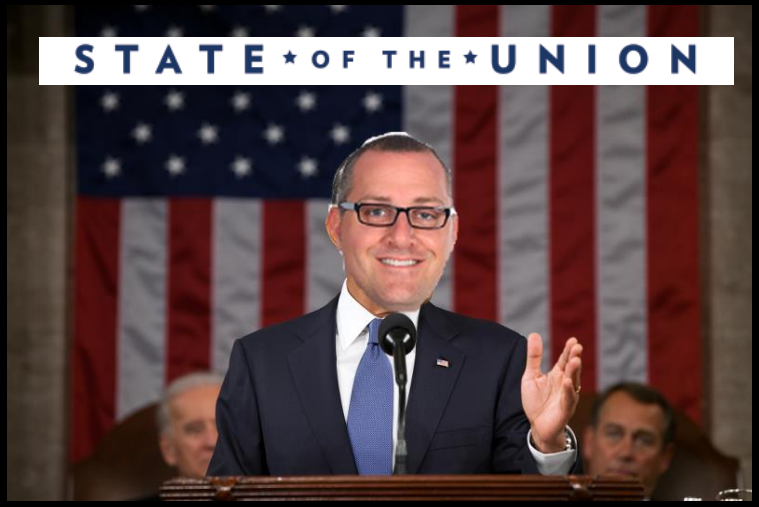
# Threat Intelligence Awakens

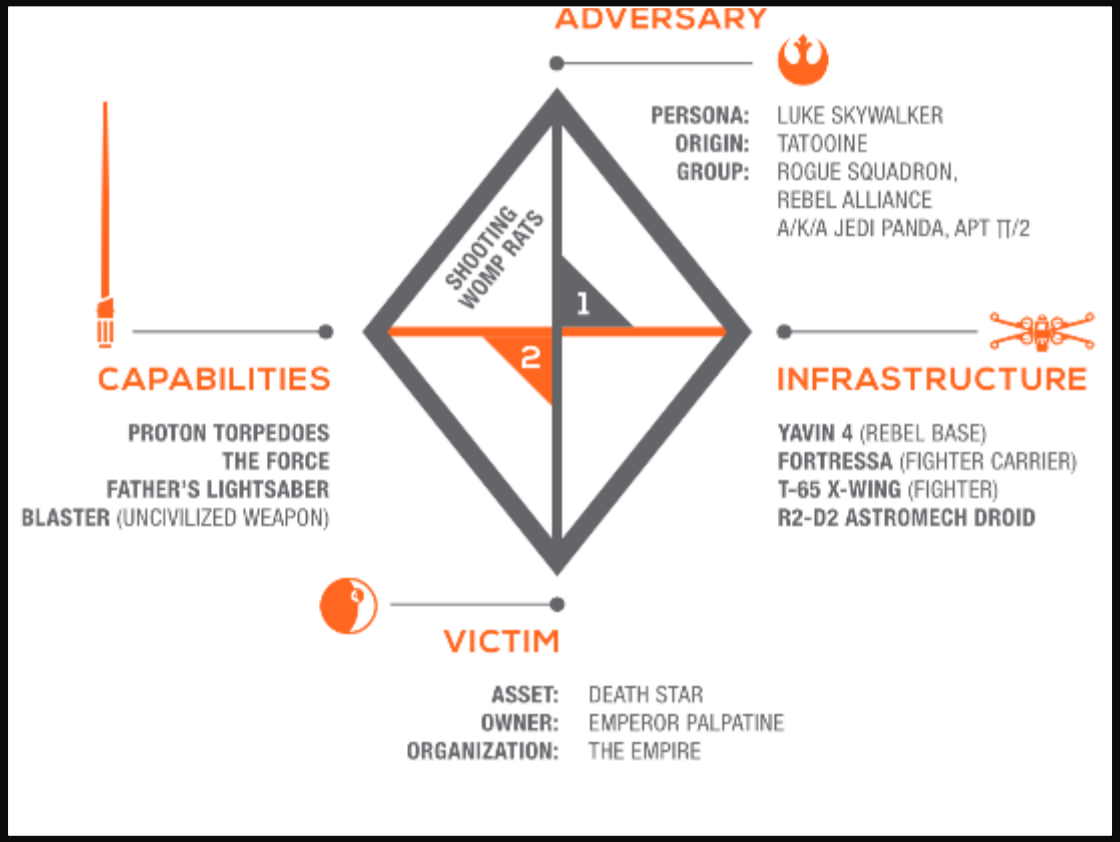
~~Rick Holland~~ (Kylo Rick)
@rickhholland
VP Strategy

