RSAConference2015
San Francisco | April 20-24 | Moscone Center

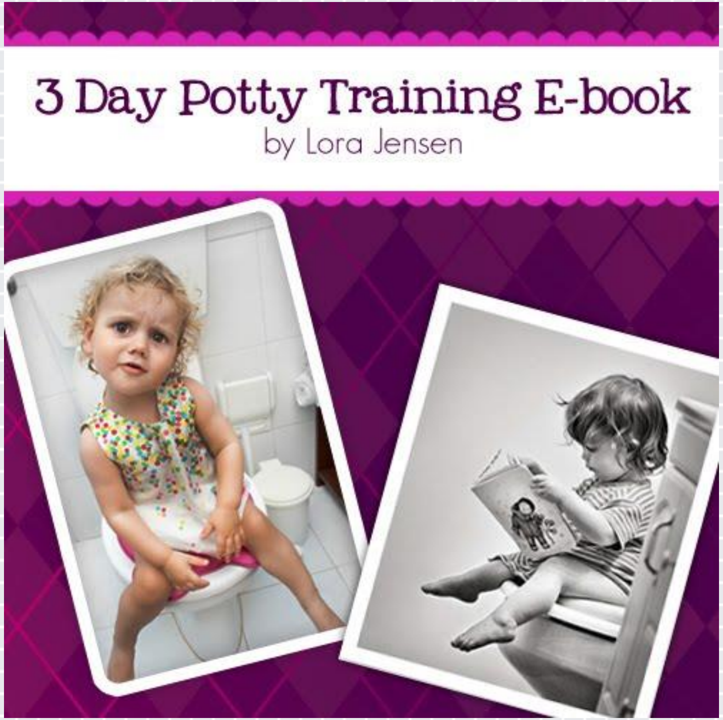
CHANGE
Challenge today's security thinking

SESSION ID: CXO-T08R

Threat Intelligence is Like Three Day Potty Training

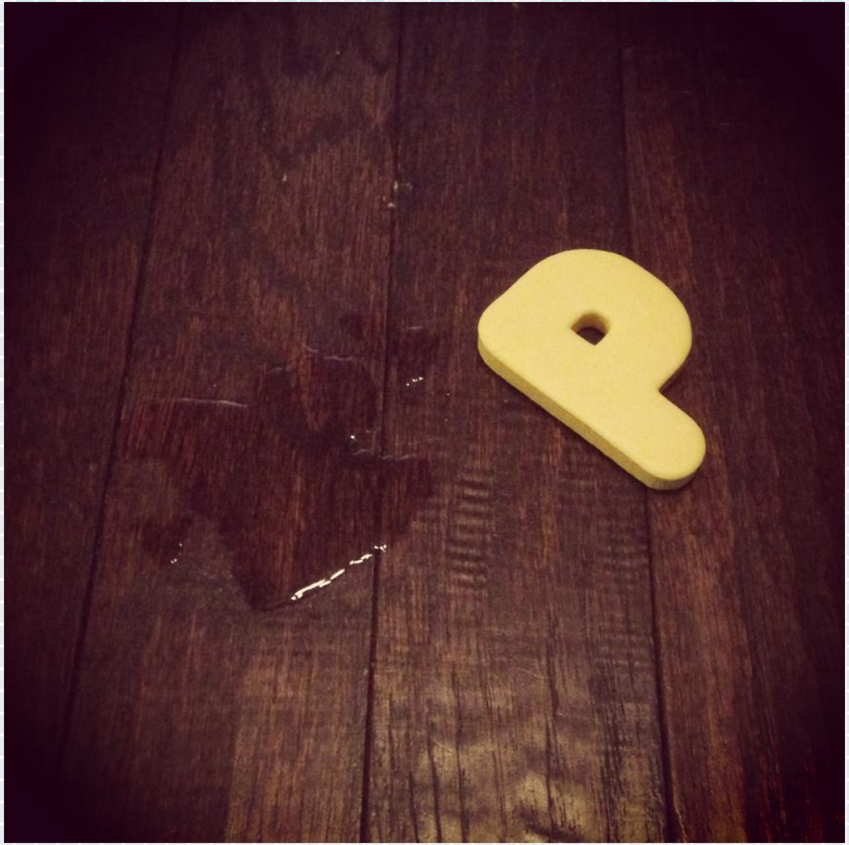
Rick Holland

Principal Analyst
Forrester Research
@rickhholland



“Potty training method that ***guarantees success*** *so you can say goodbye to diapers permanently* ***in 3 days or less!****”*

We are **320 days** into 3 day potty training.

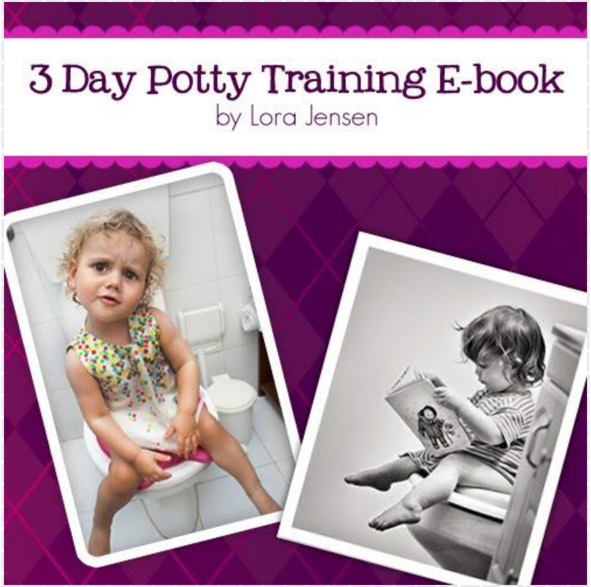


Incentive program

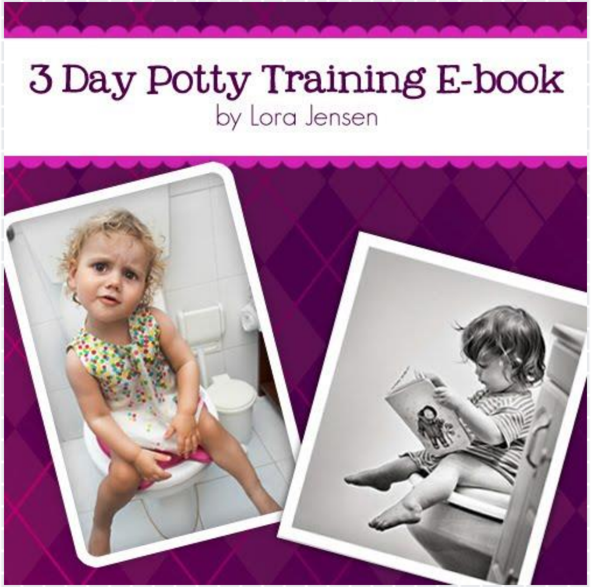
Unexpected outcomes

Unexpected outcomes

3 day threat intelligence?



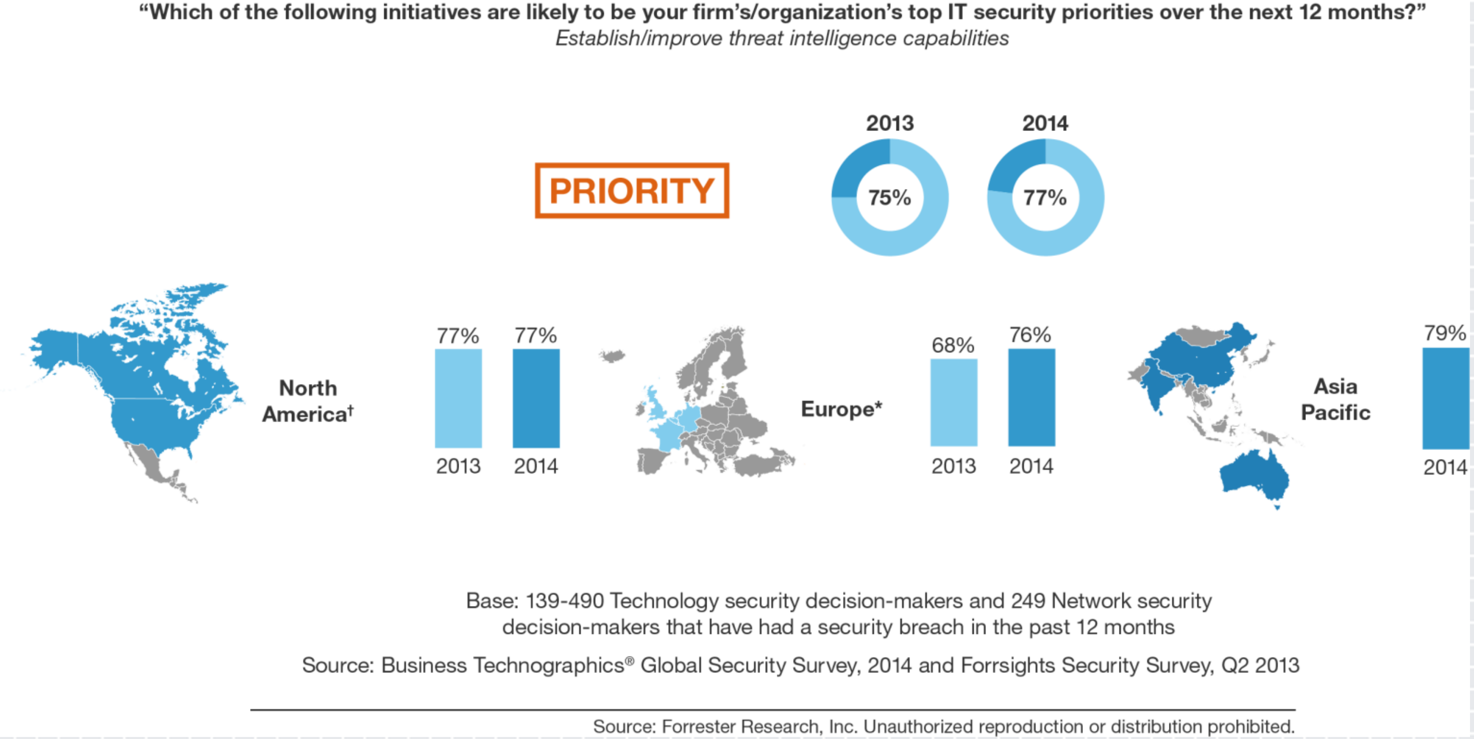
~~3 day threat intelligence?~~


3 Day Potty Training E-book
by Lora Jensen

Threat intelligence to the rescue

"Which of the following initiatives are likely to be your firm's/organization's top IT security priorities over the next 12 months?"

