Cyber Operations and Intelligence Essentials

LEADERSHIP TRACK

Bob Stasio, CISSP
Dreamit Ventures – Managing Director, SecureTech

Oct 2018 v4

About Me

Bob Stasio:

- Former US Army Captain
- Two Iraq deployments, MI Officer
- Former NSA Cyber Chief
- Cyber Wargame Consulting
- Bloomberg Head of Threat Intelligence
- IBM Threat Hunting Product Dir.

Looking For:

- Security Startups
- Immersion Partners
- Other Investors

@dreamit

Dreamit

SecureTech

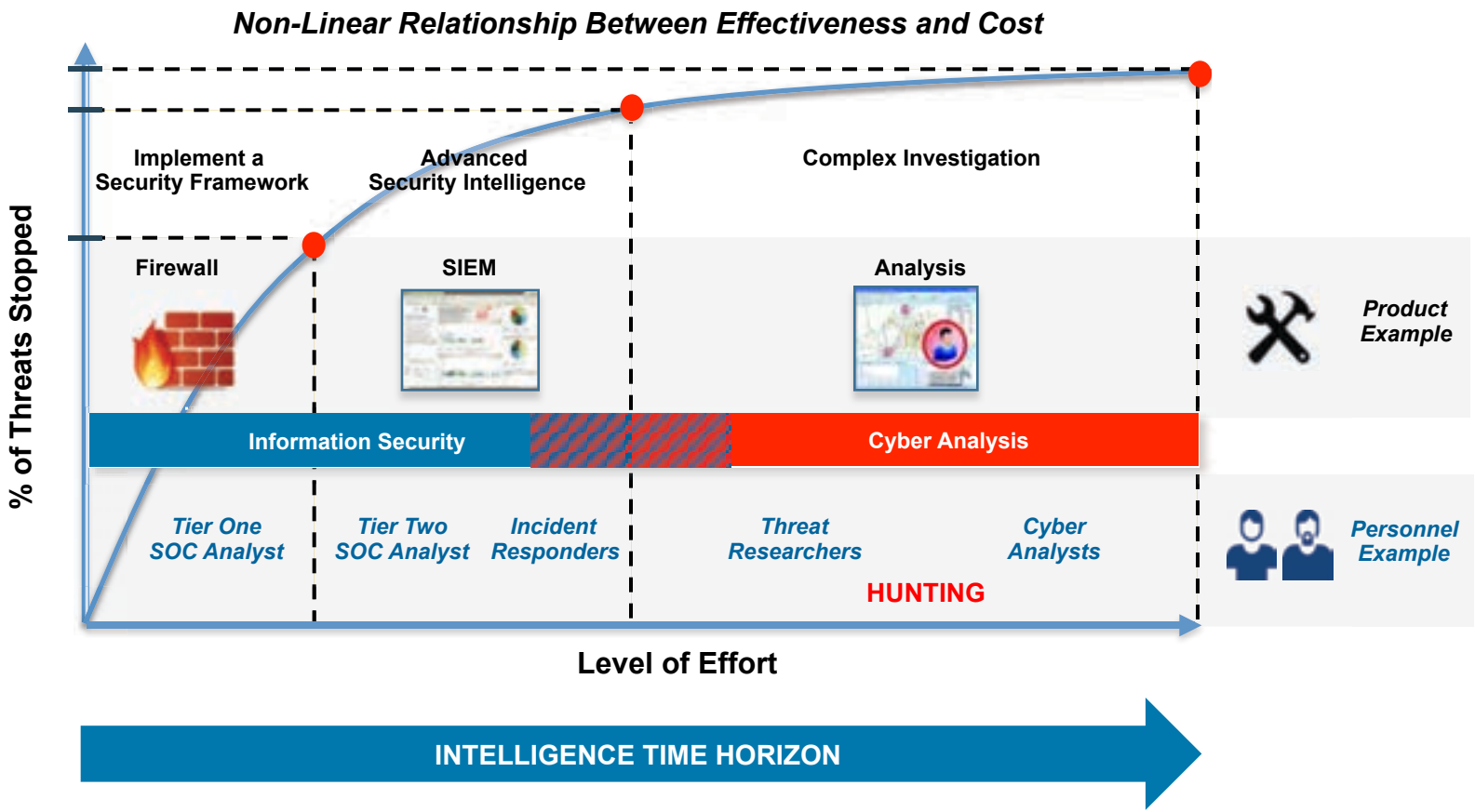
Cameron Watts, Program Manager
cameron@dreamit.com

