RSAConference2019
San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: CX0-W12

Doing Security Orchestration, Automation and Response Before It Was Born

Tim Callahan

SVP & Global Chief Security Officer
Aflac

SOAR = Security Orchestration Automation Response

SOAR Defined

Gartner defines security orchestration, automation and response (SOAR) as technologies that enable organizations to collect security threats data and alerts from difference sources, where incident analysis and triage can be performed leveraging a combination of human and machine power to define priorities and drive standardized incident response activities according to a standard workflow

Source: Gartner, Preparing Your Security Operations for Orchestration and Automation Tools, 22 February 2018

So What Does This REALLY Mean?

SOAR helps create plays in the security operations playbook in an automated workflow format that is machine driven

What Makes a Good SOAR?

Automated repetitive tasks → Increase resources on critical tasks

Automated integration, investigation and response → Faster response

Integrated existing security infrastructure → Stronger defense

Before it became SOAR, Aflac implemented a capability

Quick Aflac History

March 2014
Aflac formed it’s first formal Information Security team

April 2015
Threat & Vulnerability Management team formed

September 2015
Threat intelligence system implemented

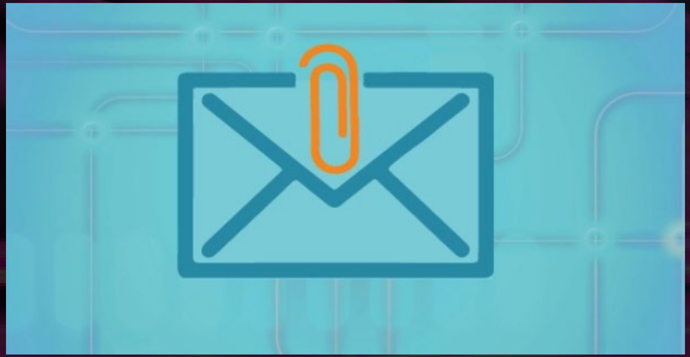
December 2016
Aflac named CS050 Award Recipient for threat intelligence system

