THREATCONNECT™

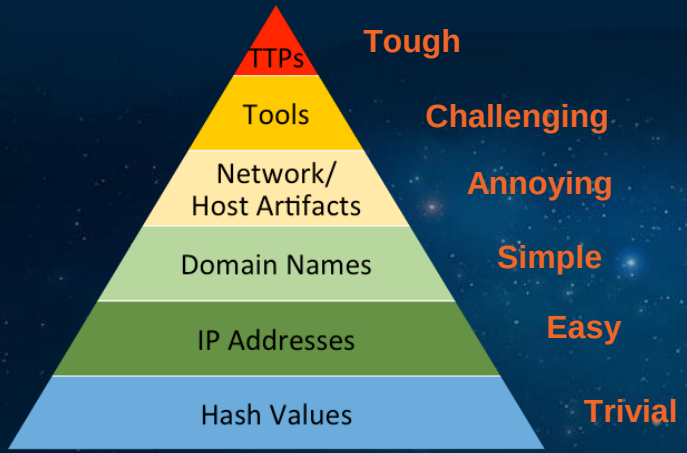
We Have the Technology; We Can Rebuild Him

February 4th, 2016

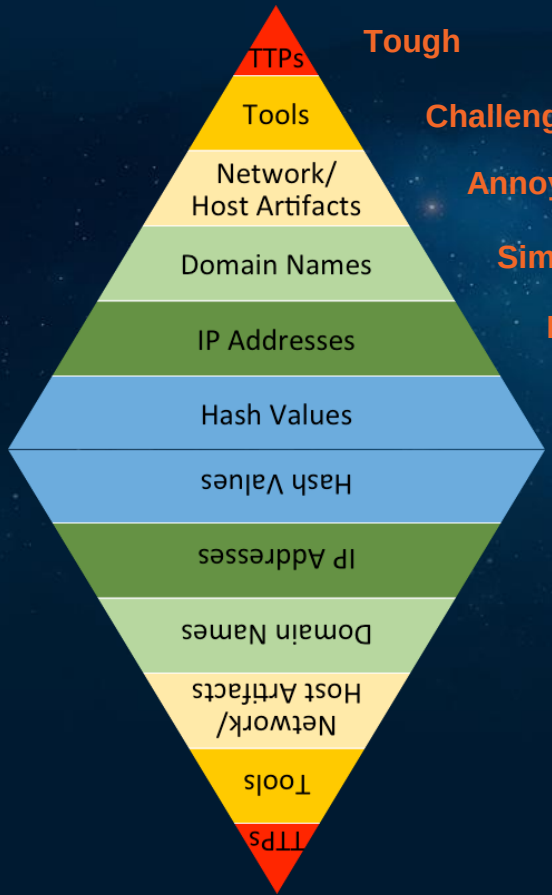
Priorities?

THREATCONNECT™

David Bianco's "Pyramid of Pain"



The Pyramid of Pain (Mirrored)



