



# Creating REAL Threat Intelligence ... with Evernote



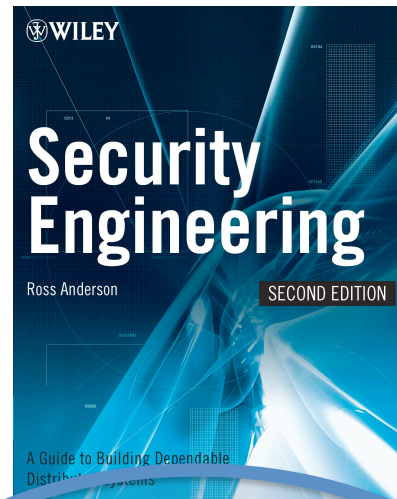
@greecs

[NovalInfosec.com](http://NovalInfosec.com)

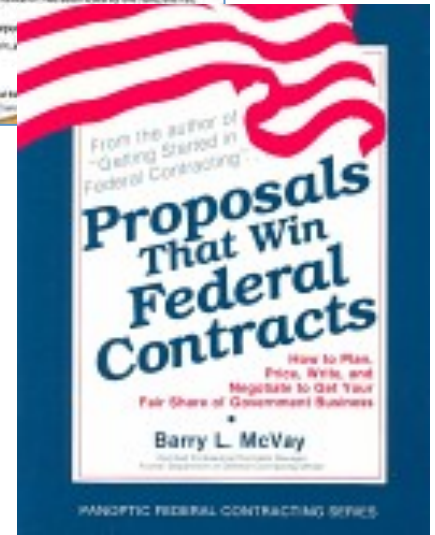
# Disclaimer

Opinions expressed are solely my own and do not express the views or opinions of my employers.





20 Yrs Industry  
16 Yrs Infosec  
5 Yrs SOC



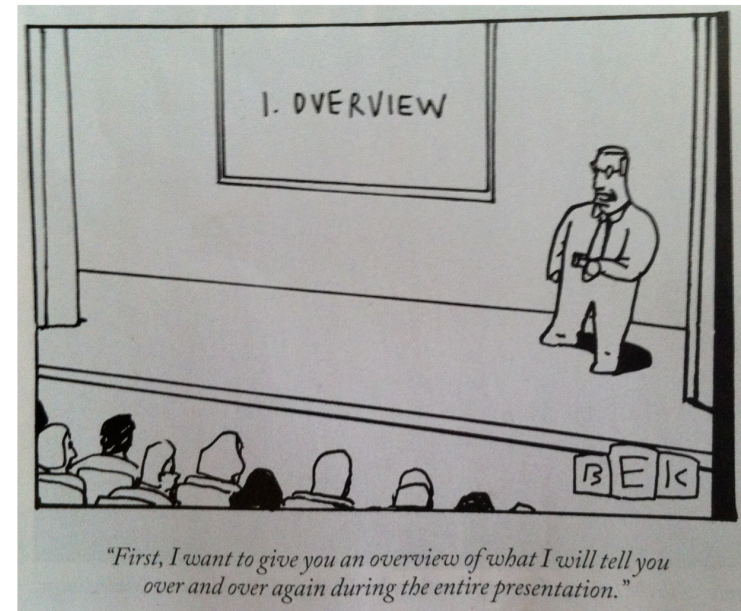
### Controller vs. FPGA Trade Study

Diffuse FPGA Trade Study V1.0

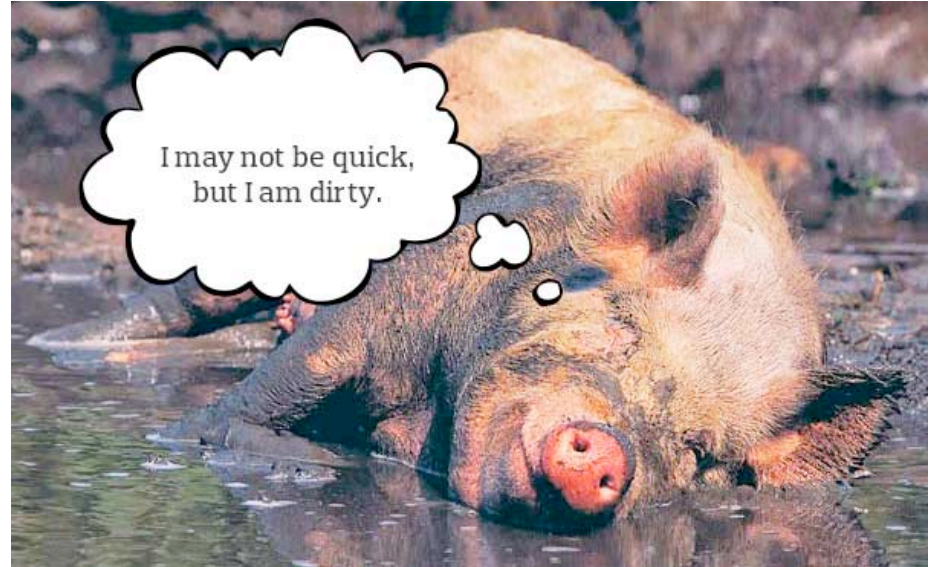
	Weight (%)	Microcontroller	Grade	Antifuse FPGA	Grade
Endurance	30%	Logical	2	Physical (rad hard by design)	5
Programming Language	20%	C	4	VHDL or Verilog	2
Power Consumption	15%	16.5 mW	4	<16.5 mW	5
Cost	10%	\$15.05	4	\$30	2
Performance	5%	\$0.00	5	\$500	2
Reconfigurable	5%	Yes	5	No	1
CubeSat Legacy	15%	Extensive	3	Unknown	1
Average Score			3.8571		2.57143
Weighted Score			3.35		3.15