Aflac's Threat Environment

Malicious Attachments

Highest threat to our employees

Commodity Malware

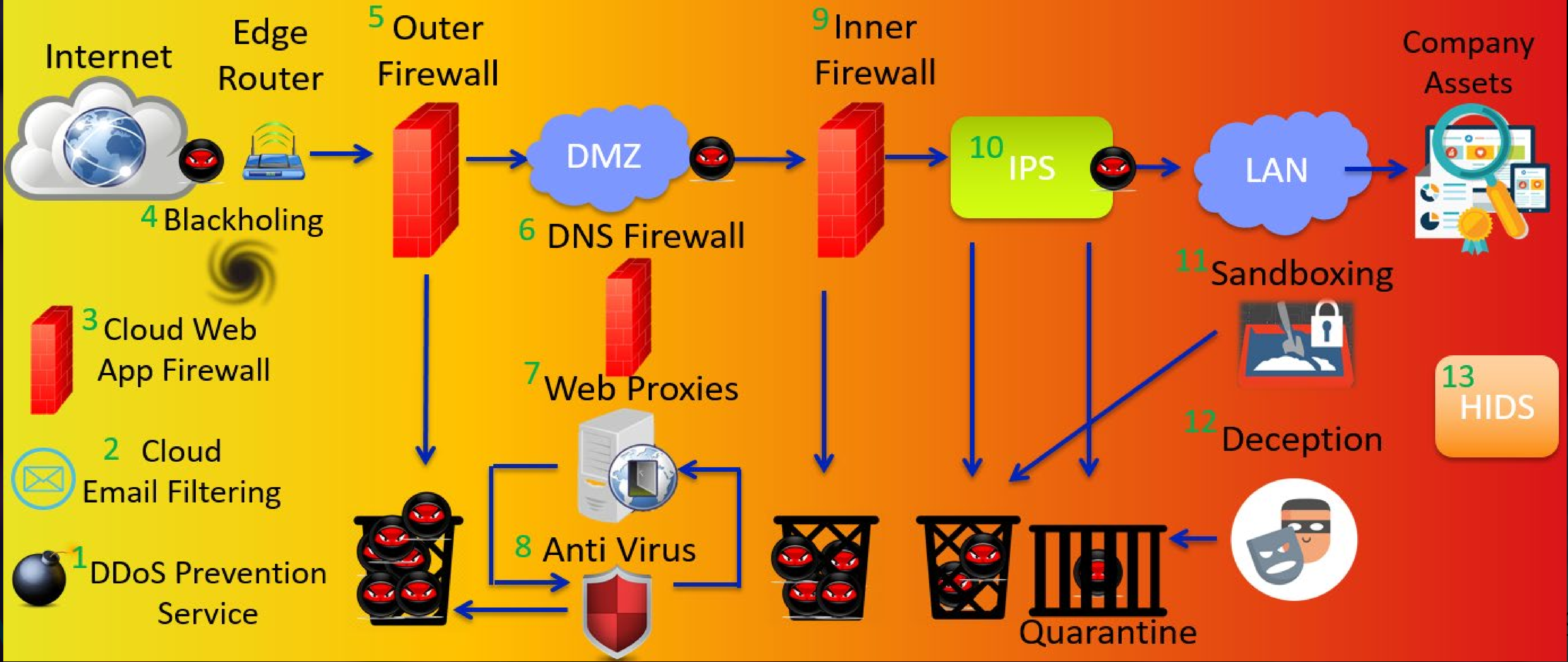


Highest threat to our field agents

Threat Plan

Fight Far

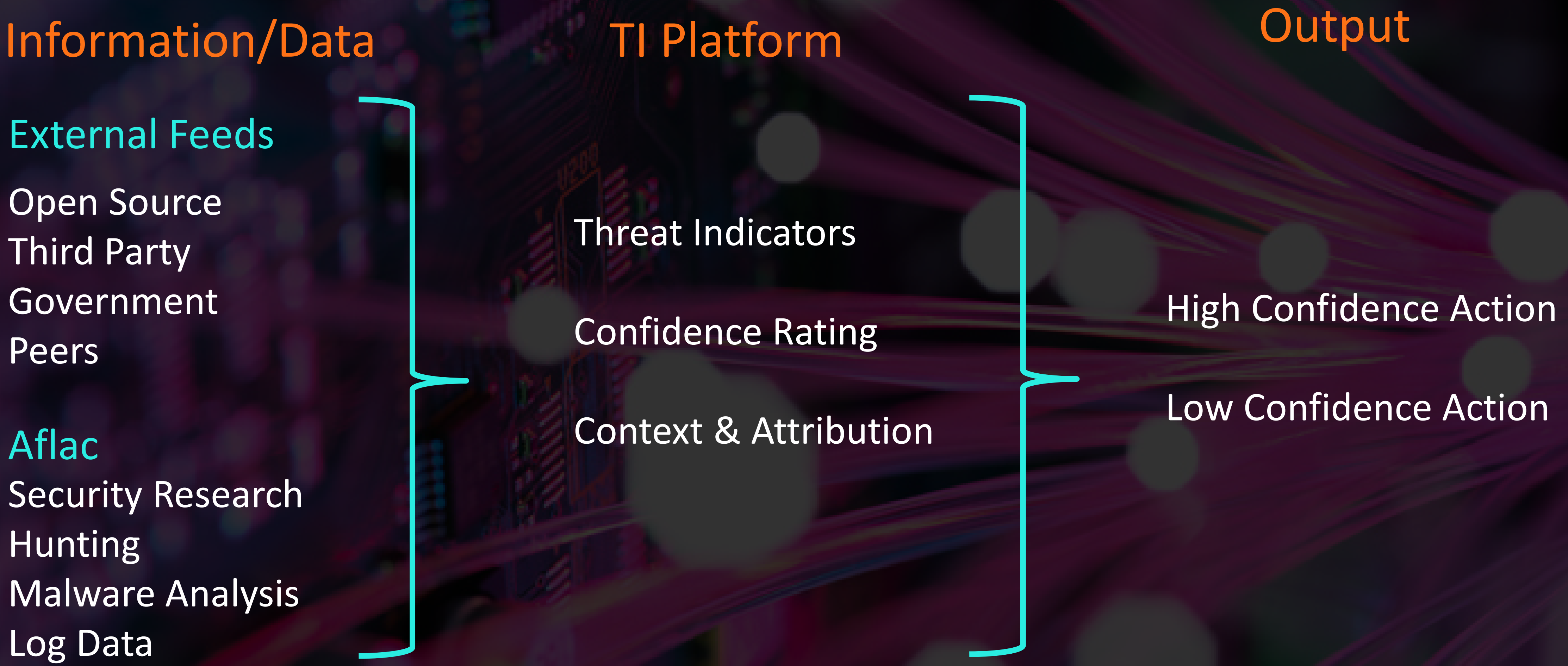
It is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier.



Key Components

- Capabilities
- Confidence Scores
- Analytics

Aflac’s Threat Intelligence Platform



Information/Data

External Feeds

Open Source
Third Party
Government
Peers

Aflac
Security Research
Hunting
Malware Analysis
Log Data

TI Platform

Threat Indicators

Confidence Rating

Context & Attribution

Output

High Confidence Action

Low Confidence Action

Confidence Scores Examples

High Confidence Score

Sandbox

Malicious files are added to automated block lists

Low Confidence Score

Unknown Analyst Information

Analyst is manually vetted for further analysis for validation of source

Aflac’s Threat Analytics System

Information/Data

Threat Intelligence Platform

Aflac

Security Infrastructure
Network Infrastructure
Systems and Applications

Operations Intelligence Platform

Big Data Analysis

Confidence Rating

Visualization

Output

Automated Alerts

Enrichment into other alerts

Manual Analysis

Confidence Scores Examples

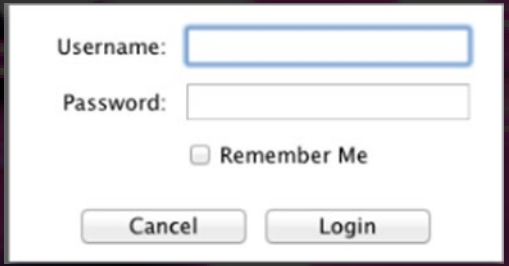
High Confidence Score

Domain that is well known to be malicious

Higher confidence scores set off automated event alerts

Low Confidence Score

Logging into network incorrectly multiple times



Lower confidence scores go through an enrichment process into other alerts

Results

49,797,351

Connections blocked with less than one dozen false positives

261

Avg. number of threat actor campaigns maintained

>8.4 Million

Average number of IoC's maintained

5

Member team able to effectively manage 8M pieces of threat intel data

Takeaways

1 If you don’t have a program, start small, but start

2 Understand your organization’s business risks

3 Evaluate opportunities for automation

4 Develop solid processes

Takeaways

5 Build a solution that best fits your organization's risk appetite

6 Expand defense in depth

7 Leverage intelligence for offensive capabilities

Questions