RSAConference2015
San Francisco | April 20-24 | Moscone Center


SESSION ID: ANF-T10

# Modern Approach to Incident Response: Automated Response Architecture

**James Carder**
Director, Security Informatics
Mayo Clinic
@carderjames

**Jessica Hebenstreit**
Senior Manager, Security Informatics
Mayo Clinic
@secitup

Monitor

Detect

Respond to Threats

# A variety of threats exist – Both internal and external to any organization. Those threats and their major characteristics are reflected in the table below:

| | Virus, Worms, and Spam | Insiders | Hacktivists | Terrorists | Organized Crime | State Sponsored |
|---|---|---|---|---|---|---|
| OBJECTIVE | Financial Gain | Revenge, Financial Gain | Defamation, Notoriety | Fundraising, Communications, Propaganda | Financial Gain | Economic Advantage |
| EXAMPLE | Scareware, Spam, Zombies | Data Destruction, Theft | DDoS, Wikileaks | Al-Qaeda Sites, ISIS | Credit, Debit Card, ACH, PHI, PCI Theft | Trade Secrets, Contracts, Legal Strategies |

# TARC Threat Analysis & Response Center

*Enterprise monitoring, altering and triage of potential **security events***

Collect logs & relevant system, network and application data.

Analyze behaviors and patterns within the data.

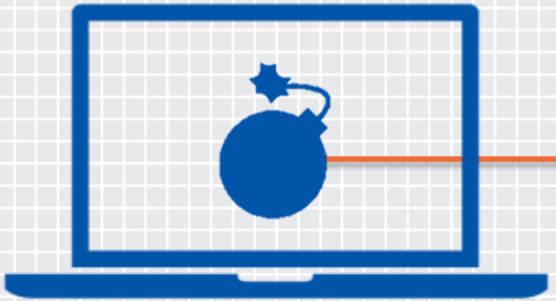
Respond & investigate anomalies in behavior or patterns.

Tactically eradicate threats

MAYO CLINIC

# INCIDENT RESPONSE

*Advanced analysis and response to large scale intrusions*



- In depth incident investigation and reporting
- In depth forensic analysis of systems and devices
- Reverse engineer malicious code used

# THREAT INTELLIGENCE

*Threat classification, attribution, indicators, warnings, and reports*

- Intelligence on attackers that have interest in Clinic;
- Attribution of attackers;
- Attacker techniques, technologies, and processes;
- Informs internal teams of relevant threats;
- Industry knowledge of breaches and exploits;
- Reporting.

# AUTOMATED RESPONSE ARCHITECTURE

Goals:

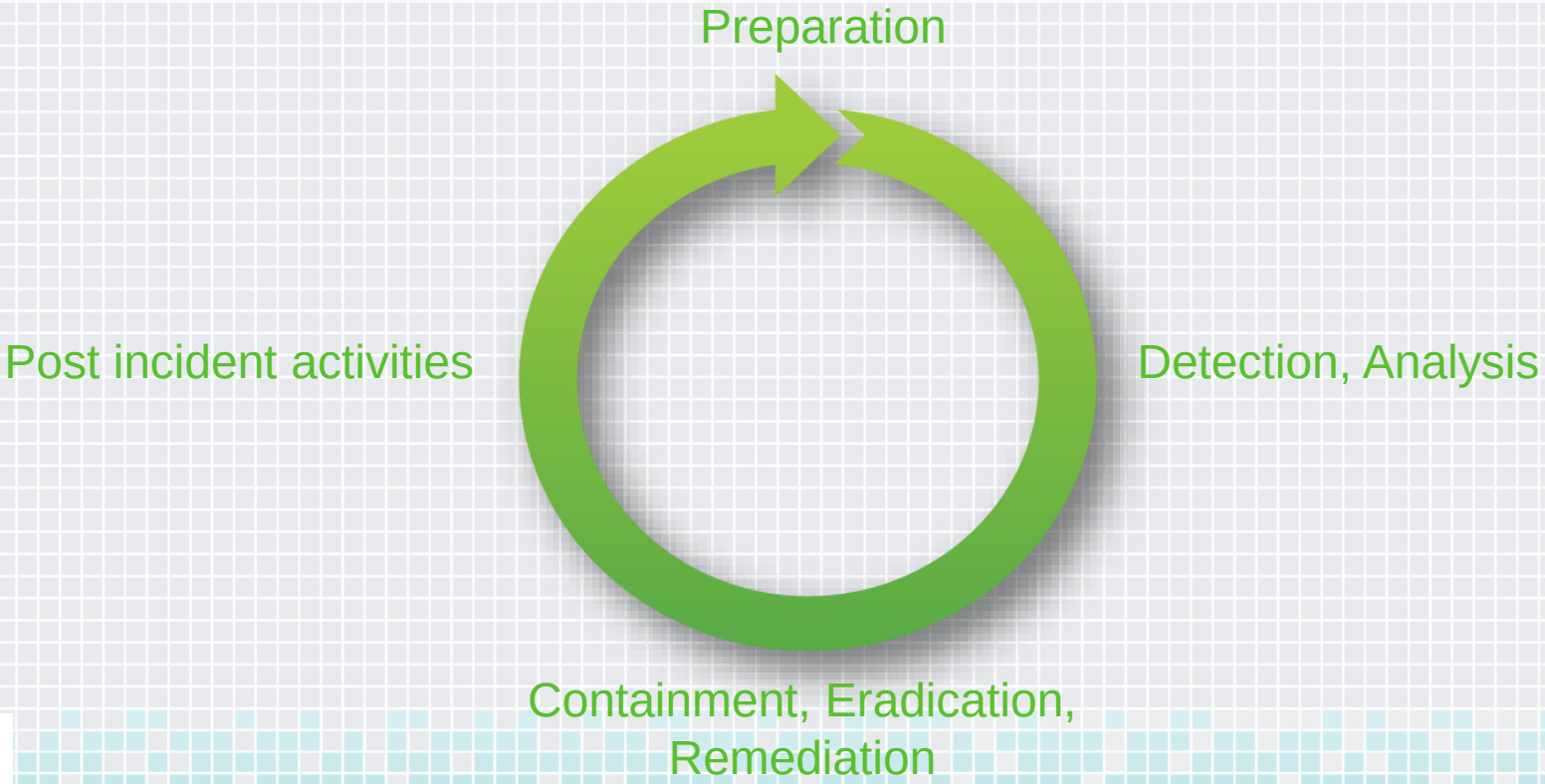
- Reduce response time from days to minutes
- Increase knowledge of internal and external threats
- Build automatic smart responses for common threats

Objectives:

- Integration of Core Technologies
- Establish enterprise visibility
- Real time threat intelligence

MAYO CLINIC

# INCIDENT RESPONSE LIFE CYCLE



# AUTOMATED RESPONSE ARCHITECTURE

## "Big Visibility" – *Visibility and Control for*

# BEFORE WE AUTOMATE

Inventory of tools

- IT Infrastructure
- Information Security Infrastructure

Evaluation of Current Processes

- IR (malware, forensic handling, communication)
- IT (remediation, cleanup, communication)

Metrics

- What takes up most of our analyst time?
- How long does it take to detect, respond, remediate?

# DETERMINING WHAT TO AUTOMATE

What causes 80% of our daily analyst work load?

- Old fashioned 80/20 rule
- What would your analyst love to not have to do anymore?

What can we do to prevent initial compromise?
- Incident lifecycle / kill chain

What are our biggest threats and targets?
- Who targets healthcare?
- What or who do they target?

# RISKS TO AUTOMATION


Inadvertent remediation of valid data/files/processes

- Can be tough when staff have admin rights
- Aided by scoring system (e.g. if validated evil by 3 different sources based on attributes)

Automation can reduce long term staff learning

- They may not learn “why or how”, only “what”
- Become automation and tool dependent

We might miss something

- catch a symptom (small scale), not the cause (large scale)
- Single event vs. chain of events


USE CASES

# INCIDENT TRIAGE AND RESPONSE TODAY

4 – 8 Hours

Attack: Inbound Phishing Email

- Threat: Financial Crime
- Email disguised as Help Desk

Detect: User Reported

- Email received by 200 people before first report
- Contains malicious attachment, installs code

Investigate: Triage and Analysis

- Search SIEM and other tools
- Analyze attachment and code
- Identify victims

Clean: Wipe code from system and email from mailboxes

- Contact IT Messaging, respond
- Contact IT Support, respond
- Contact Help Desk, respond