Establish/improve threat intelligence capabilities



Base: 139-490 Technology security decision-makers and 249 Network security decision-makers that have had a security breach in the past 12 months

Source: Business Technographics® Global Security Survey, 2014 and Forrsights Security Survey, Q2 2013

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Agenda

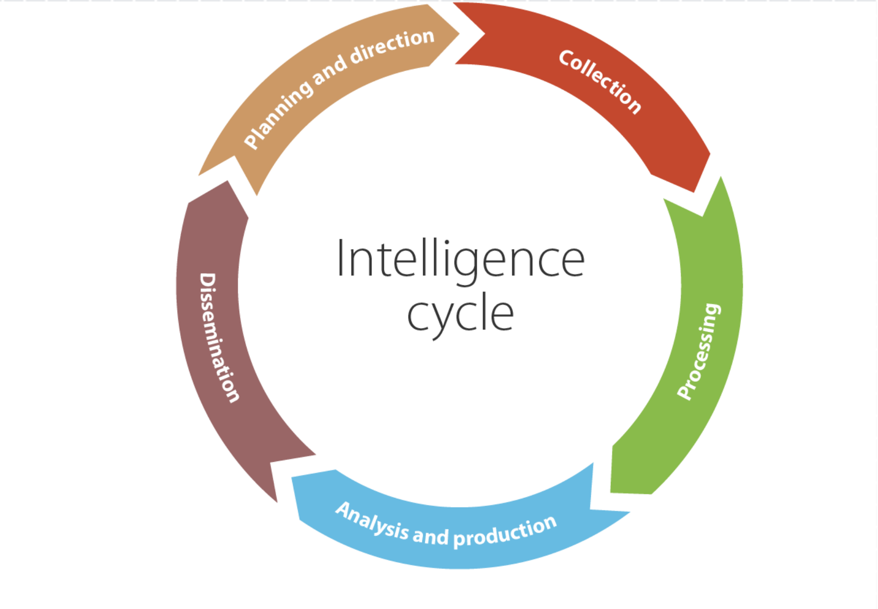
- Threat intelligence to the rescue
- Threat intelligence maturity model
  - People
  - Process
  - Technology
- Apply

#3daythreatintel

Threat intelligence maturity model

#RSAC

We have a guide – Intelligence lifecycle

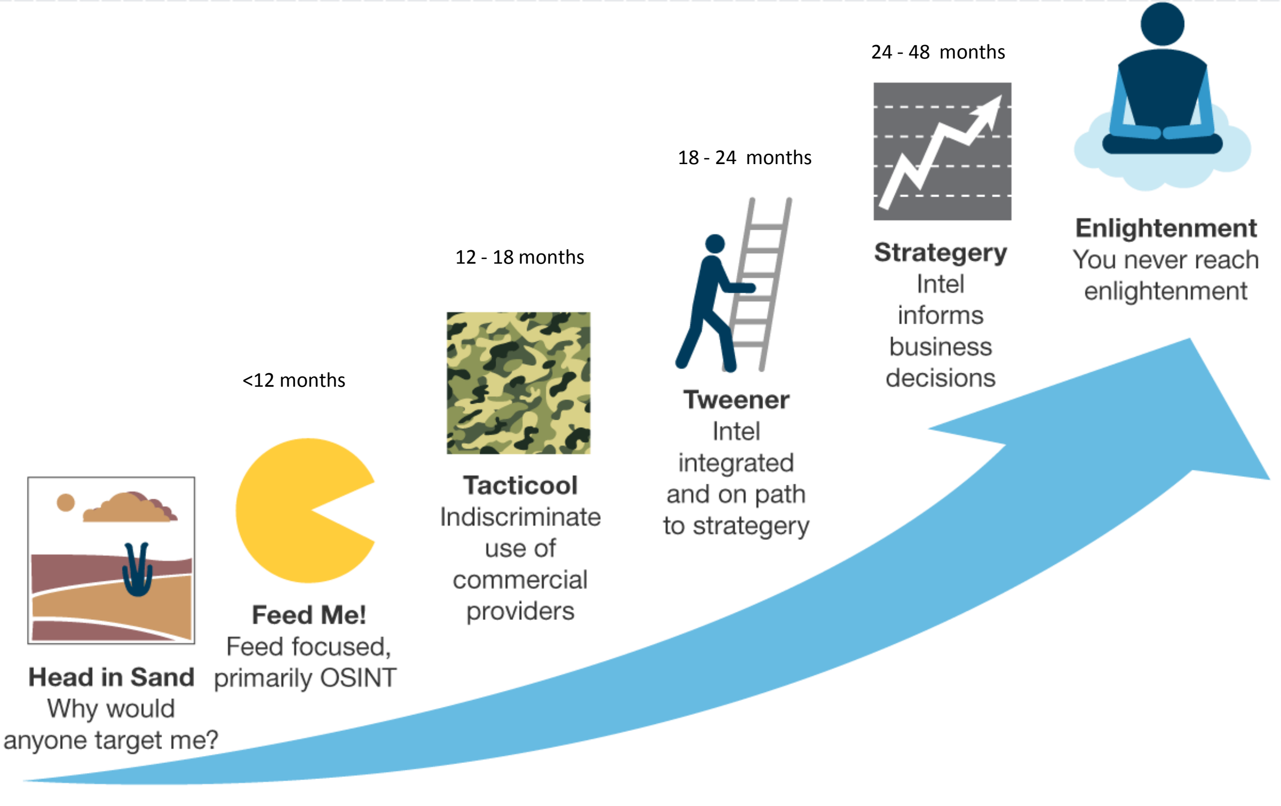


Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

For more:

- US Army Field Manual 2-0 - Intelligence
- Joint Publication 2-0 - Joint Intelligence

Threat intelligence maturity



Head in Sand
Why would
anyone target me?

<12 months

Feed Me!
Feed focused,
primarily OSINT

12 - 18 months

Tacticool
Indiscriminate
use of
commercial
providers

18 - 24 months

Tweener
Intel
integrated
and on path
to strategery

24 - 48 months

Strategery
Intel
informs
business
decisions

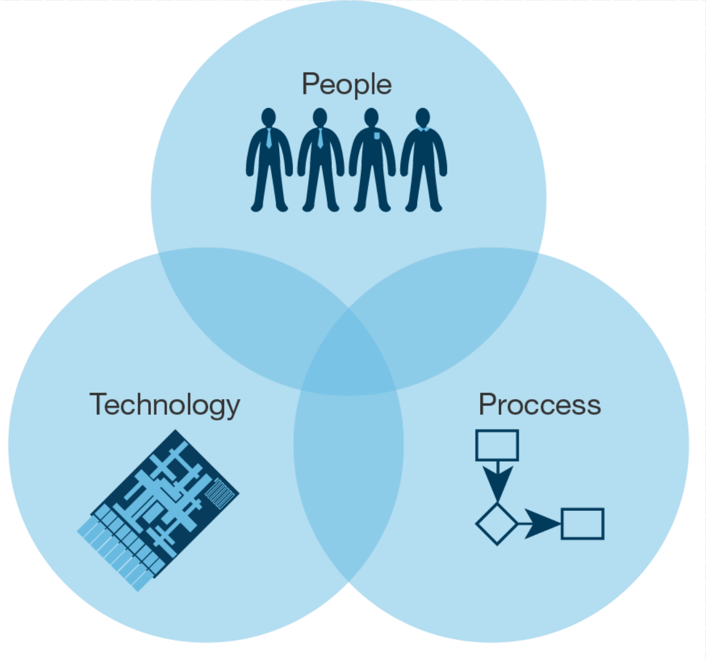
Enlightenment
You never reach
enlightenment

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Perceived maturity

Actual maturity

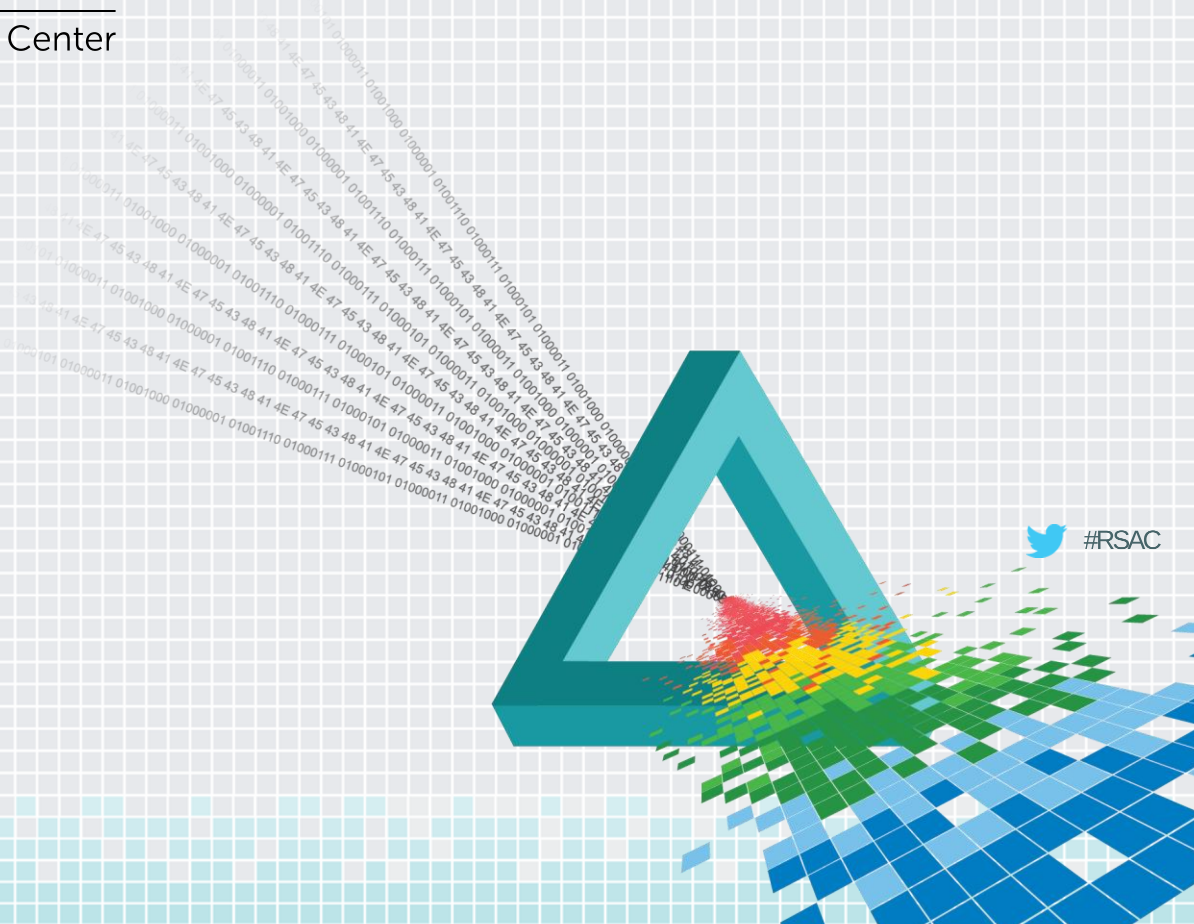
People, Process and Technology



RSAConference2015

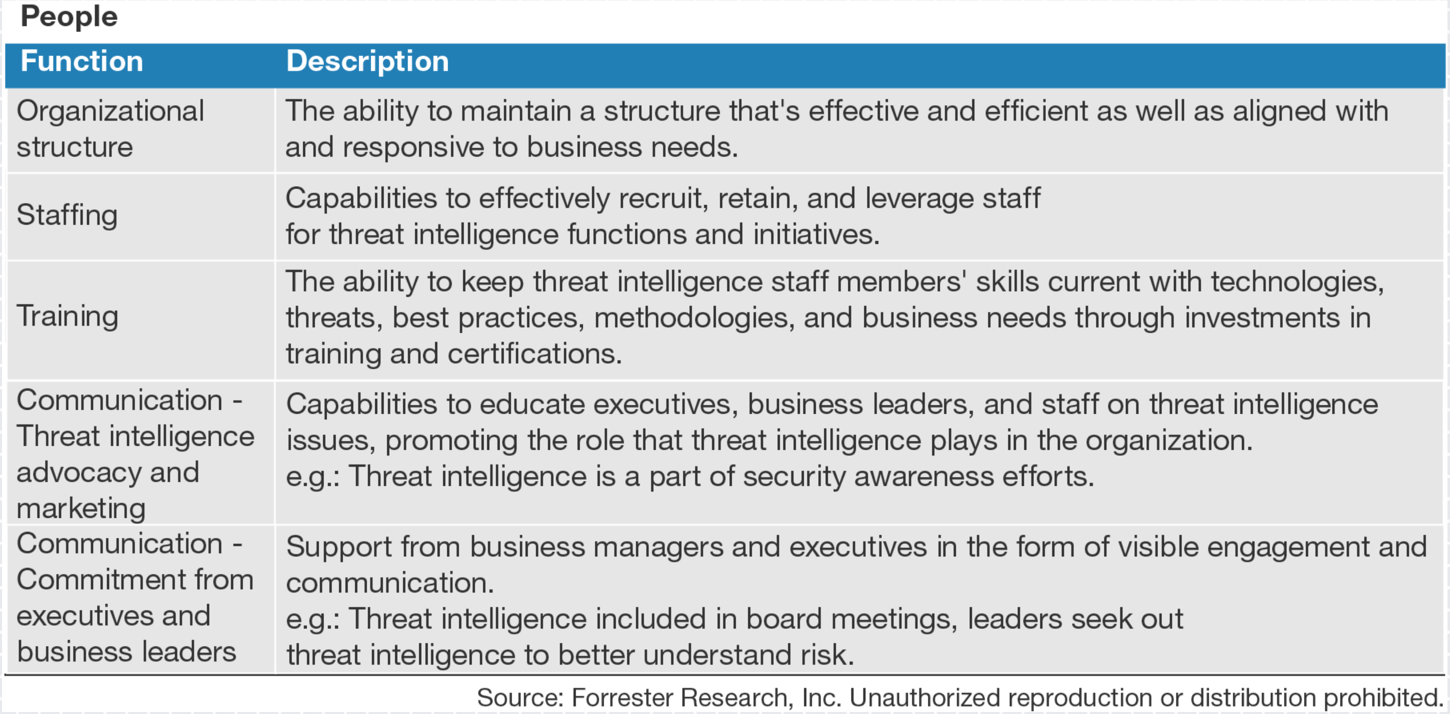
San Francisco | April 20-24 | Moscone Center