# Agenda

- Background
- Dashboarding for Fun & Profit
- The Secret Weapon
- Silos of Threat Excellence
- Evernote as an Intel Repo
- Alternatives
- Future







Over Engineering

Build (at least try to) Before Buy

Problem

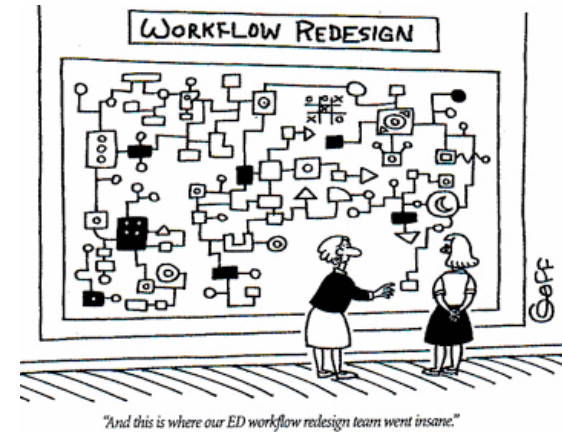
Requirements

# BACKGROUND

# Background

## Over Engineering

- Tendency to Over Complicate
- Keep It Simple Stupid
- Hiring Workflow System Example



# Background

## Build (at least try to) Before Buy



- Before Buying New Commercial Solution
  - Try Quick & Dirty Solution In-House First to get 60% There
    - Use Tools Already Have & All Familiar With
    - Setup Good Set of Processes Since Lacks Safety Checks
    - Have Smart People Actually Use Solution for 6-12 Mos.
    - Continually Evolve Processes with Lessons Learned
  - Maybe that Will Solve Your Needs
  - Else Understand What REALLY Need → Commercial
- Invest in People & Process First, then Products

Case In Point: Threat Intel Services

# Background Problem

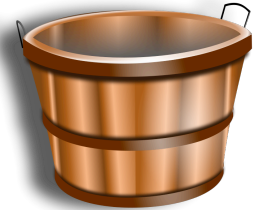


- Working as Analyst
  - Looking to Take Advantage of OS Intel
  - Required Searching Through Sites One-by-One
- Restrictions
  - No Organization Provided Option
  - No Option to Build Own System Internally
- Build My Own
  - Hosted Externally
  - Accessible Internally

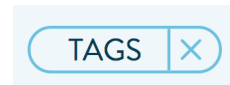
# Background Requirements



- Bucket to Dump All Data Into
  - Blog/Other Feeds
  - Data-Driven Feeds
  - Data Files
  - Other (anything else find – e.g., APT reports)



- Easily Find Data
  - Searchable
  - Categories
  - Tagging for Viewing in Different Ways



- Cloud-Based So Wouldn't Have to Maintain & Accessible Everywhere

Analyst Point of View, Not Machine





Dashboard 1.0

Dashboard 2.0

Dashboard 3.0

Take-Aways

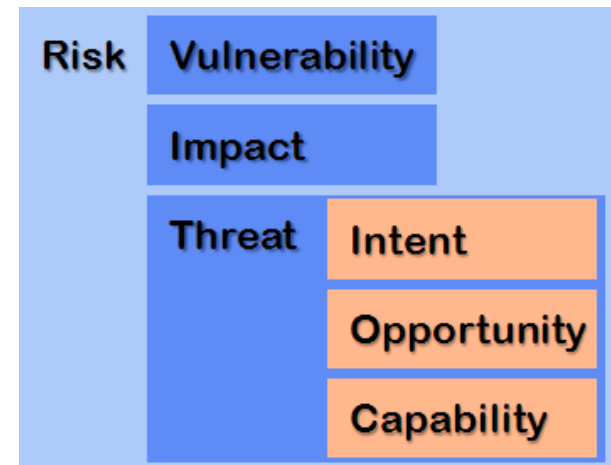
# DASHBOARDING FOR FUN & PROFIT

# Dashboarding for fun & Profit

## Dashboard 1.0



- SOC Security Engineer Position  
Many Years Ago Working to Create Dashboards
- Wanted to Measure Risk
- Use Traditional Risk Equation
  - Vulnerability Data Based on Patch & Other Tools
  - Threat? Decided to Use Vendor Threat Levels (e.g., SANS INFOCON, Symantec – normalize and average)



# Dashboarding for fun & Profit

## Dashboard 2.0 – Google Reader, iGoogle, Feedly

The image displays three overlapping web dashboards used for content aggregation and security monitoring.

