



.conf2015

Breach Management in Enterprise Security!

Brian Luger
Software Engineer, Splunk



splunk®

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

What is Breach Management?



Well... What's a Breach?

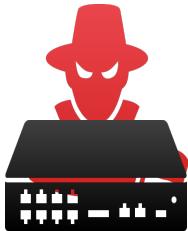


Well... What's a Breach?



Having one or more assets compromised by a threat actor that has targeted the organization in an attempt carry out a specific intent.

Breach Management



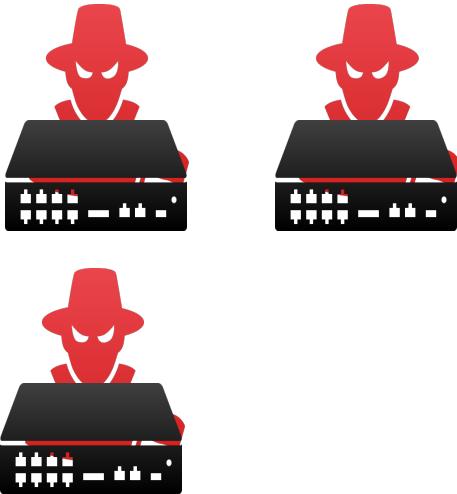
2011
2015

.conf2015

Breach Management



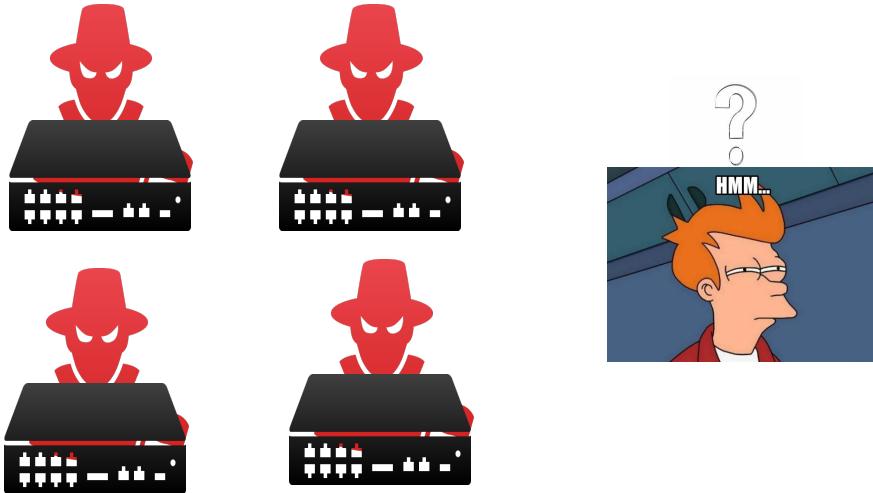
Breach Management



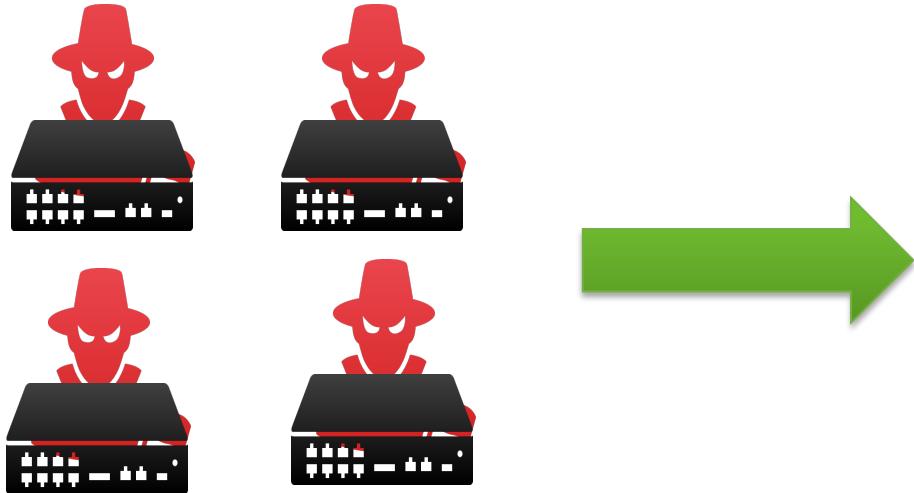
Breach Management



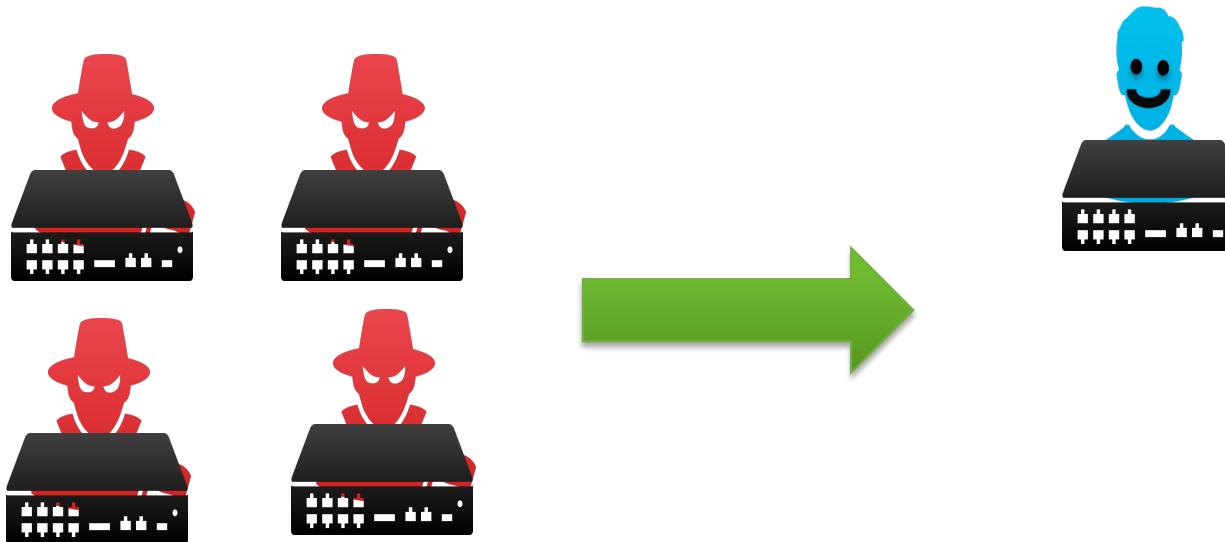
Breach Management



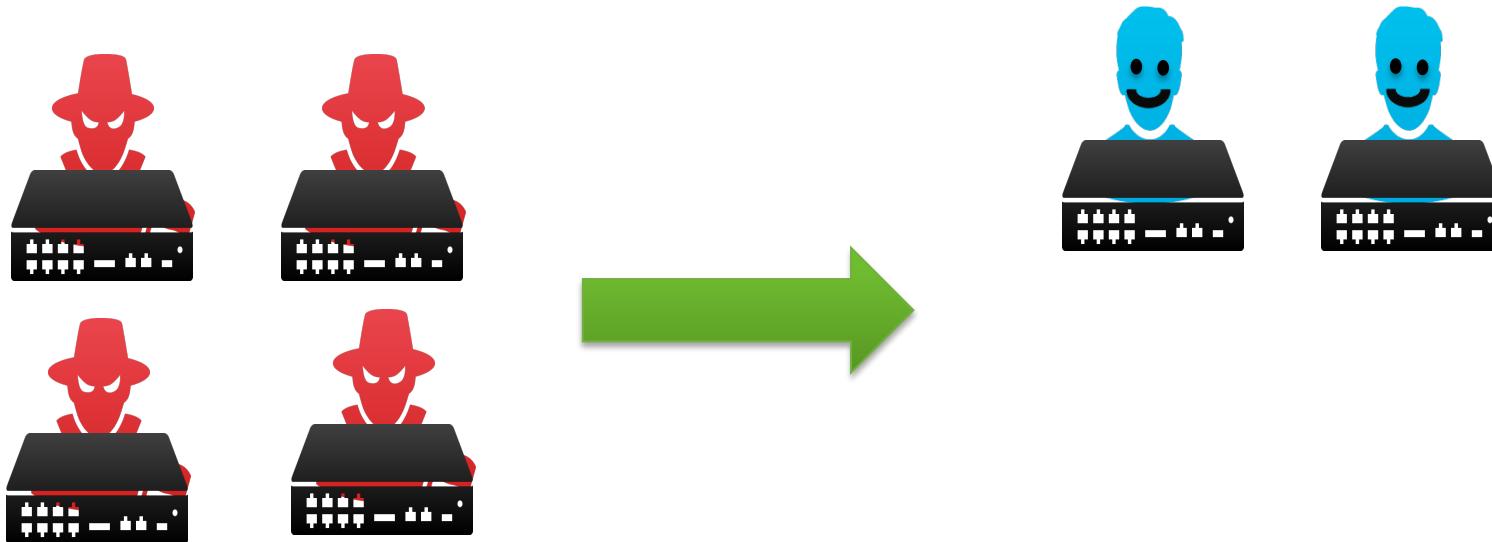
Breach Management



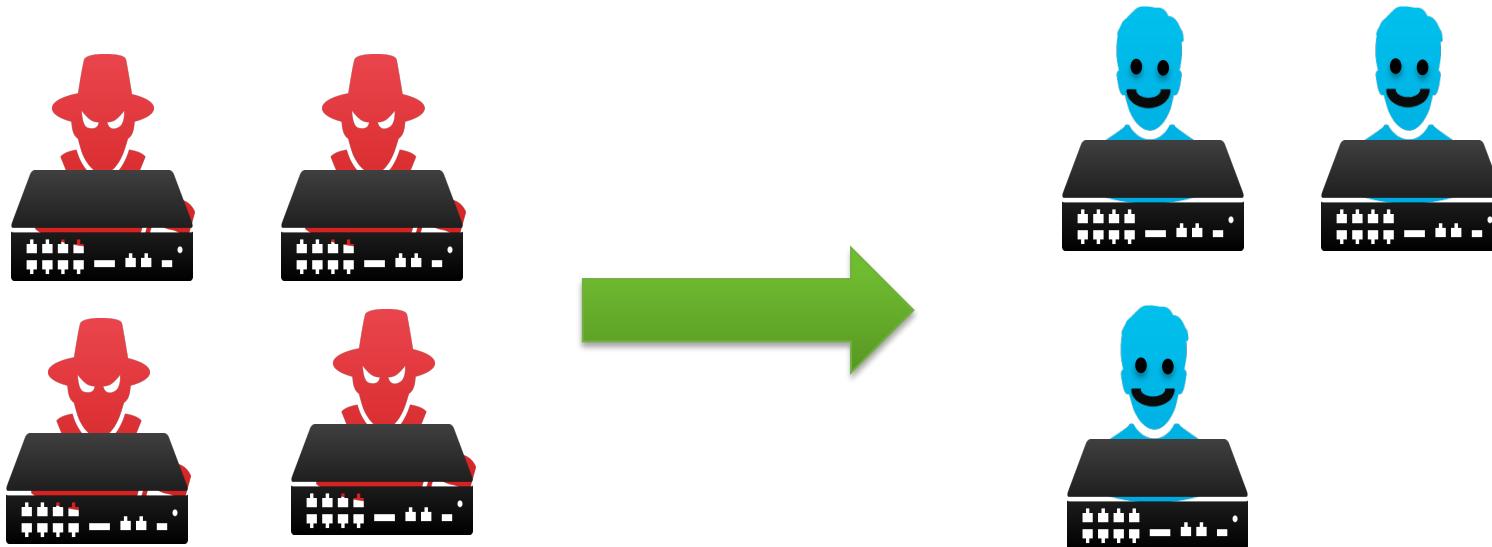
Breach Management



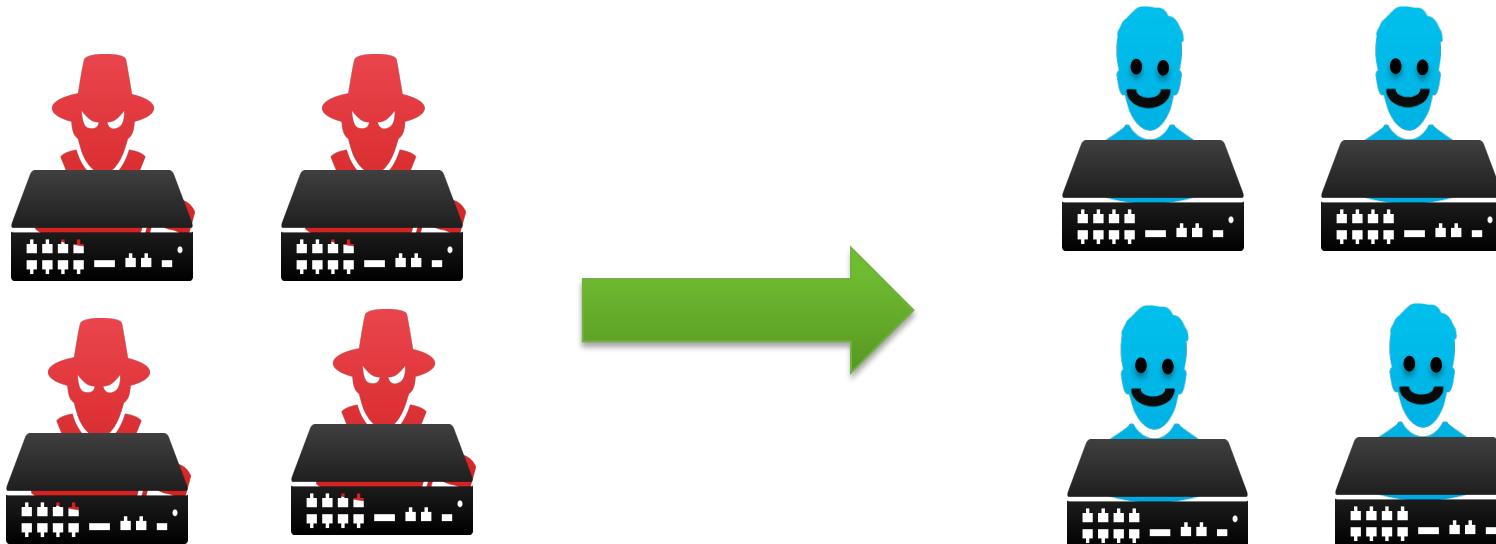
Breach Management



Breach Management



Breach Management



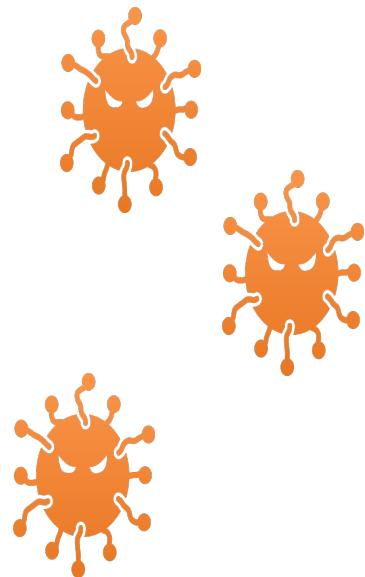
What Breach Management Is NOT



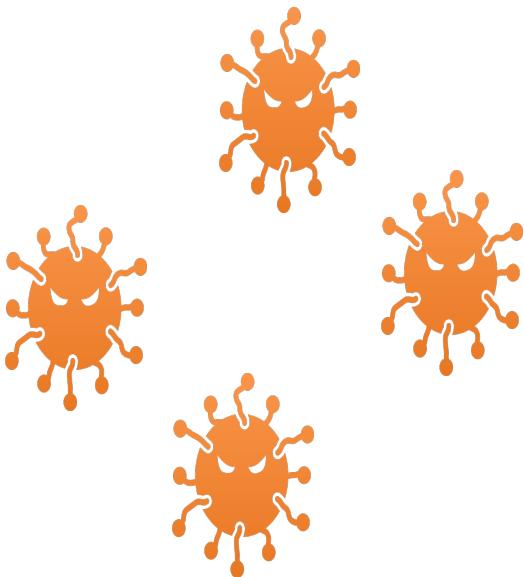
What Breach Management Is NOT



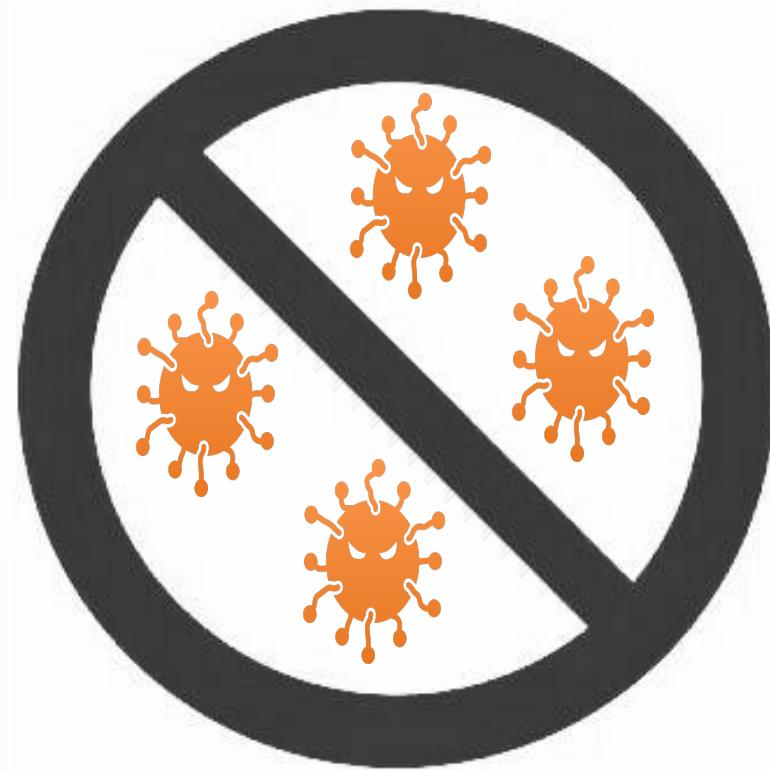
What Breach Management Is NOT



What Breach Management Is NOT



What Breach Management Is NOT



Breach Management can be Difficult



vs



Breach Management can be Difficult



VS



Breach Management can be Difficult



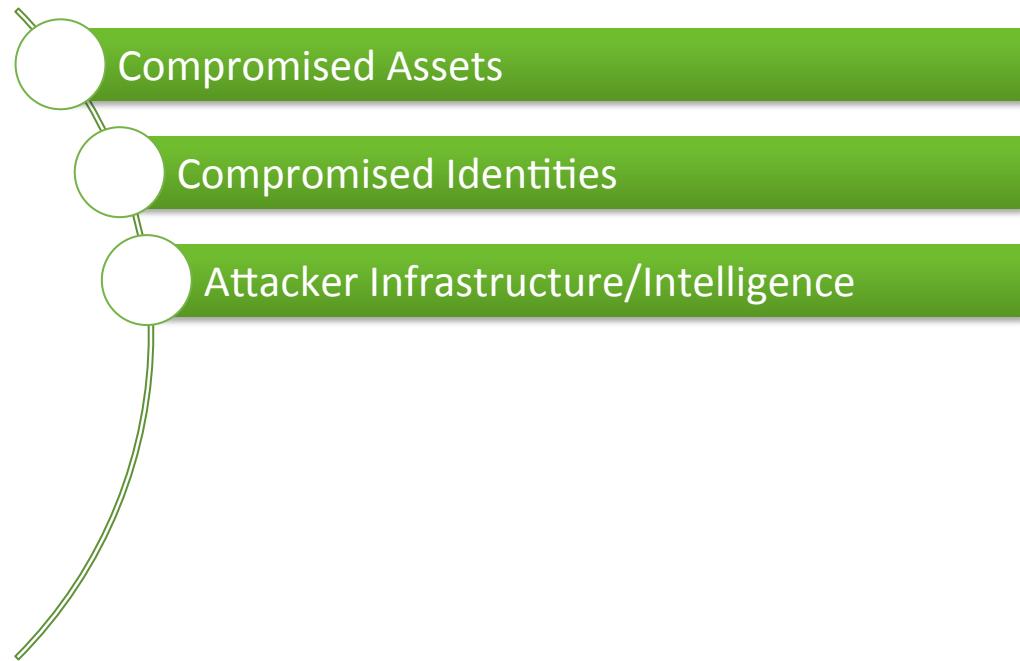
VS

A large, bold, black "VS" symbol, indicating a comparison between two sides.

Breach Management can be Difficult



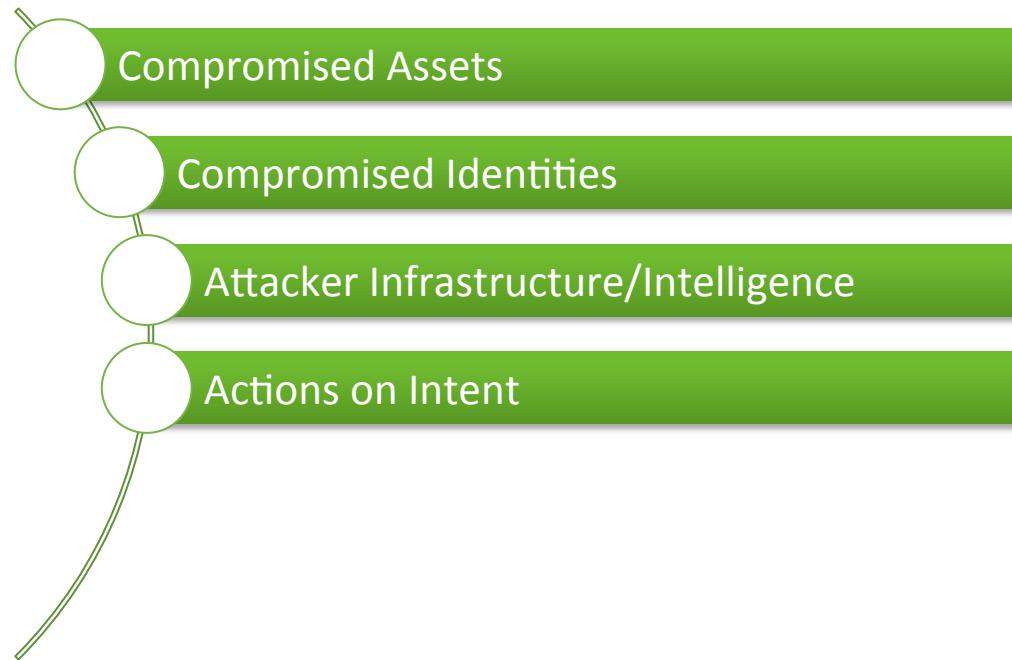
VS

A large, bold, black "VS" symbol, indicating a comparison between two sides.

Breach Management can be Difficult



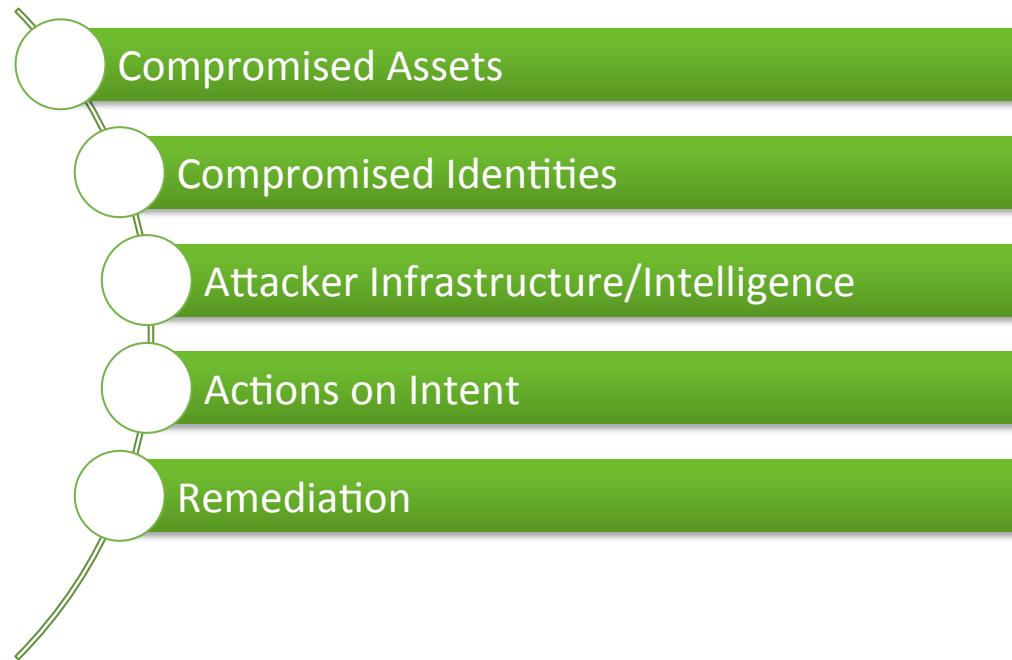
VS

A large, bold, black "VS" symbol, indicating a comparison between two sides.