digital shadows_

# A long time ago in CTI Summits far far way



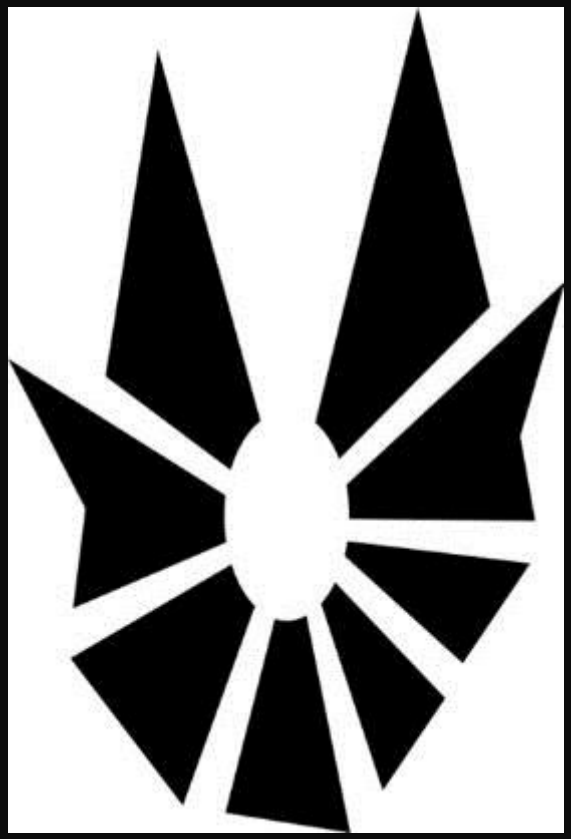

STAR WARS
THREAT INTELLIGENCE AWAKENS




# Recognizing previous work

# Episode Derp

*I felt a great disturbance in the Force, as if millions of vendors suddenly cried out with claims of* **actionable *intelligence***. I fear *something* terrible has *happened*.



# Sienar Fleet Systems


LOOKINGGLASS


CROWDSTRIKE


Recorded Future
CREATING AN INSIGHTFUL WORLD


MALCOVERY
SECURITY


PASSIVE TOTAL


BITSIGHT


THREATSTREAM


anubisnetworks


iSIGHTPARTNERS


CRITICAL
INTELLIGENCE


DIGITAL SHADOWS


NORSE


EMERGING
THREATS


FLASHPOINT

# Threat intelligence

- Providers
- Platforms
- Enrichment
- Integration

Many Bothan spies died to bring us this information (Providers)

# Providers

- Pyramid of Pain is painful for threat intel providers too
- Relevancy is hard
- Tactical, Operational, Strategic providers

# This isn’t a one stormtrooper fits all scenario

Save | Share

FOR SECURITY & RISK PROFESSIONALS

# Vendor Landscape: S&R Pros Turn To Cyberthreat Intelligence Providers For Help

*CTI Providers Must Support Every Phase Of The Intelligence Cycle*

November 3, 2015
By **Rick Holland** with Stephanie Balaouras, Claire O'Malley, Peggy Dostie


Request an Inquiry

quick scan | full report | related reports

## WHY READ THIS REPORT

The overwhelming threat landscape, coupled with the desire to transition from reactive to proactive security, is driving interest in cyberthreat intelligence. Organizations are looking to complement internally developed threat intelligence with external threat intelligence. In this report, we give S&R pros the tools to evaluate cyberthreat intelligence providers along with analysis of 20 of the top players in the space.

