

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: STR-R02

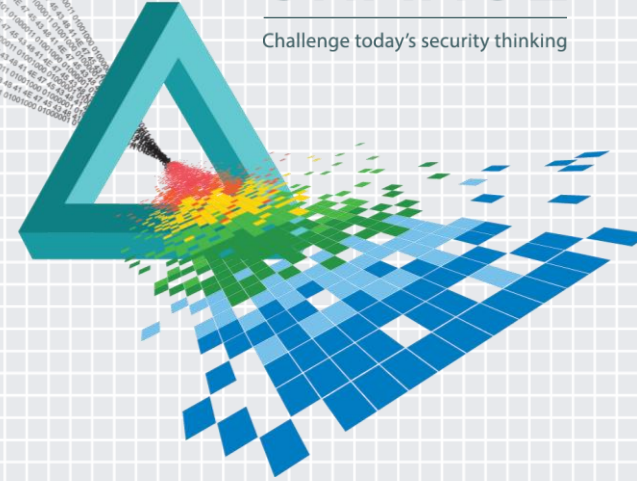
Threat Intelligence is Dead. Long Live Threat Intelligence!

Mark Orlando

Director of Cyber Operations
Foreground Security

CHANGE

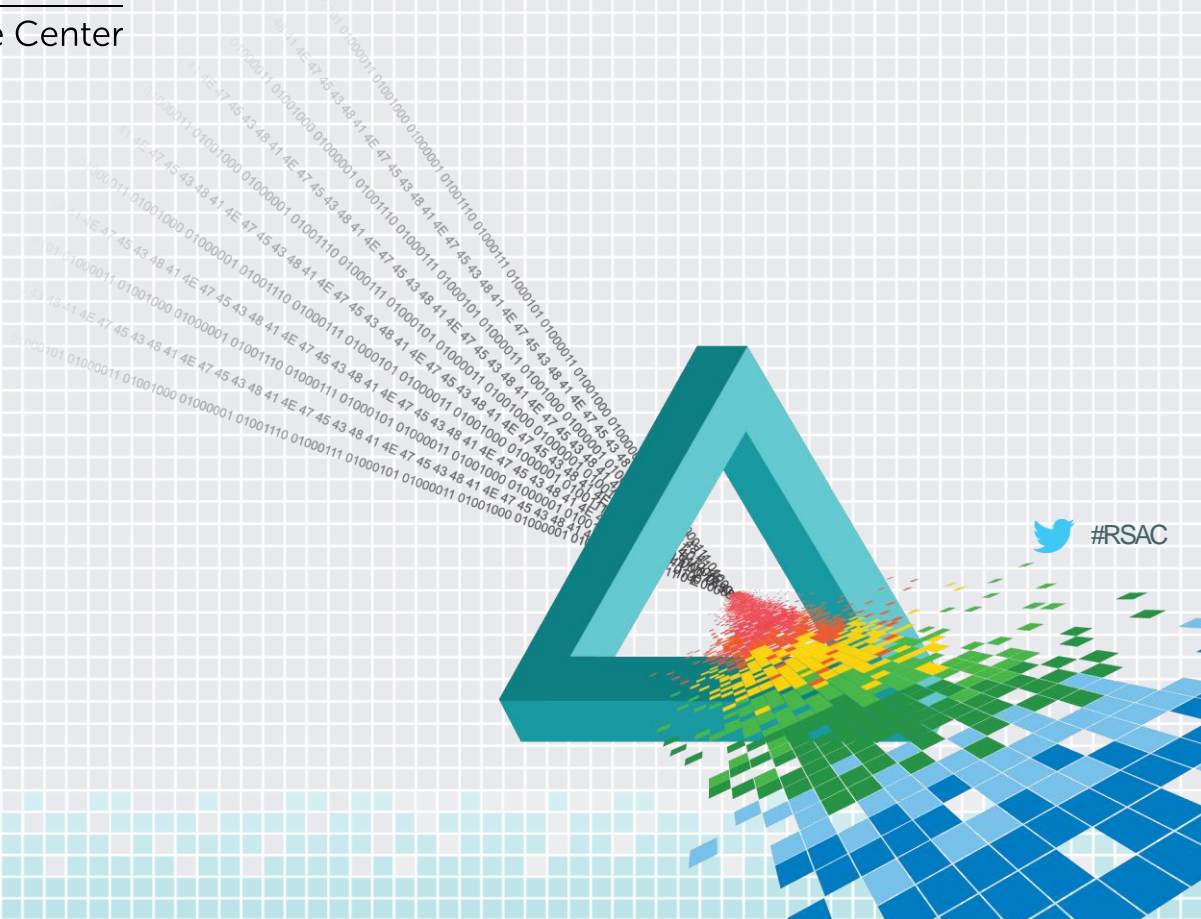
Challenge today's security thinking



RSA[®]Conference2015

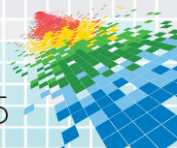
San Francisco | April 20-24 | Moscone Center

Background



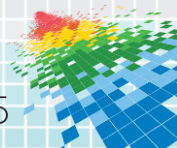
Threat Intelligence is Dead. Long Live Threat Intelligence!

- ◆ Defining and Discussing Threat Intel
- ◆ Market Offerings
- ◆ Concerns, Considerations – Mainly Quality and Utility
- ◆ Types of Indicators, What's Good and Bad
- ◆ Case Studies and What Works
- ◆ Applying What You've Learned
- ◆ Q&A



What is Threat Intelligence?

- ◆ Many different kinds; we're talking about cyber threat intelligence - more specifically, indicator-based intelligence services
- ◆ IP addresses, email addresses, strings, FQDNs, mutex, URLs, hashes
- ◆ Subscription services, products, hybrid model

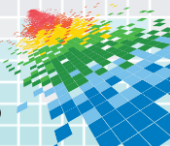


Why the Hype?

It makes us feel less like this...



...and more like this.



RSA[®]Conference2015

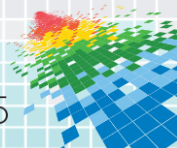
San Francisco | April 20-24 | Moscone Center

The Market



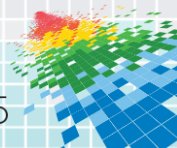
Threat Intel is Dead

- ◆ Highly commoditized – it's the new IDS signature