Bob Stasio, Managing Director
bob@dreamit.com

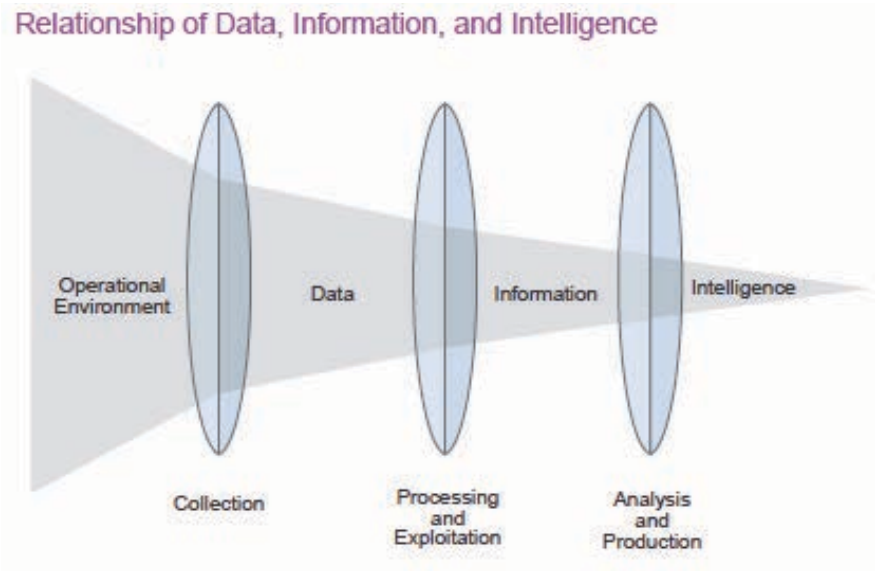
Section 1:
Objectives of Threat Hunting

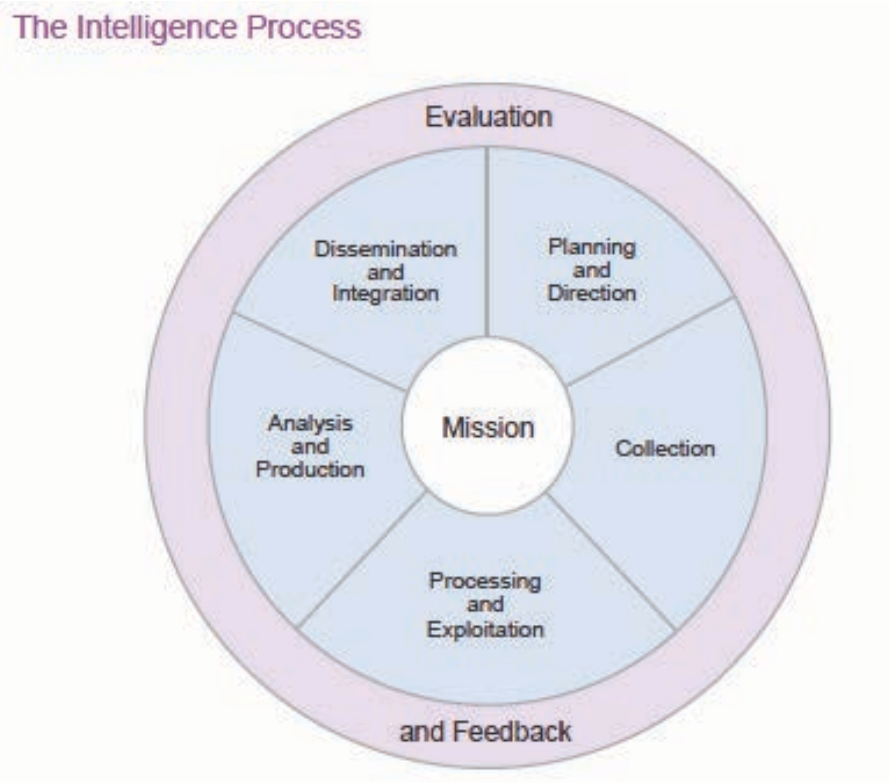
Dwell Time Examples

Cyber Analysis and Threat Hunting

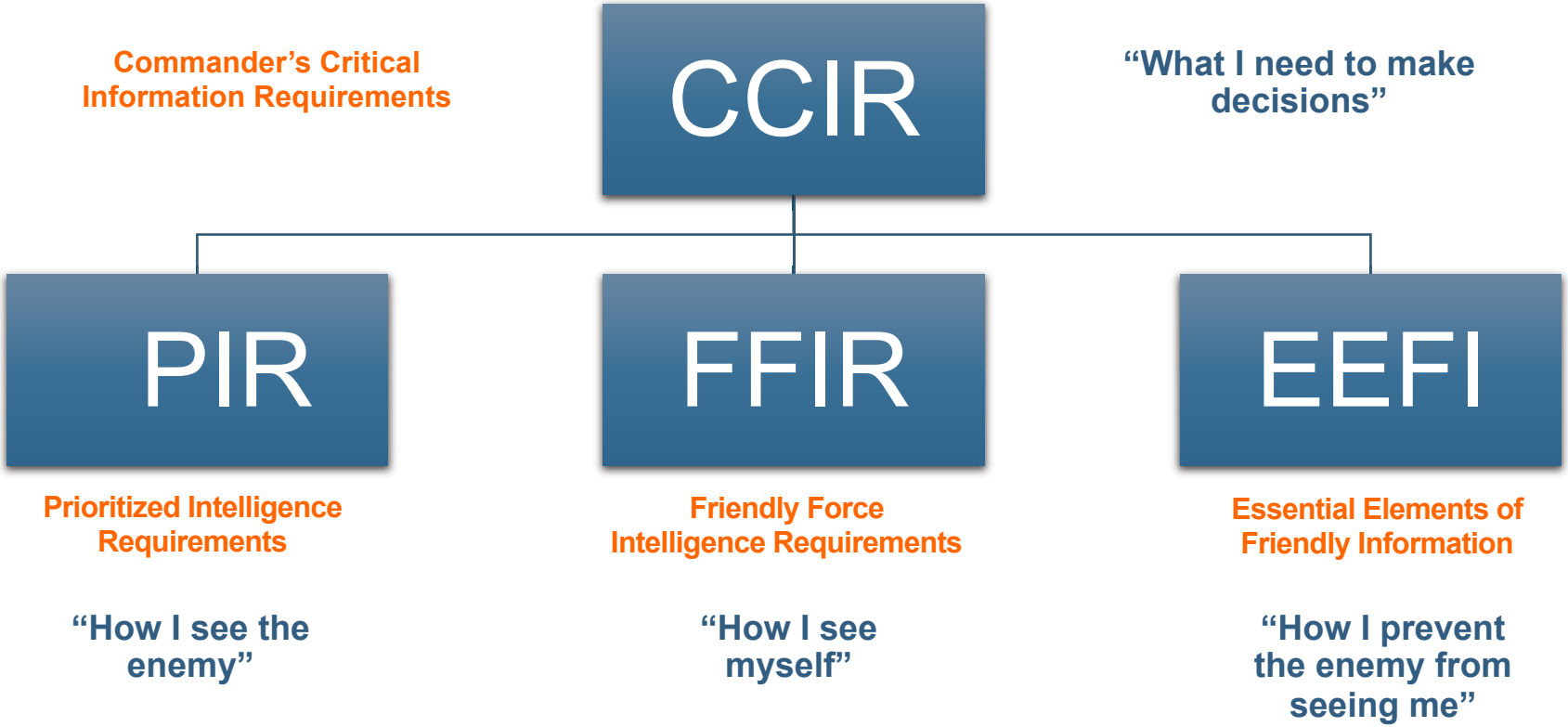


The Intelligence Cycle

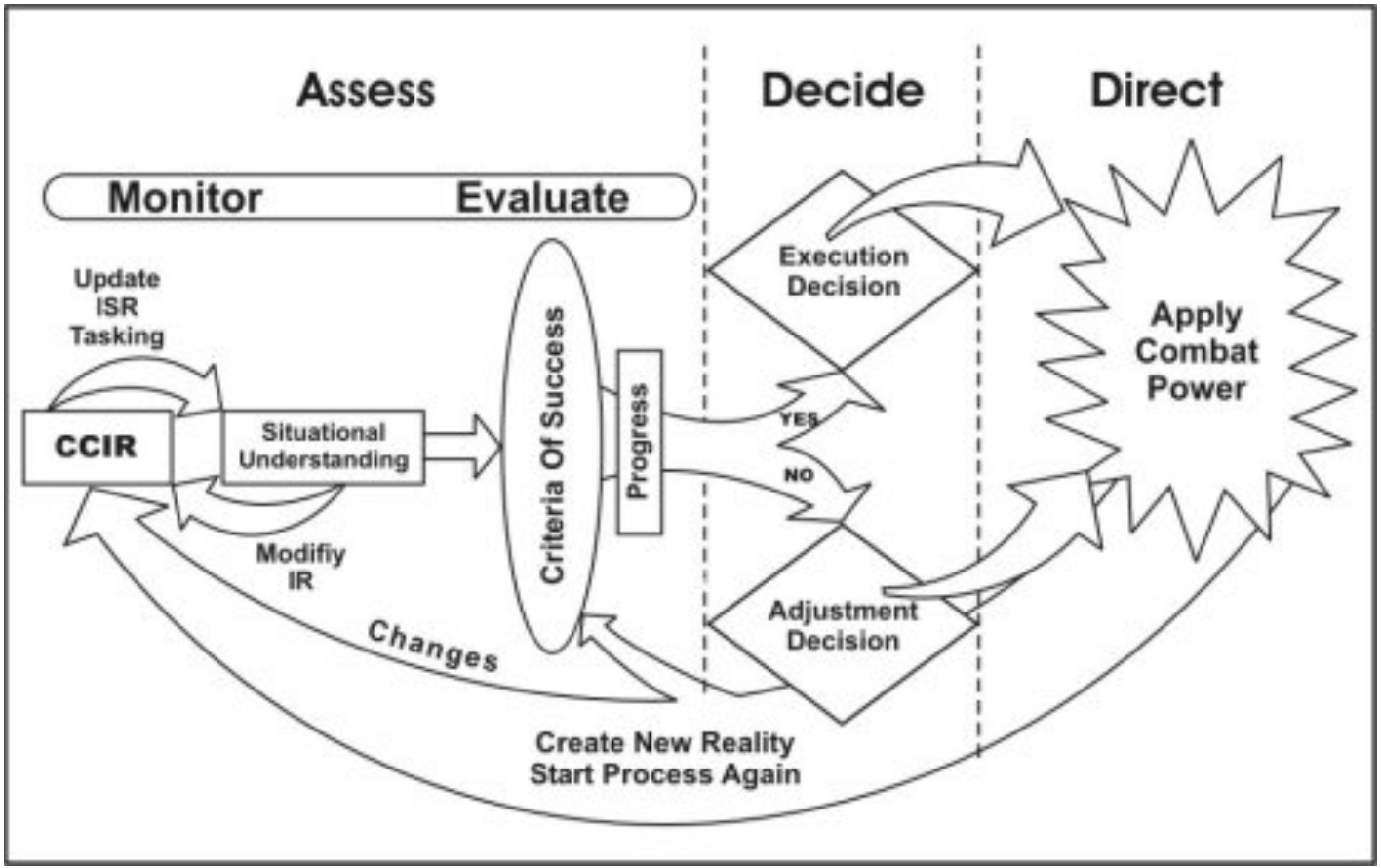




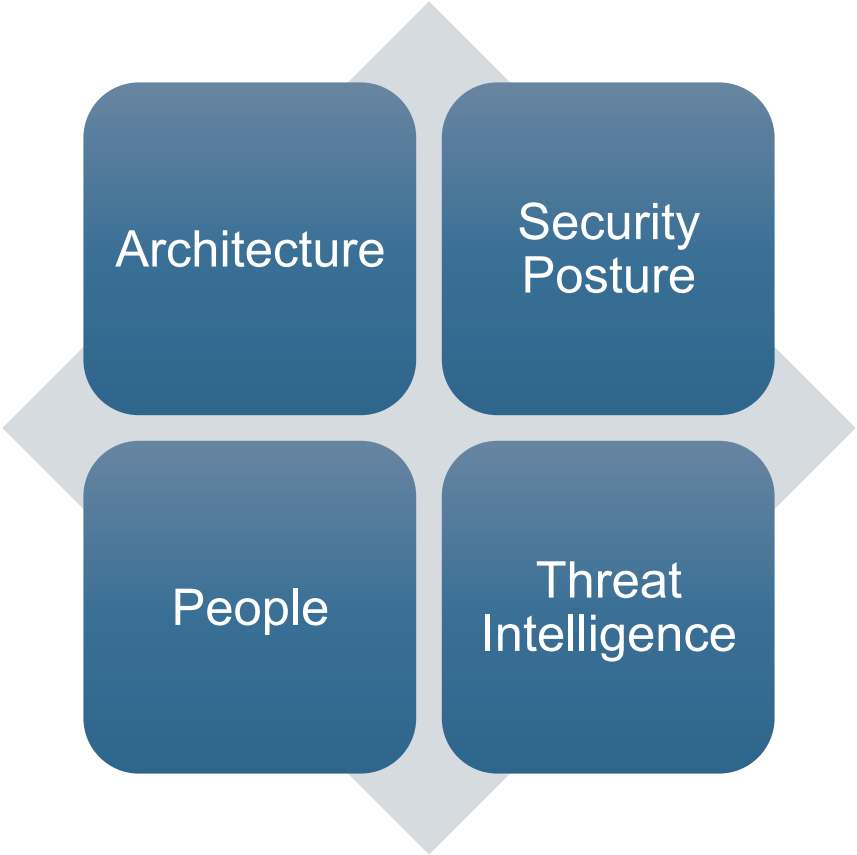
Commander's Critical Information Requirements



How CCIR Impacts Decisions



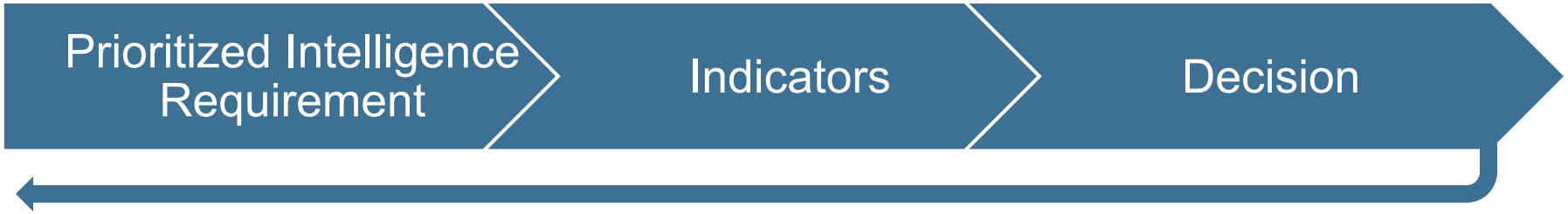
How to Determine PIRs



What is a Prioritized Intelligence Requirement (PIR)

A PIR is a question which drives intelligence collection, whose answer will ultimately drive a decision affecting the success of an organization

The PIR process derives elements for analysts to search for with their limited resources



Ask a question

Derive things to look for

Take action and refine

Example:

"Are there radical groups planning attacks against landmarks in New York?"

- **Mention of landmarks by people on a watchlist**
- **Mention purchasing explosive material**

A Law Enforcement organization could take action to interview suspect or add protection to a New York City landmark

Cyber PIRs

What software or updates have the potential of enterprise-wide proliferation like M.E.Doc? What software which has automated updates that can cause system wide infection?

Is their any activity on the darkweb indicating a new variant of NonPetya or similar ransomware?

Are all the administrators practicing least privilege access in the case of account compromise?

Are their indications of a similar nonPetya ransomware attack against similar companies?

What new proliferation techniques for ransomware are being discussed on the darkweb?