People



#RSAC

People

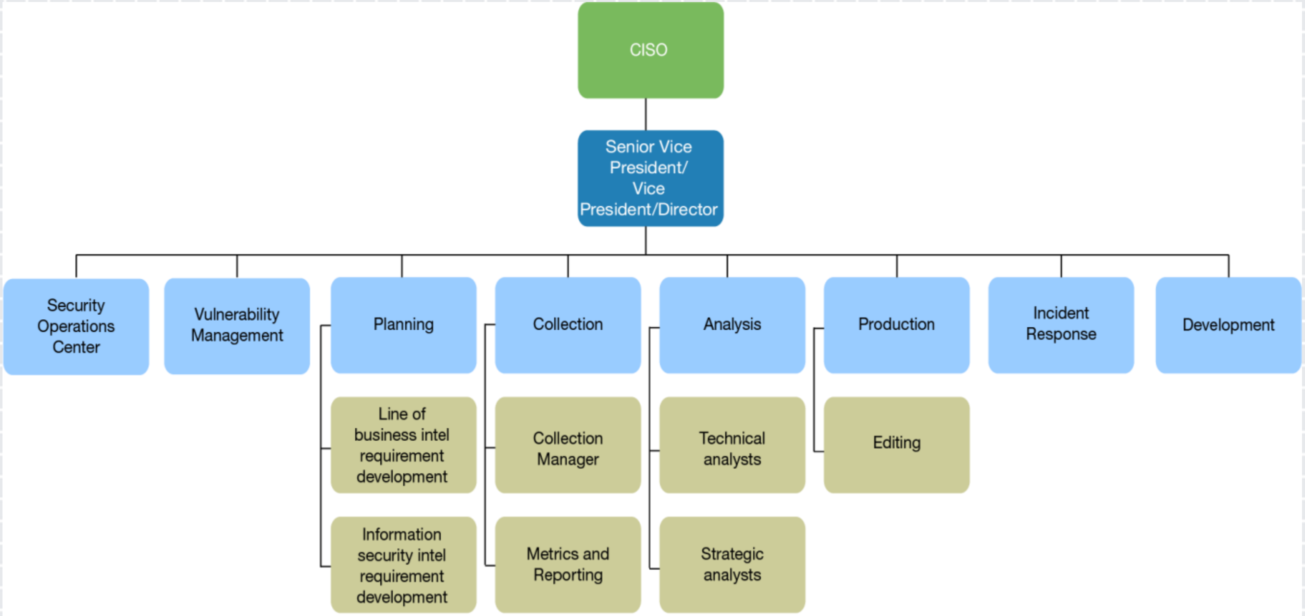


People

Function	Description
Organizational structure	The ability to maintain a structure that's effective and efficient as well as aligned with and responsive to business needs.
Staffing	Capabilities to effectively recruit, retain, and leverage staff for threat intelligence functions and initiatives.
Training	The ability to keep threat intelligence staff members' skills current with technologies, threats, best practices, methodologies, and business needs through investments in training and certifications.
Communication - Threat intelligence advocacy and marketing	Capabilities to educate executives, business leaders, and staff on threat intelligence issues, promoting the role that threat intelligence plays in the organization. e.g.: Threat intelligence is a part of security awareness efforts.
Communication - Commitment from executives and business leaders	Support from business managers and executives in the form of visible engagement and communication. e.g.: Threat intelligence included in board meetings, leaders seek out threat intelligence to better understand risk.

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Example organizational structure



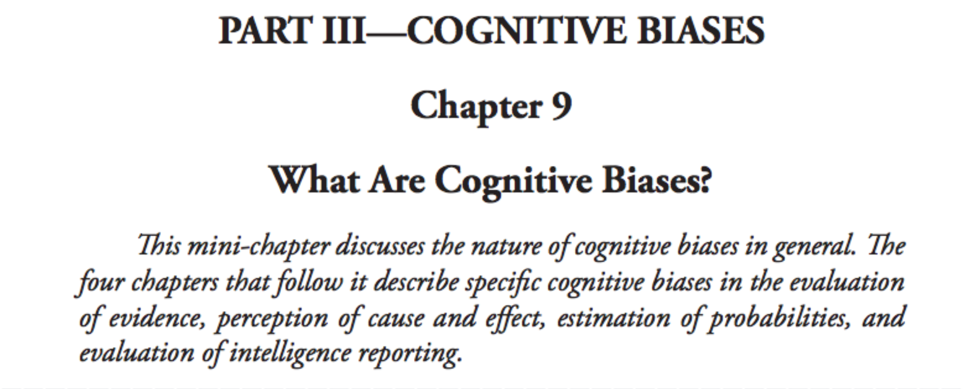
- CISO
  - Senior Vice President/ Vice President/Director
    - Security Operations Center
    - Vulnerability Management
    - Planning
      - Line of business intel requirement development
      - Information security intel requirement development
    - Collection
      - Collection Manager
      - Metrics and Reporting
    - Analysis
      - Technical analysts
      - Strategic analysts
    - Production
      - Editing
    - Incident Response
    - Development

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Finding a particular set of skills is difficult

- Technical skills + soft skills required.
- You must have a farm system to develop talent with the skills you need.
- Work with local universities
  - Provide internships.
  - Join advisory boards.

Mature organizations focus on critical thinking

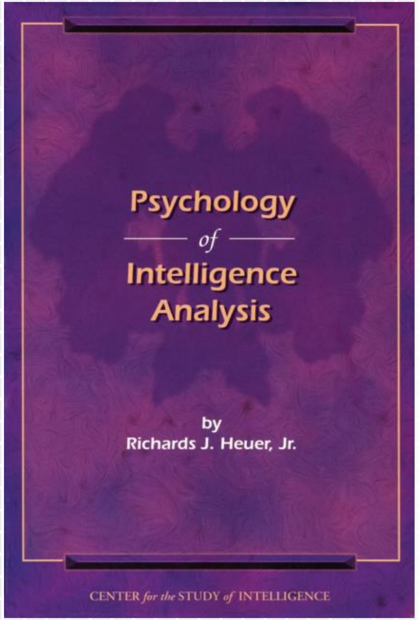


PART III—COGNITIVE BIASES

Chapter 9

What Are Cognitive Biases?

This mini-chapter discusses the nature of cognitive biases in general. The four chapters that follow it describe specific cognitive biases in the evaluation of evidence, perception of cause and effect, estimation of probabilities, and evaluation of intelligence reporting.



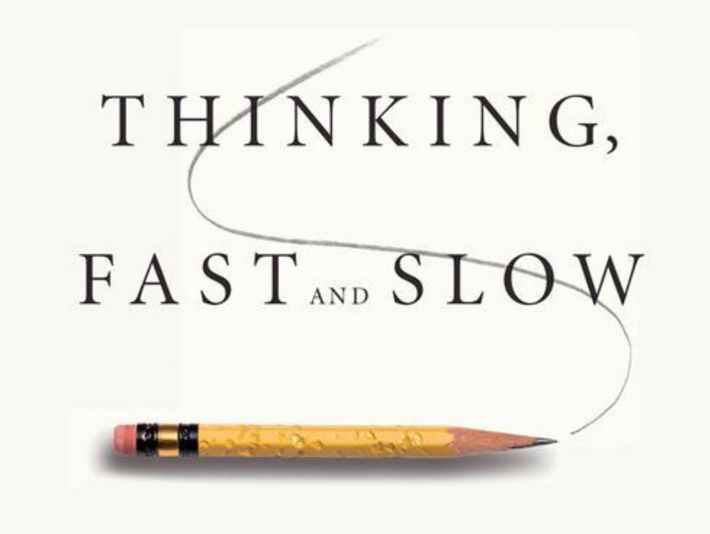
Psychology of Intelligence Analysis

by Richards J. Heuer, Jr.

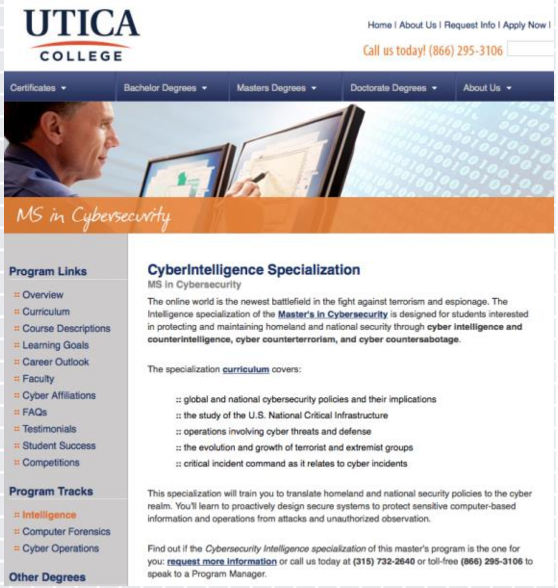
CENTER for the STUDY of INTELLIGENCE

Mature organizations focus on critical thinking

- Written by Daniel Kahneman.
- Kahneman reveals *“where we can and cannot trust our intuitions and how we can tap into the benefits of slow thinking.”*



Training



CyberIntelligence Specialization

MS in Cybersecurity

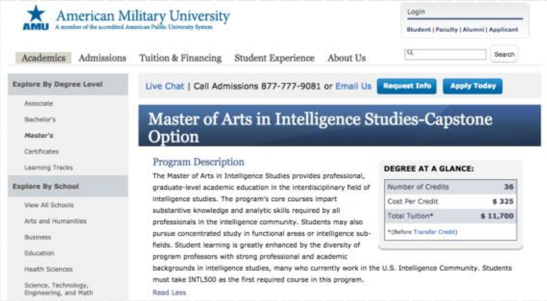
The online world is the newest battlefield in the fight against terrorism and espionage. The Intelligence specialization of the **Master's in Cybersecurity** is designed for students interested in protecting and maintaining homeland and national security through **cyber intelligence and counterintelligence, cyber counterterrorism, and cyber countersabotage**.

The specialization **curriculum** covers:

:: global and national cybersecurity policies and their implications
:: the study of the U.S. National Critical Infrastructure
:: operations involving cyber threats and defense
:: the evolution and growth of terrorist and extremist groups
:: critical incident command as it relates to cyber incidents

This specialization will train you to translate homeland and national security policies to the cyber realm. You'll learn to proactively design secure systems to protect sensitive computer-based information and operations from attacks and unauthorized observation.

Find out if the *Cybersecurity Intelligence specialization* of this master's program is the one for you: **request more information** or call us today at **(315) 732-2640** or toll-free **(866) 295-3106** to speak to a Program Manager.



