RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: HUM-W01

Be Like Water: Applying Analytical Adaptability to Cyber Intelligence

Jay McAllister

Senior Analyst
Software Engineering Institute – Carnegie Mellon University
@sei_etc

Scuttlebutt Communications

- Sells prefabricated secure meeting spaces

Company Profile

- Privately owned
- 600 employees
- Consists of two divisions
  - Products
  - Operations
    - Cyber intelligence

Scuttlebutt

A new way to meet

Cyber Intelligence Mission

- Acquire and analyze information to identify, track, and predict cyber capabilities, intentions, and activities in ways that offer courses of action to enhance decision making

Scuttlebutt

10100010010100010 Cyber

Ways to Offer Courses of Action

- Attack Alerts
- Daily Threat Summaries
- Emerging Threats Newsletters
- Threat Assessments
- After Action Reports
- Situational Awareness Briefings

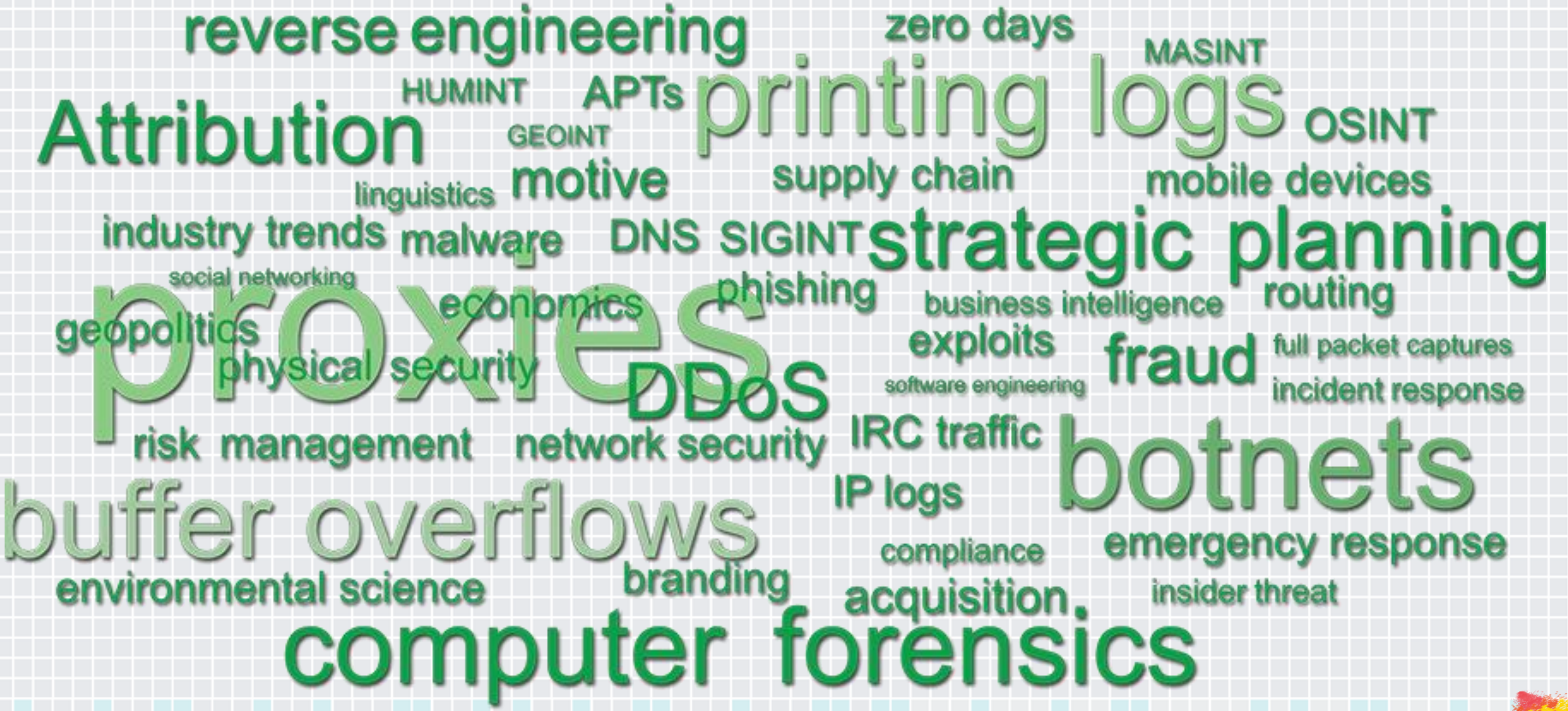
Analyst Cadre

IT professional

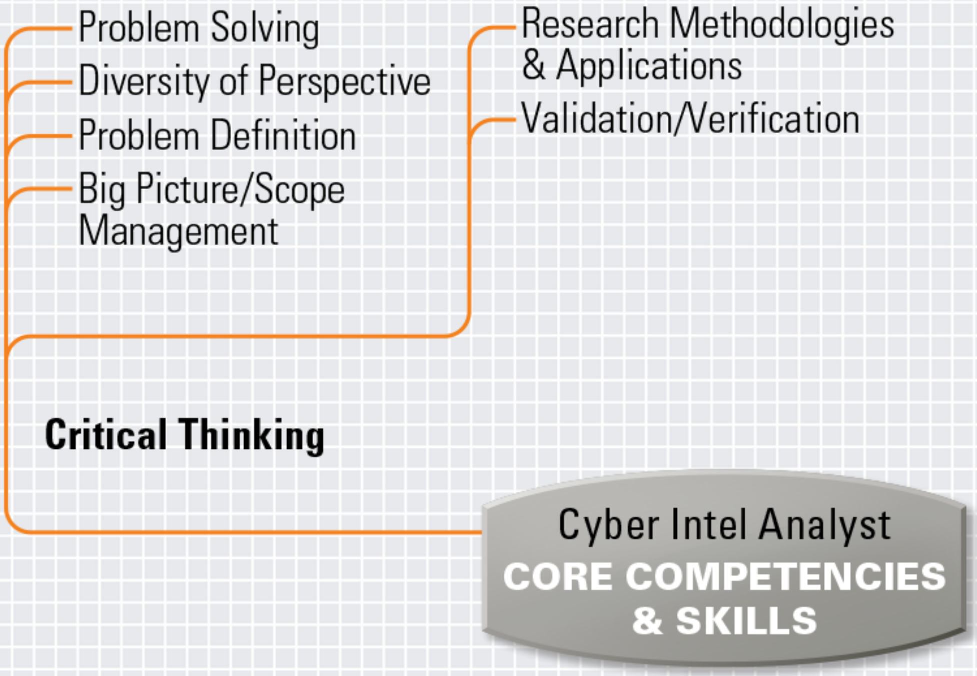
Retired military communications officer

Liberal arts graduate

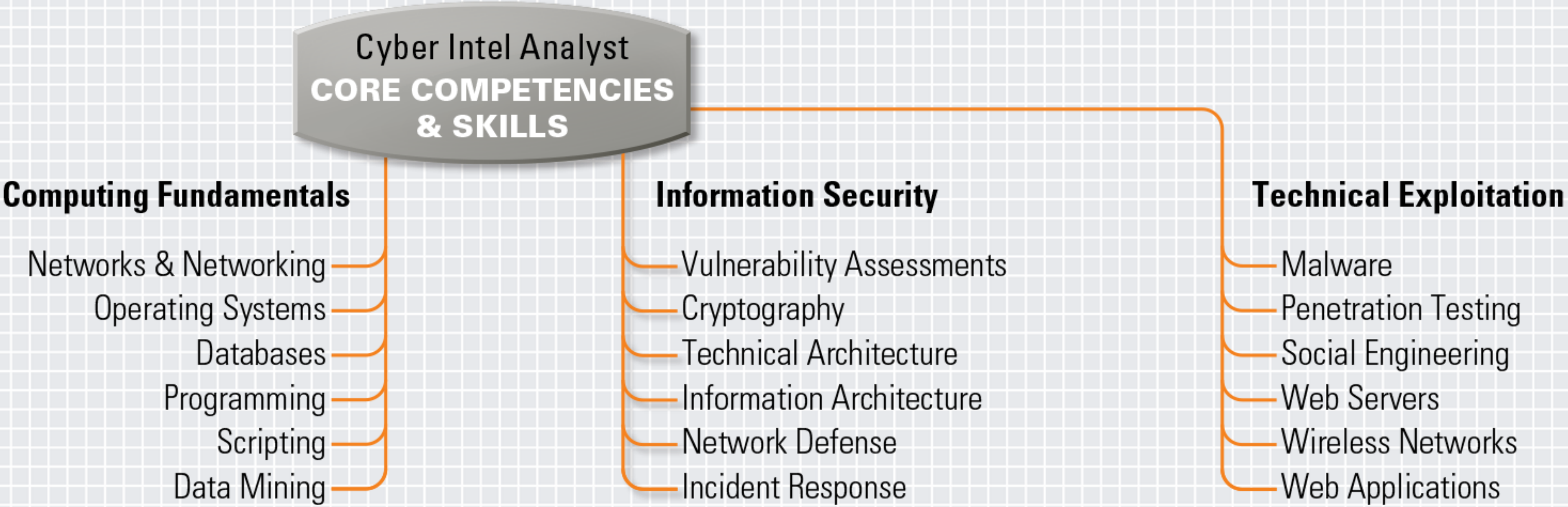
Analyst Responsibilities



Stress Critical Thinking



Fight Stress with Tools and Providers



Cyber Intel Analyst
CORE COMPETENCIES & SKILLS

Computing Fundamentals

- Networks & Networking
- Operating Systems
- Databases
- Programming
- Scripting
- Data Mining