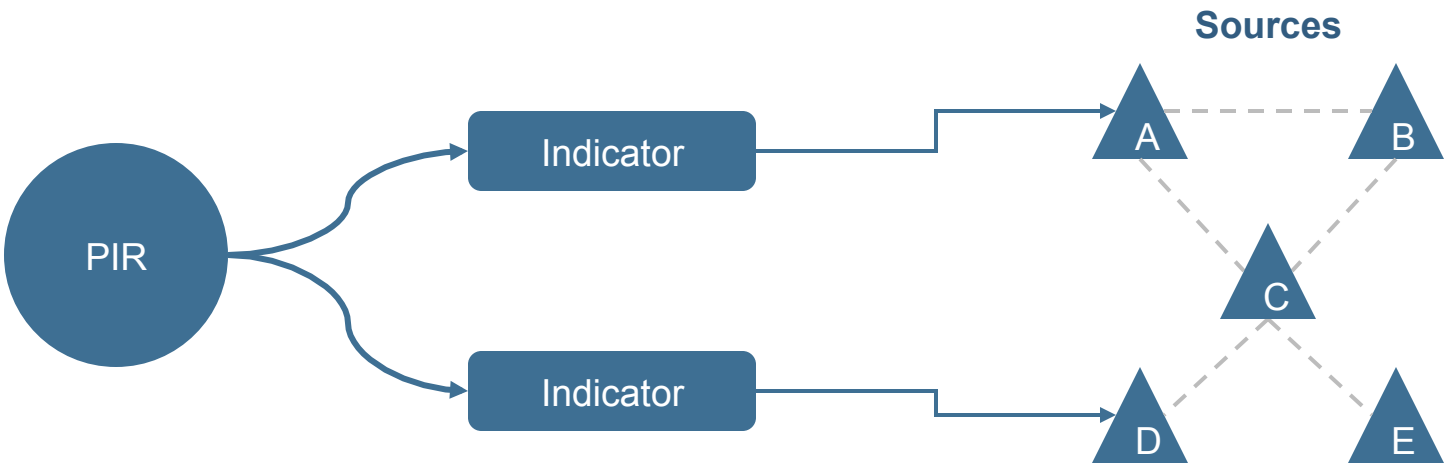
Is there evidence of additional weaponized rasnsomware leveraging Equation Group exploits?

Experts believed nonPetya was a politically-motivated attack against Ukraine by Russia, since it occurred on the eve of the Ukrainian holiday Constitution day and was targeted against an Ukrainian software company. Are there global or geopolitical events that may precipitate an additional attack from Russia state actors?

Simple PIR Matrix

Prioritized Intelligence Requirement (PIR)	Indicator	Named Area of Interest (NAI)	Last Time Information of Value (LTIOV)	Reporting
Is there evidence of additional weaponized rasnsomware leveraging Equation Group exploits?	External: community discussion, DW planning, Internal: scanning, related open ports, creation of certain files	Darkweb intelligence feeds, community forums, NW data, VM data	N/A	CCIR#3, FPCON Bravo
Are their indications of a similar nonPetya ransomware attack against similar companies?	External: pharma reporting issues, LE alerts, Internal: similar scans, targeted industry phishing attacks	Darkweb intelligence feeds, community, FBI, DHS, forums, NW data, VM data, Proofpoint	N/A	CCIR#4, FPCON Bravo

Collection Management



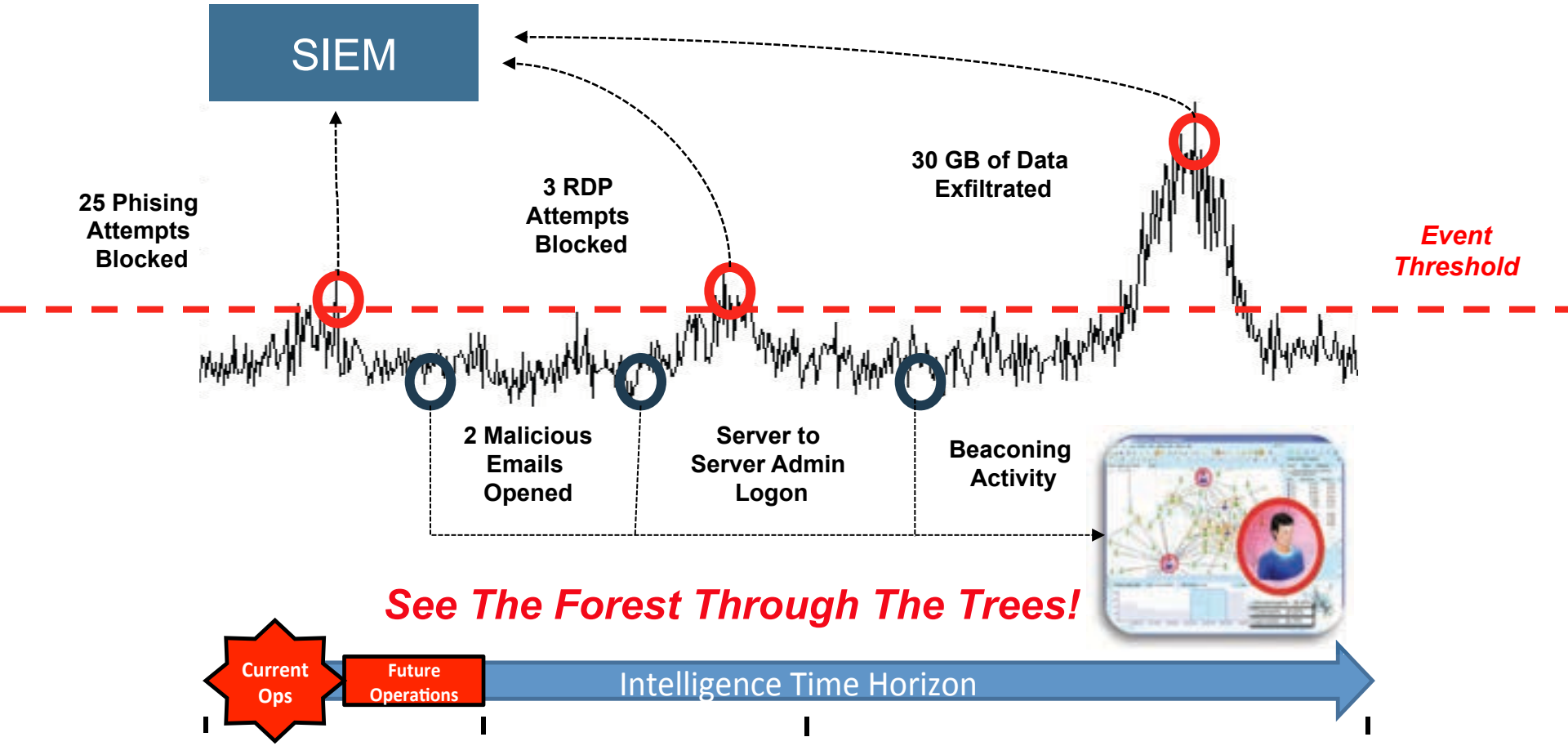
Information Sources:

- Internal
- Purchased
- Open Source
- Government
- Consortium
- Community

✓ Timely
✓ Actionable
✓ Relevant
✓ Integration

Section 2:
Building a Hunting Platform

Tipping, Queuing, and Anomaly Research Example



Why abstraction? **Data variety demands new thinking**

abstract

specific

Contextual Model

Models at this level of abstraction are **unlikely to change** unless the scope or operating environment changes significantly.

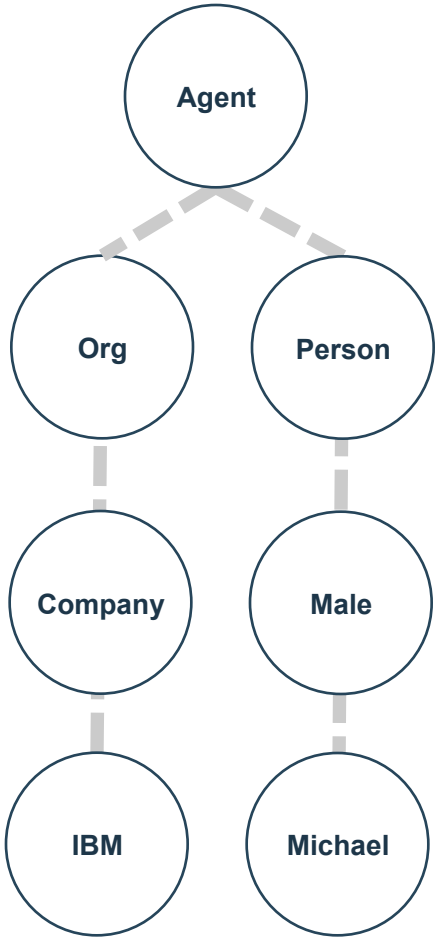
Conceptual Model

Models at this level of abstraction are **unlikely to change** unless the entity of interest itself fundamentally changes.

