Cyber Intelligence Workforce

Troy Townsend
Melissa Kasan Ludwick

September 17, 2013

Software Engineering Institute | Carnegie Mellon

Agenda

Project Background

- Research Methodology
- Findings

Training and Education

- Project Findings
- Workshop Results
- Objectives
- Traits
- Core Competencies and Skills
- Gap Analysis
- Potential Courses of Action

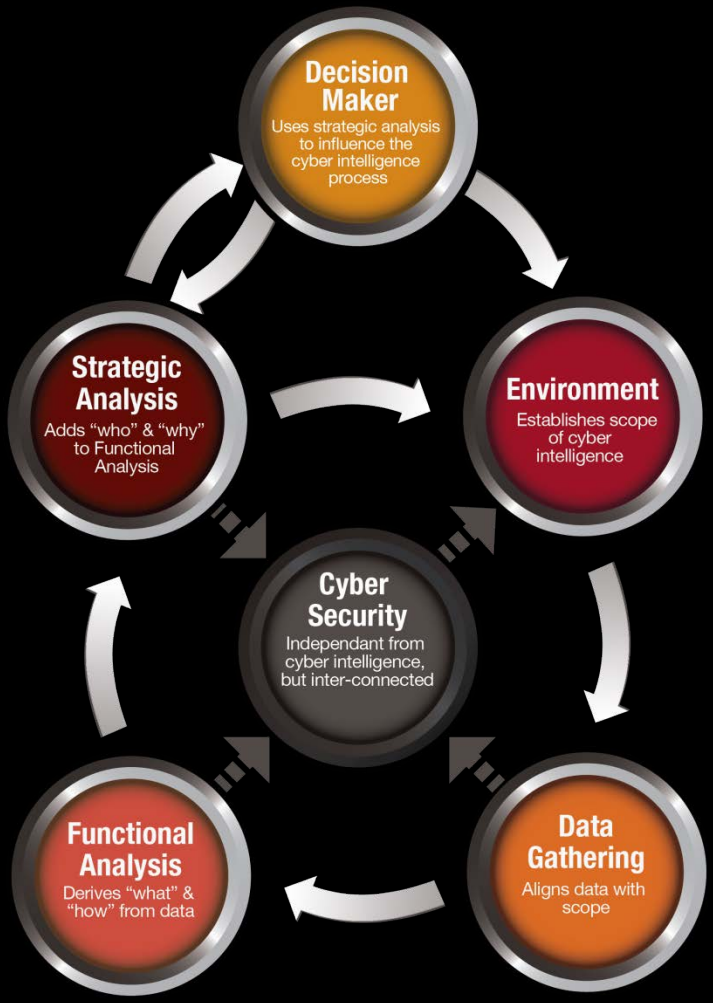
Cyber Intelligence Tradecraft Project Background

Charged with studying the state of cyber intelligence across government, industry, and academia

"*Cyber intelligence is the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities of offer courses of action that enhance decision making.*"

Goal is to advance the capabilities of organizations performing cyber intelligence by elaborating of best practices and prototyping solutions to shared challenges

Research Methodology: Cyber Intelligence Framework



Research Methodology: Participants and Baseline Sessions

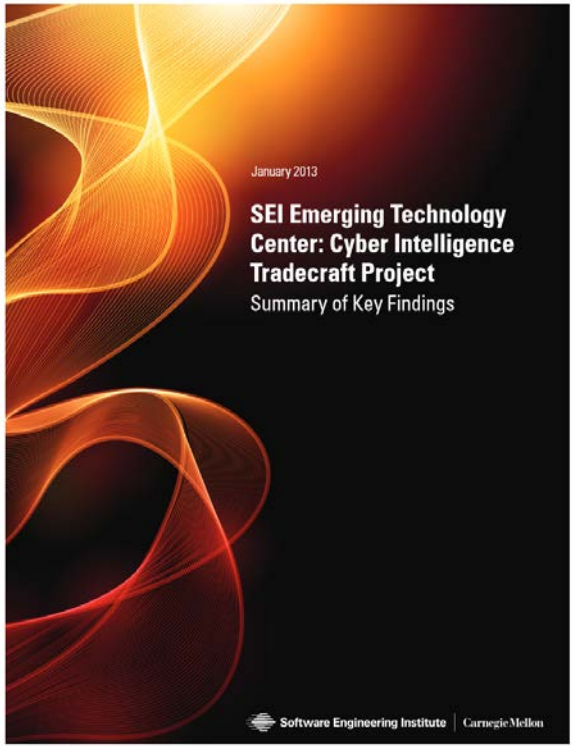
Project Participants

- 6 government agencies
- 25+ organizations from academia and industry representing financial, legal, healthcare, retail sectors

