



@CSOevents  
#CSO50

# CSO50

CONFERENCE+AWARDS

May 1-3, 2017

The Scottsdale Resort  
Scottsdale, Arizona



## Aligning Proactive Security with Modern Threats



PRODUCED BY

**CSO**  
FROM IDG

# Improving Situational Awareness to Address Rapidly Evolving Cyber Threats

**DJ Goldsworthy**

Director, Security Operations and Threat Management

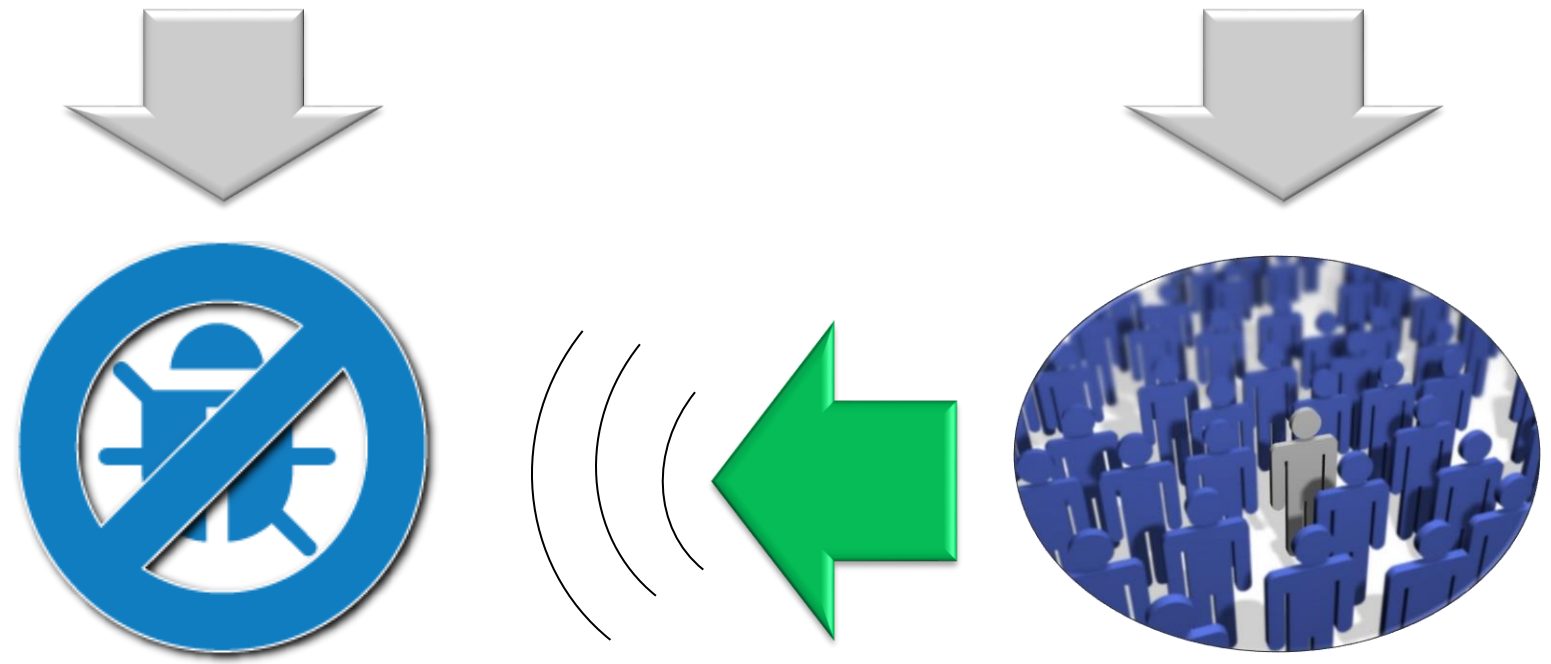
*Aflac*

# Company Overview



- Aflac, the leader of voluntary insurance sales at the worksite in the U.S., is a Fortune 500 company with more than \$26 billion in revenue and 5,300 employees.
- Aflac is insurance for daily life. We pay cash benefits fast when you're sick or hurt to help with expenses not covered by your medical insurance.
- For more than 60 years, Aflac provides financial protection to more than 50 million people worldwide. In Japan, Aflac insures 1 in 4 households. Japan accounts for 75 percent of Aflac's overall business.