**Tags:** Managed Security Services Providers (MSSPs), Security Operations & Program Governance, Vulnerability & Threat Management

## KEY TAKEAWAYS

### Cyberthreat Intelligence Provides Tactical And Strategic Value

S&R pros want to better understand the threat landscape and use that knowledge to inform strategic business decisions. At the same time, they want to integrate tactical CTI into their controls to provide better protection and detection.

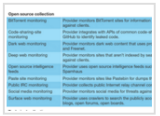
### The Intelligence Cycle Should Be The Framework For Evaluating CTI Providers

In an effort to better understand and differentiate CTI providers, S&R pros should frame their vendor analysis using the intelligence cycle and determine how the vendor supports: 1) planning and direction; 2) collection; 3) processing; 4) analysis and production; and 5) dissemination.

### S&R Pros Must Be Prepared To Quantify Threat Intelligence Benefits

The resources required to invest in internal and external threat intelligence can be significant. It's imperative that S&R leaders develop a plan to measure the return on investment in cyberthreat intelligence.

## FIGURES


# A TIP should make intel flow like The Force

- Threat intelligence should surround us and bind our security programs together, TIPs should enable this
- Gross misuse of the term “platform”
- Answering the relevancy question is a huge opportunity for TIPs

# Emerging TIP functional areas

- Ingestion
- Enrichment
- Analysis/Exploration
- Collaboration
- Integration/Orchestration

Sharing alone does not a platform make

Enrichment is delivered to the analyst (Force pull)

# Enrichment sources

- Passive DNS (Farsight)
- WHOIS (DomainTools)
- Infrastructure (PassiveTotal)
- Malware (VirusTotal)
- GeoIP (MaxMind)

# Take a look in the mirror

- We need to start focusing more efforts on internal enrichment sources
  - Identity
  - Asset
  - Data value
  - Vulnerabilities

Integrating threat intelligence today is a bit like watching Episodes 1, 2, and 3 repeatedly

# Integration

- Many APIs are weak (or non-existent)
- We perform DoS attacks against our controls
- TIPs and the emerging orchestration/automation players are trying to solve this

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life

FireEye Buys Invotas International

Nokia Shares Slump After Patent Guidance Disappoints

Strong Dollar Batters Earnings for U.S. Tech Firms

TECH

# FireEye Buys Invotas International

Cybersecurity firm acquires business spun off from CSG Systems last year

FireEye Inc.'s logo is seen outside the company's offices in Milpitas, Calif. *PHOTO: BECK DIEFENBACH/REUTERS*

