RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: AIR-W02

The State of the Union on Cyber Intelligence

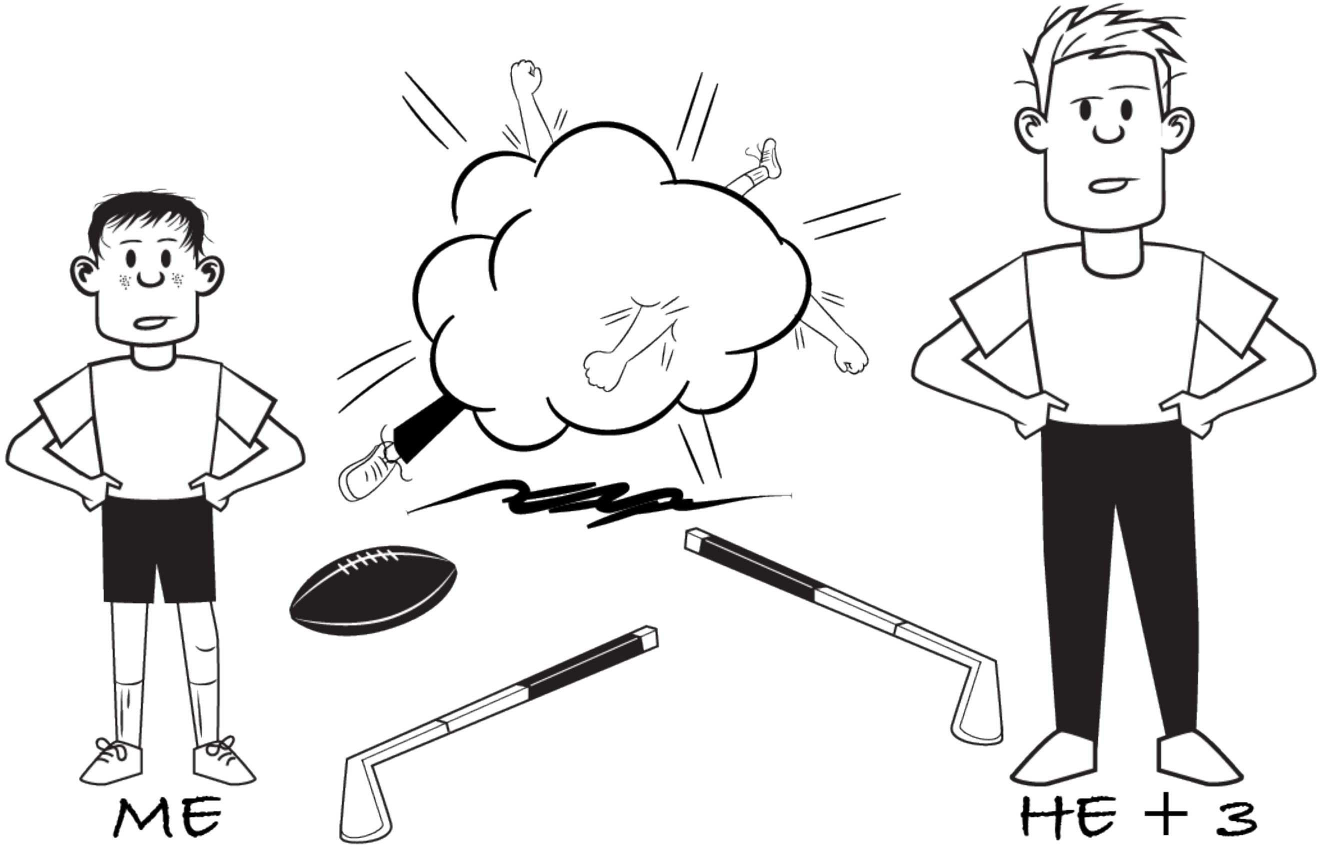
Jared Ettinger

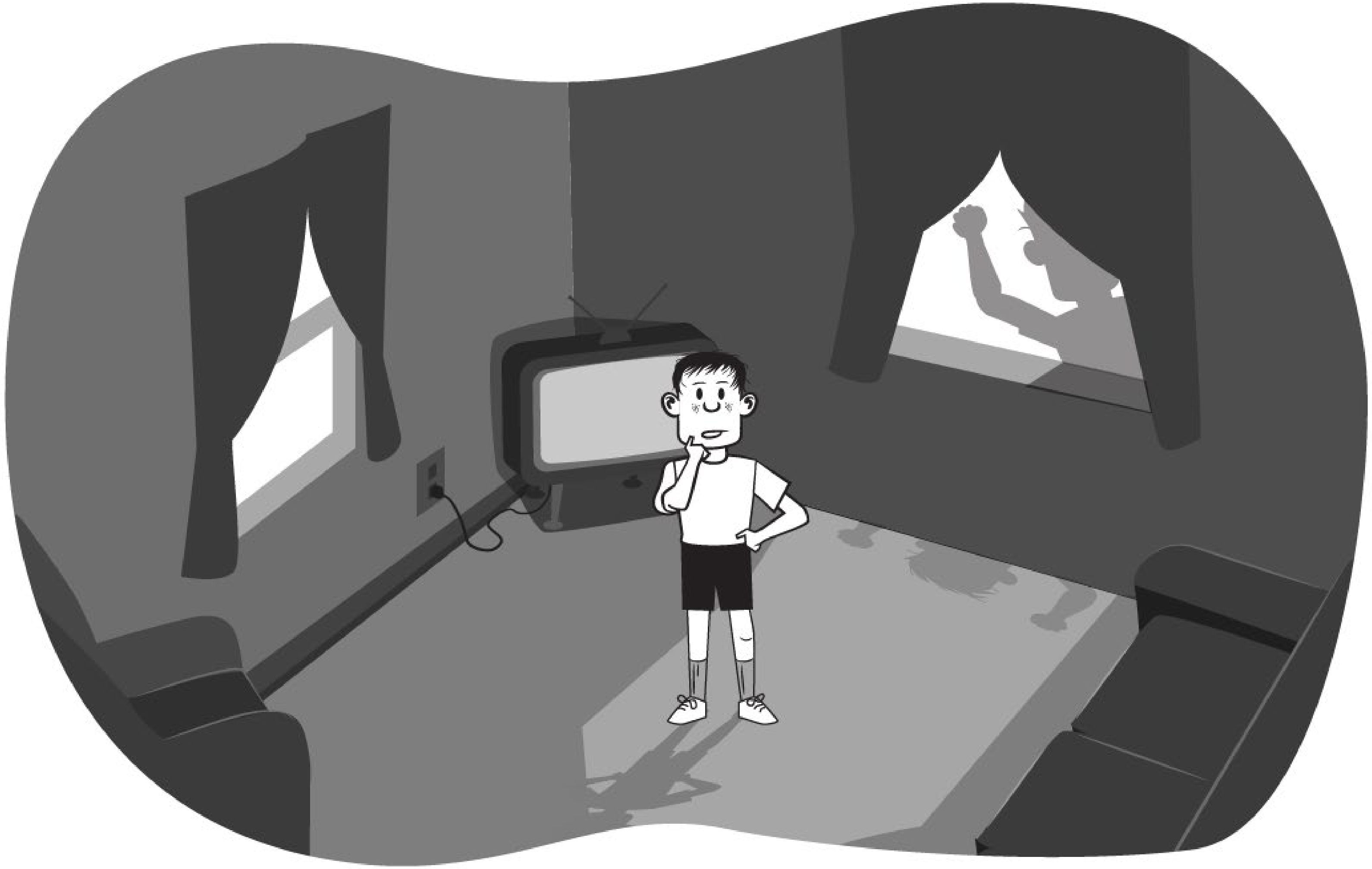
Cyber Intelligence Researcher
Adjunct Instructor
Carnegie Mellon University, Software Engineering Institute

Carnegie Mellon University Software Engineering Institute does not endorse or promote any company, agency, product, tool, or technology in this presentation.