- ◆ Poor quality control
- ◆ Short shelf life
- ◆ Promotes false sense of awareness



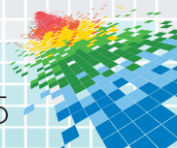
Or is it?

- ◆ If processed and applied properly, an invaluable resource
- ◆ Gets us closer to the adversary's tactics and infrastructure
- ◆ Informs defensive posture







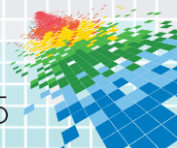
The Reality

- ◆ Cyber threat intelligence is another tool in the defender's toolbox
- ◆ Must be collected, vetted, applied, and automated for better and more timely detection without exponentially increasing workload or **sacrificing the fundamentals:**
 - ◆ Robust instrumentation
 - ◆ Awareness of one's own environment
 - ◆ Solid analytic processes



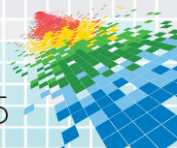
Market Offerings

OPEN SOURCE	COMMUNITY	COMMERCIAL	INTERNAL
Free	Free - \$	\$ - \$\$\$	\$ - \$\$\$\$
Format varies	Some standardization	Vendor specific	Standardized
Limited targeted intelligence	Moderate targeted intelligence	Moderate targeted intelligence	Highly targeted intelligence
Usage restrictions vary	Usage is restricted	Usage is restricted	Unrestricted usage
			



Considerations

- ◆ What are your monitoring goals?
 - ◆ Protection
 - ◆ Detection
 - ◆ Attribution and Prosecution



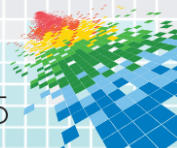
Considerations

- ◆ What are your monitoring goals?
 - ◆ Protection – good!
 - ◆ Detection – good!
 - ◆ Attribution and Prosecution – maybe...