Live Chat | Call Admissions 877-777-9081 or Email Us

Master of Arts in Intelligence Studies-Capstone Option

Program Description

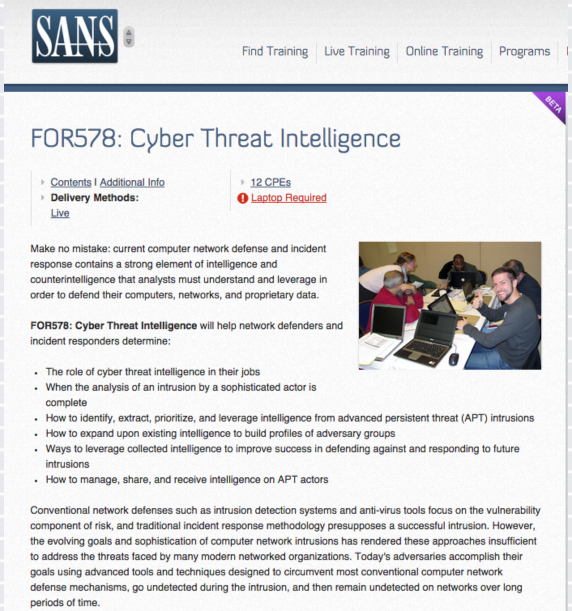
The Master of Arts in Intelligence Studies provides professional, graduate-level academic education in the interdisciplinary field of intelligence studies. The program's core courses impart substantive knowledge and analytic skills required by all professionals in the intelligence community. Students may also pursue concentrated study in functional areas or intelligence sub-fields. Student learning is greatly enhanced by the diversity of program professors with strong professional and academic backgrounds in intelligence studies, many who currently work in the U.S. Intelligence Community. Students must take INTL500 as the first required course in this program.

Read Less

DEGREE AT A GLANCE:

Number of Credits	36
Cost Per Credit	$ 325
Total Tuition*	$ 11,700

*(Before Transfer Credit)



FOR578: Cyber Threat Intelligence

- Contents | Additional Info
- Delivery Methods: Live
- 12 CPEs
- Laptop Required

Make no mistake: current computer network defense and incident response contains a strong element of intelligence and counterintelligence that analysts must understand and leverage in order to defend their computers, networks, and proprietary data.

FOR578: Cyber Threat Intelligence will help network defenders and incident responders determine:

- The role of cyber threat intelligence in their jobs
- When the analysis of an intrusion by a sophisticated actor is complete
- How to identify, extract, prioritize, and leverage intelligence from advanced persistent threat (APT) intrusions
- How to expand upon existing intelligence to build profiles of adversary groups
- Ways to leverage collected intelligence to improve success in defending against and responding to future intrusions
- How to manage, share, and receive intelligence on APT actors

Conventional network defenses such as intrusion detection systems and anti-virus tools focus on the vulnerability component of risk, and traditional incident response methodology presupposes a successful intrusion. However, the evolving goals and sophistication of computer network intrusions has rendered these approaches insufficient to address the threats faced by many modern networked organizations. Today's adversaries accomplish their goals using advanced tools and techniques designed to circumvent most conventional computer network defense mechanisms, go undetected during the intrusion, and then remain undetected on networks over long periods of time.

Real world training

- You fight like you train and you train like you fight.
- Team based training, not just individual.
- iSight Partners & Symantec provide cyber ranges.

Sponsor events at intelligence/cyber epicenters

Location	Event	Location	Event
Augusta, Georgia	BSides Augusta	Oak Ridge, Tennessee	Cyber And Information Security Research
Denver, Colorado	Rocky Mountain Information Security	Salt Lake City, Utah	BSides Salt Lake City
Columbia, Maryland	BSides Charm, Cyber Maryland	San Antonio, Texas	BSides San Antonio

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Retention is critical, your program can regress

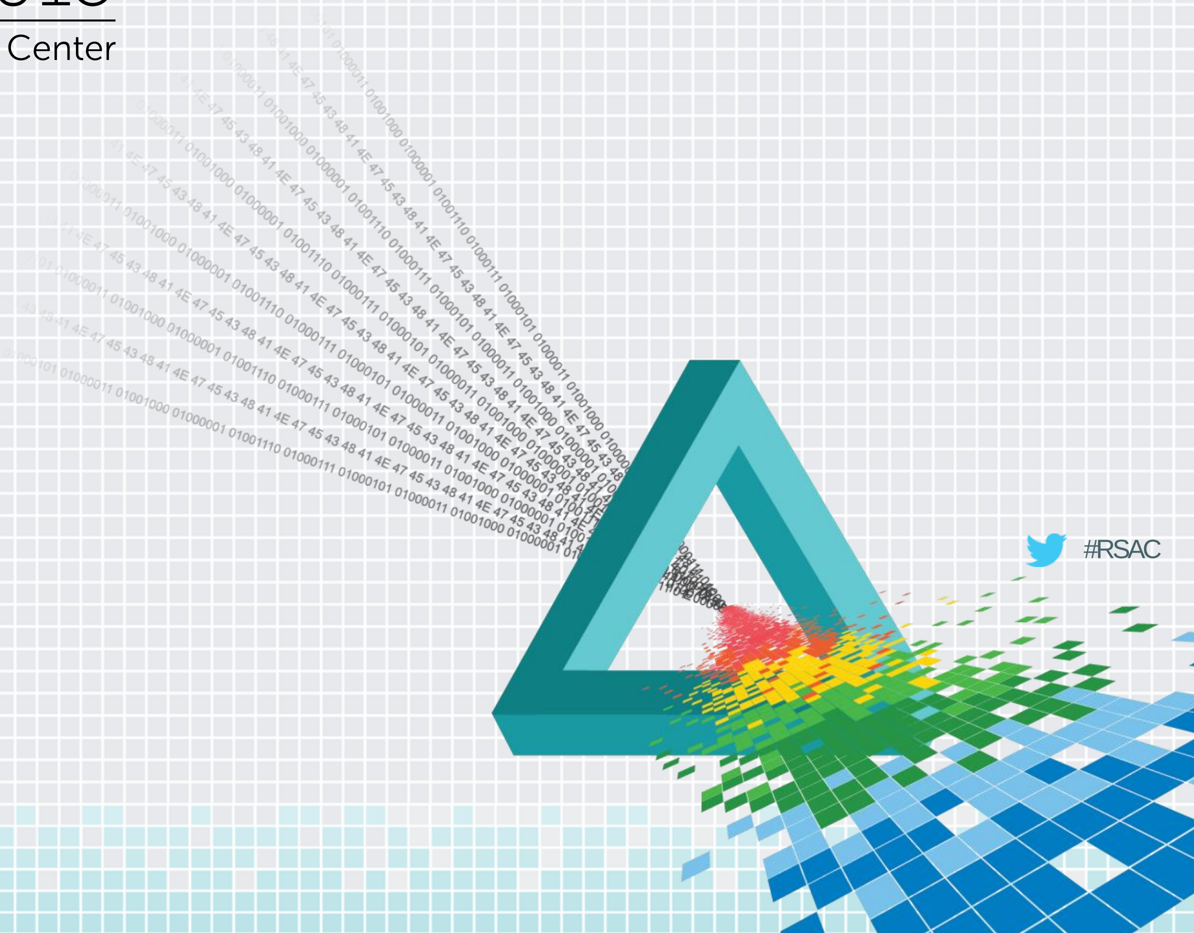
- Maturity doesn’t just evolve, it can devolve.
- You must be creative with retention strategies:
  - Remote workers
  - Training
  - Career pathing
  - Work with HR to create exceptions

#3daythreatintel

RSAConference2015

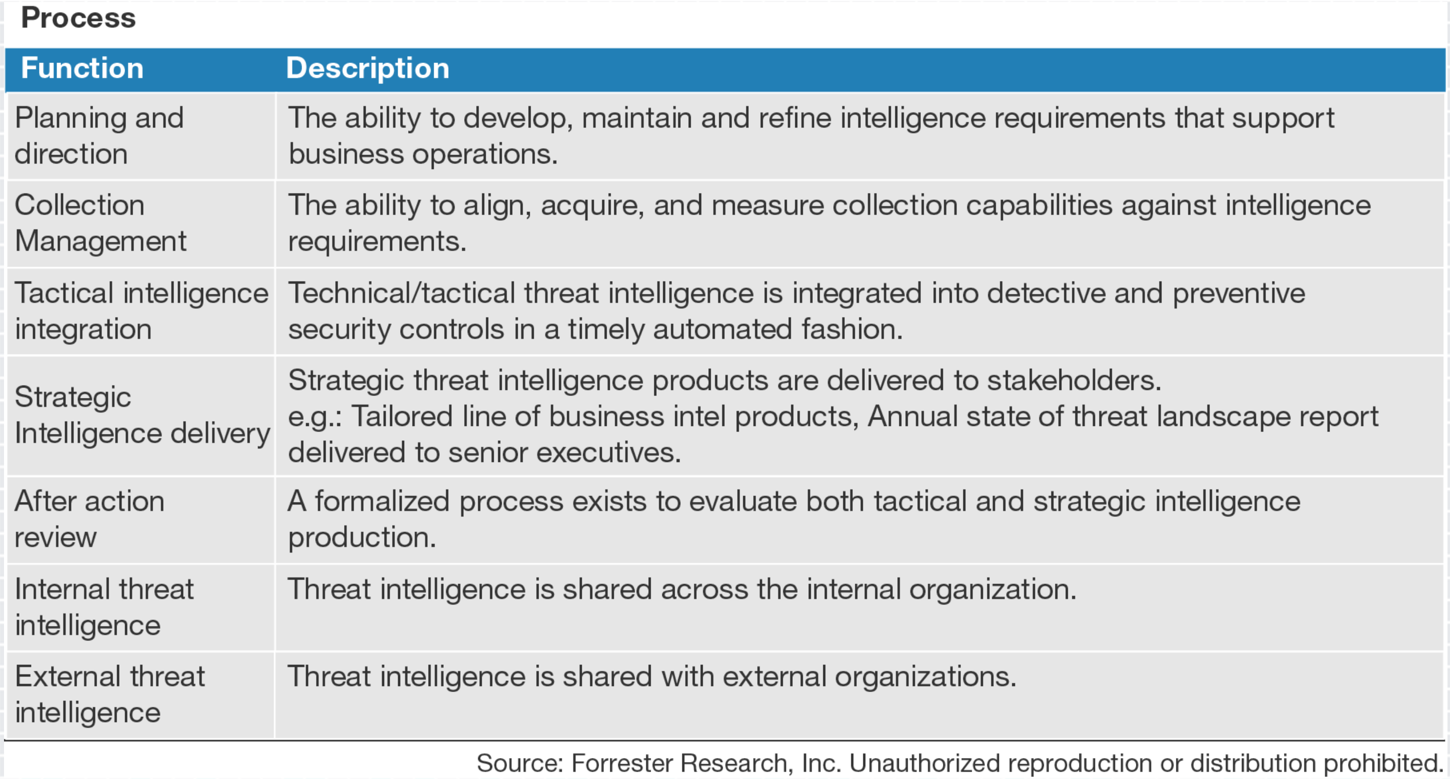
San Francisco | April 20-24 | Moscone Center

