RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

SESSION ID: AIR-R03

Practical Implementations of a Threat Intelligence Program

Craig Hall

Manager, Threat Analytic Cell
IAG

Who Am I?

- 10 years in infosec
  - Vulnerability Management
  - SOC
  - IR
  - Threat Intel
- MSSP + vendor life
  - Fortune 500s
  - Gov
  - DIB

RSAConference2019
Asia Pacific & Japan

Introduction to Cyber at IAG

Background on IAG

- Australia's largest general insurer


Symantec.
GERMANY
MIKE PENCE
Republican Vice-Presidential Nominee
DON'T GET HOOKED!

RSAConference2019
Asia Pacific & Japan

1st Attempt at Intel

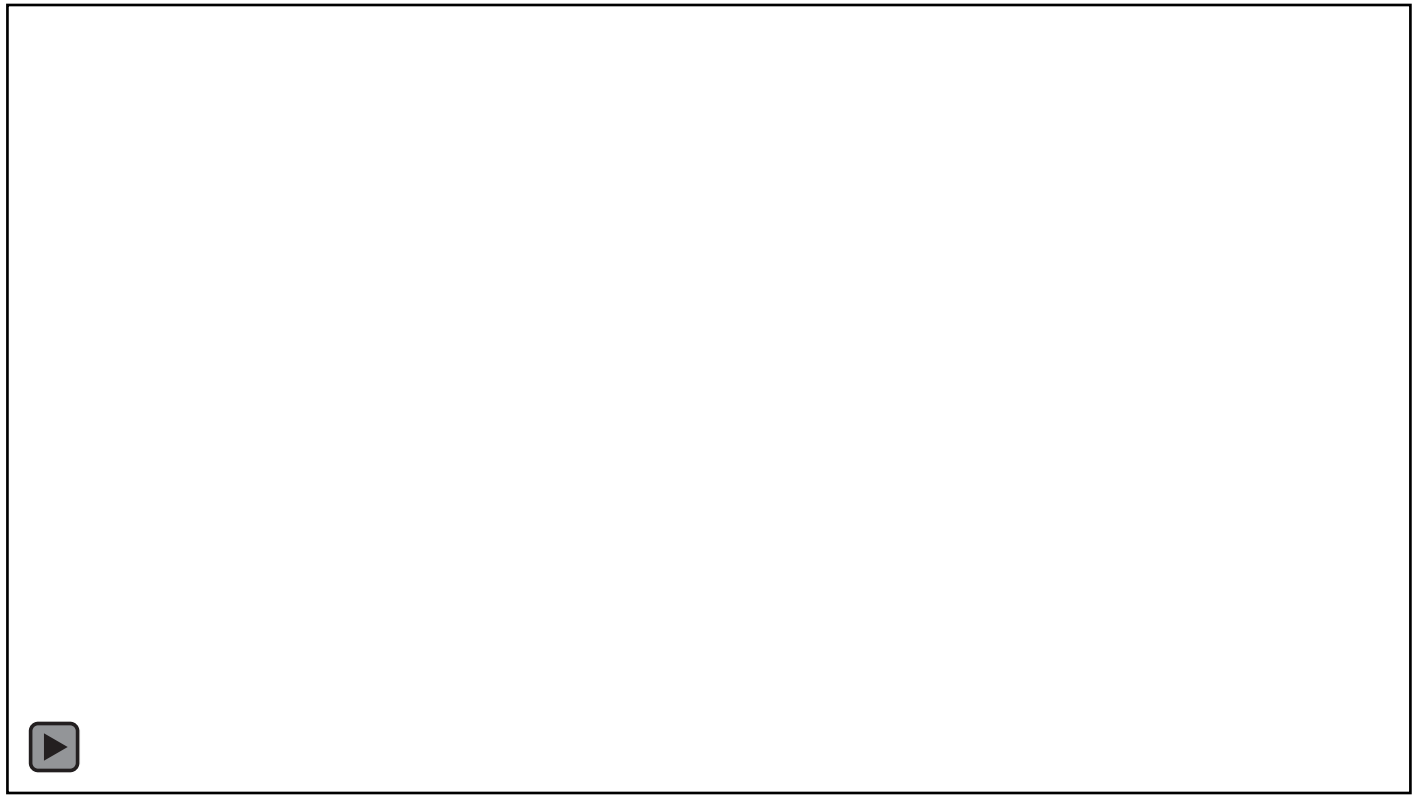
Why Threat Intel?