Considerations

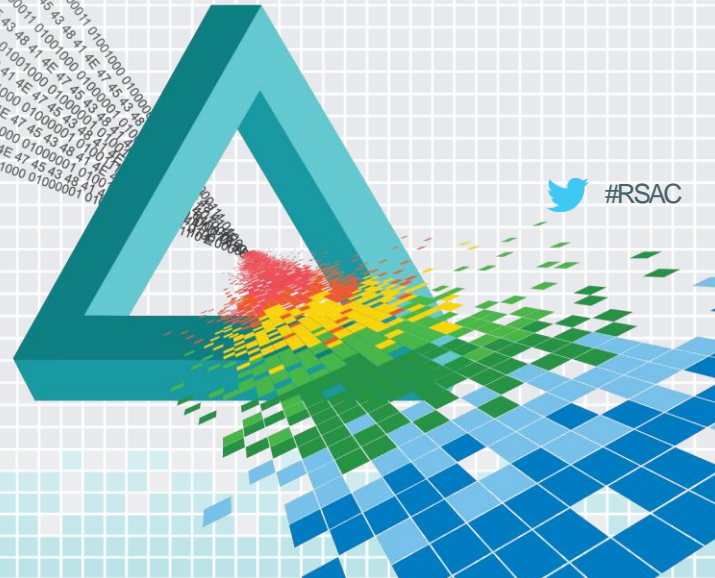
- ◆ What are your monitoring *capabilities*?
 - ◆ Tools – ingest XML/CSV/JSON, web site content, vendor provided indicators, community or industry reports
 - ◆ Staff – to collect, vet, curate, and apply
 - ◆ Awareness – threats and countermeasures within your environment, likely targets



RSA[®]Conference2015

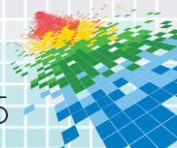
San Francisco | April 20-24 | Moscone Center

Ok, we have our intel.
What now?



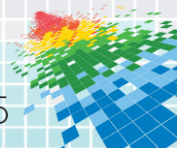
Quality and Utility

- ◆ *Scenario*: good indicators versus bad indicators
 - ◆ Malware calls out to <http://infect.p0wned.de/clickme/fool.php>
 - ◆ User agent observed:
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Trident/6.0;
6F8D132A4C9F
- ◆ Which would you pivot from?



Quality and Utility

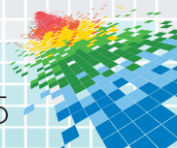
- ◆ <http://infect.p0wn3d.de/clickme/fool.php> broken down:
 - ◆ FQDN: infect.p0wn3d.de
 - ◆ Domain name: p0wn3d.de
 - ◆ URL path: [/clickme/fool.php](http://infect.p0wn3d.de/clickme/fool.php)
 - ◆ Resolved IP: 123.80.123.80



Quality and Utility

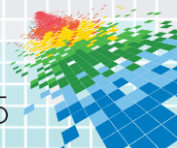
- ◆ Useful: http://www.cnn.com/adhome/malicious_ad.js
Not as useful: www.cnn.com

IP Address 23.235.47.184 - 256 other sites
hosted on this server



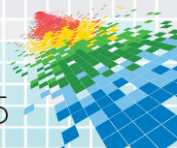
Network Indicators

- ◆ How can you vet network indicators?
- ◆ FQDN/Domain:
 - Age of domain
 - Registrant info (name, email, address)
 - Page rank
 - Reputation
 - Malware history
- ◆ Sources: WHOIS, Domaintools, Alexa, AV/web proxy vendors, VirusTotal



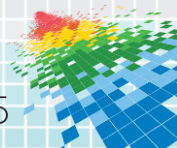
Network Indicators

- ◆ How can you vet network indicators?
- ◆ IP Address:
 - Netblock owner
 - # domains hosted on that IP
 - Malware history
- ◆ Sources: WHOIS, Domaintools, VirusTotal



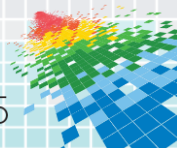
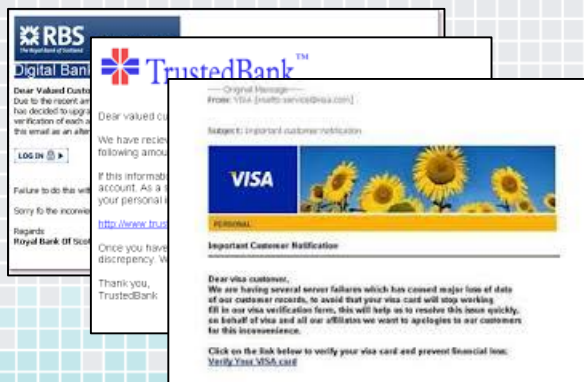
Host Indicators

