RSAConference2017
Singapore | 26–28 July | Marina Bay Sands

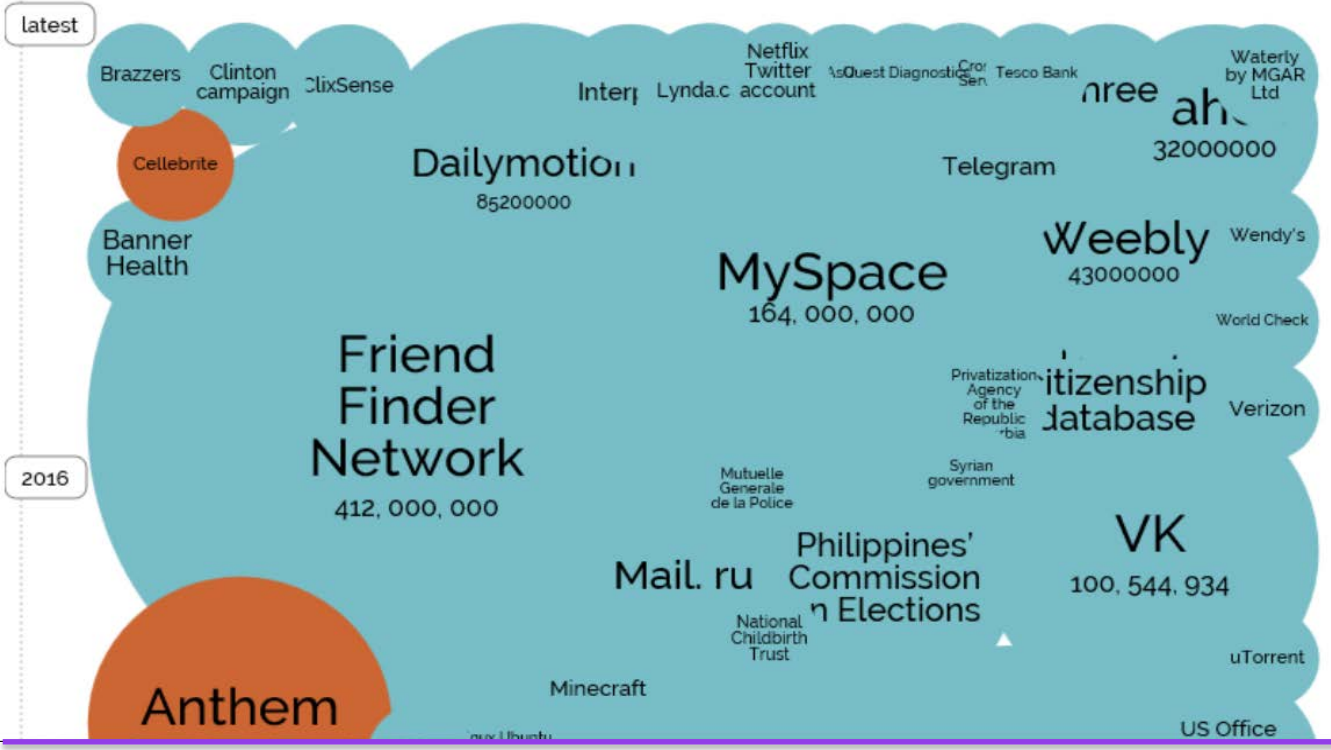
POWER OF OPPORTUNITY

SESSION ID: TTA-F02

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

Tim Callahan
SVP & Global Chief Security Officer
Aflac

Threat Landscape



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

Selected losses > 30,000 records (updated Jan 2017)

Source: www.informationisbeautiful.net

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

Find and build the right talent

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

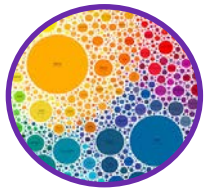
Network Infrastructure

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

Lower confidence scores go through an enrichment process and other alerts

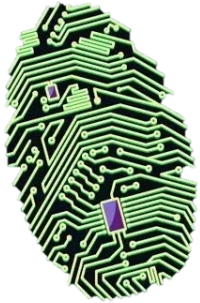
Analytics Tool Results

2,042,000

Connections have been blocked with fewer than 12 false positives

90

Average number of threat actor campaigns maintained

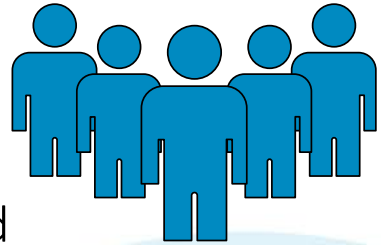


>5M

Average number of IoC's maintained

5

Member team effectively managed 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.

Incorporate Security into SDLC

Iterative

Security is added in througout the process vs. waiting for end product in waterfall

Identify Early

Integrating security in an iterative manner helps identify vulnerabilities early

Smaller Scope

Smaller scope allows us to fix defects easier which is less impact vs the waterfall method

Partnership

Agile approach creates a closer partnership with business, IT and Security which is key to security success

Build Partnership with Teams

Be a Good Partner

Vision: Communicate clearly how security aligns with business strategic objectives; “WINFM”.