Information Security

- Vulnerability Assessments
- Cryptography
- Technical Architecture
- Information Architecture
- Network Defense
- Incident Response

Technical Exploitation

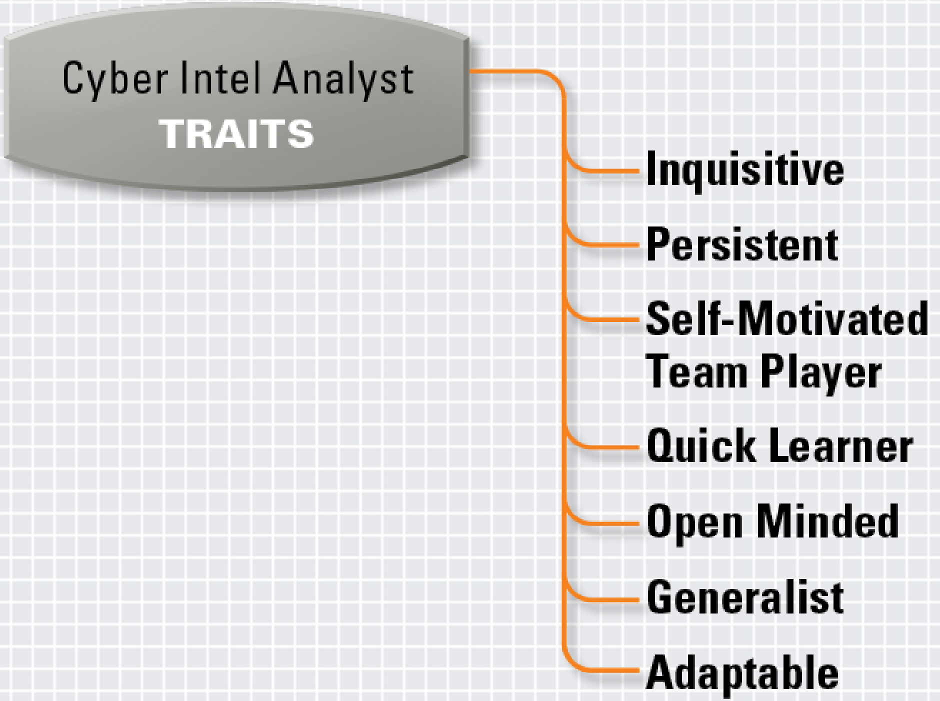
- Malware
- Penetration Testing
- Social Engineering
- Web Servers
- Wireless Networks
- Web Applications

Software Engineering Institute

- Federally funded research and development center
- Located at Carnegie Mellon University

Fight Stress with Analytical Brainpower

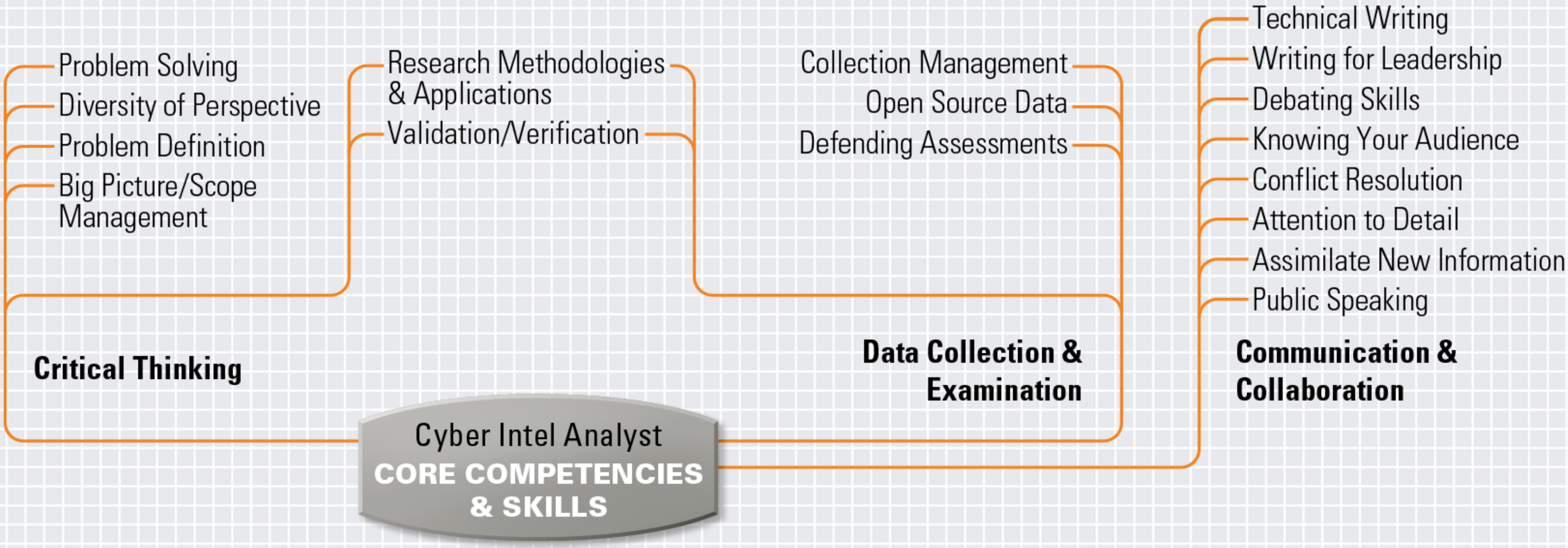
- Acquire talent with certain traits



Cyber Intel Analyst
TRAITS

- Inquisitive
- Persistent
- Self-Motivated Team Player
- Quick Learner
- Open Minded
- Generalist
- Adaptable

Fight Stress with Analytical Brainpower



Cyber Intel Analyst

CORE COMPETENCIES & SKILLS

Critical Thinking

- Problem Solving
- Diversity of Perspective
- Problem Definition
- Big Picture/Scope Management
- Research Methodologies & Applications
- Validation/Verification

Data Collection & Examination

- Collection Management
- Open Source Data
- Defending Assessments

Communication & Collaboration

- Technical Writing
- Writing for Leadership
- Debating Skills
- Knowing Your Audience
- Conflict Resolution
- Attention to Detail
- Assimilate New Information
- Public Speaking

Be Like Water

Cyber Intelligence Research Collaborators

Federal Government

- Intelligence Community
- Military
- Federal Civil Service

Industry

- Defense Contracting
- Energy
- Financial Services
- Healthcare
- Higher Education
- Information Technology
- Intelligence as a service
- Law
- Retail