Breach Management can be Difficult



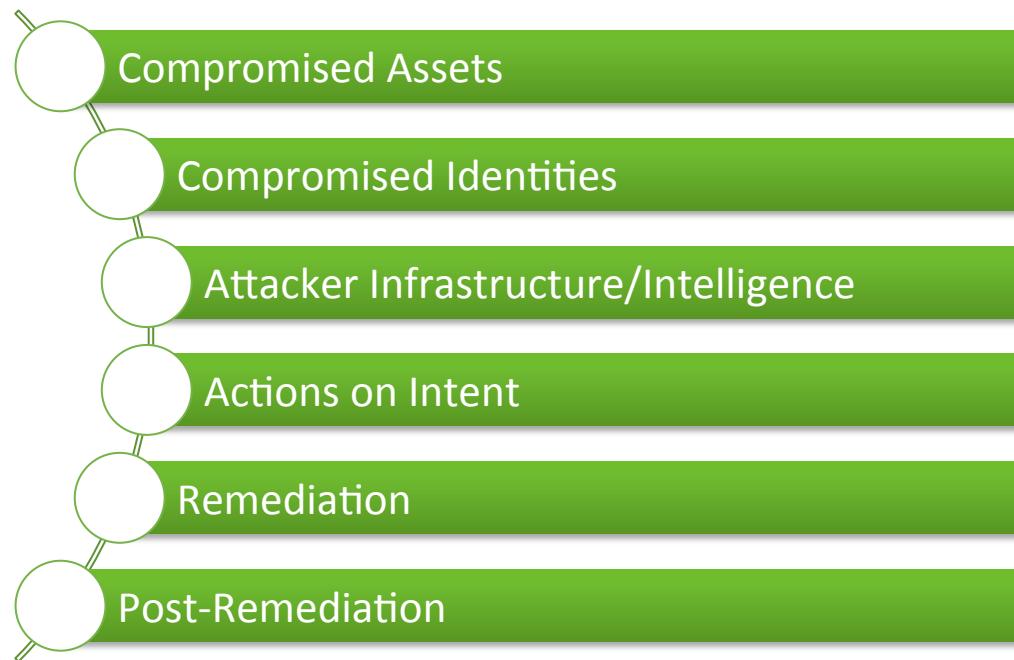
VS

A large, bold, black 'VS' symbol indicating a comparison or competition between two sides.

Breach Management can be Difficult



VS

A large, bold, black "VS" symbol indicating a comparison between two sides.

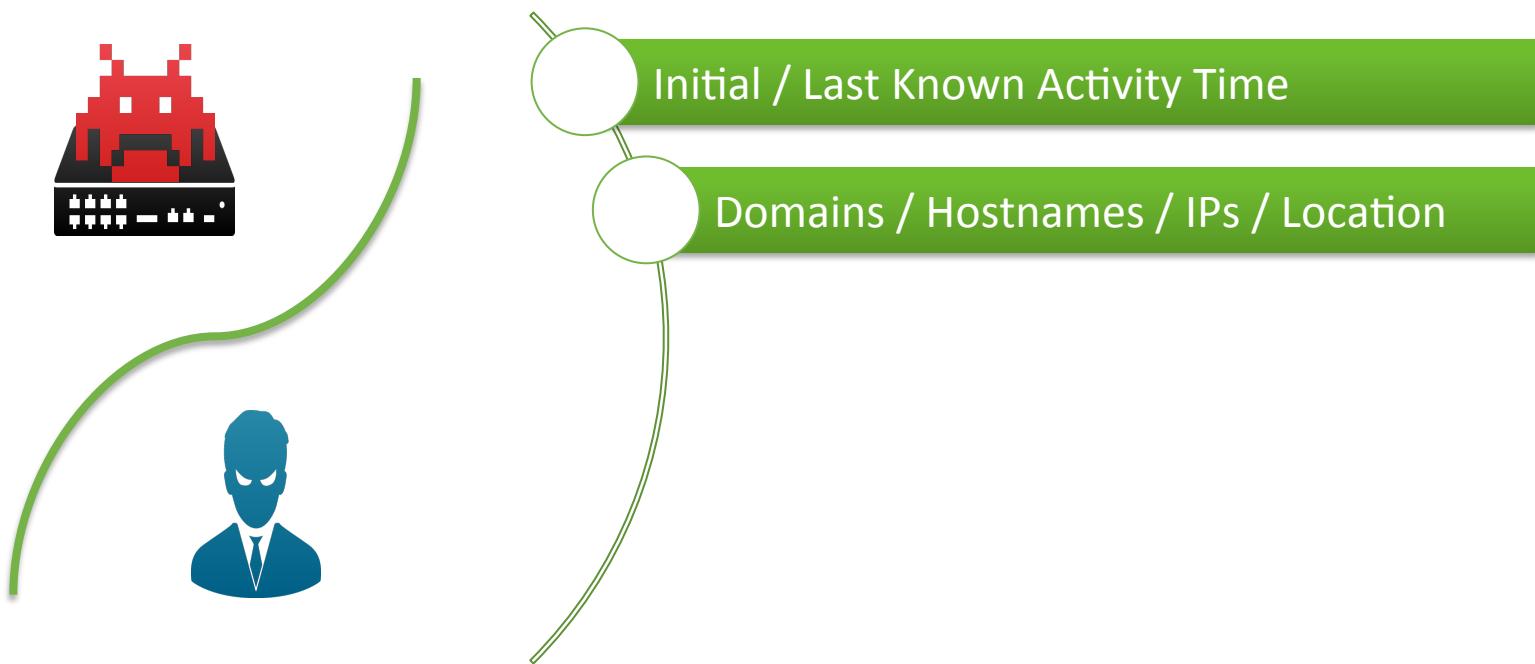
Compromised Assets & Identities



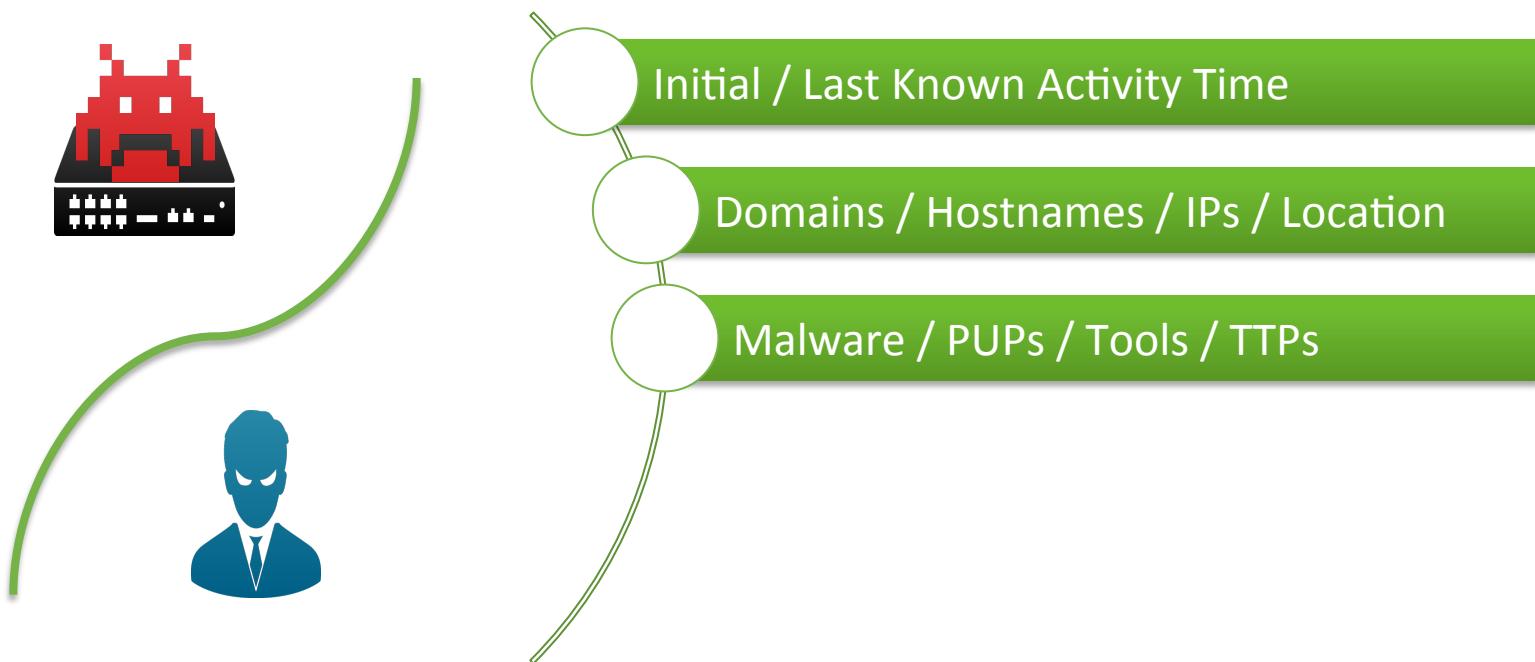
Compromised Assets & Identities



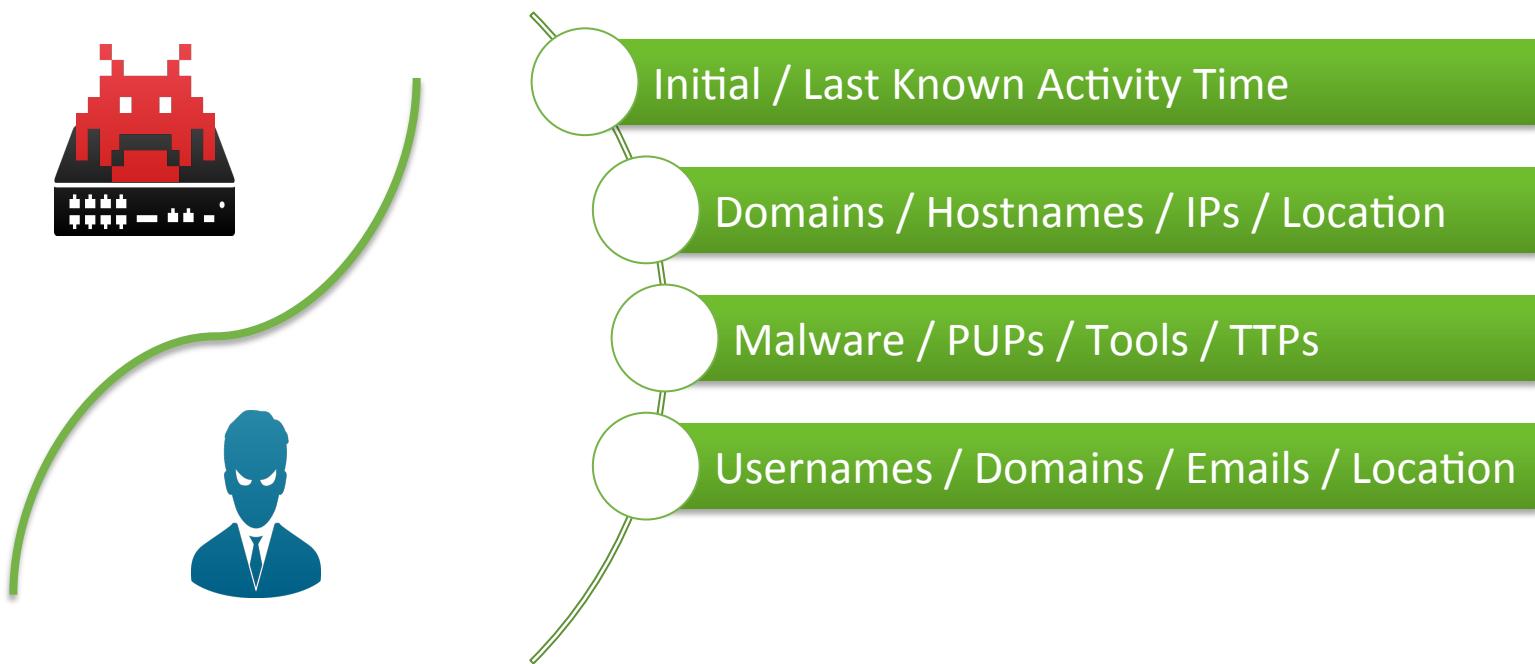
Compromised Assets & Identities



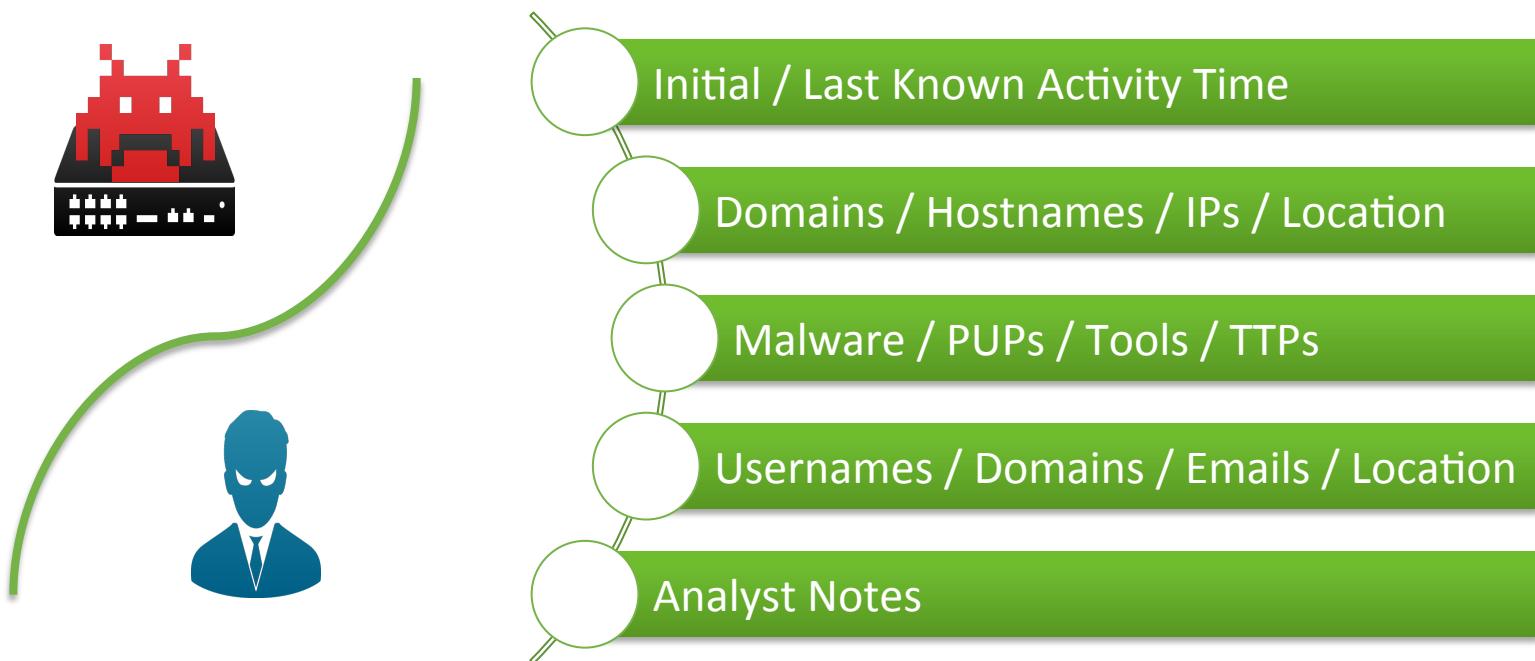
Compromised Assets & Identities



Compromised Assets & Identities



Compromised Assets & Identities



ES Assets & Identities Framework

Splunk > App: Enterprise Security >

Administrator > 4 Messages > Settings > Activity > Help > Find

Incident Review My Investigations Advanced Threat > Security Domains > Audit > Search > Configure >

Enterprise Security ES

Edit Lookup

< Back to Lookups List

Edit Lookup File

demo_asset_lookup

1	ip	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	category	pci_domain	is_expected	should_timesync	should_update	requires_av
2	6.0.0.1-9.0.0.0					low	41.040855	28.986183	Istanbul	TR	apac				true	true	
3	1.2.3.4	00:16:70:91:df:6c			CORP1.acmetech.com	medium	38.959405	-77.04	Washington D.C.	USA	americas				true	true	
4			storefront			high	37.694452	-121.894461	Pleasanton	USA	americas	poi_cardholder	trust	true	true	true	
5	192.168.12.9-192.168.12.9					critical	32.931277	-96.818167	Dallas	USA	americas	poi	trust	true	true	true	
6	2.0.0.0/8					low	50.84436	-0.98451	Havant	UK	emea	poi_sox	dmz	true	true	true	
7	192.168.15.8-192.168.15.10					medium	38.959405	-77.04	Washington D.C.	USA	americas	poi_ipaa	trust	true	true	true	
8	192.168.0.0/16					high	37.694452	-121.894461	Pleasanton	USA	americas	iso27002		true	true		
9	5.6.7.8	00:12:cf:30:27:b5	millenium-falcon			critical	32.931277	-96.818167	Dallas	USA	americas	nerciso		true	true	true	
10	192.168.15.9-192.168.15.9			acmefileserver		low	50.84436	-0.98451	Havant	UK	emea	pci	trust	true	true		
11	192.168.15.9-192.169.15.27					medium	38.959405	-77.04	Washington D.C.	USA	americas			true	true		
12	9.10.11.12	00:16:5d:10:08:9c				high	37.694452	-121.894461	Pleasanton	USA	americas	email_servers		true	true		
13		00:25:bc:42:f4:60-00:25:bc:42:f4:6f				critical	32.931277	-96.818167	Dallas	USA	americas	virtual		true	true		
14		00:25:bc:42:f4:60-00:25:bc:42:f4:60				low	50.84436	-0.98451	Havant	UK	emea	pci	wireless	true	true		
15		00:25:ac:42:f4:60-00:25:cc:42:f4:60				medium	38.959405	-77.04	Washington D.C.	USA	americas			true	true		
16			PA-dC02			high	37.694452	-121.894461	Pleasanton	USA	americas	poi_cardholder		true	true	true	
17				ACMEaPP		critical	32.931277	-96.818167	Dallas	USA	americas	poi_cardholder		true	true	true	
18				NCoRPNoDE1		high	50.84436	-0.98451	Havant	UK	emea	poi_cardholder		true	true	true	
19				AcMEDC01		high	38.959405	-77.04	Washington D.C.	USA	americas	poi_cardholder		true	true	true	
20				macFISH		high	37.694452	-121.894461	Pleasanton	USA	americas	poi_cardholder		true	true	true	
21				AcMEFW		high	38.959405	-77.04	Washington D.C.	USA	americas	poi_cardholder		true	true	true	
22				ns5gt-wlan		high	38.959405	-77.04	Washington D.C.	USA	americas	poi_cardholder		true	true	true	
23	10.252.0.0/16					high	20.8165082	-16.39597482	Mauritania	AF	emea	cardholder		true	true	true	
24	68.87.0.0/16					high	37.694452	-121.894461	Pleasanton	USA	americas	poi_cardholder	trust	true	true	true	
25	10.11.36.20				Bill_williams	critical	37.694452	-121.894461	Pleasanton	USA	americas	poi_psplunk		true	true	true	
26	110.172.158.1-110.172.158.15				b.franklin	critical	37.694452	-121.894461	Pleasanton	USA	americas	billing_ipci		true	true	true	

Cancel Save

No investigation is currently loaded. Please create (+) or load an existing one (=).

ES Assets & Identities Framework

Splunk > App: Enterprise Security >

Incident Review My Investigations Advanced Threat Security Domains Audit Search Configure Administrator 4 Messages Settings Activity Help Find Enterprise Security ES

Edit Lookup

[Edit](#) [More Info](#) [Download](#) [Print](#)

[Edit Lookup File](#)

demo_identity_lookup

1	identity	prefix	nick	first	last	suffix	email	phone	phone2	managedBy	priority	bunit	category	watchlist	startDate	endDate	work_city	work_country	work_lat	work_long
2		Mr.	Awe	Martin			mawe@acmetech.com	+1 (800)555-1562	+1 (800)555-3227		critical	americas			5/1/2003 0:17		San Jose	USA	37.3382N	121.8863W
3		Nene	Ranee	Majcher			rmajcher@acmetech.com	+1 (800)555-8762	+1 (800)555-8549			americas	contractor		9/15/96 1:55		San Jose	USA	37.3382N	121.8863W
4		Ms.	Elouise	Jennifer			ejennifer@acmetech.com	+1 (800)555-7388	+1 (800)555-2669			americas			13/23/88260		San Jose	USA	37.3382N	121.8863W
5		Mrs.	Larisa	Kerst			lkerst@acmetech.com	+1 (800)555-4897	+1 (800)555-4311	pepper	low	americas			12/12/2004 17:31		San Jose	USA	37.3382N	121.8863W
6		Miss	Miki	Pickle			mpickle@acmetech.com	+1 (800)555-5501	+1 (800)555-7321		medium	americas	pci		8/29/99 2:51		San Jose	USA	37.3382N	121.8863W
7	pepperja.koski	Dr.	Al	Allan	Seykoski		aseykoski@acmetech.com	+1 (800)555-2111	+1 (800)555-9996		high	americas		TRUE	1058023800	1215892140	San Francisco	USA	37.78N	122.41W
8			Renda	Mckittrick			rmckittrick@acmetech.com	+1 (800)555-8072	+1 (800)555-2031		critical	americas			10/28/1983 0:27		San Francisco	USA	37.78N	122.41W
9		Ms.	Katharine	Willets			kwillets@acmetech.com	+1 (800)555-7596	+1 (800)555-4546			americas	intern		2/13/77 23:14		San Francisco	USA	37.78N	122.41W
10		Mrs.	Germaine	Largin			glargin@acmetech.com	+1 (800)555-3243	+1 (800)555-6764			americas			377537400		San Francisco	USA	37.78N	122.41W
11		Miss	Roma	Acebedo			racebedo@acmetech.com	+1 (800)555-1052	+1 (800)555-6529		low	americas		TRUE	5/12/1988 19:55		San Francisco	USA	37.78N	122.41W
12	moneyjournot	Dr.	Latoya	Journot			ljournot@acmetech.com	+1 (800)555-3479	+1 (800)555-1554		medium	americas			3/2/88 2:39	3/8/01 6:21	San Francisco	USA	37.78N	122.41W
13			Elissa	Whitmoyer			ewhitmoyer@acmetech.com	+1 (800)555-9812	+1 (800)555-7122		high	americas	pcicardholder		3422707520		San Francisco	USA	37.78N	122.41W
14		Ms.	Raylene	Cloward			rcloward@acmetech.com	+1 (800)555-9908	+1 (800)555-5055	money	critical	americas	officer/pip		12/23/1994 16:10		San Francisco	USA	37.78N	122.41W
15		Mrs.	Keena	Horstman			khorstman@acmetech.com	+1 (800)555-4711	+1 (800)555-9586			americas			1/8/88 23:06		San Francisco	USA	37.78N	122.41W
16		Miss	Turtle	Edwina	Berdan		eberdan@acmetech.com	+1 (800)555-2243	+1 (800)555-7697			americas	contractor		1208450280		San Francisco	USA	37.78N	122.41W
17	lurker	Dr.	Karey	Floe			kfloe@acmetech.com	+1 (800)555-1167	+1 (800)555-9058		low	americas			2/7/1972 16:54	2/7/2002 10:43	San Jose	USA	37.3382N	121.8863W
18			Manie	Infield			minfield@acmetech.com	+1 (800)555-6705	+1 (800)555-1910		medium	americas			4/11/81 12:43		San Jose	USA	37.3382N	121.8863W
19		Ms.	Lashunda	Borkoski			lborkoski@acmetech.com	+1 (800)555-6310	+1 (800)555-3184	money	high	americas	pip		585282060		San Jose	USA	37.3382N	121.8863W
20		Mrs.	Marty	Martin	Grieves		mgrieves@acmetech.com	+1 (800)555-3560	+1 (800)555-3777		critical	americas			7/7/2003 0:17		San Jose	USA	37.3382N	121.8863W
21		Miss	Cathi	Piening			cpiening@acmetech.com	+1 (800)555-4219	+1 (800)555-1444			americas			6/28/71 1:42		San Jose	USA	37.3382N	121.8863W
22	gooseysenashouts	Dr.	Sena	Shouts			sshouts@acmetech.com	+1 (800)555-6233	+1 (800)555-9152			americas			281538060		San Jose	USA	37.3382N	121.8863W
23			Afton	Trisler			atrisler@acmetech.com	+1 (800)555-8924	+1 (800)555-2267		low	americas	intern		10/20/1996 16:04		San Jose	USA	37.3382N	121.8863W
24		Ms.	Consuela	Argento			cargoento@acmetech.com	+1 (800)555-5699	+1 (800)555-9399		medium	americas			10/2/75 16:55	7/25/83 1:03	Istanbul	Turkey	41.0136N	28.9550E
25		Mrs.	Chloe	Apela			capela@acmetech.com	+1 (800)555-8783	+1 (800)555-9838	goose	high	americas			160425780		San Jose	USA	37.3382N	121.8863W
26		Miss	Staci	Stansbury			sstansbury@acmetech.com	+1 (800)555-5911	+1 (800)555-9435		critical	americas	pci		1/26/1983 10:23		San Jose	USA	37.3382N	121.8863W

[Cancel](#) [Save](#)

No investigation is currently loaded. Please create (+) or load an existing one (=).