By JOSH BECKERMAN

Feb. 1, 2016 8:18 p.m. ET

0 COMMENTS

INVOTAS™

# THREAT INTELLIGENCE


# Indicators of Exhaustion

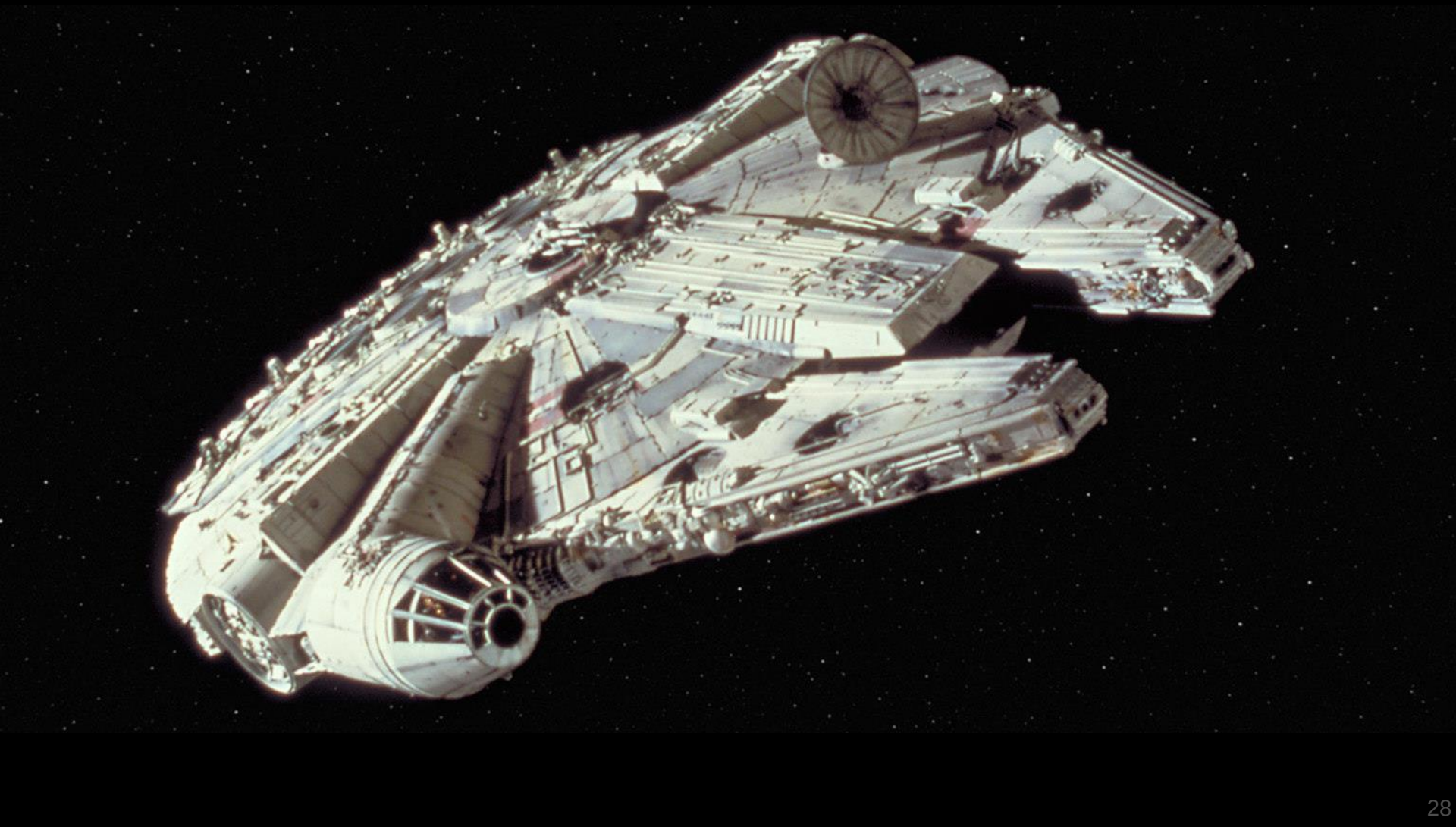

©2015 & TM Lucasfilm Ltd. All Rights Reserved. IMAX® is a registered trademark of IMAX Corporation.

# Rey is a scavenger

- Before you invest in any commercial provider, you must maximize your own intrusions
- Collect indicators & build dossiers
- No threat intel is more relevant than what is occurring within your own environment

> 35 years? And you've never fired a bowcaster? Really?