- It was the next logical step for our SOC
- We wanted to find more bad stuff
- A vendor told us to

Challenges Faced

- We flooded ourselves with data
- No collection management framework
- No use-cases for intel

Challenges Faced



Early Visions of a Threat Intel Program

[redacted] Intel Ingested
67

[redacted] Intel Ingested
46,718

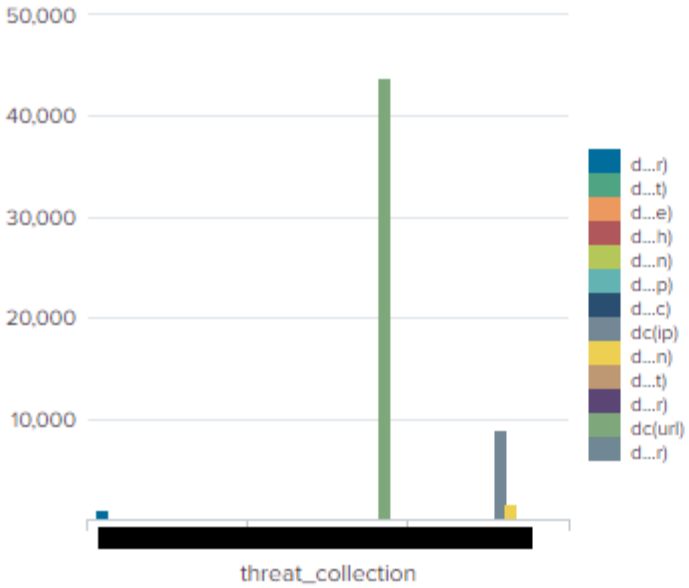
[redacted] Intel Ingested
3,368

[redacted] Intel Ingested
0

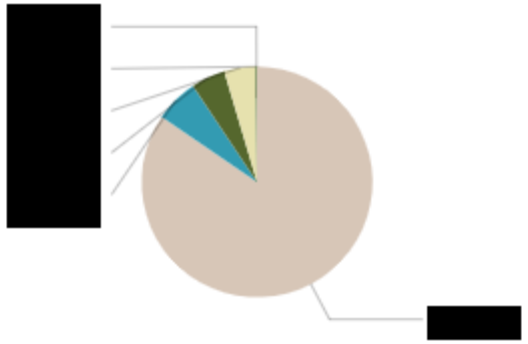
[redacted] Intel Ingested
2,638

[redacted] Intel Ingested
2,403

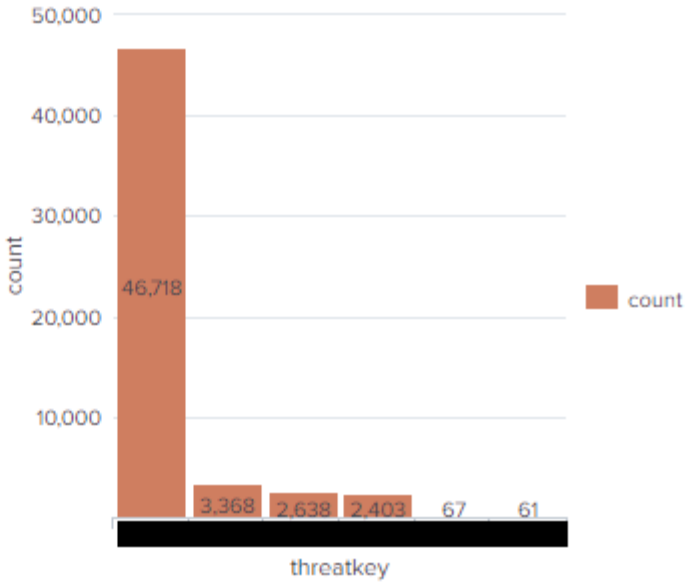
Indicators per Collection (IOC Split)