Cyber Intelligence Research Endeavors

- Research Consortium
- Graduate Course
- Tradecraft Project

Emerging Technology Center

ini Carnegie Mellon University Information Networking Institute

RSAConference2015

San Francisco | April 20-24 | Moscone Center

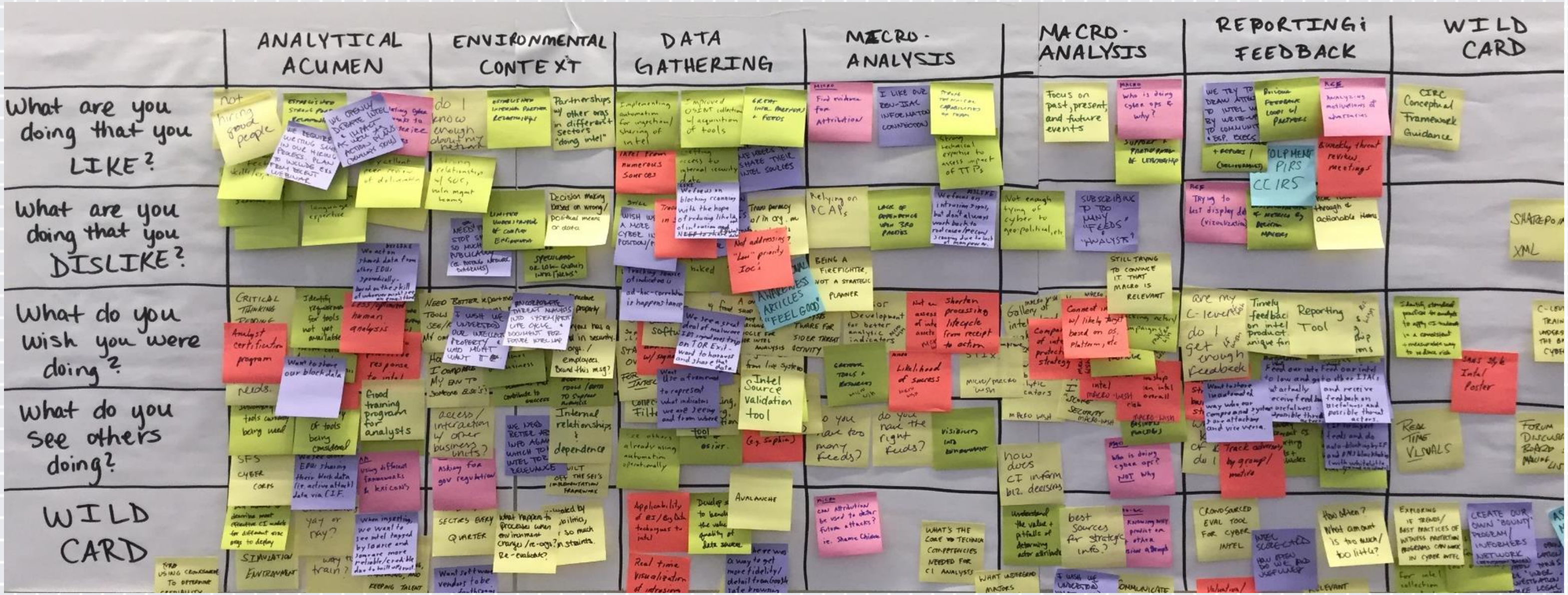
Leveraging Creative Brainstorming

#RSAC

Human-Centered Design

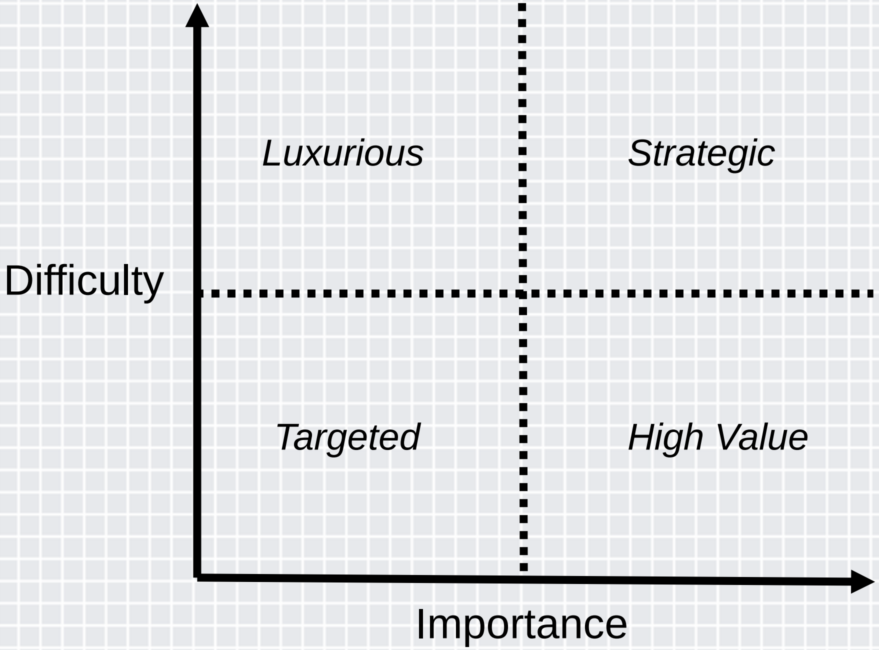
Creative Matrix

- Over 200 responses generated in ~30 minutes

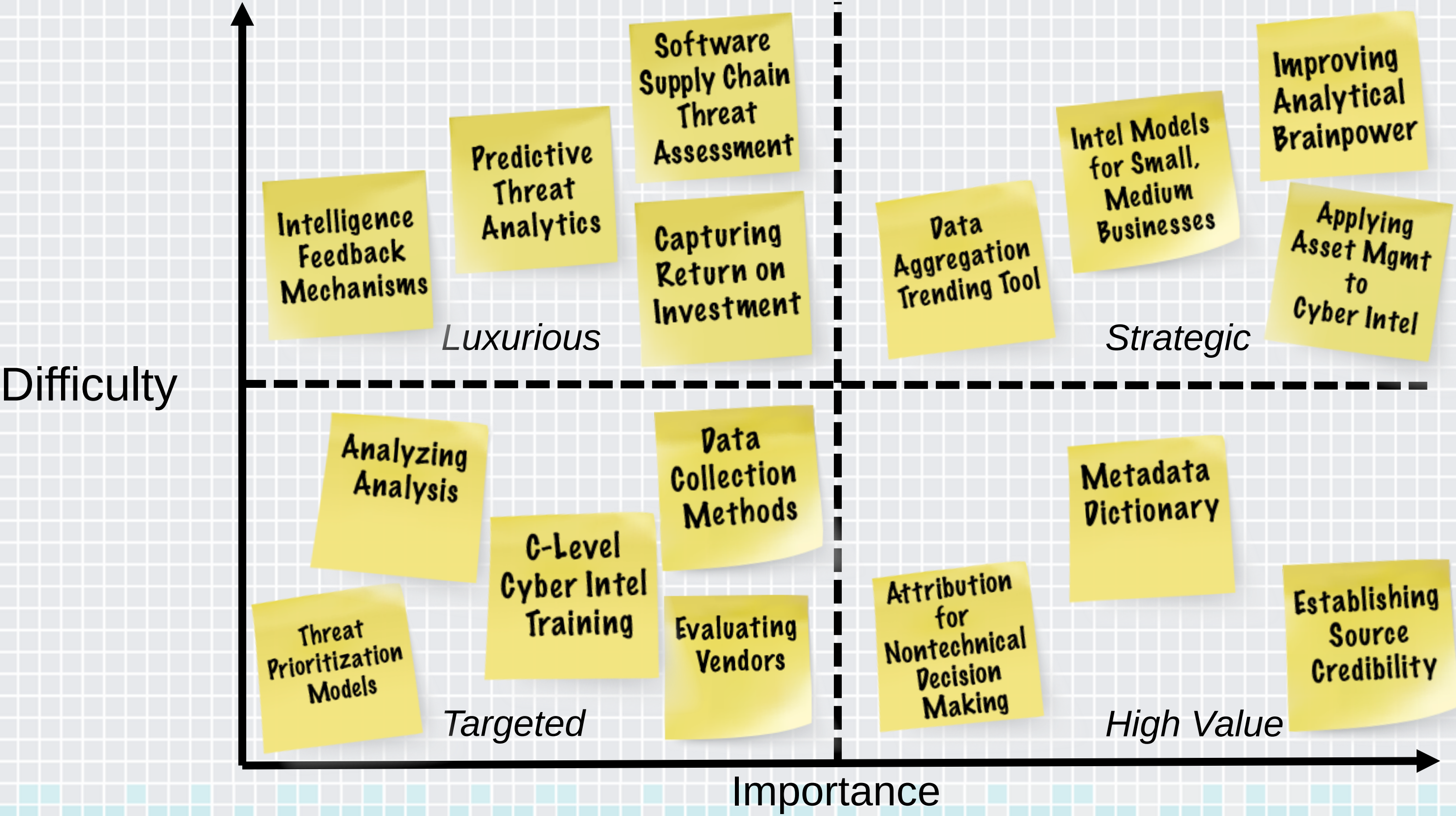

ANALYTICAL ACUMEN
ENVIRONMENTAL CONTEXT
DATA GATHERING
MICRO-ANALYSIS
MACRO-ANALYSIS
REPORTING & FEEDBACK
WILD CARD
What are you doing that you LIKE?
What are you doing that you DISLIKE?
What do you wish you were doing?
What do you see others doing?
WILD CARD

Importance and Difficulty Matrix

- Weighs importance versus cost to identify challenges with the greatest potential



Resulting Challenges



Luxurious

- Intelligence Feedback Mechanisms
- Predictive Threat Analytics
- Software Supply Chain Threat Assessment
- Capturing Return on Investment

Strategic

- Data Aggregation Trending Tool
- Intel Models for Small, Medium Businesses
- Improving Analytical Brainpower
- Applying Asset Mgmt to Cyber Intel