Baseline Sessions

- Methodologies
- Technologies
- Processes
- Training

Findings: Disclaimer



www.sei.cmu.edu/goto/cyberintel

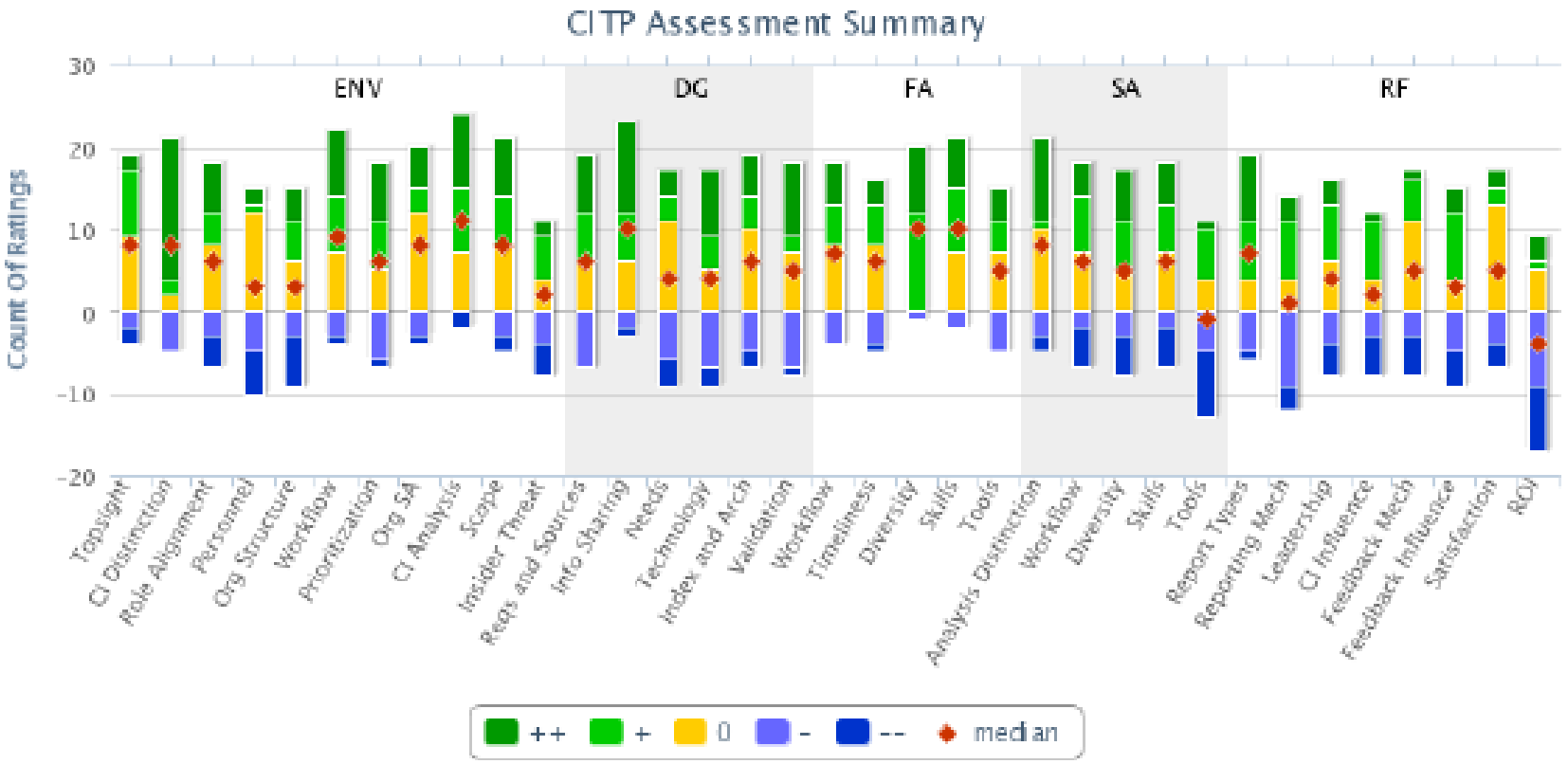
What this is:

- Snapshot of organizations' cyber intelligence process
- Synthesized based on expert judgment
  - Not a Survey Monkey endeavor, lots of prodding, poking, and reading between the lines

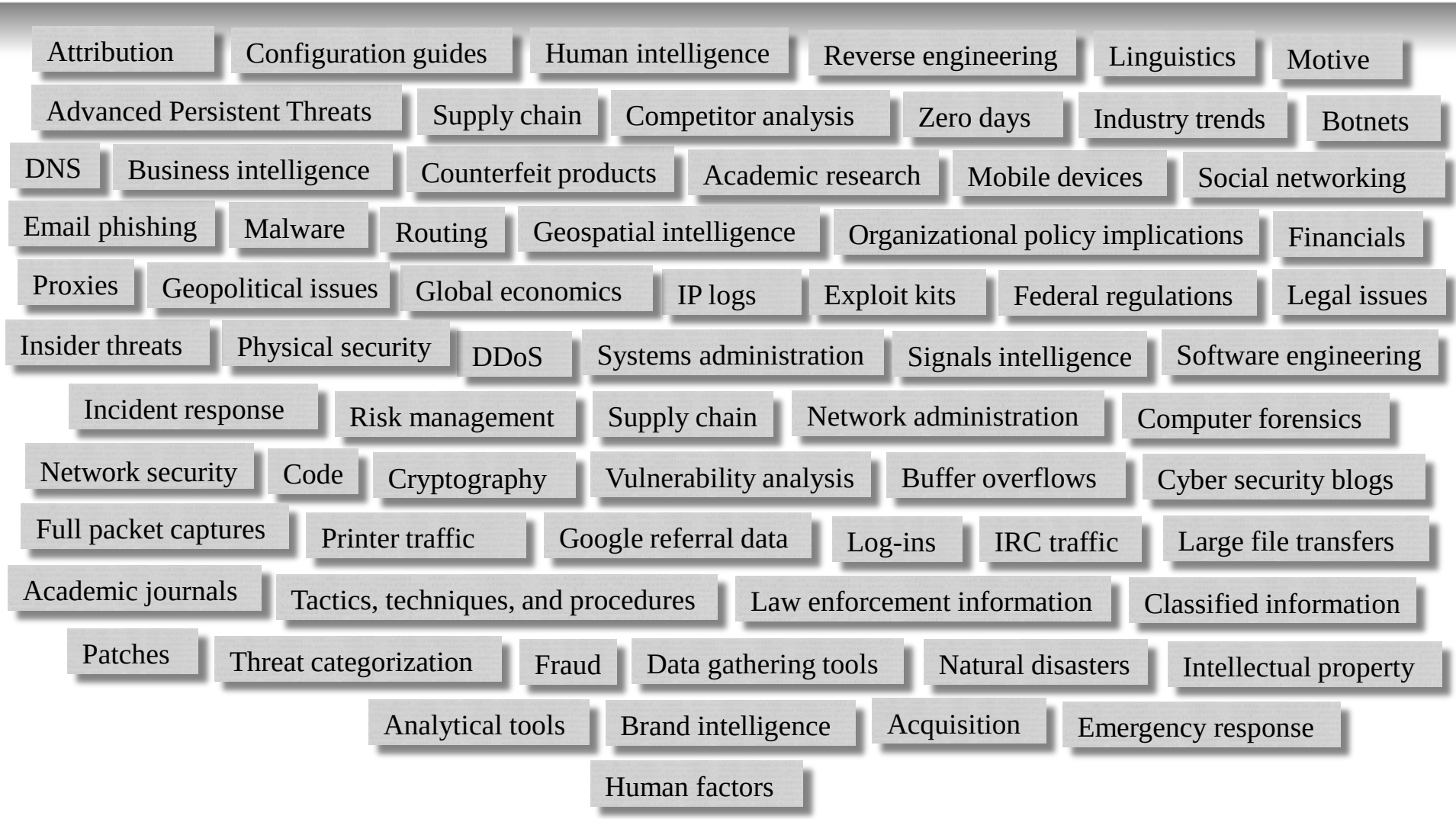
What this is *not*:

- A scorecard - Not all organizations need to be a best practice to get the job done
- Textbook ready - Relied on kindness of strangers, not independently verified data
- All encompassing - Participation bias

Findings



What Cyber Intelligence Analysts Do…



Backgrounds of Current Analysts...

DNI Tradecraft Training

Undergraduate degree in Latin

Former help desk technician

Undergraduate degree in Philosophy

Former military signal corps

Network + Certification

Analysis Training

Undergraduate degree in Computer Science

Former network security analyst

Former software engineer

A+ Certification

Classes offered at BlackHat

SANS Training

Master's in Strategic Analysis

Forensics Certification

Former think tank employee

Undergraduate degree in Sociology

Former government intelligence analyst

Defense Intelligence Agency Network Training

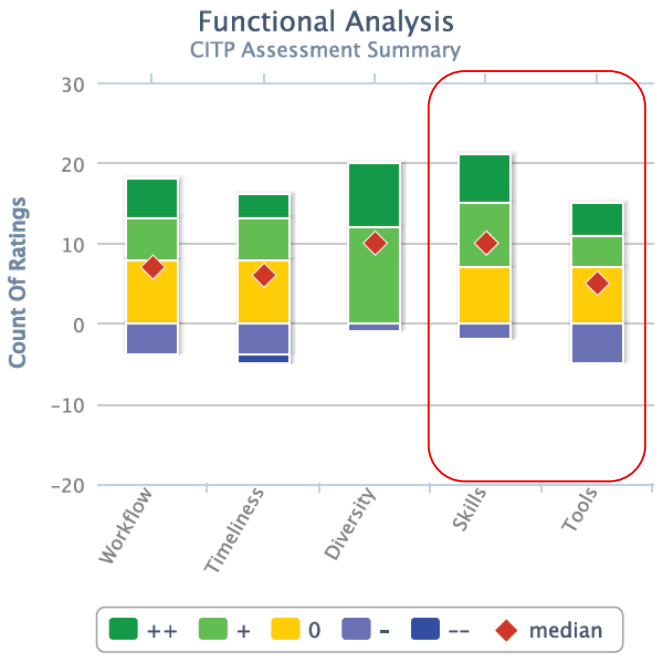
Undergraduate degree in International Relations

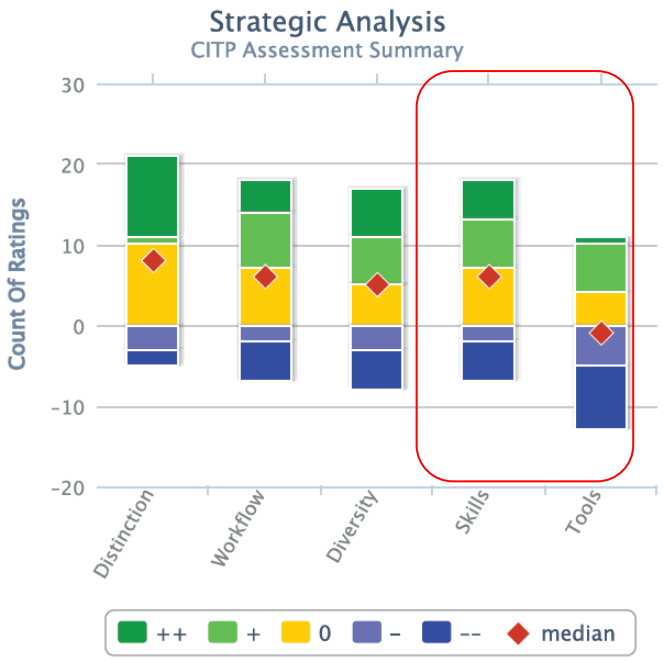
Tripwire Analytic Capability Training

CEH Certification

Former military intelligence

Project Findings: Challenges





- Resulting inefficiencies from the diverse job functions and skill sets
- Cultural differences
- Unrealistic job descriptions
- Education in silos