ES Assets & Identities Framework

Tag **Submit**

[Edit all selected](#) | [Edit all 5 matching events](#) | [Add to Investigation](#)

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	9/11/15 9:19:28,000 AM	Access	Insecure Or Cleartext Authentication Detected	High	New	unassigned	▼
>	9/11/15 6:58:32,000 AM	Network	High Volume of Traffic from 10.11.36.20 to 208.49.52.149	Critical	New	unassigned	▼
▼	9/11/15 6:58:32,000 AM	Network	High Volume of Traffic from 10.11.36.20 to 199.9.251.78	Critical	New	unassigned	▼

Description:
A large volume of traffic was observed from 10.11.36.20 to 199.9.251.78.

Additional Fields	Value	Action
Destination	199.9.251.78	▼
Destination Expected	false	▼
Destination PCI Domain	untrust	▼
Destination Requires Antivirus	false	▼
Destination Should Time Synchronize	false	▼
Destination Should Update	false	▼
Source	10.11.36.20	▼
Source Business Unit	americas	▼
Source Category	pci	▼
Source City	splunk	▼
Source Country	Pleasanton	▼
Source IP Address	USA	▼
Source Latitude	10.11.36.20	▼
Source Longitude	true	▼
Source Owner	37.694452	▼
Source Owner	-121.894461	▼
Source PCI Domain	Bill_williams	▼
Source Requires Antivirus	trust	▼
Source Should Time Synchronize	false	▼
Source Should Update	true	▼
Bytes Out	true	▼
	11402106	▼

Correlation Search:
Network - High Volume of Traffic from High or Critical Host - Rule

History:
[View all review activity for this Notable Event](#)

Contributing Events:
[View network communication involving 10.11.36.20 to 199.9.251.78](#)

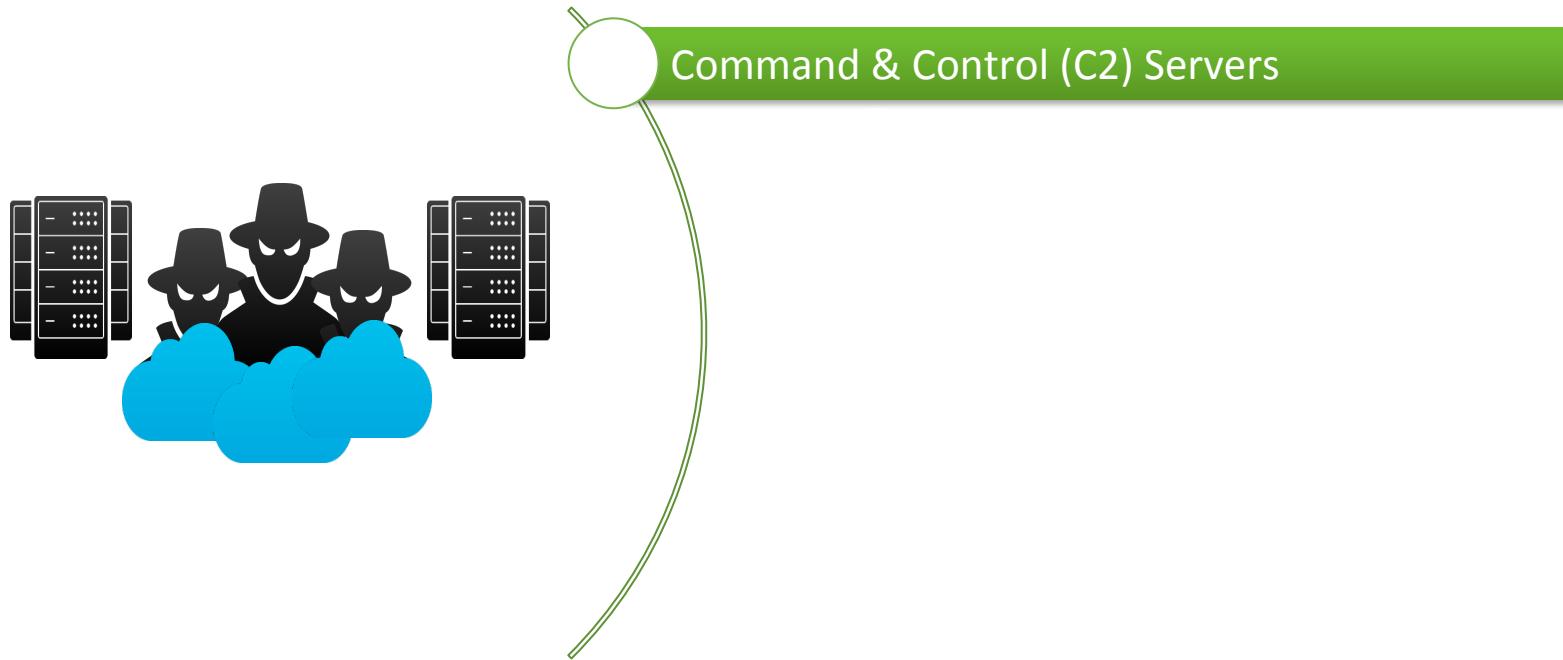
Event Details:
event_id: D74D354C-FF04-4FC2-AFA3-05C894C7452C@notable@6005482ef295ed0269d1ef3d804091eabb7e41d9
event_hash: 6005482ef295ed0269d1ef3d804091eabb7e41d9
eventtype: notable

>	9/11/15 6:58:32,000 AM	Network	High Volume of Traffic from 10.11.36.20 to 199.9.251.150	Critical	New	unassigned	▼
>	9/11/15 5:11:56,000 AM	Threat	Threat Activity Detected (ACMEDC01\$)	Low	New	unassigned	▼

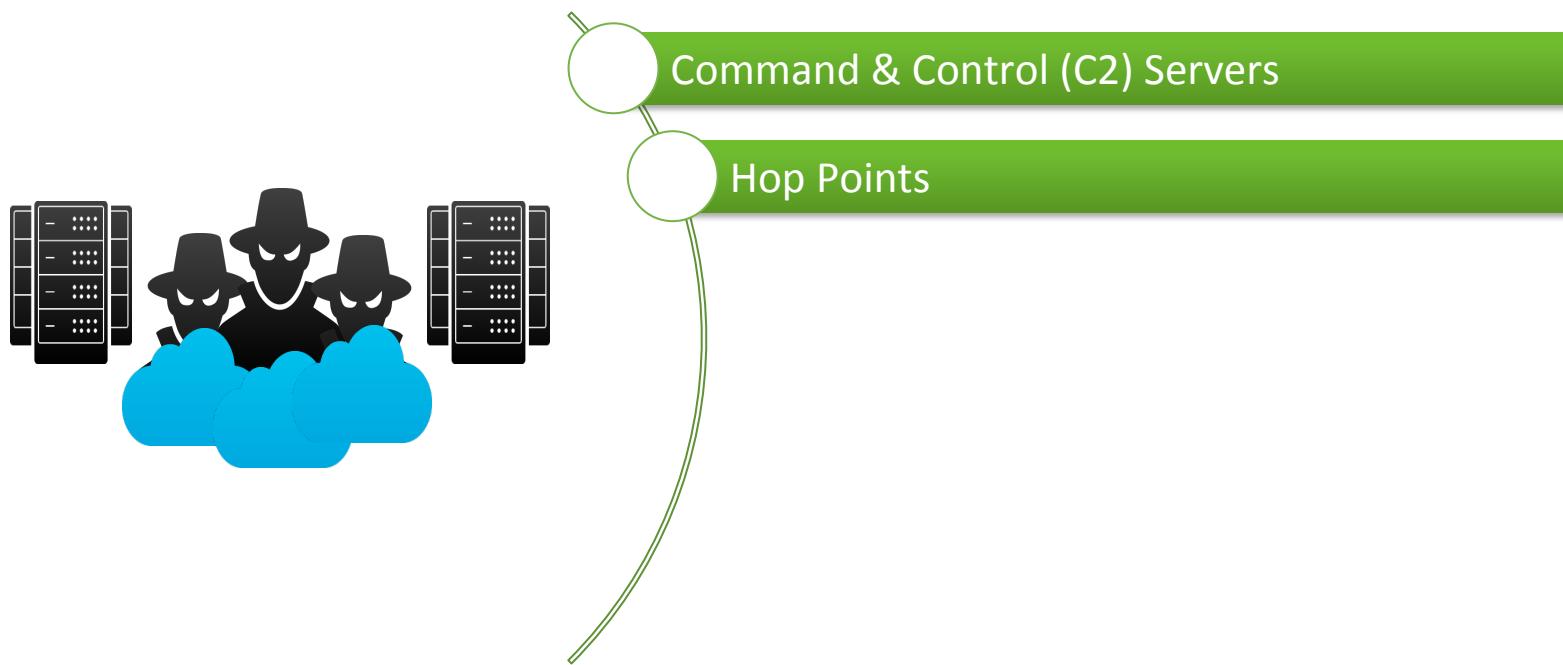
Attacker Infrastructure & Intelligence



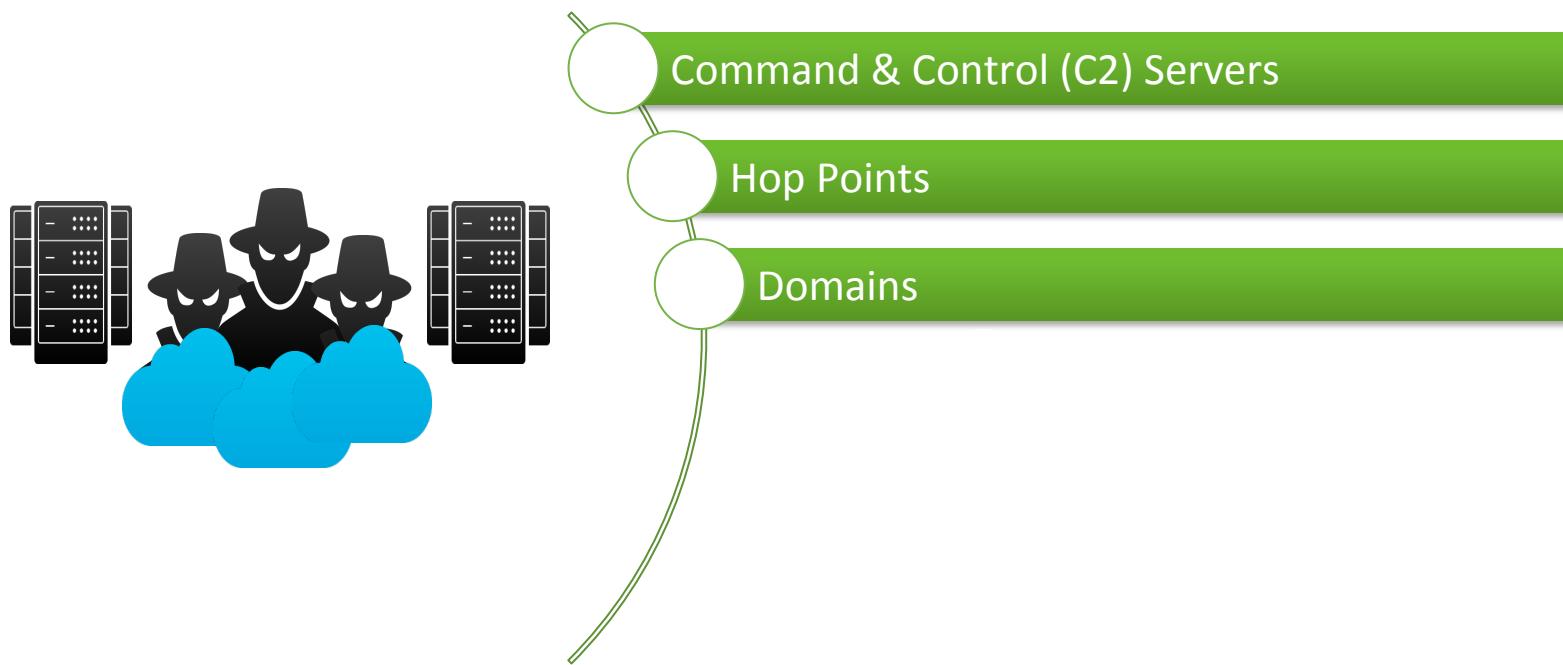
Attacker Infrastructure & Intelligence



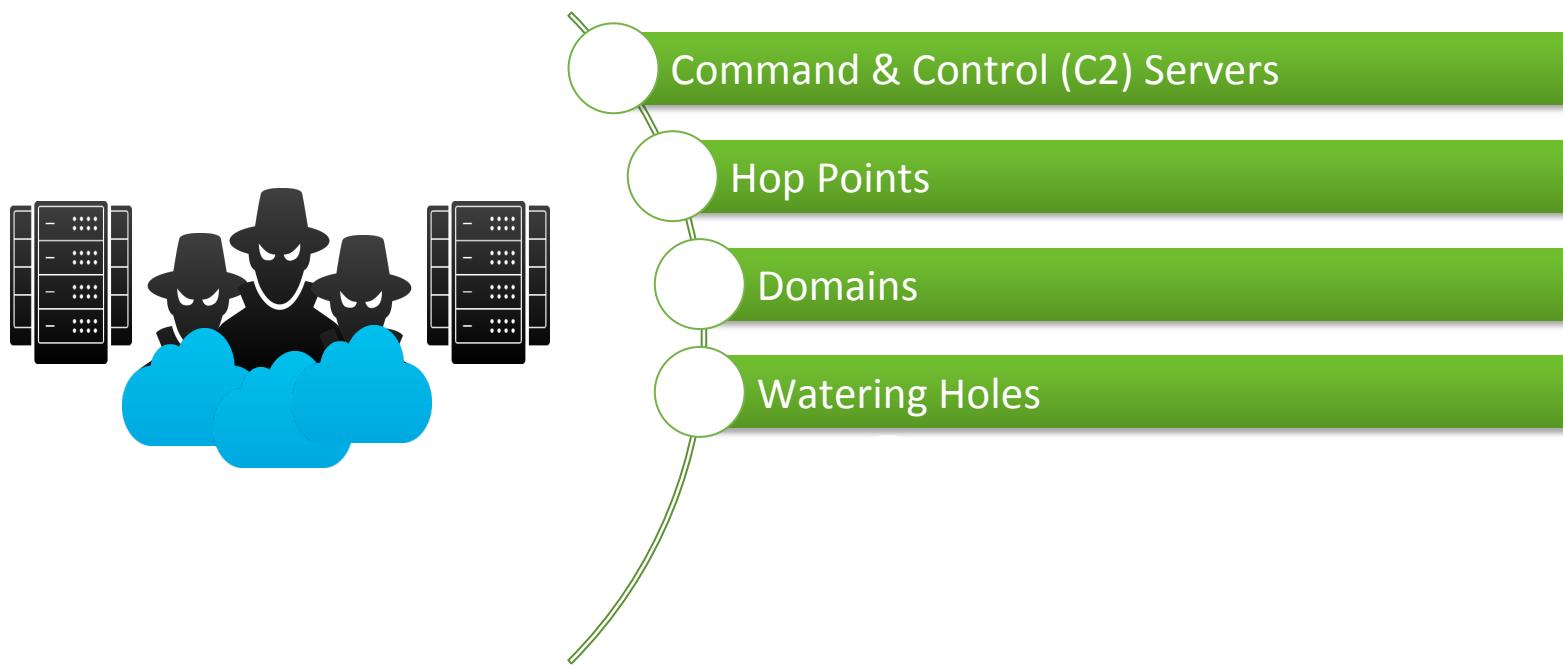
Attacker Infrastructure & Intelligence



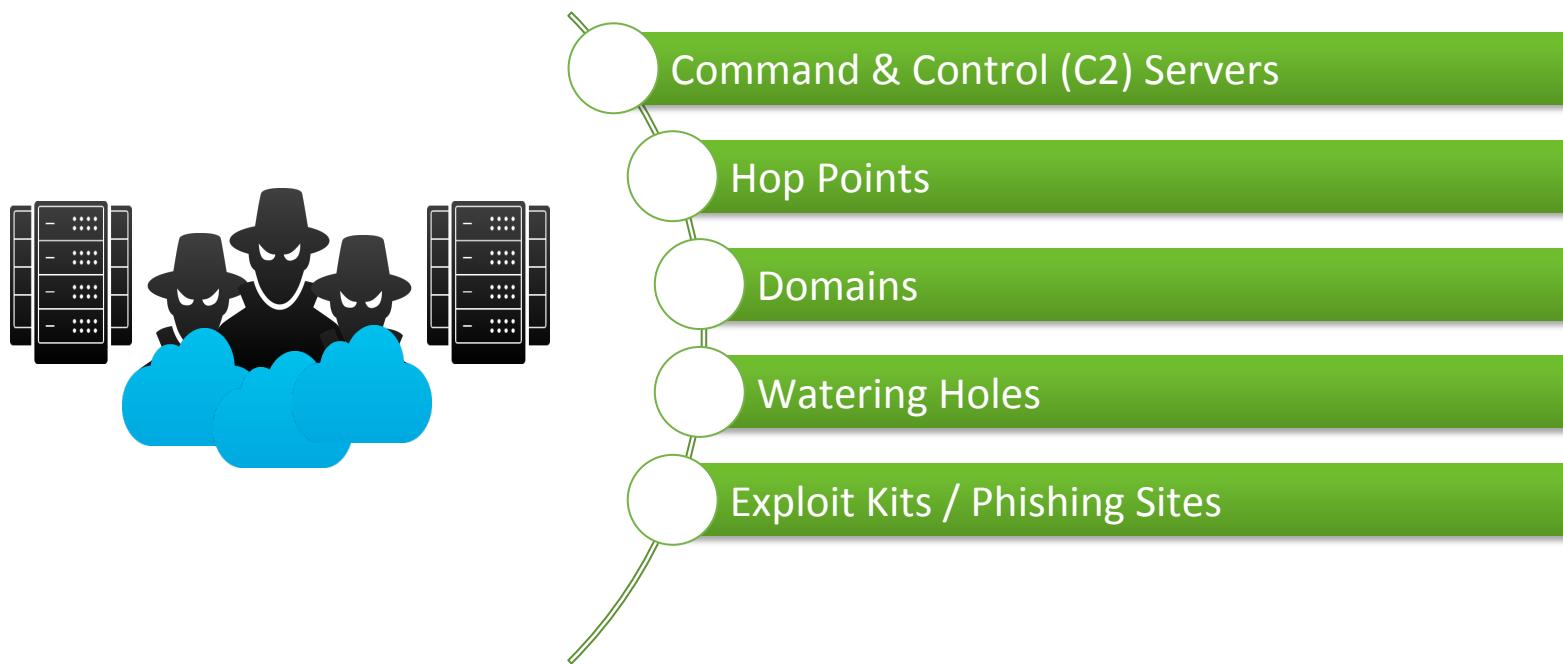
Attacker Infrastructure & Intelligence



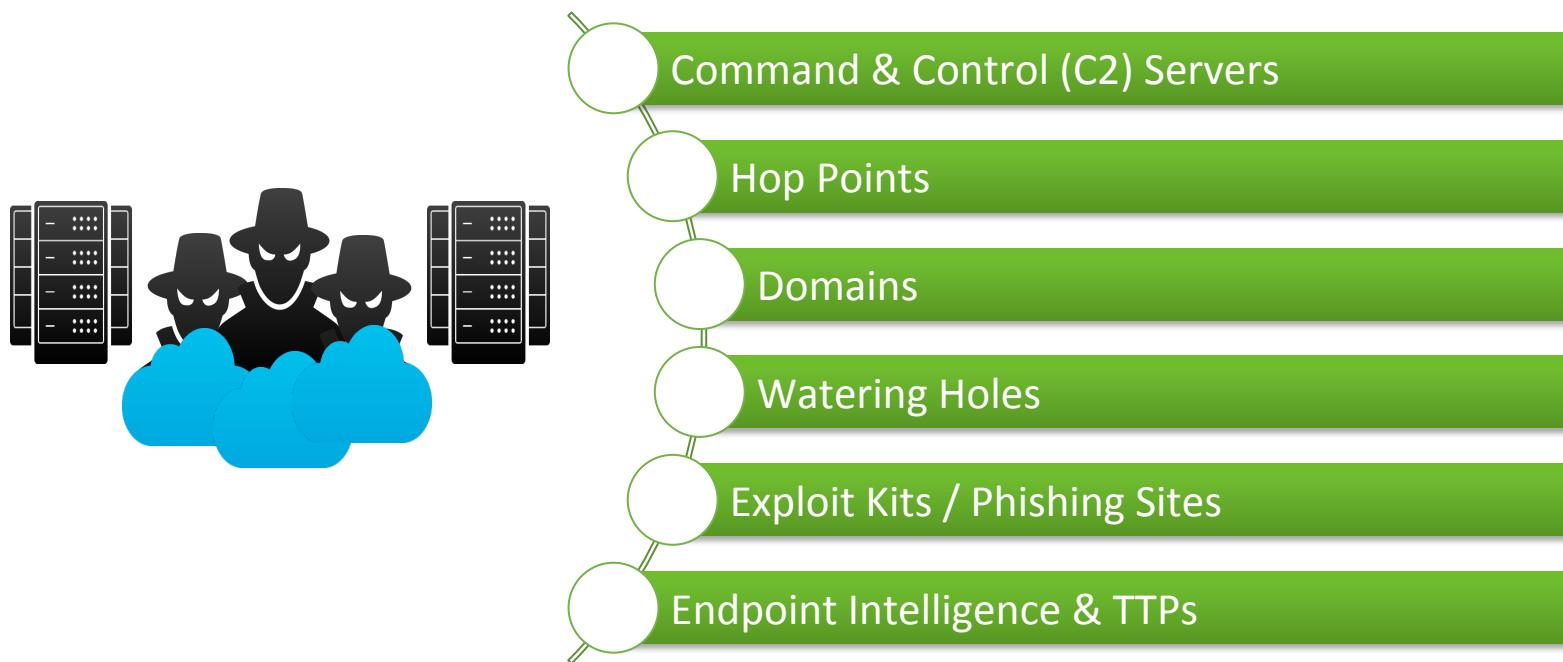
Attacker Infrastructure & Intelligence



Attacker Infrastructure & Intelligence



Attacker Infrastructure & Intelligence



ES Threat Intelligence Framework

Threat Artifacts

Threat Artifact	Threat Category	Threat Group	Malware Alias	Intel Source ID	Intel Source Path	Submit
Threat ID	All	All				