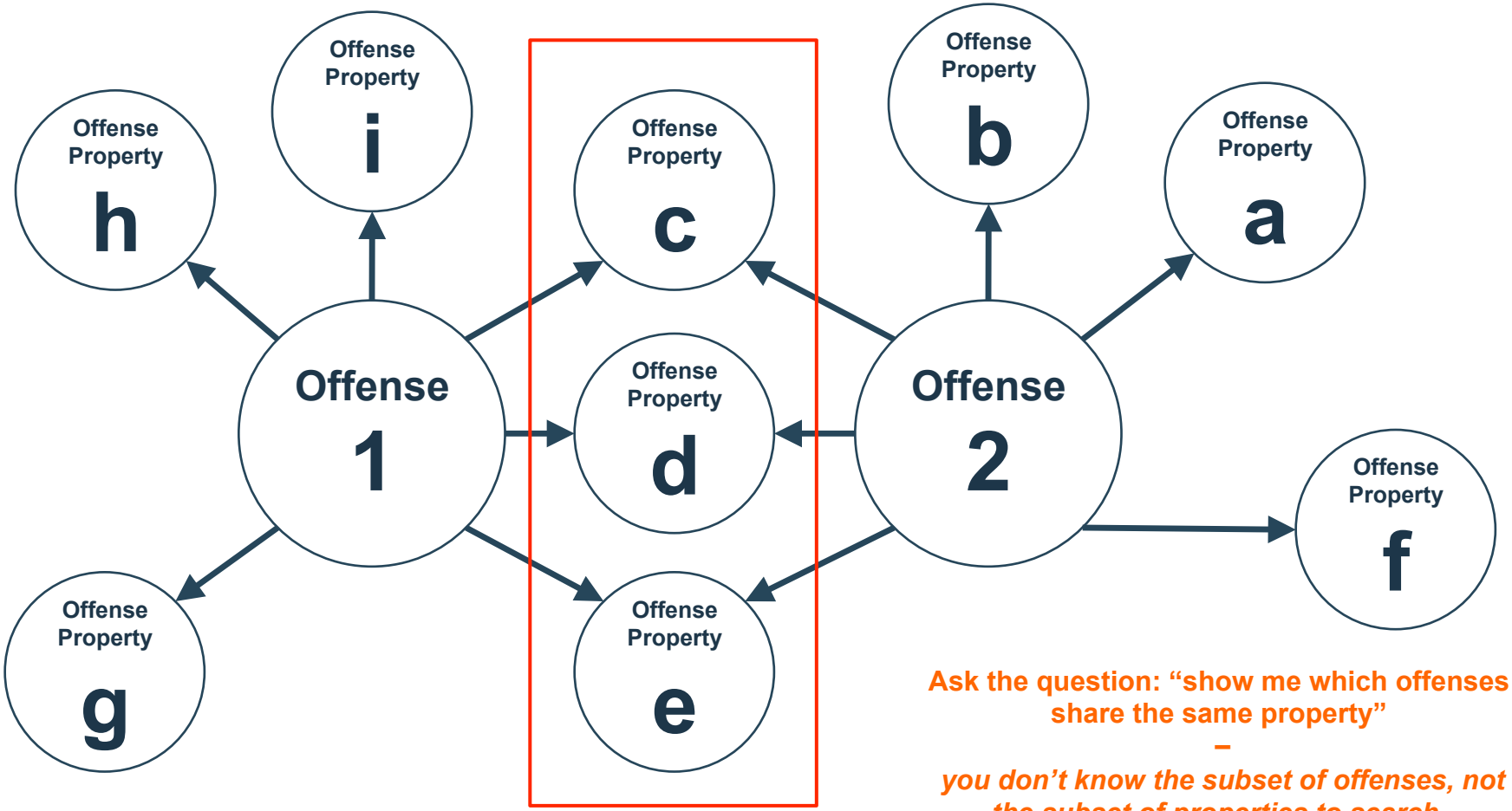
Logical Model

Models at this level of abstraction are reflect the differences between current and target state design and may support multiple Physical Models.

Physical Model



What is an Unknown Unknown Search



Ask the question: "show me which offenses share the same property"

–

you don't know the subset of offenses, not the subset of properties to search

Entity, Link or Attribute: **What drives the Data Model?**

Question:

Why do you model data as
an **Entity**?
a **Link?**
or as a **Property**?

Entity, Link or Attribute: **What drives the Data Model?**

Answer:

1. Questions (What are you trying to ask?)

2. Type of Analysis (Criminal, Intel, Fraud)

3. Volume of Data (1k, 10k, 10M, 10B, 10T)

Threat Hunting Concept Flow

Data Sources

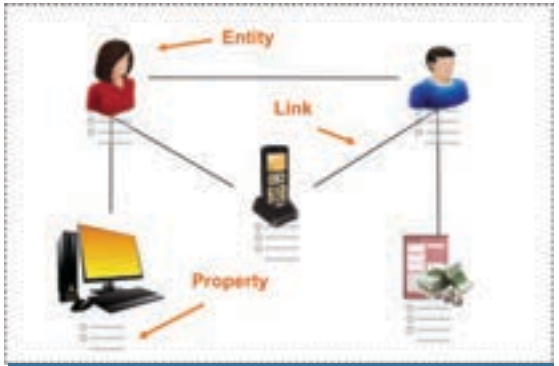
Security

Network

Endpoint

External

Graph Data

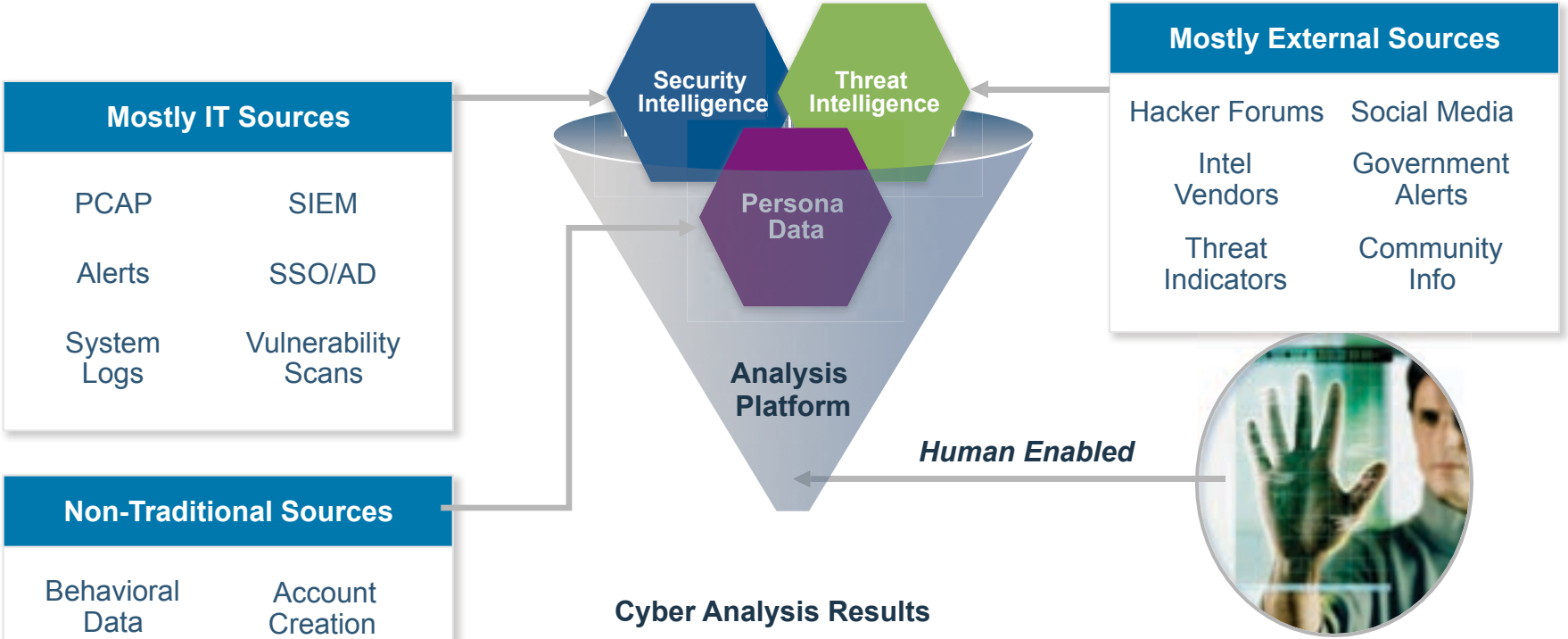


Hunting Data Model

Analytics Engine
Cognitive Engine
Rules Engine

Analysis

Centralized Data Consumed by All Sources



Cyber Analysis Results

- Integrated data feeds
- Enterprise awareness
- Compliance monitoring
- Threat discovery
- Risk management
- Enable decisions

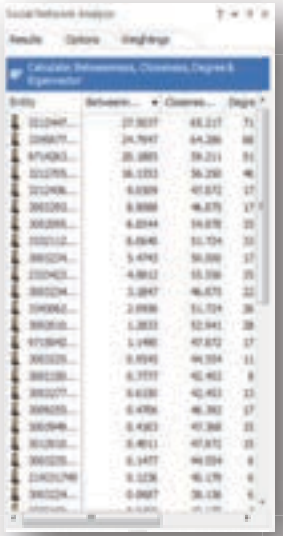
Leveraging an analytical platform and internal and external information feeds, Cyber Analysts can help form a deep understanding of the threats targeting your organization

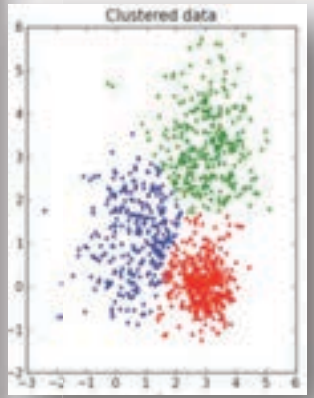
22

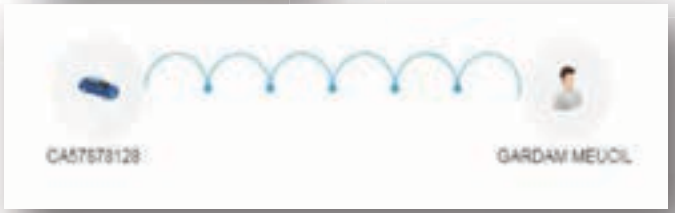
What is Needed to Conduct Threat Hunting

Anomaly / Behavioral Analytics Categories

MATHEMATICS







RULES ENGINE

CHANGE DETECTION

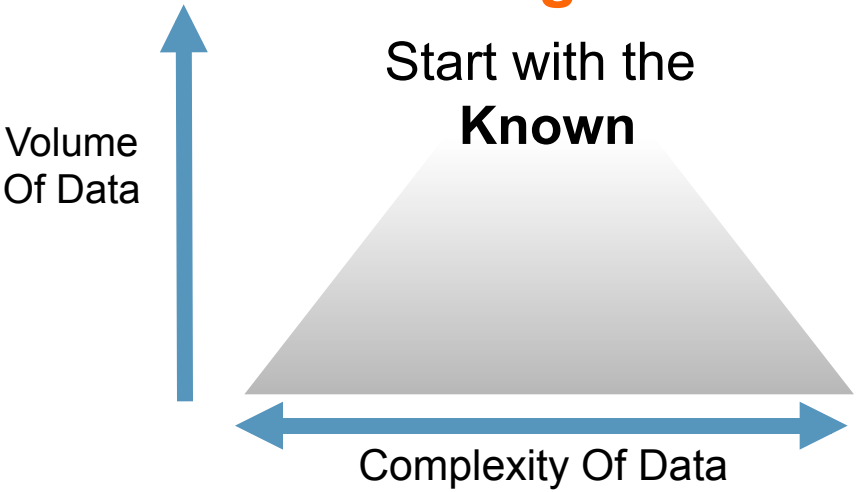
Key Differentiators of Threat Hunting Platform