Legal

DM19-0189


ME
HE + 3



Carnegie Mellon University
SEI Emerging Technology Center:
Making the Recently Possible Mission-Practical

Applied Artificial Intelligence
and Machine Learning

Advanced Computing

Human-Machine Interaction

32
ORGANIZATIONS

11
SECTORS

57
SURVEY RESPONSES

Cyber Intelligence Tradecraft Study

Conducted on behalf of the US Office of the Director of National Intelligence by the Software Engineering Institute at Carnegie Mellon University

Purpose: understand how organizations conduct cyber intelligence activities

Purpose: identify common challenges and best practices

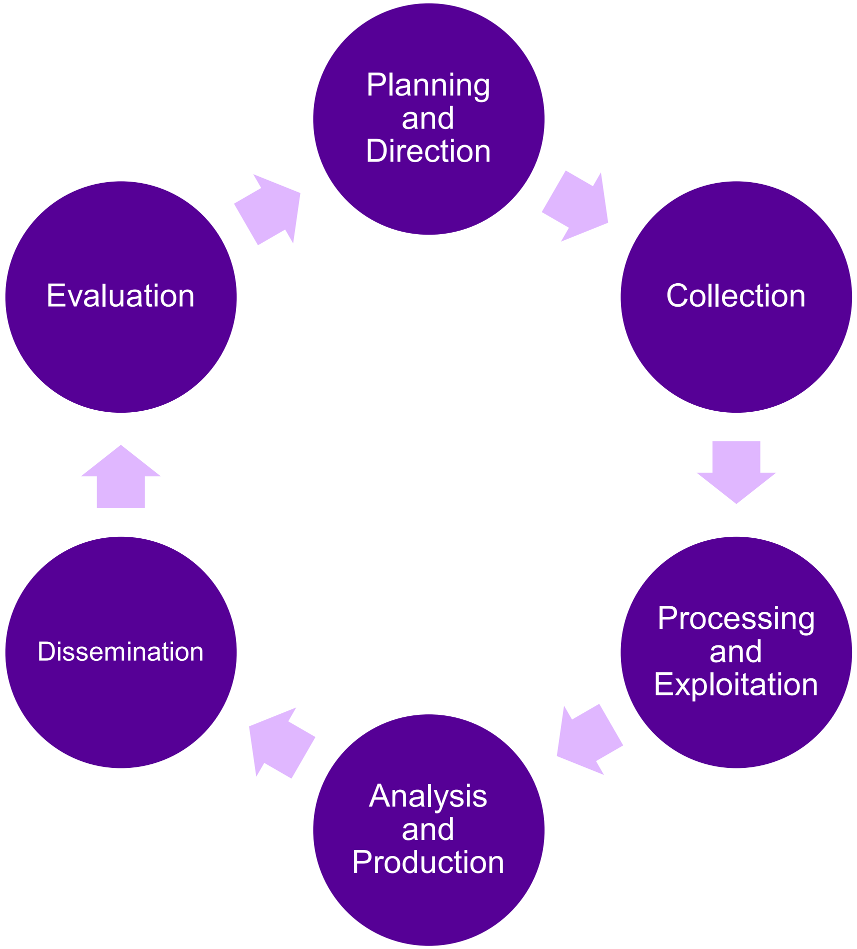
100
INTERVIEW HOURS

746
CHALLENGES

1,522
PRACTICES

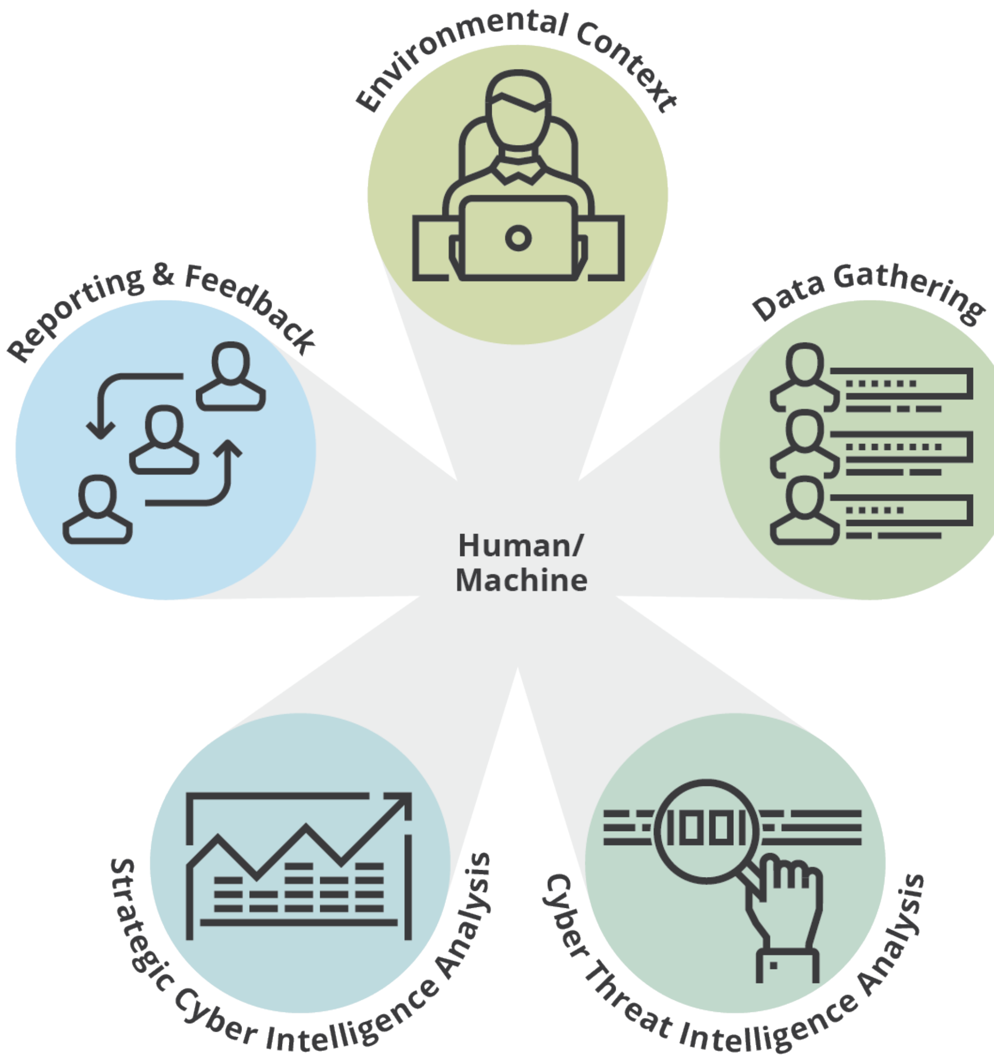
Emerging Tech
+
Cyber Intel

Use a Cyber Intelligence Analytic Framework



Traditional Intelligence Cycle

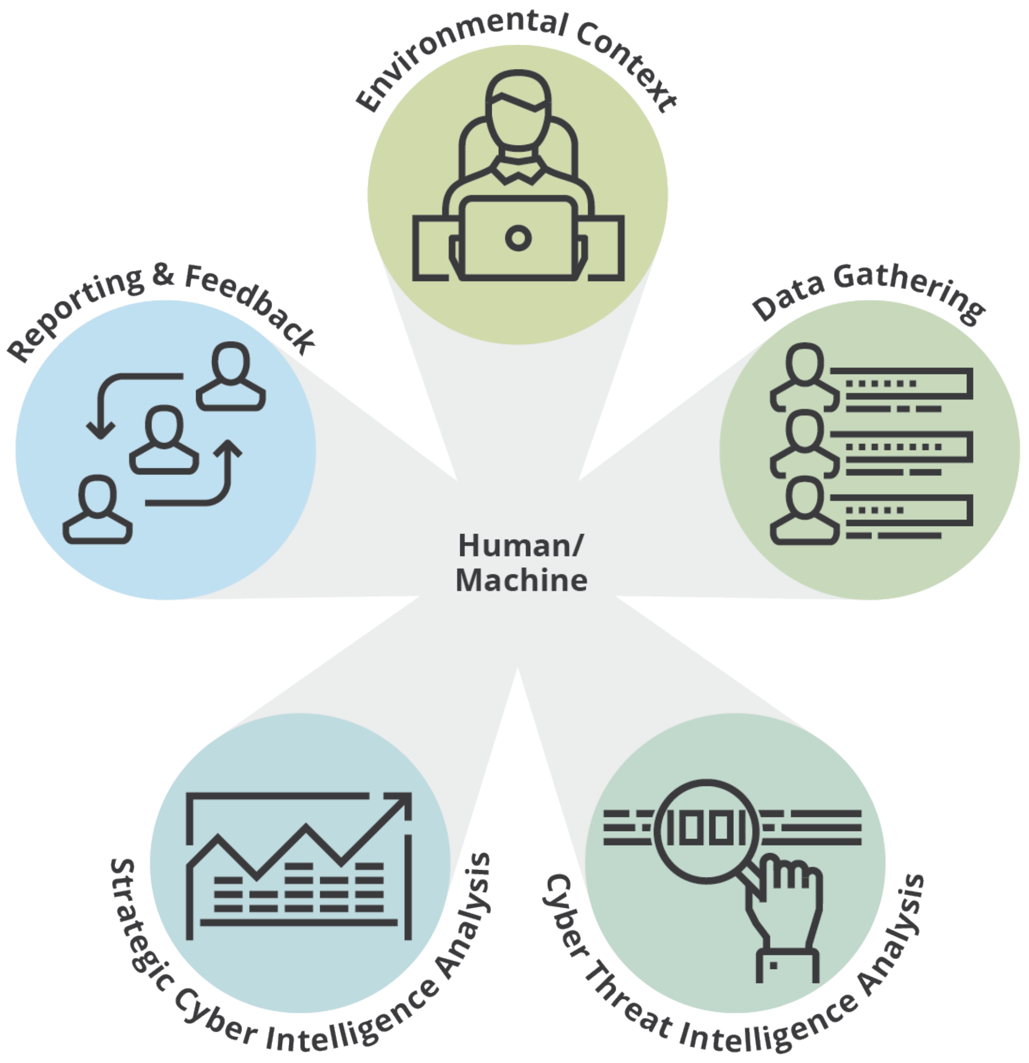
Use a Cyber Intelligence Analytic Framework