Training and Education Objectives

- Determine current state of training and education offerings for cyber intelligence analysts across academia, industry, and government
- Define the competencies and skills organizations should look for when hiring the “ideal” cyber intelligence analyst
- Identify the gaps between the currents and desired state of cyber intelligence offerings
- Identify potential courses of action

Constraints

- Reviewed ~150 courses, trainings, and certifications from government, industry, and academia
- Very few “cyber intelligence” programs; searches were expanded to include cyber security and intelligence studies
- Searches were restricted to information found mainly online, though discussions with industry and academic contacts were insightful
- Limited number of government offerings, no classified courses

CITP Workshop

Please Join Us...

Carnegie Mellon University and the Software Engineering Institute's Innovation Center invite you to attend the Cyber Intelligence Tradecraft Project Workshop.

At the workshop, you will receive your baseline and benchmark results and the state of the practice report. You also will be able to engage with the SEI Innovation Center team, other participants, and CMU faculty on the project's future prototyping efforts and CMU's cutting-edge research in related fields.

Location: Pittsburgh, Pennsylvania

Day 1: Fairmont Hotel, 510 Market St. Pgh, PA 15222 (Map and Directions)

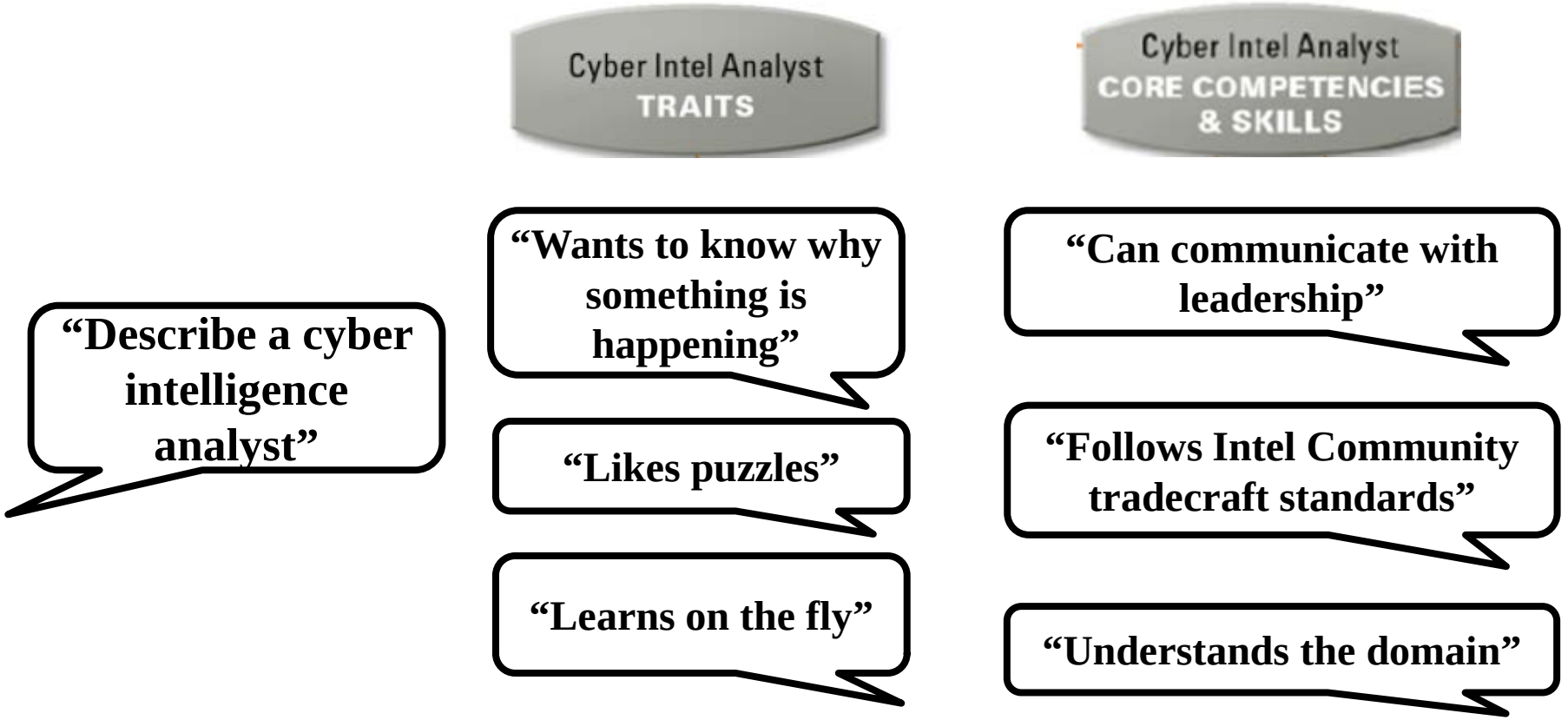
Day 2: Carnegie Mellon University, 5000 Forbes Ave. Pgh, PA 15213 (Map)

