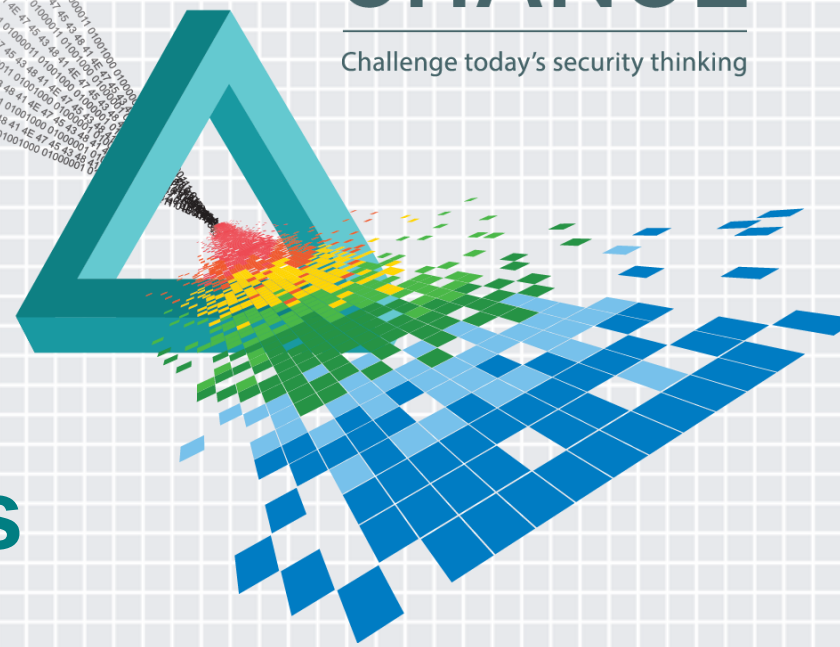
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



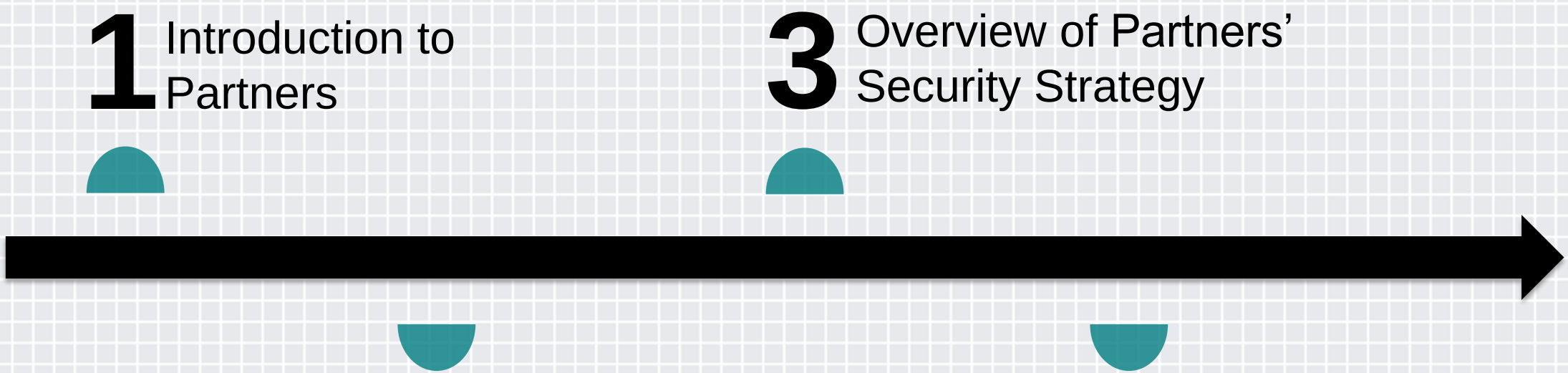
SESSION ID: SPO2-W03

A Global 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

Connectivity To Different Medical Entities

Two academic, research oriented medical centers

Home health & long-term care services

Community & specialty hospitals

Physician network

Managed care organization

Community health centers

#RSAC

RSAConference2015

San Francisco | April 20-24 | Moscone Center

What Attracts Cyber Criminals to Healthcare?