- ◆ Host-based indicators require closer inspection
- ◆ **Careful!** Watch community contributed and auto-gen content
- ◆ Generic filenames should be noted, probably not useful
- ◆ System paths alone aren't very useful
- ◆ Generate regex for generated names/hashes if possible



Email Indicators

- ◆ Spoofed sender addresses are interesting but not indicators
- ◆ Attachment names and subject lines are similarly interesting, but often tweaked or used in a single campaign only so not indicators in themselves
- ◆ Indicators derived from malicious attachments and links are better



Bad Indicators – BAD!

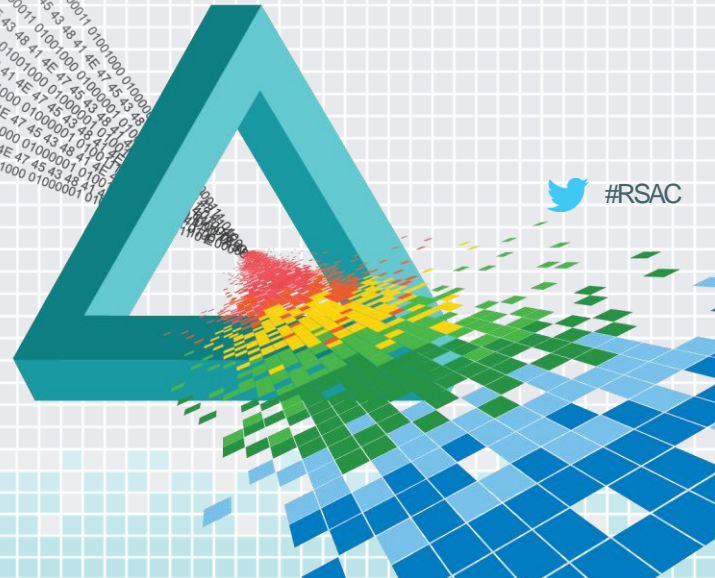
- ◆ 127.0.0.1
- ◆ RFC 1918 reserved addresses like 10.0.0.0/8
- ◆ Well known domains like google.com
- ◆ “Blank” values like 0.0.0.0



RSA[®]Conference2015

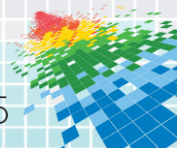
San Francisco | April 20-24 | Moscone Center

Case Studies



Case Study 1: Commercial Feed

- ◆ XML feed of domains, IP addresses, mutex, URLs, and user agent strings
- ◆ Collected and vetted by a global team of analysts
- ◆ Approximately 730 unique indicators a month



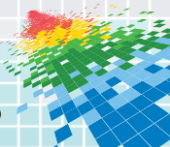
Indicator Types, Descriptions



EXPLOIT
STAGE
DL
INITIAL INFECTION
C&C

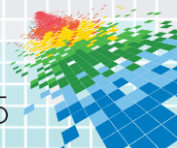


DOMAIN
IP
URL
USER AGENT
MUTEX



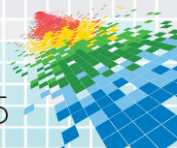
Analytic Value

- ◆ IP addresses and domains are useful, but easily modified by the attacker and are often specific to campaign or variant
- ◆ Good indicators, but indicator != incident
- ◆ Most of these come in late in the attack chain; read about David J. Bianco's Pyramid of Pain
(<http://detect-respond.blogspot.com/>)



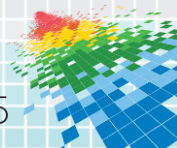
Lessons Learned

- ◆ Track hit rate, vet in advance if possible
- ◆ One bad indicator resulted in 108,000+ hits
 - ◆ **Bonus for defenders:** what does this remind you of??
- ◆ Remember the part about knowing your IT? Be mindful of where you apply indicators!