**Google Reader (129)**

mark all as read | refresh

**Gadget - Vulnerabilities** 375

- National Vulnerability Data... 329
- Vulnerabilities RSS Feed - ... 46

**Gadget - Threats** 151

- Exploit-DB updates 87
- Threats RSS Feed - Syman... 64
- IBM Internet Security System...
- Twitter / Shadowserver
- Twitter / ThreatLevel

**Gadget - Risks** 62

- F-Secure Antivirus Researc... 7
- SANS Internet Storm Cente... 55
- IBM Internet Security System...
- Latest Risks RSS Feed - Sym...
- McAfee Avert Labs

**Gadget - Vulnerabilities** 375 unread articles

**FEATURED**

Article	Count	CVE ID	Product	Description
National Vulner...	1	CVE-2015-0916 (cacti)	SQL injection vulnerabil	
National Vulner...	1	CVE-2015-0915 (maildealer)	Cross-site scripti	
National Vulner...	3	CVE-2015-1251 (chrome)	Use-after-free vulner	

**LATEST**

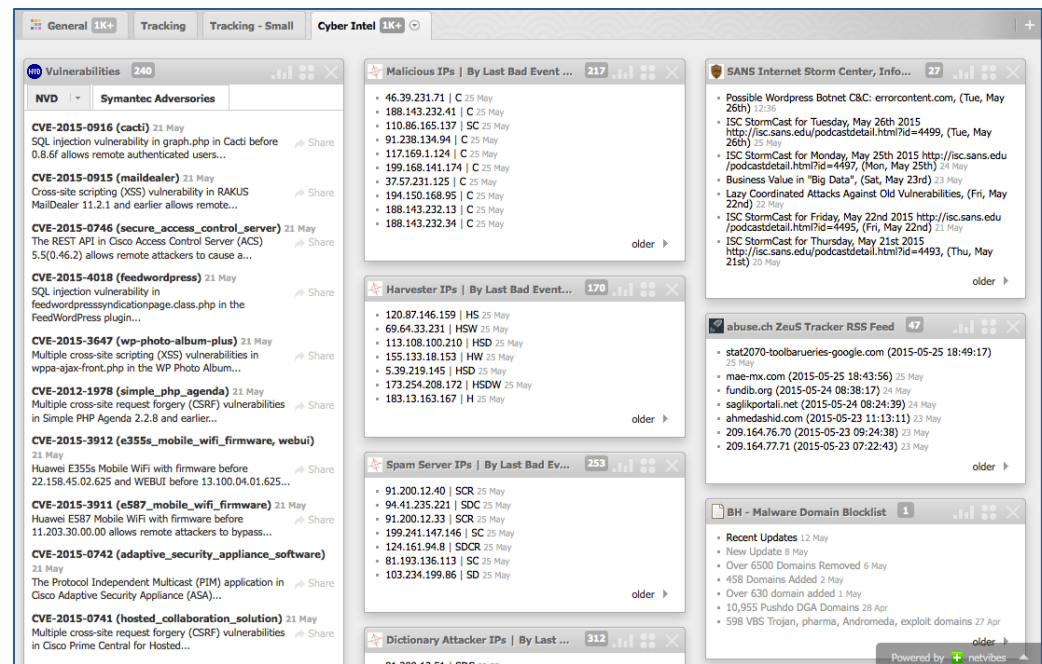
Article	Count	CVE ID	Product	Description
National Vulner...	1	CVE-2015-0746 (secure_access_control_ser		
National Vulner...		CVE-2015-4018 (feedwordpress)	SQL injectio	
National Vulner...		CVE-2015-3647 (wp-photo-album-plus)	Multi	
National Vulner...	1	CVE-2012-1978 (simple_php_agenda)	Multi	
National Vulner...		CVE-2015-3912 (e355s_mobile_wifi_firmware		
National Vulner...		CVE-2015-3911 (e587_mobile_wifi_firmware)		

# Dashboarding for fun & Profit

## Dashboard 3.0

Once upon a time...

- Moved from Feedly to Netvibes Since Designed Ground Up as Dashboard
- Added “Cyber Intel” Tab with Sources Still Active from Feedly



# Dashboarding for fun & Profit

## Take-Aways



- Nice for “Blog” Post Feeds
- Tough to Follow for Data-Driven Feeds
  - Changing Too Fast
  - Feedly Pro & NetVibes VIP
- Doesn’t Work for Periodically Updated Data Files

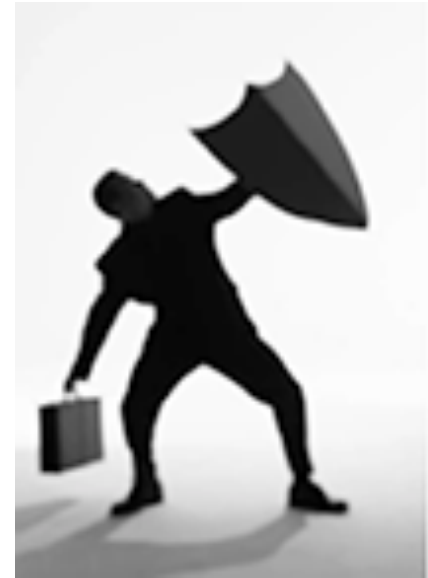
Identified Many Great Sources of Info to Collect