Targeted

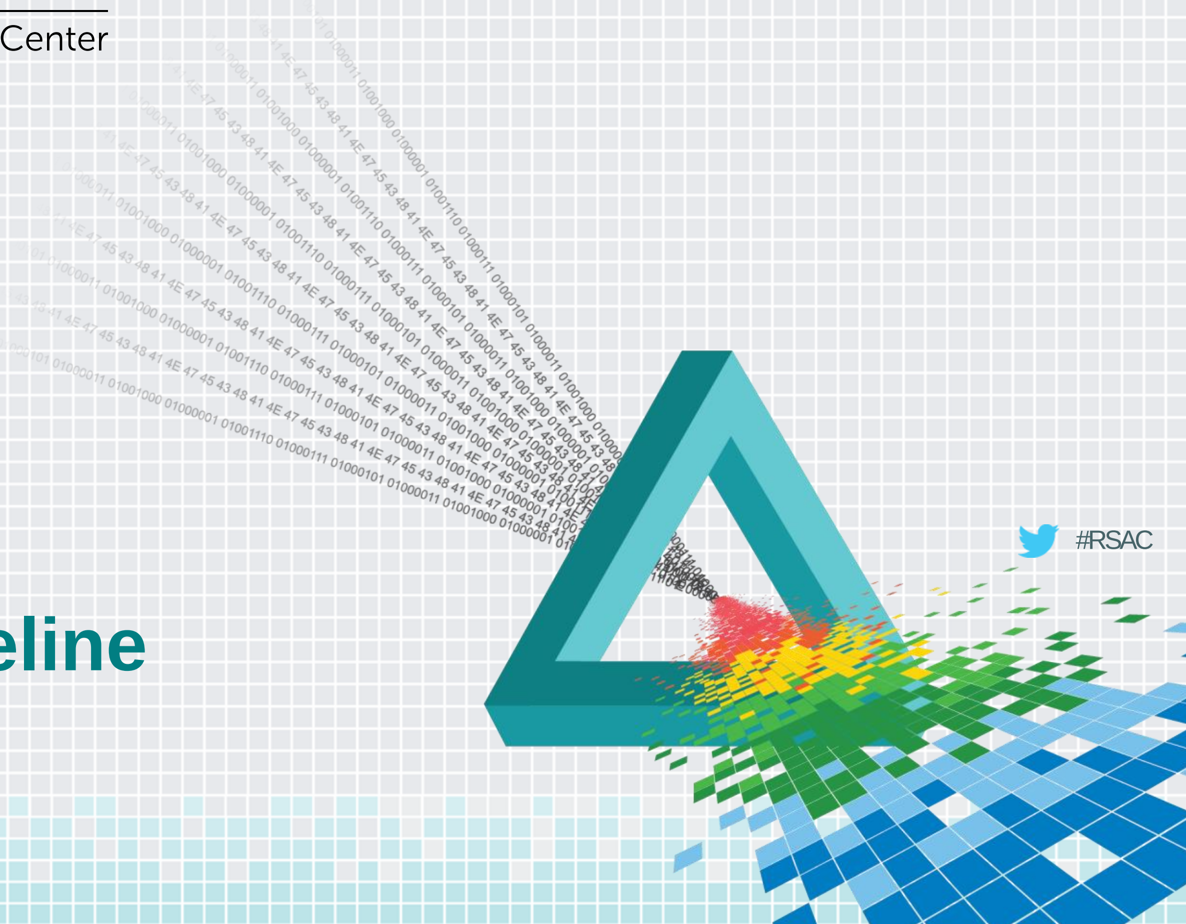
- Analyzing Analysis
- Data Collection Methods
- C-Level Cyber Intel Training
- Threat Prioritization Models
- Evaluating Vendors

High Value

- Metadata Dictionary
- Attribution for Nontechnical Decision Making
- Establishing Source Credibility

RSAConference2015

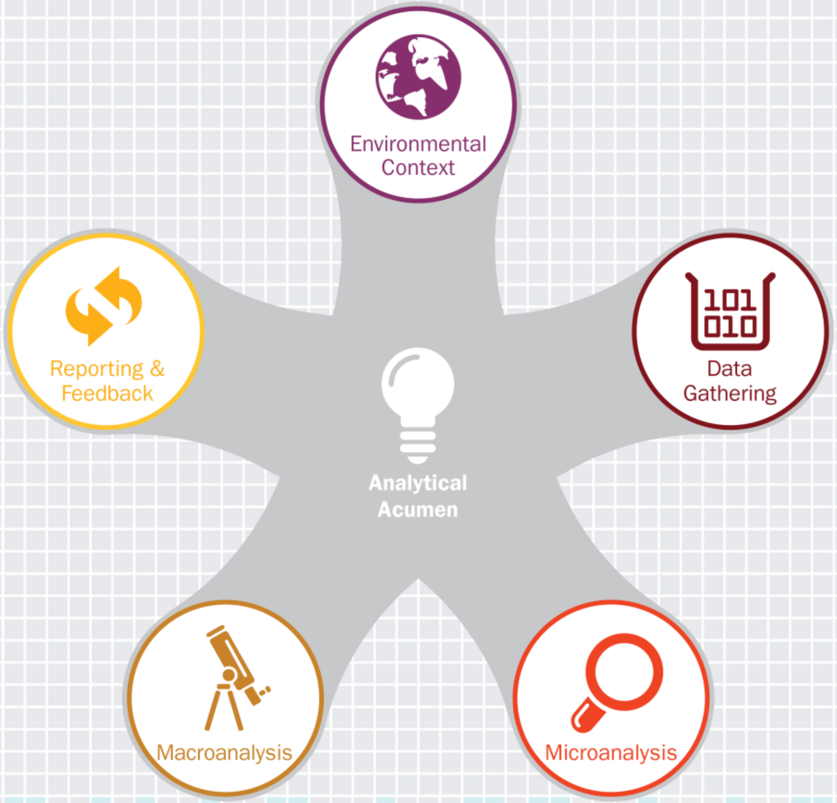
San Francisco | April 20-24 | Moscone Center



#RSAC

Establishing a Cyber Threat Baseline

The Analytic Framework



Framework Components

Analytical Acumen

- Facilitates timely, actionable, & accurate intelligence
  - Is an art and a science

Environmental Context

- Provides scope for analysis
  - Focuses on internal/external network and operations

Framework Components

Data Gathering

- Acquires and aligns data for analysis
  - Ask the right questions to get the right data

Microanalysis

- Assesses functional implications
  - Answers what and how

Framework Components

Macroanalysis

- Assesses strategic implications
  - Answers who and why

Reporting & Feedback

- Offers courses of action to enhance decision making
  - Reporting only as effective as its feedback counterpart