Environmental Context
Reporting & Feedback
Data Gathering
Human/
Machine
Strategic Cyber Intelligence Analysis
Cyber Threat Intelligence Analysis

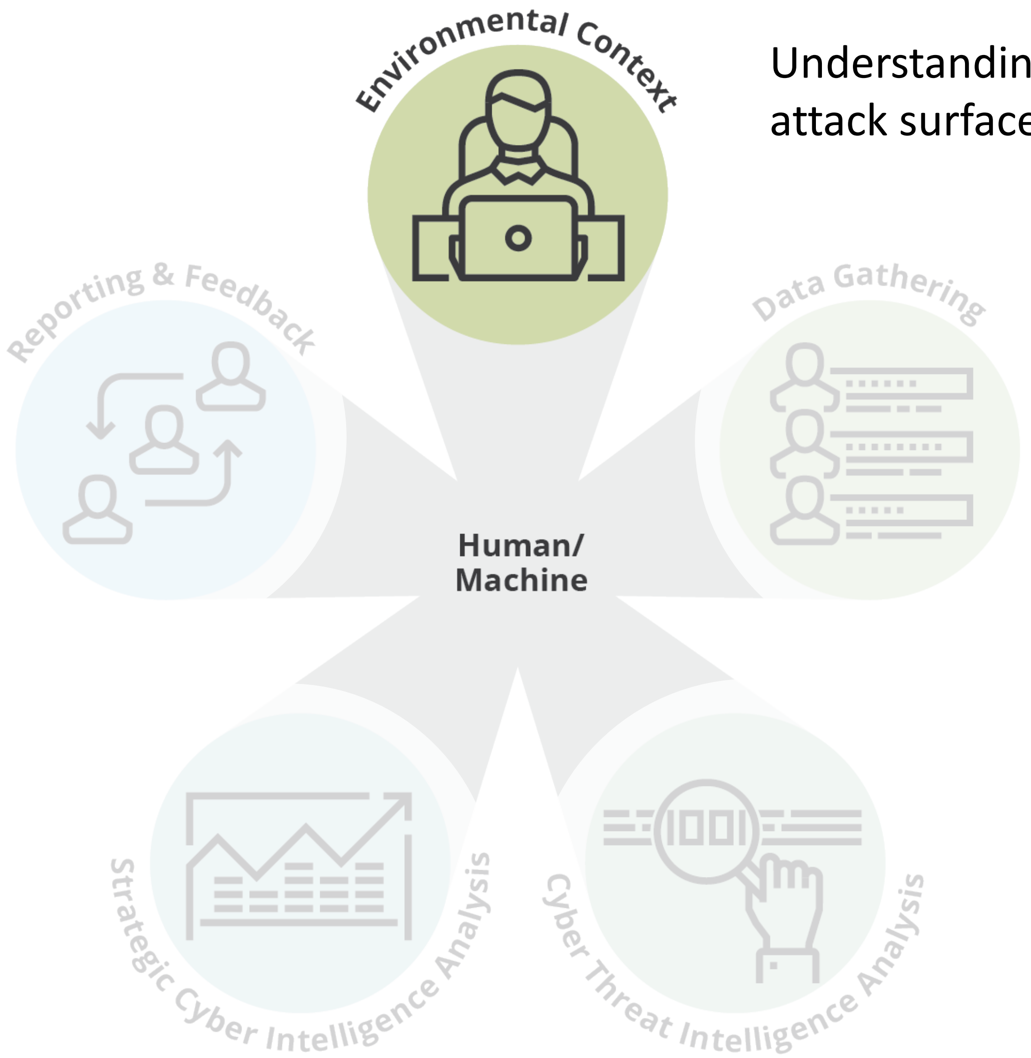
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Use a Cyber Intelligence Analytic Framework

Cyber Intelligence: The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities to offer courses of action that enhance decision making.

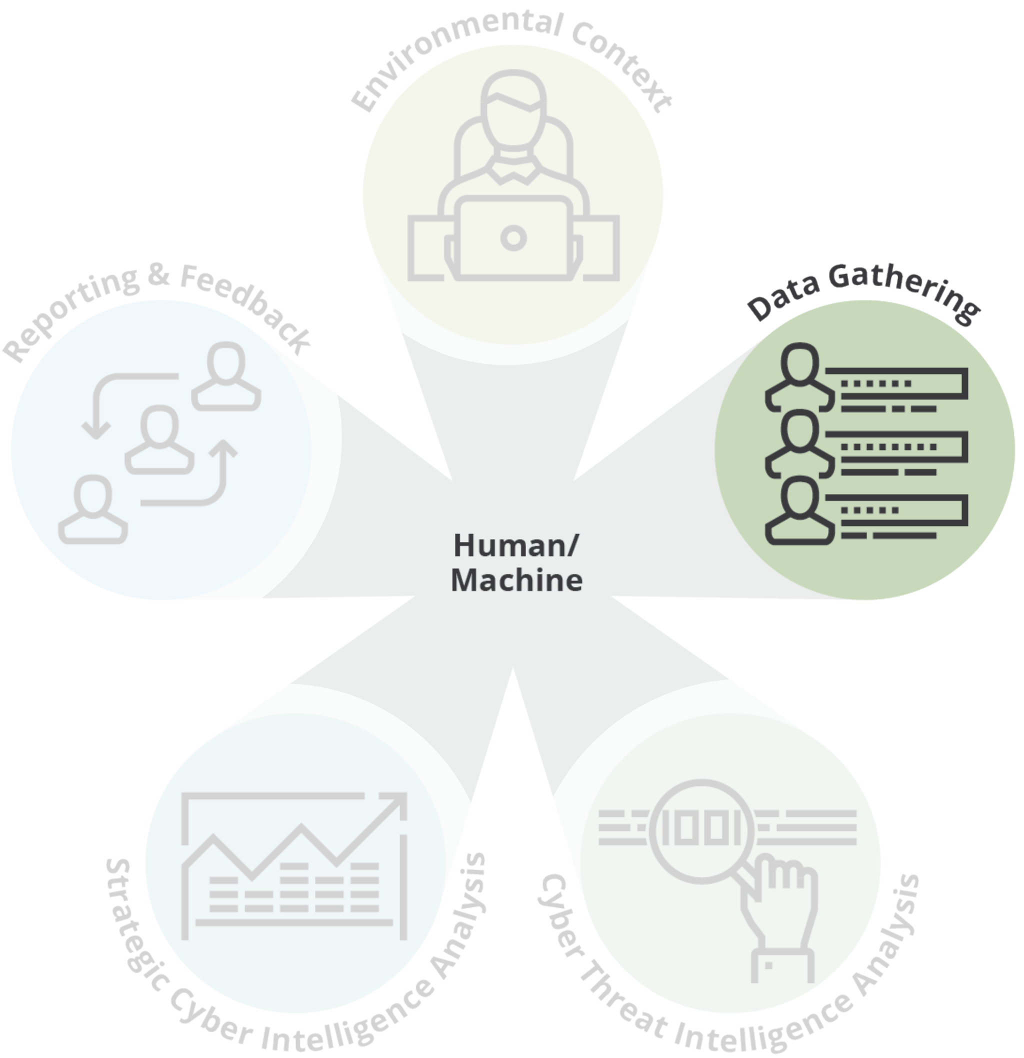


Use a Cyber Intelligence Analytic Framework


Environmental Context
Reporting & Feedback
Data Gathering
Human/
Machine
Strategic Cyber Intelligence Analysis
Cyber Threat Intelligence Analysis

