Pen-to-Paper & the Finished Report

The (Often Overlooked) Key to Generating Threat Intelligence
Who am I?

Christian Paredes (@cyint_dude)

* Booz Allen Hamilton since ~2010
* threat intel @ BAH since ~2012
* threat intel analysis & program build
consumption analysis ?? ACTION
finished reporting is the only way to:

* memorialize analysis; make it transparent and accessible
* preserve knowledge
* create accountability
WRITING TIPS:
1) Stare out of window.
2) Feel a bit sad.
3) Open a Word doc.
4) Stare at its Arctic blankness.
5) Sigh.
6) Go on Twitter.
Process faults
Cognitive limitations
Complexity of threats
A funny contradiction...

What we say

IOC ≠ Intelligence!
Context is king!
A funny contradiction...

What we say and...

What we do

IOC ≠ Intelligence!

Context is king!

1. Investigate!
2. Lots of notes, IOC
3. ~ fin ~

Source: Icons made by Anatoly from www.flaticon.com
“The capacity of working memory is tiny: it can only deal with about seven items of information at once.”

Complex threats* → Tough questions

* Bangladesh Bank SWIFT heist
* DNC hack
* GRIZZLY STEPPE

* What happened?
* Are we at risk?
* Can we detect or prevent this threat?

* ugh, 2016.
challenges result in...

- "analytic fragments"
- undocumented analysis
- unshared knowledge
- lack of continuity

Source: Icons made by Anatoly from www.flaticon.com
“If we did nothing but marvel at the achievements of our minds we would leave a lot left unsaid.”

the finished report
Write down everything you know about an adversary (tools and TTP's). Determine what you can accurately detect and hunt for what you can't.
Structure

Style

So what?
Structure
- Title
- Summary & key points
- Logical flow

Style

So what?
Structure
- Title
- Summary & key points
- Logical flow

Style
- Complete sentences
- Tailored to audience
- Conversational prose

So what?
Structure
* Title
* Summary & key points
* Logical flow

Style
* Complete sentences
* Tailored to audience
* Conversational prose
* Relevant!
* Opportunities for the organization

So what?
Structure

* Title
* Summary & key points
* Logical flow

Style

* Complete sentences
* Tailored to audience
* Conversational prose
* Relevant!
* Opportunities for the organization

So what?
Structure
- Title
- Summary & key points
- Logical flow

Style
- Complete sentences
- Tailored to audience
- Conversational prose
- Relevant!
- Opportunities for the organization

So what?
Structure
- Title
- Summary & key points
- Logical flow

Style
- Complete sentences
- Tailored to audience
- Conversational prose

Relevant!

So what?
- Opportunities for the organization
generating the finished report
TI Program

{ Institutionalize writing as critical tradecraft

{ Hone writing skills

TI Analyst
TI Program

Institutionalize writing as critical tradecraft

TI Analyst

Hone writing skills
What is it?
Hmm…
Our Tradecraft

Problem Solving
Diversity of Perspective
Problem Definition
Big Picture/Scope Management

Research Methodologies & Applications
Validation/Verification

Collection Management
Open Source Data
Defending Assessments

CRITICAL THINKING

COMPUTING FUNDAMENTALS
- Networks & Networking
- Operating Systems
- Databases
- Programming
- Scripting
- Data Mining

COMMUNICATION & COLLABORATION
- Technical Writing
- Writing for Leadership
- Debating Skills
- Knowing Your Audience
- Conflict Resolution
- Attention to Detail
- Assimilate New Information
- Public Speaking

DATA COLLECTION & EXAMINATION

INFORMATION SECURITY
- Vulnerability Assessments
- Cryptography
- Technical Architecture
- Information Architecture
- Network Defense
- Incident Response

TECHNICAL EXPLOITATION
- Malware
- Penetration Testing
- Social Engineering
- Web Services
- Wireless Networks
- Web Applications

Source: Cyber Intelligence: Preparing Today’s Talent For Tomorrow’s Threats,” INSA, September 2015.
“Good intelligence depends in large measure on clear, concise writing...The information CIA gathers and the analysis it produces mean little if we cannot convey them effectively.”

Style Manual and Writers Guide for Intelligence Publications, Central Intelligence Agency
TI Program

{ Institutionalize writing as critical tradecraft

TI Analyst

{ Hone writing skills
Really old school...

"Reading maketh a full man; conference a ready man; and writing an exact man... If a man write little, he had need have a great memory...." 

Francis Bacon, “On Studies,” early 1600s

Source: image from University of Cambridge.
Old school...

Cabinet Office @cabinetofficeuk - 30 Nov 2016
Winston Churchill was born #onthisday in 1874. Read the writing advice he sent to his officials when he was Prime Minister 📝
#CO100
UK Civil Service

63 1.8K 1.9K

Source: Tweet via UK Cabinet Office.
"Tell me what you know. Tell me what you don’t know. And then...tell me what you think...I will hold you accountable."

Secretary of State Colin Powell
September 13, 2004, Intelligence Reform Hearing

Source: image from Stephen Voss, TIME magazine.
What you **know** { notes, analytic fragments

What you **don't know** { information gaps

What you **think** { our assessments!
Finished reports...

- memorialize our knowledge of threats
- make knowledge accessible and transparent
- help drive action
- hold analysts accountable
- demonstrate value to the organization
Try this tomorrow...

- commit pen to paper
- structure + style + so what
- know + don’t know + think
- heed the old school advice!
Writing resources...

- Analytic Thinking & Presentation For Intelligence Producers, CIA
- Intelligence Community Directive 203
- The Economist