Component Attributes

Advancement

Background

Training

Impact

Partnerships

Threat Prioritization

Workflow

Establishing Source Credibility

Queen/king For A Day

Assigning Attribution

Organizational Chart

Evaluations

Roadblocks

Crisis Management

Supply Chain

Operational Resource Allocation

Timing

Information Collection Management

Information Sharing

Data Processing

Evaluating Vendors

Analytical Offerings

Intelligence Consumers

Security Analytics

Evaluations

Cyber Footprint

Tools

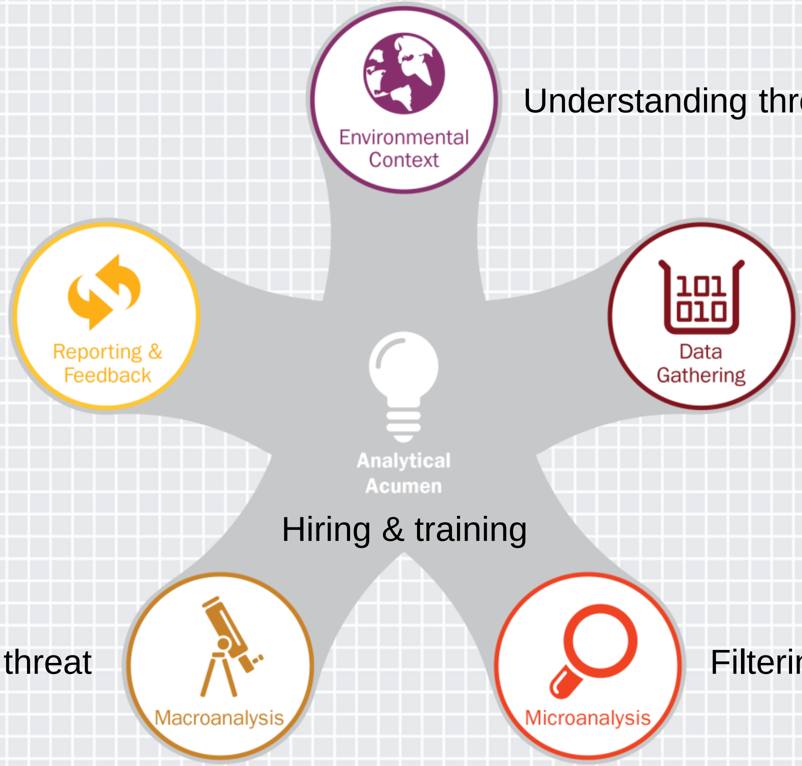
Reactive/proactive/predictive Analysis

Return On Investment

Data Integration

Feedback Mechanisms

Resulting Cyber Threat Baseline



Understanding threats to software supply chain

Capturing return on investment

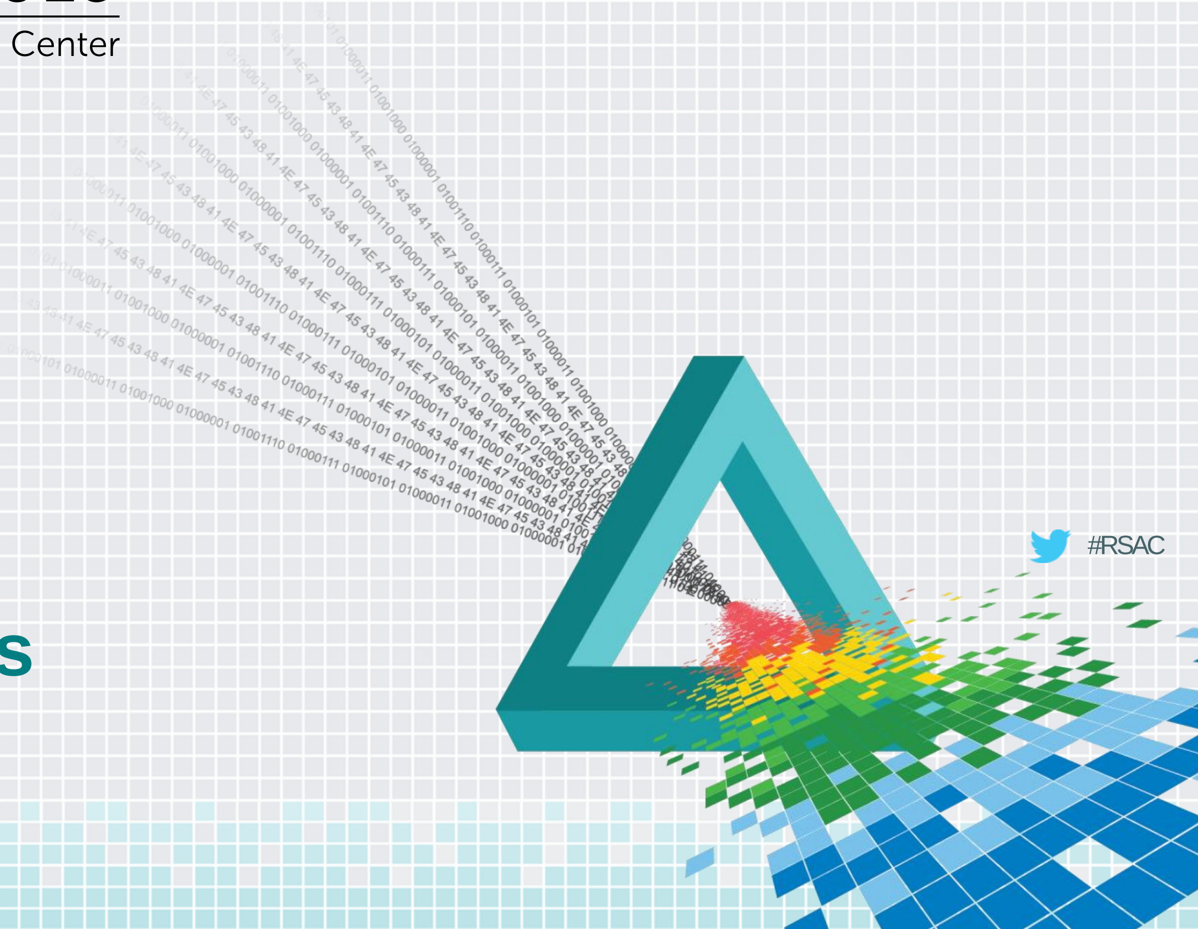
Tool acquisition and use

Hiring & training

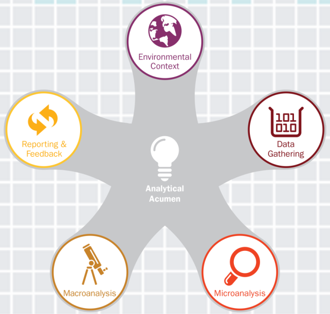
Holistically assessing a threat

Filtering critical threats from data

Holistically Assessing Threats



Three-Step Approach



- Establish a cyber threat baseline

- Leverage creative brainstorming whenever possible

- Assess threat actor potential, organizational impact, and target exposure

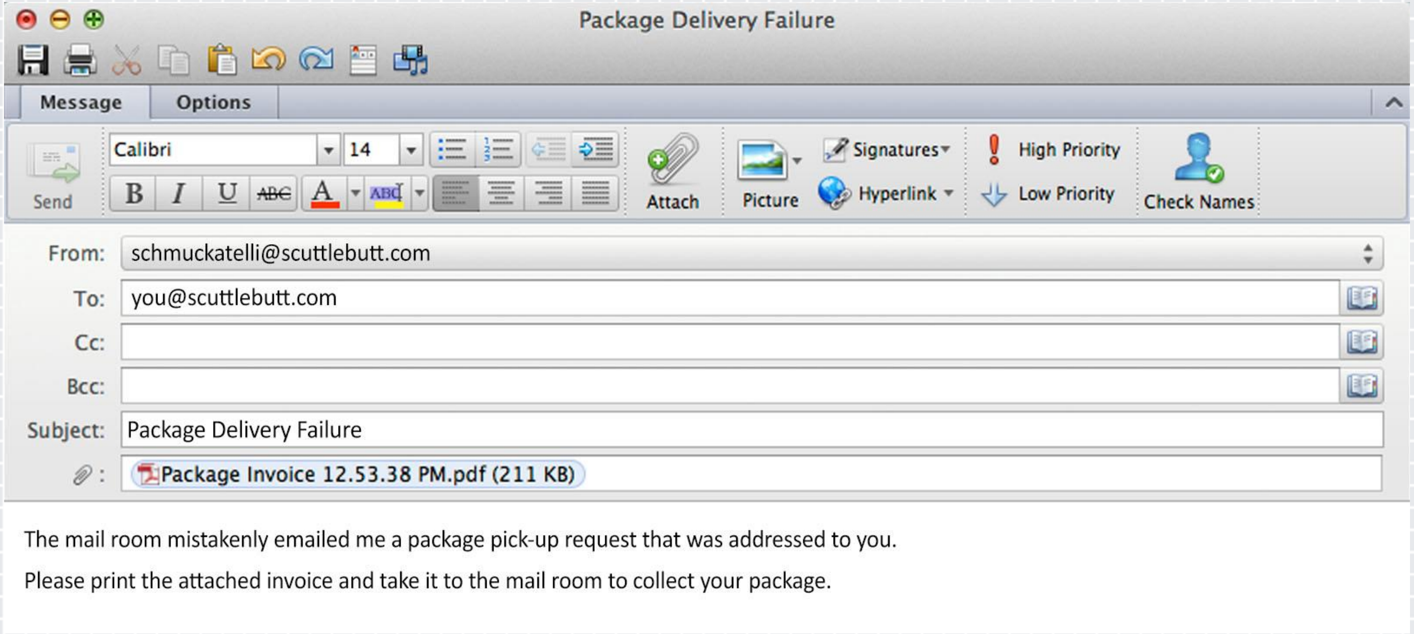
Scuttlebutt
A new way to meet

Scuttlebutt Communications

- Refresher
  - Sells prefabricated secure meeting spaces
  - Privately owned company with 600 employees
  - Perform cyber intelligence

Scuttlebutt
10100010010100010 Cyber

Example – You Receive this Email



From: schmuckatelli@scuttlebutt.com

To: you@scuttlebutt.com

Cc:

Bcc:

Subject: Package Delivery Failure

: Package Invoice 12.53.38 PM.pdf (211 KB)

The mail room mistakenly emailed me a package pick-up request that was addressed to you.

Please print the attached invoice and take it to the mail room to collect your package.

