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 the 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?

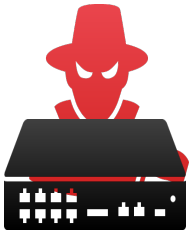
Well… What's a Breach?

Well… What's a Breach?

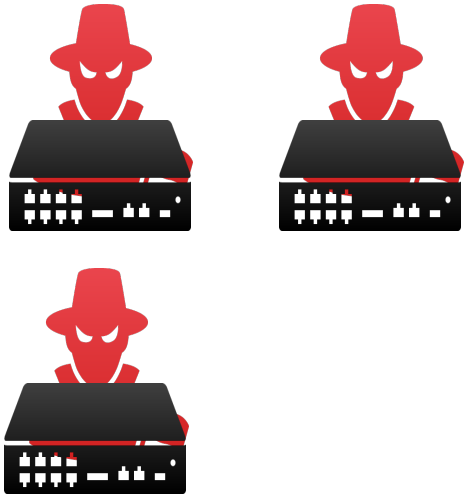
Having one or more assets compromised by a threat actor that has targeted the organization in an attempt carry out a specific intent.

Breach Management

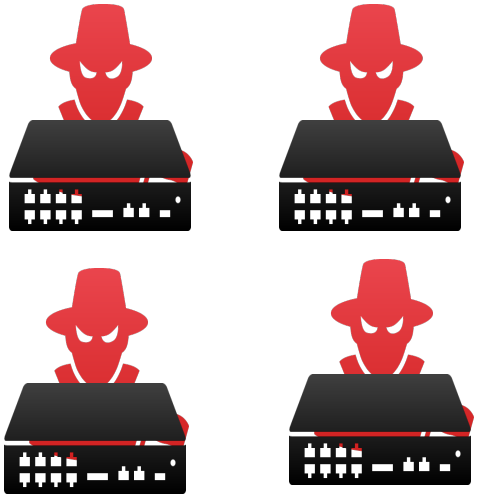
Breach Management



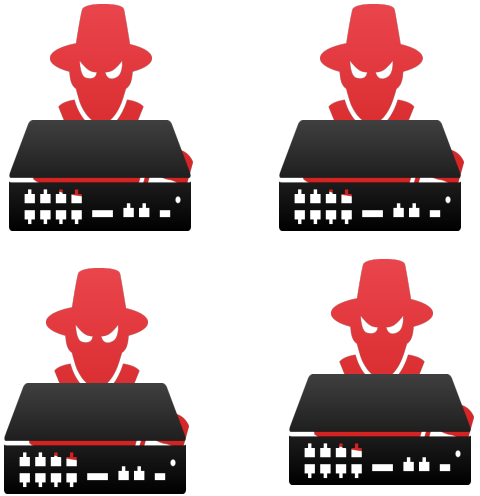
Breach Management

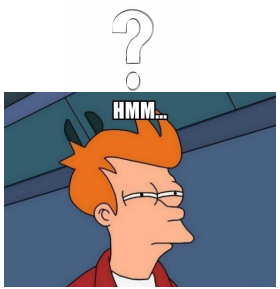


Breach Management

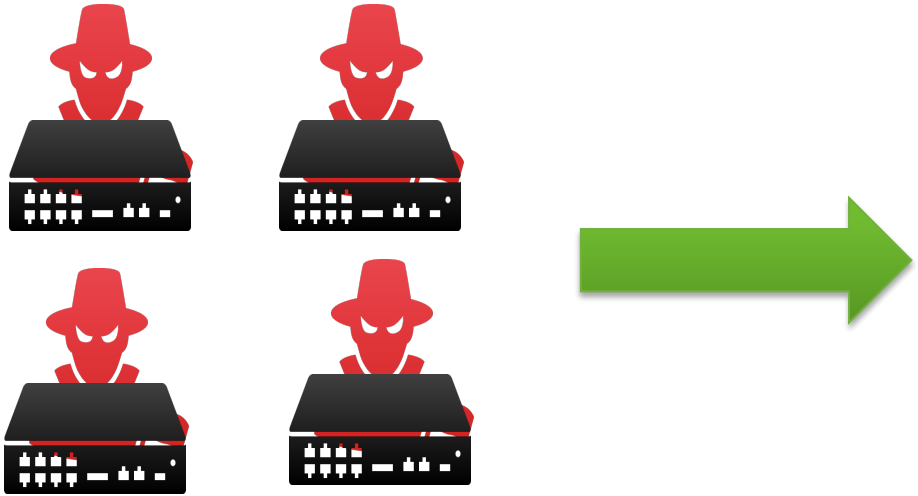


Breach Management

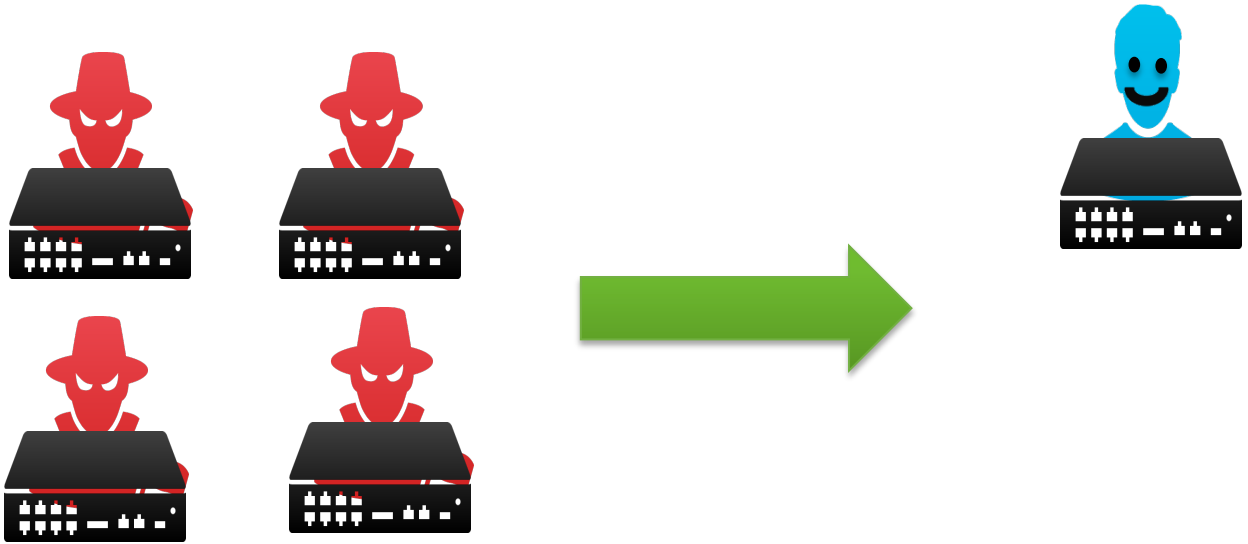




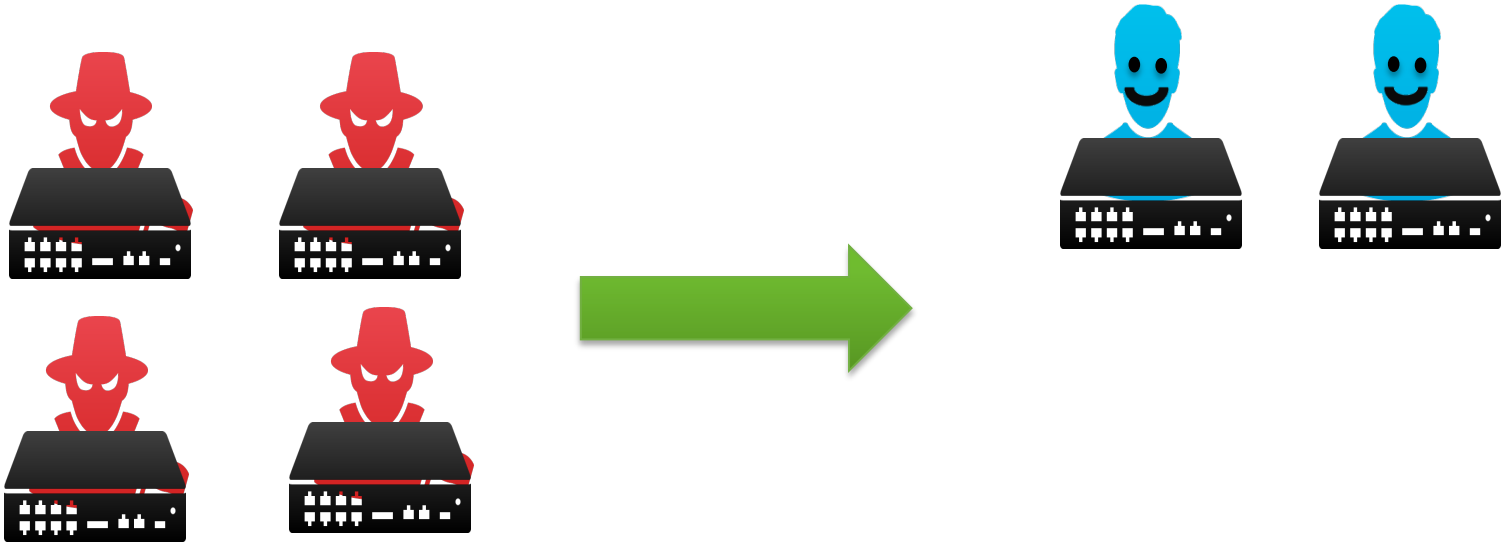