# The Problem



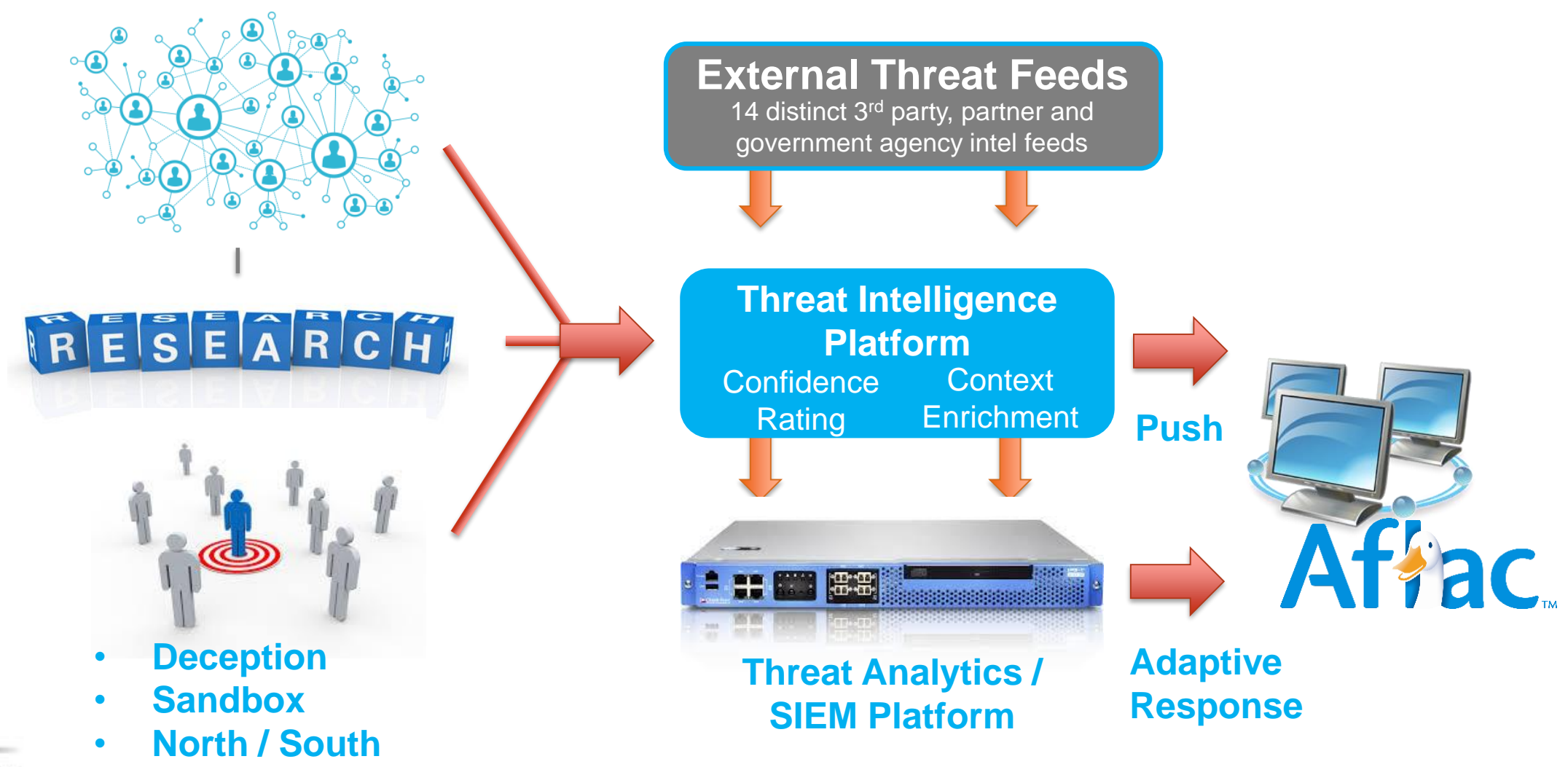
- Commodity Malware
- Crimeware
- Ransomware

**80%**

- Targeted Attack
- State Sponsored
- Insider Threat

**20%**

# Threat Intel System



# Lessons Learned

- Threat feeds are table stakes. Don't stop there!
- Automation is key and in two places:
  - Ingestion from your best sources of intel.
  - Deployment to countermeasures/remediation.
- Soft skills are incredibly important for your research team. Hire people who are plugged in!
- It helps to have someone on the team who knows integrations (python, etc.)