CITP Workshop - 2

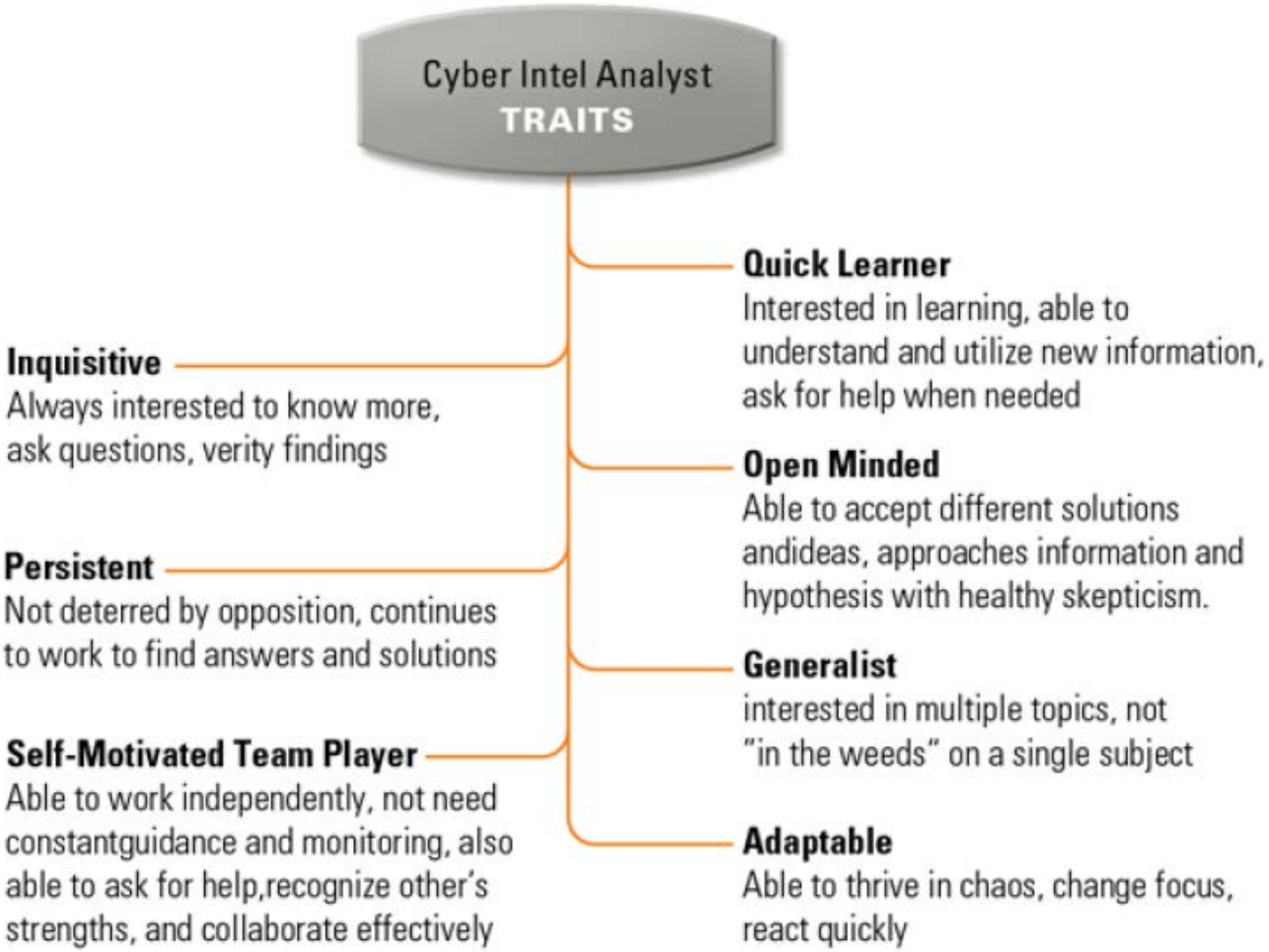
Training & Education Track

- Participants finished statements such as:
  - A good analyst can…
  - I need someone that can…
- Answers populated a wish list of desired skills and capabilities
- Participants utilized human-centered design concepts to identify improvements to current training and hiring practices