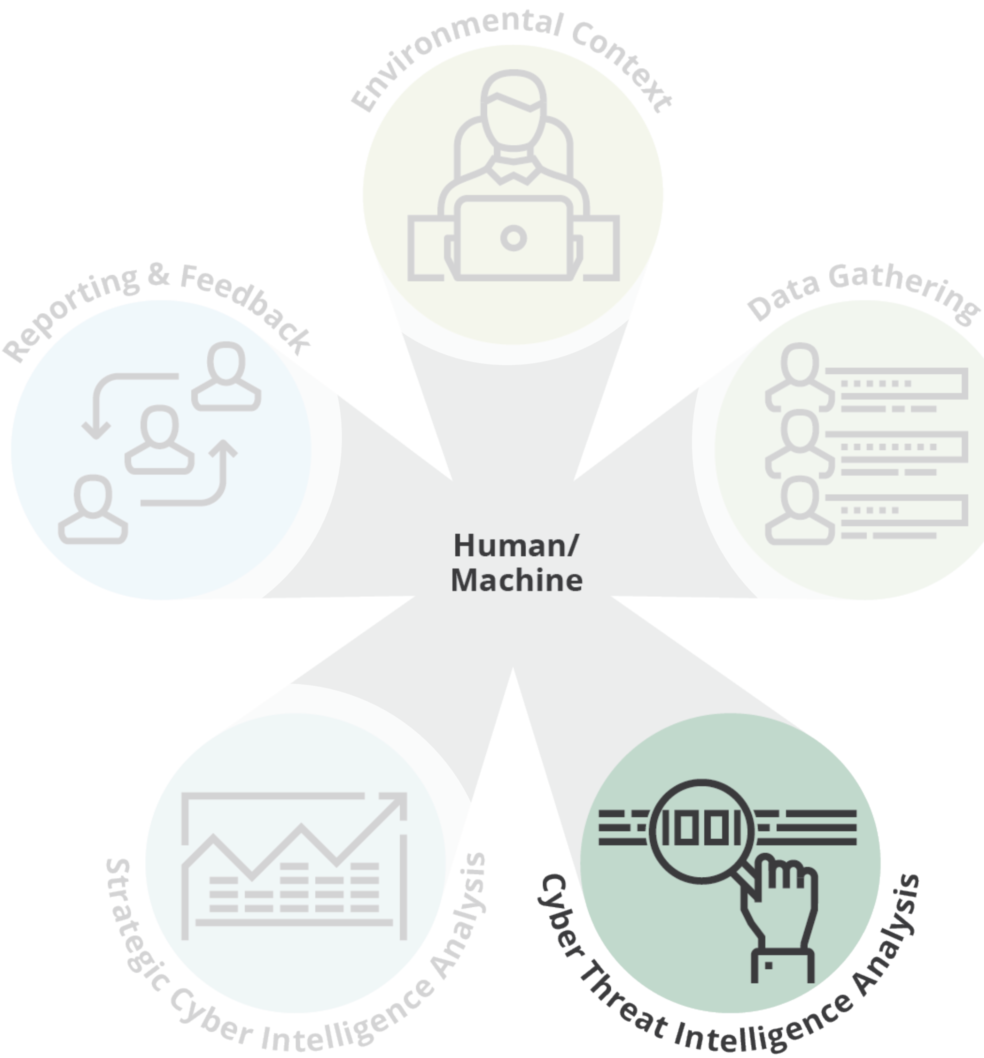
Understanding your organization's entire attack surface.

Use a Cyber Intelligence Analytic Framework


Environmental Context
Reporting & Feedback
Data Gathering
Human/
Machine
Strategic Cyber Intelligence Analysis
Cyber Threat Intelligence Analysis

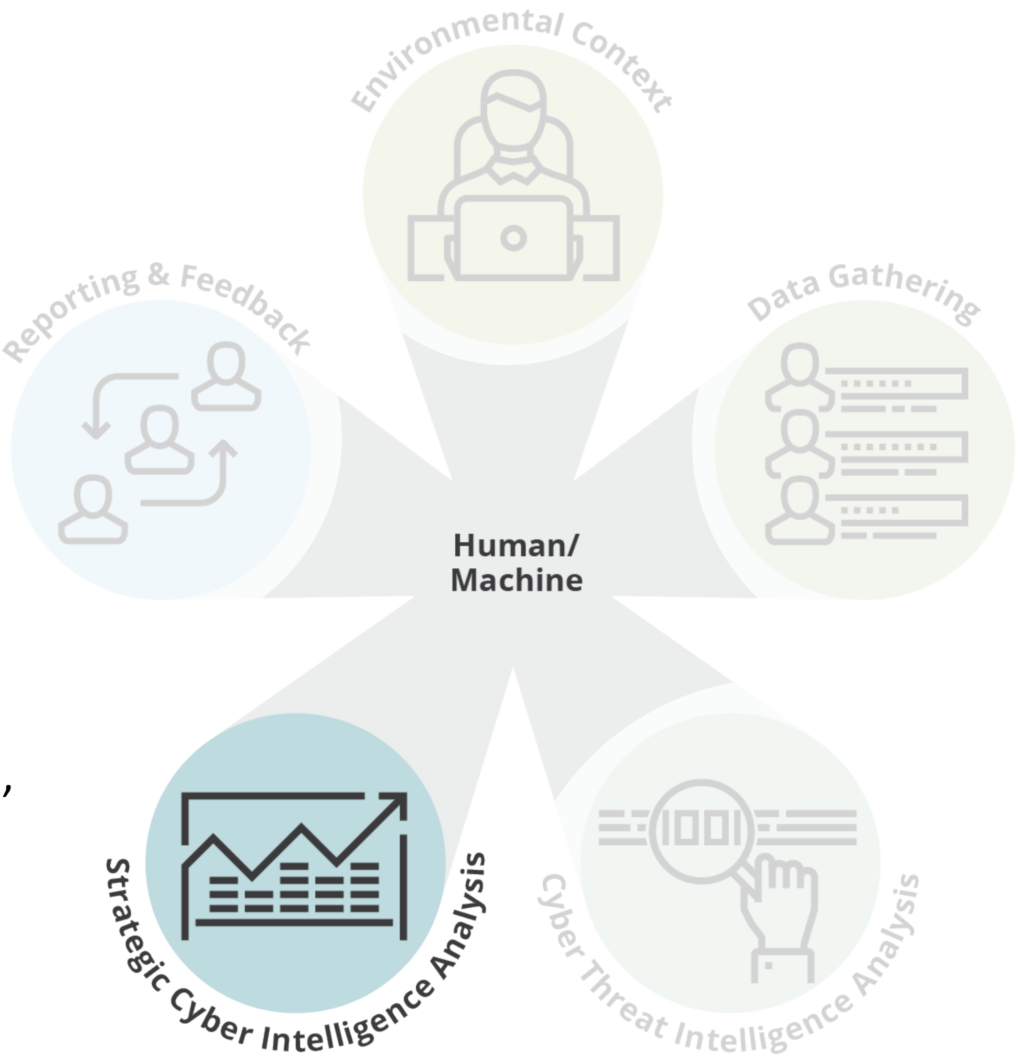
Using multiple sources to answer organizational intelligence requirements.

Use a Cyber Intelligence Analytic Framework


Environmental Context
Data Gathering
Cyber Threat Intelligence Analysis
Strategic Cyber Intelligence Analysis
Reporting & Feedback
Human/
Machine

Collecting and analyzing internal and external data pertaining to specific threats to your organization and industry to inform cybersecurity operations/actions and strategic cyber intelligence analysis.

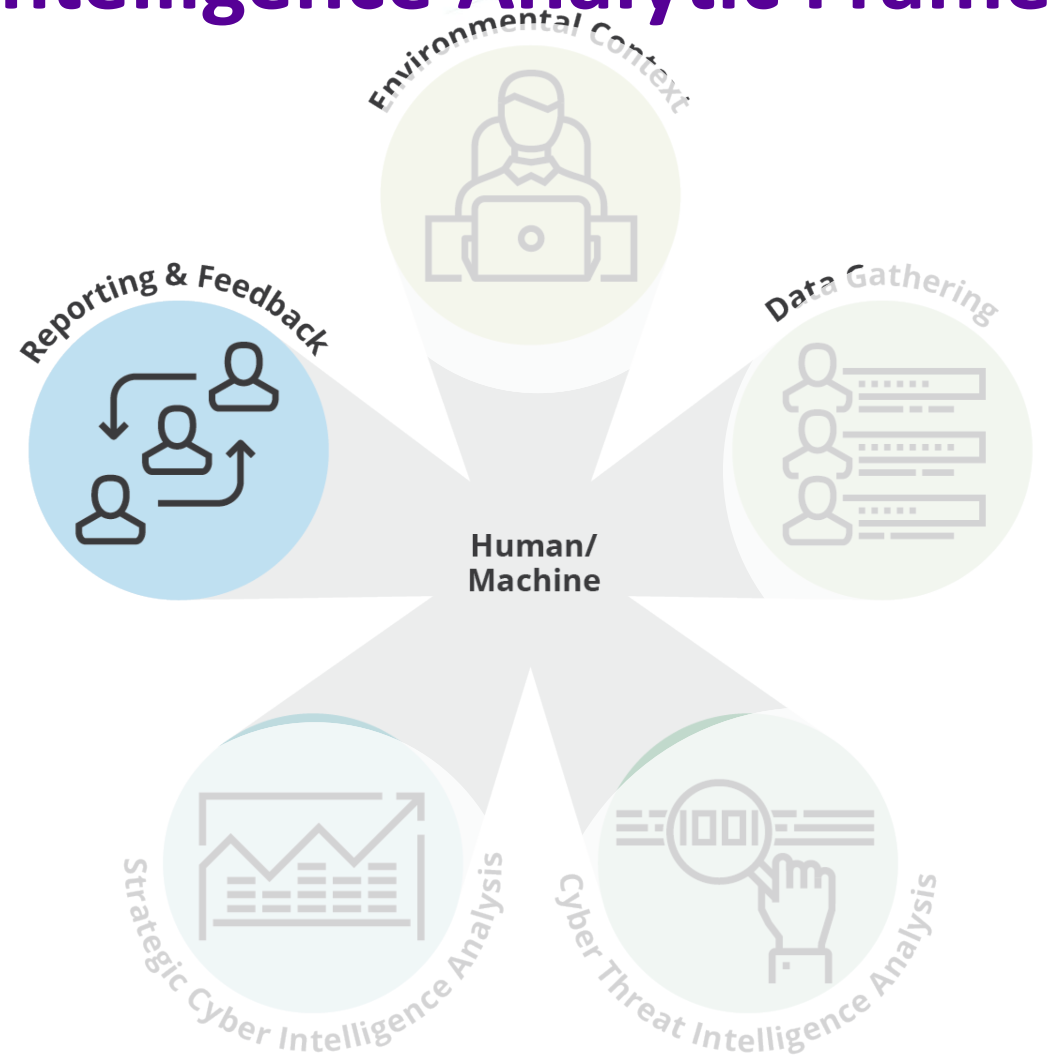
Use a Cyber Intelligence Analytic Framework