Process



#RSAC

Process



Process

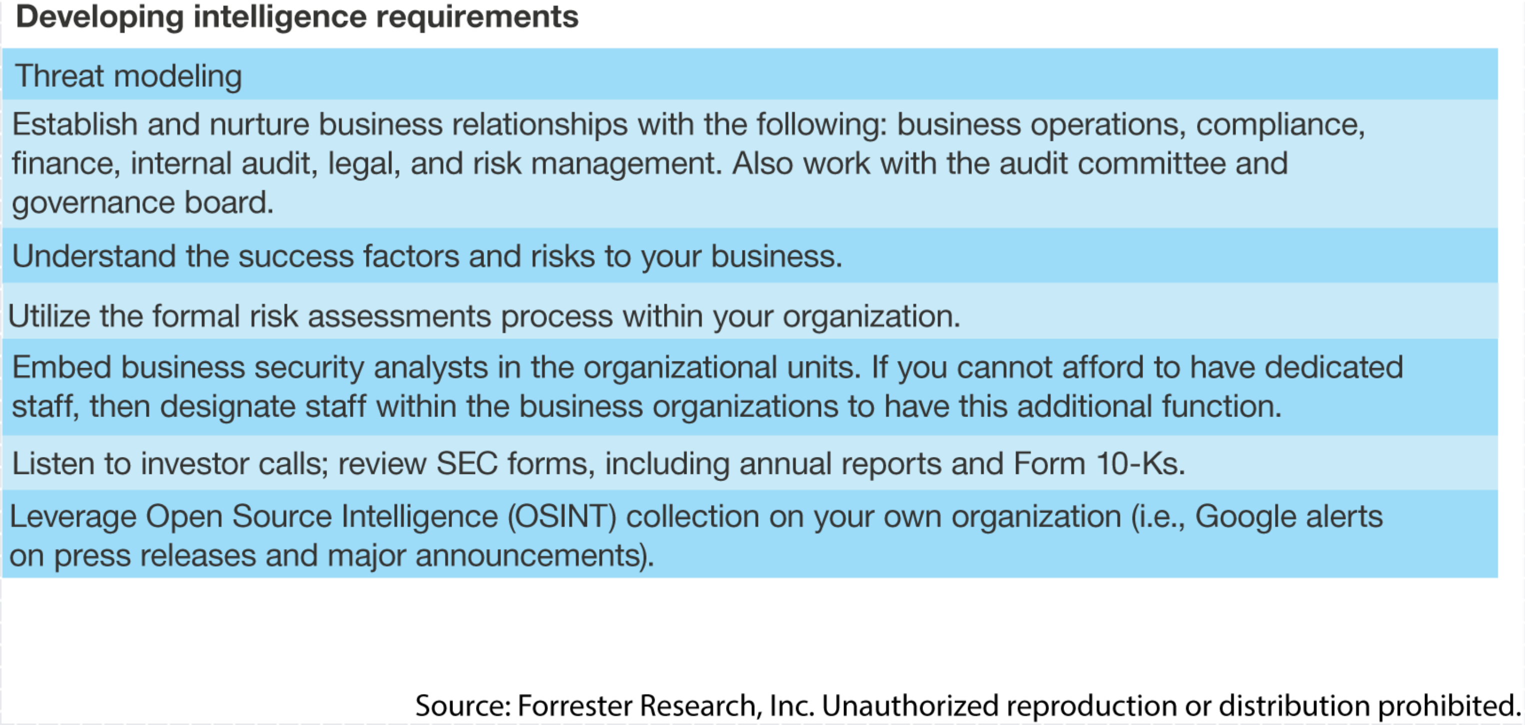
Function	Description
Planning and direction	The ability to develop, maintain and refine intelligence requirements that support business operations.
Collection Management	The ability to align, acquire, and measure collection capabilities against intelligence requirements.
Tactical intelligence integration	Technical/tactical threat intelligence is integrated into detective and preventive security controls in a timely automated fashion.
Strategic Intelligence delivery	Strategic threat intelligence products are delivered to stakeholders. e.g.: Tailored line of business intel products, Annual state of threat landscape report delivered to senior executives.
After action review	A formalized process exists to evaluate both tactical and strategic intelligence production.
Internal threat intelligence	Threat intelligence is shared across the internal organization.
External threat intelligence	Threat intelligence is shared with external organizations.

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Intel requirements are the foundation of your program

- Occurs during the "Planning & Direction" phase of the intel cycle
- Develop requirements based upon:
  - Your threat model
  - Understanding the success criteria for your business

Developing intelligence requirements



Developing intelligence requirements

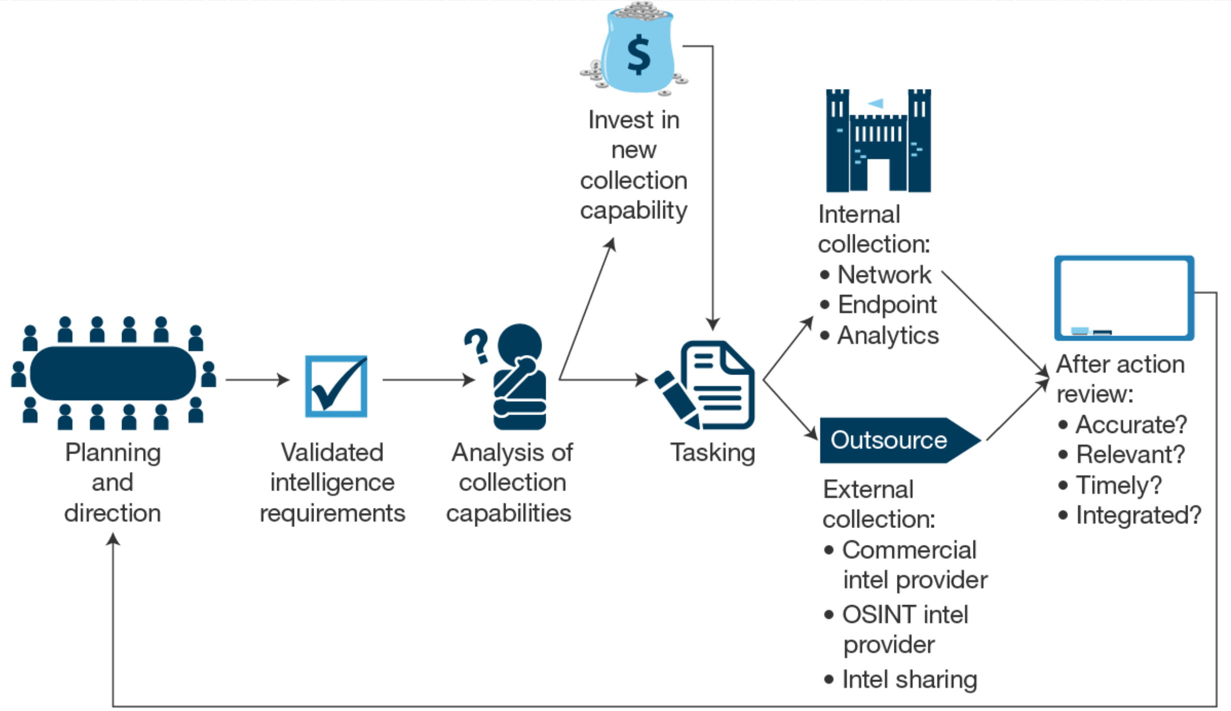
Threat modeling
Establish and nurture business relationships with the following: business operations, compliance, finance, internal audit, legal, and risk management. Also work with the audit committee and governance board.
Understand the success factors and risks to your business.
Utilize the formal risk assessments process within your organization.
Embed business security analysts in the organizational units. If you cannot afford to have dedicated staff, then designate staff within the business organizations to have this additional function.
Listen to investor calls; review SEC forms, including annual reports and Form 10-Ks.
Leverage Open Source Intelligence (OSINT) collection on your own organization (i.e., Google alerts on press releases and major announcements).

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Example intelligence requirements

- Have Chinese threat actors targeted health insurance provider x?
- What is likelihood that Lizard Squad will seek to disrupt the online gaming services of vendor x?
- What is the risk of adversary targeting the intellectual property associated with a 2017 product launch?

Collection management



Invest in new collection capability

Internal collection:
- Network
- Endpoint
- Analytics

Planning and direction

Validated intelligence requirements

Analysis of collection capabilities

Tasking

Outsource

External collection:
- Commercial intel provider
- OSINT intel provider
- Intel sharing

After action review:
- Accurate?
- Relevant?
- Timely?
- Integrated?

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Why reinvent the wheel?

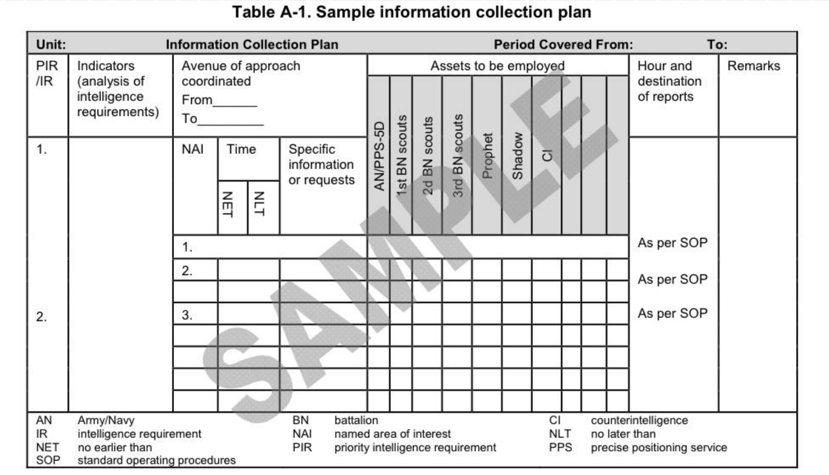


Table A-1. Sample information collection plan

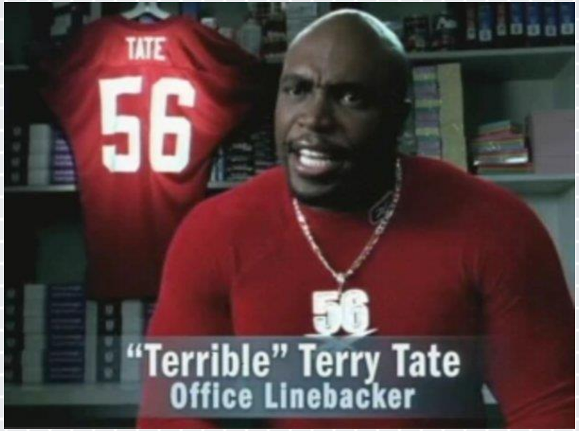
Unit:		**Information Collection Plan**								**Period Covered From:**					**To:**		
PIR /IR	Indicators (analysis of intelligence requirements)	Avenue of approach coordinated From______ To__________				Assets to be employed										Hour and destination of reports	Remarks
1.		NAI	Time		Specific information or requests	AN/PPS-5D	1st BN scouts	2d BN scouts	3rd BN scouts	Prophet	Shadow	CI					
			NET	NLT													
		1.														As per SOP	
		2.														As per SOP	
2.		3.														As per SOP	

AN	Army/Navy	BN	battalion	CI	counterintelligence
IR	intelligence requirement	NAI	named area of interest	NLT	no later than
NET	no earlier than	PIR	priority intelligence requirement	PPS	precise positioning service
SOP	standard operating procedures				

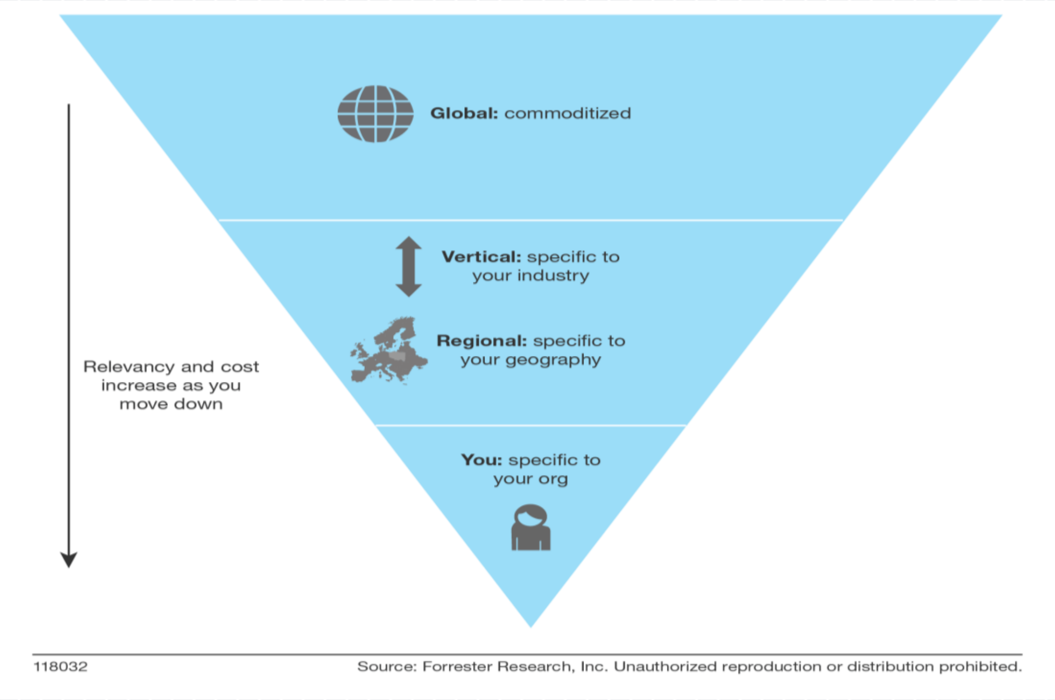
FM 3-55
INFORMATION
COLLECTION

MAY 2013
DISTRIBUTION RESTRICTION:
Approved for public release; distribution is unlimited.
HEADQUARTERS, DEPARTMENT OF THE ARMY