Overview

Customization

# THE SECRET WEAPON

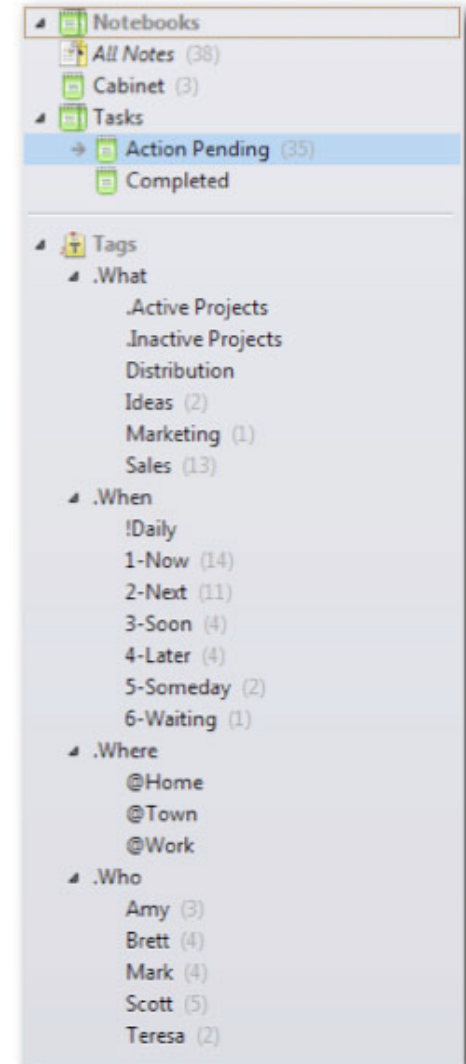


# The Secret Weapon

## Overview



- Method for Using Evernote as GTD-Based Task Mgmt System
  - Treat Evernote Like a Database
  - Notebook == Table
  - Note == Free Form Record
- Organization
  - Nested Notebooks
  - Hierarchical Tagging (provide metadata structure)
    - What → Projects
    - When → Importance – e.g., 0-6
    - Where → E.g., home, work, etc.
    - Who → E.g., people that action has to do with
    - Combination Above
- Search
  - ~ Notebook, Tag, Keyword, or Combination Thereof
  - Saved Searches



# The Secret Weapon Customization



## !When

- !0-Daily
- !1-Now
- !2-Next
- !3-Soon
- !4-Later
- !5-Some
- !6-Wait

## ].What

- > ].Community
- > ].Inactive Projects
- > ].OSINT DB
- > ].Other
- > ].Personal
- > ].Twitter Archive
- > ].Work

## @.Where

- @community
- @errands
- @home
- @personal
- @work

## ^.Who

- > ^.Active People
- > ^.Inactive People
- > ^.OSINT DB
- > ^.Twitter Archive
- > Misc

## Shortcuts

- !0-Daily
- !1-Now @community
- !1-Now @personal
- !1-Now @work
- !2-Next @community
- !2-Next @personal
- !2-Next @work

Background  
Threat Intel?  
Relevancy  
Sources

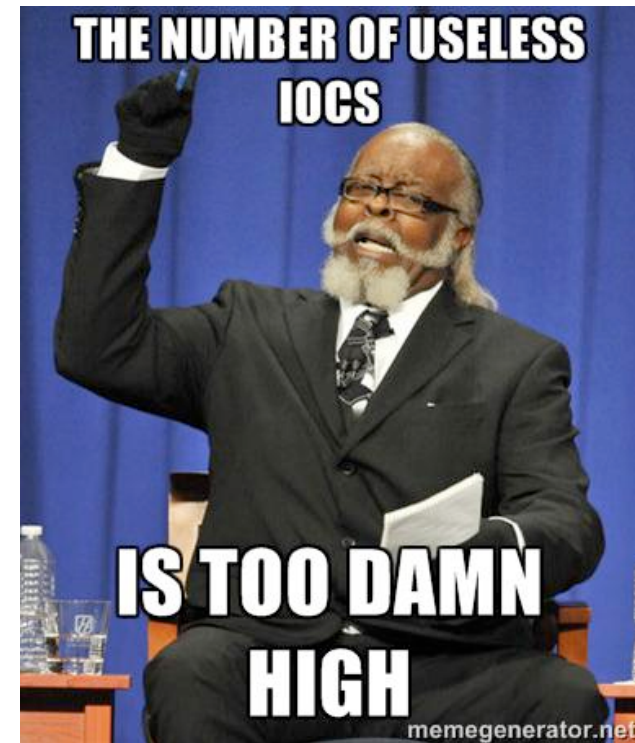


# SILOS OF THREAT EXCELLENCE

# Silos of Threat Excellence

## Background

- Threat Intel Market Growing
  - Investigating Threat Intel
  - Consulted Experts & Users of Threat Intel Services
- Basic Take-Aways
  - Fascinating Area with Lots of Cool Things Mathematically Correlated Together in Some Fancy Big Data Model
  - Follow Good Set of People on Twitter
  - Not Much Value Beyond Open Source Resources (WHY?)