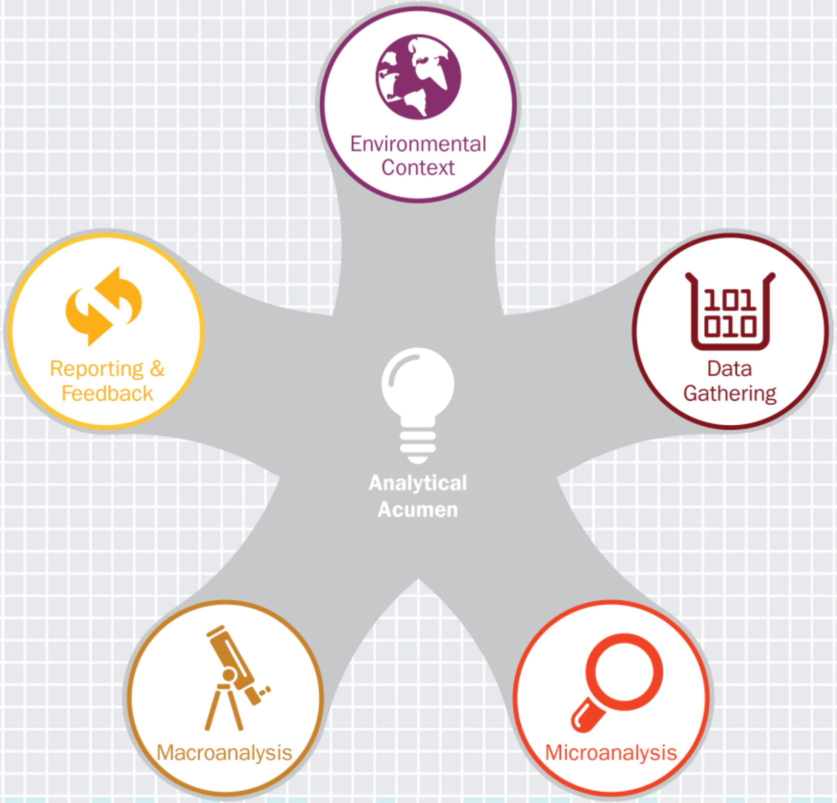
What's going on here?
Text
JAYMCALLISTE350 to 37607

Assessing the Situation

- Three-step approach
  - Establish a cyber threat baseline
  - Leverage creative brainstorming whenever possible
  - Assess threat actor potential, organizational impact, and target exposure

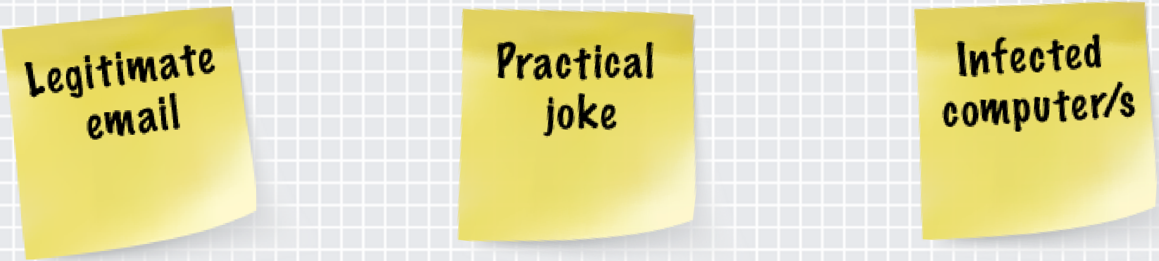
What's going on here?
Text
JAYMCALLISTE350 to 37607

Establish a Cyber Threat Baseline



Analytical Acumen

- Leverage creative brainstorming
  - Affinity clustering - Sorting items by similarity
- Possible email explanations



What's going on here?
Text
JAYMCALLISTE350 to 37607

Environmental Context

- Establish scope
  - Talk to the mail room and Jack
    - Mail room didn't do it
    - Jack didn't do it

Data Gathering

- Ask the right questions to get the right data

Is Jack's computer infected?

How did it happen?

Who did it?

If so, with what?

Why did it happen?

Where has it spread to?

What data should we collect?
Text
JAYMCALLISTE350 to 37607

Data Gathering

- Collect information

Computer scans, download and web activity

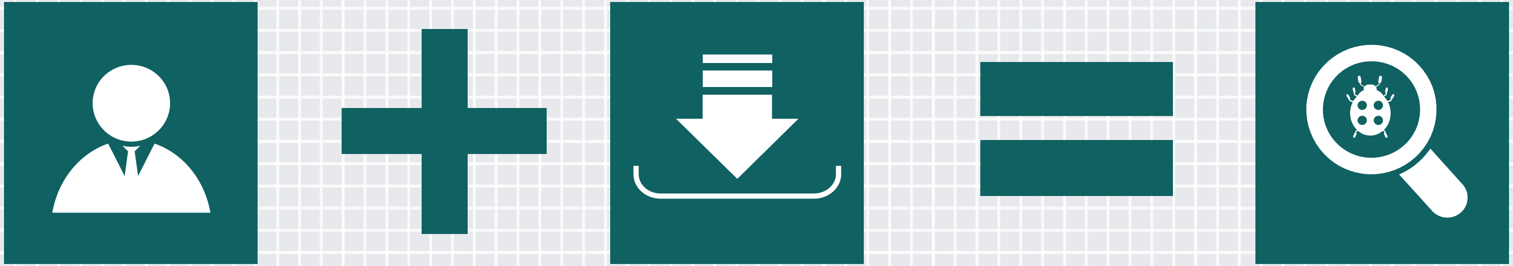
TTPs of threat actors known to target the industry

Recent activities of a criminal organization

What data should we collect?
Text
JAYMCALLISTE350 to 37607

Microanalysis

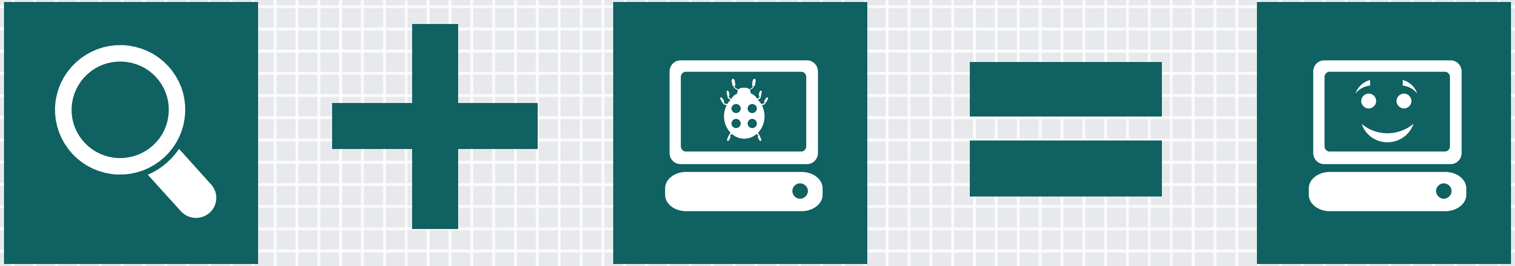
- Answer what and how



How can we remediate the problem?
Text
JAYMCALLISTE350 to 37607

Microanalysis

- Support network defense, cybersecurity, and incident response



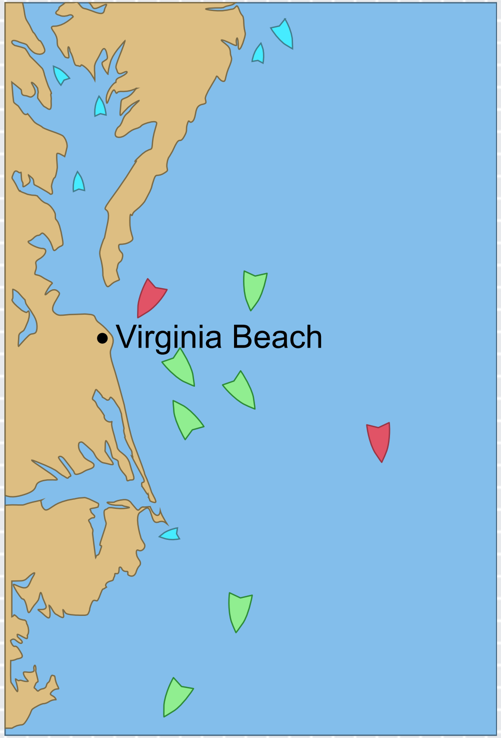
How can we remediate the problem?
Text
JAYMCALLISTE350 to 37607