For Advanced Users
Tier 3, Threat Hunters

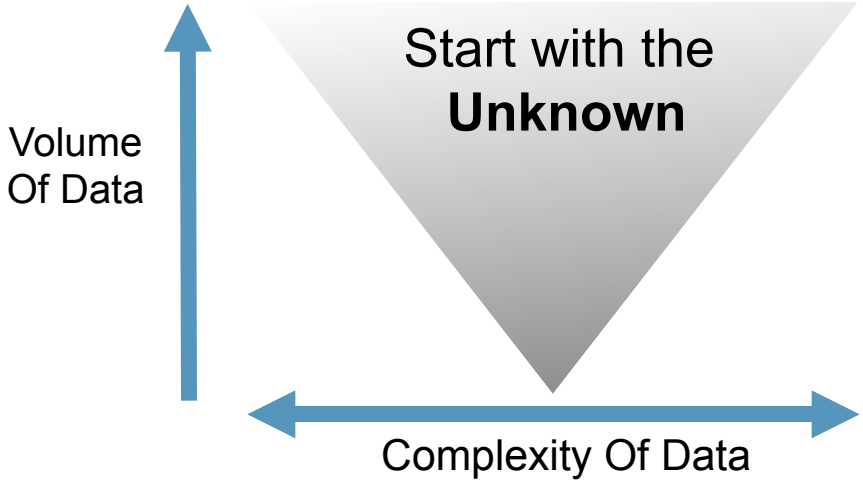
We Do Investigations
Human in the Loop

Non-Cyber Datasets
Physical, HR, Dark Web

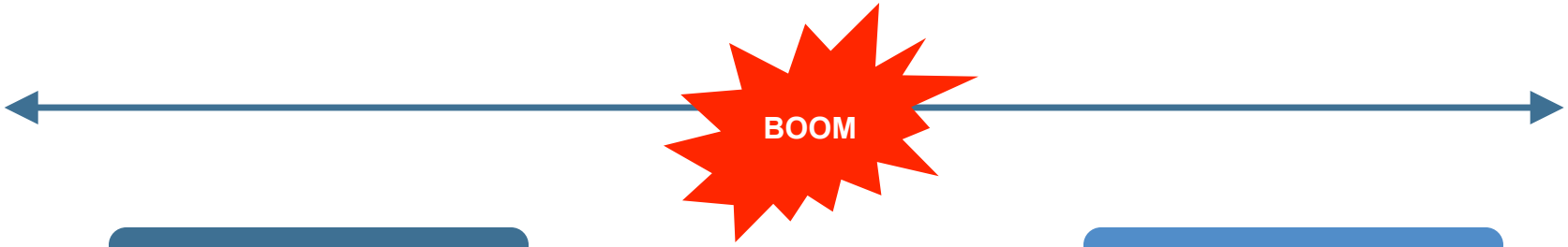
Investigations



Hunting



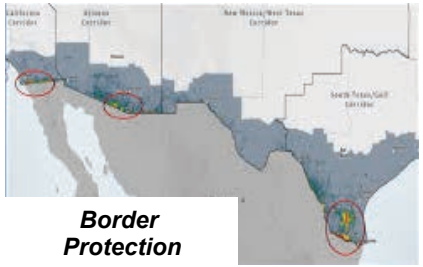
Use Case Overview



- APT Threat Detection
- Data Breach Detection
- Malware Detection
- Insider Threat

- Alert Triage
- Incident Investigations
- Threat Intel Analysis
- Situational Awareness

Intelligence Concepts are a Spectrum of Value

Concept	Value	Description	Analogy
Optimizing	Decreasing time to know, prioritizing indicators	• Seeing obvious issues from different angle • Creating efficiencies in other tools/domains • Tuning alerts to appropriate threshold • Understanding most important alerts • Connecting multiple events and alerts	 ***Alert Fatigue***
Force Multiplier	Understand trends and patterns, indicators	• Discover patterns and trends over time • Direct valuable resources for max impact • Automate ingest, searches, functions • Tip other collection sources using intel • Pinpoint problem areas with analytics	 ***Border Protection***
Predicting	Taking advantage of anomalies, preempting adversary action	• Advanced differentiated information • Using indicators to predict adv. Action • Discovering anomalies as key indicators • Stopping adversary before reaching goal • Understanding trends and how they impact	 ***Market Prediction***

Section 3:
Building a Team & Products

Building the Team

Strategy and Requirements

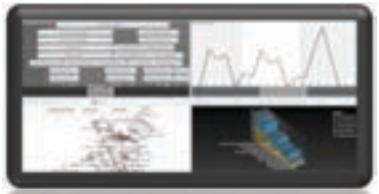
- Cyber wargame
- Identify requirements
- Identify critical structures

Capability Gap Assessment

- Adversary approach
- Gap assessment
- Social eng. assessment

Tool and Data Assessment

- Data source review
- Acquire new tools
- Acquire ext. data sets



Team Structure Build

- Define Intel cycle
- Create program SOP
- Complete strategy

Operational Implementation

- Operational training
- System optimization
- Program evaluation

Phase 1:
Development of a Team Strategy

- Step 1: Strategy and Requirements
- Step 2: Threat Based Gap Analysis
- Step 3: Tool and Data Assessment
- Step 4: Team Structure Build

Phase 2:
Implementation

- Step 1: Training Development
- Step 2: Process Development
- Step 3: Evaluation

Timeline

*Start Date - TBD

Strategy and Requirements → Gap Analysis → Tool and Data Assessment → Team Structure Build → Team Implementation

PHASE I

PHASE II

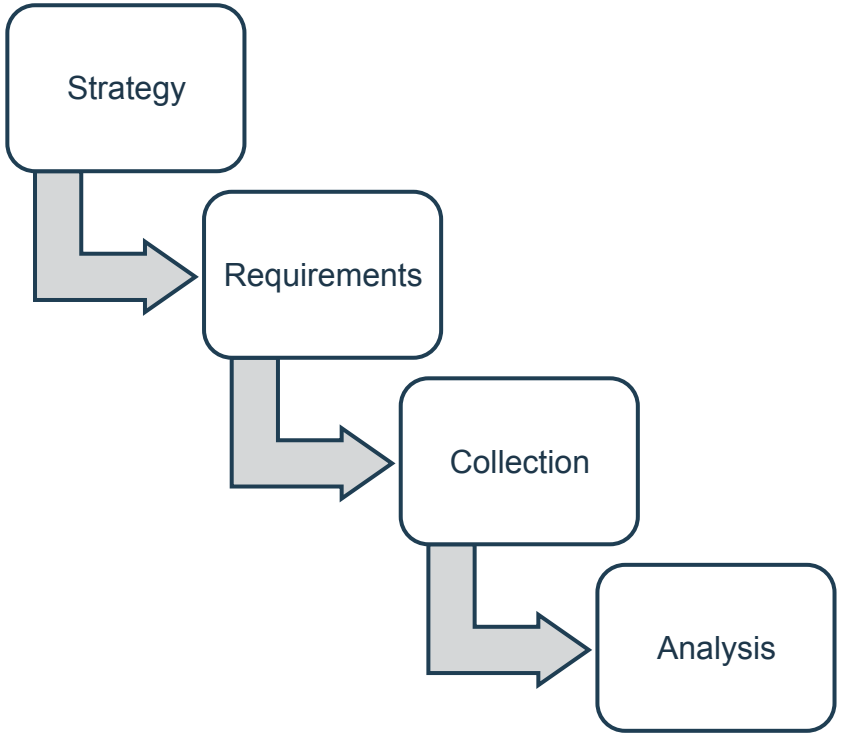
Training Dev. 6 weeks	• 2 x Trainer lv. 2 • 1 x Technical Writer
Process Dev. 5 weeks	• 2 x Analyst lv. 1
Evaluation 6 weeks	• 2 x Ethical Hacker lv. 1 • 2 x Analyst lv. 1

Strategy and Requirements: 2 Weeks

OBJECTIVES:
- **Define Customer's Knowledge Requirements**
- **Define Highly Sensitive Information**
- **Define Threat Intelligence Requirements**

METHODOLOGY:
- **Leadership Interviews**
- **Research**
- **Cyber Wargame**

DELIVERABLES:
- **Strategy Report**
- **Cyber Wargame**
- **Briefing**

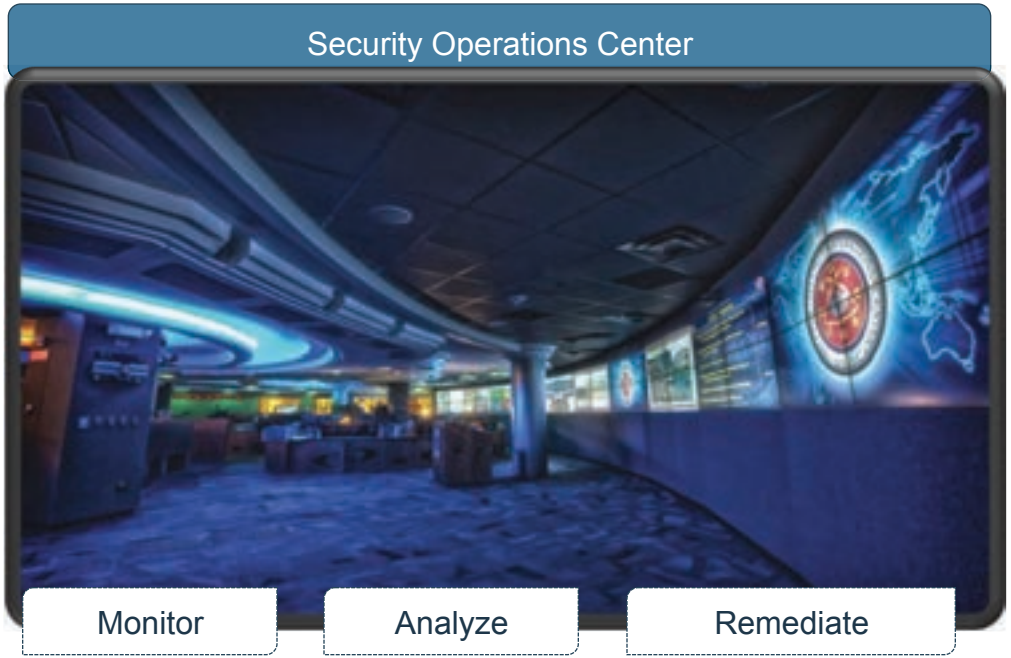


Capability Gap Assessment: 4 Weeks

OBJECTIVES:
- **Security Operations Center Objective Creation**
- **Review Current Security State (People, Process, Technology)**

METHODOLOGY:
- **Leadership Interviews**
- **Operator Interviews**
- **NOC Observation**
- **Procedure Review**