Education: Offer education opportunities to development team; train on secure coding practices.

Remediation Support: Have readily available support for security issues that arise.

Build in Automation & Streamlined Processes

Provide project teams as much work upfront as possible

1. Offer standard "build kits" to project teams to check against authentication, platform, and application security

2. Build security test cases and security validation into sprints.

3. Offer security scanning tools such as Integrated Development Environment (IDE) plugin for coding or system provisioning when implementing a new application.

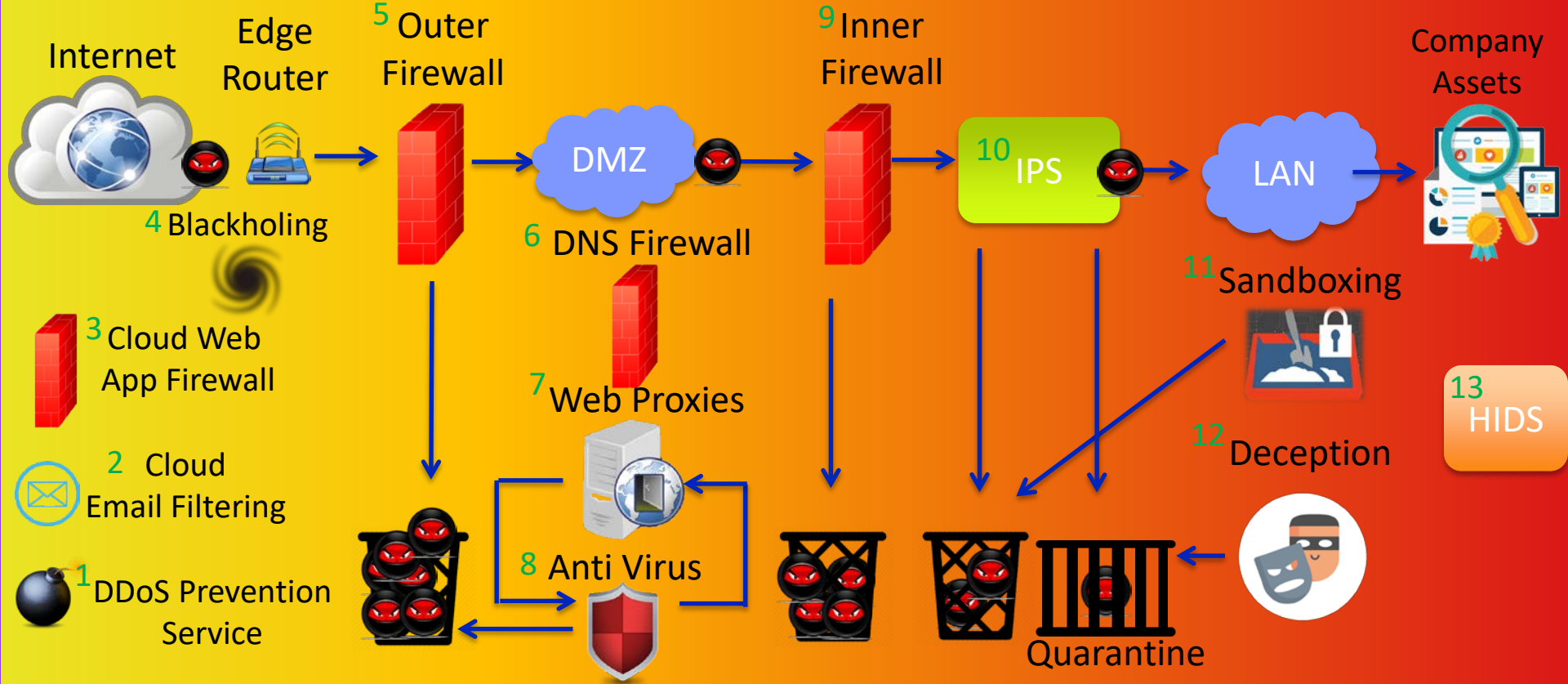
Application Development

IDE Plug In

- Source code is uploaded and scanned for vulnerabilities on vendor portal
- Vendor provides consultant services to developers for vulnerabilities solutions
- Implementing capability to scan code as it is written

Fight Far

It is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier.



Staffing

- Threats and vulnerabilities are constantly changing – Gartner predicts 25 billion devices connected to IoT by 2020 each of which brings new security challenges[1].
- The cybersecurity gap is real and unlikely to change – predicted that 1.5 million jobs will be unfulfilled by 2020[2].

1. Gartner-25 billion connected devices press release. 2. 2015 Global Information Security Workforce Study, Frost & Sullivan.

- Seek unconventional perspectives in military veterans and data scientists; such roles require aptitude, focus, and analytical skills.
- Invest in your own IT staff; experience in organizational systems and operations can be groomed into a security professional.
- Partner with local technical and vocational programs, establish internships, and participate in capstone opportunities.

Aflac Global Security

Applying Offense

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

RSA Conference 2017

Singapore

Thank You