Actionable intelligence



Mature firms invest in relevant intelligence



Global: commoditized

Vertical: specific to your industry

Regional: specific to your geography

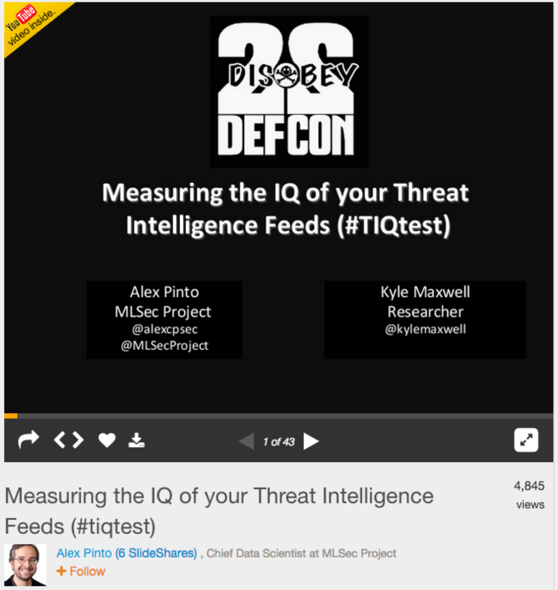
You: specific to your org

Relevancy and cost increase as you move down

118032

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Mature firms measure threat intelligence source effectiveness



Measuring the IQ of your Threat Intelligence Feeds (#TIQtest)

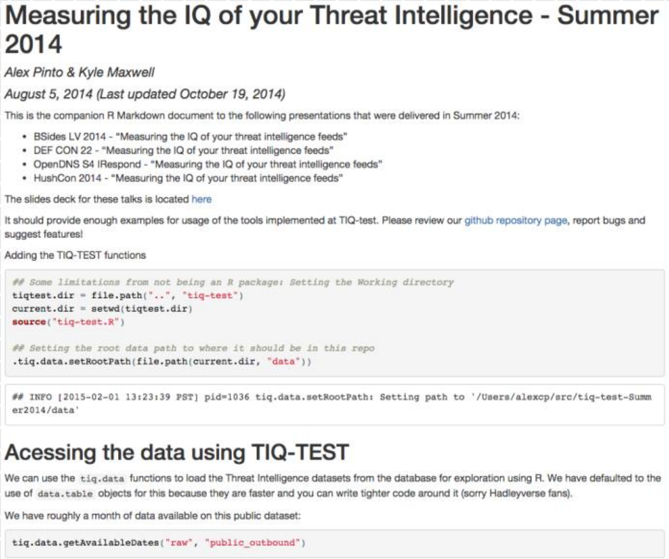
Alex Pinto
MLSec Project
@alexcpsec
@MLSecProject

Kyle Maxwell
Researcher
@kylemaxwell

Measuring the IQ of your Threat Intelligence Feeds (#tiqtest)

4,845 views

Alex Pinto (6 SlideShares) , Chief Data Scientist at MLSec Project
+ Follow



Measuring the IQ of your Threat Intelligence - Summer 2014

Alex Pinto & Kyle Maxwell

August 5, 2014 (Last updated October 19, 2014)

This is the companion R Markdown document to the following presentations that were delivered in Summer 2014:

- BSides LV 2014 - "Measuring the IQ of your threat intelligence feeds"
- DEF CON 22 - "Measuring the IQ of your threat intelligence feeds"
- OpenDNS S4 IRespond - "Measuring the IQ of your threat intelligence feeds"
- HushCon 2014 - "Measuring the IQ of your threat intelligence feeds"

The slides deck for these talks is located here

It should provide enough examples for usage of the tools implemented at TIQ-test. Please review our github repository page, report bugs and suggest features!

Adding the TIQ-TEST functions

```
## Some limitations from not being an R package: Setting the Working directory
tiqtest.dir = file.path("..", "tiq-test")
current.dir = setwd(tiqtest.dir)
source("tiq-test.R")

## Setting the root data path to where it should be in this repo
.tiq.data.setRootPath(file.path(current.dir, "data"))
```

```
## INFO [2015-02-01 13:23:39 PST] pid=1036 tiq.data.setRootPath: Setting path to '/Users/alexcp/src/tiq-test-Summ
er2014/data'
```

Acessing the data using TIQ-TEST

We can use the `tiq.data` functions to load the Threat Intelligence datasets from the database for exploration using R. We have defaulted to the use of `data.table` objects for this because they are faster and you can write tighter code around it (sorry Hadleyverse fans).

We have roughly a month of data available on this public dataset:

```
tiq.data.getAvailableDates("raw", "public_outbound")
```