DELIVERABLES:
- **Report**
- **SOC Graphic**
- **Briefing**

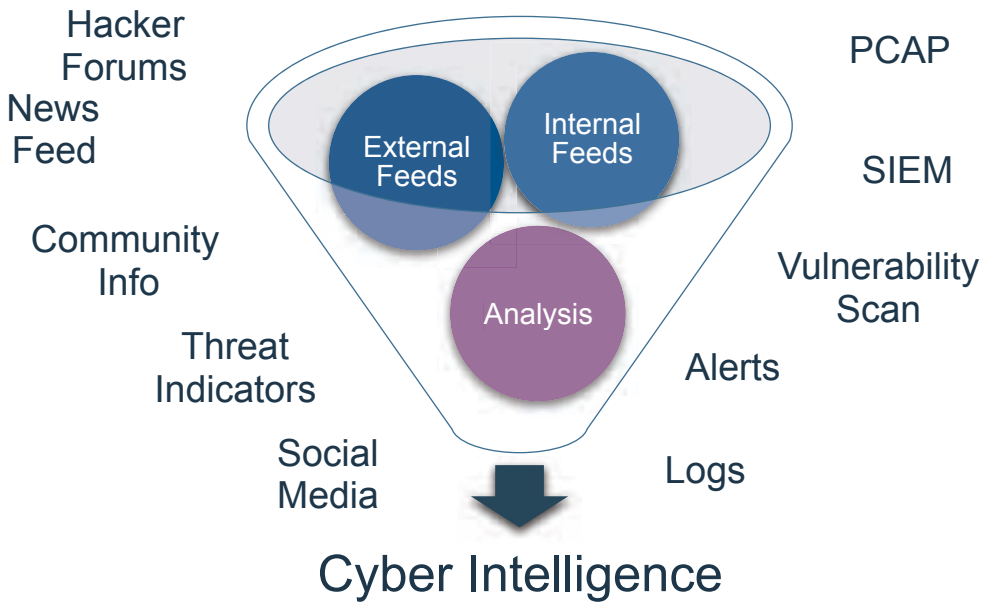


Tool and Data Assessment: 4 Weeks

OBJECTIVES:
- **Assess Data Feeds**
- **Assess Security Tools (collecting, sharing, analytic)**
- **Assess Operator Skillset**

METHODOLOGY:
- **Leadership Interviews**
- **Operator Interviews**
- **NOC Observation**
- **Procedure Review**

DELIVERABLES:
- **Report**
- **Decision Matrix**
- **Tool Recommendations**
- **Briefing**

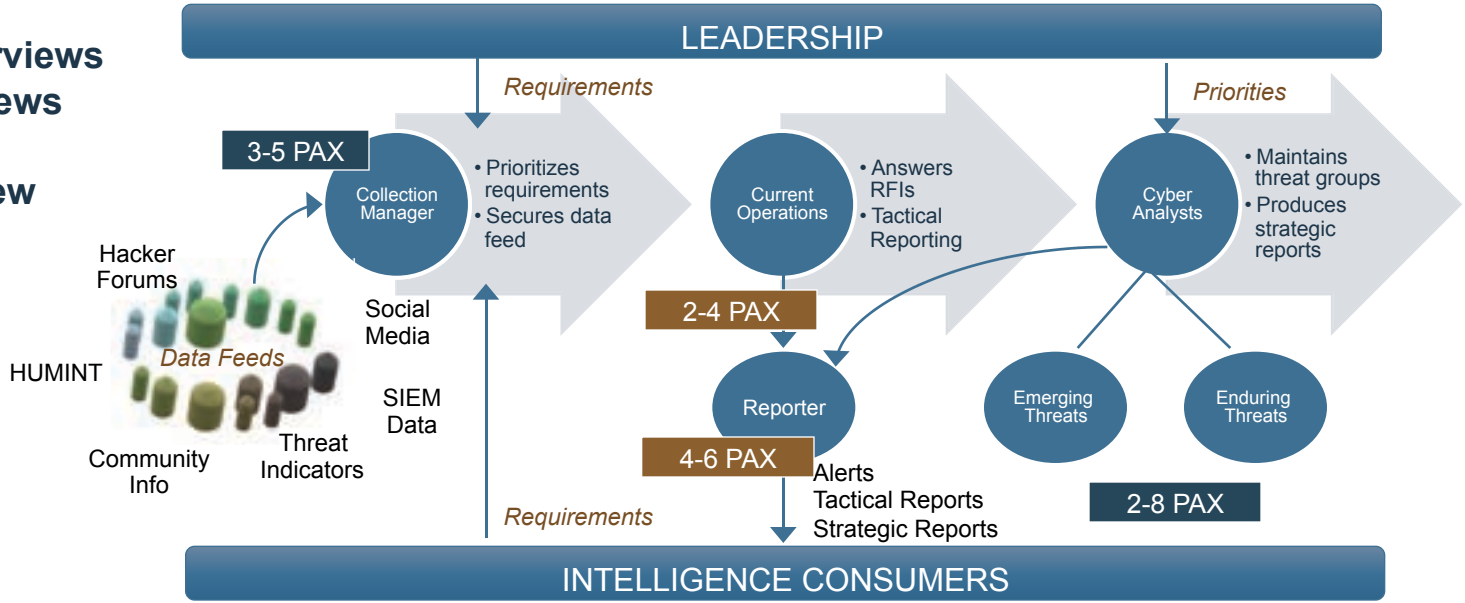


Team Structure Creation: 4 Weeks

OBJECTIVES:
- **Define Team Roles**
- **Define Operations Cycle**
- **Create Templates**

METHODOLOGY:
- **Leadership Interviews**
- **Operator Interviews**
- **Observation**
- **Procedure Review**

DELIVERABLES:
- **Team Plan**
- **Templates**
- **Roadmap**
- **Briefing**

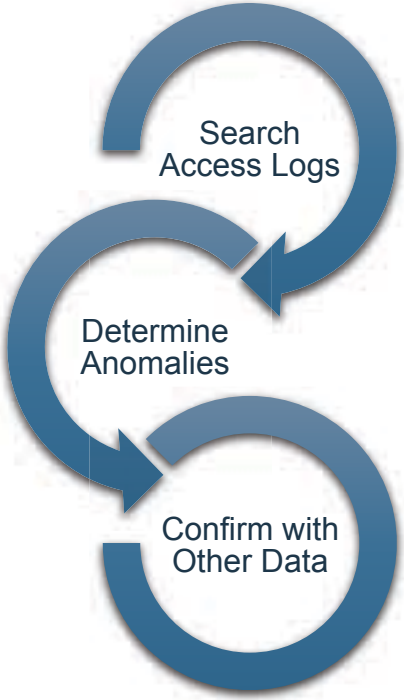


Training Plan Development: 6 Weeks

OBJECTIVES:
- **Create Training Plans**
- **Develop Workflows**

METHODOLOGY:
- **Leadership Interviews**
- **Operator Interviews**
- **NOC Observation**
- **Procedure Review**

DELIVERABLES:
- **Training Outline**
- **Workflows**
- **Briefing**



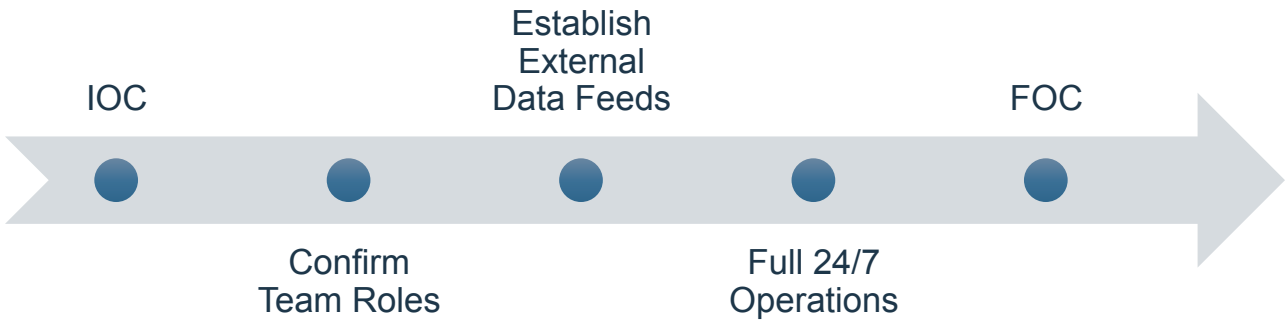
35

Team Process Development: 5 Weeks

OBJECTIVES:
- **Finalize Policy Documents**
- **Create Maturation Roadmap Objectives**

METHODOLOGY:
- **Leadership Interviews**
- **Operator Interviews**
- **Observation**
- **Procedure Review**

DELIVERABLES:
- **SOP Documents**
- **Playbooks**
- **Roadmap Objectives**
- **Transition Briefing**



36

Evaluation: 6 Weeks (repeated)