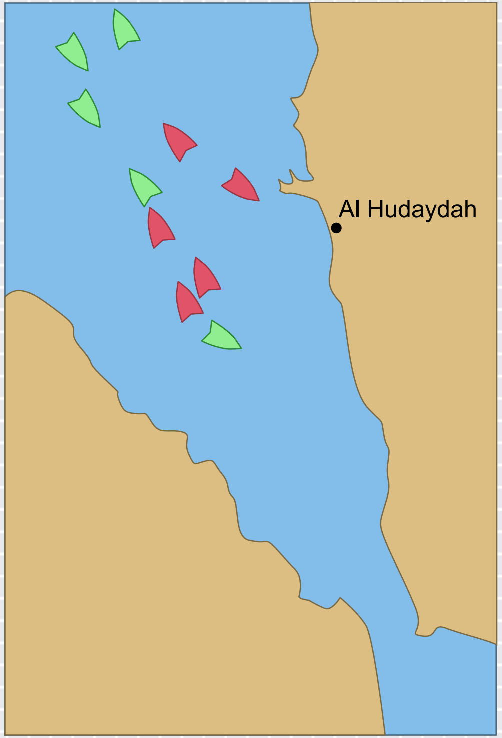
Macroanalysis

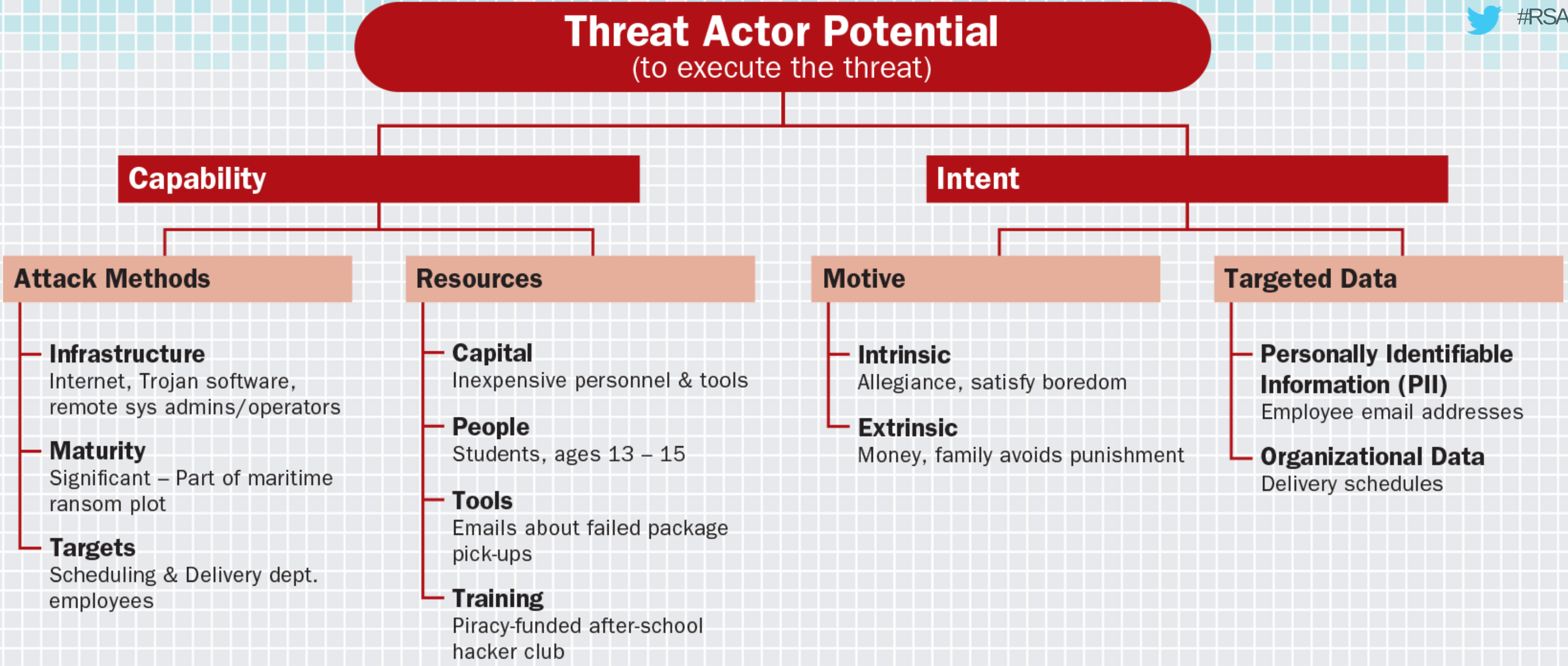
- Assess threat actor potential, organizational impact, and target exposure

What can Scuttlebutt do so the Trojan doesn’t affect the nation-state?
Text JAYMCALLISTE350 to 37607

Scuttlebutt Real-Time Order Tracking







Threat Actor Potential

(to execute the threat)

Capability

Attack Methods

- **Infrastructure**
  Internet, Trojan software, remote sys admins/operators
- **Maturity**
  Significant – Part of maritime ransom plot
- **Targets**
  Scheduling & Delivery dept. employees

Resources

- **Capital**
  Inexpensive personnel & tools
- **People**
  Students, ages 13 – 15
- **Tools**
  Emails about failed package pick-ups
- **Training**
  Piracy-funded after-school hacker club

Intent

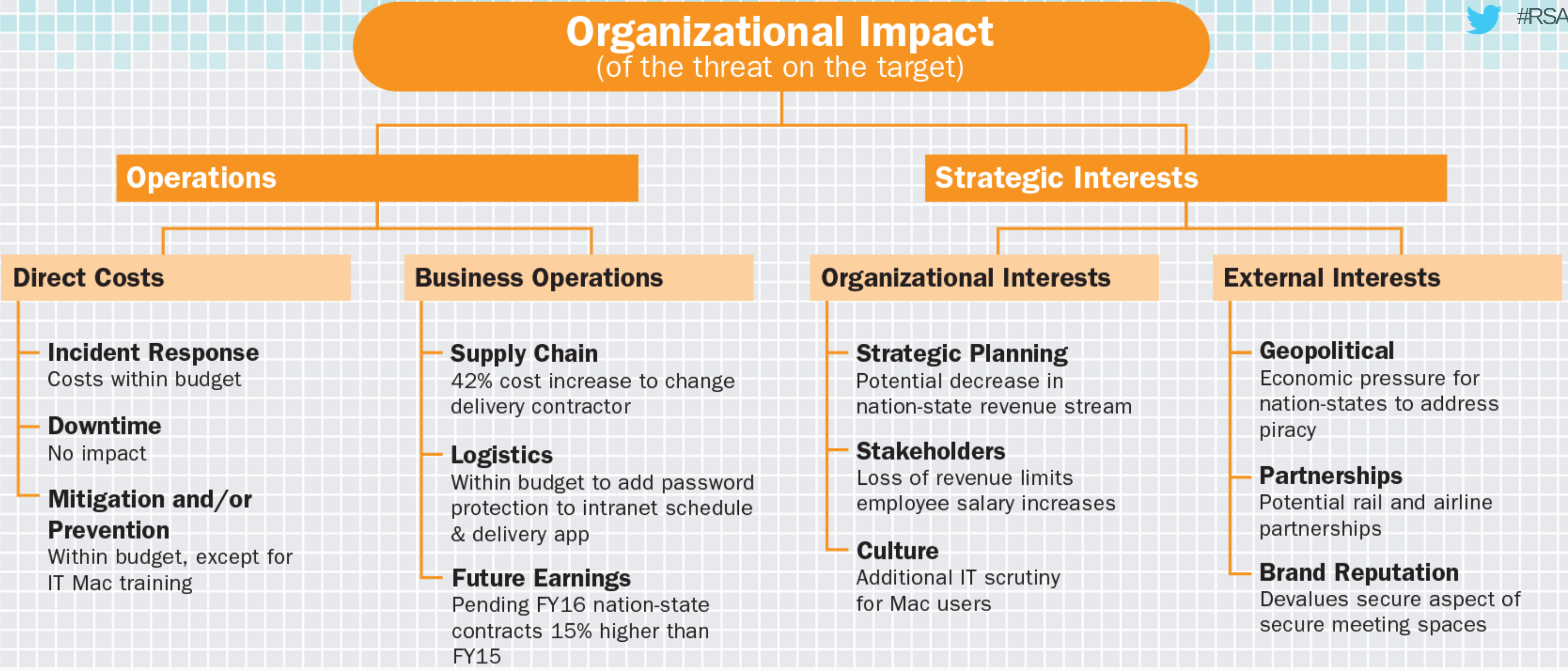
Motive

- **Intrinsic**
  Allegiance, satisfy boredom
- **Extrinsic**
  Money, family avoids punishment

Targeted Data

- **Personally Identifiable Information (PII)**
  Employee email addresses
- **Organizational Data**
  Delivery schedules

What can Scuttlebutt do so the Trojan doesn't affect the nation-state?
Text JAYMCALLISTE350 to 37607



Organizational Impact
(of the threat on the target)

Operations

Direct Costs

Incident Response
Costs within budget

Downtime
No impact

Mitigation and/or Prevention
Within budget, except for IT Mac training

Business Operations

Supply Chain
42% cost increase to change delivery contractor

Logistics
Within budget to add password protection to intranet schedule & delivery app