# The ship that made the Kessel Run in ~~fourteen~~ twelve parsecs



# She may not look like much, but she's got it where it counts

- You don’t have the best technology and most expensive intel sources to be effective
- You probably will never have a fusion center but you can make threat intelligence work
- The Millennium Falcon approach (DIY / Open Source tools) is perfectly acceptable

# Collaborate, find your Bros

# Collaborate, don’t just share IOCs

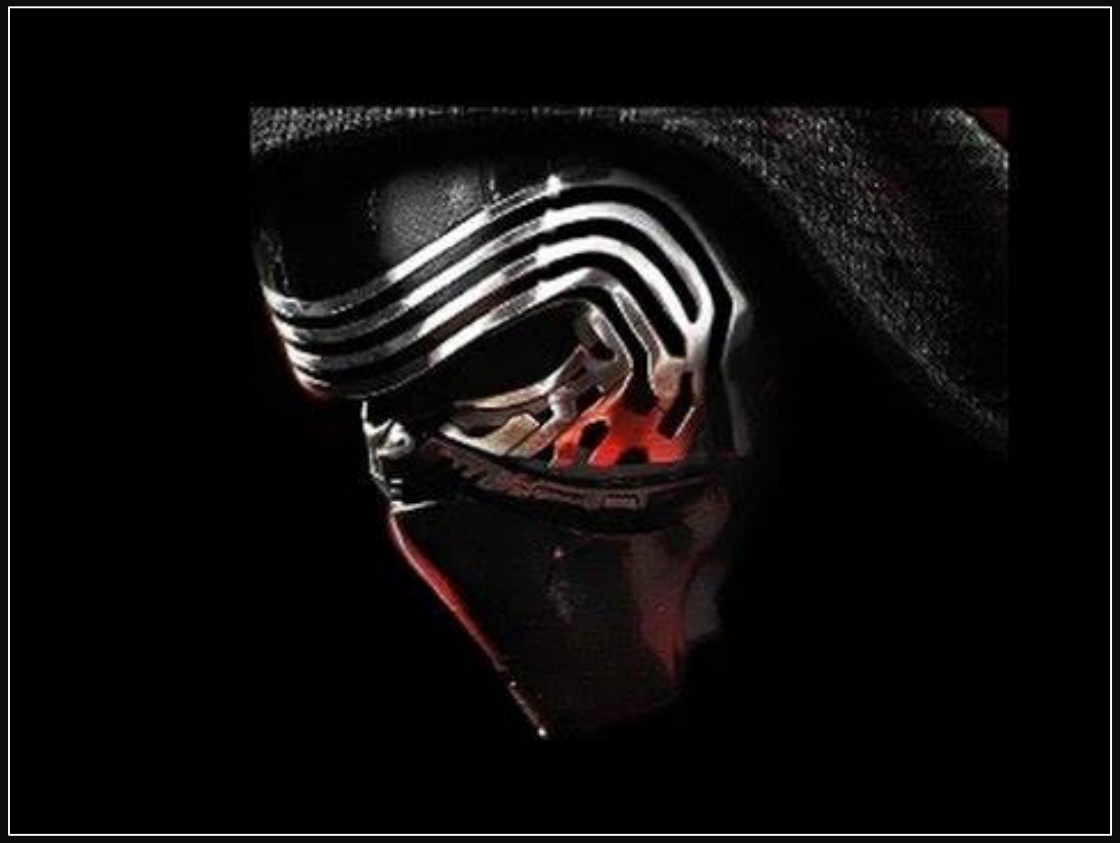
- For most sharing is putting the cart before the horse
- Share processes & tradecraft
- Share cool leather jackets

# Spawn camping

# Camp on your adversaries

- Segment the network
- Adversaries will re-spawn, funnel them to make hunting scalable

# ANALYSTS



That’s all she is, yes. A scavenger from that inconsequential Jakku.

Fear leads to anger. Anger leads to hate. Hate leads to poor analysis.