Threat Overview Network Endpoint Certificate Email

Threat Overview

source_id	source_path	source_type	threat_group	threat_category	malware_alias	count
0c7902c-67f8-479c-9f44-4d985106365a	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel.ioc	ioc	APT	Utility		5
0c7902c-61f8-479c-9f44-4d985106365a	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel_1.ioc	ioc	APT1.1	Utility1.1		5
c32ab7b5-49cb-40cc-8a12-e5f3ba91311	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/email_intel.ioc	ioc	Email APT	Email Utility		6
fireeye-stix-57b16e67-4292-46a3-ba64-60c1a491723d	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivx-report-with-indicators.xml	stix	⊕ F (and 6 more)	⊕ APT (and 2 more)		503
6d2a1b03-b216-4cd8-9a9e-8827af6ebf93	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/http_intel.ioc	ioc	HTTP APT	HTTP Utility		10
fc2d3e44-80a6-4add-ad94-de9f289e62ff	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/ip_intel.ioc	ioc	IP APT	IP Utility		9
6bd24113-2922-4d25-b490-f7271747ba948	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/process_intel.ioc	ioc	Process APT	Process Backdoor		12
4a2c5f60-f4c0-4844-ba1f-a14dac9fa36c	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/registry_intel.ioc	ioc	Registry APT	Registry Backdoor		9
7f9a6986-f00a-4071-99d3-484c9158beba	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/service_intel.ioc	ioc	Service APT	Service Backdoor		6
e651c4e4-6cce-4fcf-8bd4-ebc203907ef4	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/user_intel.ioc	ioc	User APT	User Utility		2

« prev 1 2 3 next »

Endpoint Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count
file_intel	stix	undefined	undefined		1355
file_intel	stix	F	APT		194
file_intel	stix	admin338	APT		194
file_intel	stix	japanorus	APT		194
file_intel	stix	menupass	APT		194
file_intel	stix	nitro	APT		194
file_intel	stix	th3bug	APT		194
file_intel	stix	wl	APT		194
process_intel	stix	undefined	undefined		15
registry_intel	ioc	Registry APT	Registry Backdoor		9

« prev 1 2 next »

Email Artifacts

threat_collection	source_type	ip	domain	url	http	total	threat_group	threat_category	malware_alias
ip_intel	csv	0	10091	0	0	10091	malware_domains	threatlist_domain	
ip_intel	csv	6146	0	0	0	6146	iblocklist_tor	threatlist	
ip_intel	csv	5817	0	0	0	5817	iblocklist_proxy	threatlist	
ip_intel	csv	3662	0	0	0	3662	iblocklist_spyware	threatlist	
ip_intel	stix	0	2046	0	0	2046	undefined	undefined	
ip_intel	csv	1499	0	0	0	1499	iblocklist_web_attacker	threatlist	
ip_intel	stix	164	145	0	0	309	F	APT	
ip_intel	stix	164	145	0	0	309	admin338	APT	
ip_intel	stix	164	145	0	0	309	japanorus	APT	
ip_intel	stix	164	145	0	0	309	menupass	APT	

« prev 1 2 next »

Certificate Artifacts

threat_collection	source_type	ip	domain	url	http	total	threat_group	threat_category	malware_alias
ip_intel	csv	0	10091	0	0	10091	malware_domains	threatlist_domain	
ip_intel	csv	6146	0	0	0	6146	iblocklist_tor	threatlist	
ip_intel	csv	5817	0	0	0	5817	iblocklist_proxy	threatlist	
ip_intel	csv	3662	0	0	0	3662	iblocklist_spyware	threatlist	
ip_intel	stix	0	2046	0	0	2046	undefined	undefined	
ip_intel	csv	1499	0	0	0	1499	iblocklist_web_attacker	threatlist	
ip_intel	stix	164	145	0	0	309	F	APT	
ip_intel	stix	164	145	0	0	309	admin338	APT	
ip_intel	stix	164	145	0	0	309	japanorus	APT	
ip_intel	stix	164	145	0	0	309	menupass	APT	

« prev 1 2 next »

No investigation is currently loaded. Please create (+) or load an existing one (=).



ES Threat Intelligence Framework

Threat Activity

Threat Group Threat Category Search Threat Match Value Last 24 hours Submit Advanced Filter...

THREAT MATCHES Unique Count **36k** +36k **THREAT COLLECTIONS** Unique Count **9** +9 **THREAT CATEGORIES** Unique Count **13** +13 **THREAT SOURCES** Unique Count **22** +22 **THREAT ACTIVITY** Total Count **37k** +37k

Threat Activity Over Time

time

Legend:

- certificate_intel
- email_intel
- file_intel
- ip_intel
- process_intel
- registry_intel
- service_intel
- user_intel

Most Active Threat Collections

threat_collection	search	sparkline	dc(artifacts)	count
ip_intel	Email Address Matches Network Resolution Matches Source And Destination Matches		788	36969
process_intel	Network Resolution Matches Process Matches Source And Destination Matches		2	268
email_intel	Email Address Matches Email Subject Matches File Name Matches Network Resolution Matches Source And Destination Matches		1	115
file_intel	File Hash Matches File Name Matches		24	32

No investigation is currently loaded. Please create (+) or load an existing one (=).

Most Active Threat Sources

source_id	source_path	source_type	count
iblocklist_logmein	/usr/local/bamboo/splunk-install/current/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/blocklist_logmein.csv	csv	34635
iblocklist_spyware	/usr/local/bamboo/splunk-install/current/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/blocklist_spyware.csv	csv	1082
iblocklist_proxy	/usr/local/bamboo/splunk-install/current/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/blocklist_proxy.csv	csv	625
iblocklist_web_attacker	/usr/local/bamboo/splunk-install/current/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/blocklist_web_attacker.csv	csv	401
6bd24113-2922-4d25-b490-ft27f47ba948	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/process_intel.loc	ioc	267
iblocklist_tor	/usr/local/bamboo/splunk-install/current/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/blocklist_tor.csv	csv	171

ES Threat Intelligence Framework

9/11/15 5:11:56.000 AM	Threat	Threat Activity Detected (218.57.11.26)	Low	New	unassigned	v																								
	<p>Description: Threat activity (218.57.11.26) was discovered in the "dest" field based on threat intelligence available in the ip_intel collection</p> <p>Additional Fields</p> <table><tbody><tr><td>Destination</td><td>Value 218.57.11.26</td></tr><tr><td>Destination Expected</td><td>false</td></tr><tr><td>Destination PCI Domain</td><td>untrust</td></tr><tr><td>Destination Requires Antivirus</td><td>false</td></tr><tr><td>Destination Should Time Synchronize</td><td>false</td></tr><tr><td>Destination Should Update</td><td>false</td></tr><tr><td>Source</td><td>83.66.67.236</td></tr><tr><td>Source Expected</td><td>false</td></tr><tr><td>Source PCI Domain</td><td>untrust</td></tr><tr><td>Source Requires Antivirus</td><td>false</td></tr><tr><td>Source Should Time Synchronize</td><td>false</td></tr><tr><td>Source Should Update</td><td>false</td></tr></tbody></table> <p>Action</p> <p>Correlation Search: Threat - Threat List Activity - Rule</p> <p>History: View all review activity for this Notable Event</p> <p>Contributing Events: View all threat activity involving dest="218.57.11.26"</p> <p>Original Event: View original event</p> <p>Threat Category APT APT APT</p> <p>Threat Collection ip_intel</p> <p>Threat Collection Key fireeye:stix:b7b16e67-4292-46a3-ba64-60c1a491723d:fireeye:observable-0426f8e3-b907-4433-e92c-6e2815f2c431</p> <p>Threat Description This report spotlights Poison Ivy (PIVY), a RAT that remains popular and effective a full eight years after its release, despite its age and familiarity in IT security circles. Poison Ivy is a remote access tool that is freely available for download from its official web site at www.poisonivy-rat.com. First released in 2005, the tool has gone unchanged since 2008 with version 2.3.2. Poison Ivy includes features common to most Windows-based RATs, including key logging, screen capturing, video capturing, file transfers, system administration, password theft, and traffic relaying. Poison Ivy's wide availability and easy-to-use features make it a popular choice for all kinds of criminals. But it's probably most notable for its role in many high profile, targeted APT attacks. These APTs pursue specific targets, using RATs to maintain a persistent presence within the target's network. They move laterally and escalate system privileges to extract sensitive information—whenever the attacker wants to do so. Because some RATs used in targeted attacks are widely available, determining whether an attack is part of a broader APT campaign can be difficult. Equally challenging is identifying malicious traffic to determine the attacker's post-compromise activities and assess overall damage—these RATs often encrypt their network communications after the initial exploit. In 2011, three years after the most recent release of PIVY, attackers used the RAT to compromise security firm RSA and steal data about its SecurID authentication system. That data was subsequently used in other attacks. The RSA attack was linked to Chinese threat actors and described at the time as extremely sophisticated. Exploiting a zero-day vulnerability, the attack delivered PIVY as the payload. It was not an isolated incident. The campaign appears to have started in 2010, with many other companies compromised. PIVY also played a key role in the 2011 campaign known as Nitro that targeted chemical makers, government agencies, defense contractors, and human rights groups. Six active a year later, the Nitro attackers used a zero-day vulnerability in Java to deliver PIVY as a payload of a Java exploit. This exploit was delivered via Internet Explorer, used in what is known as a "strategic web compromise" attack against visitors to a U.S. government website and a variety of others. RATs require live, direct, real-time human interaction by the APT attacker. This characteristic is distinctly different from crimeware (malware focused on cybercrime), where the criminal can issue commands to their botnet of compromised endpoints whenever they please and set them to work on a common goal such as a spam relay. In contrast, RATs are much more personal and may indicate that you are dealing with a dedicated threat actor that is interested in your organization specifically.</p> <p>Threat Group F admin338 japanbug nitro th3bug wl menupass</p> <p>Threat Key fireeye:stix:b7b16e67-4292-46a3-ba64-60c1a491723d:fireeye-pivy-report-with-indicators.xml</p> <p>Threat Match Field dest</p> <p>Threat Match Value 218.57.11.26</p> <p>Threat Source ID fireeye:stix:b7b16e67-4292-46a3-ba64-60c1a491723d</p>	Destination	Value 218.57.11.26	Destination Expected	false	Destination PCI Domain	untrust	Destination Requires Antivirus	false	Destination Should Time Synchronize	false	Destination Should Update	false	Source	83.66.67.236	Source Expected	false	Source PCI Domain	untrust	Source Requires Antivirus	false	Source Should Time Synchronize	false	Source Should Update	false					
Destination	Value 218.57.11.26																													
Destination Expected	false																													
Destination PCI Domain	untrust																													
Destination Requires Antivirus	false																													
Destination Should Time Synchronize	false																													
Destination Should Update	false																													
Source	83.66.67.236																													
Source Expected	false																													
Source PCI Domain	untrust																													
Source Requires Antivirus	false																													
Source Should Time Synchronize	false																													
Source Should Update	false																													

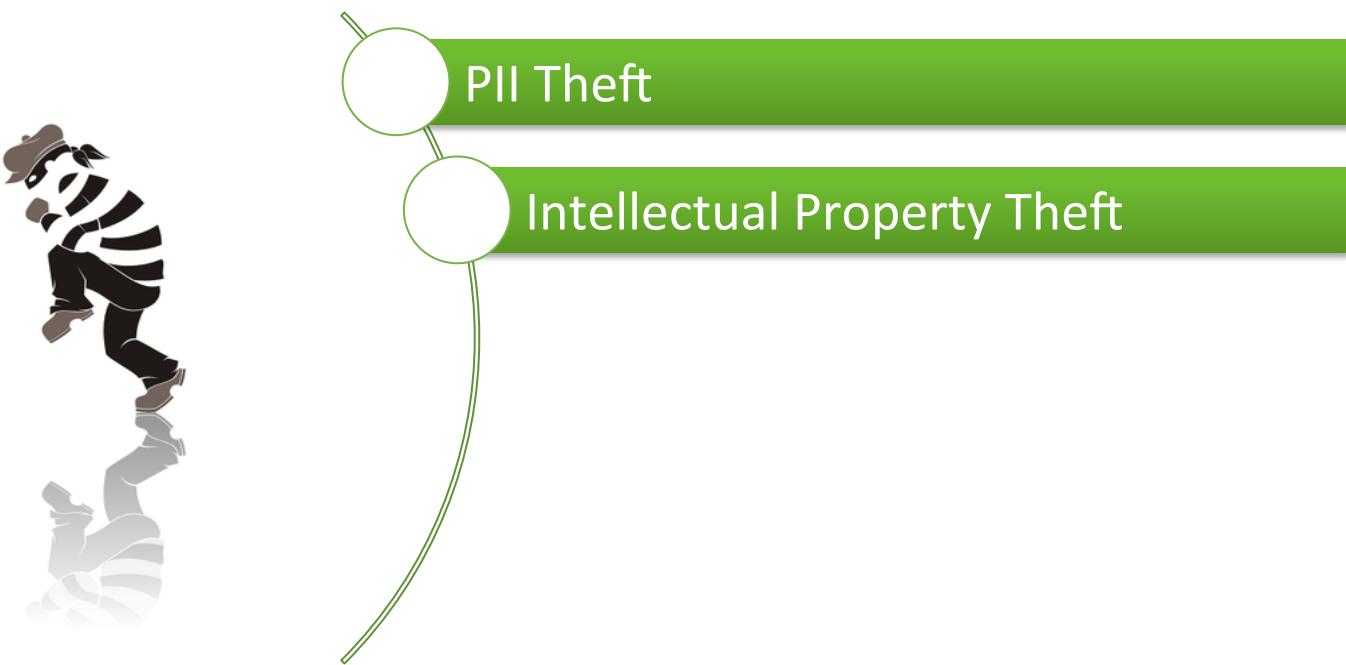
Actions on Intent



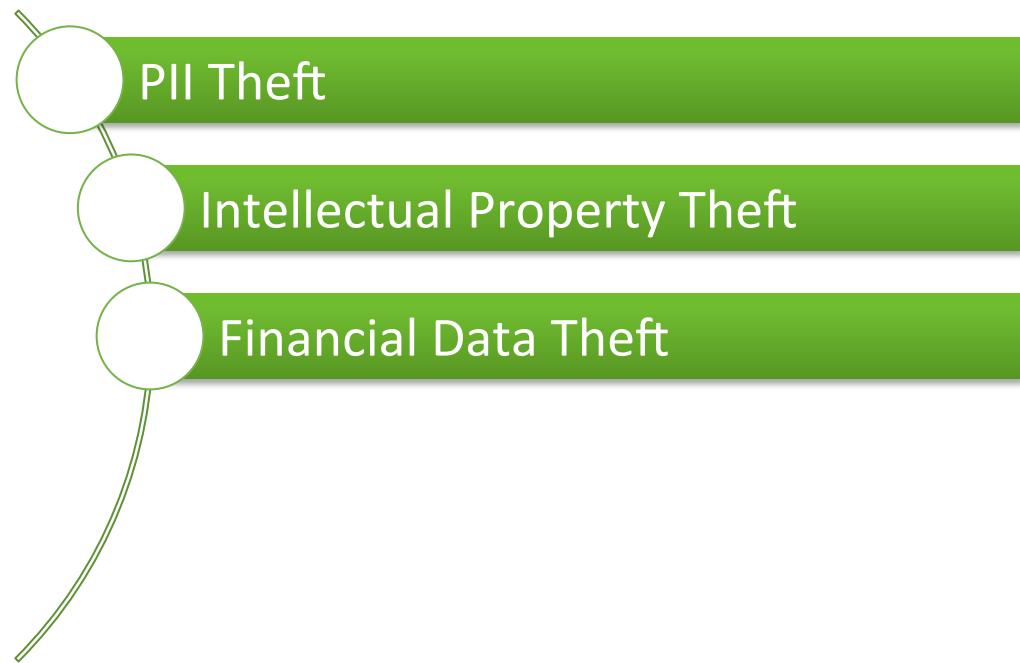
Actions on Intent



Actions on Intent



Actions on Intent



Actions on Intent



Actions on Intent



ES & Action on Intent

Incident Review

Urgency

CRITICAL	15
HIGH	178
MEDIUM	5238
LOW	36444
INFO	0

Status

Name

Owner

Search

Security Domain

Time

Last 24 hours

Tag

Submit

41,875

Format Time

1 hour per column

Job Smart Mode

12:00 AM Fri Sep 11 6:00 AM 12:00 PM

8,000 5,000 8,000 5,000

Create Tags

Field Value

event_id=D74D354C-FF04-4FC2-AFA3-05C894C7452C@notable@@9655733411133baa521a4ede6f8142f0ae958fb

Tag(s)

EXFIL-EMAIL

Comma or space separated list of tags.

Cancel Save

Edit all selected | Edit all 41875 matching events | Add to Investigation

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	9/11/15 1:10:17.000 PM	Threat	Watchlisted Event Observed	Medium	New	unassigned	▼
>	9/11/15 1:10:17.000 PM	Threat	Watchlisted Event Observed	Medium	New	unassigned	▼
>	9/11/15 1:08:15.000 PM	Threat	Watchlisted Event Observed	Medium	New	unassigned	▼
▼	9/11/15 1:06:29.000 PM	Network	Unusual Volume of Network Activity	Medium	New	unassigned	▼

Description:

An unusual volume of network activity was detected. 1655 unique sources have generated network traffic in the past 15 minutes and 124029 network events have been observed in the same time period.

Additional Fields Value Action

Event Details:

event_id D74D354C-FF04-4FC2-AFA3-05C894C7452C@notable@@9655733411133baa521a4ede6f8142f0ae958fb

event_hash 9655733411133baa521a4ede6f8142f0ae958fb

eventtype notable

>	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	9/11/15 1:02:13.000 PM	Threat	Watchlisted Event Observed	Medium	New	unassigned	▼
>	9/11/15 1:02:13.000 PM	Threat	Watchlisted Event Observed	Medium	New	unassigned	▼
>	9/11/15 1:02:13.000 PM	Threat	Watchlisted Event Observed	Medium	New	unassigned	▼
>	9/11/15 1:00:14.000 PM	Threat	Watchlisted Event Observed	Medium	New	unassigned	▼
>	9/11/15 12:58:11.000 PM	Endpoint	Host Sending Excessive Email (10.11.36.8)	High	New	unassigned	▼
>	9/11/15 12:58:04.000 PM	Threat	Watchlisted Event Observed	Medium	New	unassigned	▼
>	9/11/15 12:56:03.000 PM	Threat	Watchlisted Event Observed	Medium	New	unassigned	▼
>	9/11/15 12:56:03.000 PM	Threat	Watchlisted Event Observed	Medium	New	unassigned	▼
>	9/11/15 12:56:03.000 PM	Threat	Watchlisted Event Observed	Medium	New	unassigned	▼

Correlation Search:
Network - Unusual Volume of Network Activity - Rule

History:
View all review activity for this Notable Event

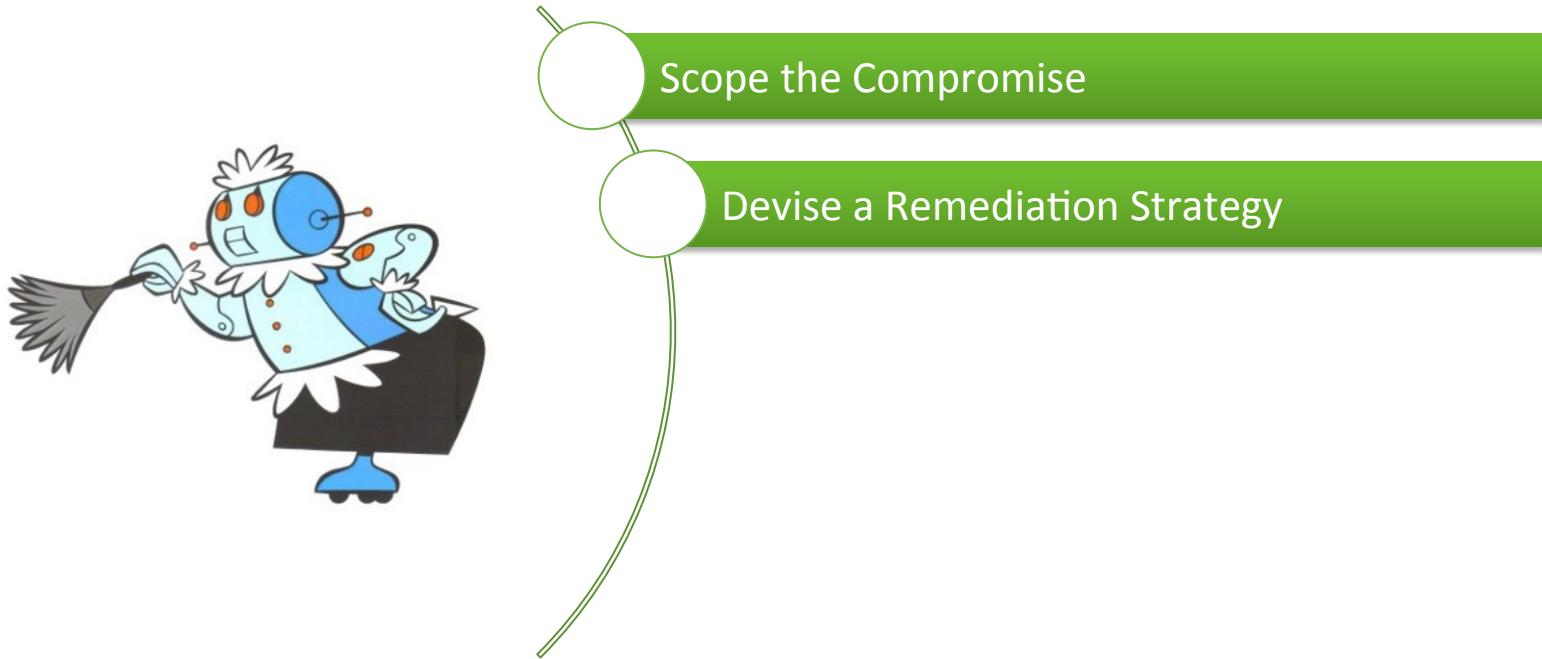
Remediation



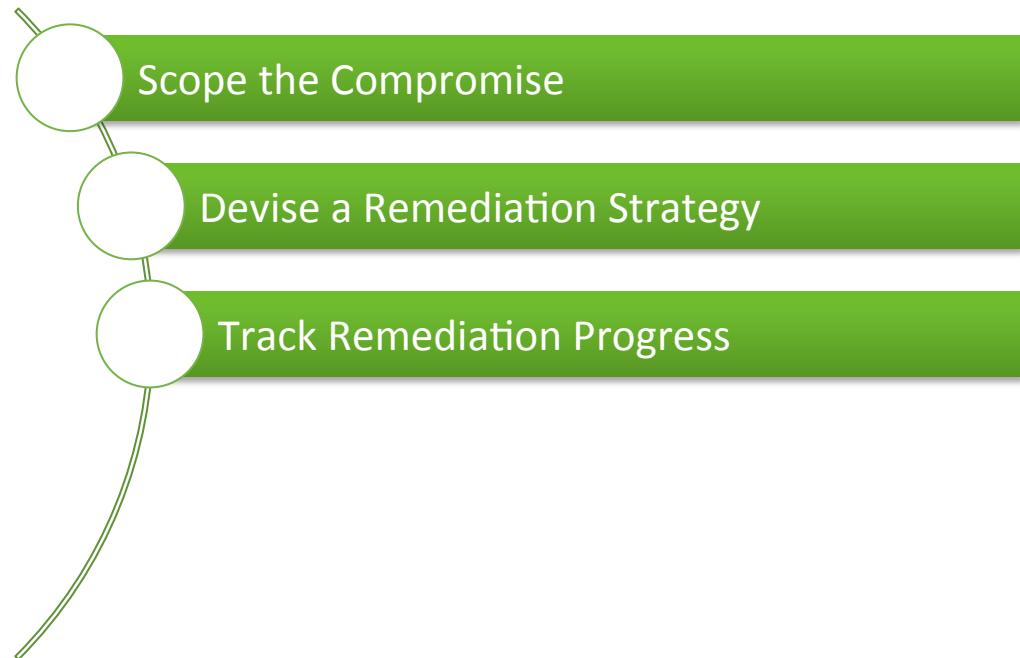
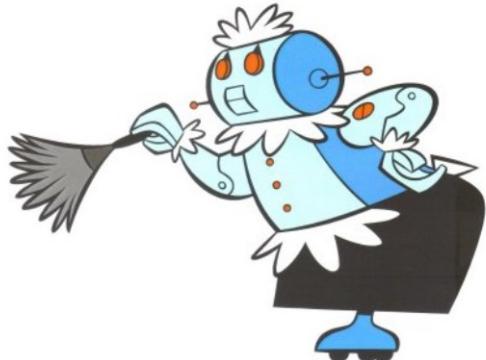
Remediation