Environmental Context
Reporting & Feedback
Data Gathering
Human/
Machine
Strategic Cyber Intelligence Analysis
Cyber Threat Intelligence Analysis

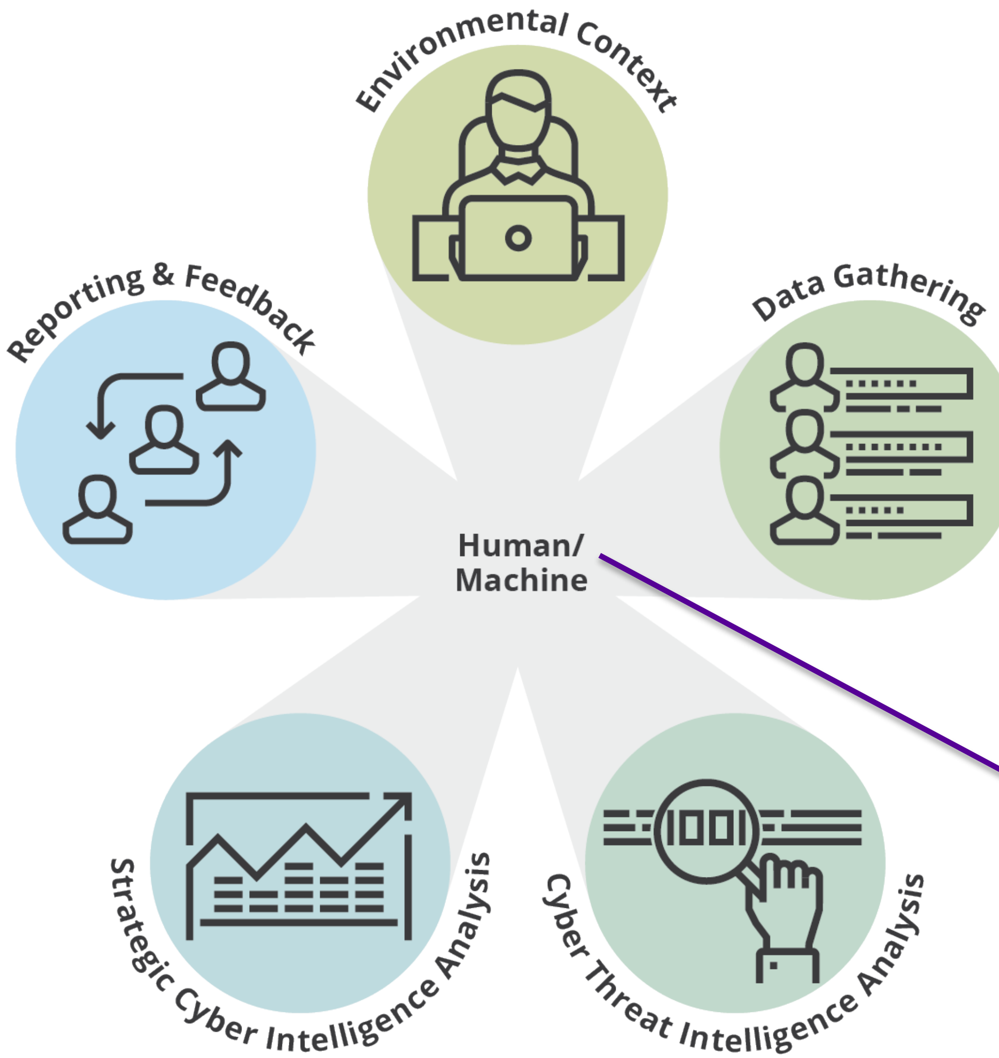
Holistically assessing threats, emerging technologies and geopolitics for risks and opportunities now and in the future.

Use a Cyber Intelligence Analytic Framework

Formal and informal **two-way** communication that helps identify intelligence requirements, intelligence gaps, concepts needing further explanation and opportunities for collaboration.


Environmental Context
Reporting & Feedback
Data Gathering
Human/
Machine
Strategic Cyber Intelligence Analysis
Cyber Threat Intelligence Analysis

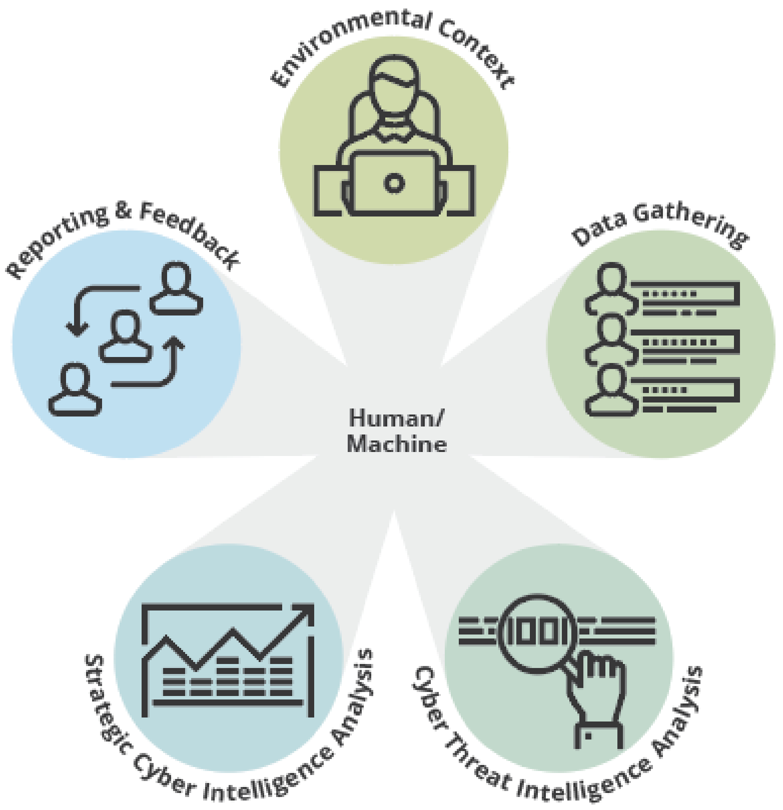
Use a Cyber Intelligence Analytic Framework


Environmental Context
Data Gathering
Reporting & Feedback
Human/
Machine
Strategic Cyber Intelligence Analysis
Cyber Threat Intelligence Analysis

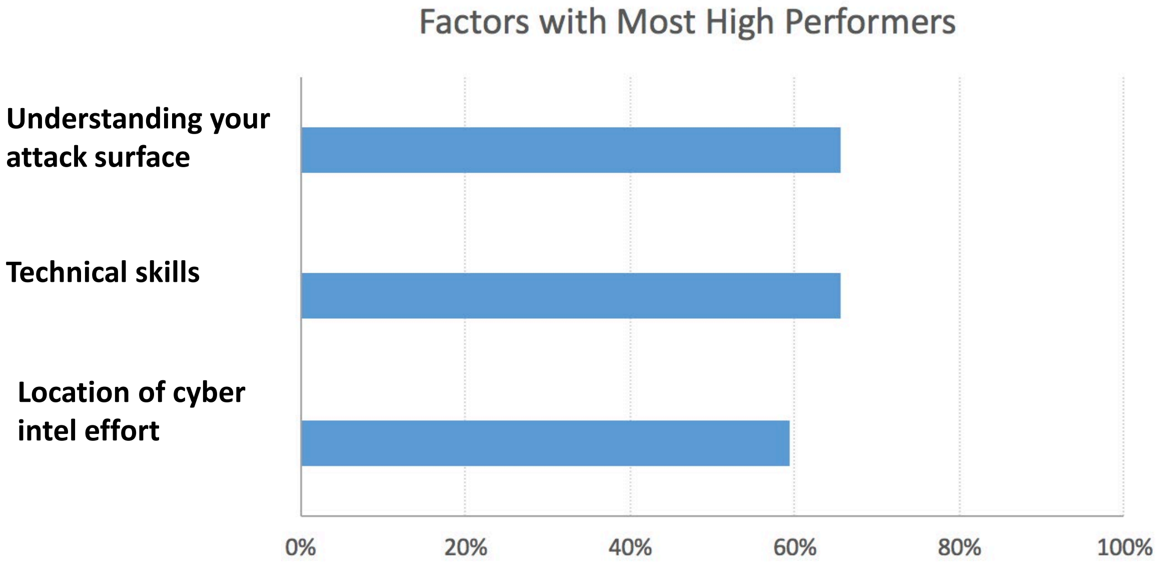
Opportunity:
Cyber intel and emerging tech