Breach Management



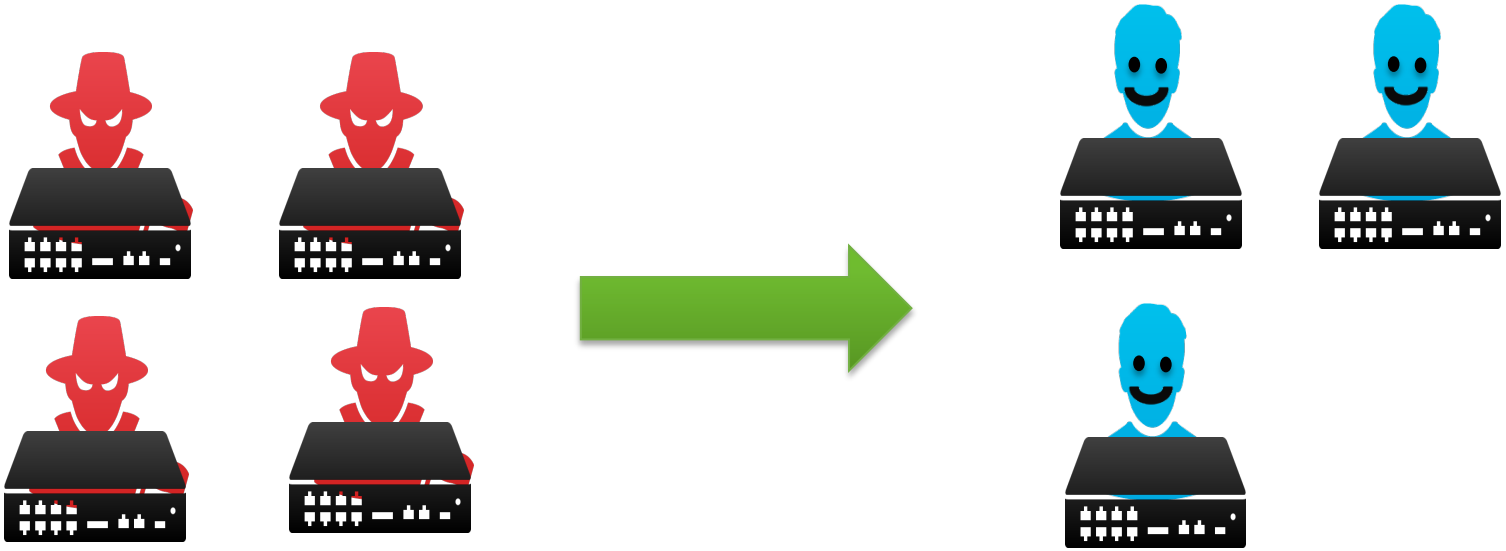
Breach Management



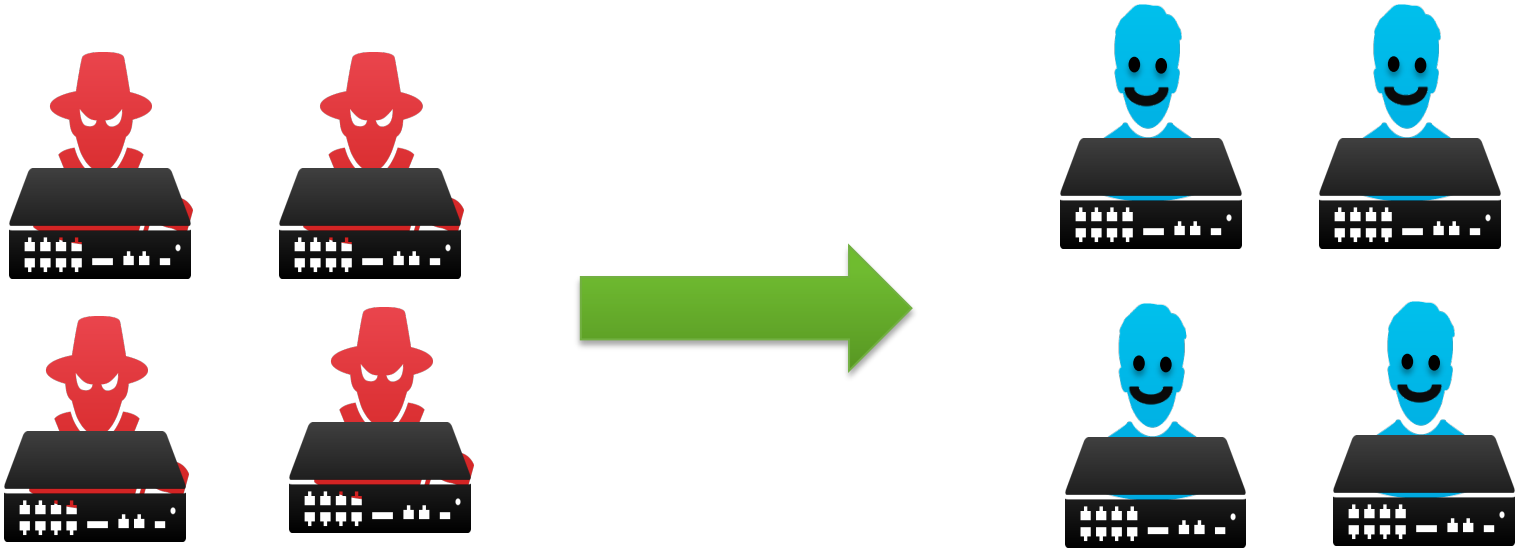
Breach Management



Breach Management



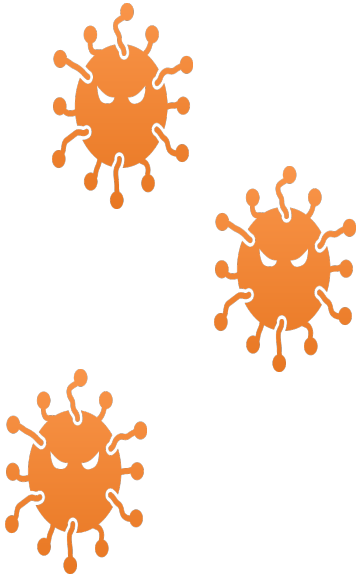
Breach Management



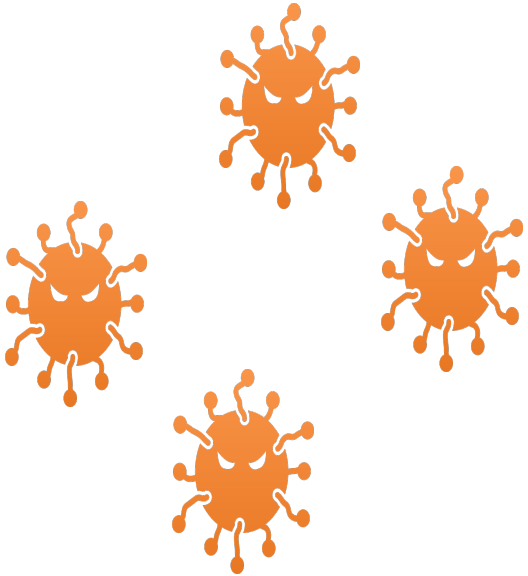
What Breach Management Is NOT

What Breach Management Is NOT

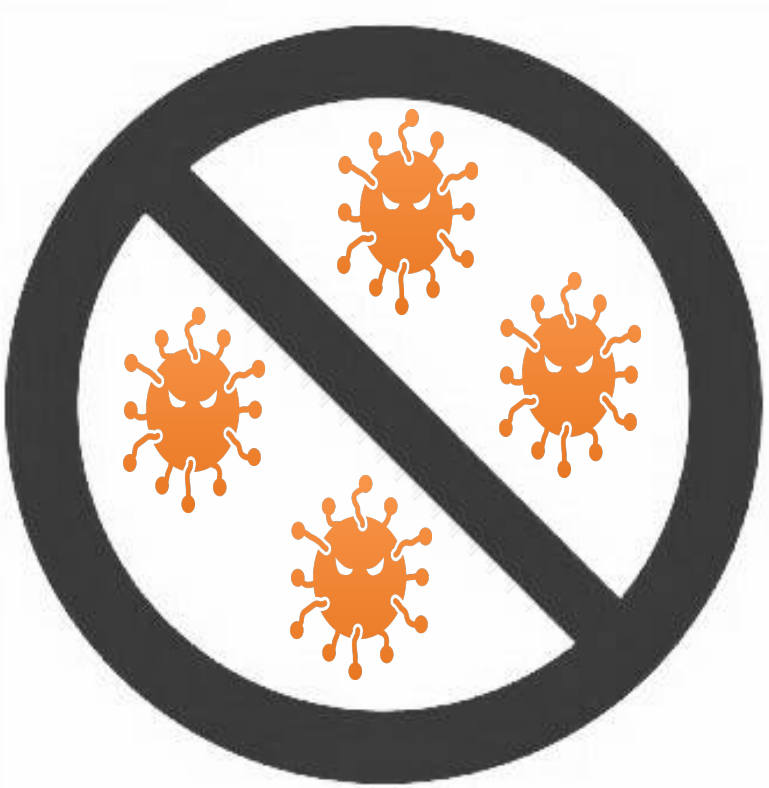
What Breach Management Is NOT



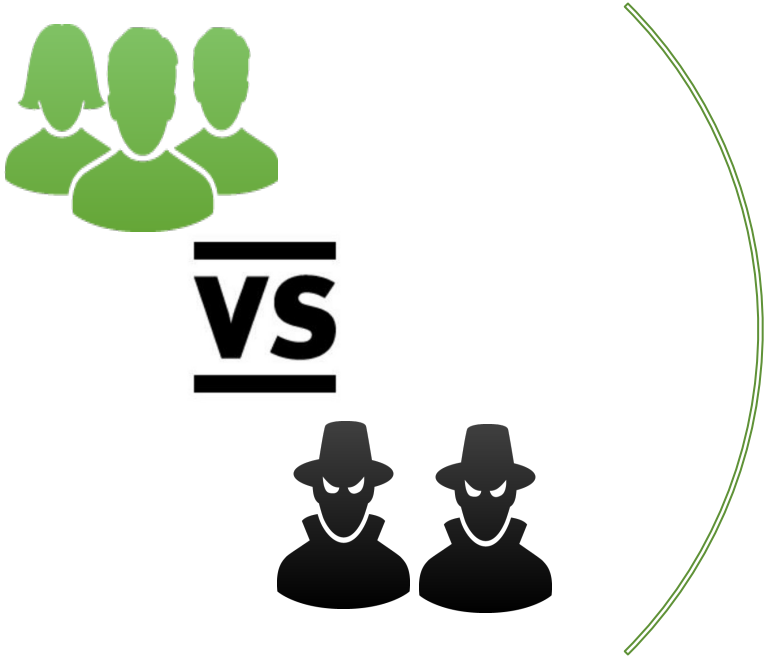
What Breach Management Is NOT



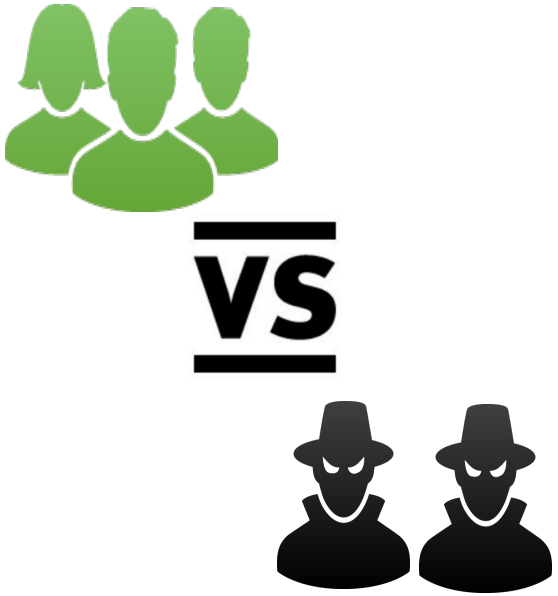
What Breach Management Is NOT



Breach Management can be Difficult

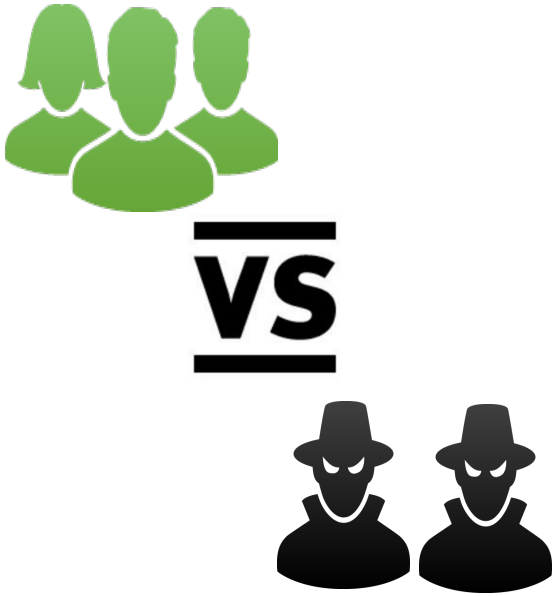


Breach Management can be Difficult



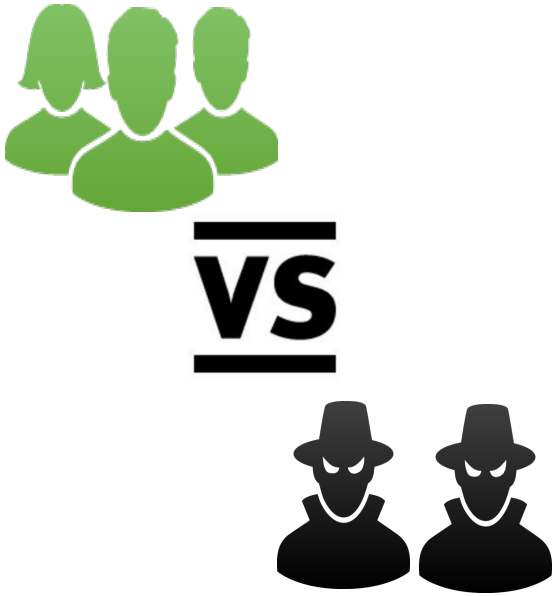