Tough

Challenging

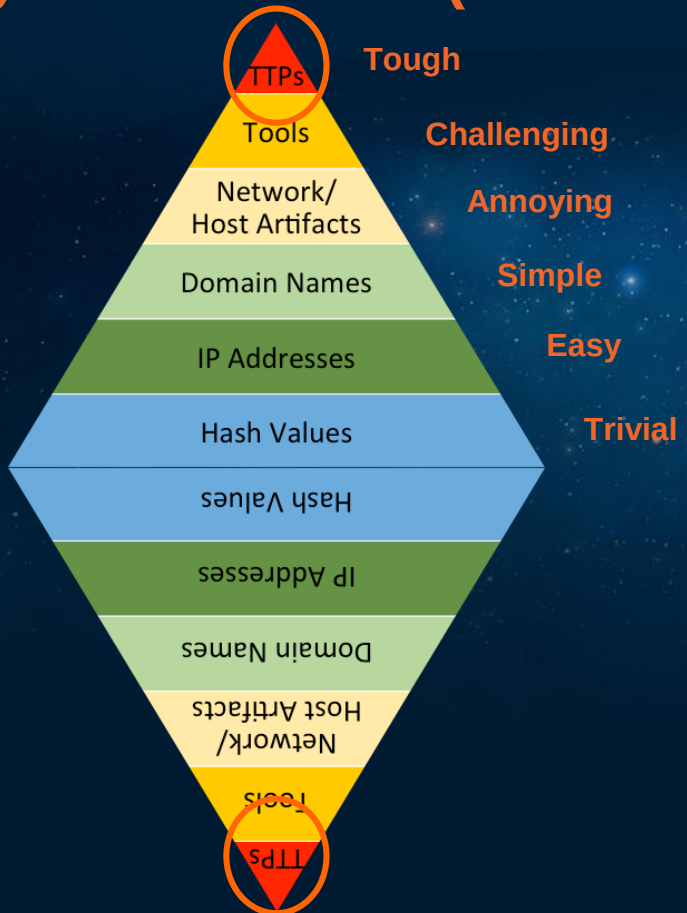
Annoying

Simple

Easy

Trivial

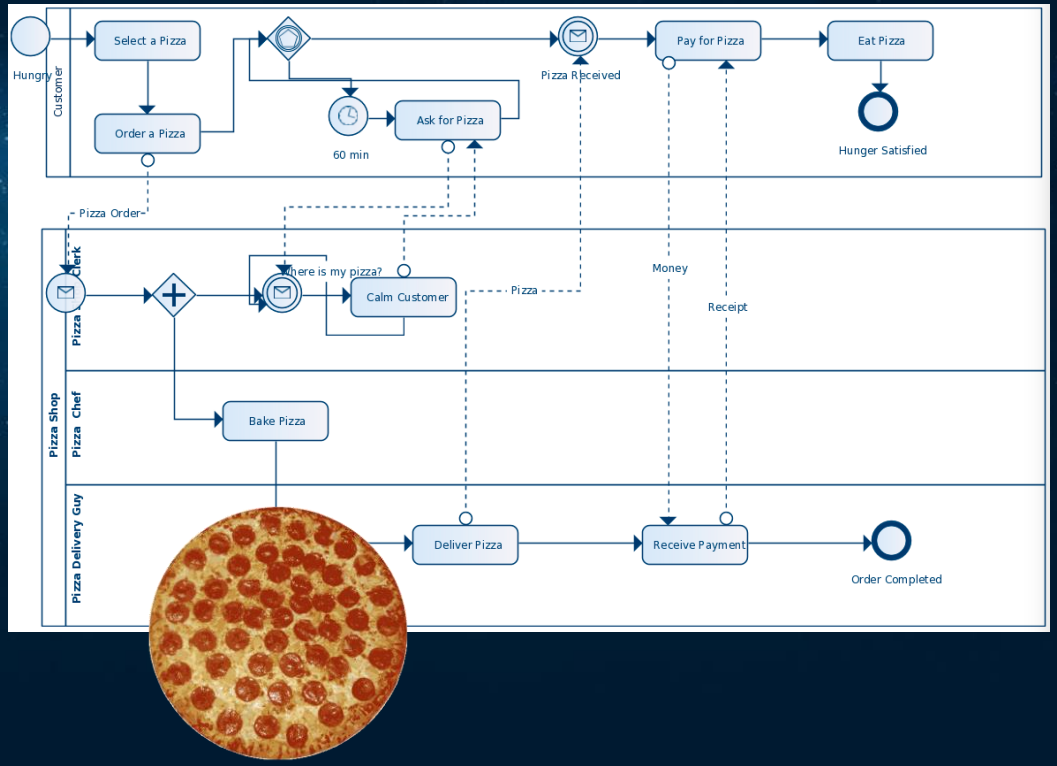
The Pyramid of Pain (Mirrored)



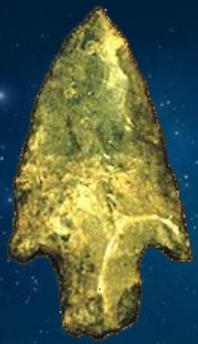
- TTP's = Tactics, Techniques & Procedures
- For the "back office" types TTP's can be translated as "business processes"
- I'm **NOT** talking about sharing the Adversary TTP's (*while that is always nice*)
- I'm talking about Sharing **My** TTP's as a Defender how do I do things like:
  - *Create*
  - *Enrich*
  - *Analyze*
  - *Interpret*
  - *Decide*
  - *Act*

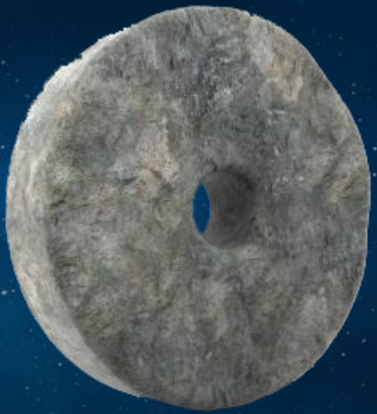
The Business of Threat Intelligence

- Mature businesses have processes
- Businesses processes should be measurable
- Business processes should demonstrate value (*save organizational resources - time & money*)