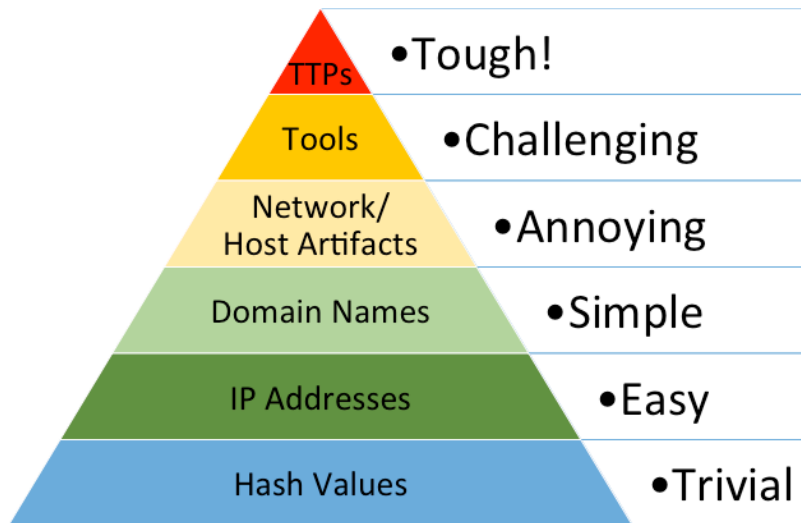


“When your threat intel solution is feeling more like a threat intel problem...” - @JohnLaTwC

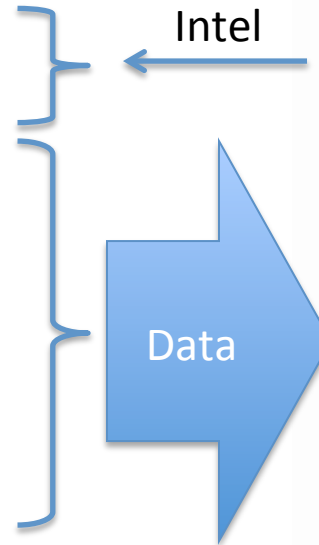


# Silos of Threat Excellence

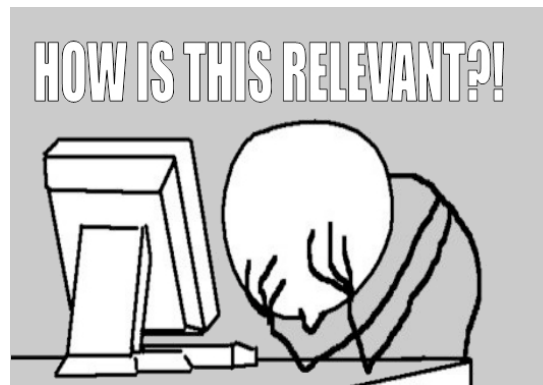
## Threat Intel?