Compromised Assets

Breach Management can be Difficult



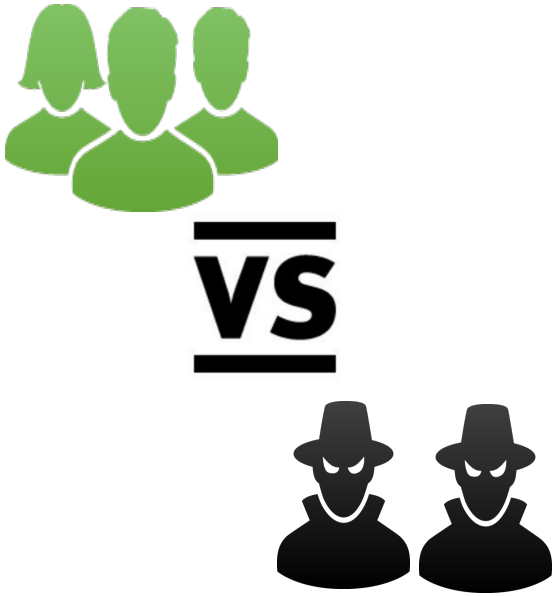
- Compromised Assets
- Compromised Identities

Breach Management can be Difficult



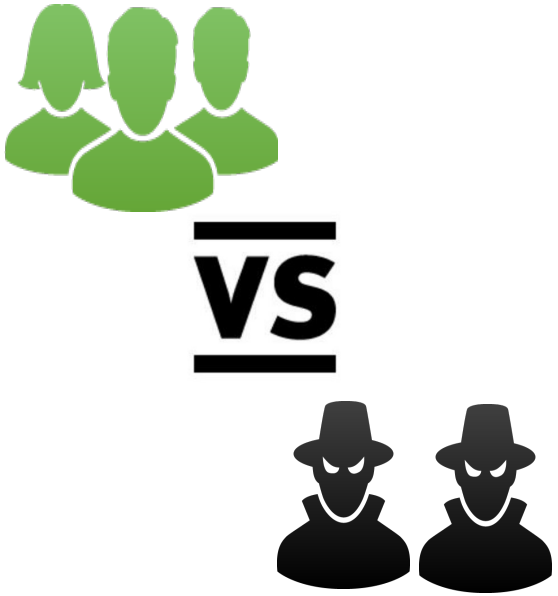
- Compromised Assets
- Compromised Identities
- Attacker Infrastructure/Intelligence

Breach Management can be Difficult



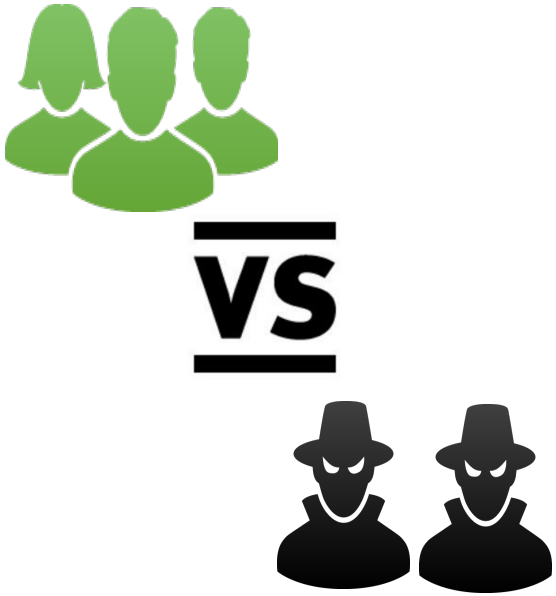
- Compromised Assets
- Compromised Identities
- Attacker Infrastructure/Intelligence
- Actions on Intent

Breach Management can be Difficult



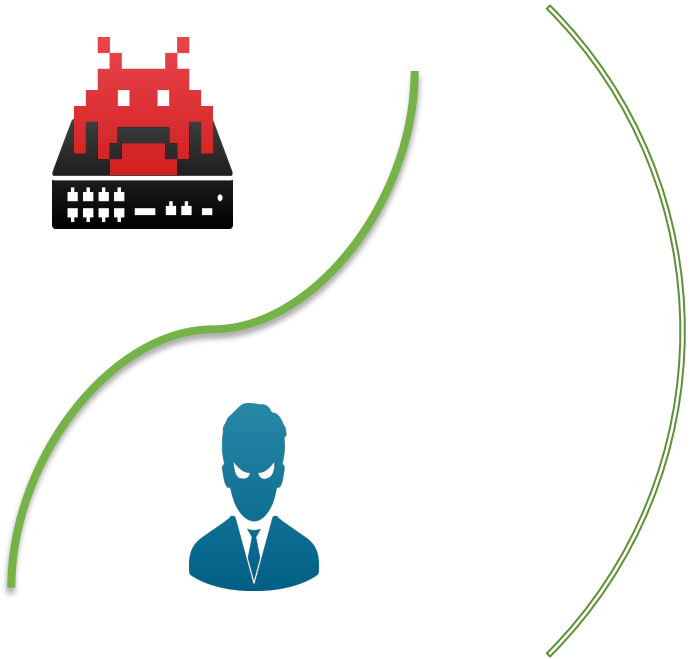
- Compromised Assets
- Compromised Identities
- Attacker Infrastructure/Intelligence
- Actions on Intent
- Remediation