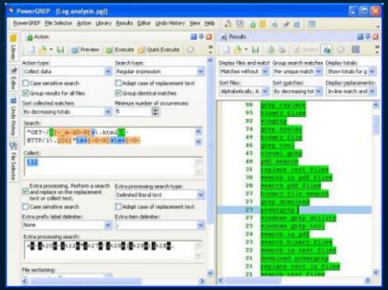


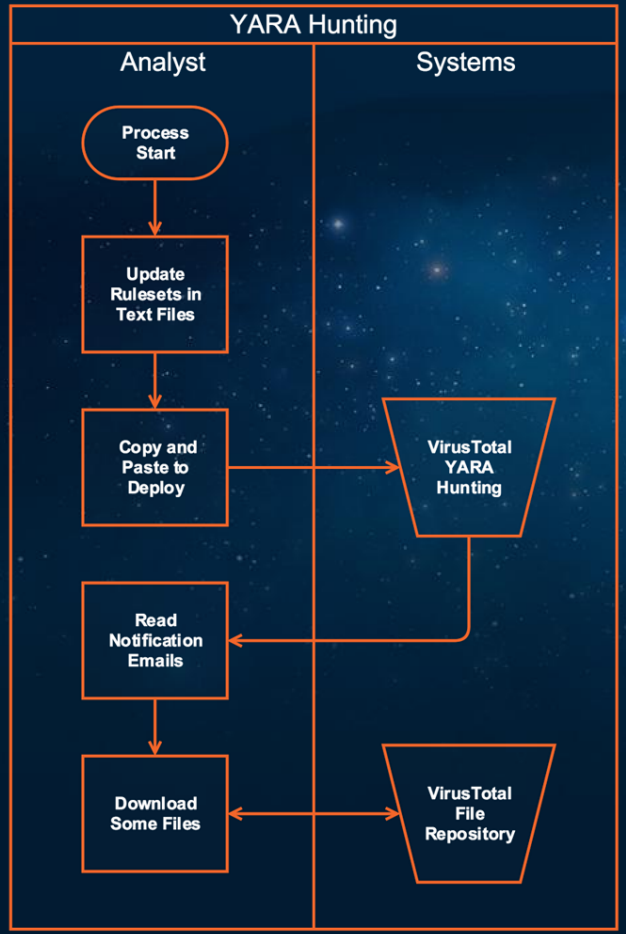
The Paleolithic Age of Threat Intel: Tools of the Trade

