

# RSA<sup>®</sup>Conference2017

San Francisco | February 13–17 | Moscone Center

#RSAC

POWER OF  
OPPORTUNITY

SESSION ID: CXO-W11

## An Aflac Case Study: Moving a Security Program from Defense to Offense

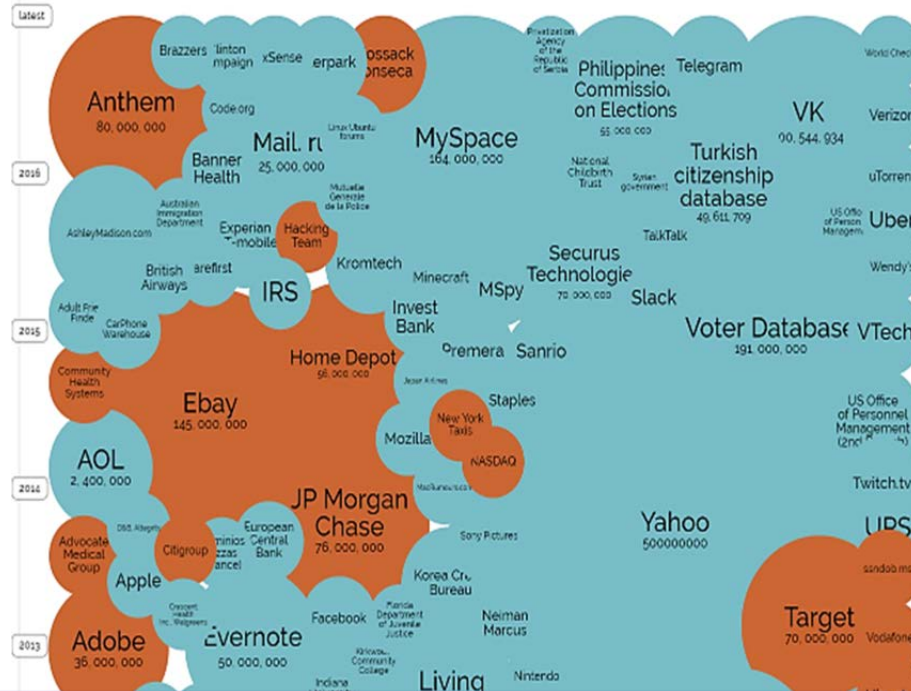


**Tim Callahan**

SVP & Global CISO  
Aflac

# Threat Landscape

Selected losses > 30,000 records (updated 10/15/16)



Security risks are growing at a faster pace than the industry can react or adapt to

# How to Build a Good Offense



## Intelligence

Leverage several types of sources



## Analytics

Find a solution that best applies to your environment



## Fight Far

Build more layers in between assets and threats



## Staff

Security tools are important, but building and finding the right talent is also important

# Intelligence

## Internal

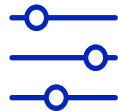


Analyze network traffic, log files, security appliances and even employee behavior



## External

Open sources, organization memberships, vendors, government programs (DHS)



## Dark Web

Monitoring the dark web helps companies see planned attacks against them or see stolen credentials

# Analytics

## Information/Data

### Threat Intelligence Platform



### Corporate Infrastructure



Security Infrastructure



Network Infrastructure



Systems and Applications

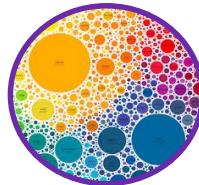
## Op Intelligence Platform



Big Data Analysis



Confidence Rating



Visualization

## Output

### High Confidence Action



Automated Alerts

### Low Confidence Action



Enrichment into other alerts

# Confidence Scores

## High Confidence Score

Domain that is well-known to be malicious



Higher confidence scores set off automated event alerts

## Low Confidence Score

Logging in to network incorrectly multiple times

A login form with a white background and a thin black border. It contains the following elements: a 'Username:' label followed by a text input field; a 'Password:' label followed by a text input field; a 'Remember Me' checkbox with the text 'Remember Me' to its right; and two buttons at the bottom, 'Cancel' and 'Login', each with a light gray background and rounded corners.

Lower confidence scores go through an enrichment process and other alerts

# Analytics Tool Results

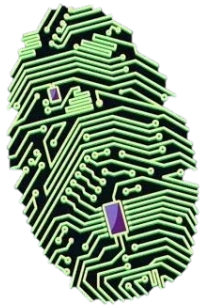


2,042,000

Connections have been blocked with fewer than 12 false positives

90

Average number of threat actor campaigns maintained



>5M

Average number of IoT's maintained

5

Member team effectively manage 5M pieces of threat intel data



# Capabilities



**DNS Firewall:** Performing automated checks against aggregated list of dangerous domains to “sinkhole” or block the connection attempts associated with malware.



**Blackholing:** A technique in which an internet service provider (ISP) dumps packets coming from a certain domain or address.



**DDoS Service:** Prevention of attacks that attempt to exhaust the resources available to a network, application or service so genuine users cannot gain access.





# Staff Challenges



## Threats and vulnerabilities constantly changing

Gartner's prediction about the Internet of Things is that we'll have 25 billion connected devices globally by 2020 – each bringing new security challenges.<sup>1</sup>

## The cybersecurity skills gap is real

This is unlikely to change in the near future, as it is predicted that 1.5 million jobs will be unfilled by 2020.<sup>2</sup>

# Seek Unconventional Perspective

## Military/Veterans

- Experience (SOC, security administration, monitoring)
- Aptitude and focus

## Data Scientists

- Ability to make correlations and predictions
- Analytical skills to spot trends and patterns



# Invest into the Future

## Grow from within

- Look within your own IT staff
- Years of experience of systems and operations can be groomed into a security professional

## Use local opportunities

- Work with technical and vocational programs in your area
- Establish internship programs and participate in capstone opportunities
- Aflac's internship and apprenticeship program gives exposure and experience



# Be Pre-emptive



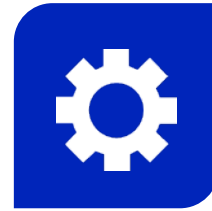
## Intelligence

Review, add and diversify your intelligence sources



## Analytics

Find a solution that not only produces intelligence but takes action with the intelligence



## Fight Far

Review your current security capabilities and build in additional layers to create distance



## Staff

Think outside the box by changing your hiring strategies and invest in local schools/programs