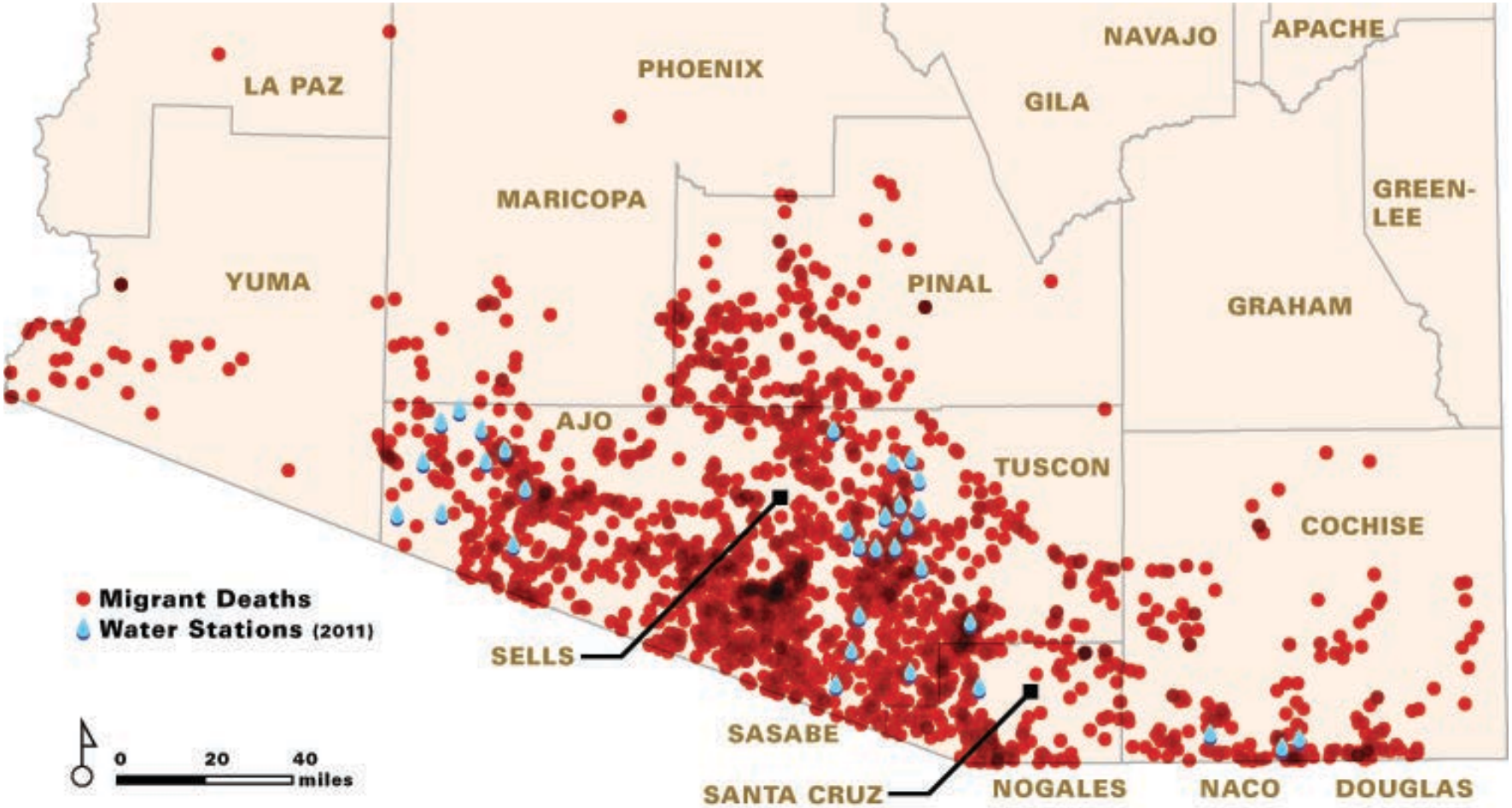
OBJECTIVES:
- **Evaluate SOC Effectiveness**
- **Conduct Vulnerability Assessment**

METHODOLOGY:
- **Lab Training**
- **Table-top Training**
- **Logical Assessment**
- **Other Assessments**

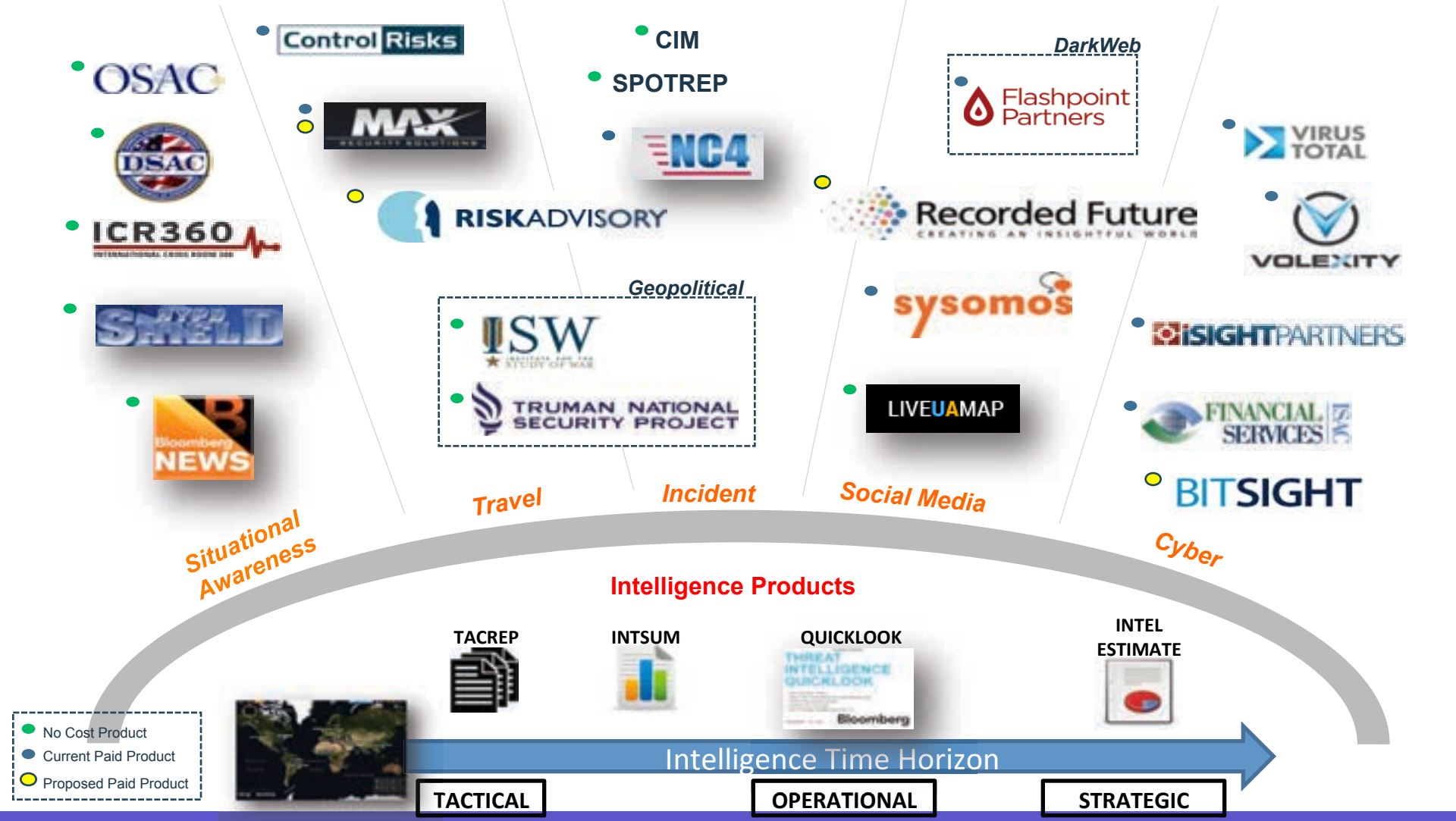
DELIVERABLES:
- **Simulation Exercise**
- **Assessment Report**
- **Recommendations**
- **Briefing**

37

Tipping and Queuing



Sources


OSAC
DSAC
ICR360
SHIELD
Bloomberg NEWS
Situational Awareness
Control Risks
MAX
RISKADVISORY
Travel
CIM
SPOTREP
NC4
Geopolitical
ISW
TRUMAN NATIONAL SECURITY PROJECT
Incident
DarkWeb
Flashpoint Partners
Recorded Future
CREATING AN INSIGHTFUL WORLD
sysomos
LIVEUAMAP
Social Media
VIRUS TOTAL
VOLEXITY
iSIGHTPARTNERS
FINANCIAL SERVICES ISAC
BITSIGHT
Cyber
Intelligence Products
TACREP
INTSUM
QUICKLOOK
THREAT INTELLIGENCE QUICKLOOK
Bloomberg
INTEL ESTIMATE
No Cost Product
Current Paid Product
Proposed Paid Product
Intelligence Time Horizon
TACTICAL
OPERATIONAL
STRATEGIC

SOURCE RECOMMENDATION

Buy now to fill Intelligence Gaps:

MAX SECURITY SOLUTIONS → Add additional Asia Intelligence subscription package for regional travel alerts. For High Risk travel. → Cost: + $24,000/year

RISKADVISORY → Travel and geopolitical alerts, also allows longitudinal analysis with database of previous incidents. → Cost: + $35,000/year

BITSIGHT → Real-time cyber risk scoring, breach detection, and reputation awareness. Possible use for VRMA. → Cost: + $2,500/year

Recommend POC to Determine Value:

Recorded Future → Social media, open source aggregation, leak detection and publication of data. → Cost: + $150,000/year + $50,000/year API

Strategic Considerations:

Control Risks $230,000/year
NC4 $51,000/year
→ Source assessment determined intel is slow, incomplete, and difficult to use. Our peers have turned away from these vendors to other industry leaders.
→ *Consider* **Bundle replacement** → ANVIL, iHS, GLOBAL rescue

iSIGHTPARTNERS $800,000/year
→ Quality cyber intelligence reports and IOC feed, but estimating little value in vulnerability feed and underutilizing bespoke analysis/investigations.
→ *Consider* **Reduce iSight investment, supplement** → DIGITAL SHADOWS

Source Reliability and Accuracy

	Rating	Description
A	Reliable	No doubt about the source's authenticity, trustworthiness, or competency. History of complete reliability.
B	Usually reliable	Minor doubts. History of mostly valid information.
C	Fairly reliable	Doubts. Provided valid information in the past.
D	Not usually reliable	Significant doubts. Provided valid information in the past.
E	Unreliable	Lacks authenticity, trustworthiness, and competency. History of invalid information.
F	Cannot be judged	Insufficient information to evaluate reliability. May or may not be reliable.

	Rating	Description
1	Confirmed	Logical, consistent with other relevant information, confirmed by independent sources.
2	Probably true	Logical, consistent with other relevant information, not confirmed.
3	Possibly true	Reasonably logical, agrees with some relevant information, not confirmed.
4	Doubtfully true	Not logical but possible, no other information on the subject, not confirmed.
5	Improbable	Not logical, contradicted by other relevant information.
6	Cannot be judged	The validity of the information can not be determined.

THREAT INTELLIGENCE QUICKLOOK

- QUICKLOOK Number: 14-0001, v3
- SUBJECT: Social Engineering Attacks from “FIN4” Hacking Group
- ATTENTION: Company executives, financial related employees
- SOURCES: FireEye Report *Hacking the Street?*, December 1st, 2014
- ANALYST: Bob Stasio

December // 04 // 2014

FIN4 THREAT OVERVIEW

SUMMARY:
Since mid-2013, a criminal group known as "FIN4" have been targeting financial and M&A executives in order to acquire non-public information. FIN4 targets individuals with information about impending market catalysts that will cause stocks to rise. The most commonly used attack vector by FIN4 is a socially engineered email lure (phishing) which focuses on capturing username and passwords, thus giving the attacker sustained access to private communications.