# INCIDENT TRIAGE AND RESPONSE TOMORROW

4 – 8 Minutes

Attack: Inbound Phishing Email

- Threat: Financial Crime
- Email disguised as Help Desk

Detect: Technology

- Email received by 20 people, technology detected
- Contains malicious attachment, installs code

Investigate: Triage and Analysis

- Search SIEM and other tools
- Analyze attachment and code
- Identify victims

Clean: Wipe code from system and email from mailboxes

- Remove code from system
- Remove email from mailboxes

MAYO CLINIC

# INCIDENT TRIAGE AND RESPONSE TODAY

Several to Hours to Weeks or More

## Attack: Watering hole

- Researcher unknowingly visits compromised website
- Ad on compromised site installs malware on researcher's endpoint

## Detect: Technology

- Web based malware detection appliance detects malware and sends alert to SIEM

## Investigate: Triage and Analysis

- Analyst manually gathers evidence and log files and analyzes data
- Manually initiate image of memory and/or disk
- Manually submit malware to sandbox and Malware analysts

## Response: Clean malware and Initiate Blocks

- Manually create tickets to other supporting teams to clean system or reimage
- Manually create ticket to NOC to block C2

MAYO CLINIC

# INCIDENT TRIAGE AND RESPONSE TOMORROW

Minutes to few hours

## Attack: Watering hole

- Researcher unknowingly visits compromised website
- Ad on compromised site installs malware on researcher's endpoint

## Detect: Technology

- Web based malware detection appliance detects malware and sends alert to SIEM

## Investigate: Triage and Analysis

- Analyst has data readily available in alarm to analyze
- Automated response engages Enterprise DFIR system to create image of memory and/or disk for analysis
- Automated response engages affected endpoint; grabs a copy of the malware and submits to sandbox
- Sandbox runs automated analysis

## Response: Clean malware and Initiate Blocks

- C2 automatically blocked due to proactive threat monitoring
- Malware analyst confirms high fidelity threat, approves pre-configured auto response
- Smart SIEM engages end point to remediate system via deletion/cleaning of malware

MAYO CLINIC

# INCIDENT TRIAGE AND RESPONSE TODAY

Weeks or more

## Attack: Anomalous Behavior

- Employee accesses directories outside of normal behavior pattern
- Accesses information related to sensitive research

## Detect: User Reported

- Goes undetected until reported to security team, if ever

## Investigate: Triage and Analysis

- Analyst manually gathers evidence and log files and analyzes data
- User's access likely remains intact while data analyzed


## Respond: Manually Create Tickets for Supporting Teams

- Contact IT NOC, respond
- Contact Investigative Legal Department, respond
- Contact Various IT Teams, respond

# INCIDENT TRIAGE AND RESPONSE TODAY

minutes

Attack: Anomalous Behavior

- Employee accesses directories outside of normal behavior pattern
- Accesses information related to sensitive research

Detect: Technology

- System has already learned normal baseline for user
- Creates alarm for analyst automatically

Investigate: Triage and Analysis

- Analyst has data readily available in alarm to analyze


Respond: Automatically clean and mitigate

- Automated response engages Domain Controller to disable user account
- Automated response engages Access Switch to disable network port
- Tickets to other supporting teams automatically opened

MAYO CLINIC

# INCIDENT TRIAGE AND RESPONSE TODAY

Weeks or more

| | |
|---|---|
| Attack: Unknown Command and Control | • Perimeter monitoring technology/service alerts, if we're lucky (rarely for new stuff) |
| Detect: Luck | • Goes undetected until reported to security team, if ever |
| Investigate: Triage and Analysis | • Analyst manually gathers evidence and log files and analyzes data<br>• User's access likely remains intact while data analyzed |
| Respond: Manually Create Tickets for Supporting Teams | • Contact IT NOC, respond<br>• Contact Investigative Legal Department, respond<br>• Contact Various IT Teams, respond |

# INCIDENT TRIAGE AND RESPONSE TOMORROW

Weeks or more

Attack: Unknown Command and Control

- Newly registered domains (domain tools, etc.)
- Domain Generation Algorithms (DGAs)