Breach Management can be Difficult

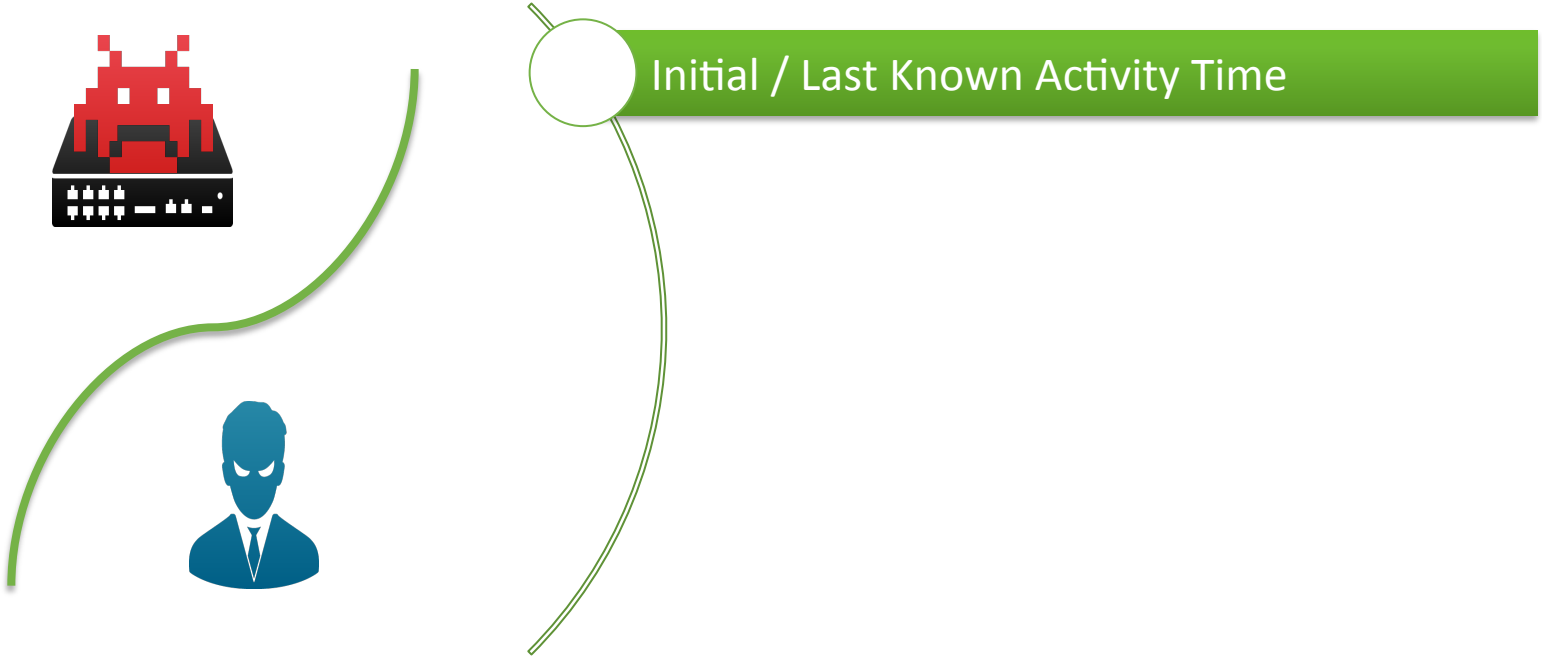


- Compromised Assets
- Compromised Identities
- Attacker Infrastructure/Intelligence
- Actions on Intent
- Remediation
- Post-Remediation

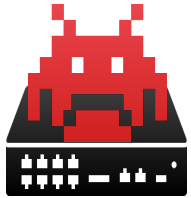
Compromised Assets & Identities



Compromised Assets & Identities

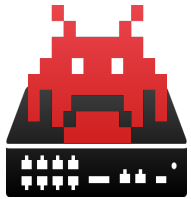


Compromised Assets & Identities



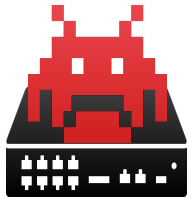
- Initial / Last Known Activity Time
- Domains / Hostnames / IPs / Location

Compromised Assets & Identities



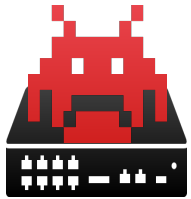
- Initial / Last Known Activity Time
- Domains / Hostnames / IPs / Location
- Malware / PUPs / Tools / TTPs

Compromised Assets & Identities



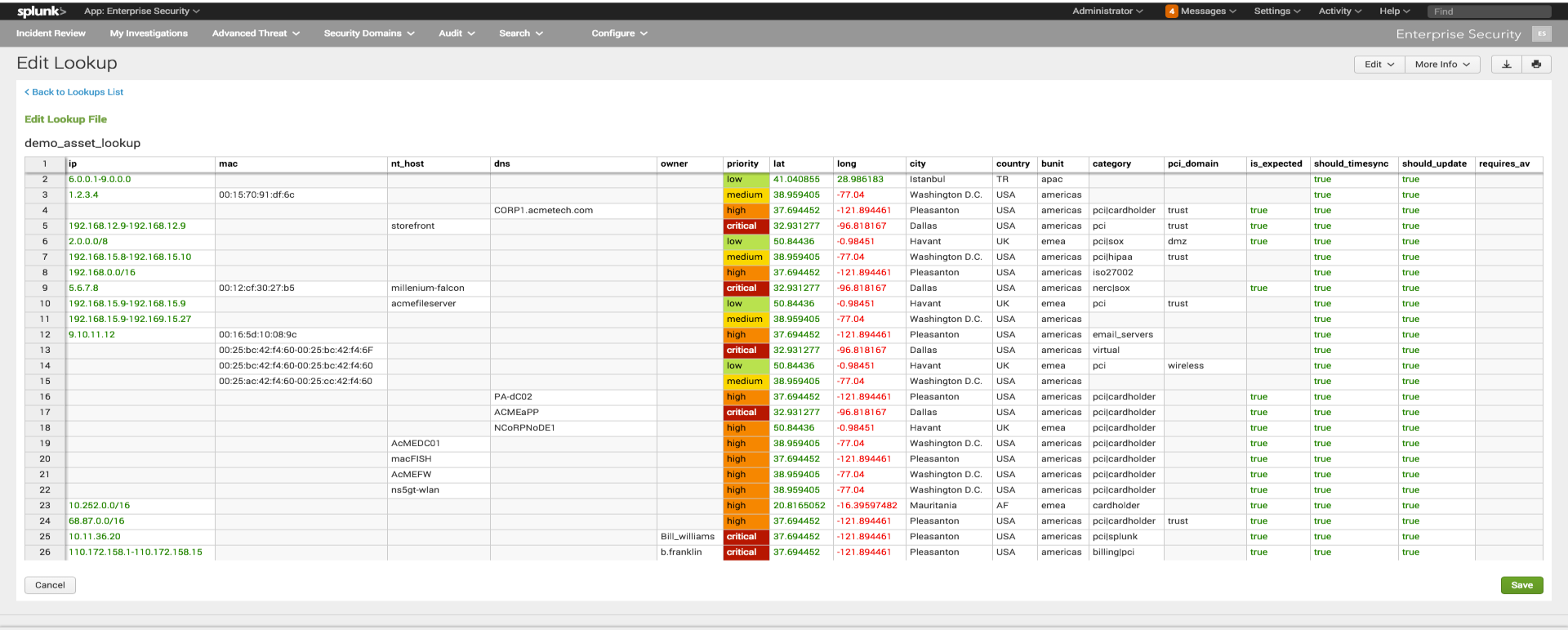
- Initial / Last Known Activity Time
- Domains / Hostnames / IPs / Location
- Malware / PUPs / Tools / TTPs
- Usernames / Domains / Emails / Location