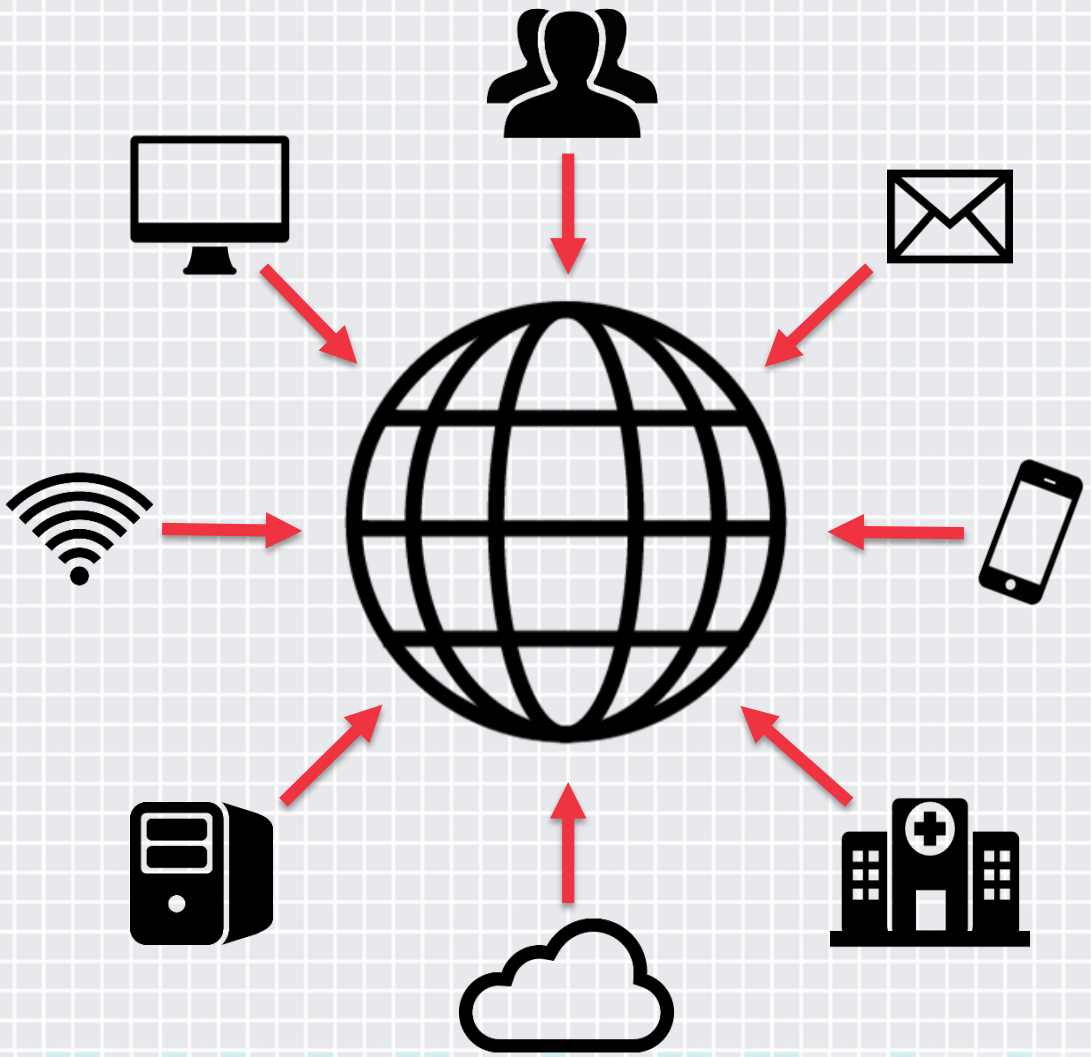
#RSAC

PARTNERS HEALTHCARE

Abundance of Highly Valuable Data

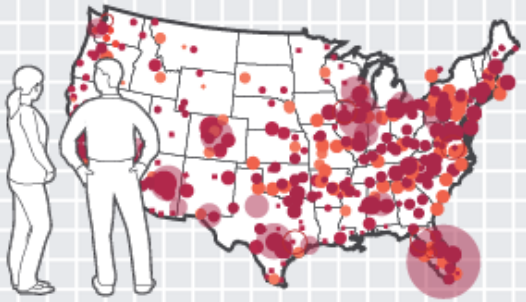
- Protected health information
- Research data
- Employee data

Numerous Points Of Entry



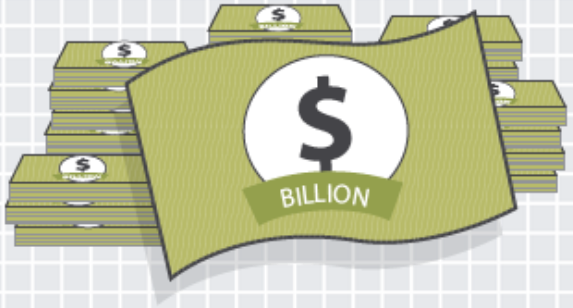
$150-$250

Average cost per breached medical record.