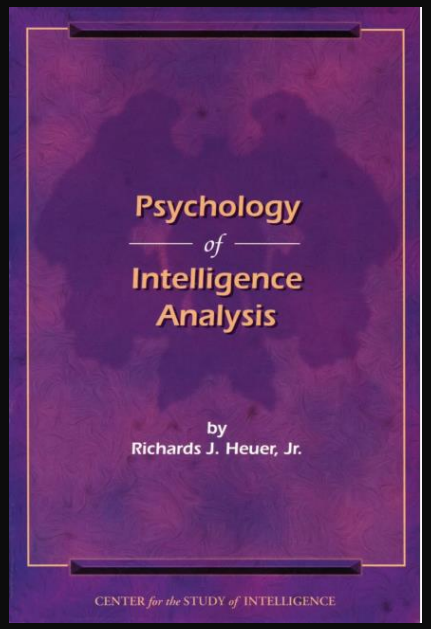
# Avoid analytical pitfalls

## PART III—COGNITIVE BIASES

### Chapter 9

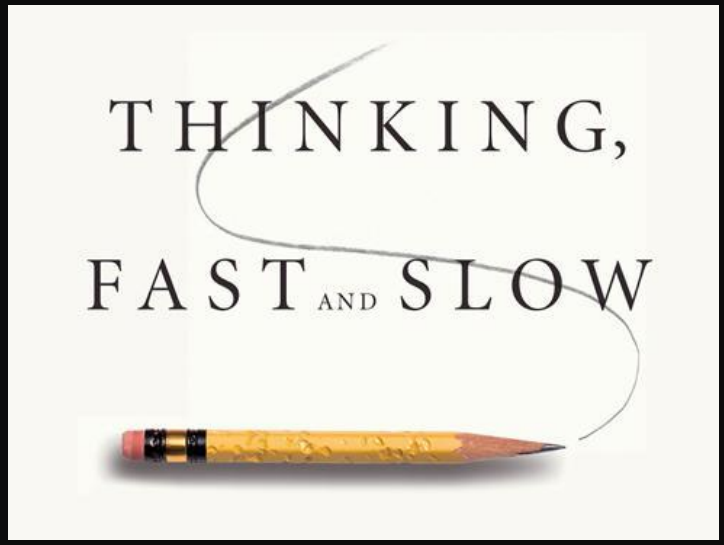
### What Are Cognitive Biases?