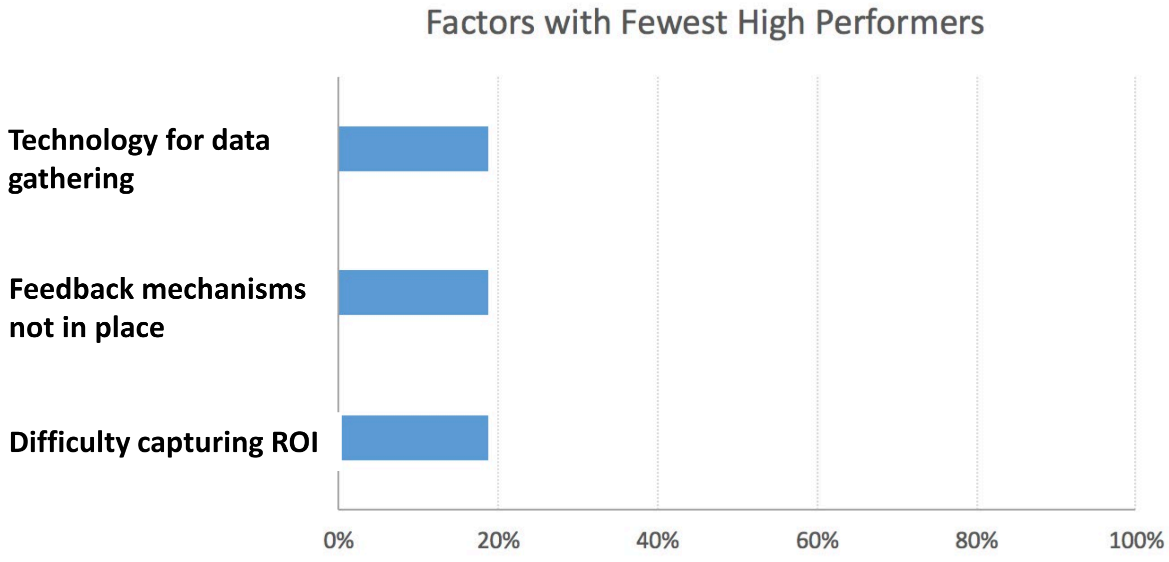
Applying AI/ML to Cyber Intelligence

- Your cyber intelligence workflow must be repeatable, consistent, and well-defined to be operationally effective.
- Machine Learning alone cannot save bad data
- Better data = simpler models

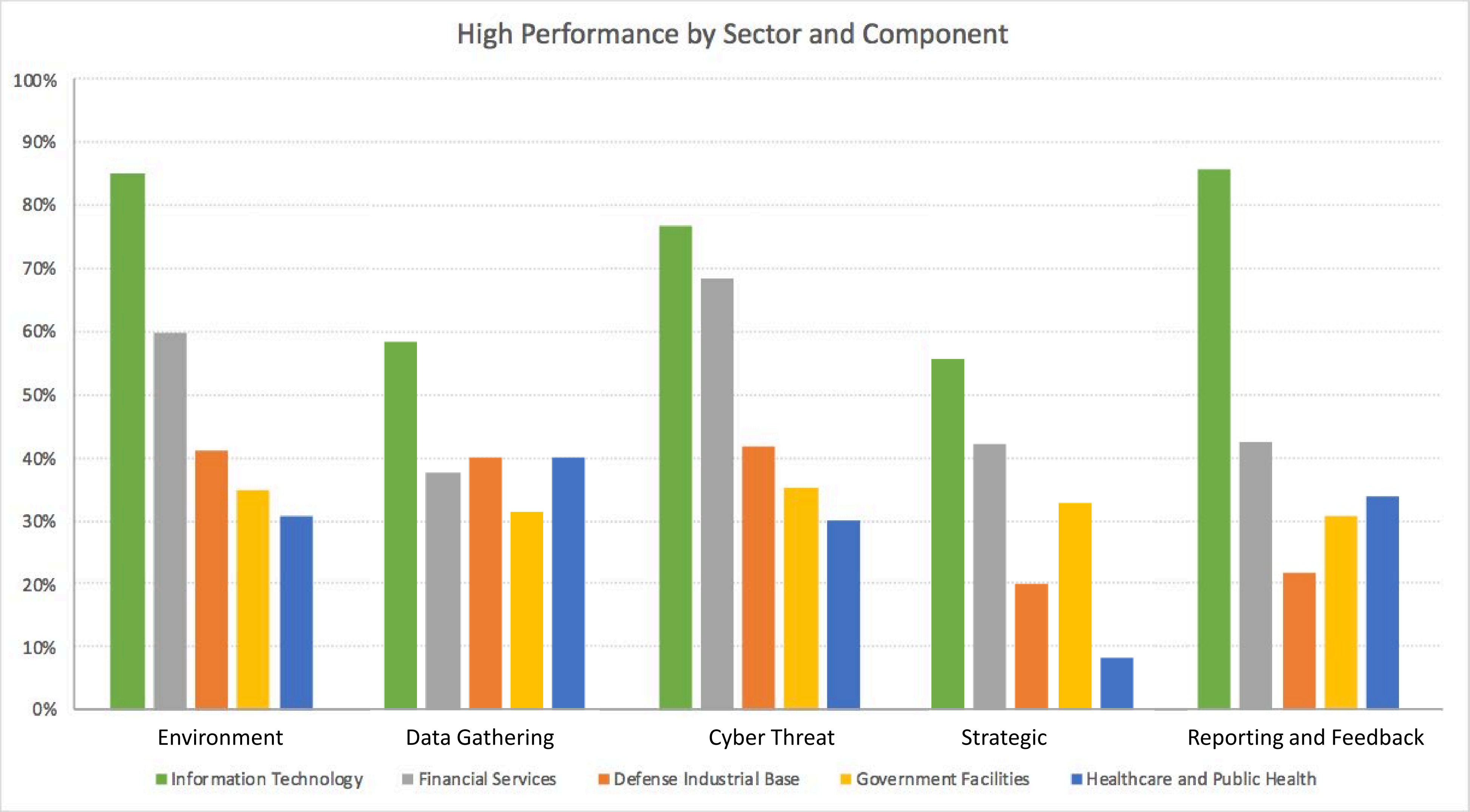

Environmental Context
Data Gathering
Reporting & Feedback
Human/
Machine
Strategic Cyber Intelligence Analysis
Cyber Threat Intelligence Analysis

Early Results:
Where are participants doing the best? The worst?





Early Results: Which sectors show high performance?



Identifying (MANY) Common Challenges and Best Practices

ENVIRONMENT

- Cybersecurity is Cyber Intelligence
- Silos of Excellence are not really excellent
- We need more people
- Challenges with recruiting and retaining people
- Team Roles and Responsibilities Unclear
- Poor Access to Decision Makers
- Cyber Intelligence Workflows are only conceptual / incomplete
- Lack of a repeatable formal threat prioritization process
- We can only focus on today
- No Insider Threat Program
- Sharing with Insider Threat Team Unidirectional

- Do a Crown Jewel Exercise
- Create a Defined Cyber Intelligence Team
- Use NIST NICE 800-181
- Elevate the CISO in the Organization
- Fusion Centers Enhance Collaboration
- Virtual or Physical Fusion Centers
- Get Serious About Physical Security
- Map data collected to Public Threat Frameworks to Answer SIRs
- Prioritize Threats based on Threat Actor Potential, Target Exposure, and Organizational Impact
- All Data All The Time
- Recognize the Importance of the Future
- Have an Insider Threat Team

DATA GATHERING

- No Information Needs and Intelligence Requirements
- Static Information Needs and Requirements
- Participation with Fusion Centers and ISACs Can't Be Just Checking the Box
- External Information Sharing: Not Where It Needs To Be
- No process for aligning data sources to Information Needs, Intelligence Requirements, and Information Requirements
- I have my sources – and don't know anything about your sources
- Using Outdated Tools and Technologies
- Data Normalization and Ingestion
- Data Source Validation

- Have a Intelligence Requirements Framework
- Create a Collection Management Team
- Beyond the Appearance of a Fusion Center
- Your Fusion Center Should Serve as Your Organization's ISAC
- Technology Advances Information Sharing
- Form an Emerging Technology Team and Automate Repeatable Tasks
- Use a wide variety of Sources
- Diversity in Tool Technology is Good
- Use Admiralty Code

CYBER THREAT INTELLIGENCE ANALYSIS

- No Formal CTIA Workflow / Email as ticketing system
- Cyber threat intelligence analysis Not Incorporated into Larger Cyber Intelligence Workflow
- Inability to Create Cyber threat intelligence analysis Reports; Reports Not Timely and Lacking Data Source Validation
- Cyber Intelligence Teams Lack Diversity in Technical Skills
- Small Cyber Intelligence Teams and Limited Opportunities for Training Hampers Effective Cyber Threat Intelligence Analysis:
- Challenges purchasing and building customized tools and technology

- SOAR Technologies Save Time and Resources
- Formulized Process to consistently Create Actionable Cyber threat intelligence analysis Reports
- Get a team with depth and breadth in technical disciplines
- Hire for 3.14
- Culture that Encourages Everyday Learning and Training
- Open-Source, Paid and Customized Tools and Technologies to support Cyber Threat Intelligence Analysis
- Machine Learning for Cyber Threat Intelligence Analysis

STRATEGIC CYBER INTELLIGENCE ANALYSIS

- SCIA A Priority for Most, Yet Implementation Challenges Remain
- No SCIA Workflow
- Not doing Cyber Attribution
- Organizations lack personnel and leadership commitment to perform SCIA
- Incorporating Diverse Disciplines to Produce Strategic Cyber Intelligence
- No SCIA Tools
- Analytical Tradecraft is What?