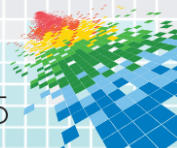
Case Study 2: Community Feed

- ◆ Unstructured but context-rich reports
- ◆ Distributed among defenders within a specific community of interest
- ◆ Approximately 460 unique indicators a month



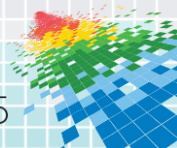
Analytic Value

- ◆ Great context, provides use cases and approximate expiration timeframes for indicators
- ◆ Generally more relevant given community focus
- ◆ Fewer indicators simplifies vetting



Lessons Learned

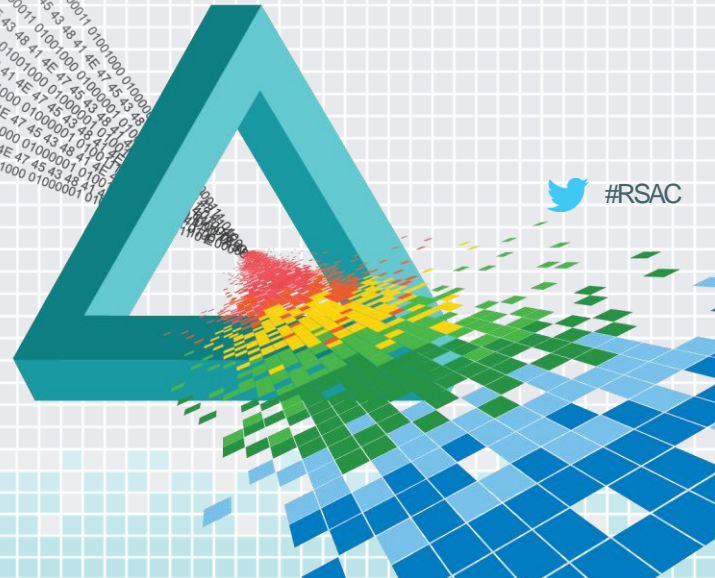
- ◆ Manual report review can be very time consuming
- ◆ Automated indicator extraction from Word or PDF can be challenging
- ◆ Indicators have shorter shelf lives; possibly more campaign-specific infrastructure



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

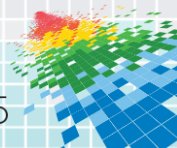
Putting It All Together



What Works

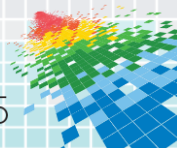
- ◆ Cast a wide net
- ◆ Automate!
 - ✓ Collection
 - ✓ Normalization
 - ✓ **Vetting – remember this? →**
 - ✓ Tagging
 - ✓ Ingestion
- ◆ Lots of sample scripts out there

- ◆ FQDN/Domain:
 - Age of domain
 - Registrant info (name, email, address)
 - Page rank
 - Reputation
 - Malware history



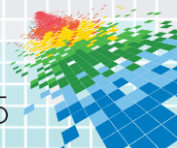
What Works

- ◆ Curating: tag, classify, or annotate intel-based events
- ◆ Collect metrics such as:
 - ◆ *Reuse*: How many overlaps between commercial, community, open source?
 - ◆ *Utility*: How many investigations has a given source supported?
 - ◆ *Applicability*: How relevant is an intel product to your business or sector?
- ◆ Data-driven analysis

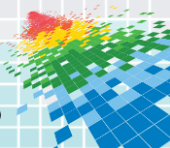
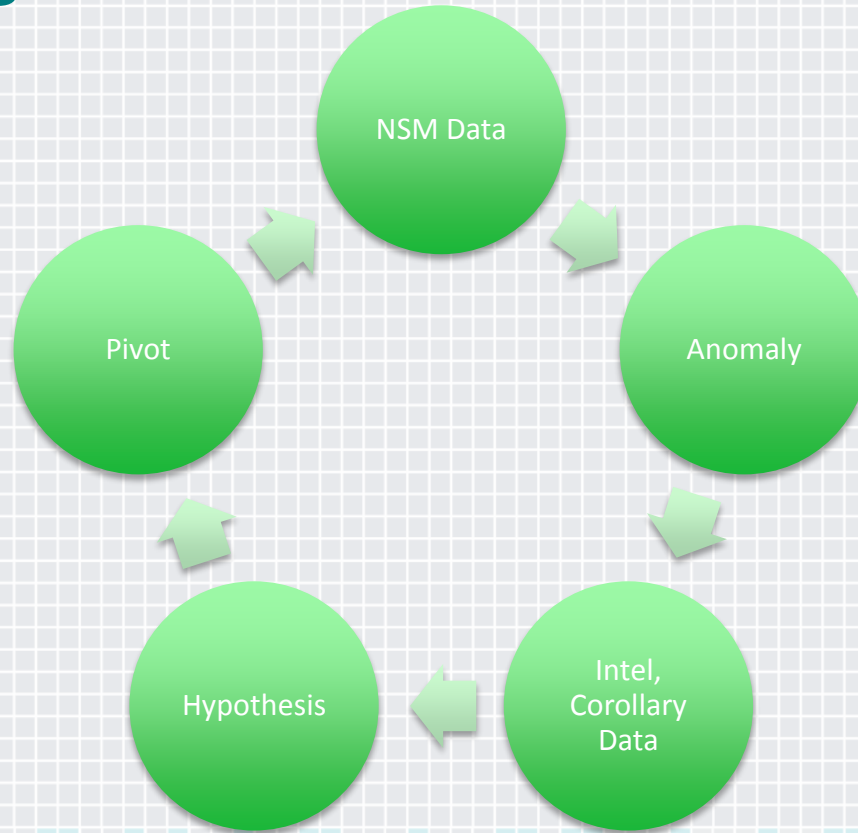