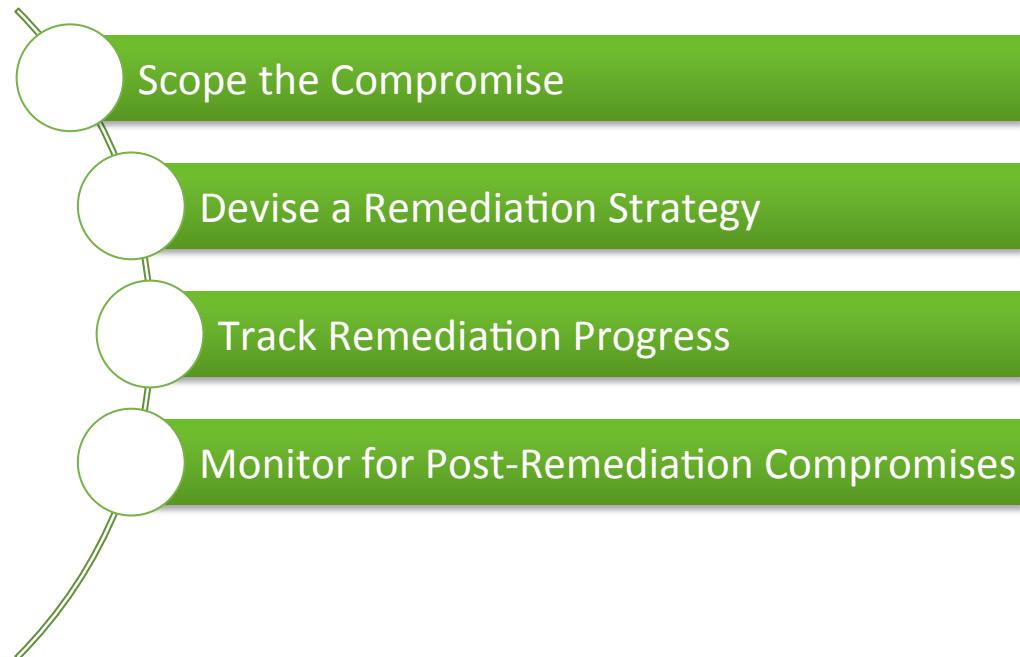
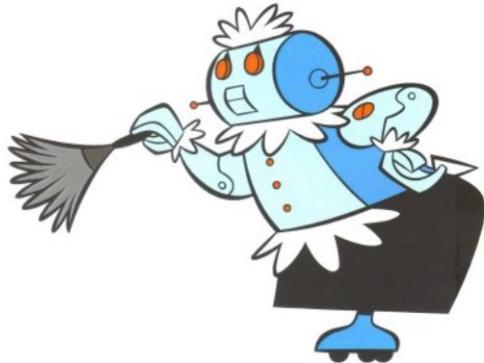
Remediation



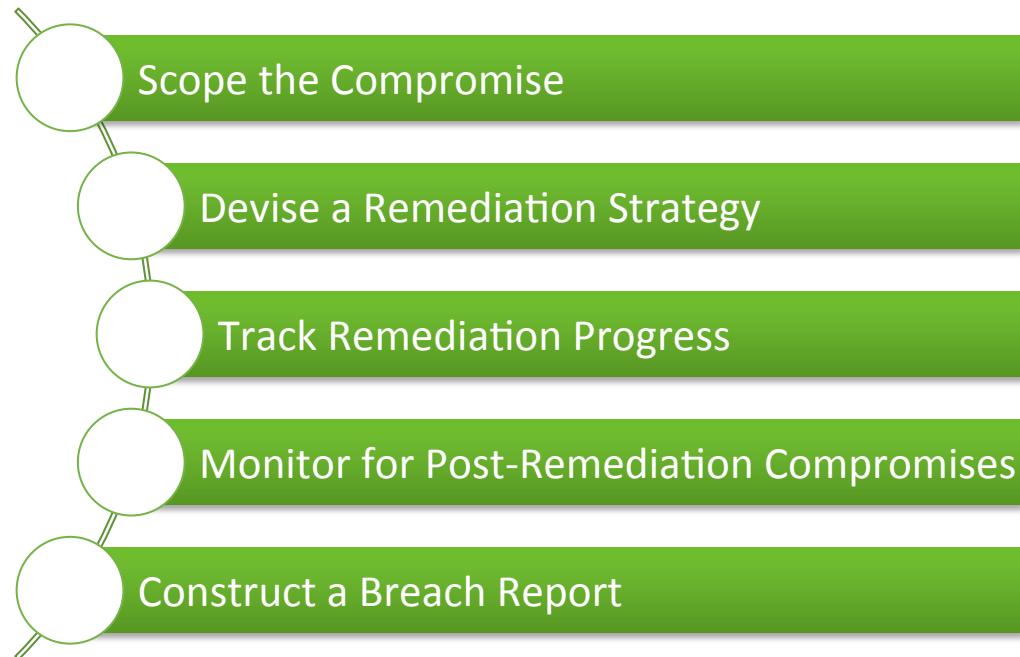
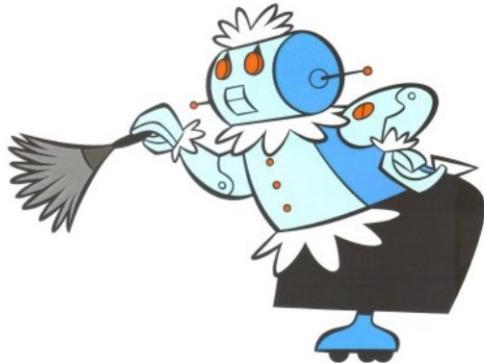
Remediation



Remediation



Remediation



ES Incident Review

Splunk > App: Enterprise Security >

Security Posture Incident Review My Investigations Advanced Threat > Security Domains > Audit > Search > Configure >

Administrator > Messages > Settings > Activity > Help > Find

Enterprise Security ES

Incident Review

Urgency

Critical	0
High	1
Medium	3
Low	0
Info	0

Status Name

Owner Search

Security Domain Time

Tag

4 of 18,399 events matched

Format Timeline >

Job >

1 hour per column

	Sep 11, 2015 10:00 AM	2
1	6:00 PM Thu Sep 10 2015	12:00 AM Fri Sep 11
	6:00 AM	12:00 PM

Edit all selected | Edit all 41875 matching events | Add to Investigation

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	9/11/15 1:06:29.000 PM	Network	Unusual Volume of Network Activity	Medium	New	unassigned	<input type="button" value="v"/>
>	9/11/15 1:02:13.000 PM	Threat	Watchlisted Event Observed	Medium	New	unassigned	<input type="button" value="v"/>
>	9/11/15 12:58:11.000 PM	Endpoint	Host Sending Excessive Email (10.11.36.8)	High	New	unassigned	<input type="button" value="v"/>
>	9/11/15 12:48:01.000 PM	Threat	Watchlisted Event Observed	Medium	New	unassigned	<input type="button" value="v"/>

About Support File a Bug Documentation Privacy Policy © 2005-2015 Splunk Inc. All rights reserved.

ES Incident Review

Splunk > App: Enterprise Security >

Administrator > Messages > Settings > Activity > Help > Find

Enterprise Security

Incident Review

Urgency

CRITICAL	1
HIGH	1
MEDIUM	2
LOW	0
INFO	0

Status

Name

Owner

Security Domain

Time

Tag

Submit

Edit Events

Status: In Progress

Urgency: High

Owner: esanalyst

Comment: We need to investigate this system...

Cancel Save changes

1 hour per column

12:00 AM Fri Sep 11 6:00 AM 12:00 PM

1 2 1

Edit all selected | Edit all 4 matching events | Add to Investigation

i	Time	Security Domain	Title	Urgency
>	9/11/15 1:06:29.000 PM	Network	Unusual Volume of Network Activity	Critical
>	9/11/15 1:02:13.000 PM	Threat	Watchlisted Event Observed	Medium
> (checked)	9/11/15 12:58:11.000 PM	Endpoint	Host Sending Excessive Email (10.11.36.8)	High
>	9/11/15 12:48:01.000 PM	Threat	Watchlisted Event Observed	Medium

Status	Owner	Actions
Resolved	esanalyst	▼
New	unassigned	▼
New	unassigned	▼
New	unassigned	▼

© 2005-2015 Splunk Inc. All rights reserved.

ES Incident Review

Splunk > App: Enterprise Security >

Administrator > Messages > Settings > Activity > Help > Find

Enterprise Security

Incident Review

Urgency

Critical	1
High	1
Medium	2
Low	0
Info	0

Status

Name

Owner

Search

Format Time

2

1

Create new investigation

Cancel Save

Job Smart Mode

1 hour per column

6:00 PM Thu Sep 10 2015

12:00 AM Fri Sep 11

6:00 AM

12:00 PM

1

2

Tag

BREACH!

Submit

Add to Investigation

You are saving 2 selected events

Select an Investigation BREACH1 (ID: 55f30e487...)

Cancel Save

Edit all selected | Edit all 4 matching events | Add to Investigation

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
> <input checked="" type="checkbox"/>	9/11/15 1:06:29.000 PM	Network	Unusual Volume of Network Activity	Critical	Resolved	esanalist	
> <input type="checkbox"/>	9/11/15 1:02:13.000 PM	Threat	Watchlisted Event Observed	Medium	New	unassigned	
> <input checked="" type="checkbox"/>	9/11/15 12:58:11.000 PM	Endpoint	Host Sending Excessive Email (10.11.36.8)	High	New	unassigned	
> <input type="checkbox"/>	9/11/15 12:48:01.000 PM	Threat	Watchlisted Event Observed	Medium	New	unassigned	

About Support File a Bug Documentation Privacy Policy © 2005-2015 Splunk Inc. All rights reserved.

ES Investigator Timeline

splunk > App: Enterprise Security >

Administrator > Messages > Settings > Activity > Help > Find

Security Posture Incident Review My Investigations Advanced Threat > Security Domains > Audit > Search > Configure >

Enterprise Security 

BREACH1
(no description defined)

[Create New Entry](#)

< Back to Investigation Management

[Timeline](#) [List](#) Type: All [Filter](#)

9:58 AM
September 11, 2015

Notable Event (Host: | Sourcetype: stash)

09/11/2015 12:00:00 -0400, search_name="Endpoint - Host Sending Excessive Email - Rule", search_now=1441990500.000, info_min_time=1441986600.000, info_max_time=1441990200.000, info_search_time=1441990585.934, WhereCIX="o.3399538398", count=26, dest_count=26, src="10.11.36.8"

10:06 AM
Notable Event (Host: | Sourcetype: stash)



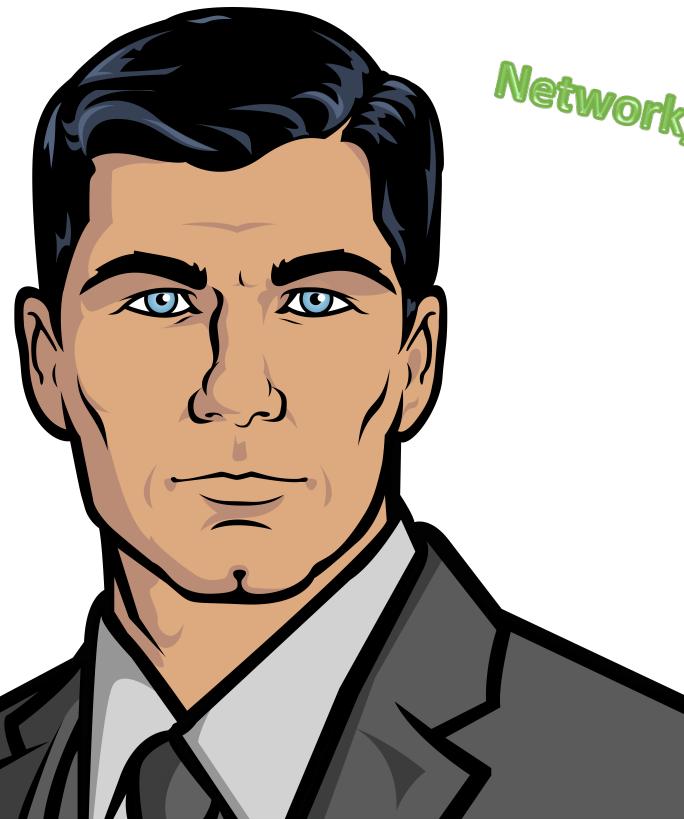
9:58 AM 10:00 AM 10:02 AM 10:06 AM



Splunk Enterprise Security



Splunk Enterprise Security



Network/Endpoint Detection!

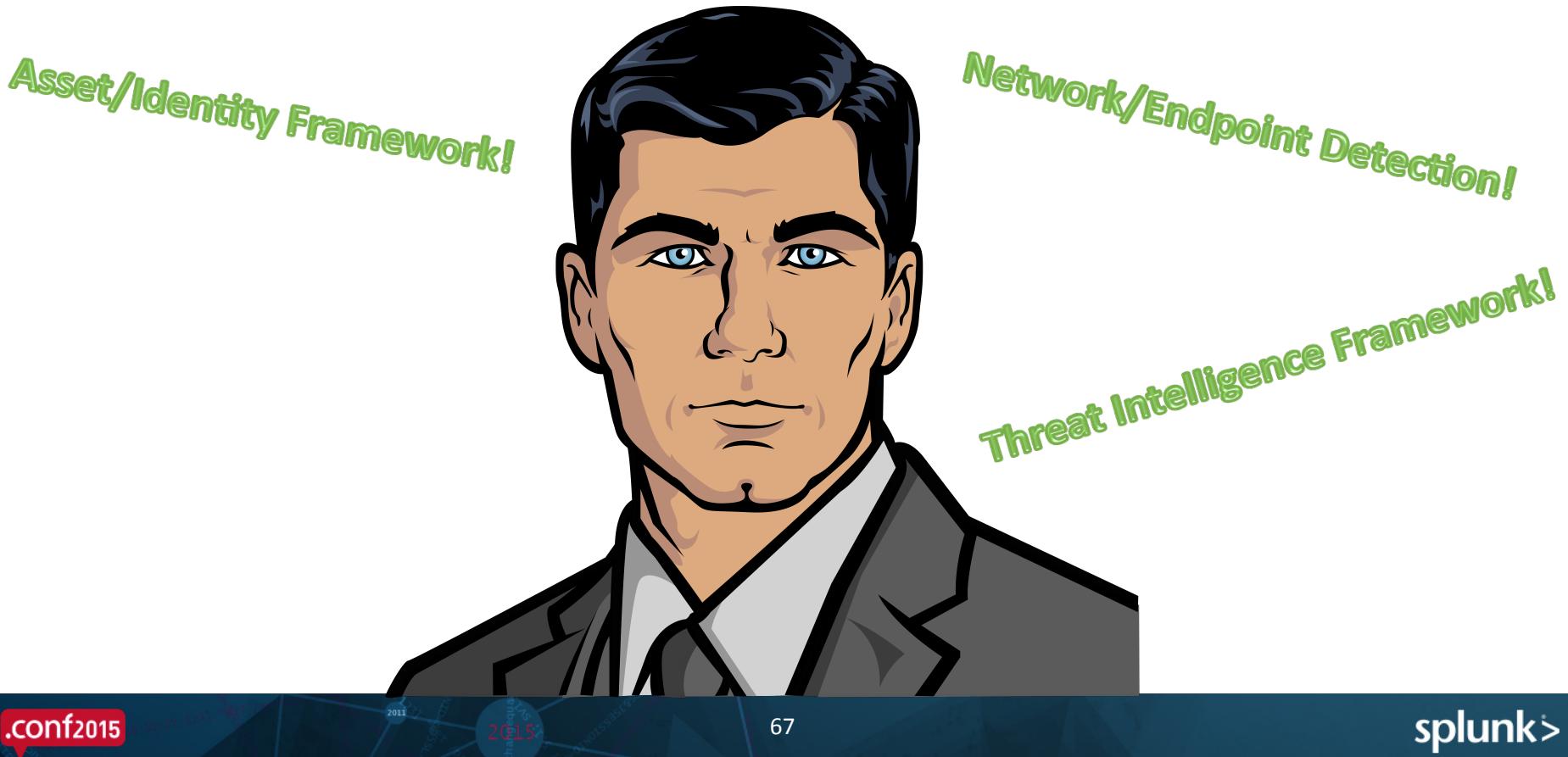
Splunk Enterprise Security

Asset/Identity Framework!

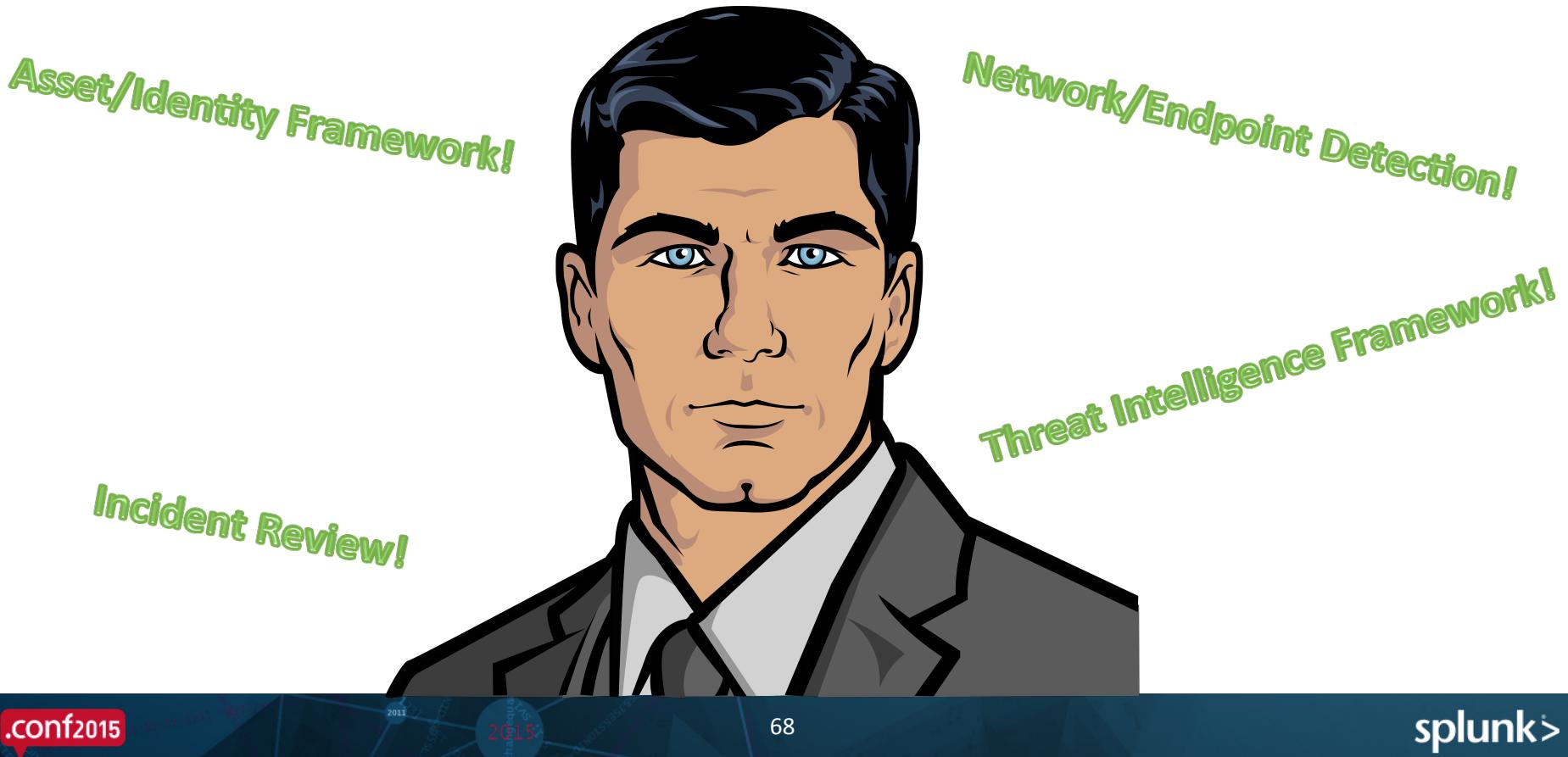
Network/Endpoint Detection!



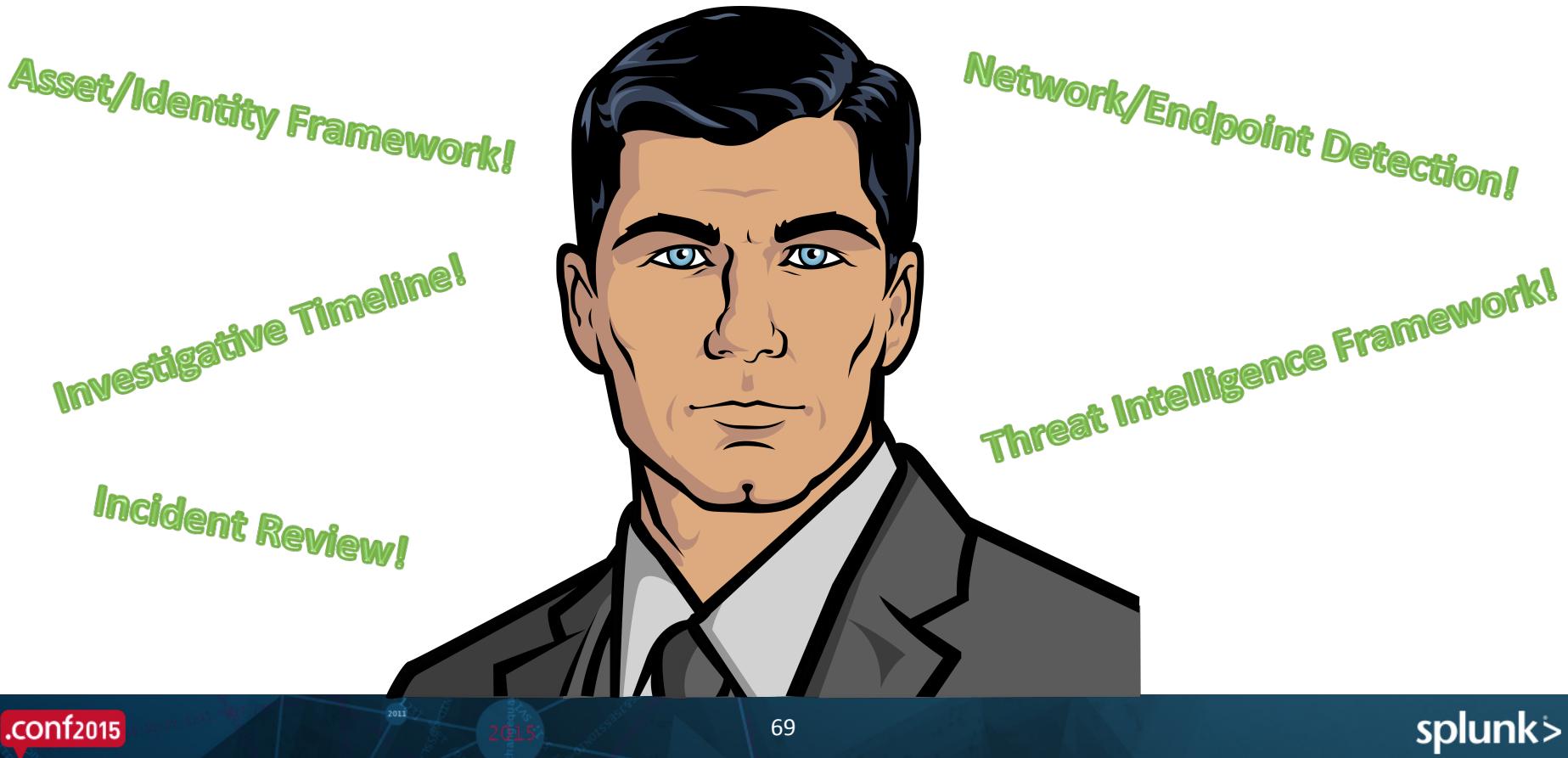
Splunk Enterprise Security



Splunk Enterprise Security



Splunk Enterprise Security



Splunk Enterprise Security

DETECT



memegenerator.net

Just Detected a Breach, Now What?