Indicators per Collection (Source Split)



Indicators per Collection (Source Split)



Great Peer Examples

ANZ Bank

Target

RSAConference2019
Asia Pacific & Japan

2nd Attempt at Intel

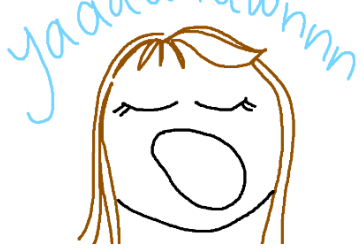
My* goals of TI

- What are the capabilities of the people currently attacking us?
- What is happening to my peers?
- What bad things will happen next?

*your goals may differ

Understanding Our Threat Model

Not people



People who aren't good at computers

People who are good at computers

People who are good at computers and are experienced attackers

People who are good at computers and are experienced attackers (including kinetic actions)

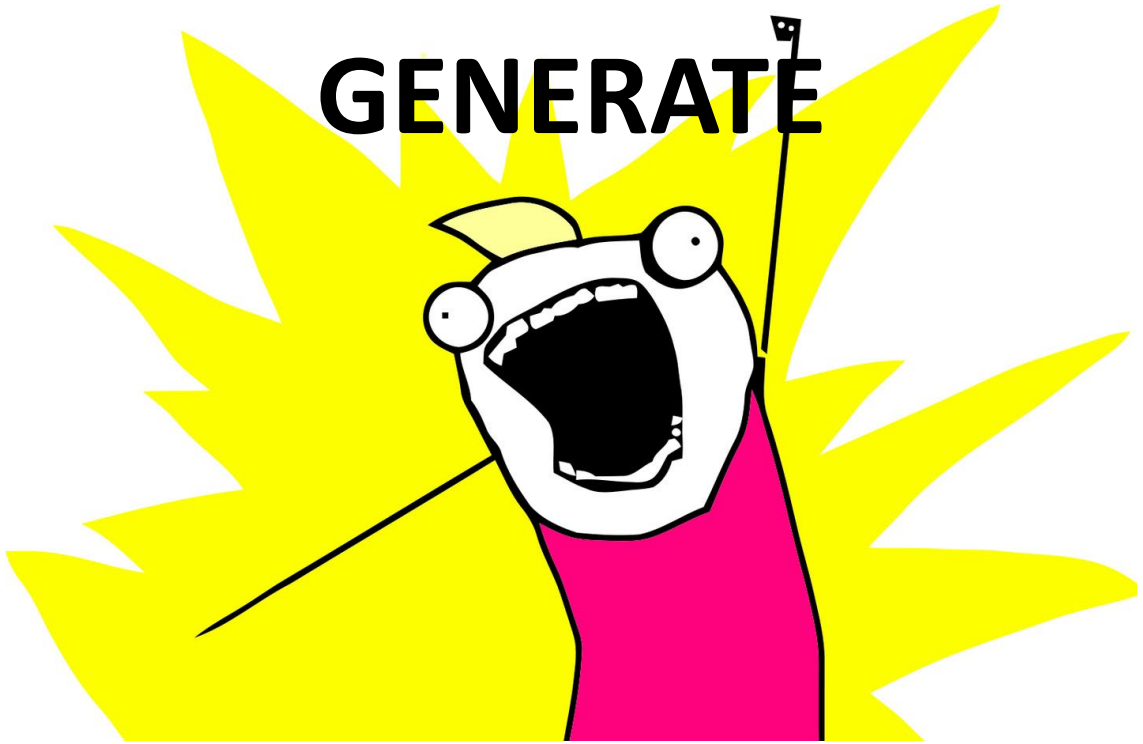
WHO ARE YOUR CUSTOMERS?