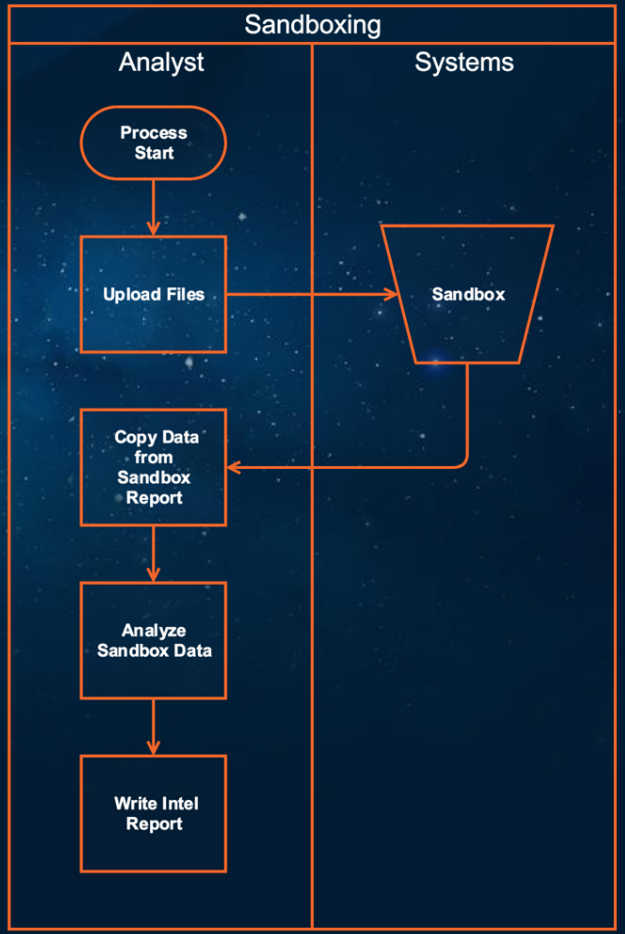


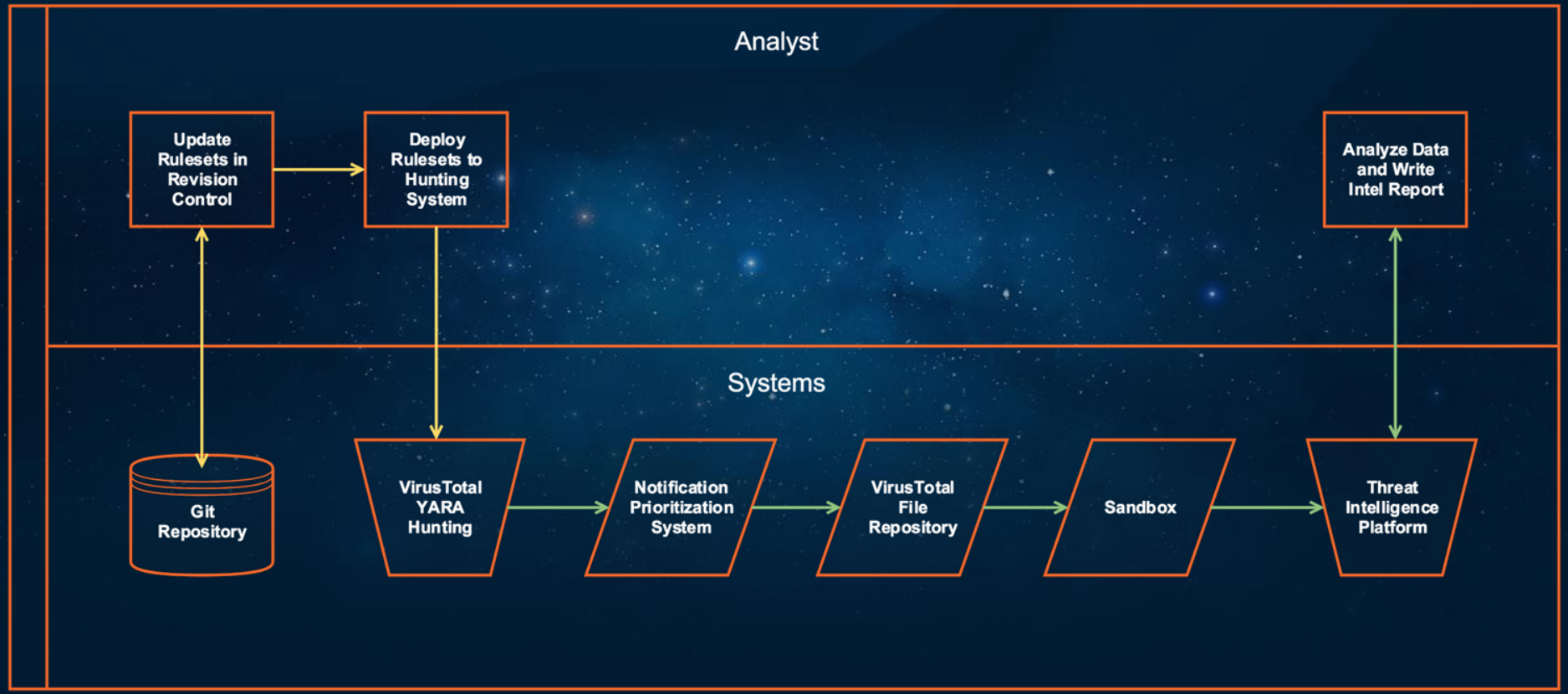


Brand	Bottle Size	Beginning Inventory (units)	Purchases (units)	Ending Inventory (units)	Usage (units)	Cost per Unit	Usage Cost	Selling Price per unit	Retail Sales Potential
Date		9/9/04		9/15/04					
Beck's	12	150	120	100	170	$0.66	$112.20	$2.50	$425.00
Bud Light	12	300	192	300	192	$0.66	$126.72	$3.50	$672.00
Budweiser	12	219	144	314	49	$0.66	$32.34	$3.50	$171.50
Coors Light	12	100	120	200	20	$0.66	$13.20	$3.50	$70.00
Corona	12	116	120	167	69	$0.66	$45.54	$3.50	$241.50
Genesee	12	58	144	114	88	$0.50	$44.00	$2.50	$220.00
Genesee Light	12	40	192	45	187	$0.50	$93.50	$2.50	$467.50
Michelob	12	83	144	84	143	$0.66	$94.38	$3.50	$500.50
Michelob Light	12	55	120	114	61	$0.66	$40.26	$3.50	$213.50
Michelob Ultra Light	12	30	192	16	206	$0.66	$135.96	$3.50	$721.00
Mike's Hard Lemonade	12	162	192	58	296	$0.66	$195.36	$3.50	$1,036.00
Miller Genuine Draft	12	146	144	47	243	$0.70	$170.10	$3.50	$850.50
Miller Lite	12	108	144	66	256	$0.70	$179.20	$3.50	$896.00
Molson Ice	12	118	120	68	170	$0.75	$127.50	$3.50	$595.00
O'Doul's	12	80	144	24	200	$0.52	$104.00	$2.50	$500.00
Red Dog	12	214	192	214	192	$0.70	$134.40	$3.50	$672.00