Compromised Assets & Identities



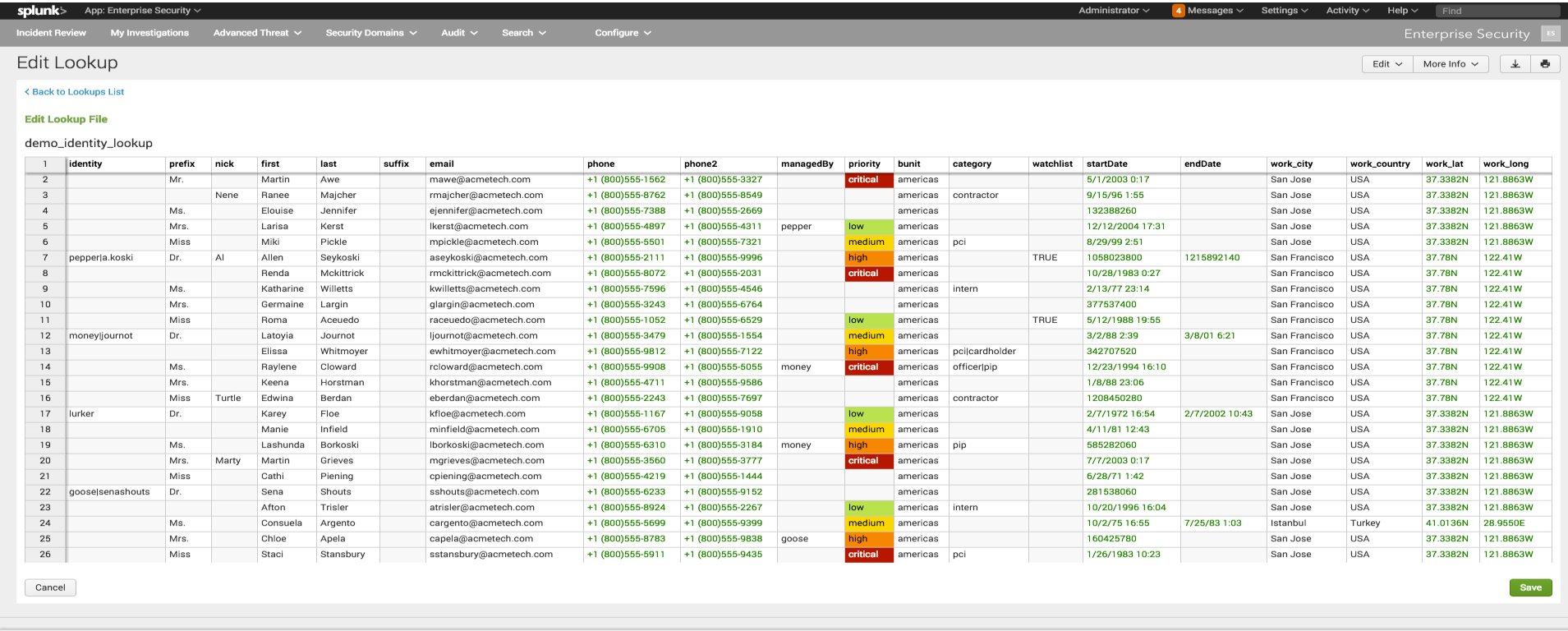
- Initial / Last Known Activity Time
- Domains / Hostnames / IPs / Location
- Malware / PUPs / Tools / TTPs
- Usernames / Domains / Emails / Location
- Analyst Notes

ES Assets & Identities Framework



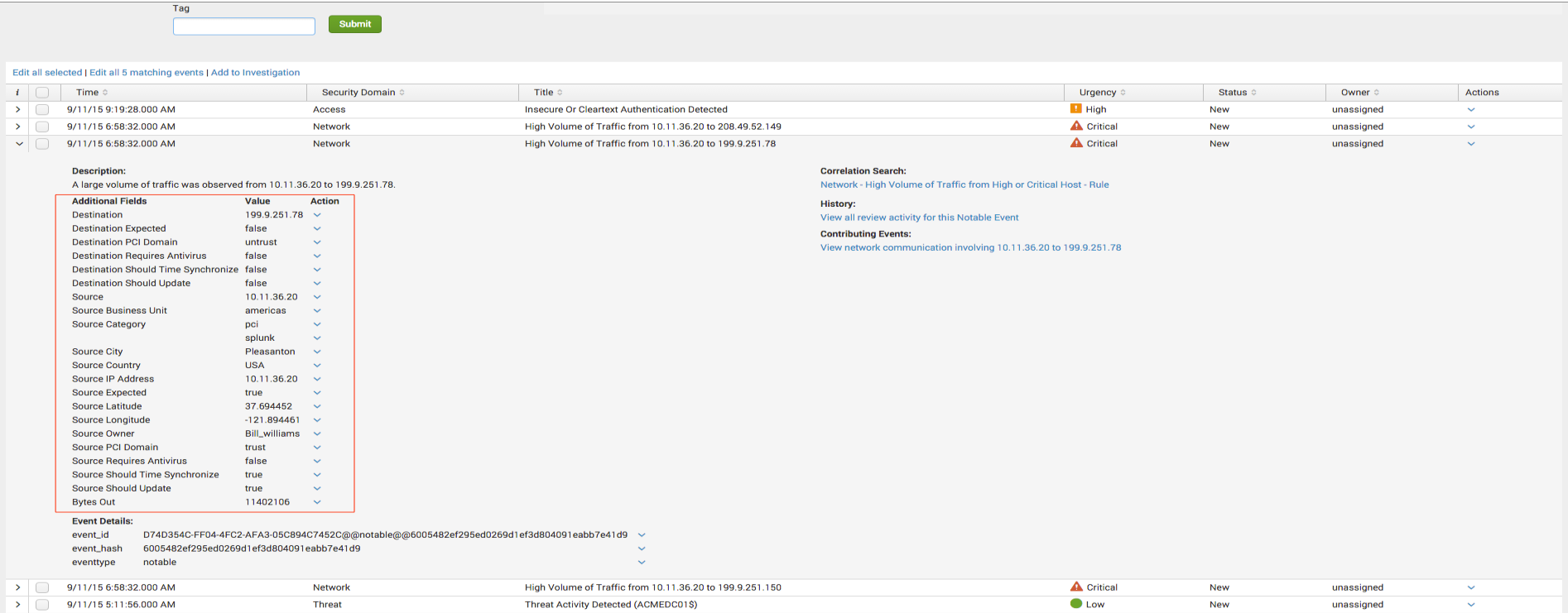
1	ip	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	category	pci_domain	is_expected	should_timesync	should_update	requires_av
2	6.0.0.1-9.0.0.0					low	41.040855	28.986183	Istanbul	TR	apac				true	true	
3	1.2.3.4	00:15:70:91:df:6c				medium	38.959405	-77.04	Washington D.C.	USA	americas				true	true	
4				CORP1.acmetech.com		high	37.694452	-121.894461	Pleasanton	USA	americas	pci|cardholder	trust	true	true	true	
5	192.168.12.9-192.168.12.9		storefront			critical	32.931277	-96.818167	Dallas	USA	americas	pci	trust	true	true	true	
6	2.0.0.0/8					low	50.84436	-0.98451	Havant	UK	emea	pci|sox	dmz	true	true	true	
7	192.168.15.8-192.168.15.10					medium	38.959405	-77.04	Washington D.C.	USA	americas	pci|hipaa	trust		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	nerc|sox		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	pci|cardholder		true	true	true	
17				ACMEaPP		critical	32.931277	-96.818167	Dallas	USA	americas	pci|cardholder		true	true	true	
18				NCoRPNoDE1		high	50.84436	-0.98451	Havant	UK	emea	pci|cardholder		true	true	true	
19			AcMEDC01			high	38.959405	-77.04	Washington D.C.	USA	americas	pci|cardholder		true	true	true	
20			macFISH			high	37.694452	-121.894461	Pleasanton	USA	americas	pci|cardholder		true	true	true	
21			AcMEFW			high	38.959405	-77.04	Washington D.C.	USA	americas	pci|cardholder		true	true	true	
22			ns5gt-wlan			high	38.959405	-77.04	Washington D.C.	USA	americas	pci|cardholder		true	true	true	
23	10.252.0.0/16					high	20.8165052	-16.39597482	Mauritania	AF	emea	cardholder		true	true	true	
24	68.87.0.0/16					high	37.694452	-121.894461	Pleasanton	USA	americas	pci|cardholder	trust	true	true	true	
25	10.11.36.20				Bill_williams	critical	37.694452	-121.894461	Pleasanton	USA	americas	pci|splunk		true	true	true	
26	110.172.158.1-110.172.158.15				b.franklin	critical	37.694452	-121.894461	Pleasanton	USA	americas	billing|pci		true	true	true	

ES Assets & Identities Framework



	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.		Martin	Awe		mawe@acmetech.com	+1 (800)555-1562	+1 (800)555-3327		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			132388260		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	pepper|a.koski	Dr.	Al	Allen	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	Willetts		kwilletts@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	Aceuedo		raceuedo@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	money|journot	Dr.		Latoyia	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	pci|cardholder		342707520		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	goose|senashouts	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		cargento@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