*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.*

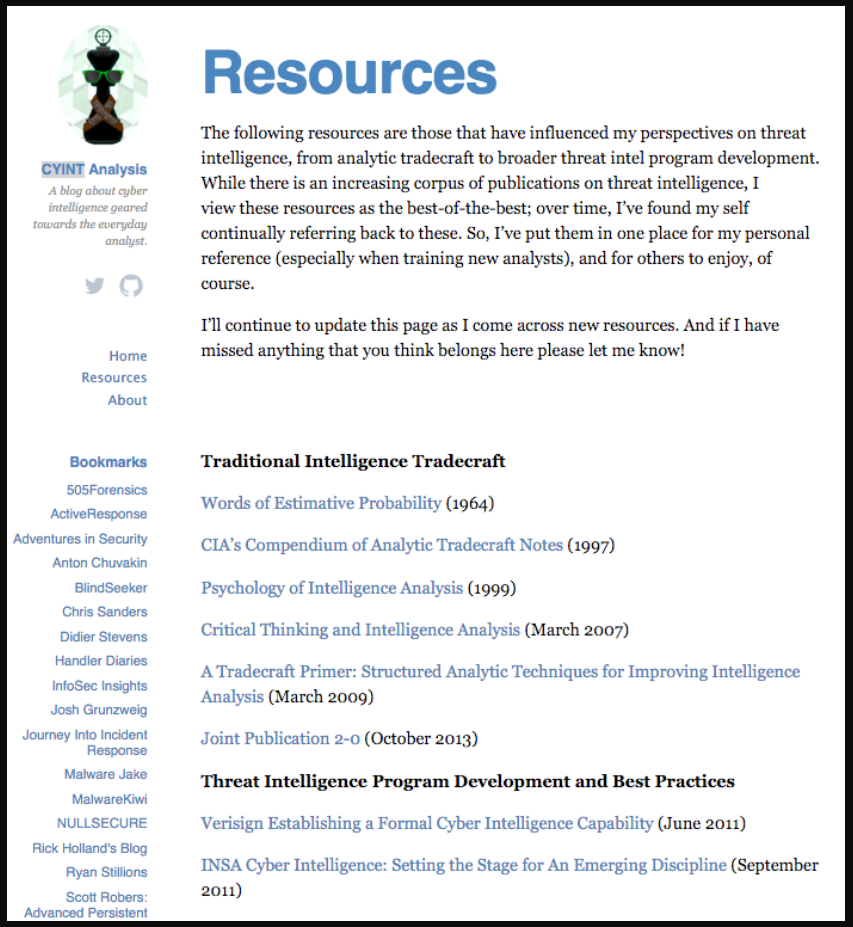


# Avoid analytical pitfalls

Daniel Kahneman reveals "where we can and cannot trust our intuitions and how we can tap into the benefits of slow thinking."



# Check out: cyintanalysis.com



CYINT Analysis

*A blog about cyber intelligence geared towards the everyday analyst.*

Home
Resources
About

**Bookmarks**

505Forensics
ActiveResponse
Adventures in Security
Anton Chuvakin
BlindSeeker
Chris Sanders
Didier Stevens
Handler Diaries
InfoSec Insights
Josh Grunzweig
Journey Into Incident Response
Malware Jake
MalwareKiwi
NULLSECURE
Rick Holland's Blog
Ryan Stillions
Scott Robers: Advanced Persistent

## Resources

The following resources are those that have influenced my perspectives on threat intelligence, from analytic tradecraft to broader threat intel program development. While there is an increasing corpus of publications on threat intelligence, I view these resources as the best-of-the-best; over time, I've found my self continually referring back to these. So, I've put them in one place for my personal reference (especially when training new analysts), and for others to enjoy, of course.

I'll continue to update this page as I come across new resources. And if I have missed anything that you think belongs here please let me know!

**Traditional Intelligence Tradecraft**

Words of Estimative Probability (1964)

CIA's Compendium of Analytic Tradecraft Notes (1997)

Psychology of Intelligence Analysis (1999)

Critical Thinking and Intelligence Analysis (March 2007)

A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis (March 2009)

Joint Publication 2-0 (October 2013)

**Threat Intelligence Program Development and Best Practices**

Verisign Establishing a Formal Cyber Intelligence Capability (June 2011)

INSA Cyber Intelligence: Setting the Stage for An Emerging Discipline (September 2011)

# Avoid analysis paralysis

- Actionable intelligence must be timely
- Don’t spend so much time performing analysis that timeliness suffers
- Ask yourself What Would Han Solo Do (WWHSD)?

# This can take too long

I never answer that question until after I've

# Easier to track down Luke than to hire intel analysts?

# Not enough analysts to go around

- Many are going to have to rely upon intel providers and MSSPs for support
- Look at providers who offer analysts on demand or tailored intelligence offerings

# You need threat intel younglings

# Retention is critical

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

# I’VE  HAVE A BAD FEELING

#CTISummit

#CTIAwakens

# Many intel programs are setup for failure

- Buy Buy Buy! Chasing silver bullets
- Buy all the feedz!
- Not prepared to demonstrate the value of threat intelligence program

# Do this

- Conduct after action reviews post intrusion and capture intelligence
- Measure and track - Time to detection, containment, remediation
- Analyze all intel sources and track sightings. Periodically reevaluate sources
- Produce your own strategic intelligence


Avoid this

# Previous public work

- SANS CTI Summit 2013 – If It Bleeds We Can Kill It
- SANS CTI Summit 2014 – Threat Intelligence Buyers Guide
- SANS CTI Summit 2015 – State of Cyber Threat Intelligence Address
- RSA Conference 2015 – Threat Intelligence is Like Three Day Potty Training

# Thank you!

@rickhholland