- Do SCIA
- Focus on Strategic Intelligence and Proactively Collaborate with other Teams
- Cyber Attribution IS Important
- Critical Thinking most valued skill for SCIA
- Have SCIA Tools
- Analytical Tradecraft IS Important

REPORTING AND FEEDBACK

- No Formal Reports Produced
- Not Doing Predictive Analytics
- Actionable Recommendations are for Cybersecurity only
- Executive Leadership (CISO and up) Not Interested in Cyber Intelligence
- Challenges Getting In Front of Leadership
- Leadership not Cyber Savvy
- Minimal Feedback Mechanism for Analysts
- No Feedback: Unclear if Cyber Intelligence Analysis Influence Leadership Decisions
- Unclear if Leadership and Consumers are satisfied with cyber intelligence reports
- Challenges Demonstrating ROI

- Diverse Product Line
- Reports are Accessible
- Actionable and Predictive Analysis
- Leadership Actively Involved
- Leadership Uses Cyber Intel to Make Decisions
- Leadership Is Accessible
- Board Involvement
- Analysts Receive Feedback
- Build Trust
- Demonstrating ROI is Easier

How you view the problem defines how you respond

Cybersecurity ≠ Cyber Intelligence

Create a distinct Cyber Intelligence Team

Conduct a Crown Jewel Exercise to Understand Your Environment

Understand Environment and Attack Surface

- Threat Actor Potential
- Organizational Exposure to The Threat
- Organizational Impact of the Threat

High-performing organizations conduct this exercise to identify

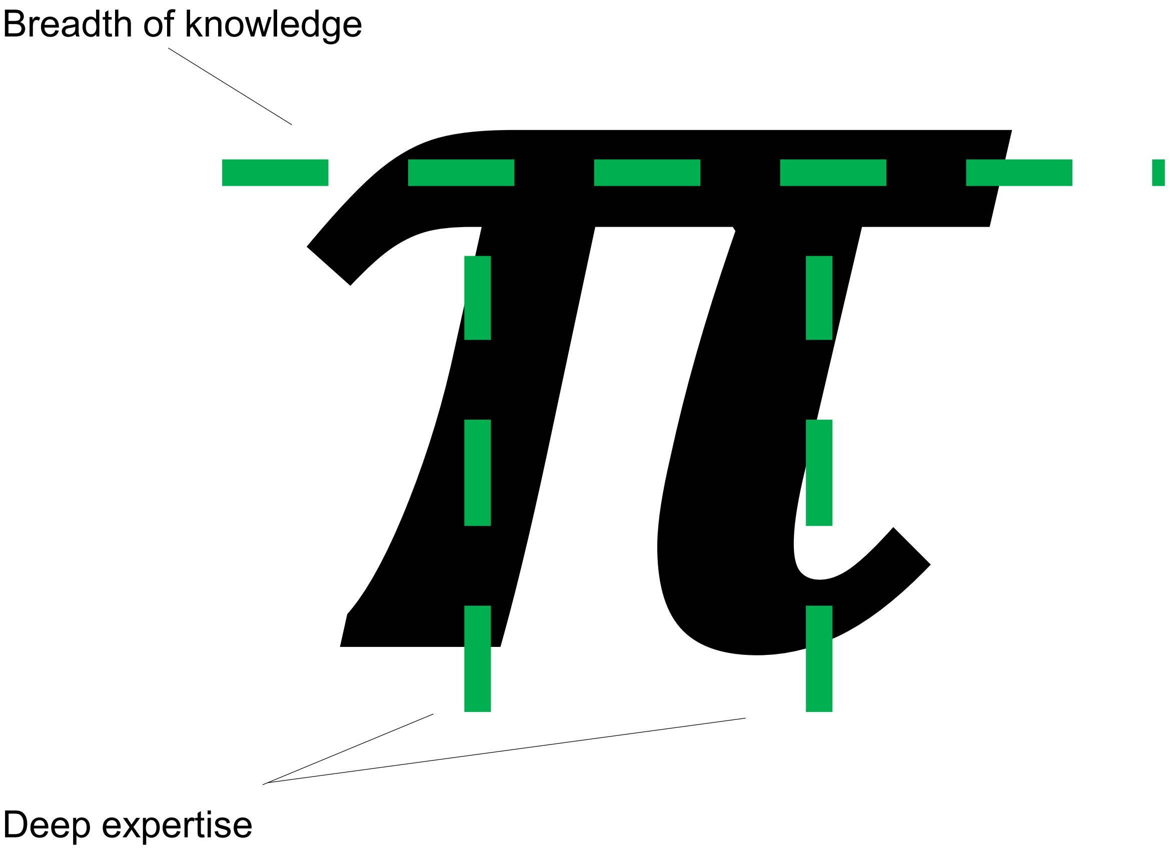
- critical assets
- owners
- risks
- interactions

Building your cyber intelligence team

“NIST NICE 800-181”

Very technical teams overall; diversity of perspective an asset

Recruiting and Retaining staff



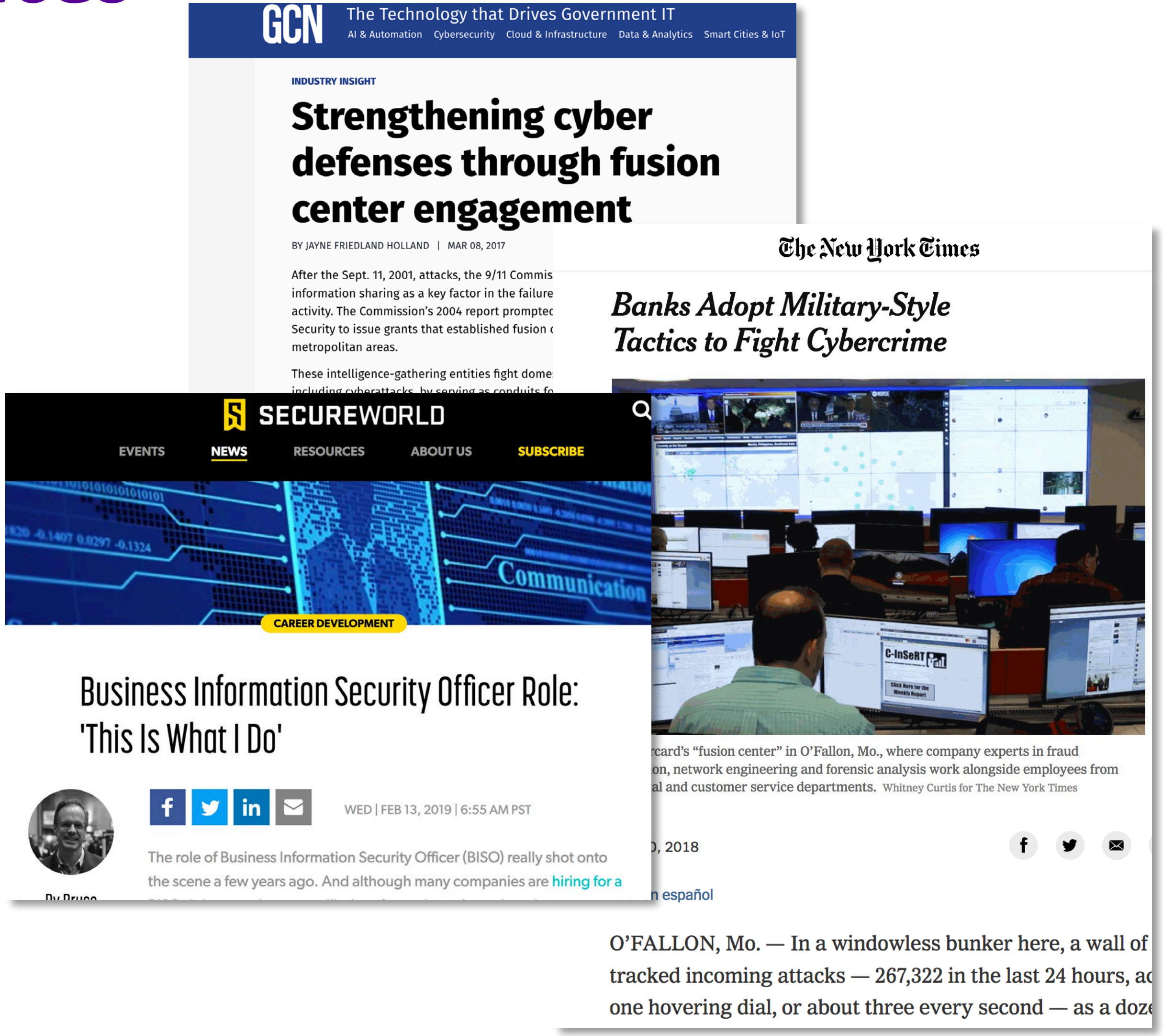
Organizations’ Tech and Practices

Fusion Centers

- pioneered by financial organizations, now being adopted in other industries
- help break down barriers, and bring in diversity of thought