ES Assets & Identities Framework



Attacker Infrastructure & Intelligence

Attacker Infrastructure & Intelligence

Command & Control (C2) Servers

Attacker Infrastructure & Intelligence

- Command & Control (C2) Servers
- Hop Points

Attacker Infrastructure & Intelligence

- Command & Control (C2) Servers
- Hop Points
- Domains

Attacker Infrastructure & Intelligence

- Command & Control (C2) Servers
- Hop Points
- Domains
- Watering Holes

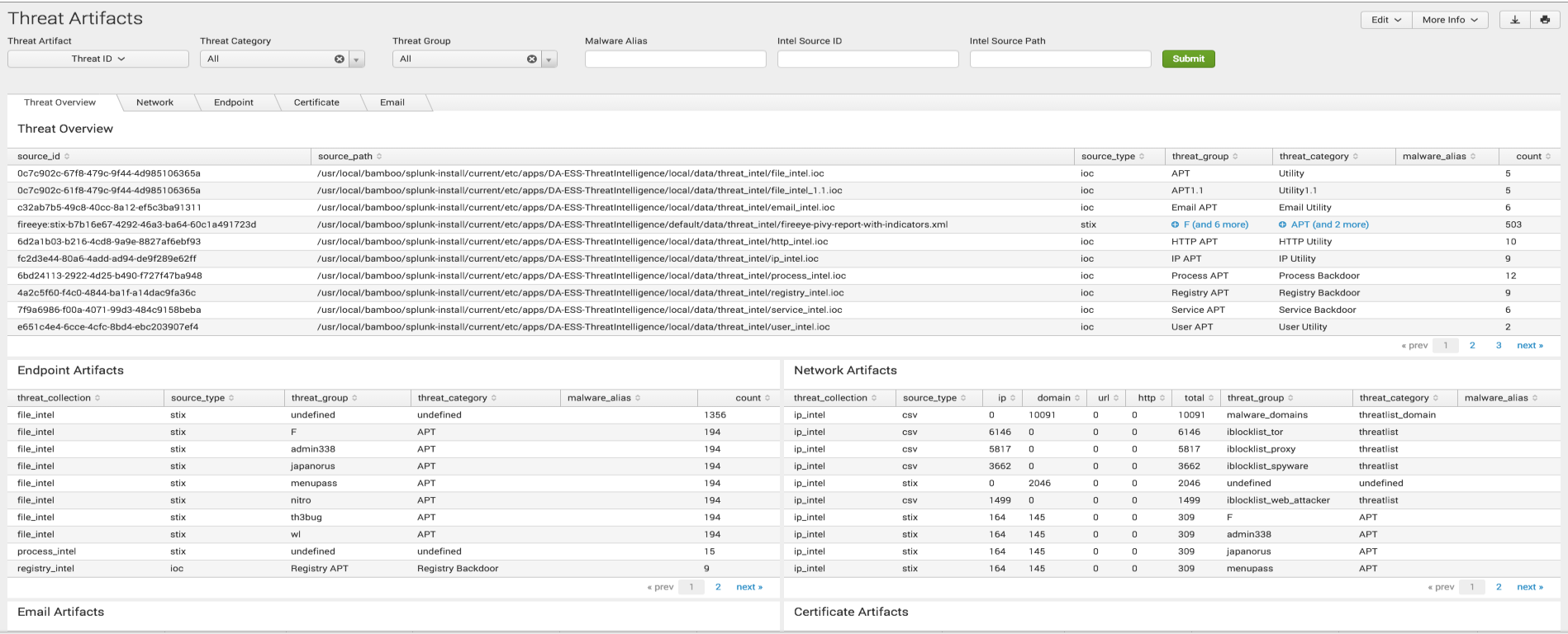
Attacker Infrastructure & Intelligence

- Command & Control (C2) Servers
- Hop Points
- Domains
- Watering Holes
- Exploit Kits / Phishing Sites

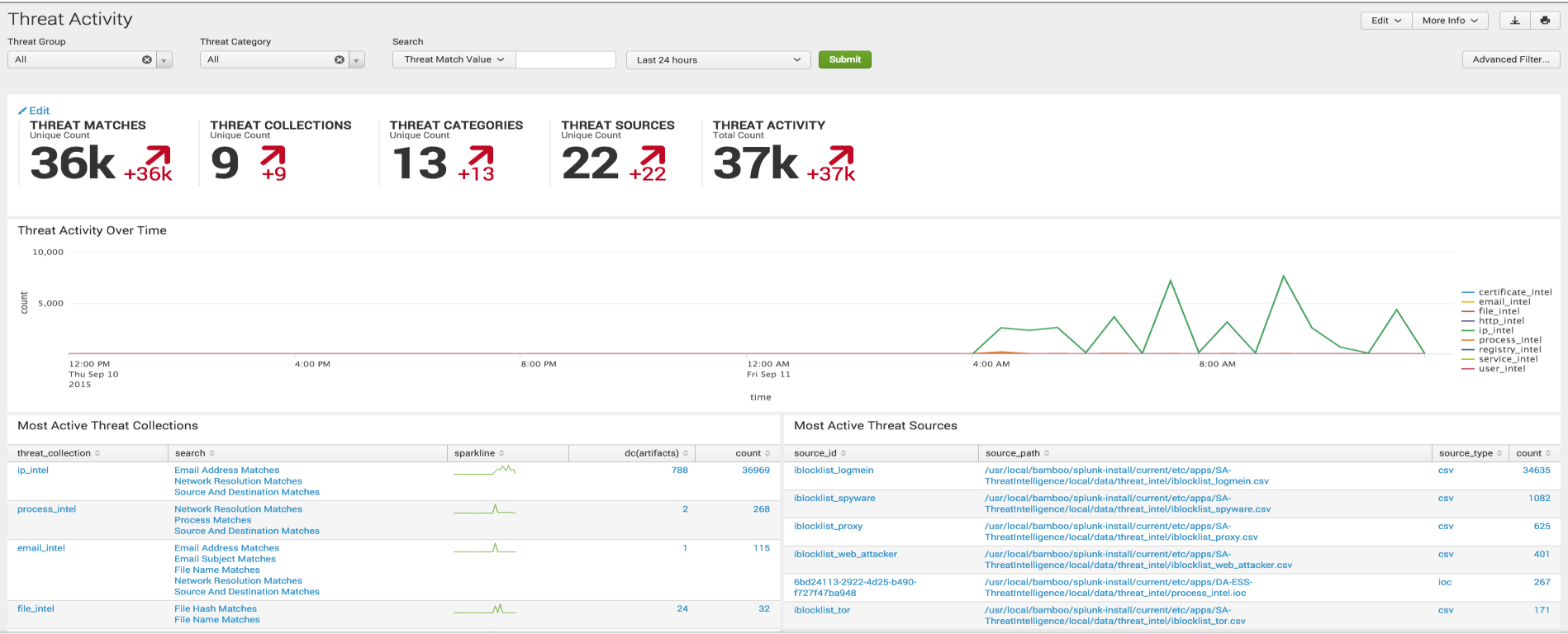
Attacker Infrastructure & Intelligence

- Command & Control (C2) Servers
- Hop Points
- Domains
- Watering Holes
- Exploit Kits / Phishing Sites
- Endpoint Intelligence & TTPs

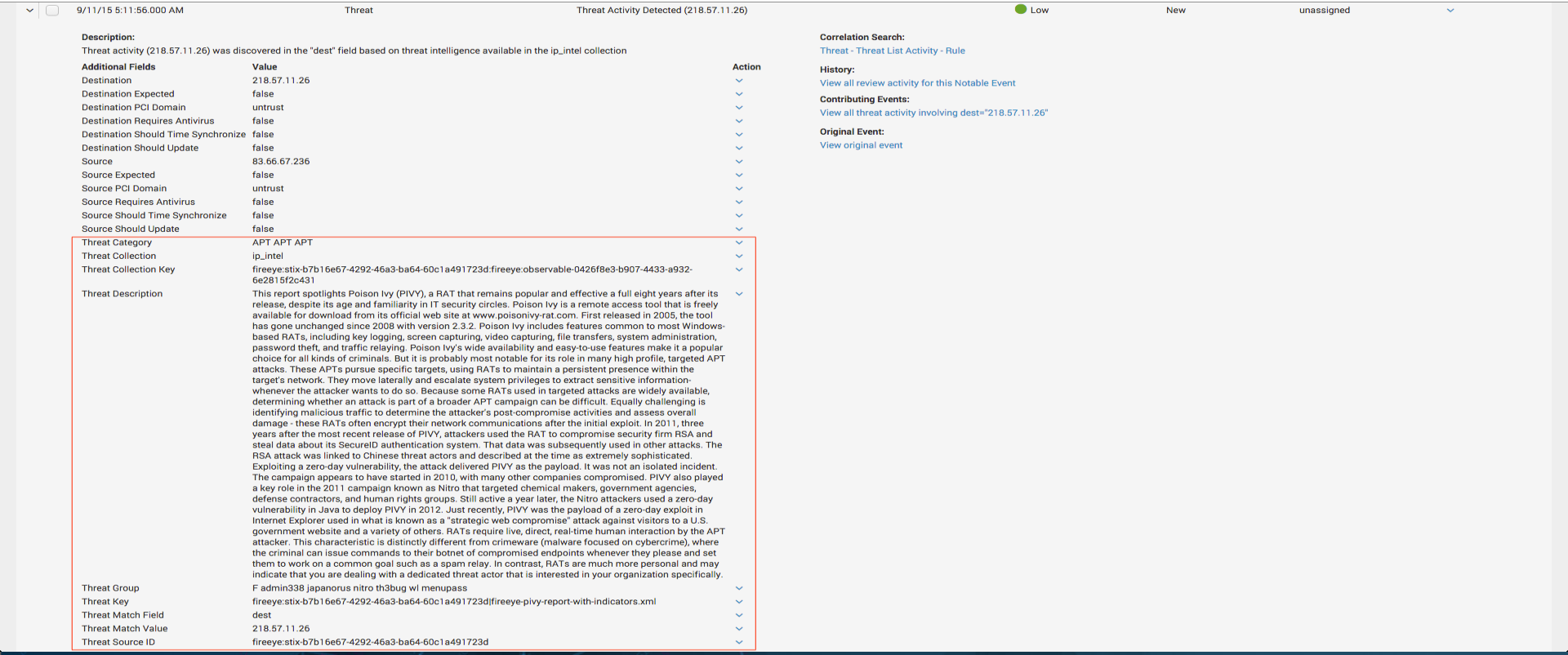
ES Threat Intelligence Framework



ES Threat Intelligence Framework



ES Threat Intelligence Framework



9/11/15 5:11:56.000 AM | Threat | Threat Activity Detected (218.57.11.26) | Low | New | unassigned

Description:
Threat activity (218.57.11.26) was discovered in the "dest" field based on threat intelligence available in the ip_intel collection

