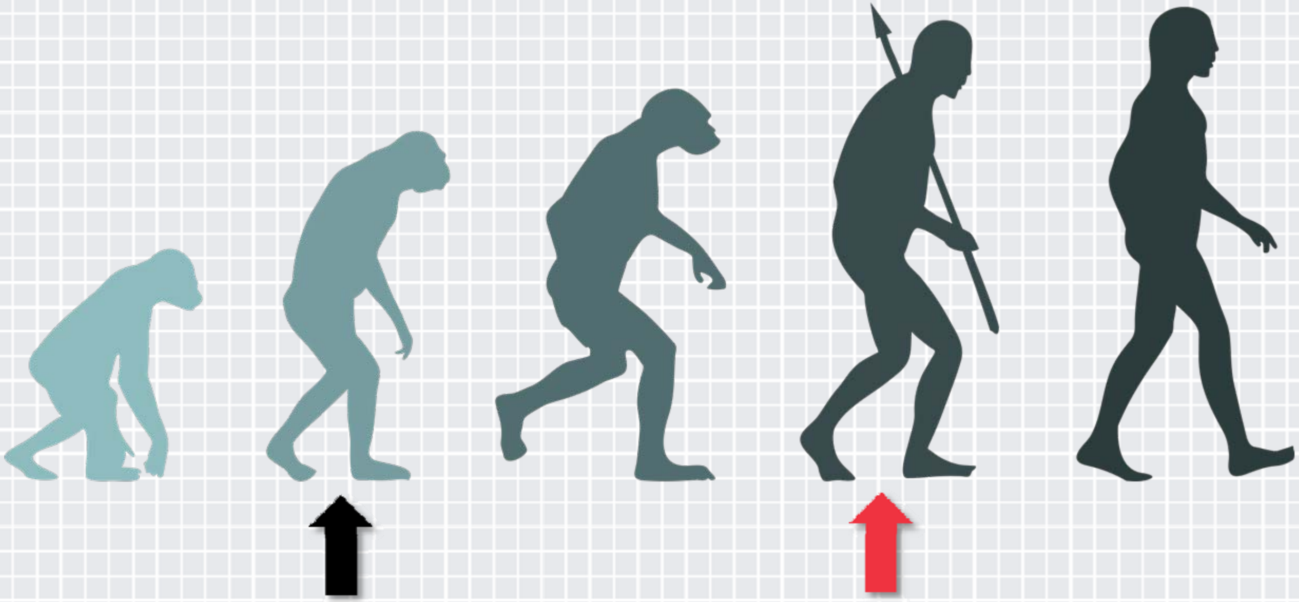
The Lone Hacker Is A Thing Of The Past



Cyber Criminals Are Well Connected



Always Two Steps Ahead of Us



Us

Attackers

…And Their Attacks Are Deadly

- Advanced persistent threats
- DDoS and TDoS
- Zero-day exploits
- Spear phishing
- Social engineering
- Trojans
- Anonymous proxies (i.e. TOR)