Avoid Expense in Depth

Expense in Depth

Unified threat management

Web proxy

Wireless intrusion detection system

Data loss prevention

Two factor authentication

Next-generation firewall

Intrusion prevention system

Containerization

Configuration management

Encryption

Passive vulnerability scanner

Network analysis and visibility

Software inventory tools

Mobile device management

Malware analysis

Automated asset inventory discovery tool

Antivirus

Patch management

Blackbox testing

System hardening

Sandbox

Blacklisting

Configuration auditing

SIM

Microvisor security

Big data analytics

Digital rights management

File activity monitoring

Host firewalls

Network encryption

Privileged user monitoring

Email proxy

Vulnerability scanner

Antispyware

Application wrapping

Data execution prevention

Intrusion detection system

Database activity monitoring

DDoS mitigation

Forensics

Continuous vulnerability assessment

Network intrusion prevention

Web application firewall

Network access control

Firewall

Application white listing

Host intrusion prevention

Endpoint visibility

Application control

Endpoint analysis

File integrity monitoring

Predictive threat modeling

Secure file transfer

Threat Intelligence

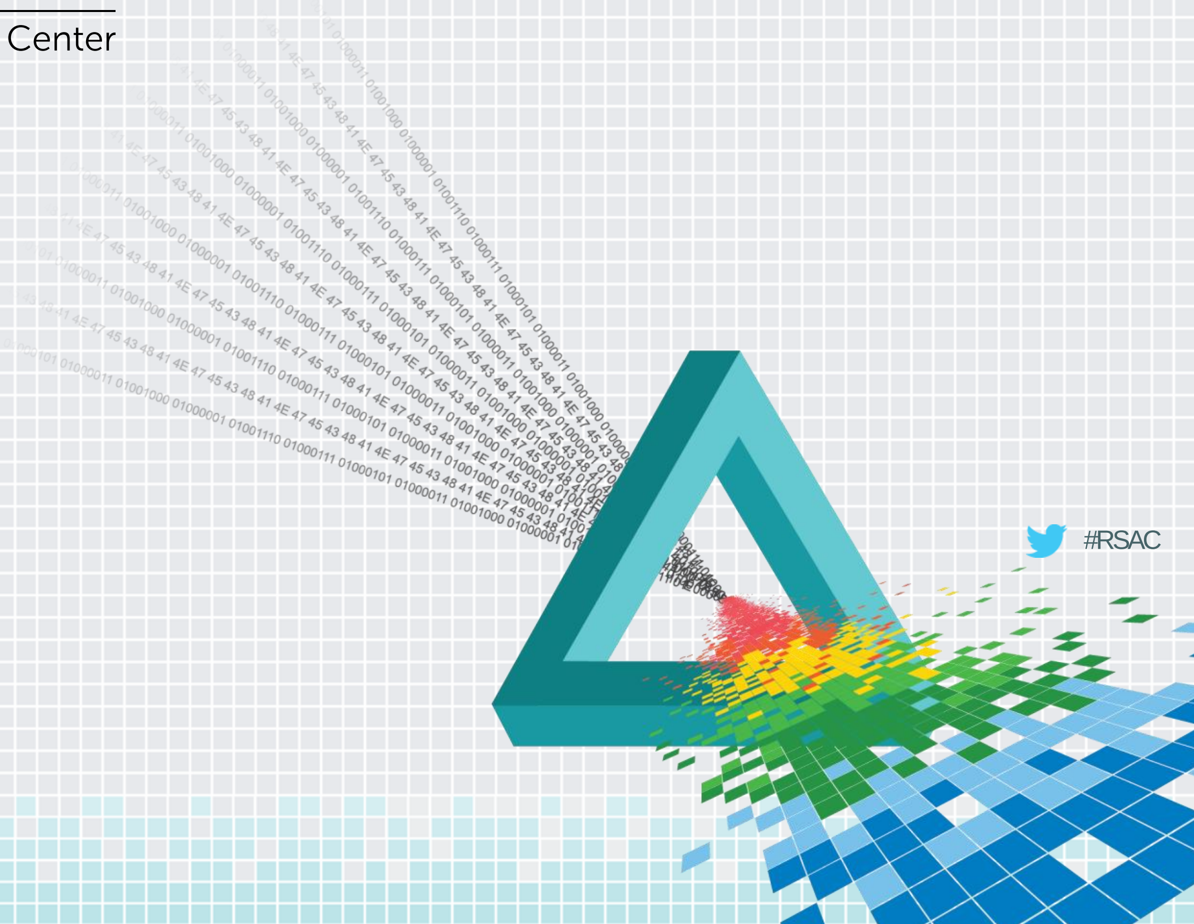
Wireless intrusion prevention system

Whitebox testing

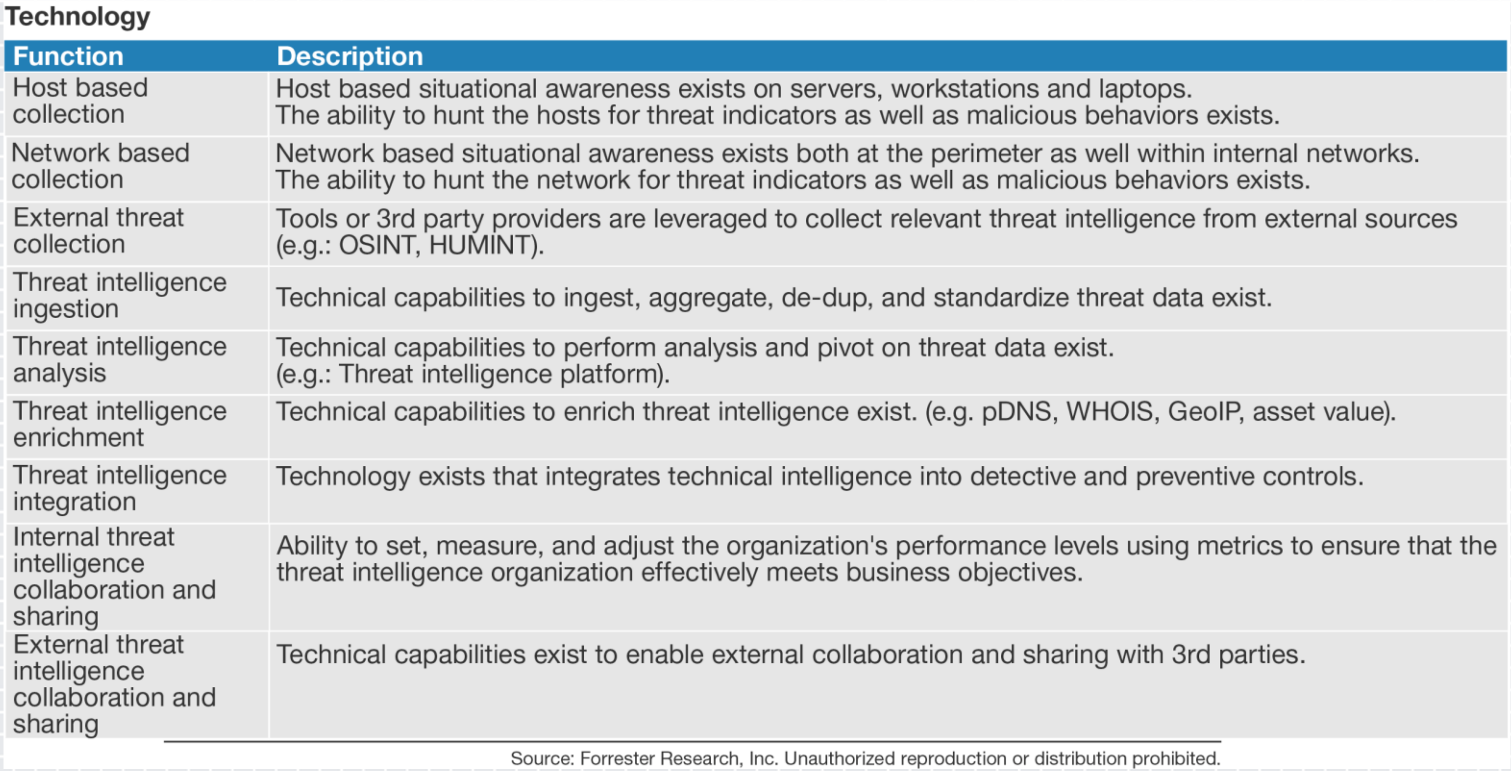
RSAConference2015

San Francisco | April 20-24 | Moscone Center

Technology



Technology

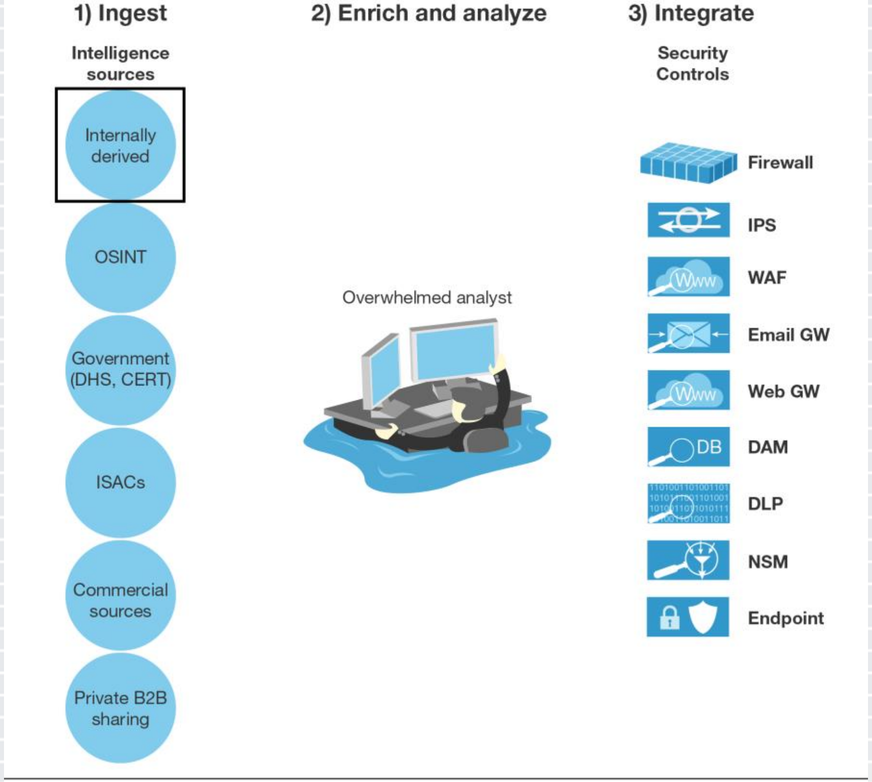


Technology

Function	Description
Host based collection	Host based situational awareness exists on servers, workstations and laptops. The ability to hunt the hosts for threat indicators as well as malicious behaviors exists.
Network based collection	Network based situational awareness exists both at the perimeter as well within internal networks. The ability to hunt the network for threat indicators as well as malicious behaviors exists.
External threat collection	Tools or 3rd party providers are leveraged to collect relevant threat intelligence from external sources (e.g.: OSINT, HUMINT).
Threat intelligence ingestion	Technical capabilities to ingest, aggregate, de-dup, and standardize threat data exist.
Threat intelligence analysis	Technical capabilities to perform analysis and pivot on threat data exist. (e.g.: Threat intelligence platform).
Threat intelligence enrichment	Technical capabilities to enrich threat intelligence exist. (e.g. pDNS, WHOIS, GeoIP, asset value).
Threat intelligence integration	Technology exists that integrates technical intelligence into detective and preventive controls.
Internal threat intelligence collaboration and sharing	Ability to set, measure, and adjust the organization's performance levels using metrics to ensure that the threat intelligence organization effectively meets business objectives.
External threat intelligence collaboration and sharing	Technical capabilities exist to enable external collaboration and sharing with 3rd parties.

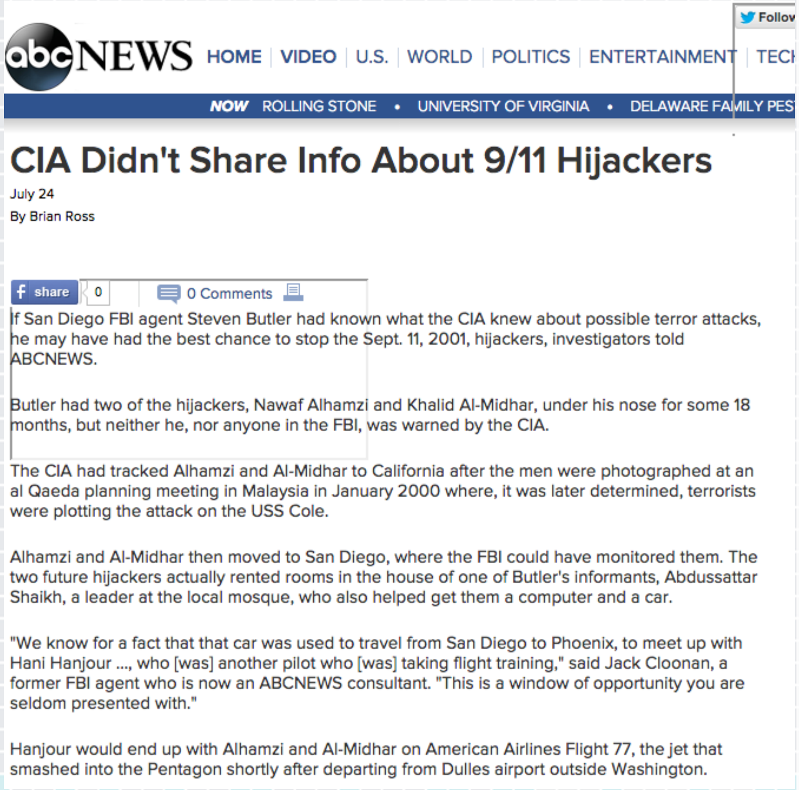
Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Operationalizing threat intelligence



Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

When actionable intelligence isn’t integrated


Follow
abcNEWS
HOME | VIDEO | U.S. | WORLD | POLITICS | ENTERTAINMENT | TECH
NOW ROLLING STONE • UNIVERSITY OF VIRGINIA • DELAWARE FAMILY PES
share 0
0 Comments

CIA Didn't Share Info About 9/11 Hijackers

July 24

By Brian Ross

If San Diego FBI agent Steven Butler had known what the CIA knew about possible terror attacks, he may have had the best chance to stop the Sept. 11, 2001, hijackers, investigators told ABCNEWS.

Butler had two of the hijackers, Nawaf Alhamzi and Khalid Al-Midhar, under his nose for some 18 months, but neither he, nor anyone in the FBI, was warned by the CIA.

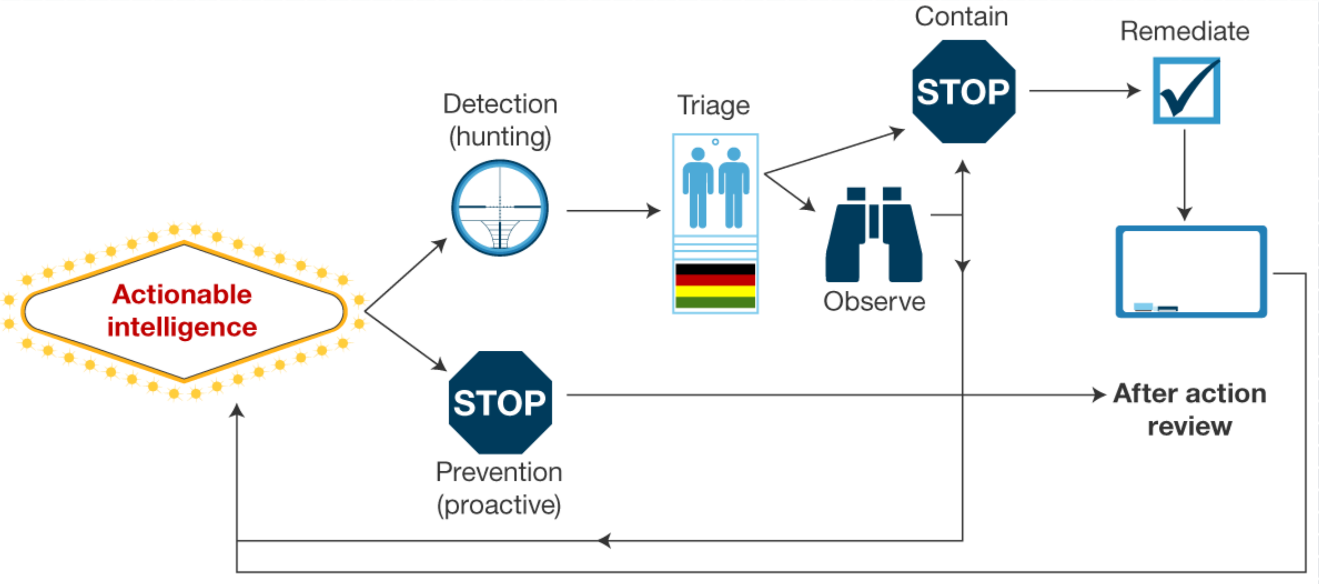
The CIA had tracked Alhamzi and Al-Midhar to California after the men were photographed at an al Qaeda planning meeting in Malaysia in January 2000 where, it was later determined, terrorists were plotting the attack on the USS Cole.

Alhamzi and Al-Midhar then moved to San Diego, where the FBI could have monitored them. The two future hijackers actually rented rooms in the house of one of Butler's informants, Abdussattar Shaikh, a leader at the local mosque, who also helped get them a computer and a car.

"We know for a fact that that car was used to travel from San Diego to Phoenix, to meet up with Hani Hanjour ..., who [was] another pilot who [was] taking flight training," said Jack Cloonan, a former FBI agent who is now an ABCNEWS consultant. "This is a window of opportunity you are seldom presented with."