2.32 million

Victims of medical ID theft in 2014—and growing.*



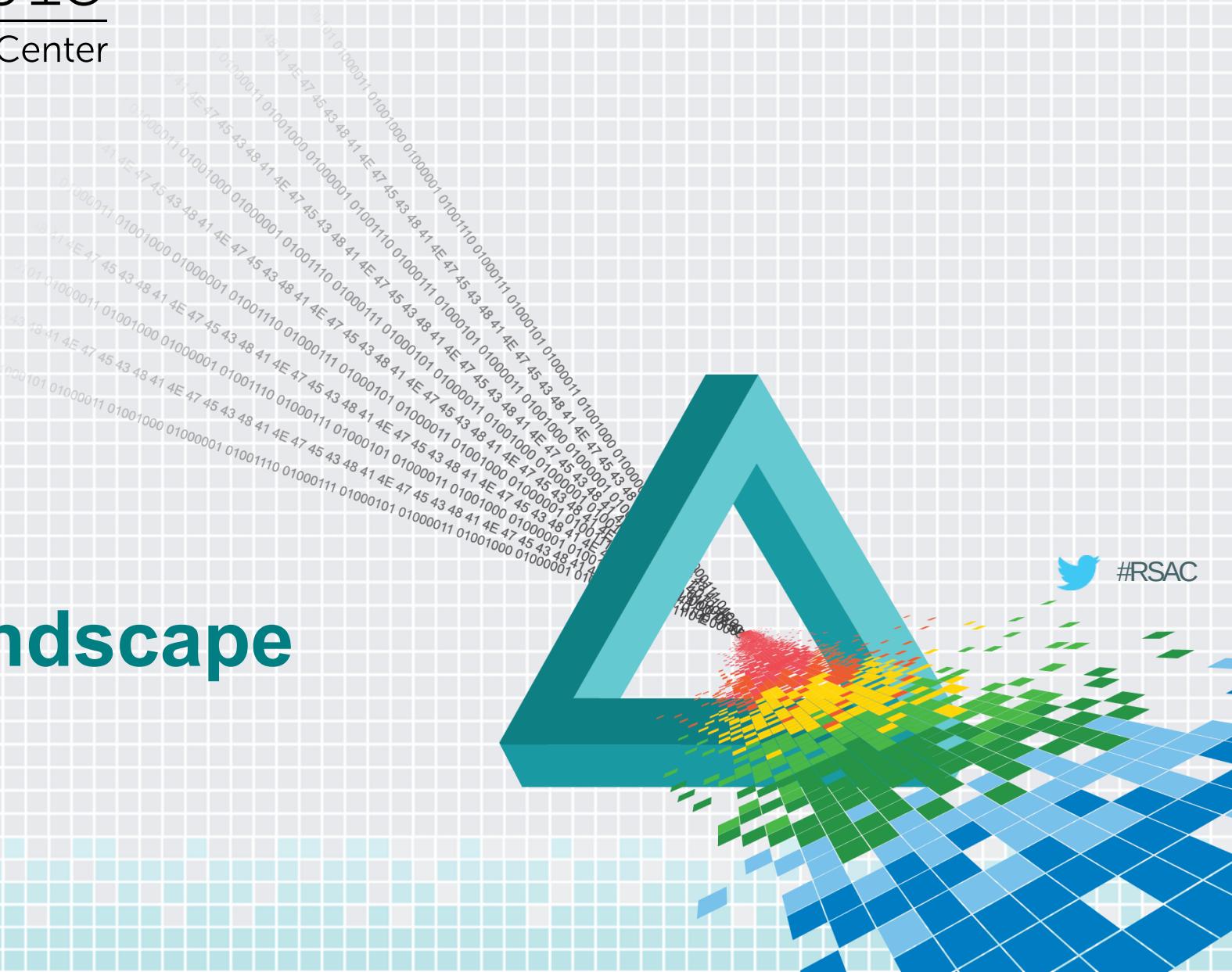
$5.6 billon

Yearly cost to the healthcare industry, due to breaches.

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

RSAConference2015

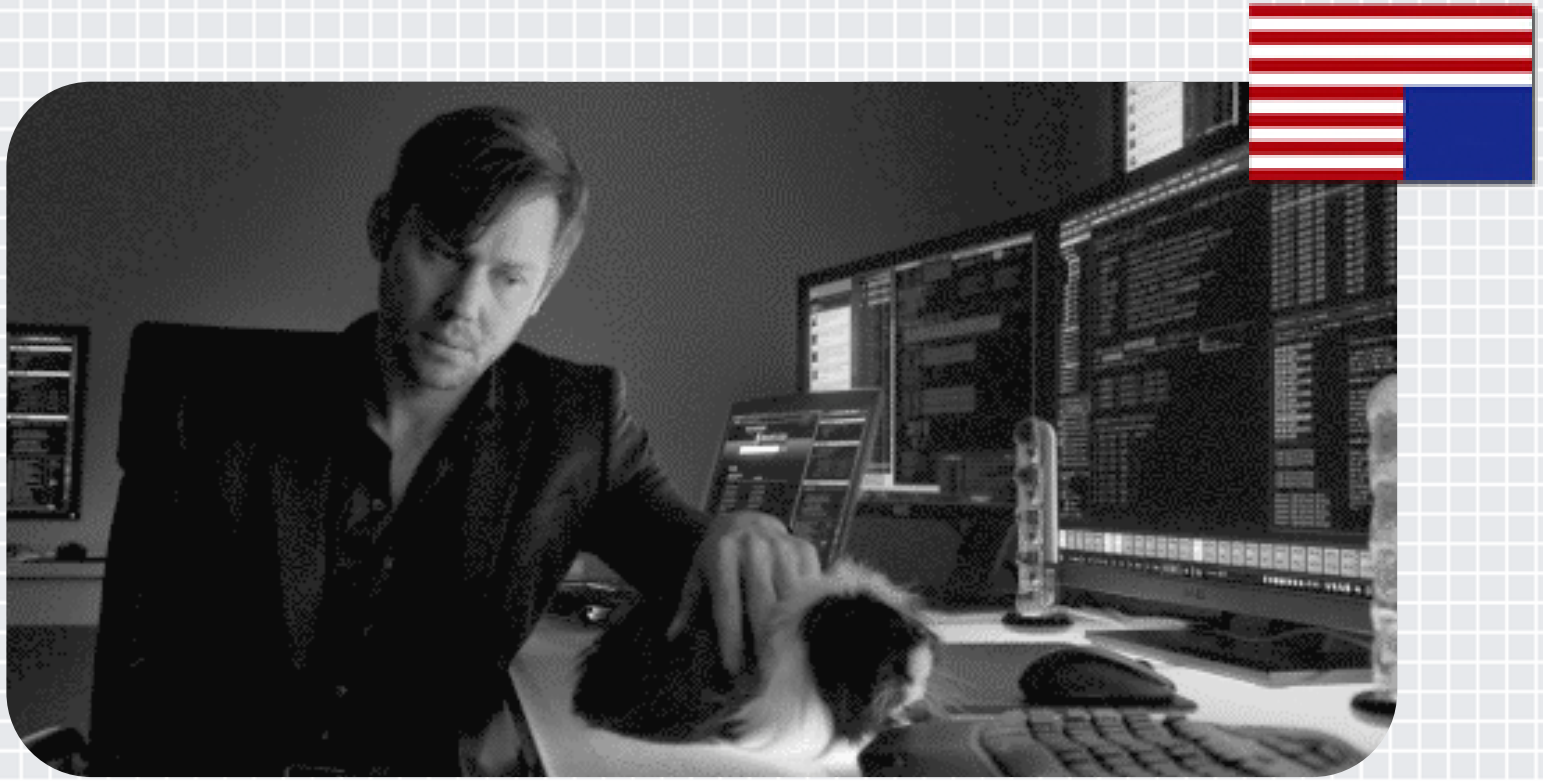
San Francisco | April 20-24 | Moscone Center