Detect: Script Report

- Analyze output of DNS log parsing script and send to SIEM

Investigate: Triage and Analysis

- Analyst looks for supporting indicators
- Queries domain history
- Smart SIEM engages end point to grab copy of malware

Respond: Clean malware and Initiate Blocks

- Malware analyst confirms high fidelity threat, approves pre-configured auto response
- Smart SIEM engages end point to remediate system via deletion/cleaning of malware

MAYO CLINIC

# INTELLIGENCE AND AUTOMATED RESPONSE

- Indicators of compromise (IOC) are automatically searched in enterprise
- Changes to threat environment immediately detected
- Instantaneously provides context around incident
- Easily correlating similar methods being used over long periods of time

# ACTIONABLE DATA TYPES

## Finished Intelligence Reporting

- Analysis Documents
- Blogs
- RSS Feeds

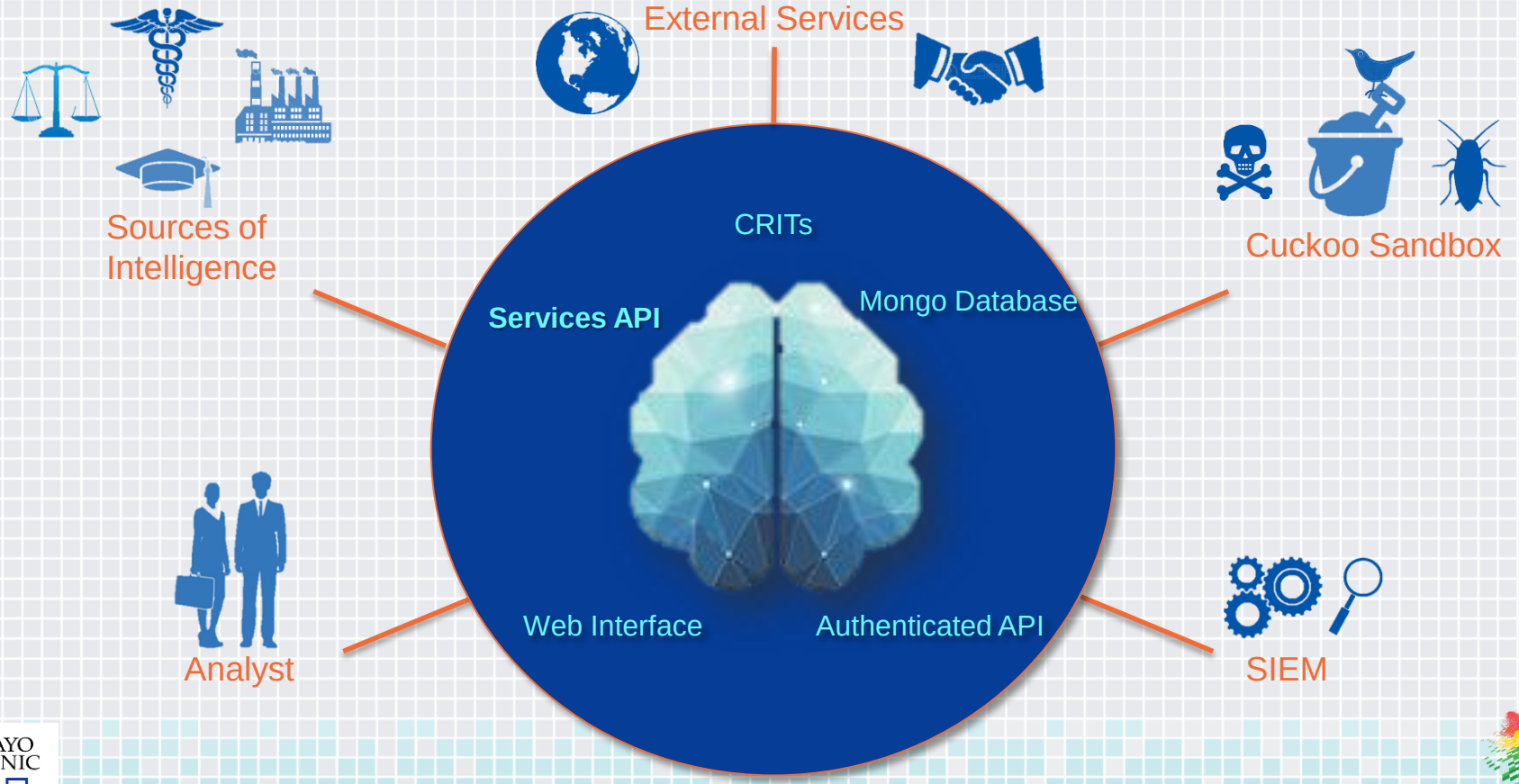
## Indicators of Compromise (IOC)

