RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **SEM-M03K**

Prioritizing Threats: What Would Threat Researchers Do (WWTRD)

MODERATOR: **A.J. Nash**
Director, Cyber Intelligence Strategy
Anomali
linkedin.com/in/nashaj/

PANELISTS:

Tim Gallo
Solutions Architect, Intelligence & Services
FireEye
linkedin.com/in/timjgallo/

Chris Cochran
Threat Intelligence & Operations Lead
Netflix
linkedin.com/in/chriscochrancyber/

Jon DiMaggio
Sr. Threat Intelligence Analyst
Symantec
linkedin.com/in/jondimaggio/

#RSAC

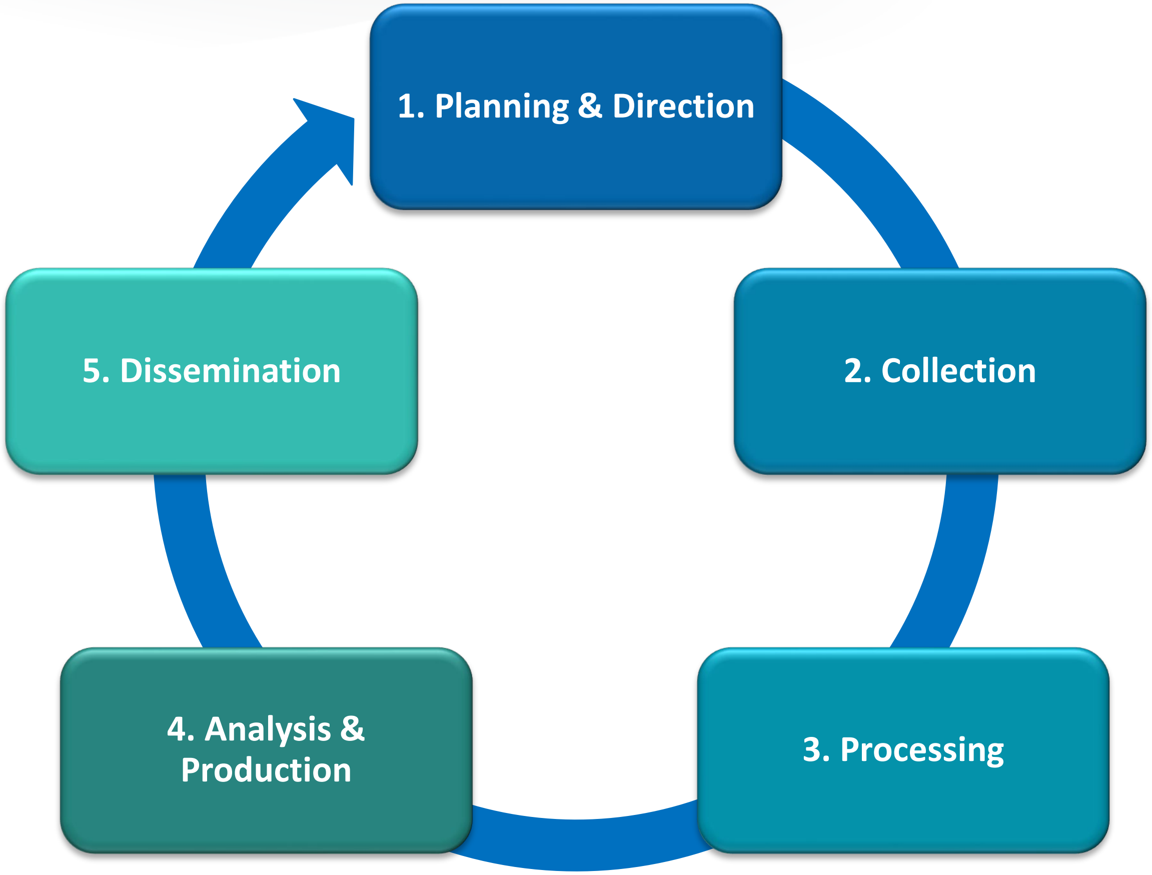
RSA®Conference2020

Building Intelligence Programs

A high-level look at how we do what we do

Building Intelligence Programs

- **Planning and Direction**
  - Stakeholders
  - Intelligence Requirements
- **Collection**
  - Collection Plan
  - Vendor Selection
- **Processing**
  - Technology-Powered
- **Analysis and Production**
  - Tradecraft and Standards
- **Dissemination**
  - Formats and Process



Challenges Facing Researchers and Hunters

It’s a tough job but somebody has to do it

Challenges Facing Researchers and Hunters

- Evolution of Adversaries
  - Malicious activity vs. motivations
- Changing Tools and Mindsets of Researchers/Hunters
- Attribution & Group Tracking
  - What are criteria?

RSAConference2020

APT 41 / GREF Case Study

How does this work in the real world?

Apt 41/GREF Case Study

- APT 41 Overview
  - Chinese espionage activity in parallel with financially motivated operations
- Symantec
- FireEye
- Impact to Customers

Apply What You Have Learned Today

- You should be able to:
  - Assess how well your intelligence organization is aligned with the Intelligence Cycle
  - Understand the challenges and pitfalls of attribution
  - Recognize there is more than one way to approach assessments
  - Critically examine vendor conclusions for overstatement or logical fallacies

RSA®Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID:

SEM-M03K - Prioritizing Threats: What Would Threat Researchers Do (WWTRD)

MODERATOR: **A.J. Nash**
Director, Cyber Intelligence Strategy
Anomali
linkedin.com/in/nashaj/

PANELISTS:

Tim Gallo
Solutions Architect, Intelligence & Services
FireEye
linkedin.com/in/timjgallo/

Chris Cochran
Threat Intelligence & Operations Lead
Netflix
linkedin.com/in/chriscochrancyber/

Jon DiMaggio
Sr. Threat Intelligence Analyst
Symantec
linkedin.com/in/jondimaggio/

#RSAC