Building A Collection Management Framework

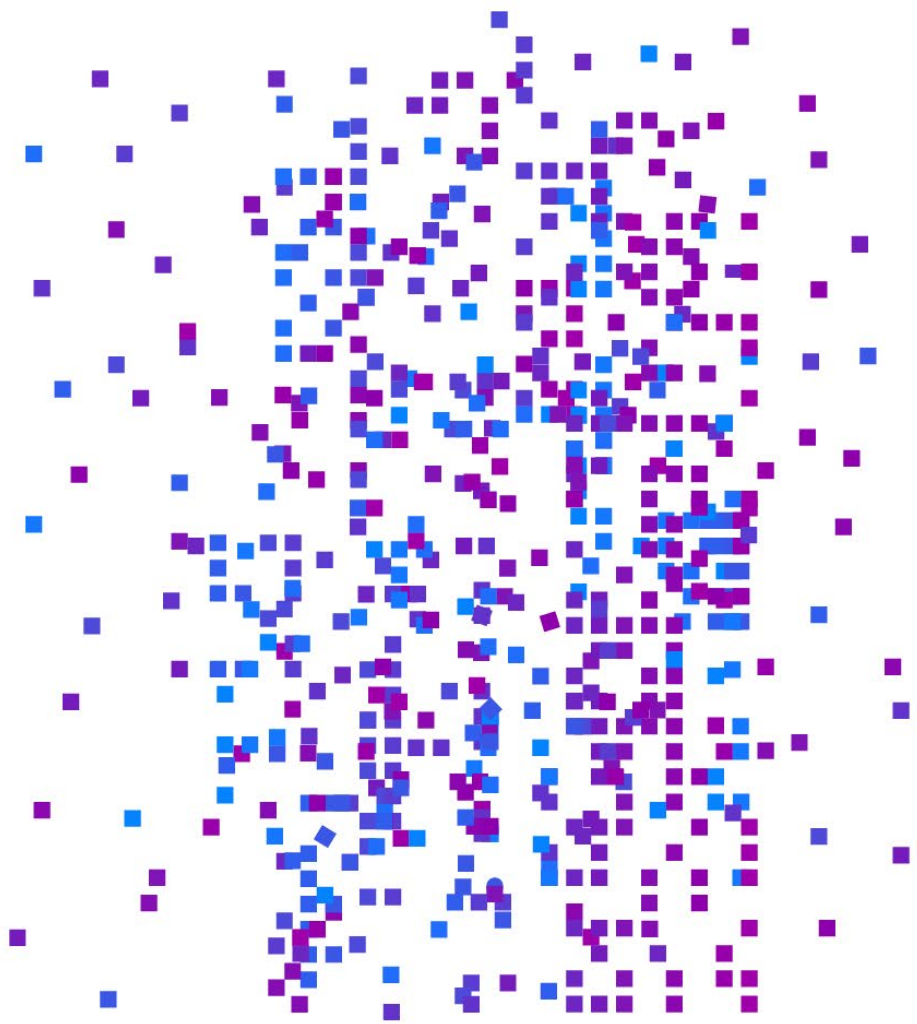
External

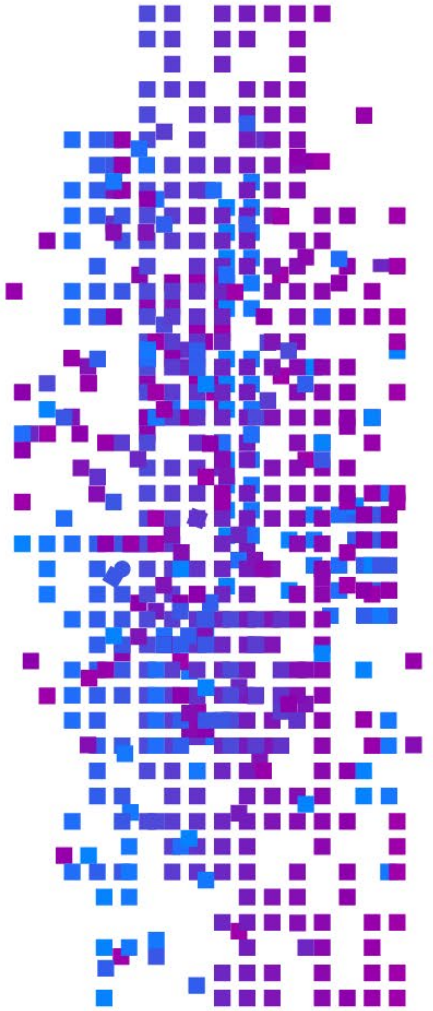
- Governments
- FS-ISAC
- Commercial
- Fight clubs