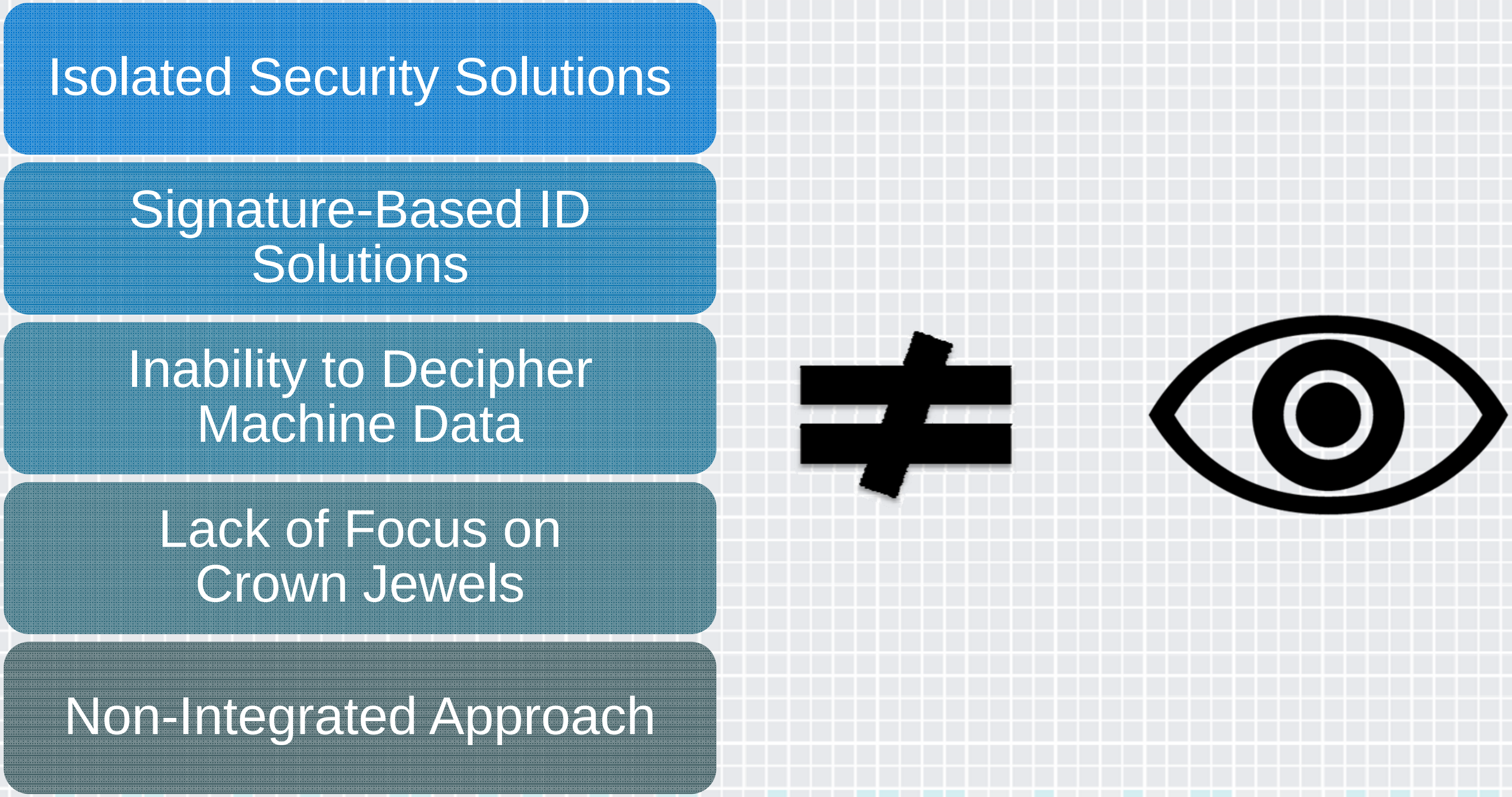
RSAConference2015

San Francisco | April 20-24 | Moscone Center

The Ideal Security Solution

Visibility + Control

Traditional Approach To Security



Isolated Security Solutions

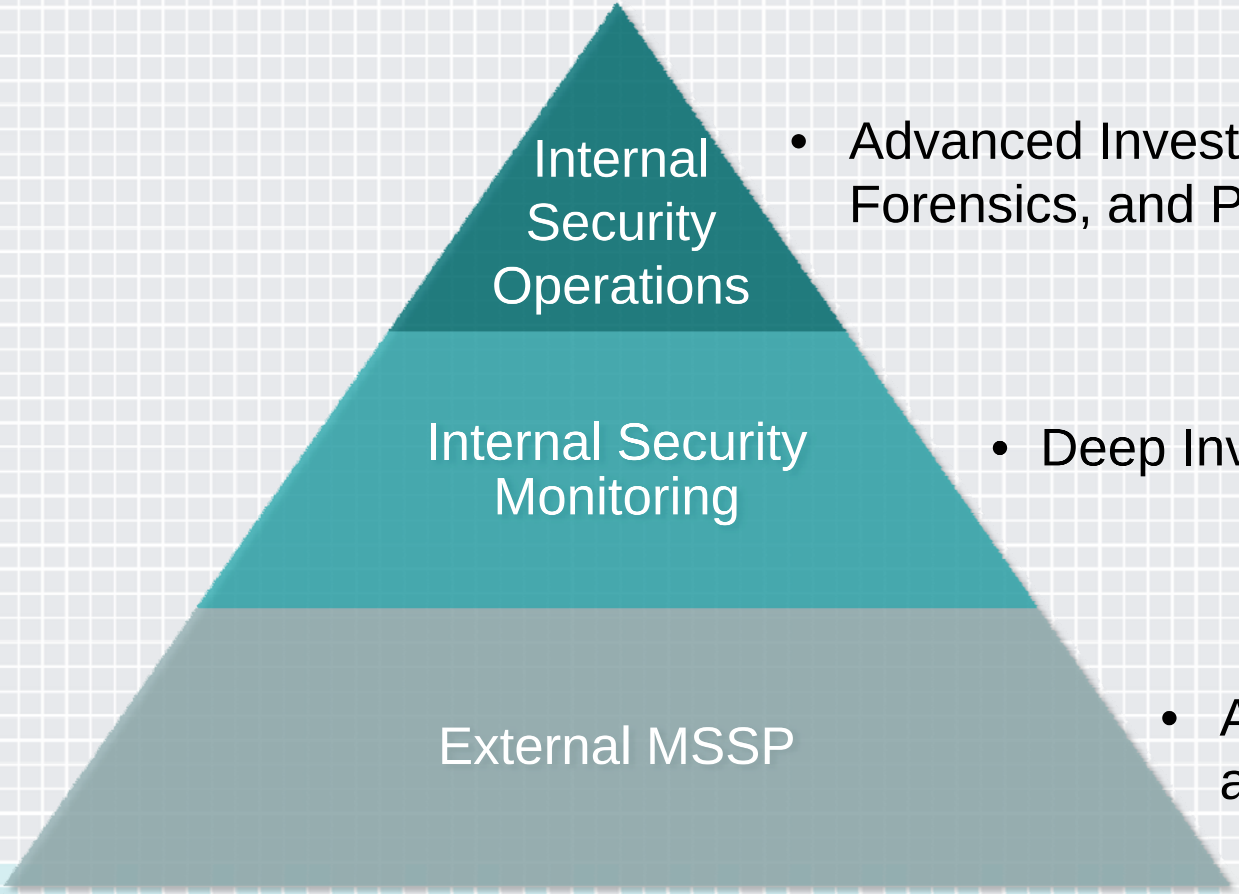
Signature-Based ID Solutions