What Works

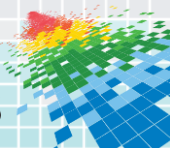
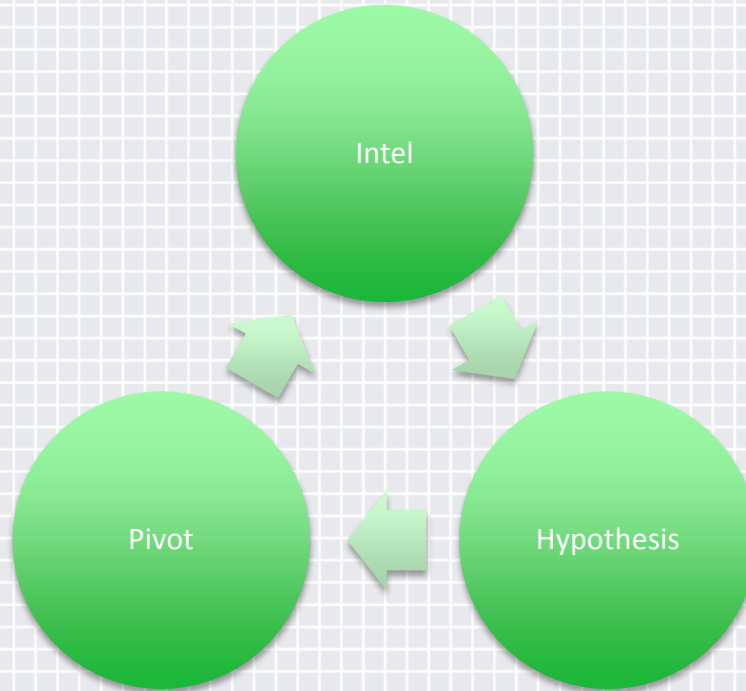
- ◆ Understand technical capabilities
 - ◆ Many tools can't process contextual data; in some cases, not even the entire indicator (see “**bad indicators**”)
 - ◆ APIs are great, present performance and capability challenges
 - ◆ Look at previously mentioned description and transmission standards
- ◆ Build workflows for better critical thinking, not just alerting



What Works

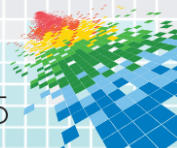


What Doesn't Work



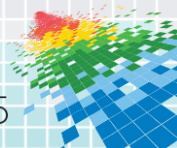
Apply What You've Learned

- ◆ Identify likely objectives like your user base and critical IT assets
- ◆ Brush up on NSM and Intel Analysis:
 - ◆ The Practice of Network Security Monitoring, by Richard Bejtlich
 - ◆ Practical Network Security Monitoring, by Chris Sanders
 - ◆ *Psychology of Intelligence Analysis*, by Richards Heuer, Jr.
<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf>



Apply What You've Learned

- ◆ In the next few months:
 - ◆ Vet and measure your intelligence independently of detection efforts
 - ◆ Look for patterns and overlaps
 - ◆ Track hit rates
 - ◆ Evaluate indicator quality
 - ◆ Weave these efforts into your NSM infrastructure management processes



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

Questions?