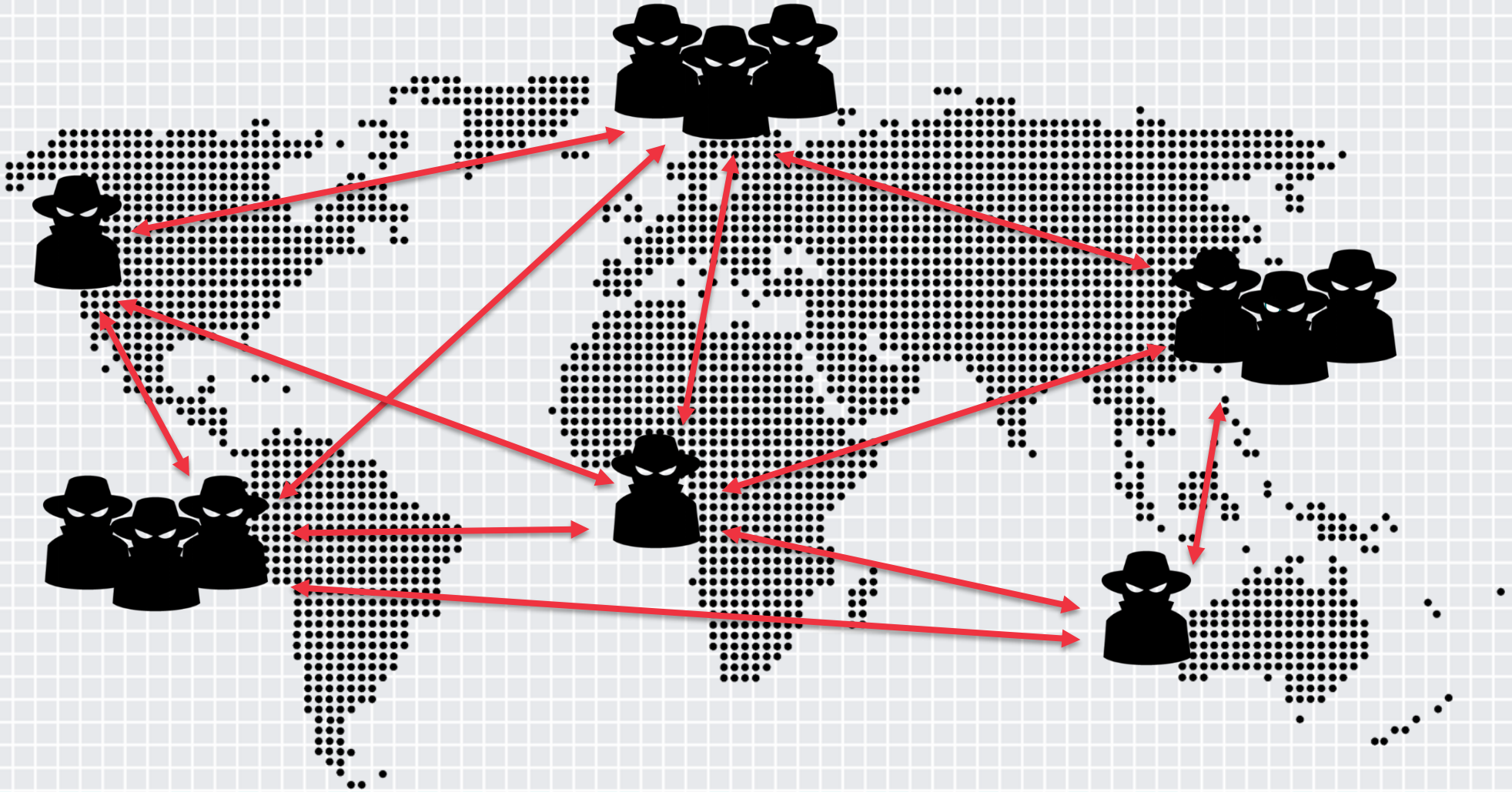
#RSAC

Today's Threat Landscape

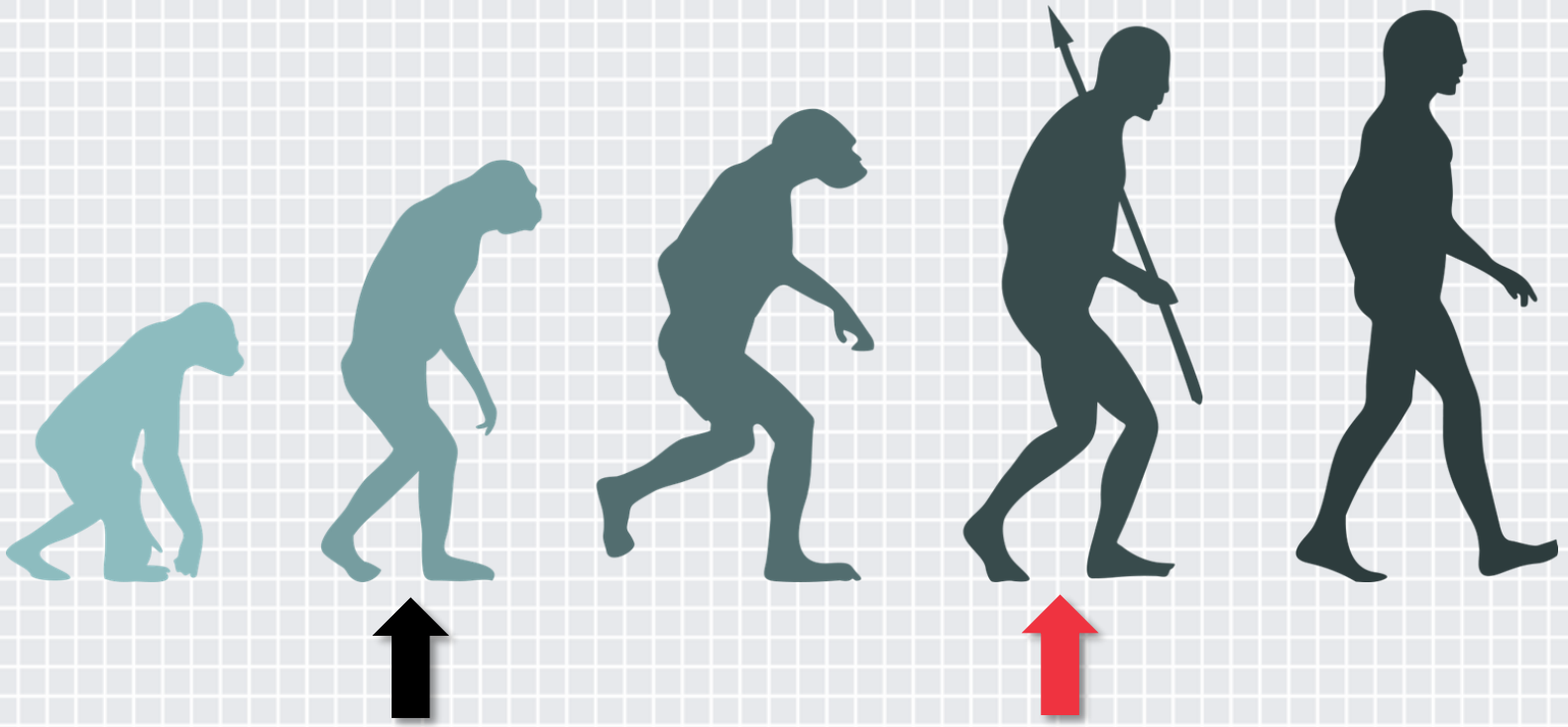
The Lone Hacker Is A Thing Of The Past



Cyber Criminals Are Well Connected



Always Two Steps Ahead of Us



…And Their Attacks Are Deadly

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