FREQUENT TARGETS

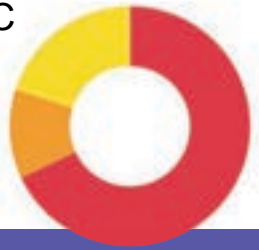
Since mid-2013, FIN4 has targeted over 100 organizations such as advisory firms, legal counsel, and investment banking. The following types of individuals are commonly targeted: C-Level executives and senior leadership, legal counsel, regulatory risk, and compliance personnel, researchers, scientists, advisors. FIN4 has a high-level of knowledge of their victims and uses convincing phishing lures to gain access to email accounts.

On multiple occasions, FIN4 has targeted several parties involved in a single business deal, to include law firms, consultants, and the public companies involved in negotiations. They also have mechanisms to organize the data they collect and have taken steps to evade detection.

SECTOR SPECIFIC ATTACKS

FIN4 heavily targets healthcare and pharmaceutical companies as stocks in these industries can move dramatically in response to news of clinical trial results, regulatory decisions, or safety and legal issues.

FIN4 VICTIMS



Threat indicators and mitigation

Threat Tactics

FIN4 conducts reconnaissance on victims and uses other hijacked email accounts to “spearphish” targets

Email content is sophisticated and relevant to a pending deal which entices user to trust recipient and content

Email displays a dialog box that mimics the Windows Authentication prompt for user domain credentials

Credentials are transmitted to a server controlled by FIN4 which is used to hijack the account, steal information, and infect other victims

What to do

The relative simplicity of FIN4’s tactics (spearphishing, theft of valid credentials, lack of any malware installed on victim machines) makes their intrusion activity difficult to detect. However, there are a few basic security steps to mitigate the threat:

- Maintain high situational awareness of emails concerning upcoming acquisitions. Even though it may appear to come from a trusted source, if any prompts ask for credentials while reading email or opening documents, report the incident to security immediately. Also see www.xxxxxxx.om
- The CRCO CIRT team is aware of the risk and actively monitoring Acme, co. domain email technical indicators of threat. Be aware that the attack vector may come through your personal email and then try to obtain corporate credentials. Use extra caution with HTML links, attachments, and prompts associated with personal email.

EXAMPLES OF FIN4 ATTACKS

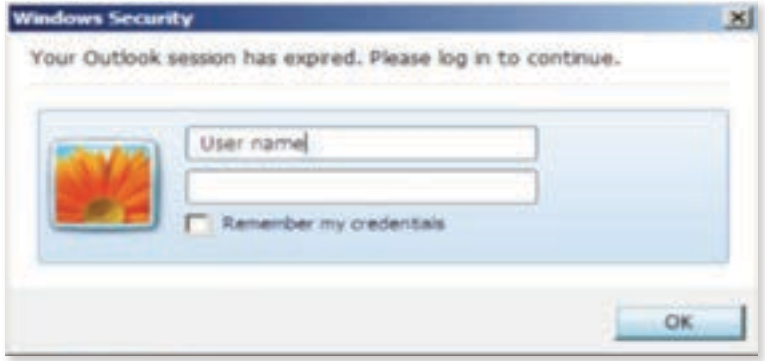


Fig. 1: Malicious prompt to capture credentials

Fig. 2: Generic lure document

```
Subject: employee making negative comments about you and the company

From: <name>@<compromised company's domain>

I noticed that a user named FinanceBull82 (claiming to be an employee) in an investment discussion forum posted some
negative comments about the company in general (executive compensation mainly) and you in specific (overpaid and
incompetent). He gave detailed instances of his disagreements, and in doing so, may have unwittingly divulged
confidential company information regarding pending transactions.

I am a longtime client and I do not think that this will bode well for future business. The post generated quite a
few replies, most of them agreeing with the negative statements. While I understand that the employee has the right
to his opinion, perhaps he should have vented his frustrations through the appropriate channels before making his
post.

The link to the post is located here (it is the second one in the thread):
http://forum.<domain>/redirect. php?url=http://<domain>%2fforum%2fequities%2f375823902%2farticle. php\par
```

Fig. 3: Phishing email to an executive

Section 4:
Case Studies

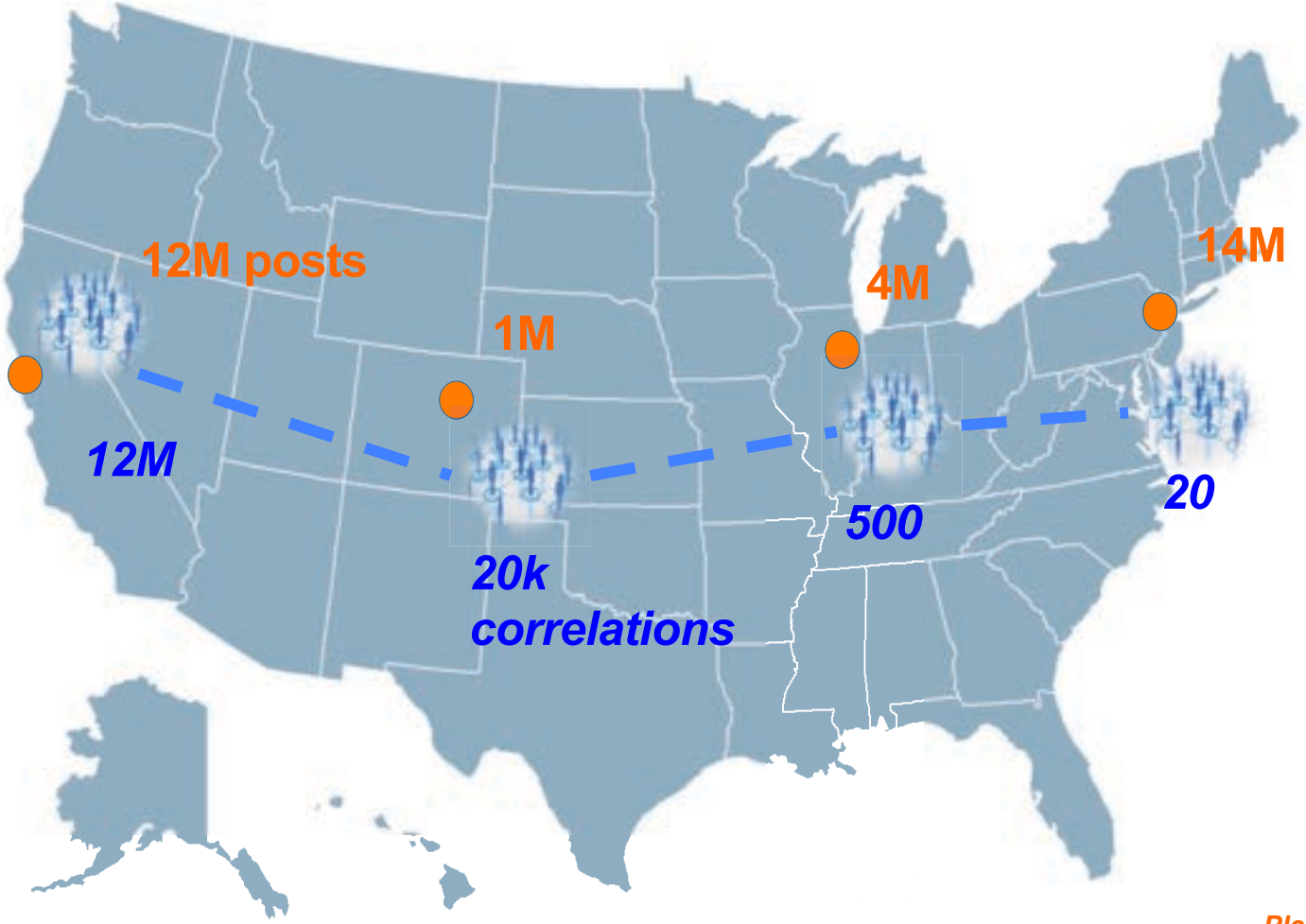
Use Case Mapping

- **SOC Use Cases**
  Threat Hunting
  Incident Investigations
  Event Correlation
- **Threat Intel Use Cases**
  Campaign Tracking
  Intel Report Production
- **Insider Threat Use Cases**
  Threat Discovery
  Watchlists
  Vetting

- **Physical Security Use Cases**
  Political Unrest Assessments
  Building Threat Assessments
  Theft Investigations
- **VIP Protection Use Cases**
  Stakeholder Threat Assessment
  Reputation Investigation
- **Travel Risk Use Cases**
  Area Threat Assessment
  Event Threat Assessment

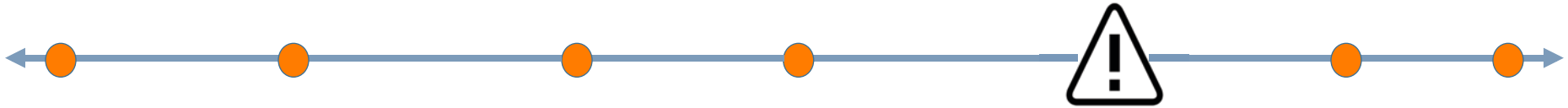
- **Internal Fraud Use Cases**
  Privilege Misuse
  Money Laundering
  Insider Trading
- **External Fraud Use Cases**
  Account Takeover
  Organized Crime Investigation
- **SIU Use Cases**
  Insurance Fraud
  Complex Fraud Investigation

Customer Stakeholder Protection Use Case



Please See Notes

Case Study: Insider Threat Example



07 Feb	12 Mar	05 May	620am 09 May	12-15 May	03 Jun	06 Jun
Relevant SM Post	Relevant SM Post	Report Released	File Printed	Security alerted as Intercept tries to verify with another source	Suspect Arrested	Article Published

Analyst Notes

- Crease noticed in image, likely a print out
- Six people printed the document, find commonality
- Only one user also emailed the Intercept
- Consistently coming into work before normal hours
- Searched for items outside her normal role
- Vicious and proactive social media posts
- Evidence of profile masking and evasion

Data Sources

- ✓ Print logs
- ✓ Connection Logs
- ✓ Proxy Logs
- ✓ Email Logs
- ✓ Email Content
- ✓ Badge Logs
- ✓ HR Records
- ✓ Search Logs
- ✓ Social Media
- ✓ Entity Resolution

Insider Threat Use Case

(1) - DLP Alert from SOC

SIEM

Insider Threat Team

(2) – Badge Records Physical Security

(3) – Social Media Search

(4) – HR Records

(5) – Print Logs

(6) – Legal Team

Looking For:

- Security Startups
- Immersion Partners
- Other Investors

@dreamit

Dreamit

SecureTech

Cameron Watts, Program Manager
cameron@dreamit.com

Bob Stasio, Managing Director
bob@dreamit.com