Just Detected a Breach, Now What?



ES Breach Management App



ES Breach Management App



ES Breach Management App



ES Breach Management App



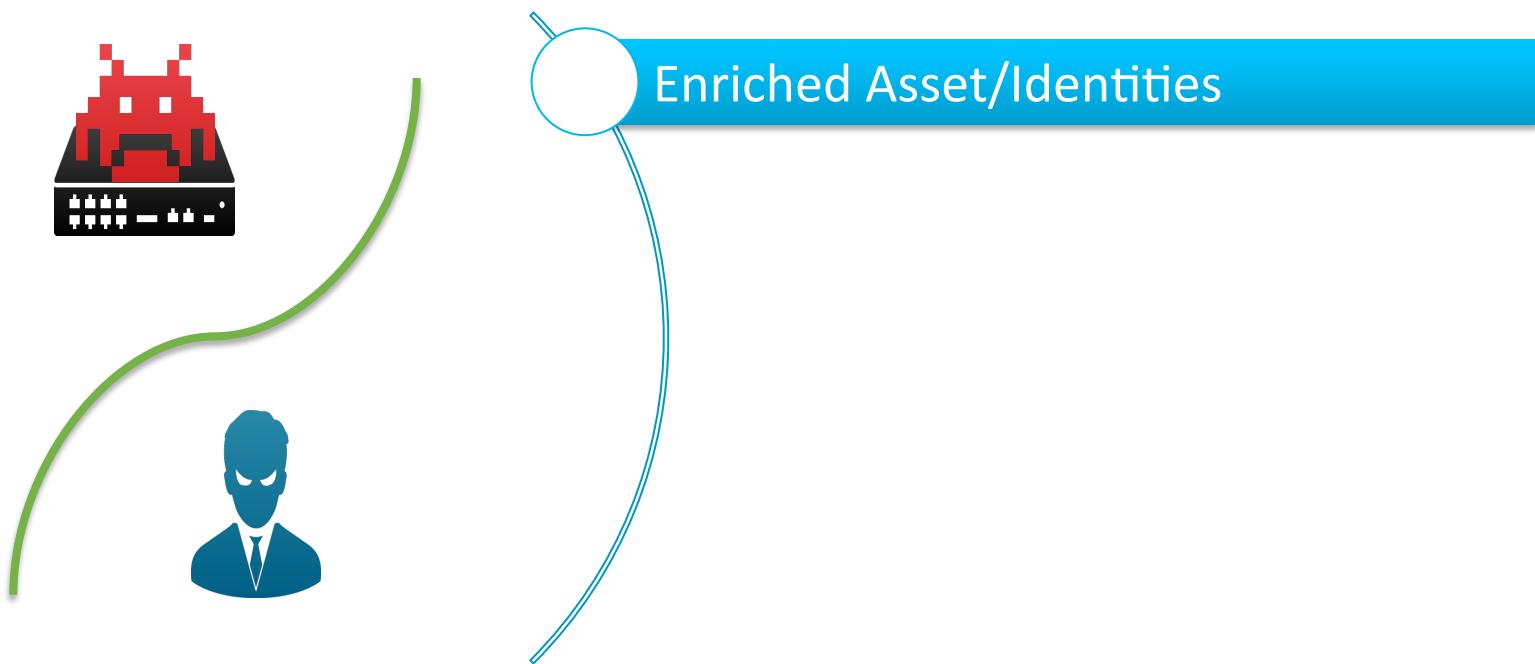
ES Breach Management App



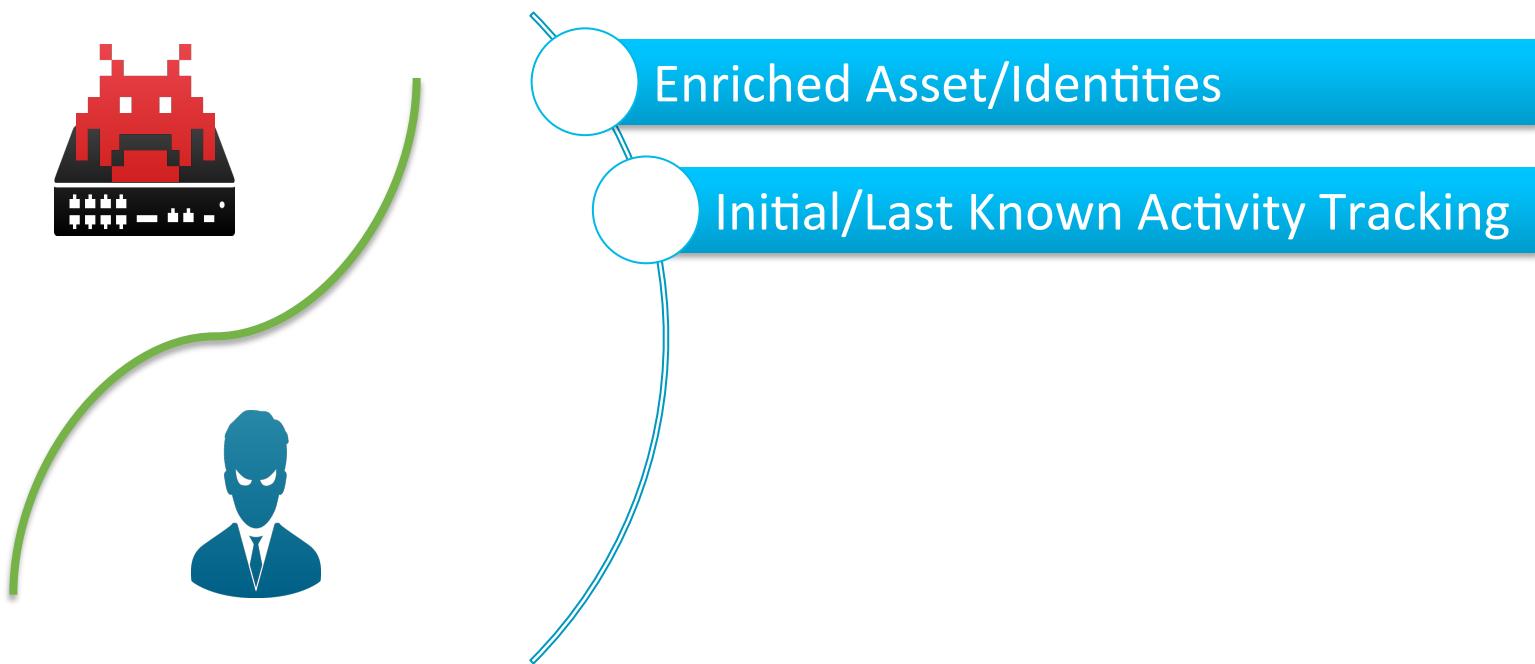
Track Compromised Assets/Identities



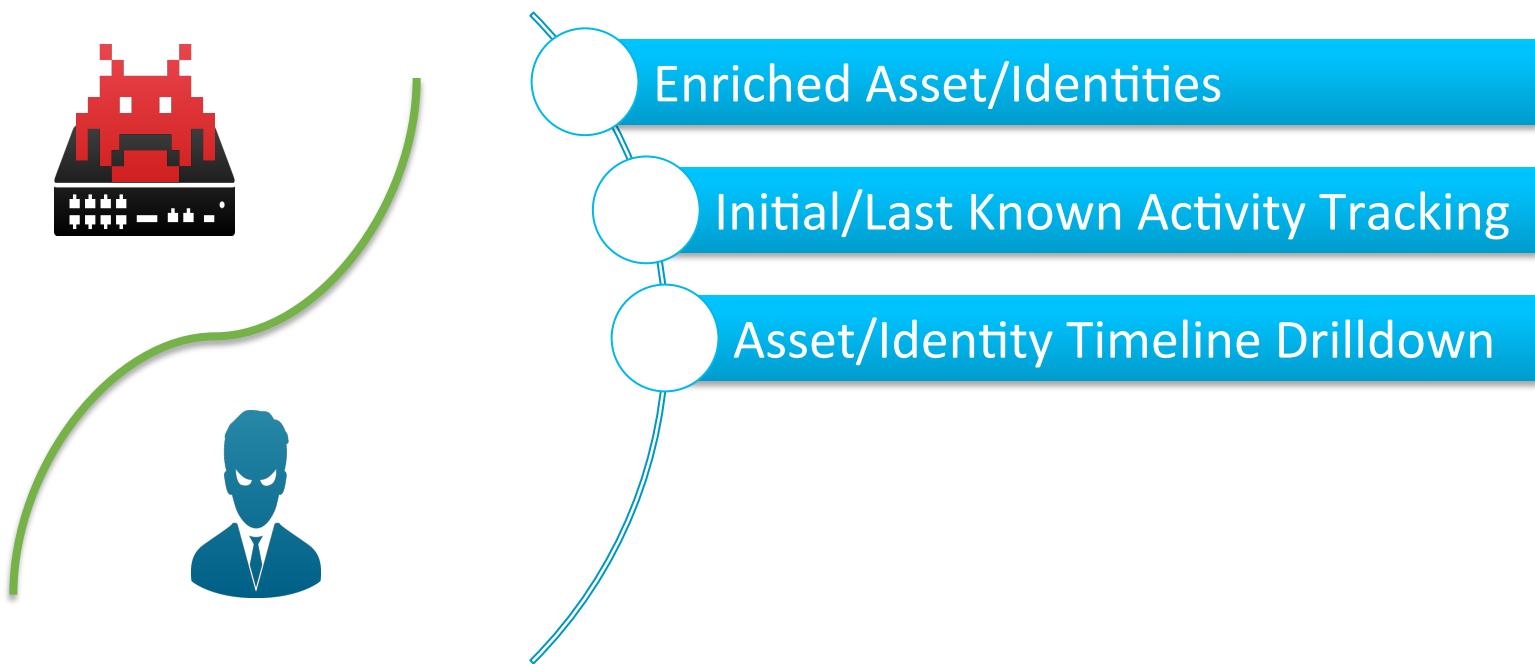
Track Compromised Assets/Identities



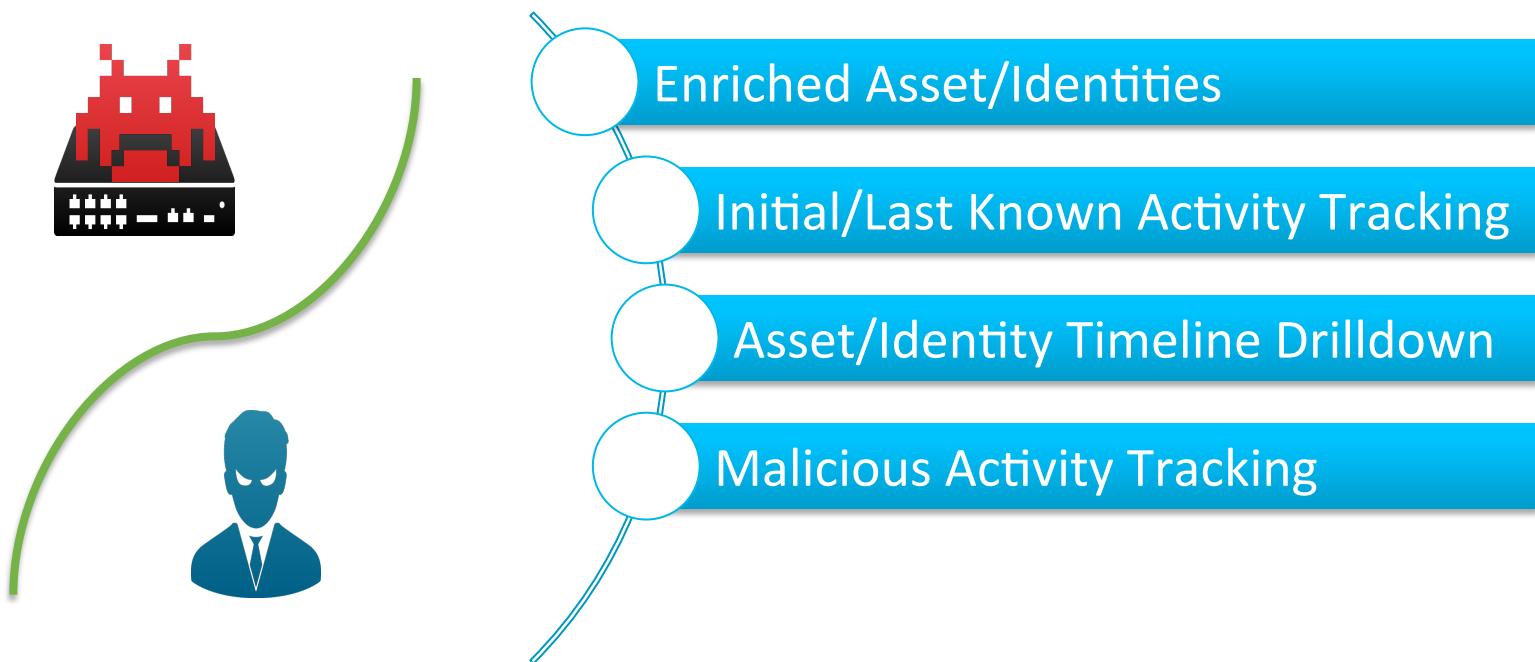
Track Compromised Assets/Identities



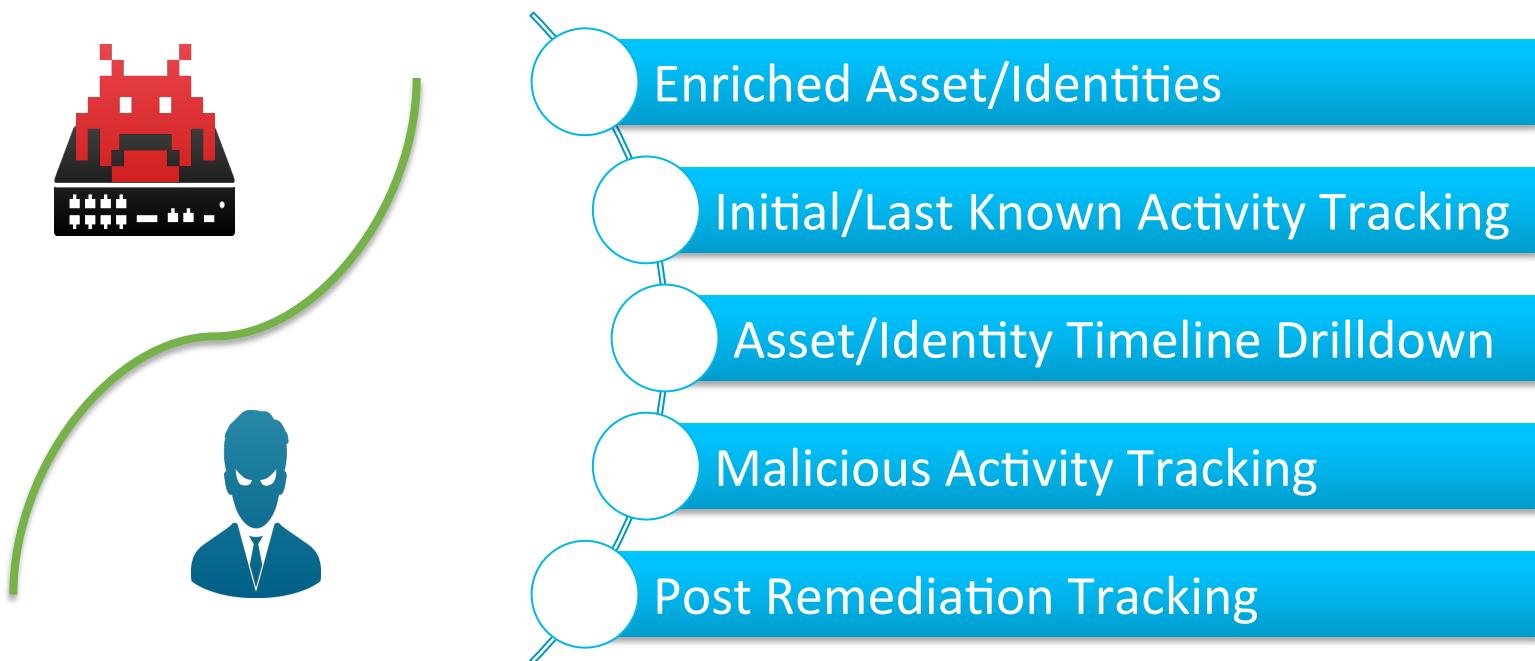
Track Compromised Assets/Identities



Track Compromised Assets/Identities



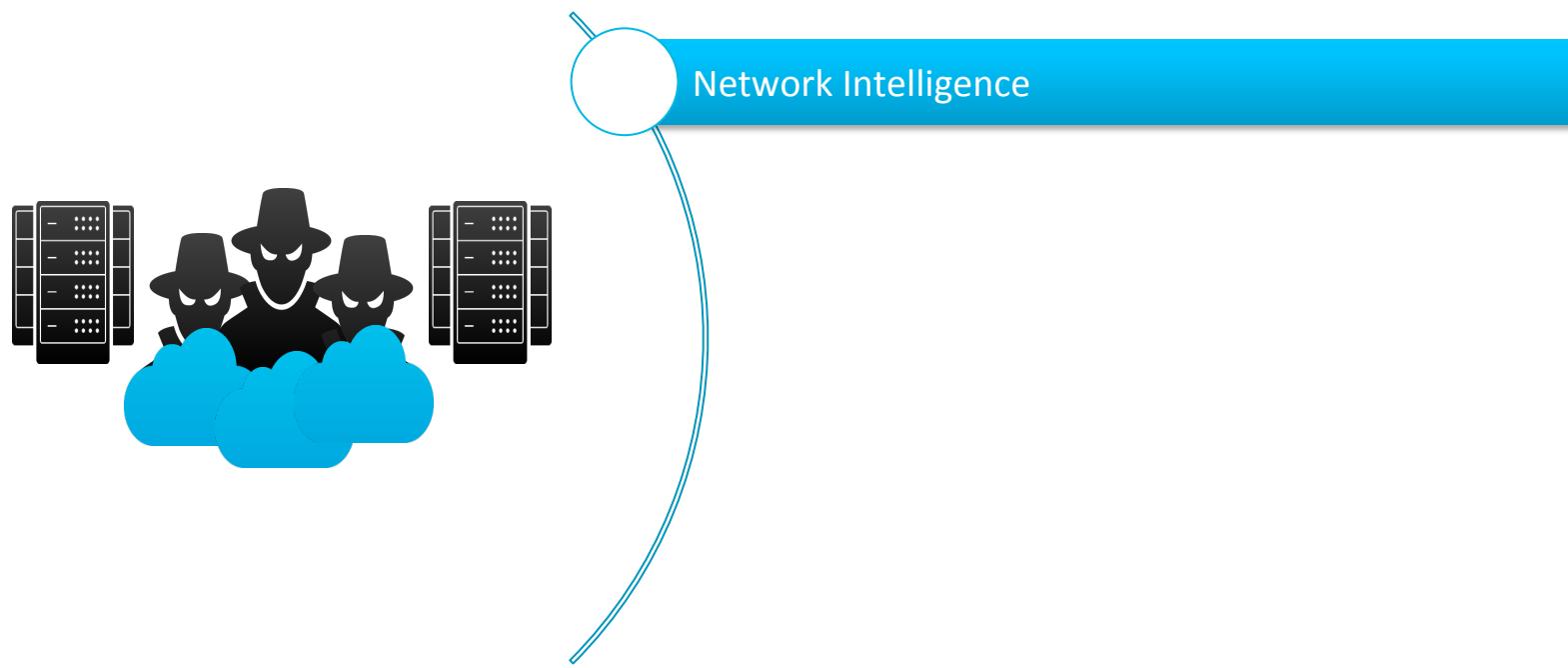
Track Compromised Assets/Identities



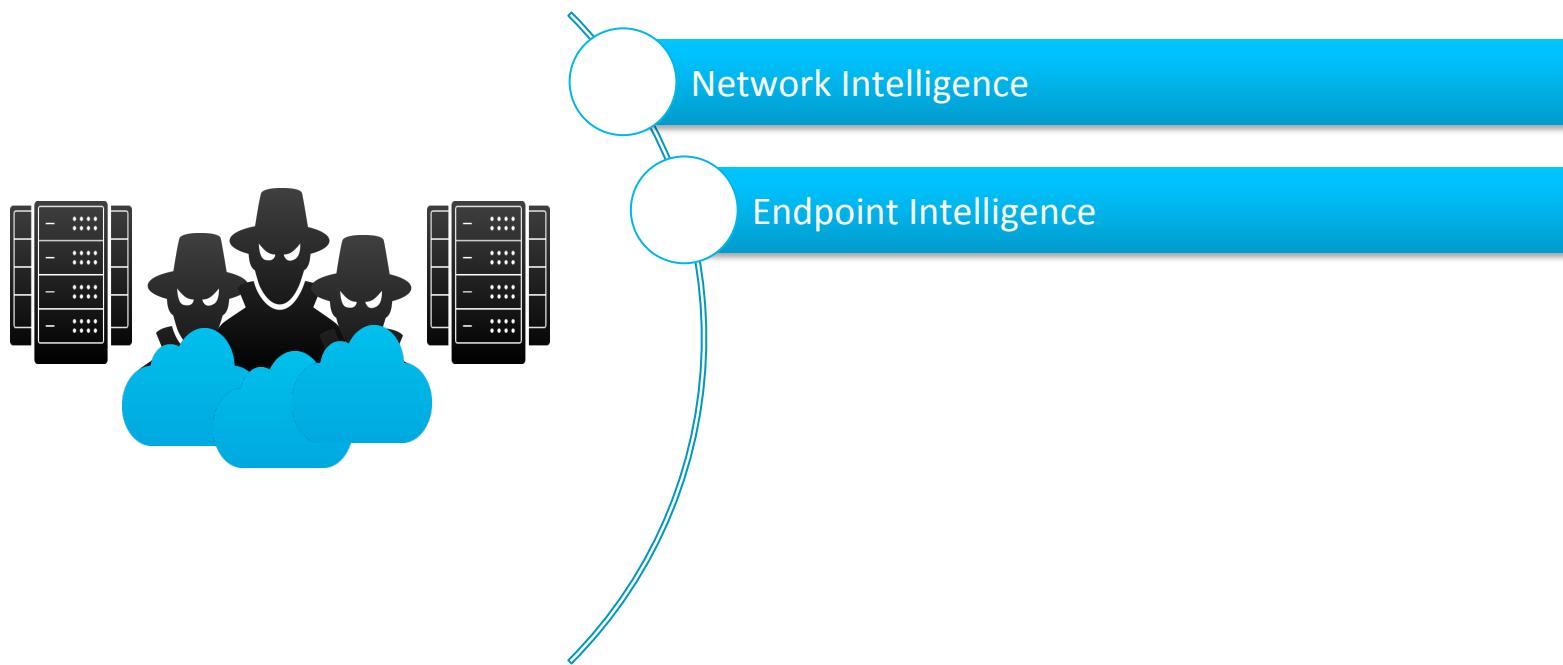
Track Attacker Infrastructure/Intelligence