Red Stripe	12	190	144	67	270	$0.95	$256.50	$3.50	$945.00
Rolling Rock	12	247	120	256	111	$0.78	$86.58	$3.50	$388.50
Smirnoff Ice	12	87	192	79	200	$0.89	$178.00	$3.50	$700.00
Tona	12	106	120	49	177	$0.70	$123.90	$3.50	$619.50
TOTALS					3300		$2,293.64		$10,905.00




YARA Hunting
Analyst
Systems
Process Start
Update Rulesets in Text Files
Copy and Paste to Deploy
VirusTotal YARA Hunting
Read Notification Emails
Download Some Files
VirusTotal File Repository

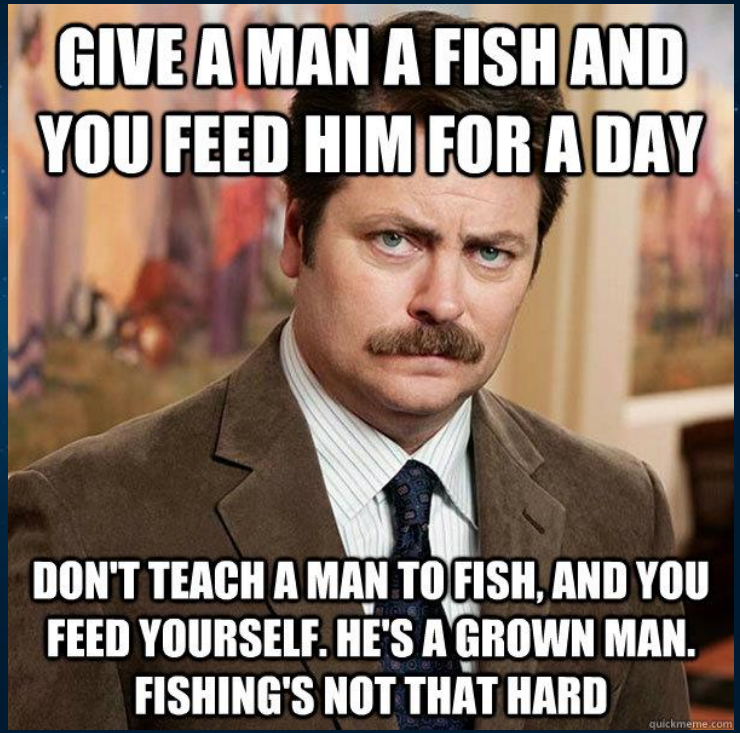

Sandboxing
Analyst
Systems
Process Start
Upload Files
Sandbox
Copy Data from Sandbox Report
Analyze Sandbox Data
Write Intel Report


Analyst
Update Rulesets in Revision Control
Deploy Rulesets to Hunting System
Analyze Data and Write Intel Report
Systems
Git Repository
VirusTotal YARA Hunting
Notification Prioritization System
VirusTotal File Repository
Sandbox
Threat Intelligence Platform

Demo Videos

Conclusion

- Threat Intelligence Sharing can go beyond sharing atomic Indicators
- "Teach a man to fish" applies here
- Where do you place the most value, the process or the product?
- Attach your Threat Intelligence Processes to powerful engines that help security investments scale.



Questions?