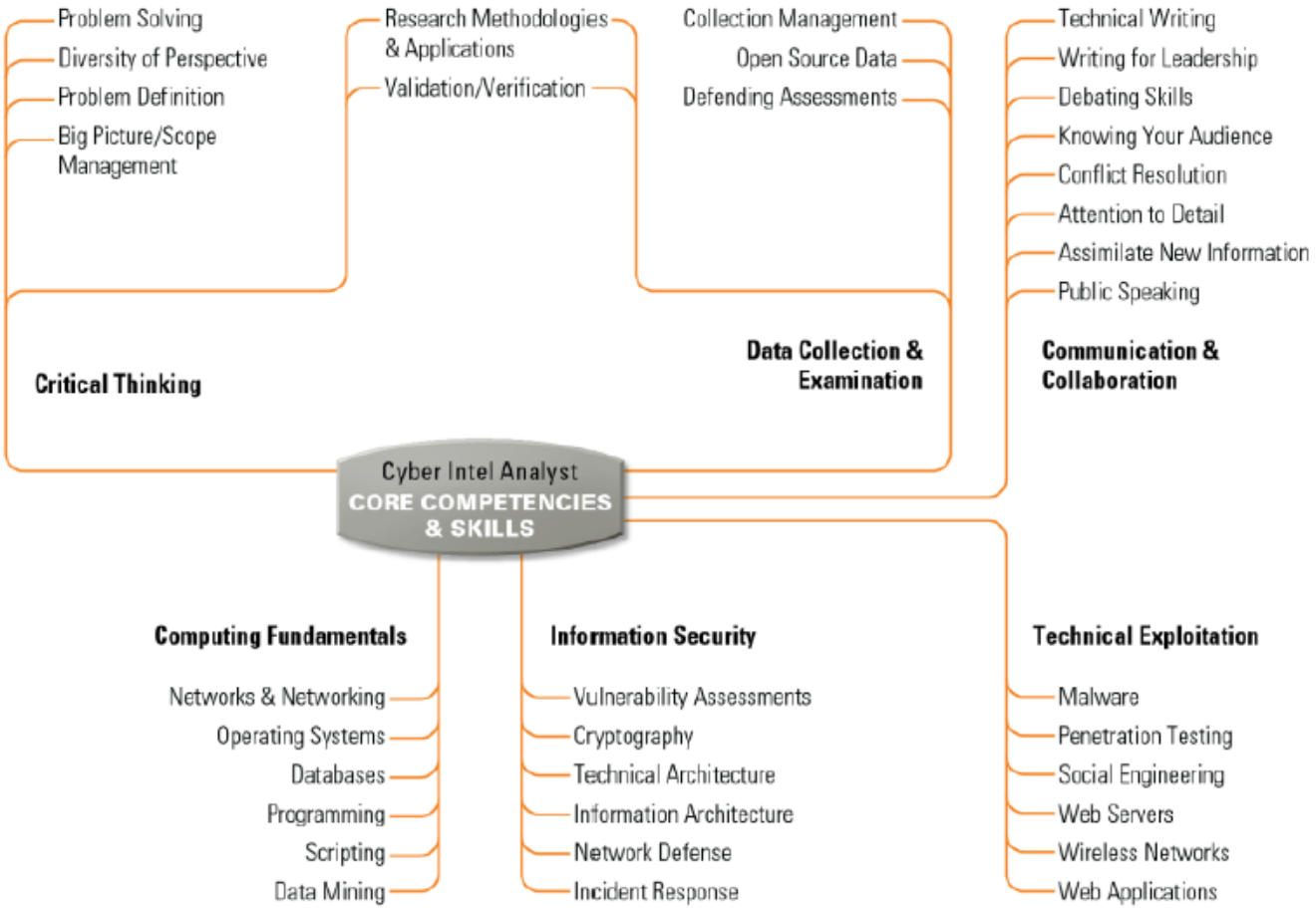
Traits vs Competencies



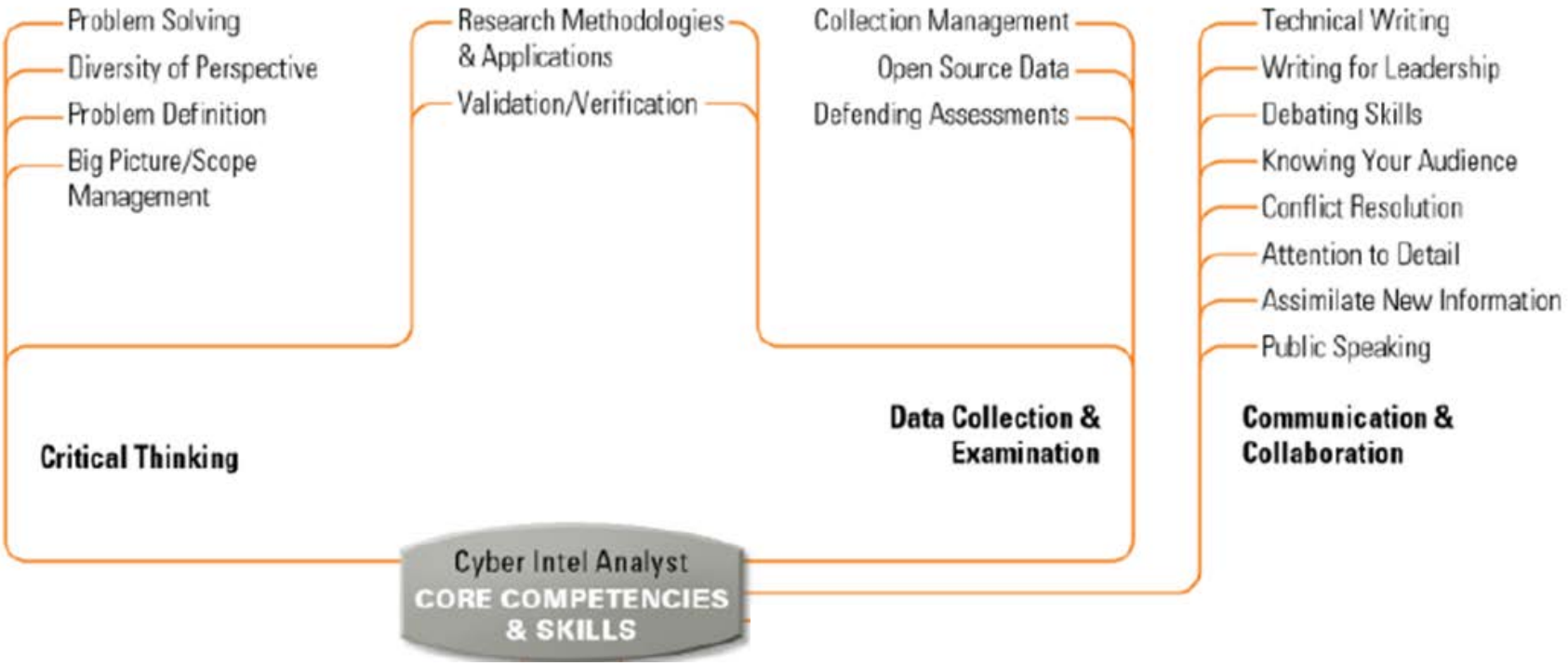
Traits



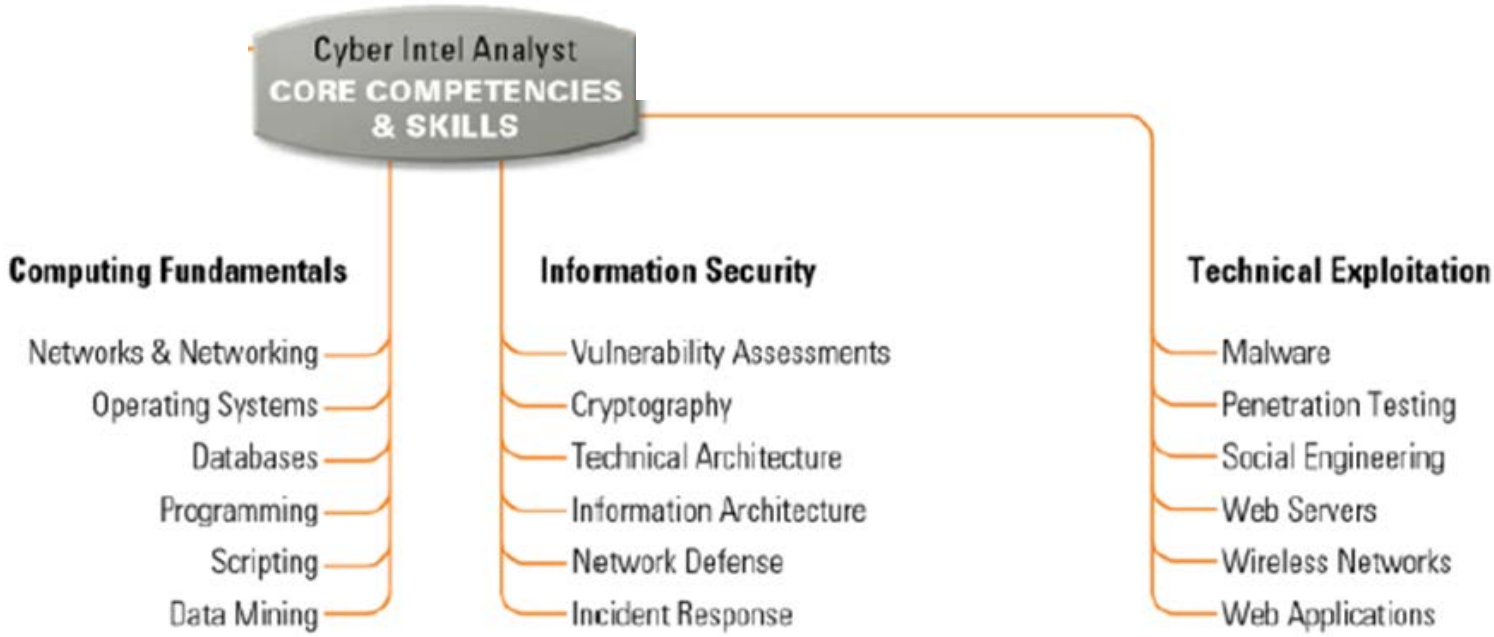
Core Competencies and Skills



Core Competencies: Analytic Competencies



Core Competencies: Technical Competencies



Gap Analysis

		Courses	
Competency	**Skill**	**Good**	**Maybe**
Critical Thinking	Problem Definition	NONE	NONE
	Problem Solving		AMU - Intelligence Operations
			AMU - Analytics II
			AMU Threat Analysis
			MU - Analytic Techniques
			MU - Cyber Threat Analysis
			ASU - Advanced Intelligence analysis: Operating in Complex Environments
	Diversity of Perspective	NONE	NONE
	Big Picture/Summarization/Synthesis		ASU - Grand Strategy, Intelligence Analysis, and Rationality
	Scope Management	HPU - Intelligence Team Management	UM - Intelligence Management and Oversight
	Research Methodologies & Applications	UM - Intelligence Analysis: Consumers, Uses, and Issues	DC3 - Cyber Analyst Course
		UDM - Research Methods	UM - Library Research Skills
		NPS - Cyber Systems and Operations Research Methods	
		HPU - Open Source Intelligence	
		MU - Research Methods in Intelligence	
		AMU - Research Methods	
		ASU - Introduction to Research Methods	
	Skepticism/Validation/Verification	HPU - Vetting	
Data Collection & Examination	Research Methodologies & Applications	UM - Intelligence Analysis: Consumers, Uses, and Issues	DC3 - Cyber Analyst Course