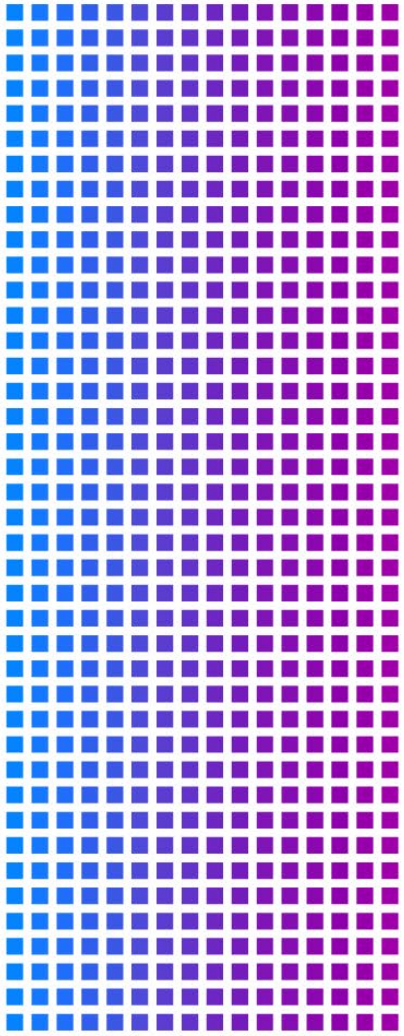
Internal



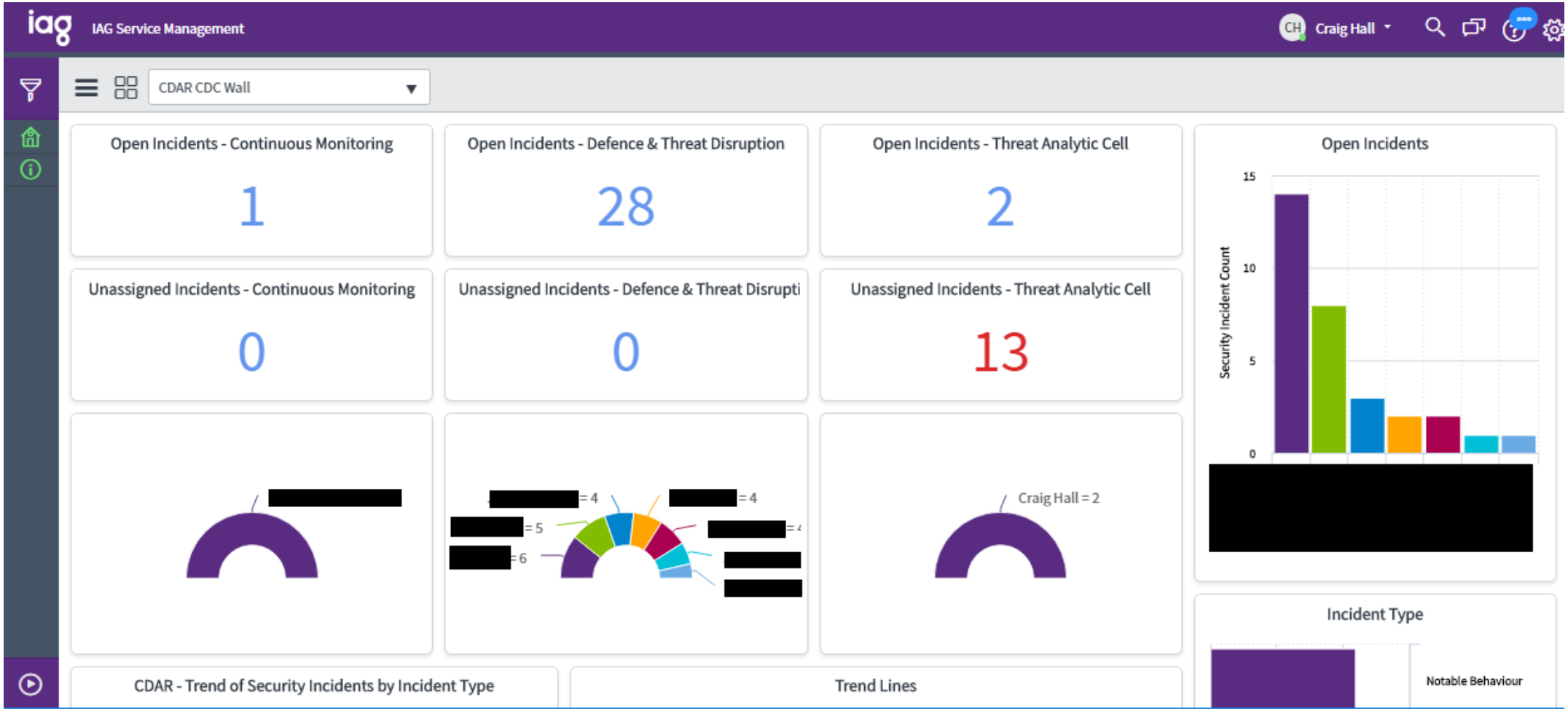
Manipulation of data



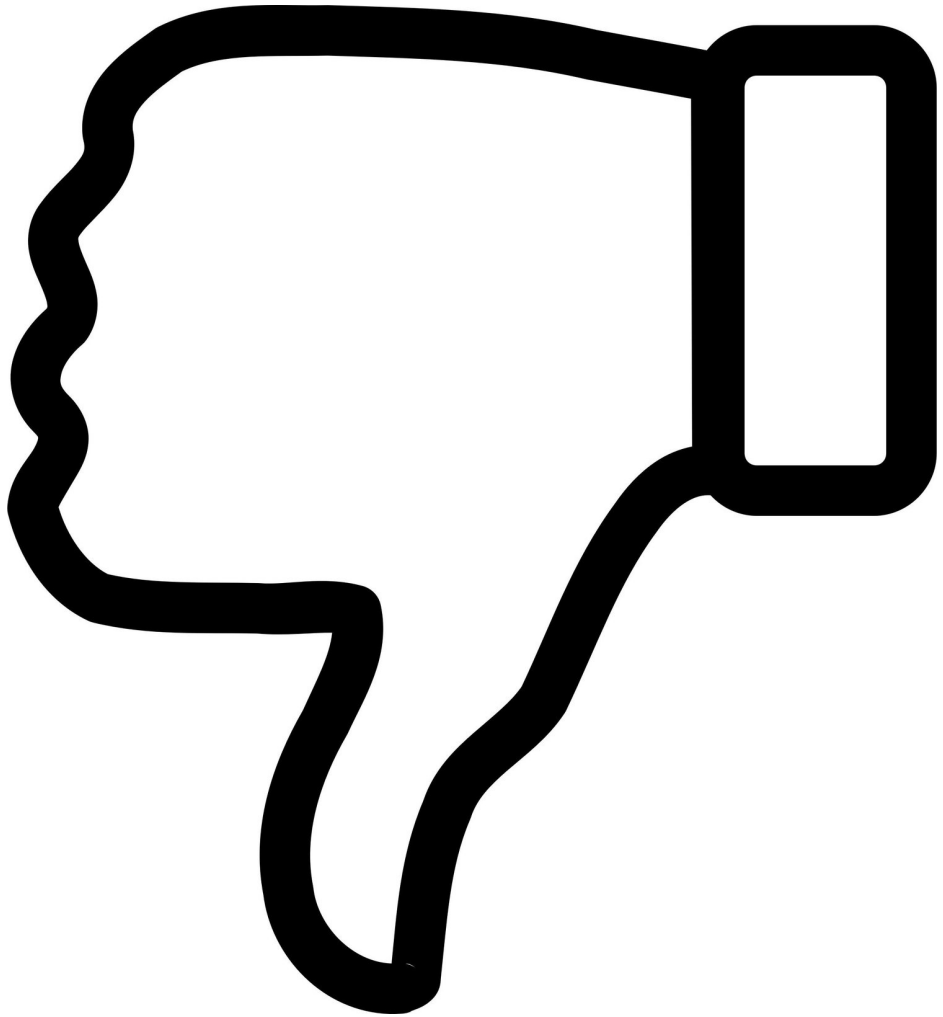




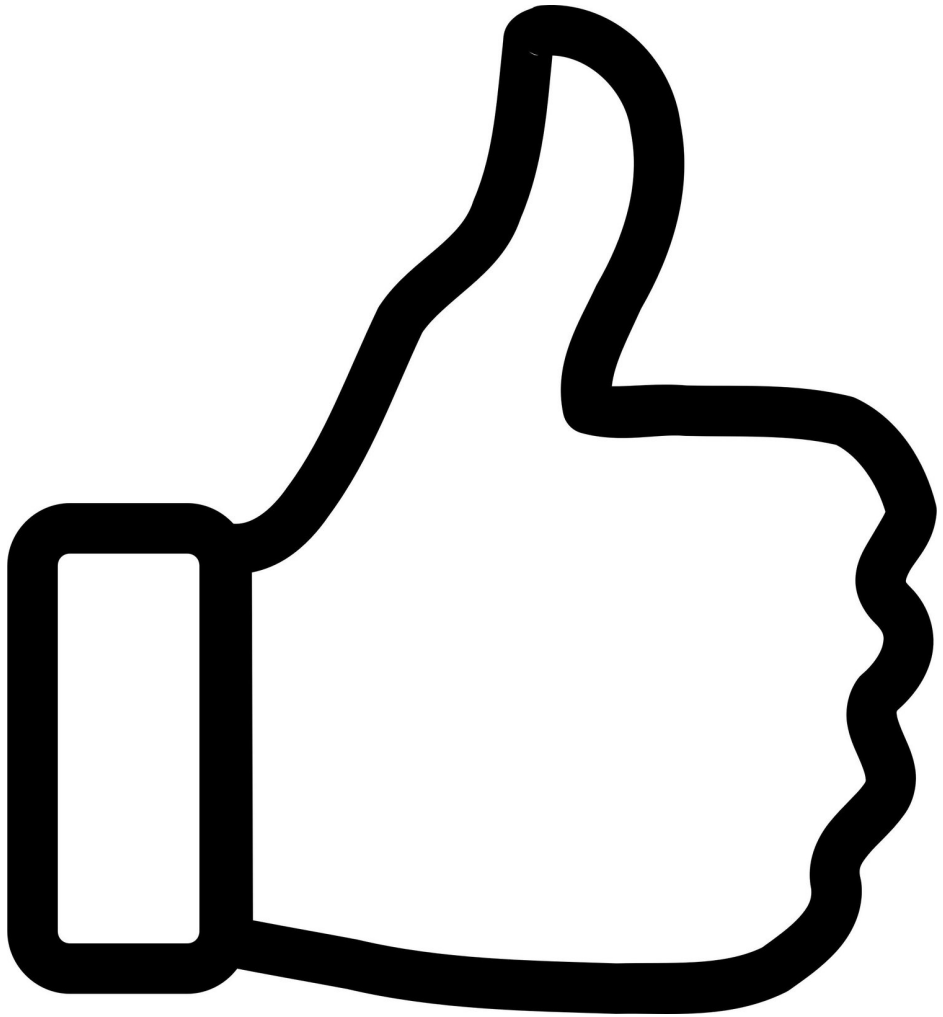
Acting on it


IAG Service Management
Craig Hall
CDAR CDC Wall
Open Incidents - Continuous Monitoring
1
Open Incidents - Defence & Threat Disruption
28
Open Incidents - Threat Analytic Cell
2
Unassigned Incidents - Continuous Monitoring
0
Unassigned Incidents - Defence & Threat Disrupti
0
Unassigned Incidents - Threat Analytic Cell
13
Craig Hall = 2
Open Incidents
Security Incident Count
15
10
5
0
Incident Type
Notable Behaviour
CDAR - Trend of Security Incidents by Incident Type
Trend Lines