Additional Fields	Value	Action
Destination	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	
Threat Category	APT APT APT	
Threat Collection	ip_intel	
Threat Collection Key	fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d:fireeye:observable-0426f8e3-b907-4433-a932-6e2815f2c431	
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 is 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 SecureID 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. Still active a year later, the Nitro attackers used a zero-day vulnerability in Java to deploy PIVY in 2012. Just recently, PIVY was the payload of a zero-day exploit in 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.	
Threat Group	F admin338 japanorus nitro th3bug wl menupass	
Threat Key	fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d|fireeye-pivy-report-with-indicators.xml	
Threat Match Field	dest	
Threat Match Value	218.57.11.26	
Threat Source ID	fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d	

Correlation Search:
Threat - Threat List Activity - Rule

History:
View all review activity for this Notable Event

Contributing Events:
View all threat activity involving dest="218.57.11.26"

Original Event:
View original event

Actions on Intent

Actions on Intent

PII Theft

Actions on Intent

- PII Theft
- Intellectual Property Theft

Actions on Intent

- PII Theft
- Intellectual Property Theft
- Financial Data Theft

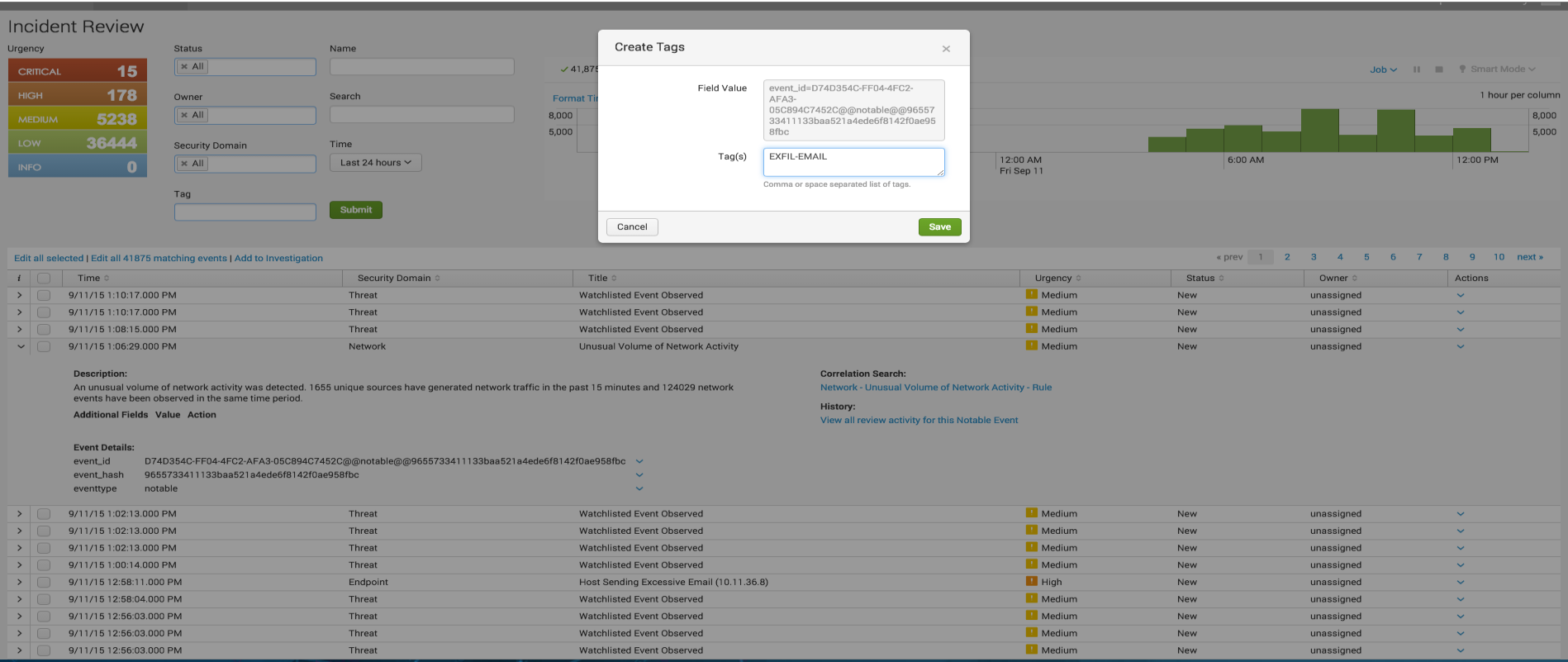
Actions on Intent

- PII Theft
- Intellectual Property Theft
- Financial Data Theft
- Political/Corporate Motives

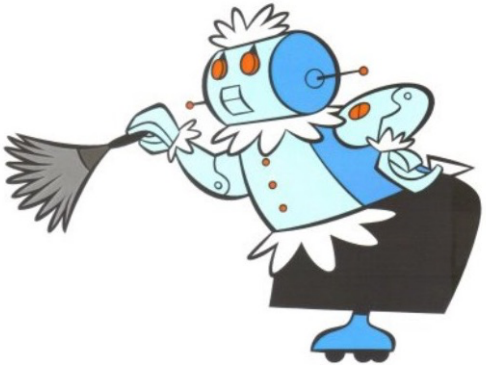
Actions on Intent

- PII Theft
- Intellectual Property Theft
- Financial Data Theft
- Political/Corporate Motives
- Control System Tampering

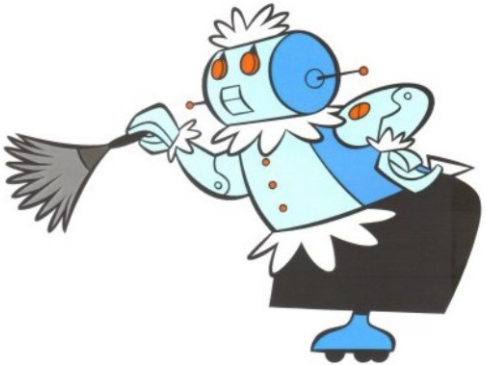
ES & Action on Intent



Remediation

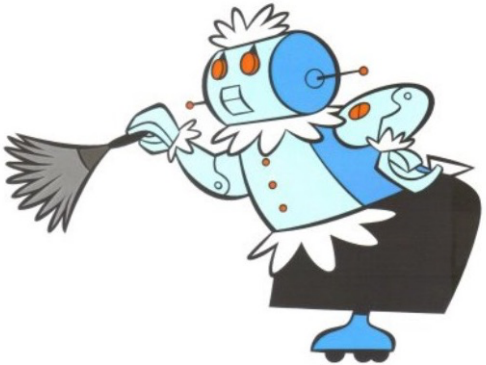


Remediation



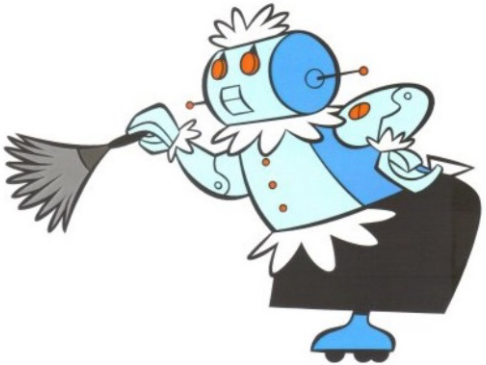
- Scope the Compromise

Remediation



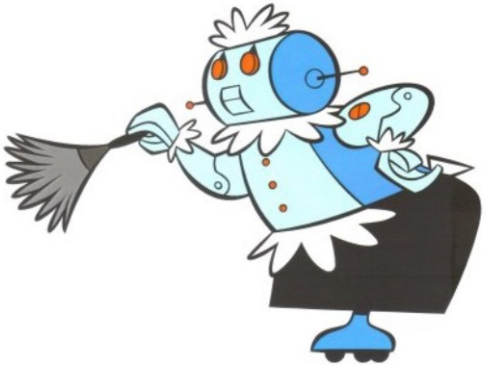
- Scope the Compromise
- Devise a Remediation Strategy

Remediation



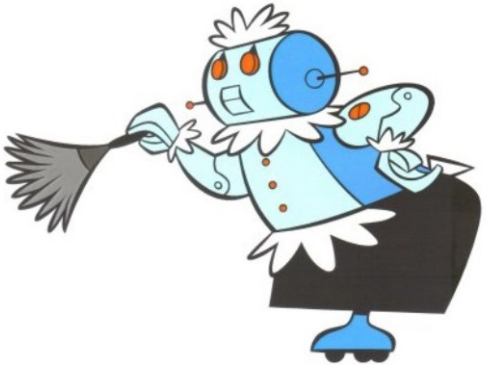
- Scope the Compromise
- Devise a Remediation Strategy
- Track Remediation Progress