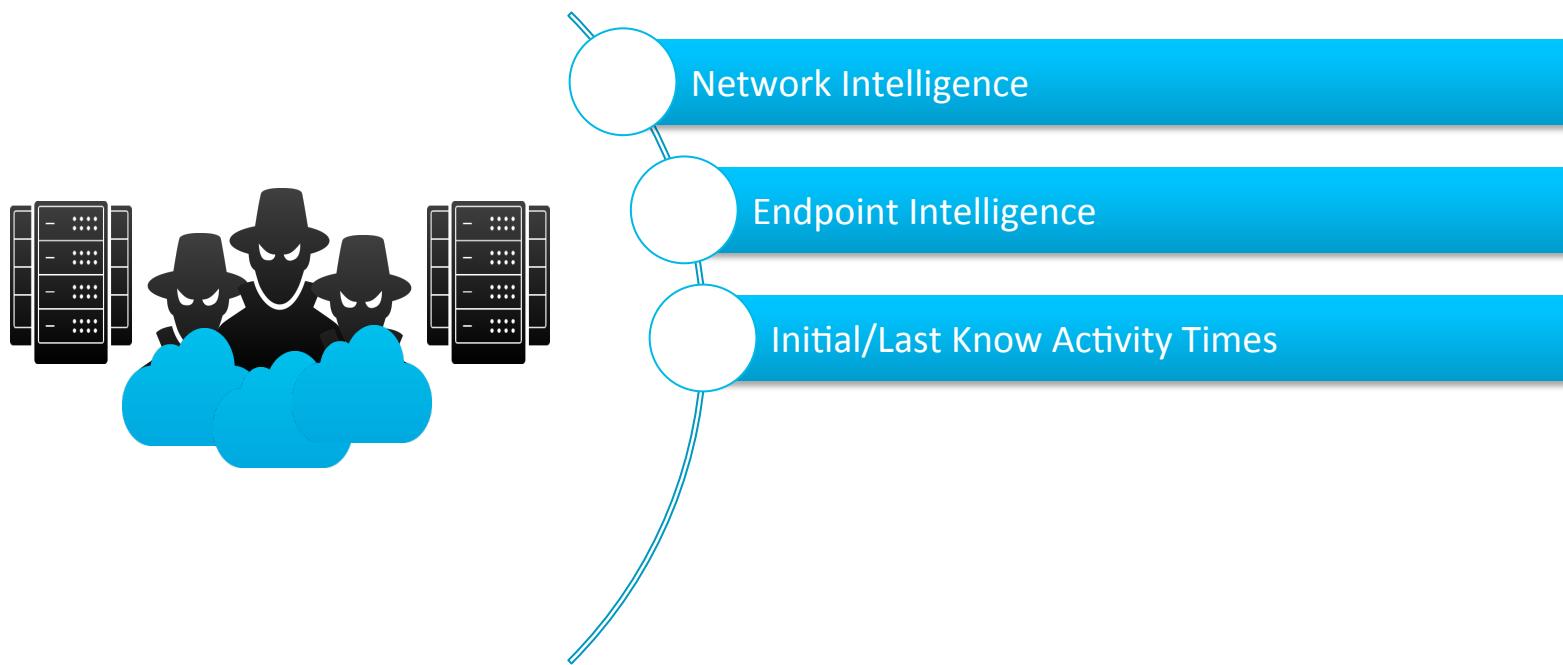
Track Attacker Infrastructure/Intelligence



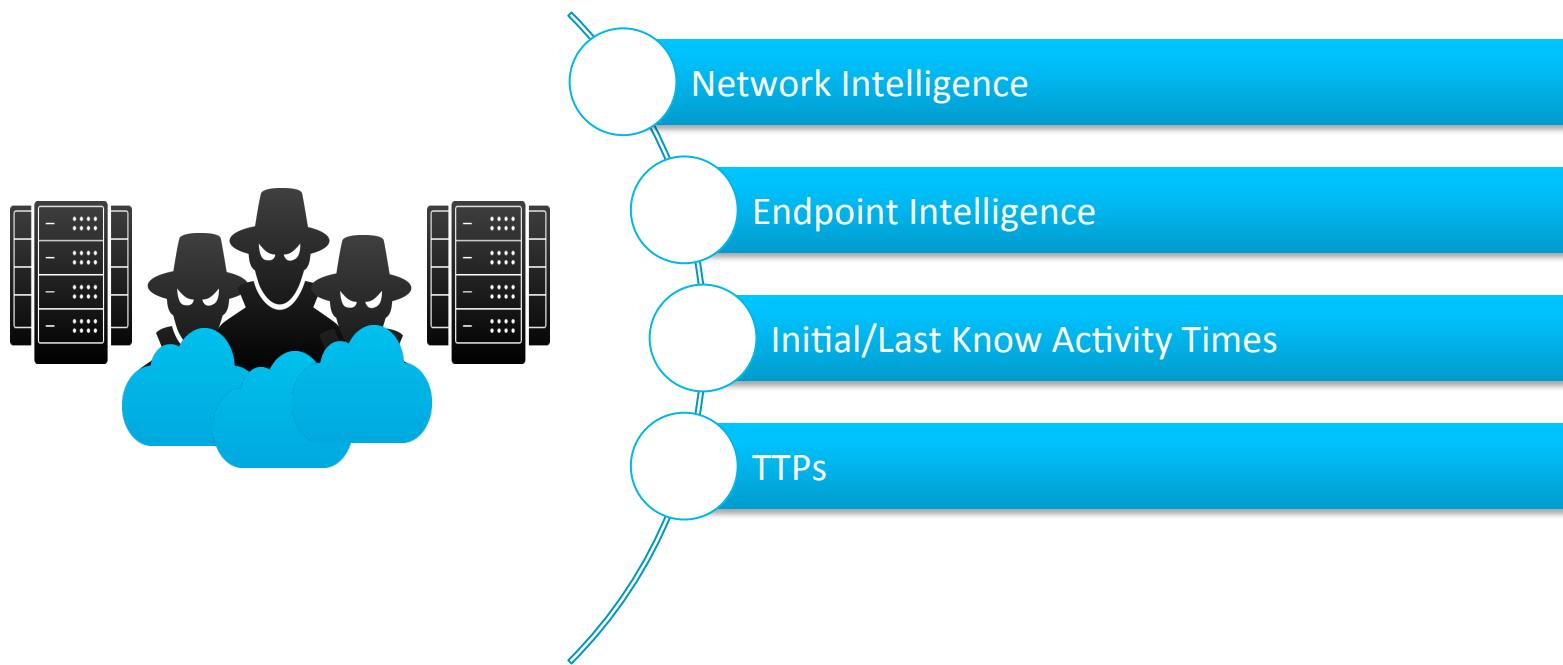
Track Attacker Infrastructure/Intelligence



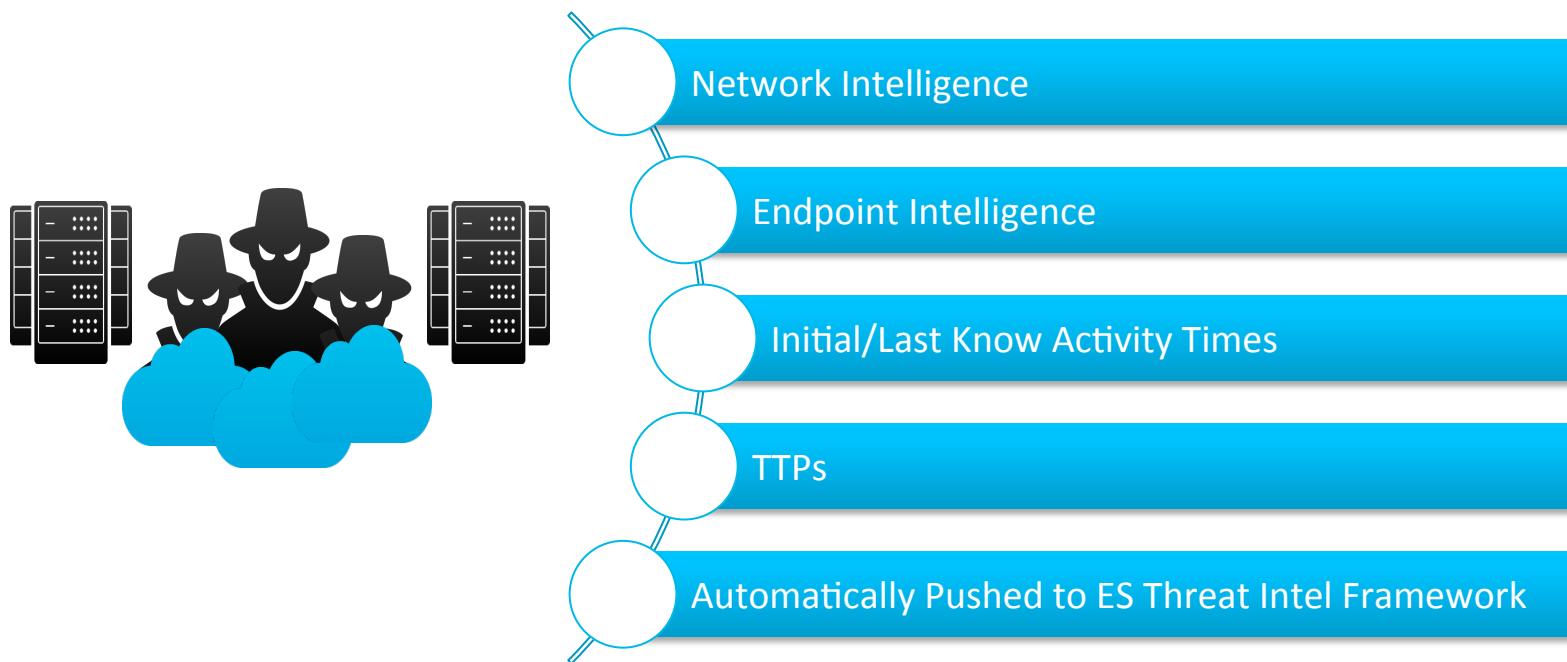
Track Attacker Infrastructure/Intelligence



Track Attacker Infrastructure/Intelligence



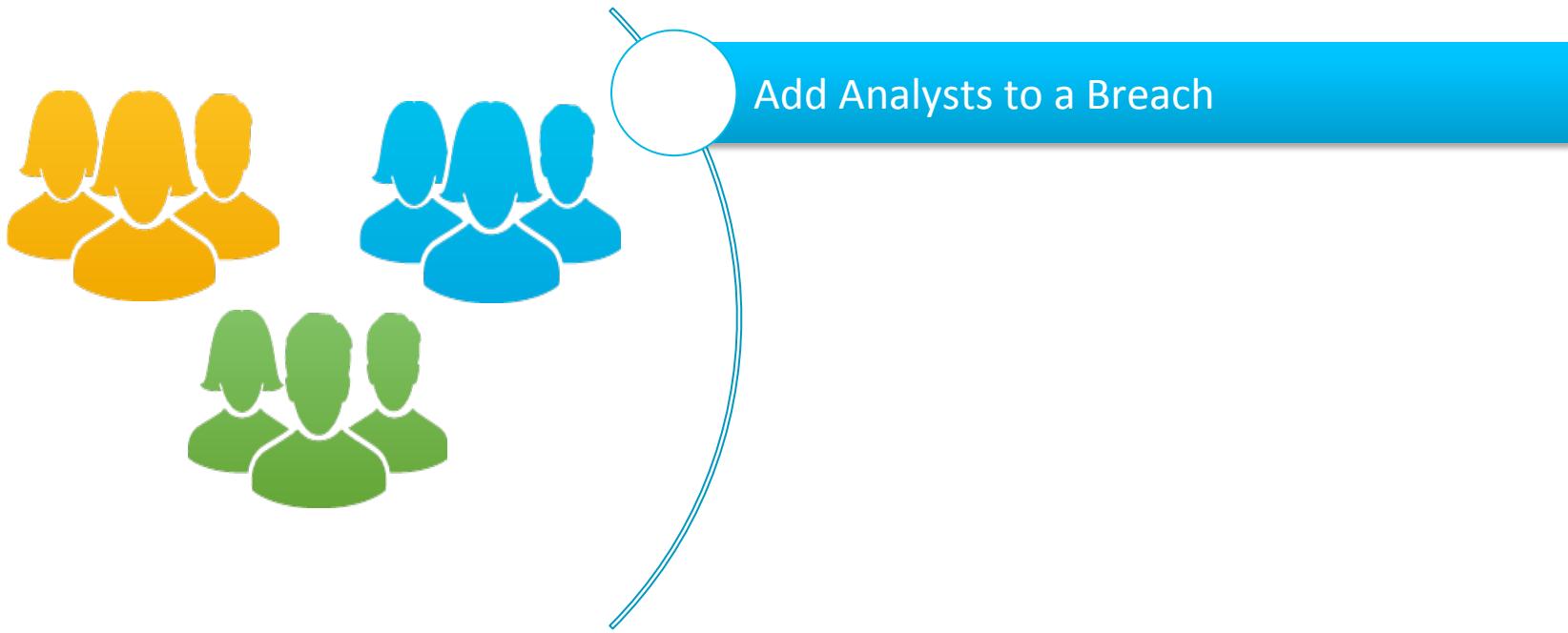
Track Attacker Infrastructure/Intelligence