- Comma Separated Value Files
- Text Files
- STIX
- OpenIOC

## Raw Data Types

- Malware Samples
- Packet Capture Files
- Mail Samples

# Threat Intelligence Architecture



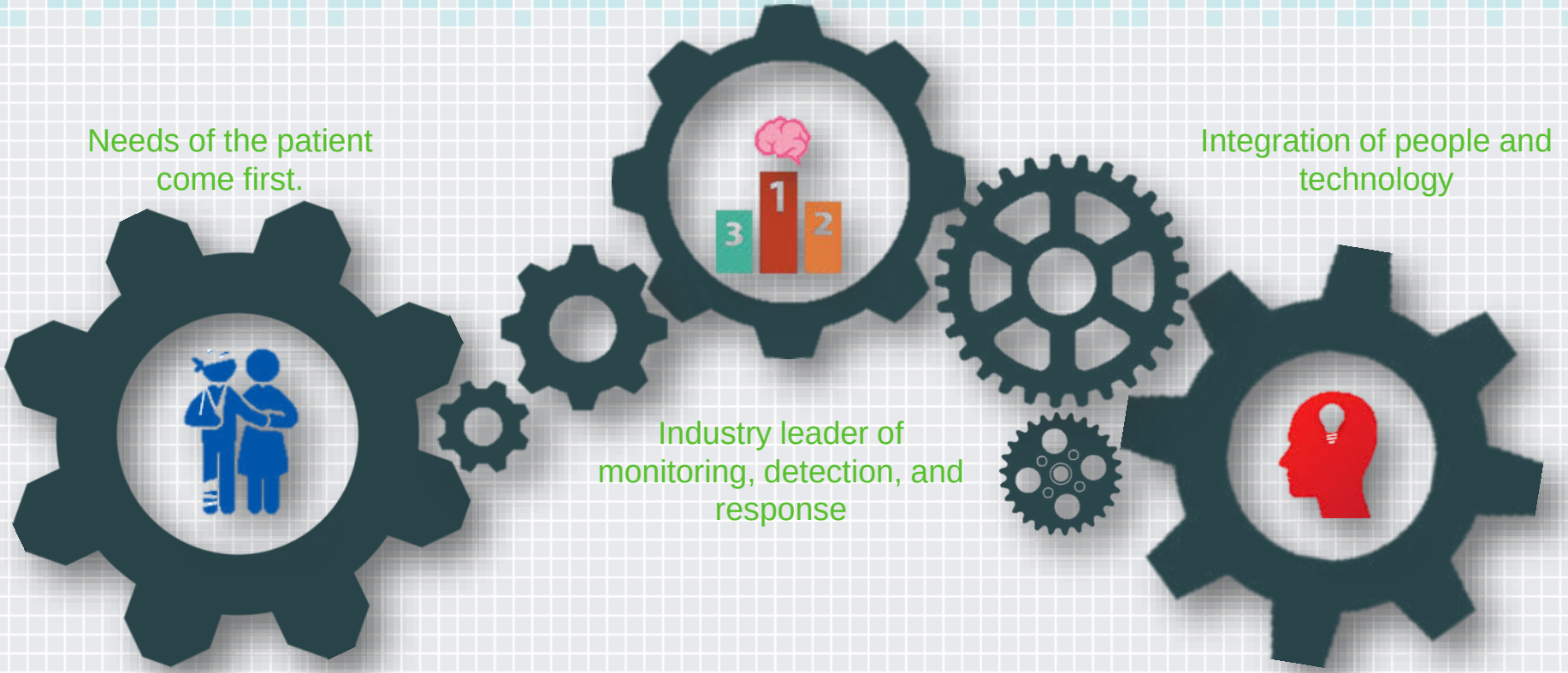
# Measuring Success

Mean time from:

- Detection to response
- Response to remediation
- Remediation to reporting

Needs of the patient come first.