Inability to Decipher Machine Data

Lack of Focus on Crown Jewels

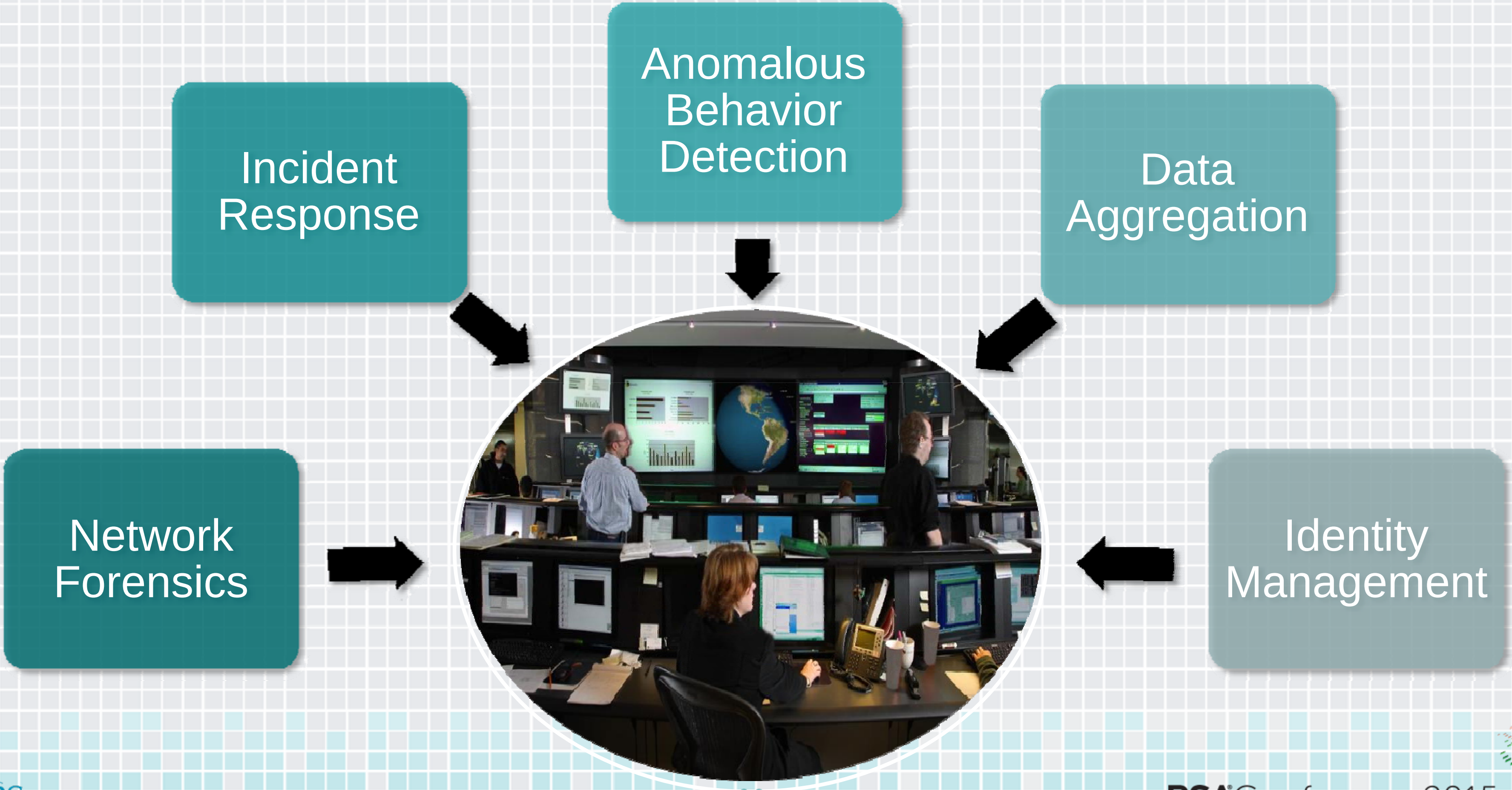
Non-Integrated Approach

Tiered Security Approach



- Advanced Investigations, Network Forensics, and Proactive Threat Analysis
- Deep Investigation and Monitoring
- Advanced Investigations, Forensics, and Proactive Threat Analysis