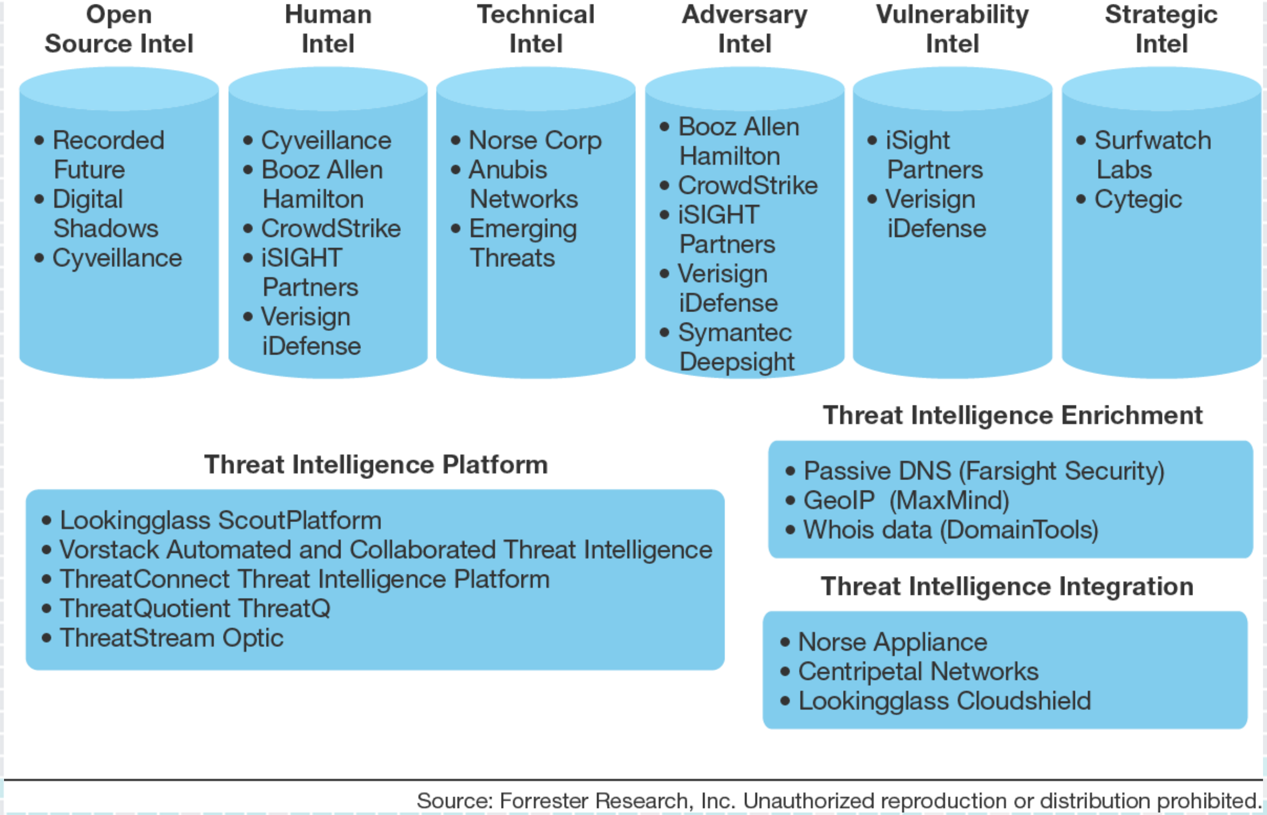
Hanjour would end up with Alhamzi and Al-Midhar on American Airlines Flight 77, the jet that smashed into the Pentagon shortly after departing from Dulles airport outside Washington.

Mature orgs integrate actionable intelligence



Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Threat intelligence market overview



Open Source Intel

- Recorded Future
- Digital Shadows
- Cyveillance

Human Intel

- Cyveillance
- Booz Allen Hamilton
- CrowdStrike
- iSIGHT Partners
- Verisign iDefense

Technical Intel

- Norse Corp
- Anubis Networks
- Emerging Threats

Adversary Intel

- Booz Allen Hamilton
- CrowdStrike
- iSIGHT Partners
- Verisign iDefense
- Symantec Deepsight

Vulnerability Intel

- iSight Partners
- Verisign iDefense

Strategic Intel

- Surfwatch Labs
- Cytegic

Threat Intelligence Platform

- Lookingglass ScoutPlatform
- Vorstack Automated and Collaborated Threat Intelligence
- ThreatConnect Threat Intelligence Platform
- ThreatQuotient ThreatQ
- ThreatStream Optic

Threat Intelligence Enrichment

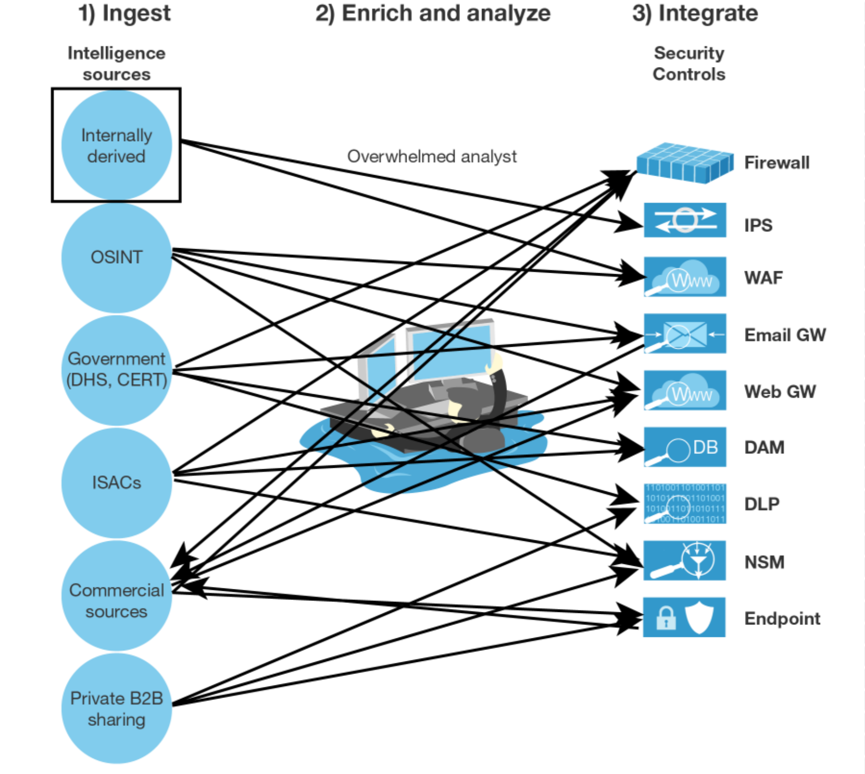
- Passive DNS (Farsight Security)
- GeoIP (MaxMind)
- Whois data (DomainTools)

Threat Intelligence Integration

- Norse Appliance
- Centripetal Networks
- Lookingglass Cloudshield

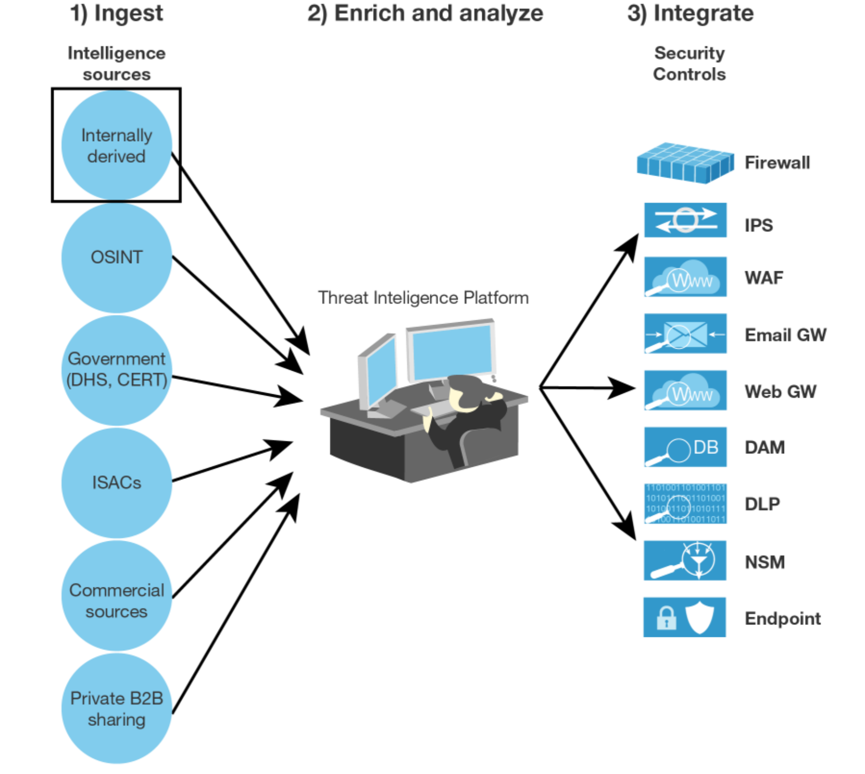
Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Operationalizing threat intelligence – This?



Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Operationalizing threat intelligence – Or This?



Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Mature orgs rely upon Threat Intelligence Platforms

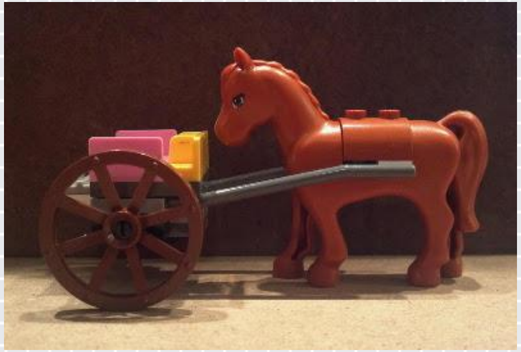
- You need a quarterback to orchestrate your intelligence work.
- You don't manage threat intel, you analyze and integrate it.

Threat Intelligence Platform functions

- Ingest threat intelligence and normalize it.
- Rate intelligence sources (over time.)
- Provide an analyst workspace.
- Provide visualization and pivoting.
- Provide enrichment.
- Enable internal and external collaboration/sharing.

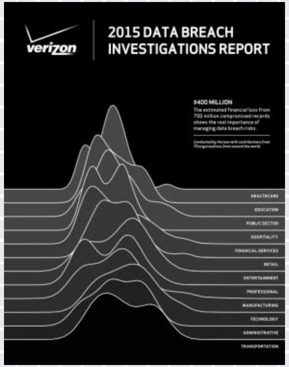
Threat intelligence sharing

- Sharing alone does not a threat intel platform make.
- Sharing is a function of a threat intel platform.
- If you cannot take action on shared intel it has little value.



Speed of sharing

- “We need to close the gap between sharing speed and attack speed.”
- “75% of attacks spread from Victim 0 to Victim 1 within one day (24 hours).”



verizon

2015 DATA BREACH INVESTIGATIONS REPORT

$400 MILLION
The estimated financial loss from 700 million compromised records shows the real importance of managing data breach risks.

Conducted by Verizon with contributions from 70 organizations from around the world.

STIX could be the answer

- STIX gained momentum in 2014, but still has a long way to go.
- Be on the look out for “checkbox STIX.”
- Ask vendors what specific use cases do they support.
- Join the conversation: https://stix.mitre.org/community/registration.html

Oversight

Prepare for the Bobs

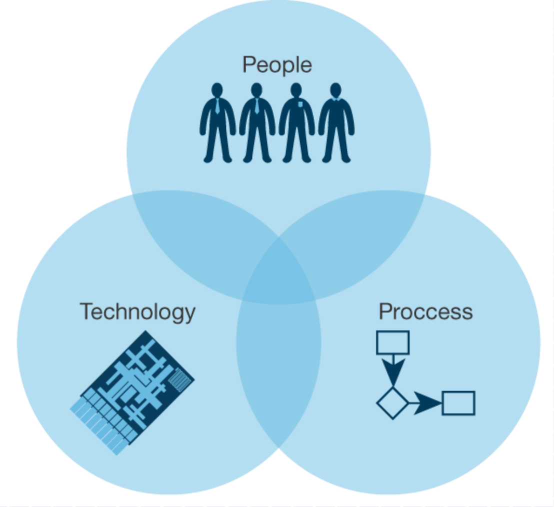
- How effective were your investments? Avoid Expense in Depth with after action reviews.
- Measure and track:
  - Time to detection, containment, remediation.
- If you cannot measure these items, invest in the situational awareness technology required to do so.

Mature firms produce strategic intelligence

- Produce your own customized version of the Verizon DBIR.
- Produce daily digest of top cybersecurity stories and their impacts.
- Use strategic intelligence products to improve the external perspective of security.

Summary

- There is no magic threat intelligence pixie dust.
- People, process and technology are all required for success.
- Threat intelligence is a long journey that ebbs and flows.



Apply what you have learned today

- Next week you should:
  - Begin a gap analysis of your existing collection capabilities.
  - Reach out to any commercial intelligence providers and have them explain why their intelligence products are aligned with your firm.
  - Start building dossiers on all future incidents and intrusions.

Apply what you have learned today

- In the first three months following this presentation you should:
  - Develop standing intelligence requirements.
  - Reevaluate all your intelligence sources, are they accurate, integrated, relevant and timely?

Apply what you have learned today

- Within six months you should:
  - Implement a strategy to recruit, train, and retain threat intelligence resources.
  - Deliver one strategic intelligence product: Analyze your intrusions and the strategic implications for your organization.

The wrong choices can be costly

VS

The wrong choices can be costly

VS

$250 / annually – It adds up

Thank you!

- Rick Holland
- +1 469.221.5359
- rholland@forrester.com
- @rickhholland
- #3daythreatintel