What is still not going well



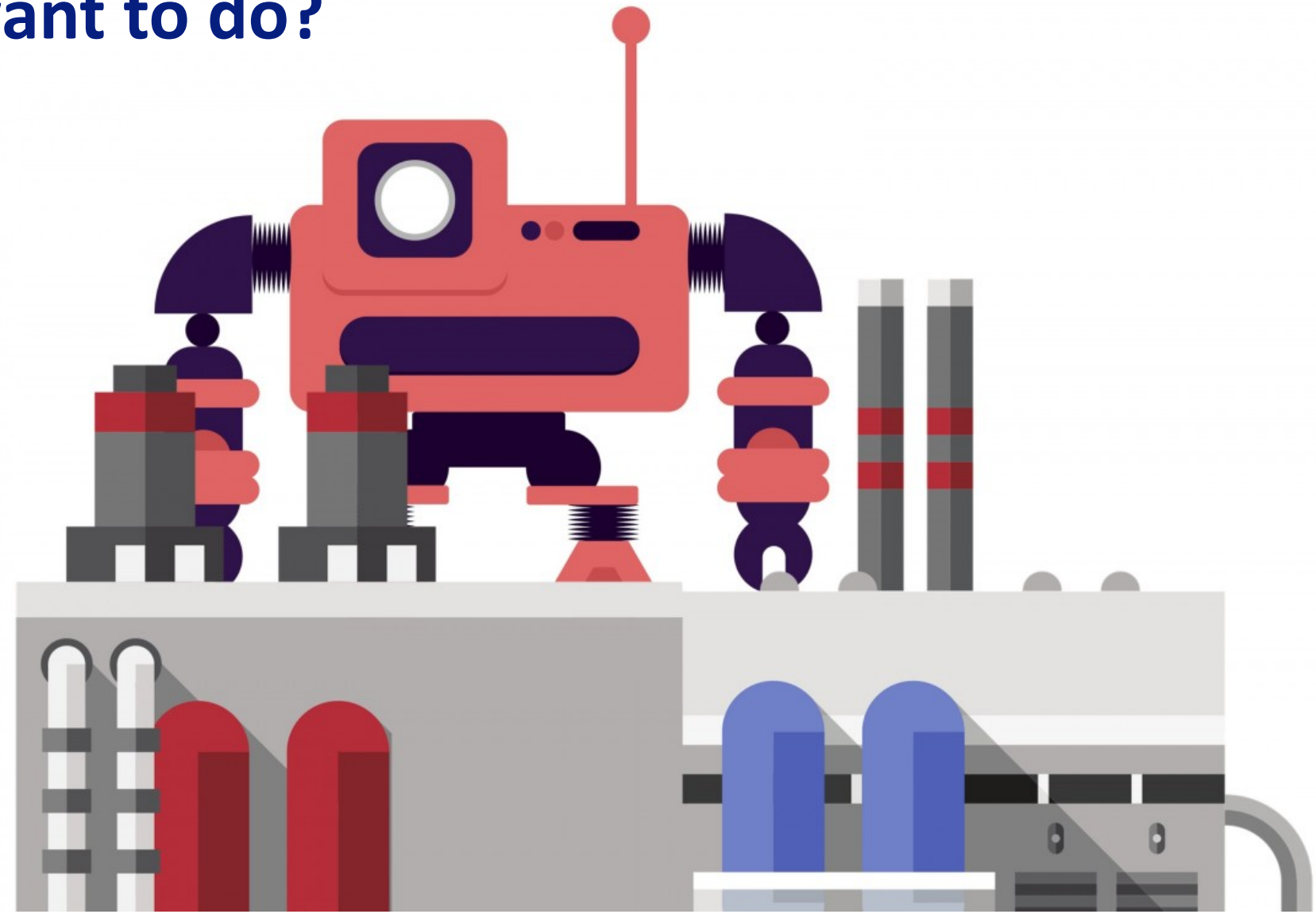
What is going well



RSAConference2019
Asia Pacific & Japan

Future

What I want to do?



What I want you to do?

- Recognize that threat intel isn't too hard for you
- Appreciate that threat intel makes life hard for the attackers
- Use TI to solve problems

RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

SESSION ID: AIR-R03

Practical Implementations of a Threat Intelligence Program

Craig Hall

Manager, Threat Analytic Cell
IAG