“The Pyramid of Pain” - David Bianco

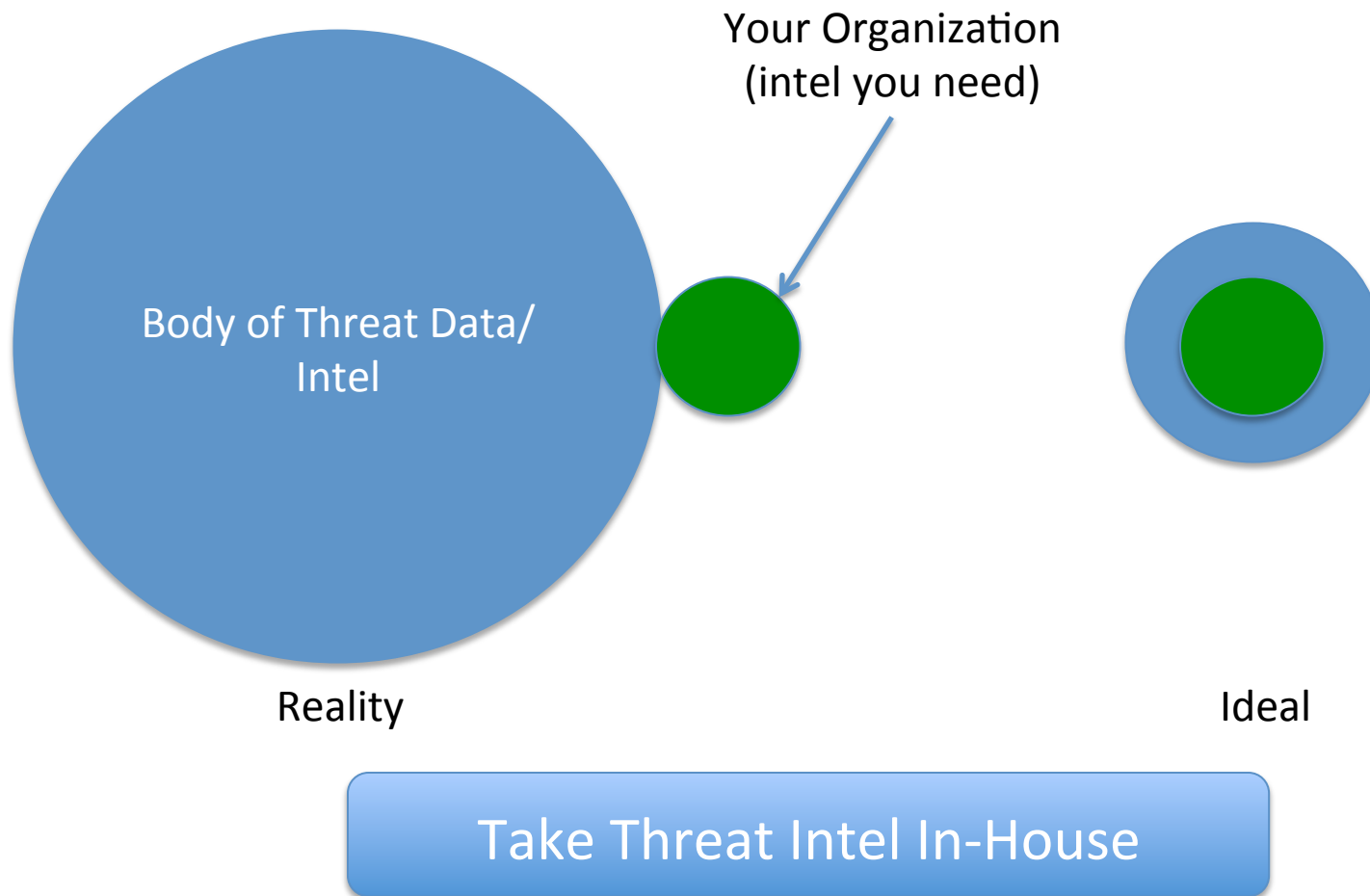


“An Introduction to Cyber Intelligence” – Rob Lee



# Silos of Threat Excellence

## Relevancy



# Silos of Threat Excellence Sources



- Open Source Intel
  - Historically Lots of OS Resources (e.g., MalwareDomainList, Zeus Tracker, ...)
  - Don't Forget Social Networks (e.g., certain people/resources on Twitter)
- Information Sharing
  - Many Existing Groups (e.g., ISACs)
  - Email Lists/Bulletin Boards but Slowly Migrating to Standardized Formats (TAXII, STIX)
- Log Collection
  - Dump of Desired Logs for Later Analysis If Needed
- SIEM
  - Log of Security Alerts
  - Correlations (but not many take advantage of)
- Case Tracking
  - Pretty Simple with Many Existing Workflow Systems (Open → Working → ... → Closed)
  - Many Existing OS / Proprietary Solutions (eTicket, Help Desk Lite, Remedy, SharePoint)

Ah Ha  
OSINT  
Beyond OSINT  
Analysis  
EN Search  
Analytics Framework  
Alternatives



# EVERNOTE AS AN INTEL REPO

# Evernote as an Intel Repo

Ah Ha



Dashboarding + Secret Weapon + Threat Intel  
= Evernote as an Intel Repo

- Define Notebooks & Hierarchical Tags for Metadata
- Perfect Open & Flexible Framework to Build Off Of
- Easy to Use Over Heavy Database or Workflow Management System
- Start Dumping All Feeds/Data into Evernote Bucket



# Evernote as an Intel Repo

## OSINT

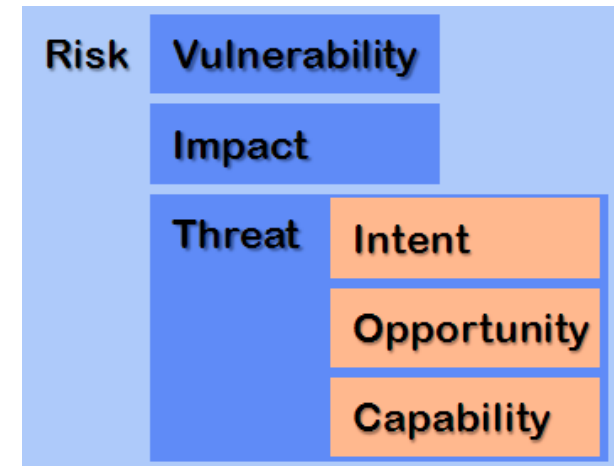


- Archive of Organization Relevant Data from Open Source Resources
- Benefits
  - “Database” Can Search and Pivot Around In
  - Annotation of Notes
- Dumping
  - Automated via Feeds
  - Clip into Evernote with Browser Add-On
- Recommended Tagging Structure

# Evernote as an Intel Repo OSINT



- Threat
  - MalwareDomainList (RSS)
  - Zeus Tracker (RSS)
  - SSL Blacklist (RSS)
  - Malware-Analysis Traffic (RSS)
  - Dynamoo (RSS)
  - @sshbrute, @netmenaces (Twitter)
- Vulnerability
  - Offensive Security Exploit Database (RSS)
  - NIST NVD CVE (RSS)
  - US CERT All Products (RSS)
- Situational Awareness
  - SANS ISC Blog (RSS)
  - ThreatBrief (RSS)