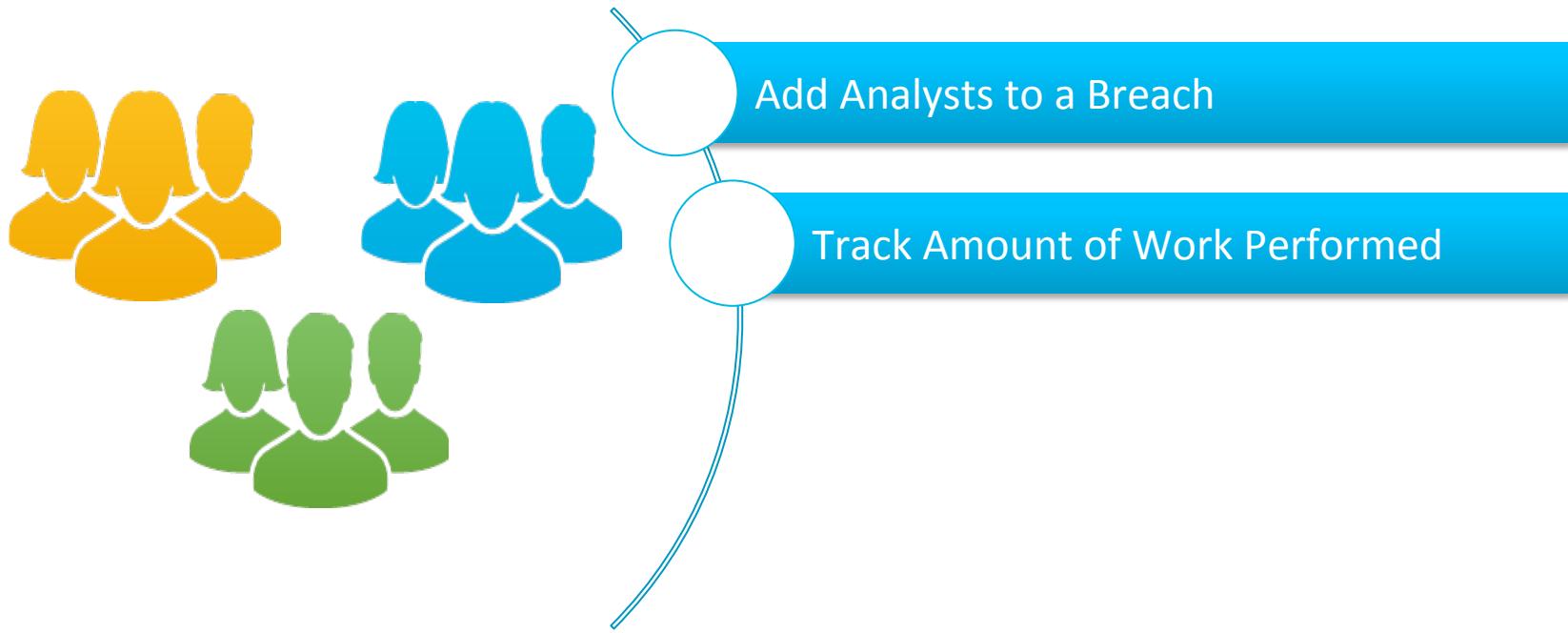
Analyst Assignment



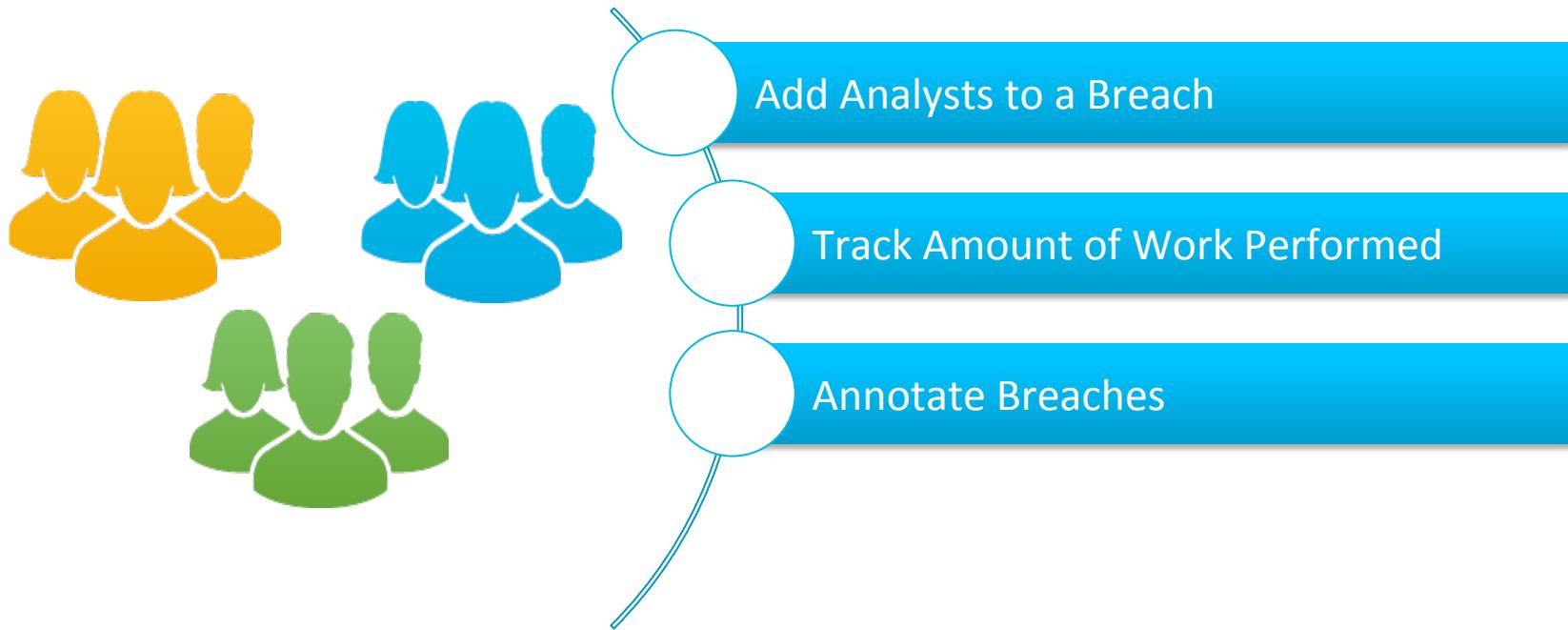
Analyst Assignment



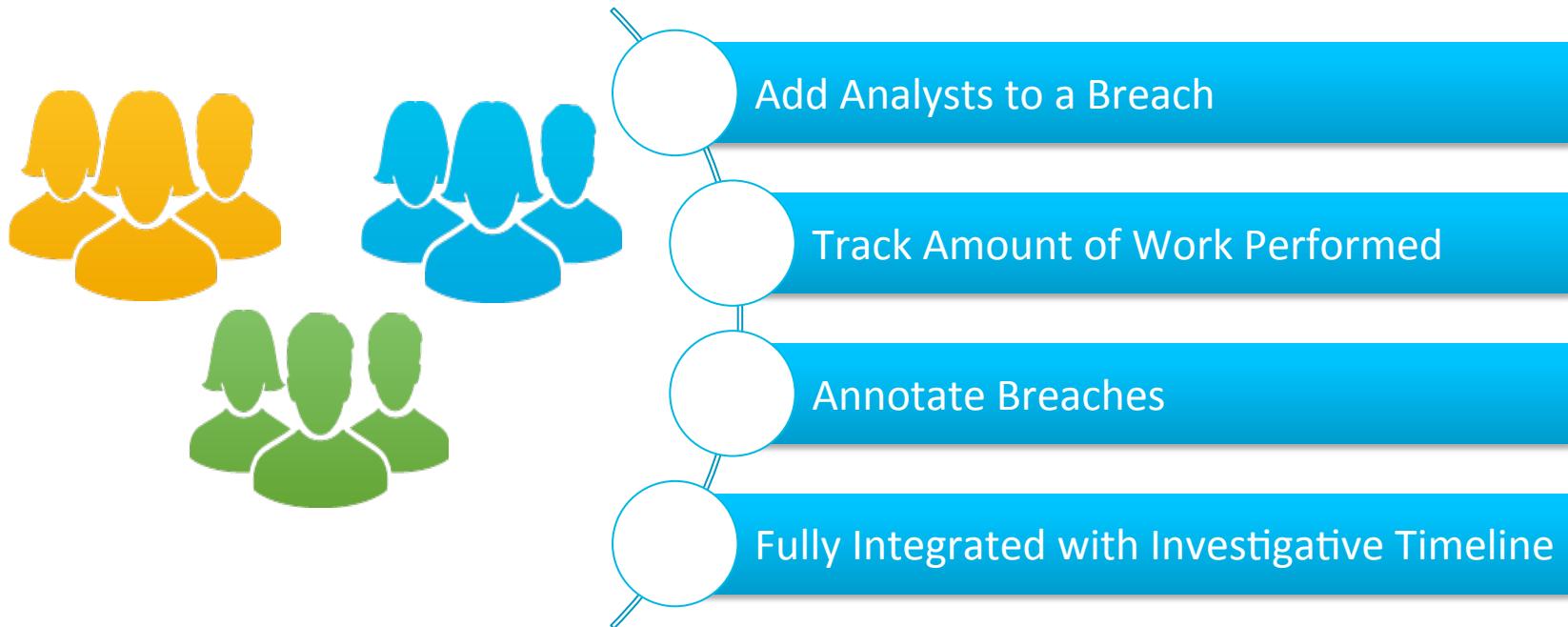
Analyst Assignment



Analyst Assignment



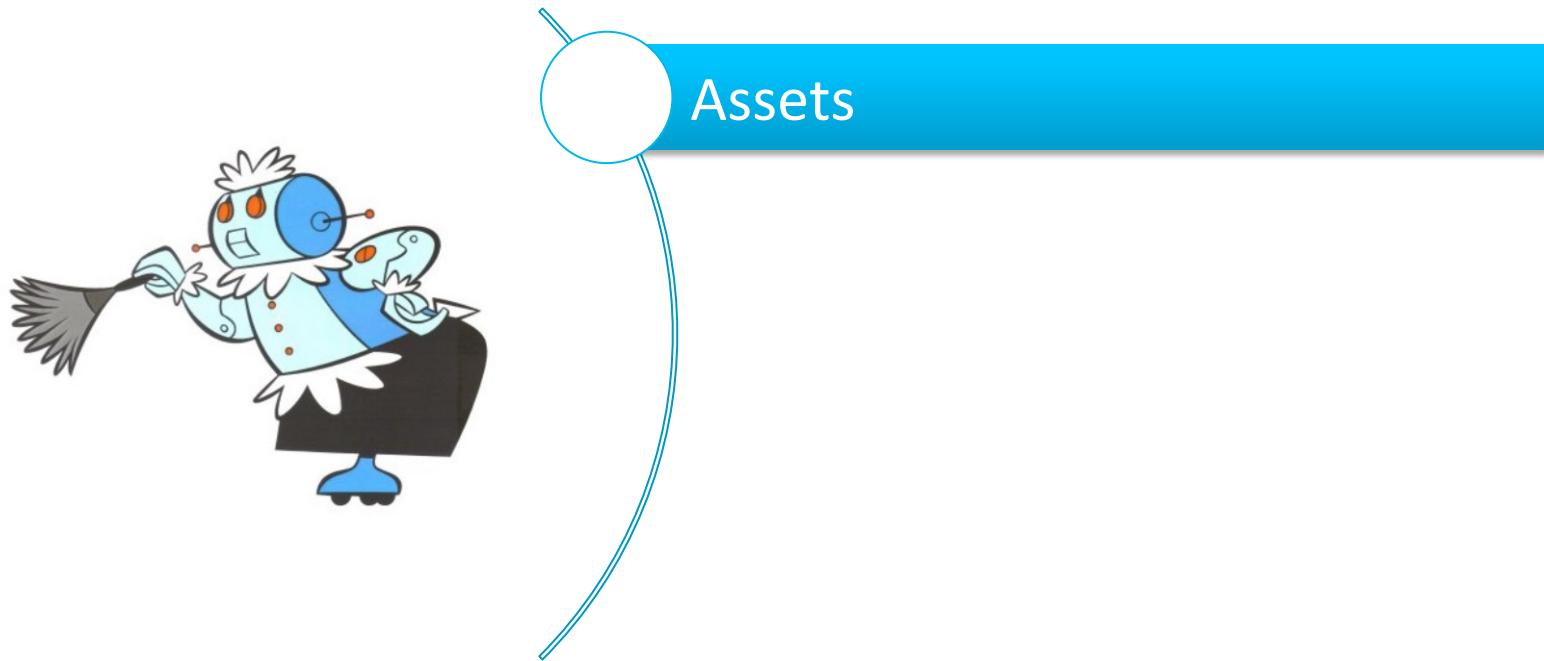
Analyst Assignment



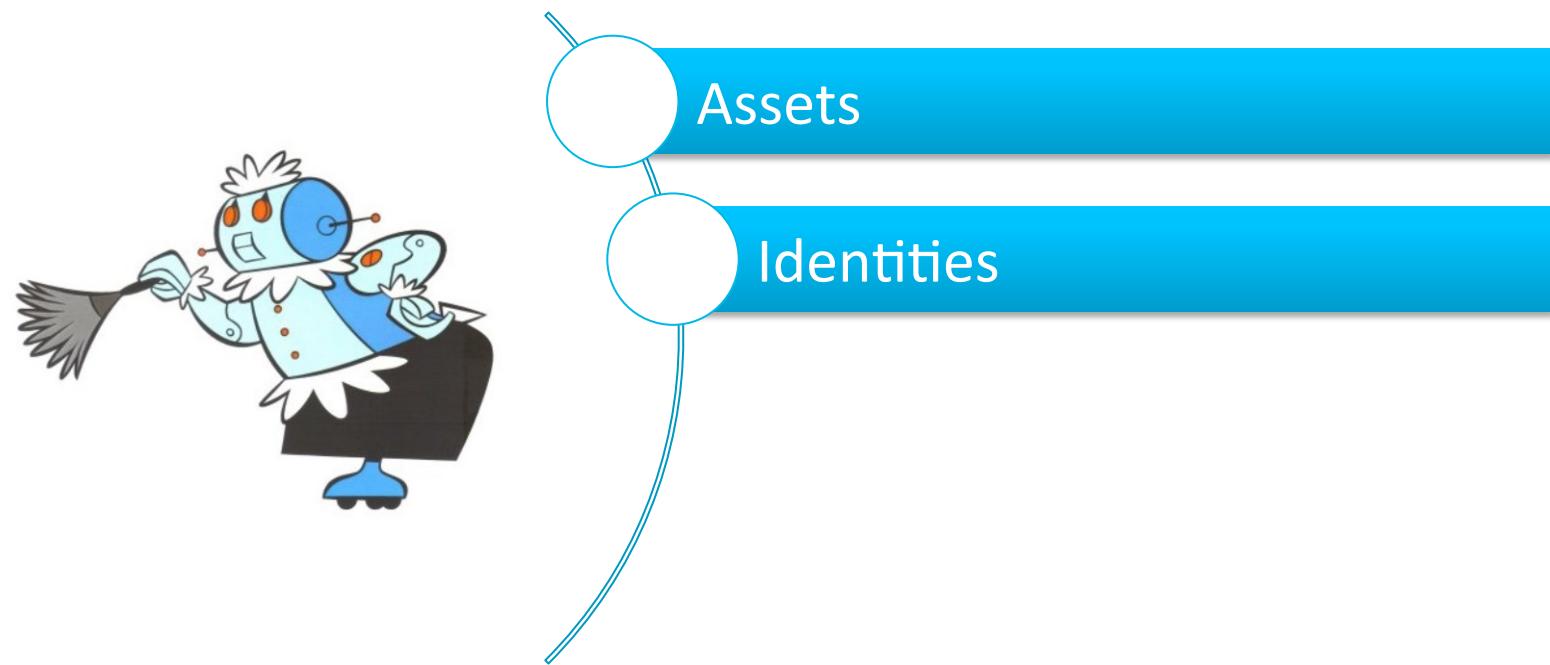
Track Remediation Progress



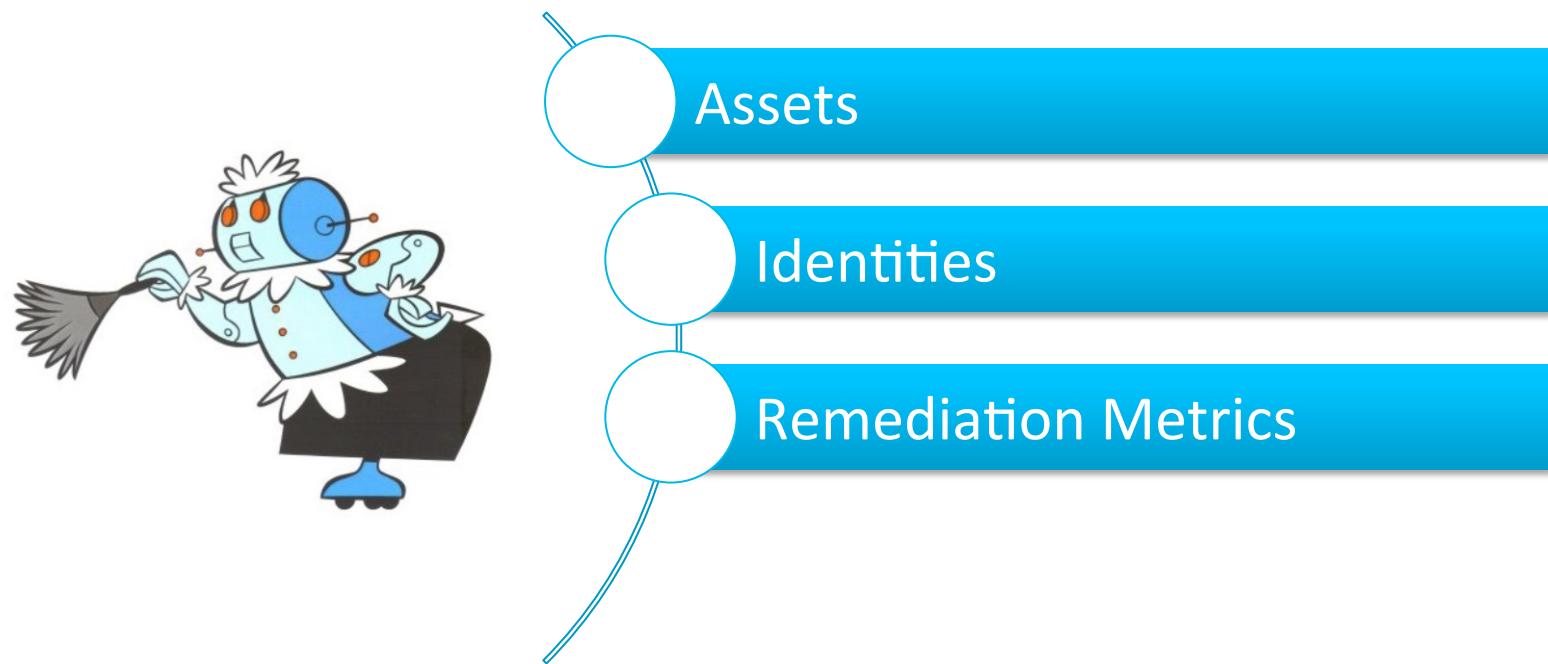
Track Remediation Progress



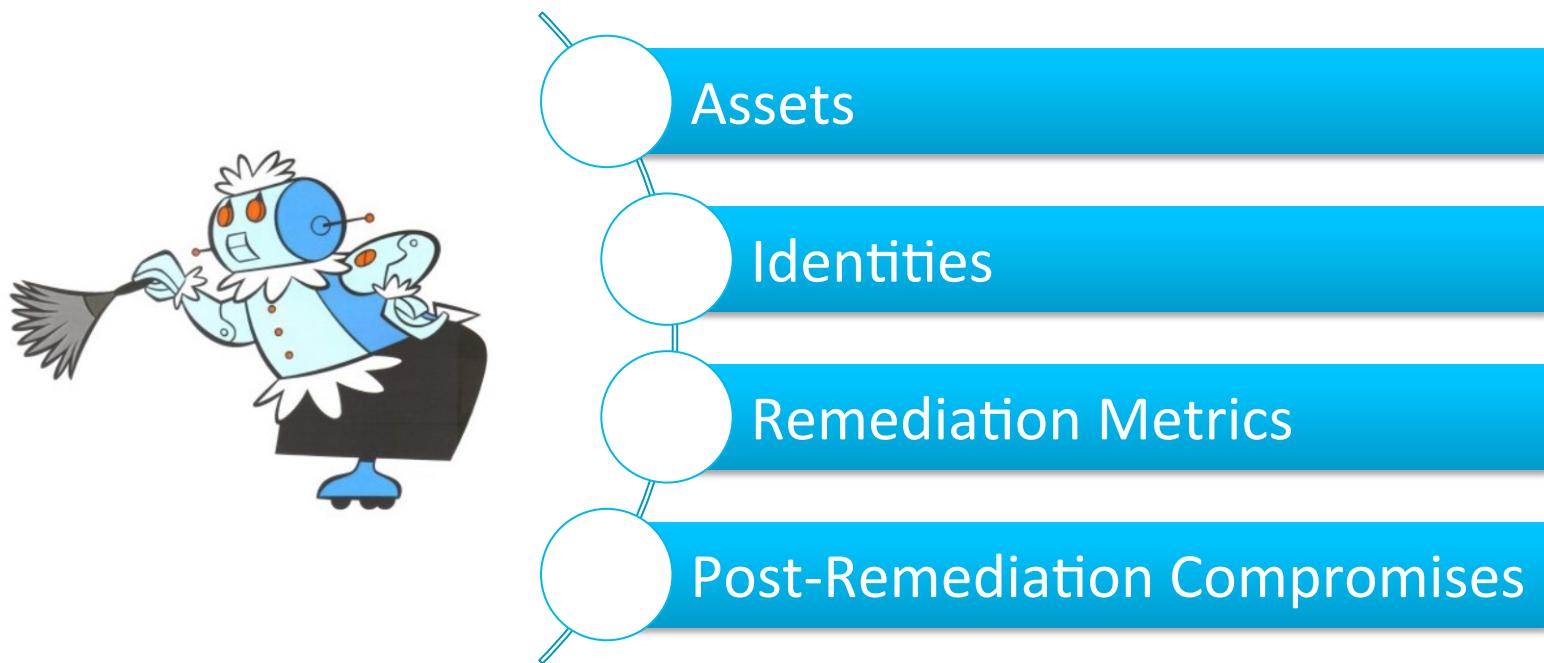
Track Remediation Progress



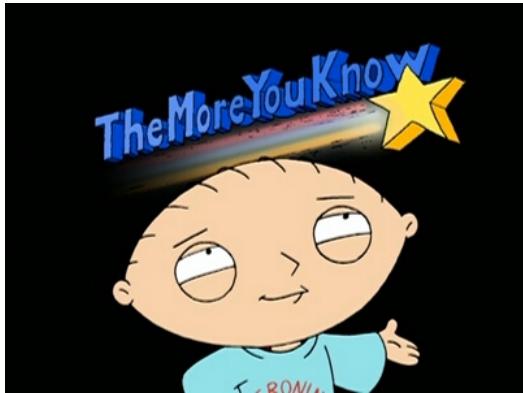
Track Remediation Progress



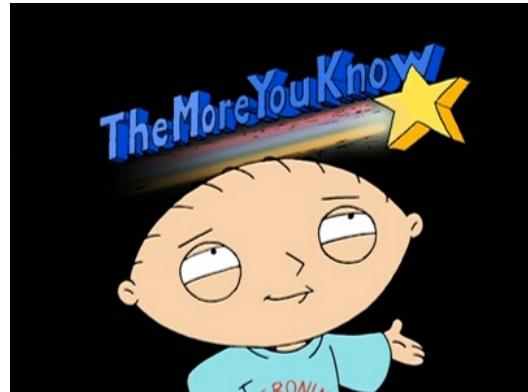
Track Remediation Progress



Takeaways

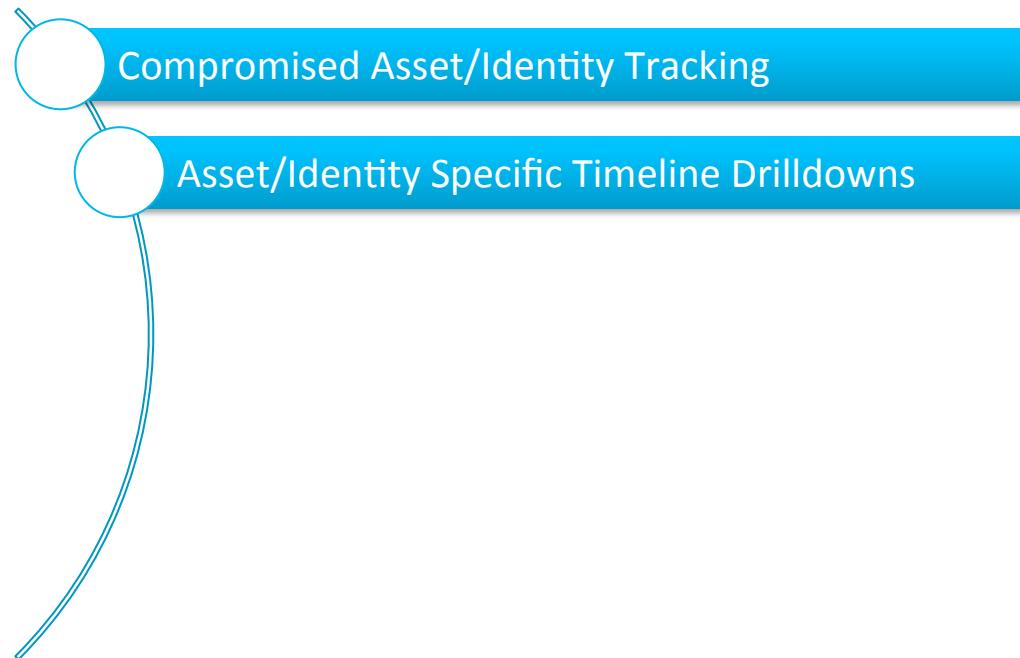
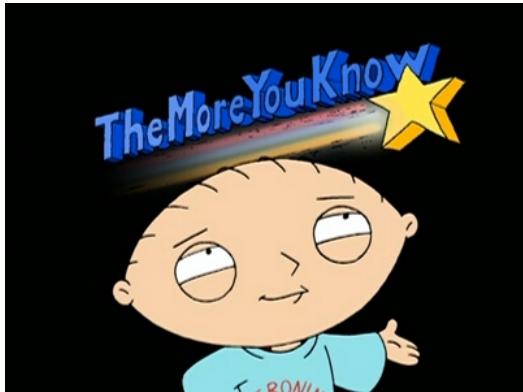


Takeaways

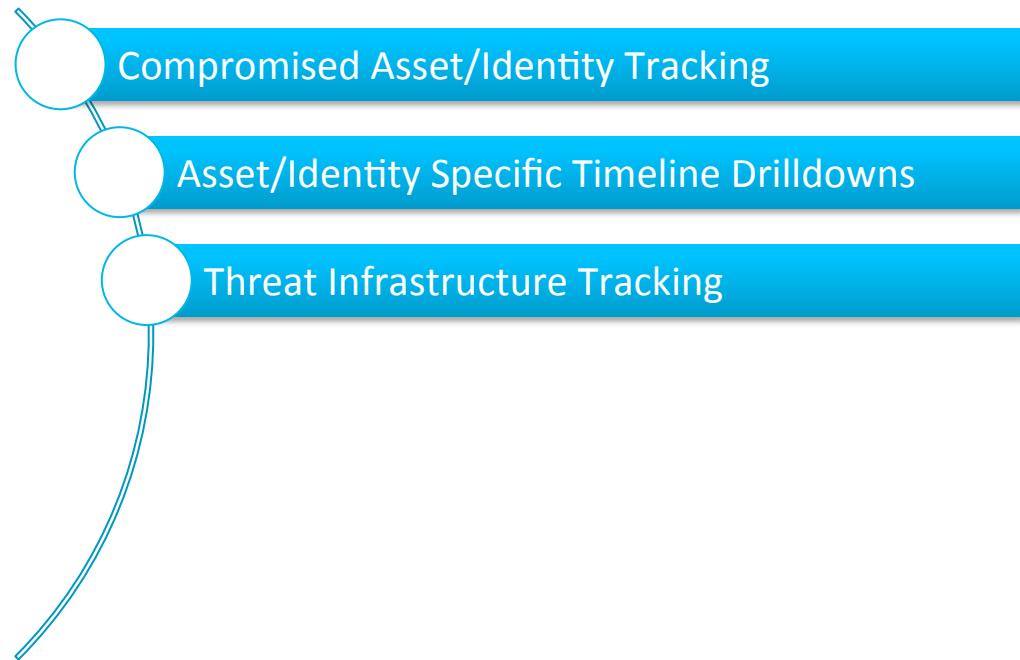
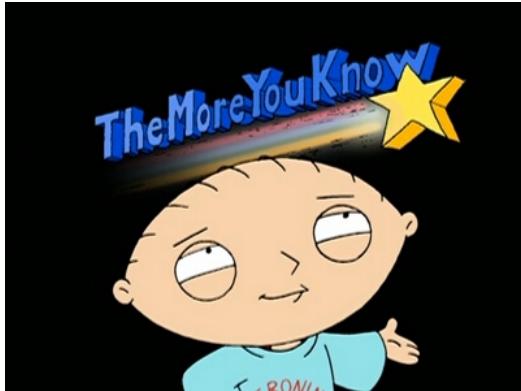


Compromised Asset/Identity Tracking

Takeaways



Takeaways

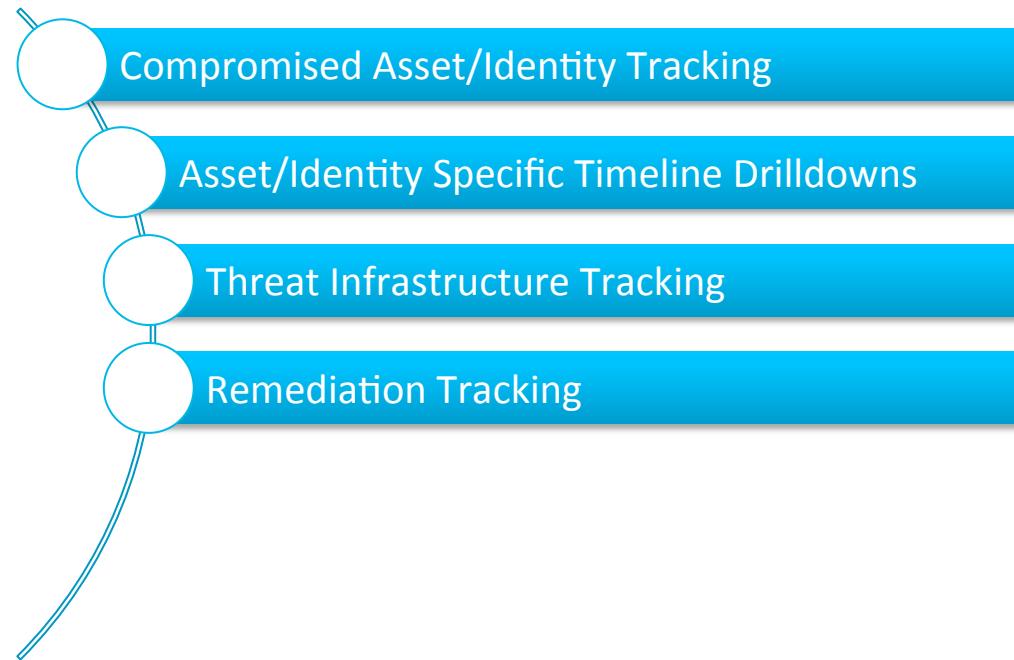
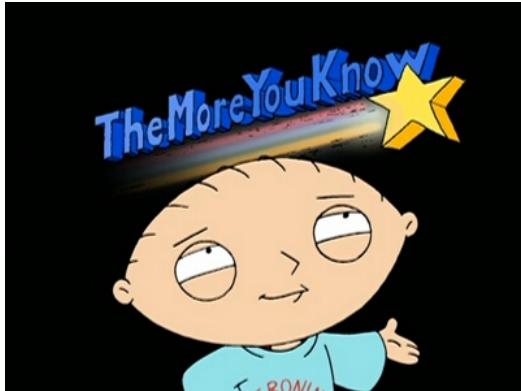


Compromised Asset/Identity Tracking

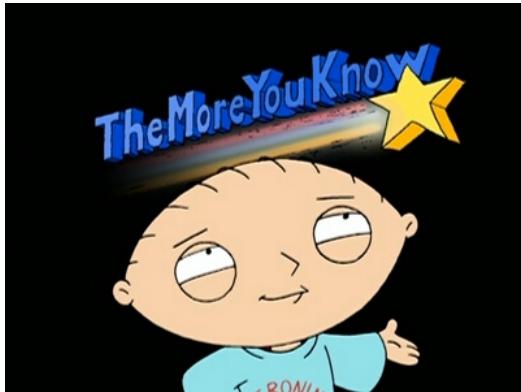
Asset/Identity Specific Timeline Drilldowns

Threat Infrastructure Tracking

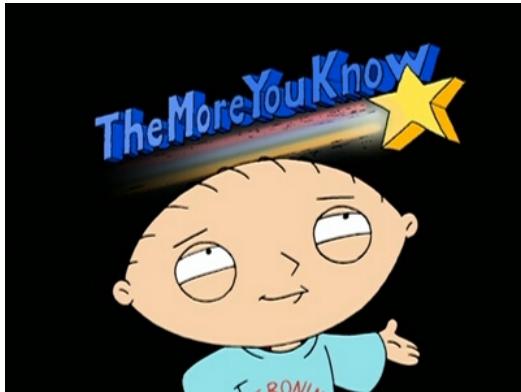
Takeaways



Takeaways



Takeaways



- Compromised Asset/Identity Tracking
- Asset/Identity Specific Timeline Drilldowns
- Threat Infrastructure Tracking
- Remediation Tracking
- One-Stop Breach Management Solution
- Complete Integration with Enterprise Security 4.0

Additional Information



@InTheorium

Splunk Blog: <http://blogs.splunk.com/author/bluger/>

Questions?

Preview ☺



.conf2015

2015



THANK YOU

splunk®