Integration of people and technology



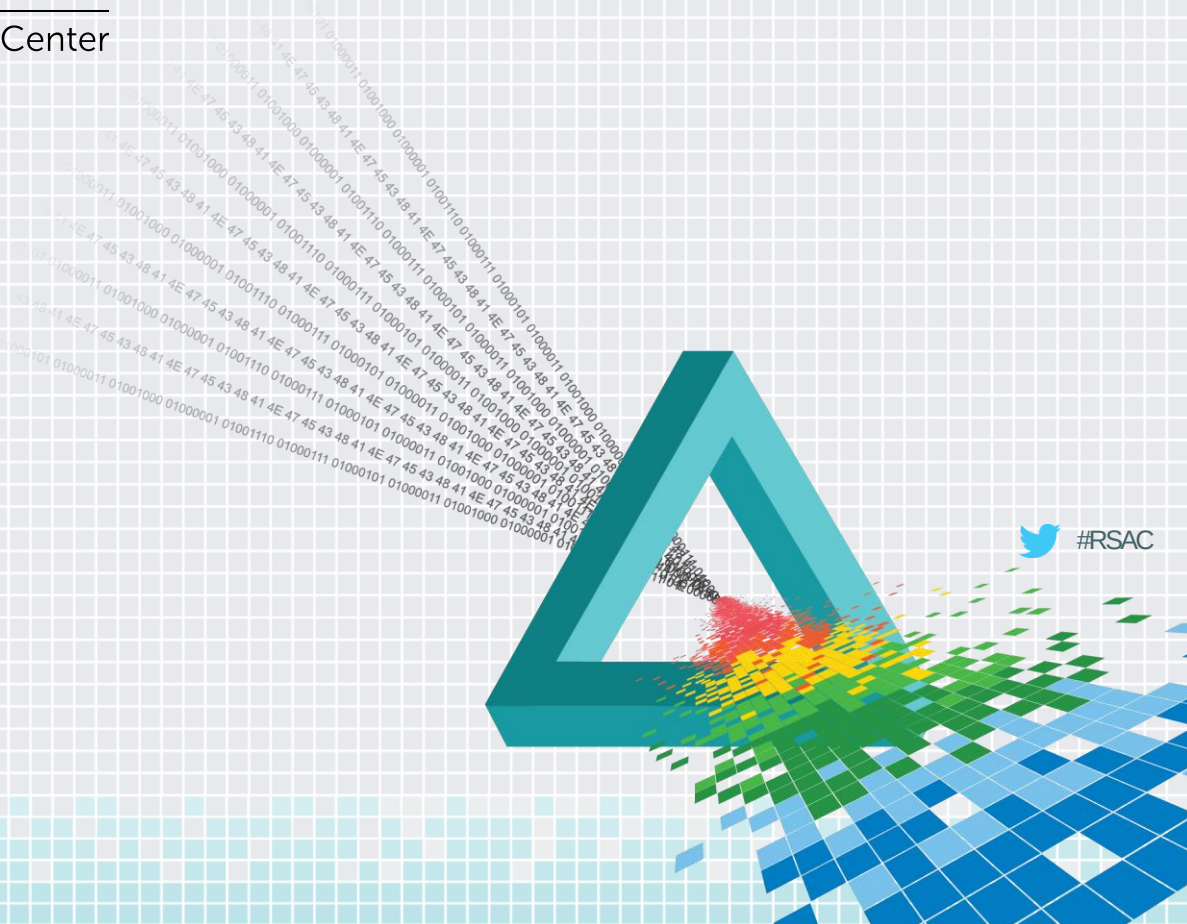

Industry leader of monitoring, detection, and response

MAYO CLINIC

# Apply What You Have Learned Today

- Next week you should:
  - Map your technologies to the incident response life cycle
  - Create use cases based on law of dual advantage (eliminate pain while finding evil)
- In the first three months following this presentation you should:
  - Inventory identities, networks, systems, and applications (get the baseline, understand normal)
  - No really….understand normal
  - Pressure your vendors (API integrations)
- Within six months you should:
  - Enterprise implementation of your use cases (detection, respond, remediation)

# Questions



RSAConference2015

San Francisco | April 20-24 | Moscone Center

# Thank You!