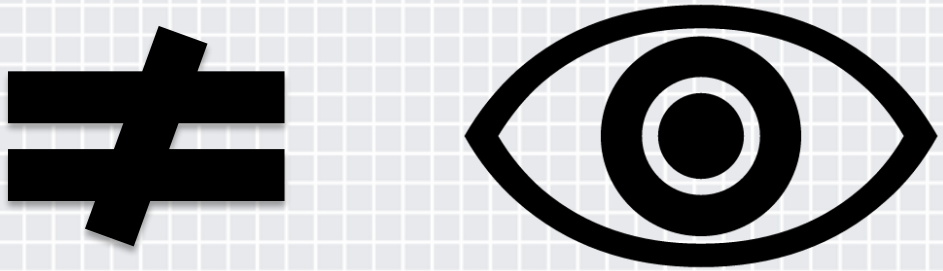
The Ideal Security Solution

#RSAC

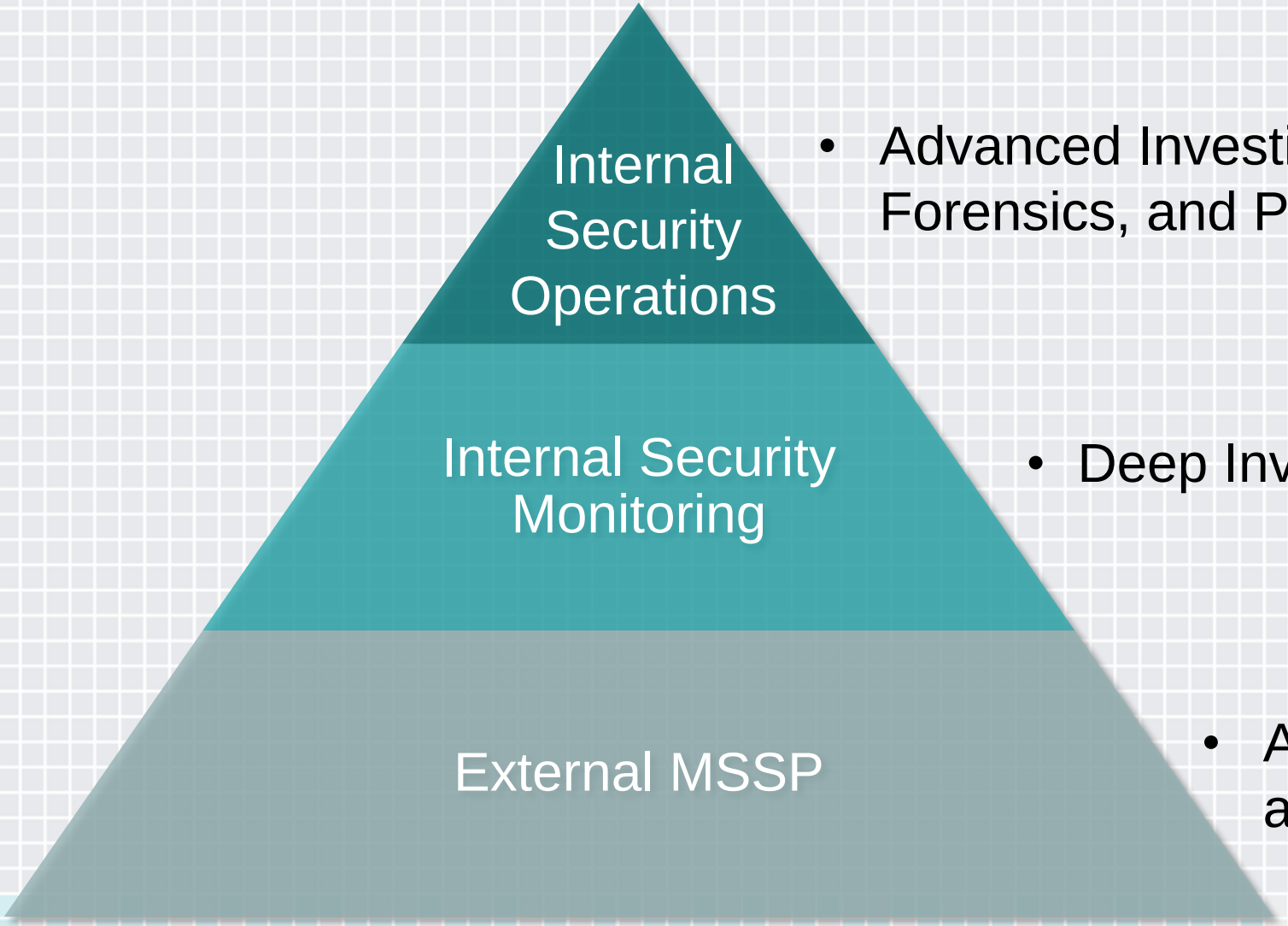
Visibility + Control

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

Network Forensics

Security Analytics

- Holistic view of enterprise data
- E-W and N-S traffic

Data Aggregation