# Evernote as an Intel Repo

## OSINT



▼ ].What

▶ ].Community

▶ ].Inactive Projects

▼ ].OSINT DB

]All NCAS Products

]Blog

]Domains

]Exploit-DB

]HostsList

]ISC

]NVD

]NVD-Analyzed

]OSINT-DB

]SSLBL

]Zeus Tracker

Created

Yesterday, 7:46 AM

Friday, May 22, 2015 at

Tuesday, May 19, 2015 at

Monday, May 18, 2015 at

Thursday, May 14, 2015 at

▶ @.Where

▼ ^.Who

▶ ^.Active People

▶ ^.Inactive People

▼ ^.OSINT DB

^Abuse.ch

^MalwareDomains

^MAT

^MDL

^NIST

^Offensive Security

^SANS

^US-CERT

The US-CERT (National Cyber Security Center) modified or updated the vulnerability information.

The vulnerability information is available in the [National Cyber Security Center Vulnerability Scoring System](#).

High - Vulnerability

# Evernote as an Intel Repo

## OSINT - Automation

- Email into Evernote
  - Sign Up for Service Using Evernote Email
- IFTTT for RSS Feeds
  - Easily to Implement
  - Limit of Only Getting Partial Data
  - Write Own RSS Scraper / FiveFilter
- IFTTT Interface with Twitter
- IFTTT with Email Integration
  - Helps Some if Offer Mailing List with Full Data
- StormStack - Open Source Clone+ of IFTTT
- Scripts
  - E.g., Retrieve Files & Insert into Evernote





```
#!/bin/bash
```

# Evernote as an Intel Repo

## OSINT – IFTTT Automation



if 

then 


New tweet by specific user  
[@sshbrute](#)

Create a note in [grecls's Evernote](#)


**Recipe Title**  
If new item from Twitter user SSHBrute, then Create a note in GreCs #OSINT-DB  
use '#' to add tags

**Action**


Create a note  
This Action will create a new note in the notebook you specify.

 **Title**


@  :

 **Body**

via Twitter <http://twitter.com/>

 **Notebook**


Leave blank for default notebook

 **Tags**

Comma separated

**Trigger**

New tweet by a specific user  
This Trigger fires every time the Twitter user you specify tweets.

 **Username to watch**

# Evernote as an Intel Repo

## OSINT – Script Automation



```
#!/bin/bash
# Next get so don't have to write a file.
remote_desc="malwaredomains_domains"
remote_file="http://mirror1.malwaredomains.com/files/domains.txt"
local_path=[REDACTED]
email_address=[REDACTED]
email_subject="@Greccs OSINT DB #]OSINT-DB #^MalwareDomains #]Domains"
check_date=`date +%Y-%m-%d-%Y %T`

if [ ! -f $local_path/${remote_desc}_sha_previous.sha1sum ]
then
    touch $local_path/${remote_desc}_sha_previous.sha1sum
fi
sha_previous=`cat $local_path/${remote_desc}_sha_previous.sha1sum`

# Download latest file and hash it
wget -q -O $local_path/_temp_download $remote_file
sha_latest=$(sha1sum $local_path/_temp_download | gawk '{print $1}')

if [[ "$sha_latest" != "$sha_previous" ]]
then
    echo "$check_date Updated $remote_file detected" >> $local_path/${remote_desc}_update.log
    mail -s "$remote_file Update $email_subject" $email_address < $local_path/_temp_download
    echo "$sha_latest" > $local_path/${remote_desc}_sha_previous.sha1sum
else
    echo "$check_date No update to $remote_file" >> $local_path/${remote_desc}_update.log
fi

rm -f _temp_download

exit
malwaredomains_domains_update (END)
```

Thanks for Initial Script:  
Ameer M.

# Evernote as an Intel Repo

## Beyond OSINT



- Inputs
  - Information Sharing
    - Shared Evernote Notebook for Partner Group
    - Create Note, Place in Shared Notebook to Distribute, & Use Standard Tags to Track
  - Other: Log Collection, SIEM
- Analysis
  - Case Tracking
    - Evernote Notebook with a Note per Investigation
    - Establish Note Template
    - Tags to Id Workflow (e.g., Open, Working, Closed)
  - Other: Indicator DB, Adversary DB, ...