		UDM - Research Methods	UM - Library Research Skills
		NPS - Cyber Systems and Operations Research Methods	
		HPU - Open Source Intelligence	
		MU - Research Methods in Intelligence	
		AMU - Research Methods	
		ASU - Introduction to Research Methods	
	Skepticism/Validation/Verification	HPU - Vetting	
	Collection Management	ISA - Intelligence Collection	ASU - Intelligence Analysis and National Security Perspectives
		ISA - Cyber Collections	HPU - Intelligence Operations
		HPU - Intelligence Collection	HPU - Intelligence Practicum
		HPU - Recruitment Cycle	
		HPU - All Source Intelligence	
		NPS - Cyber Systems and Operations Research Methods	
		UM - Intelligence Collection: Sources and Challenges	
		SN - Cyber Intelligence Training	
		AMU - Collection	
	Open Source Data	HPU - Open Source Intelligence	ISA - Cyber Collections
		AMU - SIGINT	UM - Intelligence Collection: Sources and Challenges
	Defending Assessments	NONE	NONE
Communication & Collaboration	Defending Assessments	NONE	NONE
	Technical Writing	ERAU - Technical Report Writing	HPU - Writing for Publication
	Writing for Leadership	CMU - Professional Writing	HPU - Writing for Publication
		ISA - Analyst Training: Writing, Analysis, and Preparing Briefings	
	Debating Skills	NONE	NONE
	Knowing your Audience	NONE	NONE