- Deciphers machine-generated data
- Consolidates logs into one view

Activity Monitoring

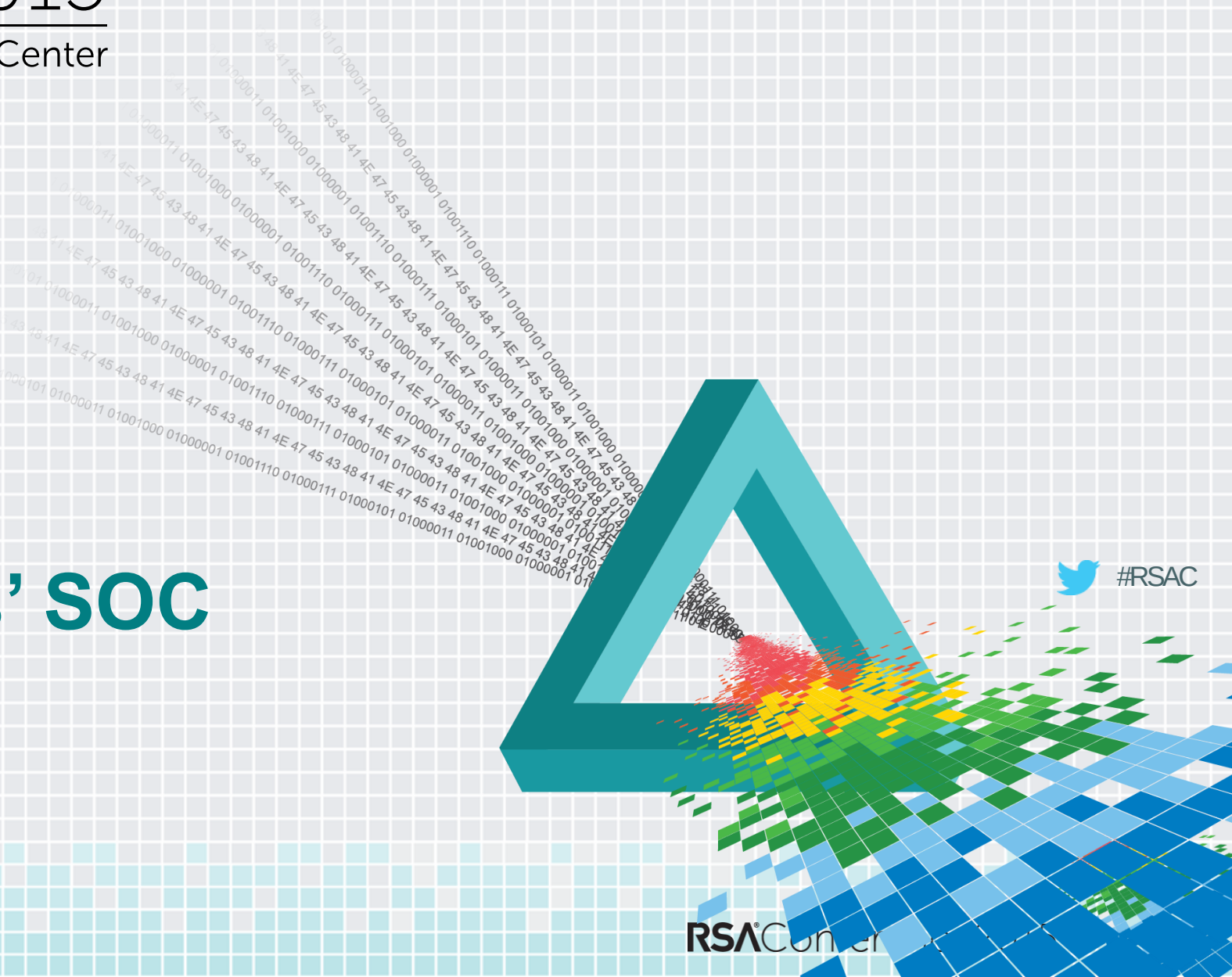
- Monitors endpoints in real-time
- Flags any suspicious endpoint activity

Anomalous Behavior Detection

- Predefines standard behavior for the network
- Indicates unusual access within the system