Partners' Security Operations Center Strategy



Incident Response

Anomalous Behavior Detection

Data Aggregation

Network Forensics

Identity Management

#RSAC

RSAConference2015

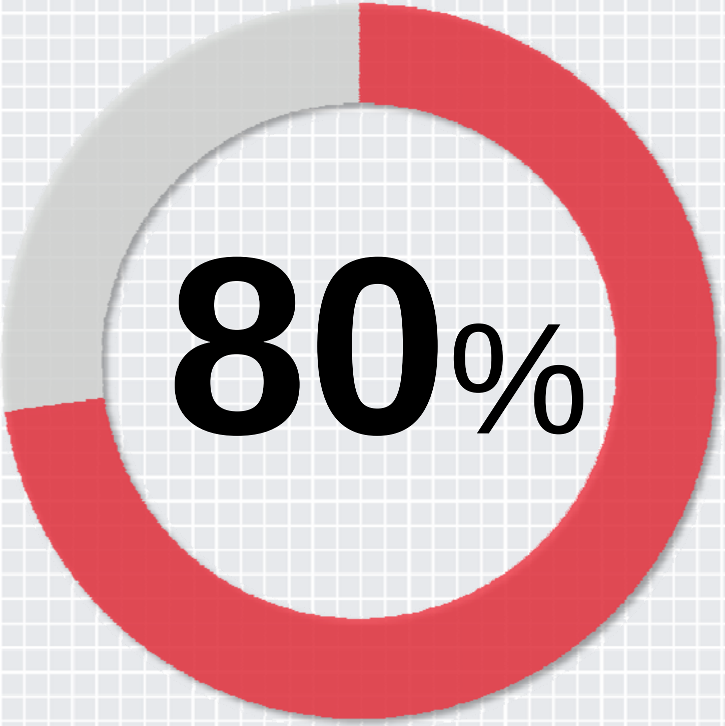
San Francisco | April 20-24 | Moscone Center