CITP Training and Education 21

Current offerings address little more than 50% of the identified competencies & skills

Discrepancies between needed skills and current training opportunities

Inconsistent/nonexistent training paths for cyber intelligence analysts

No academic programs that offers the ideal mix of technical and non-technical classes

Difficult for academic institutions to provide training using relevant tools and technology, especially using current data and threats

Potential Courses of Action

Assess current analysts and identify appropriate training to address deficiencies

- Use competencies mind map to review current skillset
- Target specific skills to improve, seek training to address the gaps

Hire differently

- Review and rewrite job descriptions tailored to needed competencies and skills
- Used list of traits to ask interview questions and determine if candidate has natural ability

Potential Courses of Action - 2

Explore internships and apprenticeships

- Partner with academic institutions to gain short term talent and provide feedback to schools

Rethink the traditional classroom

- Explore advanced tradecraft technology leveraging cyber intelligence, computer science, and visual analytics
- Put students in real world scenarios to enable successful learning
  - Conduct multi-source analysis
  - Emphasize the information that is critical to make recommendations and decisions
  - Demonstrate the impact of strategic decisions

For more information

Cyber Intelligence Tradecraft Project Team
SEI Emerging Technology Center @SEI_ETC
citp-info@sei.cmu.edu

Troy Townsend @TLTownie
CITP Team Lead
tltownsend@sei.cmu.edu

Melissa Kasan Ludwick
SEI Emerging Technology Center
mkasan@sei.cmu.edu

This material is based upon work funded and supported by Office of the Director of National Intelligence (ODNI) 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 sponsored by the United States Department of Defense. 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 Office of the Director of National Intelligence (ODNI) or the United States Department of Defense.

DM-0000458

Backup Material

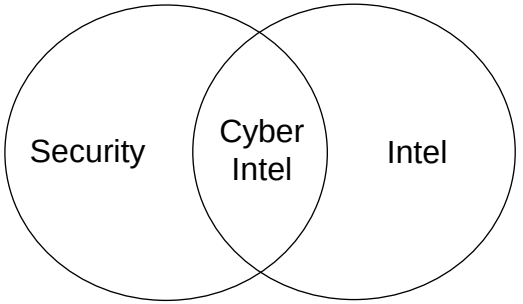
Distinguishing between functions

Cyber security

- Find the threat, fix the vulnerability, move on

Cyber intelligence

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

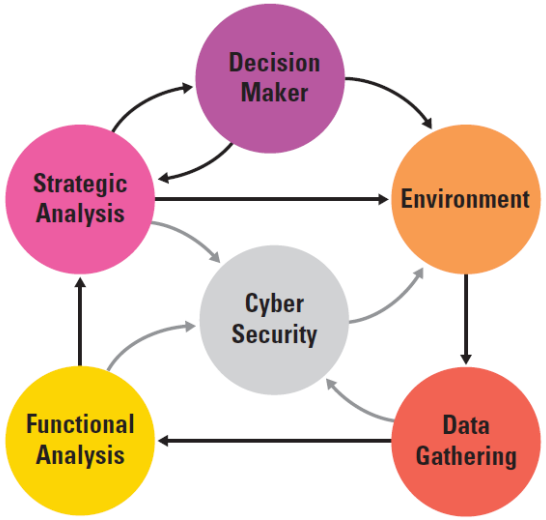


Functional analysis

- Answers “what” and “how:” Analyst identifies a compromised machine from proxy server logs and U.S. CERT security bulletins

Strategic analysis

- Answers “who” and “why:” Analyst takes functional analysis and compares it to vendor threat actor profiles to determine why the machine was compromised to predict the next possible target



Overcoming Challenges

Education

Current state

- BA, MS in intelligence
  - Limited cyber focus

Future potential

- Undergraduate
  - Major vs. minor
- Graduate
  - Certificate
  - Master's program

Carnegie Mellon University

Training

Current state

- Limited cyber specific paths for analytical core - public or private
  - Ad-hoc training when time, $ permit

Future potential

- Certification program
  - Mix functional and strategic
  - Implement life-long learning
  - Creativity to engage adult learners

Software Engineering Institute
Carnegie Mellon

Gap Analysis – 2 – back

Competency	Skill
Critical Thinking	Problem Definition
	Diversity of Perspective
Data Collection & Examination	Defending Assessments
Communication & Collaboration	Defending Assessments
	Debating Skills
	Knowing your Audience
	Attention to Detail
	Assimilate New Information
Technical Exploitation	Malware
	Web Servers
	Web Applications
Information Security	Information Architecture
Computing Fundamentals	Databases
	Scripting