Business Information Security Officers (BISOs)

- strategic viewpoint
- often go hand-in-hand with fusion centers



GCN The Technology that Drives Government IT

AI & Automation Cybersecurity Cloud & Infrastructure Data & Analytics Smart Cities & IoT

INDUSTRY INSIGHT

Strengthening cyber defenses through fusion center engagement

BY JAYNE FRIEDLAND HOLLAND | MAR 08, 2017

After the Sept. 11, 2001, attacks, the 9/11 Commis information sharing as a key factor in the failure activity. The Commission’s 2004 report promptec Security to issue grants that established fusion c metropolitan areas.

These intelligence-gathering entities fight dome including cyberattacks, by serving as conduits fo

SECUREWORLD

EVENTS NEWS RESOURCES ABOUT US SUBSCRIBE

CAREER DEVELOPMENT

Business Information Security Officer Role: 'This Is What I Do'

By Bruce

WED | FEB 13, 2019 | 6:55 AM PST

The role of Business Information Security Officer (BISO) really shot onto the scene a few years ago. And although many companies are hiring for a

The New York Times

Banks Adopt Military-Style Tactics to Fight Cybercrime

rcard’s “fusion center” in O’Fallon, Mo., where company experts in fraud on, network engineering and forensic analysis work alongside employees from al and customer service departments. Whitney Curtis for The New York Times

), 2018

n español

O’FALLON, Mo. — In a windowless bunker here, a wall of tracked incoming attacks — 267,322 in the last 24 hours, ac one hovering dial, or about three every second — as a doze

Intelligence Requirements and Collection Management Team

Organizational Intelligence Priorities Framework

Create a Collection Management Team

Intelligence Aggregator vs Intelligence Originator

Security Orchestration Automation and Response (SOAR)

- Automate Incident Response and Enrichment Tasks
- SOAR technologies can be enhanced by AI/ML

Admiralty Code for High Performance

High-performing organizations are adopting the Admiralty Code to assess the data *and* the data source.

Source Reliability

a.	Reliable
b.	Usually Reliable
c.	Fairly Reliable
d.	Not Usually Reliable
e.	Unreliable
f.	Cannot Be Judged

Information Credibility

1.	Confirmed
2.	Probably True
3.	Possibly True
4.	Doubtfully True
5.	Improbable
6.	Cannot be Judged

Strategic Cyber Intelligence Analysis

- Attribution enables organizations to **anticipate and not always be on defense**
- It's about both threats AND opportunities
- Only some organizations are doing strategic cyber intelligence analysis

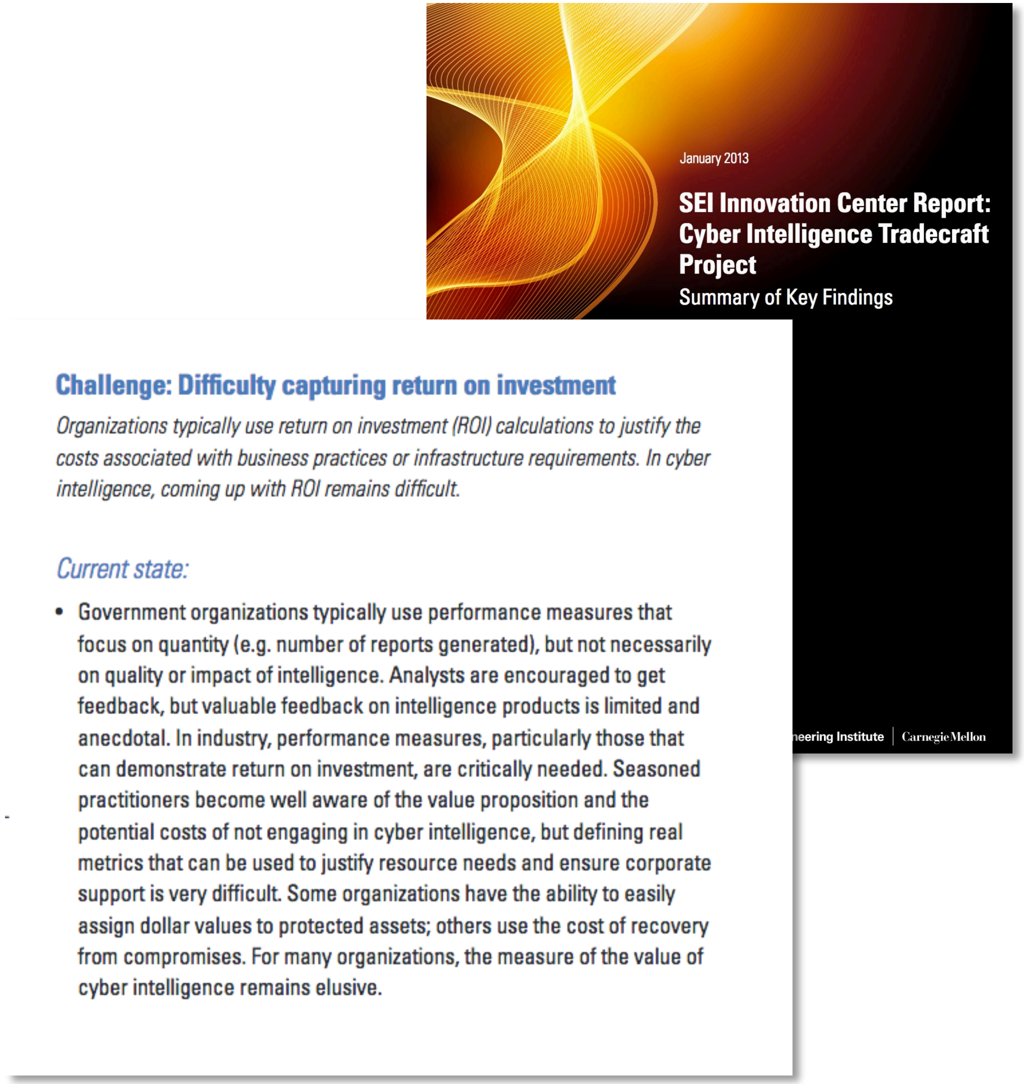
Traits, Core Competencies and Skills

Strategic Cyber Intelligence Analysts:

- Critical Thinking – Problem Solving skills
- Communication Skills

Reporting and Feedback

- Type/frequency of reports
- Leadership involvement/ Getting the word out
- Demonstrating ROI is getting better, room for improvement



January 2013

SEI Innovation Center Report: Cyber Intelligence Tradecraft Project

Summary of Key Findings

neering Institute | CarnegieMellon

Challenge: Difficulty capturing return on investment

Organizations typically use return on investment (ROI) calculations to justify the costs associated with business practices or infrastructure requirements. In cyber intelligence, coming up with ROI remains difficult.

Current state:

- Government organizations typically use performance measures that focus on quantity (e.g. number of reports generated), but not necessarily on quality or impact of intelligence. Analysts are encouraged to get feedback, but valuable feedback on intelligence products is limited and anecdotal. In industry, performance measures, particularly those that can demonstrate return on investment, are critically needed. Seasoned practitioners become well aware of the value proposition and the potential costs of not engaging in cyber intelligence, but defining real metrics that can be used to justify resource needs and ensure corporate support is very difficult. Some organizations have the ability to easily assign dollar values to protected assets; others use the cost of recovery from compromises. For many organizations, the measure of the value of cyber intelligence remains elusive.

Apply - Do This

Next week you should

- Advocate for a Cyber Intelligence Team

In the first three months following this presentation you should

- Use NIST NICE 800-181
- Start a crown jewel exercise
- Start to create a Fusion Center

Within six months to a year you should

- Form Collection Management Team
- Incorporate the Cyber Intelligence Analytic Framework
- Adopt NATO or Admiralty Code Grading System

Cyber Intel Analysts: Please do this all the time…

- Believe in your own professional judgments
- “People don’t care how much you know, until they know how much you care.” - John C. Maxwell
- It’s better to be mistaken than to be wrong
- Feedback is a gift
- Write the memo

MORE FIGHTING AND I LOST

Jared Ettinger
Cyber Intelligence Researcher
jeettinger@sei.cmu.edu

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.