Future Earnings
Pending FY16 nation-state contracts 15% higher than FY15

Strategic Interests

Organizational Interests

Strategic Planning
Potential decrease in nation-state revenue stream

Stakeholders
Loss of revenue limits employee salary increases

Culture
Additional IT scrutiny for Mac users

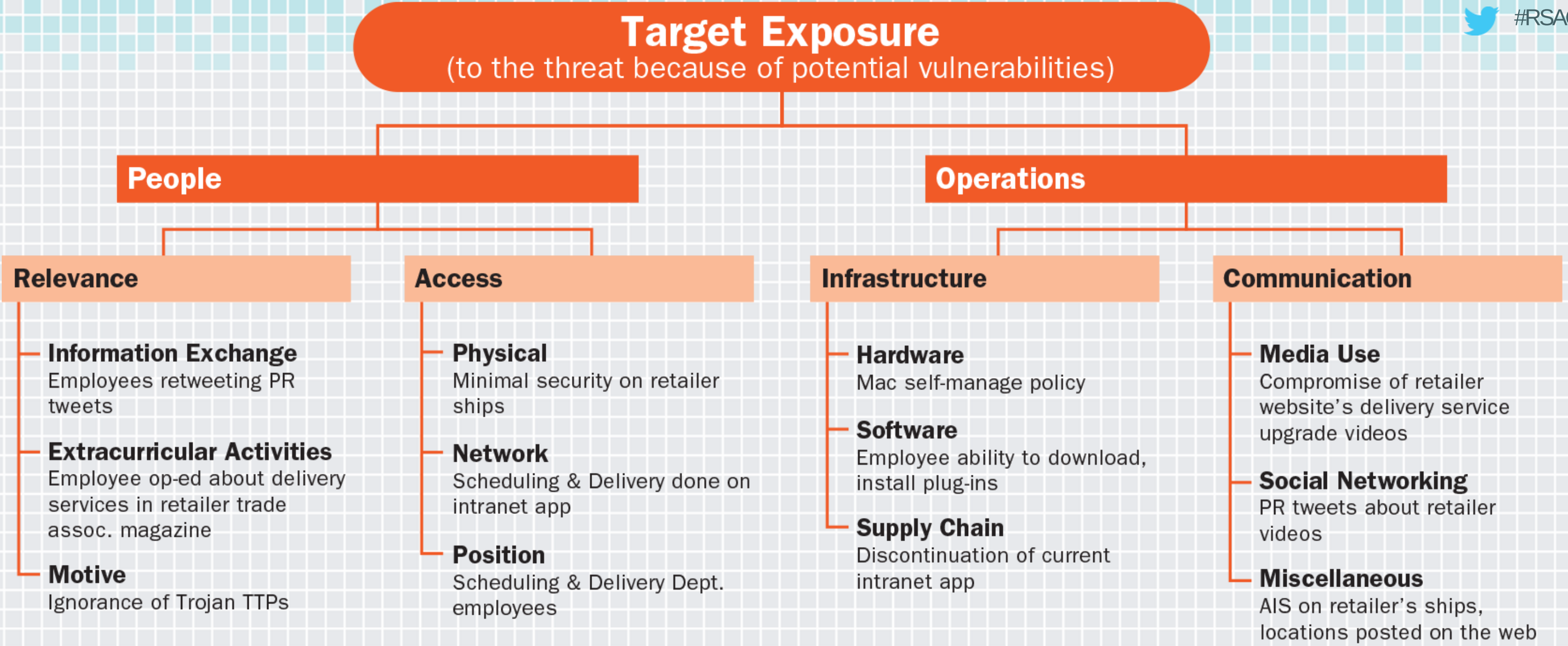
External Interests

Geopolitical
Economic pressure for nation-states to address piracy

Partnerships
Potential rail and airline partnerships

Brand Reputation
Devalues secure aspect of secure meeting spaces

What can Scuttlebutt do so the Trojan doesn’t affect the nation-state?
Text JAYMCALLISTE350 to 37607



Target Exposure
(to the threat because of potential vulnerabilities)

People

Relevance

- **Information Exchange**
  Employees retweeting PR tweets
- **Extracurricular Activities**
  Employee op-ed about delivery services in retailer trade assoc. magazine
- **Motive**
  Ignorance of Trojan TTPs

Access

- **Physical**
  Minimal security on retailer ships
- **Network**
  Scheduling & Delivery done on intranet app
- **Position**
  Scheduling & Delivery Dept. employees

Operations

Infrastructure

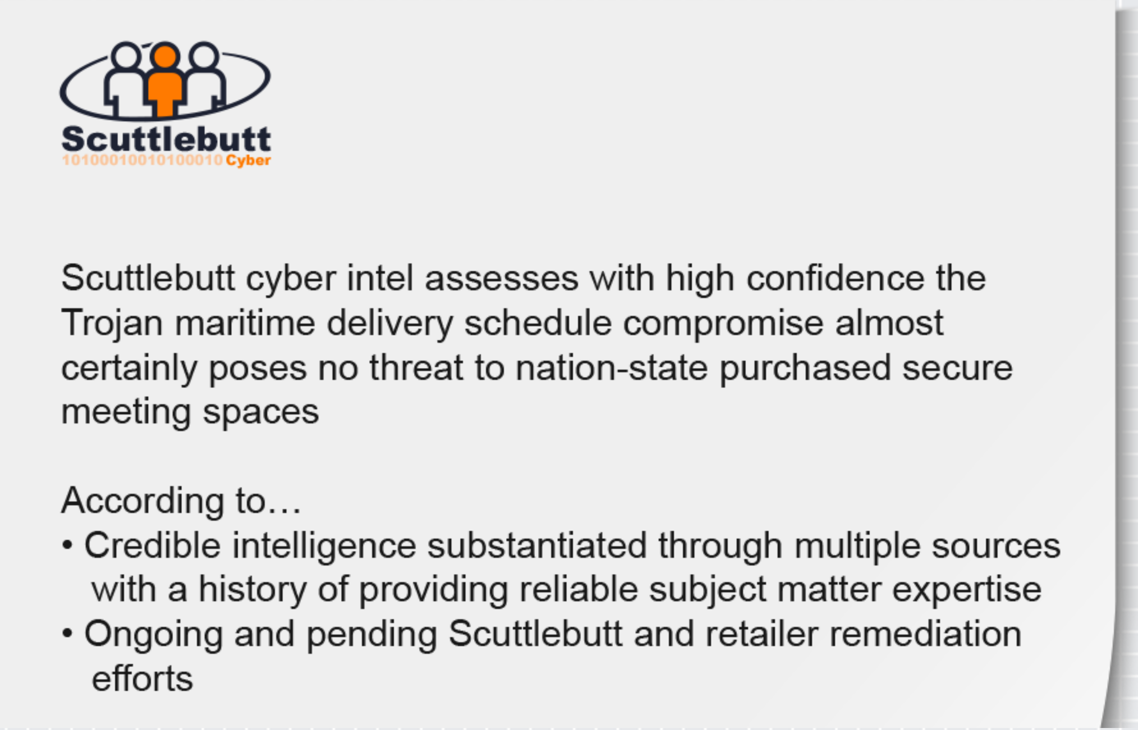
- **Hardware**
  Mac self-manage policy
- **Software**
  Employee ability to download, install plug-ins
- **Supply Chain**
  Discontinuation of current intranet app

Communication

- **Media Use**
  Compromise of retailer website's delivery service upgrade videos
- **Social Networking**
  PR tweets about retailer videos
- **Miscellaneous**
  AIS on retailer's ships, locations posted on the web

What can Scuttlebutt do so the Trojan doesn't affect the nation-state?
Text JAYMCALLISTE350 to 37607

Reporting…



Scuttlebutt
10100010010100010 Cyber

Scuttlebutt cyber intel assesses with high confidence the Trojan maritime delivery schedule compromise almost certainly poses no threat to nation-state purchased secure meeting spaces

According to…

- Credible intelligence substantiated through multiple sources with a history of providing reliable subject matter expertise
- Ongoing and pending Scuttlebutt and retailer remediation efforts

…and Feedback

Exercise feedback?

Text

JAYMCALLISTE350 to 37607

Overall Result

- Limits intelligence tunnel vision by understanding all causes and effects of potential threats

RSAConference2015

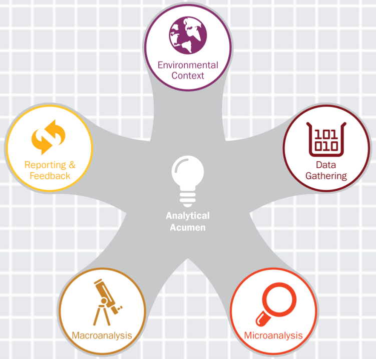
San Francisco | April 20-24 | Moscone Center

#RSAC

Applying Analytical Adaptability

Moving Forward

- Practice creative brainstorming
- Follow @sei_etc for baseline and holistic assessment templates
- Use the templates to baseline analysis and assess threats



Environmental Context

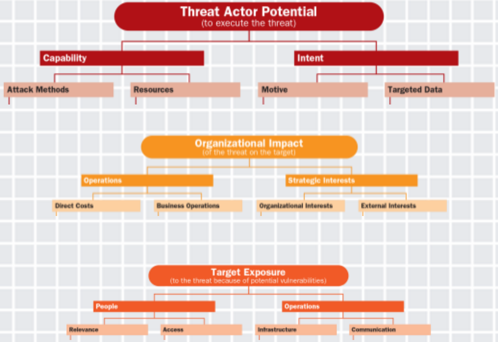
Reporting & Feedback

Data Gathering

Analytical Acumen

Macroanalysis

Microanalysis



Threat Actor Potential
(to execute the threat)

Capability

Attack Methods

Resources

Intent

Motive

Targeted Data

Organizational Impact
(of the threat on the target)

Operations

Direct Costs

Business Operations

Strategic Interests

Organizational Interests

External Interests

Target Exposure
(to the threat because of potential vulnerabilities)

People

Relevance

Access

Operations

Infrastructure

Communication

RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: HUM-W01

Be Like Water: Applying Analytical Adaptability to Cyber Intelligence

Jay McAllister

jjmcallister@sei.cmu.edu
@sei_etc

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0002289