# Evernote as an Intel Repo

## EN Search



- How to Find Find All Data Threw into Evernote
  - Tags
  - Basic Search
  - Advanced Search
    - Specific Notebooks, Tags, Terms, Dates
    - “AND” Boolean Support
- Example
  - Search for IP & Find Note
  - Run Secondary Search Around that Timeline
  - Discovery Similar Happenings
- Saved Searches (e.g., finding open cases)

# Evernote as an Intel Repo

## Analytics – Input Reserved Tags



	Priority, Confidence, Rep	Data Type	Workflow or State	Source or Who Added/Upd
	When	What	Where	Who
<b>OSINT DB</b>		OSINT DB NVD Exploit-DB Zeus Tracker	OSINT DB (no tag -> new) Useful Useless	OSINT DB NIST Offensive Sec Abuse.ch
<b>Intel Sharing</b>		Intel Sharing DIB FS-ISAC	Intel Sharing (no tag -> new) Relevant Irrelevant	Intel Sharing Company A Company B Company C
<b>Log Collect.</b>		Logger Web Logs ...	Logger (no tag -> new) ...	Logger NovalInfosec ...
<b>SIEM</b>		SIEM Site Lockout File Change	SIEM (no tag -> new) Investigating Reviewed	SIEM NovalInfosec

# Evernote as an Intel Repo

## Analytics – Analysis Reserved Tags



	Priority, Confidence, Rep	Data Type	Workflow or State	Source or Who Added/Upd
	When (!./!)	What ([./])	Where (@./@)	^.Who (^./^)
<b>Case Tracking</b>	Case Tracking High Medium Low	<b>** Case Tracking</b> CAS10000 CAS10001	Case Tracking Inbox Working Closed	Case Tracking jsmith acren
<b>Indica. DB</b>	Indicator DB HVI MVI LVI	<b>** Indicator DB</b> 192.168.2.50 smith@tch.com	Indicator DB Suggested Active Inactive	Indicator DB jsmith acren
<b>Advers. DB</b>	Adversary Important Not Important	<b>** Adversary</b> ABC DEF	Adversary Proposed Tracking Dormant	Adversary jsmith acren

Only Tag if Relevant

Primary Tags (\*\*) Used to Cross-Ref

# Alternatives

- Log Management Solutions

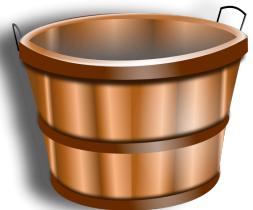
graylog  logstash splunk>

- SIEMs

 ossim by AlienVault nitrosecurity  ArcSight 

- Others

 MediaWiki Because ideas want to be free.   SharePoint 



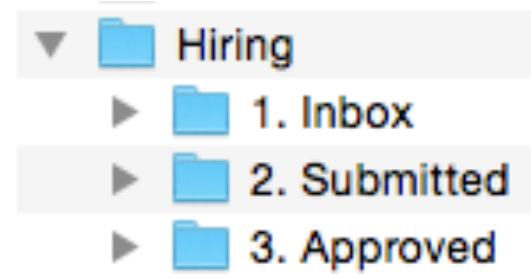
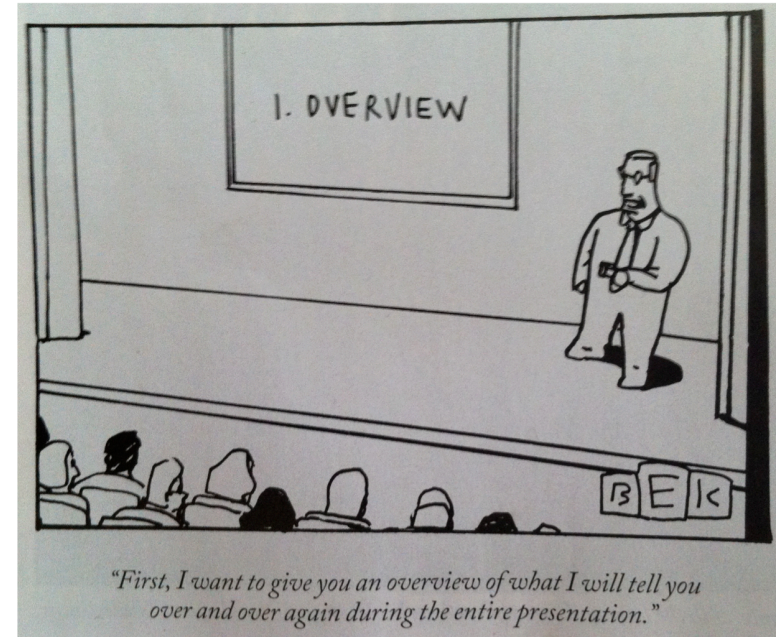
# Future



- More/Improved OSINT Resources
  - Deconflict Sites with Multiple Feeds & Add if Needed
  - File Base Pulls (script / replace existing RSS)
  - Vendor APT Reports
  - Integration with CIF to Centralize/Tag Data
- Improved/Formalized Tagging Structures
- API Automation (e.g., auto tagging IP addresses)
- 3<sup>rd</sup> Party App that Uses Evernote as Backend

# Conclusion

- Lots of Point Solutions but None Bring Together Like Good 'ol Evernote
- Start with Evernote to "Figure Stuff Out"
- In End Determine REAL Requirements
  - Solution Fine As Is
  - Build In-House/Buy Commercial Full Out Solution



# Thanks & Questions



- Twitter
- Website
- Contact

[@greCs](#)

[Novainfosec.com](http://Novainfosec.com), [@novainfosec](#)

<http://bit.ly/nispcontact>