RSAConference2015

San Francisco | April 20-24 | Moscone Center

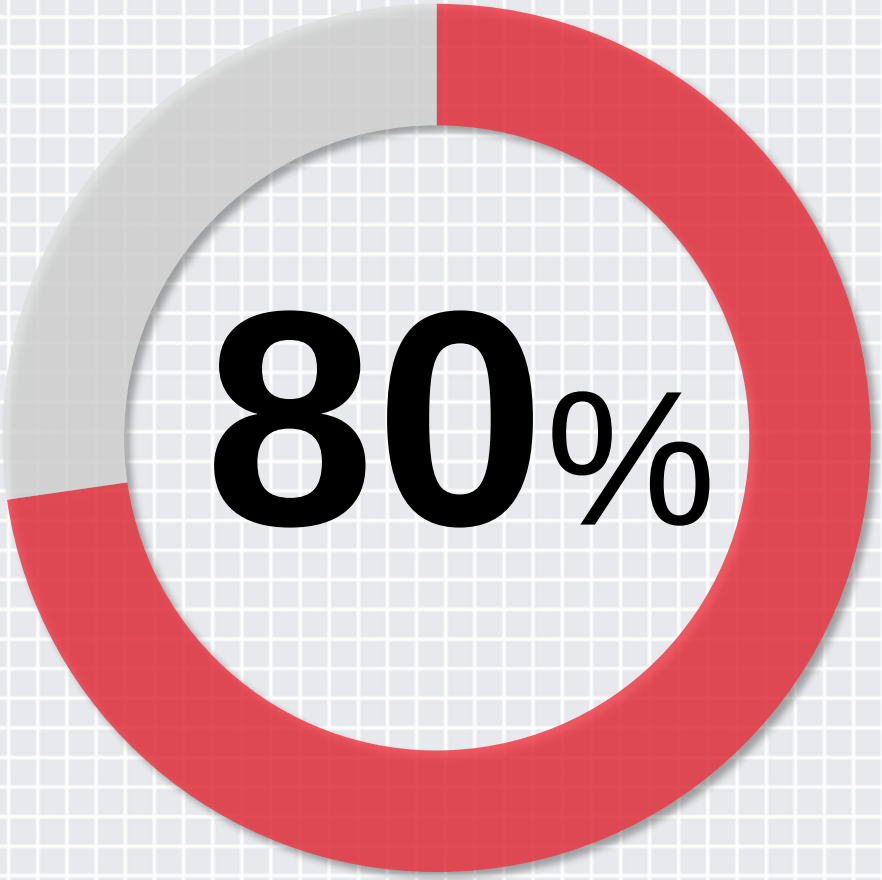


Impact of Partners' SOC Strategy

#RSAC

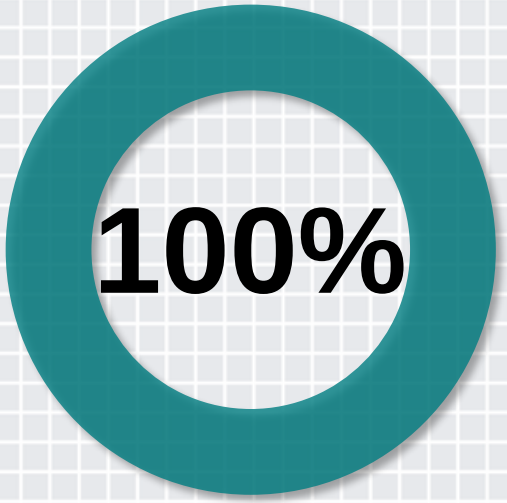
PARTNERS HEALTHCARE

Incident Response

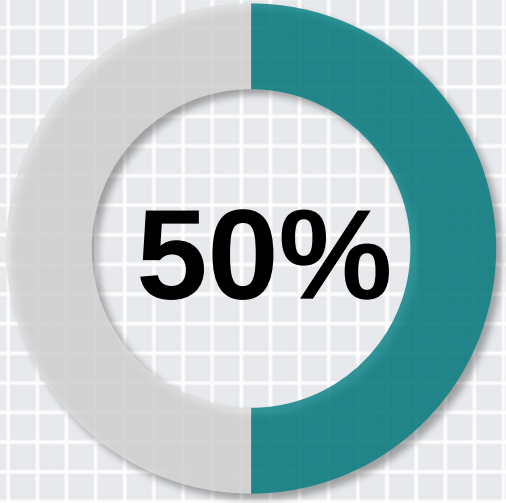


Of incidents are detected through automation

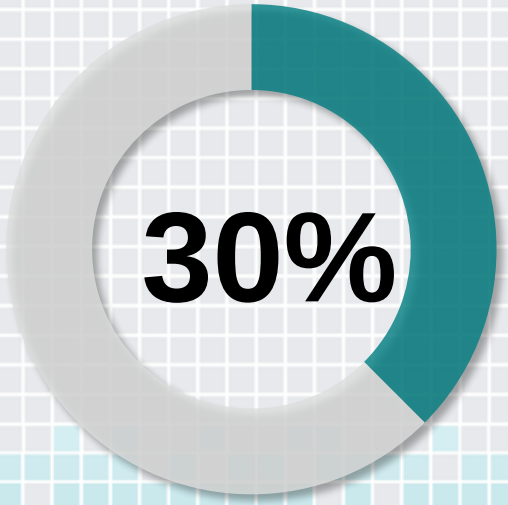
Incident Response



Reduction in detection time

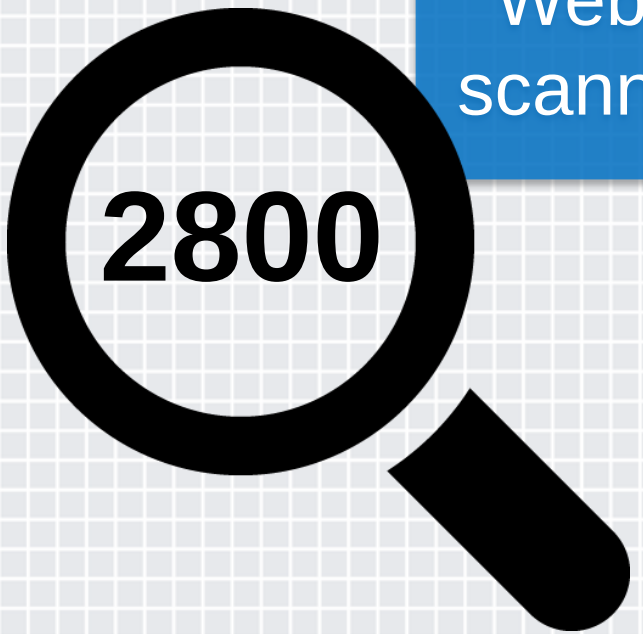


Reduction in time to collect and analyze



Reduction in event duration

Increased Visibility



Web Applications scanned bi-monthly

11 billon

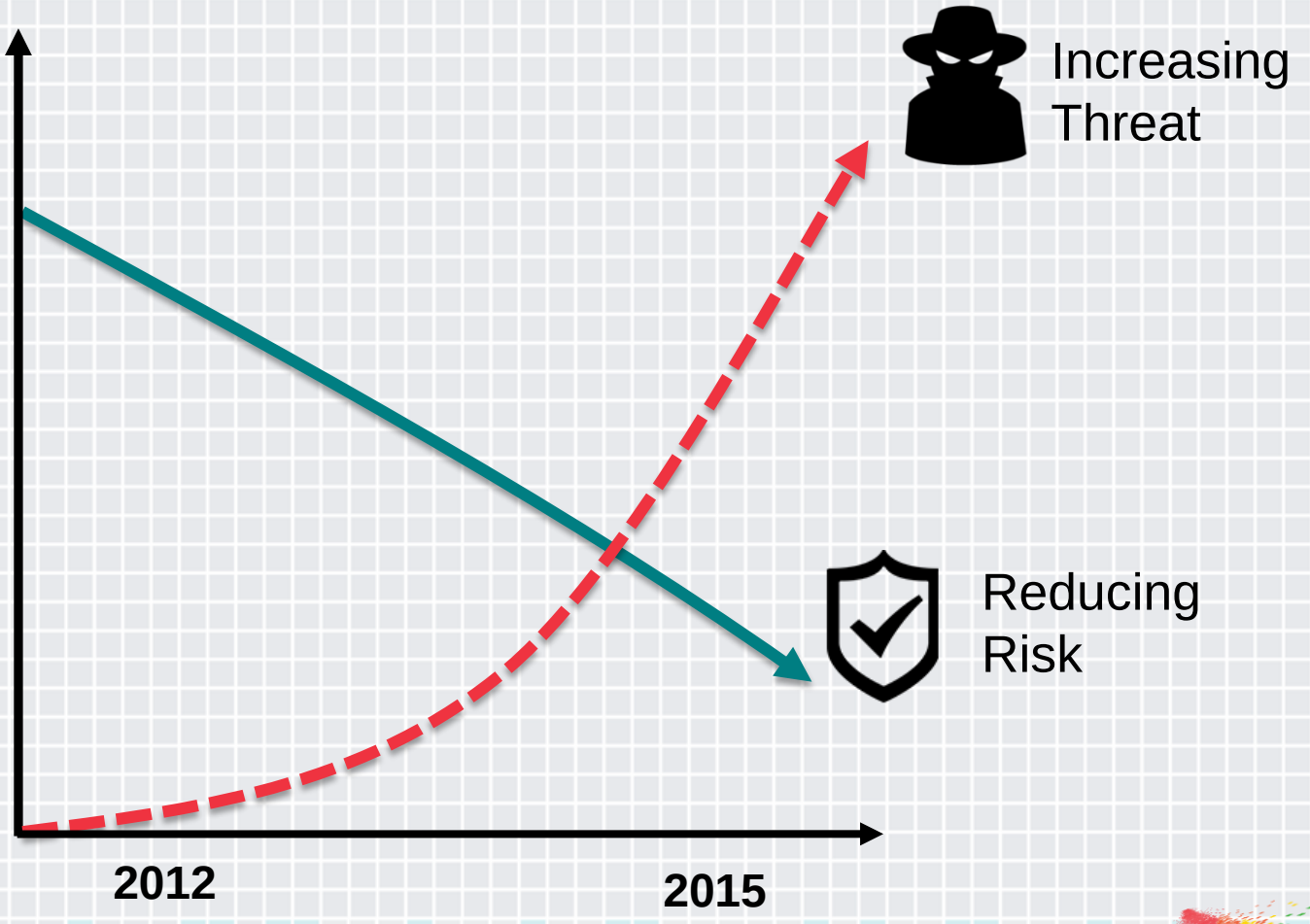
Logs per month in 2014

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

Appendix

Sources

- http://www.emc.com/security/rsa-ecat.htm
- http://www.crowdstrike.com/endpoint-activity-monitoring/
- http://www.splunk.com/en_us/resources/operational-intelligence.html
- http://www.emc.com/security/security-analytics/security-analytics.htm
- *Filkins, Barbara, "*SANS Health Care Cyberthreat Report 2014," NORSE, Feburary 2014.
- **http://hitconsultant.net/2014/03/21/infographic-the-epidemic-of-healthcare-cyber-attacks/**
- Fourth Annual Benchmark Study on Patient Privacy & Data Security," Ponemon Institute, March 2014
- **http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf?_ga=1.172114915.1943093614.1418003182**
- **https://www.splunk.com/content/dam/splunk2/pdfs/technical-briefs/building-a-soc-with-splunk-tech-brief.pdf**
- http://www.partners.org/About/Media-Center/Videos/Better-Living-New-Spaulding-Rehab.aspx
- https://www.llis.dhs.gov/sites/default/files/Boston%20Marathon%20Bombings%20Hospital%20Readiness%20and%20Response.pdf