#RSAC

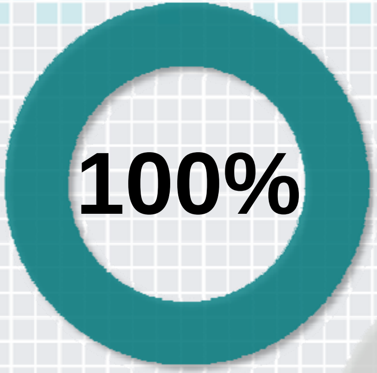
Impact of Partners' SOC Strategy

PARTNERS HEALTHCARE

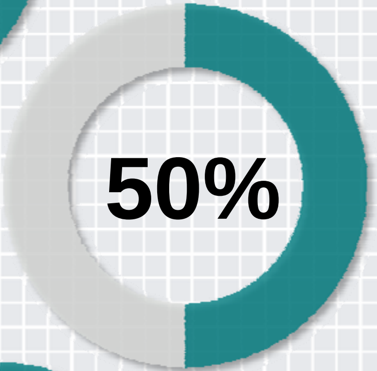
Incident Response



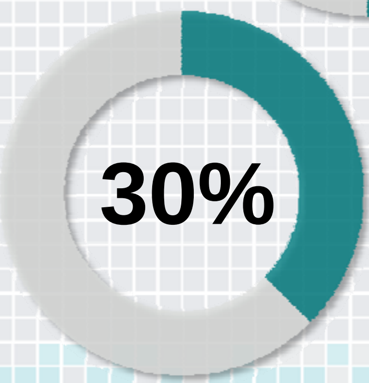
⚠ Of incidents are detected through automation



Reduction in detection time



Reduction in time to collect and analyze



Reduction in event duration

Increased Visibility

2800

Web Applications scanned bi-monthly

11 billon

Logs per month in 2014

24 billon

Logs per month in 2015

Reducing Risk Over Time

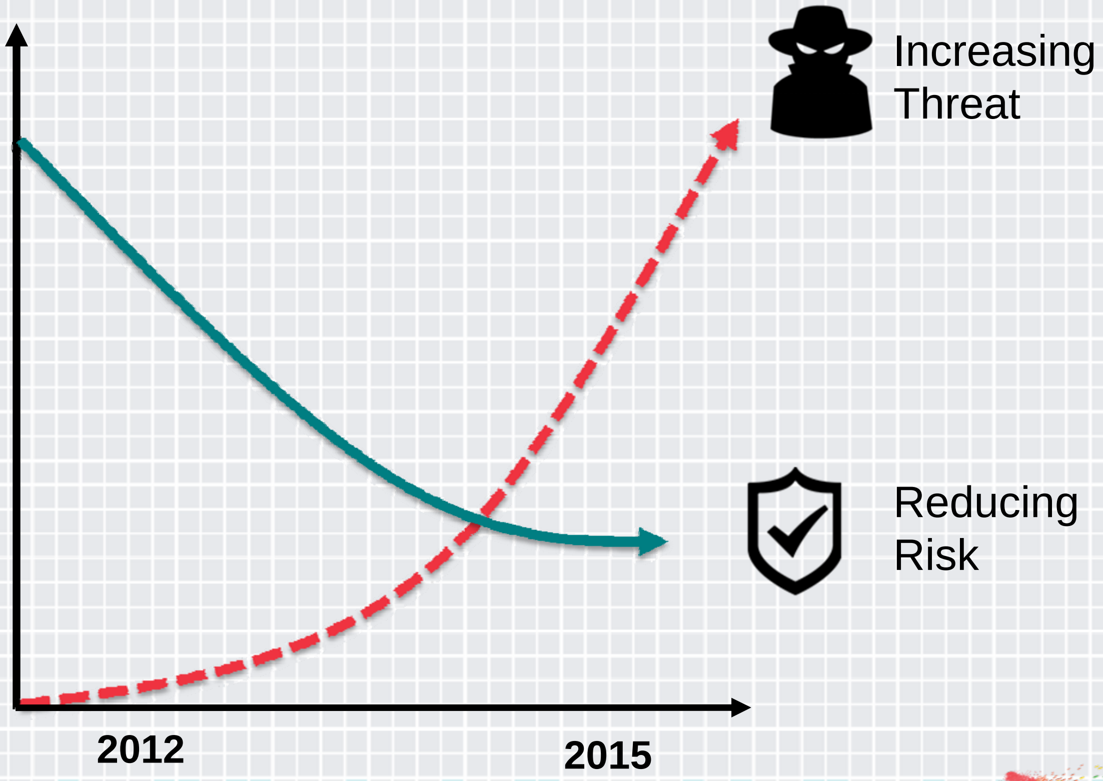
Policies

Processes

People

Business

Technology



Apply What You Have Learned Today

- Next week you should:
  - Review your enterprise security strategy.
  - Re-assess your current technology solutions.
- Within three months you should:
  - Identify gaps in technology, policies, and processes.
  - Enhance or leverage solutions to full capabilities.
- Within six months you should:
  - Integrate select security solutions which allow visibility and interoperability amongst all enterprise systems.
  - Create policies and processes to compliment those solutions.

QUESTIONS?

Jigar Kadakia
Chief Information Security & Privacy Officer

Partners HealthCare

One Constitution Center

Charlestown, MA 02129

TEL: +1 617 643 7121

Jkadakia@Partners.org