Remediation



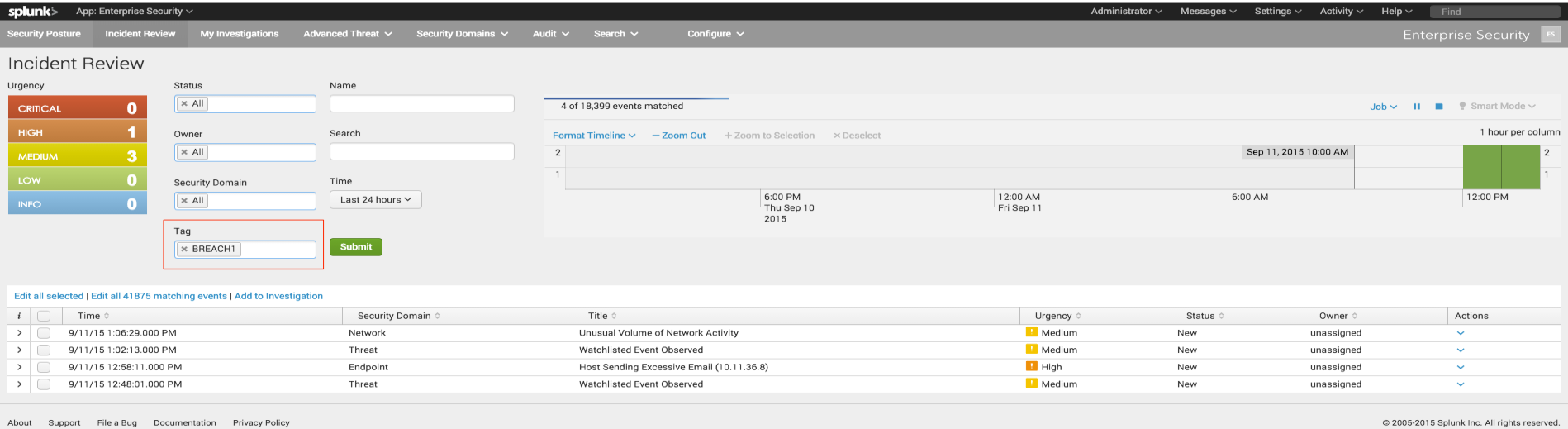
- Scope the Compromise
- Devise a Remediation Strategy
- Track Remediation Progress
- Monitor for Post-Remediation Compromises

Remediation

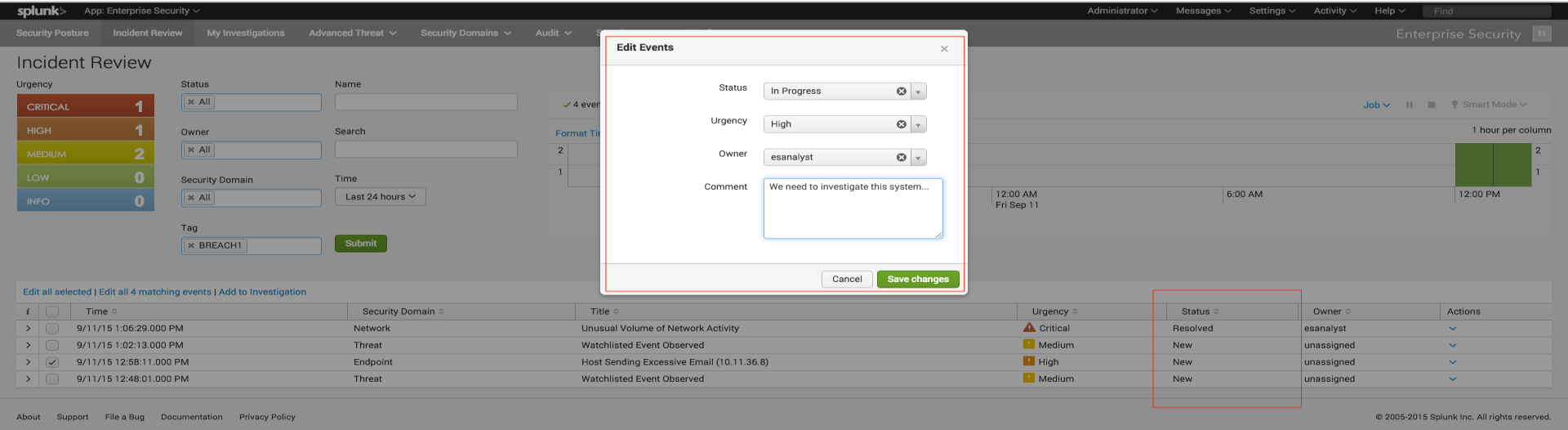


- Scope the Compromise
- Devise a Remediation Strategy
- Track Remediation Progress
- Monitor for Post-Remediation Compromises
- Construct a Breach Report

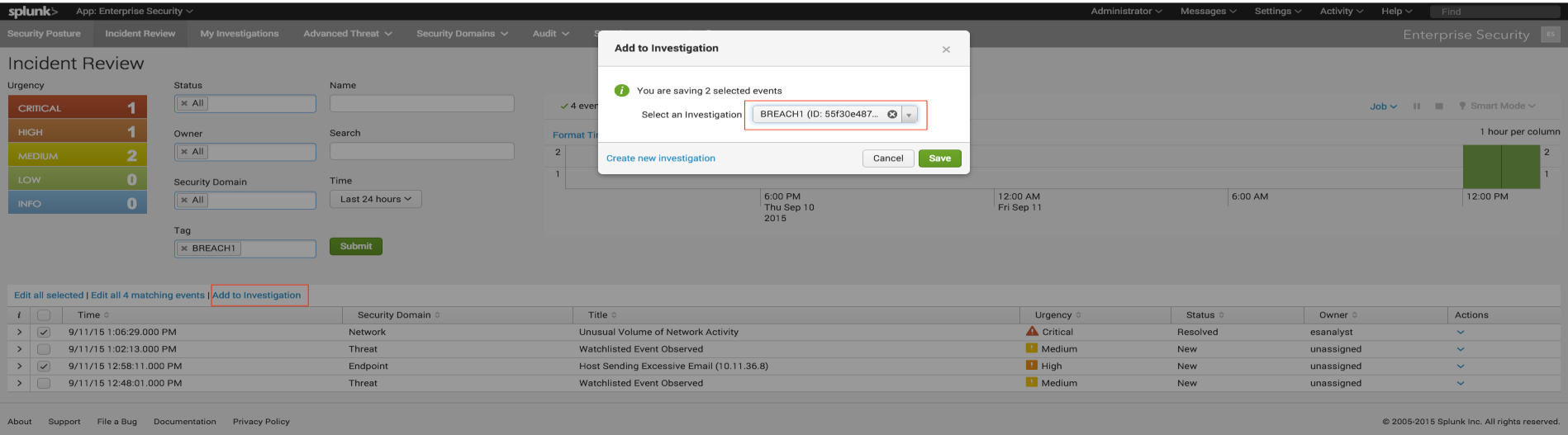
ES Incident Review



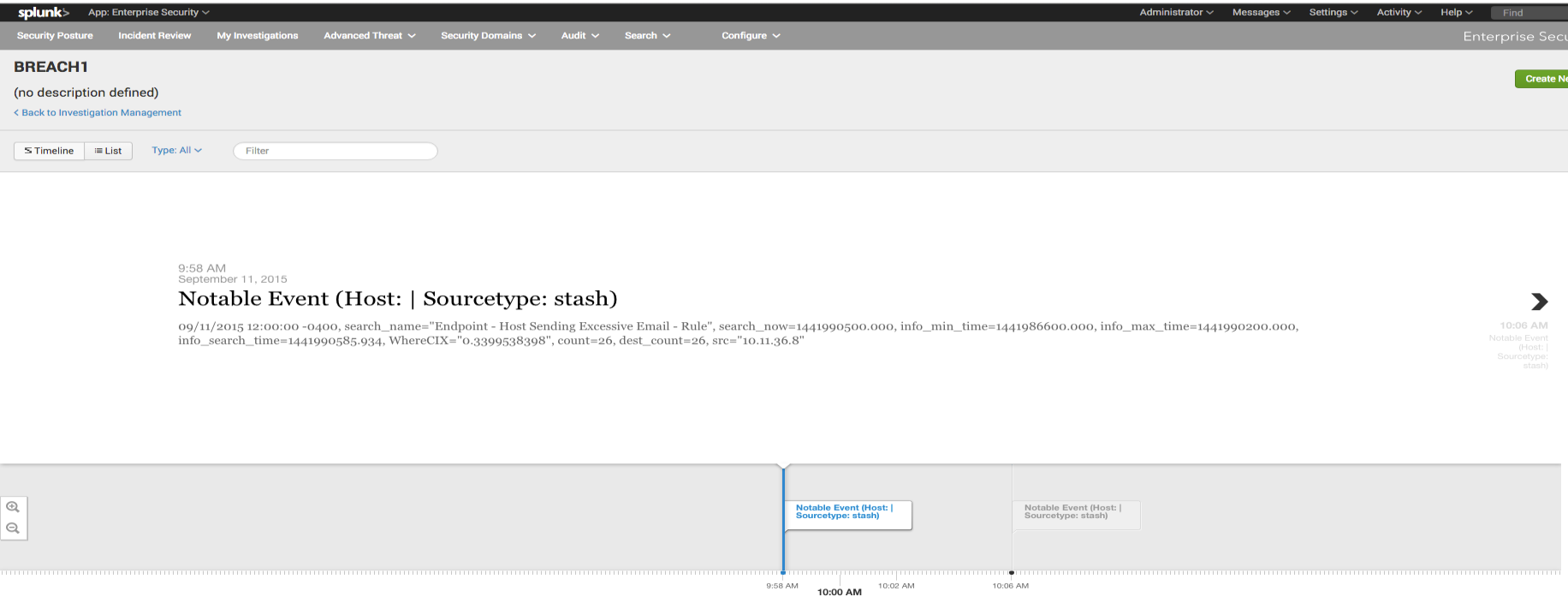
ES Incident Review



ES Incident Review



ES Investigator Timeline



Splunk Enterprise Security

Splunk Enterprise Security

Network/Endpoint Detection!

Splunk Enterprise Security

Asset/Identity Framework!

Network/Endpoint Detection!

Splunk Enterprise Security

Asset/Identity Framework!

Network/Endpoint Detection!

Threat Intelligence Framework!

Splunk Enterprise Security

Asset/Identity Framework!

Network/Endpoint Detection!

Threat Intelligence Framework!

Incident Review!

Splunk Enterprise Security

Asset/Identity Framework!

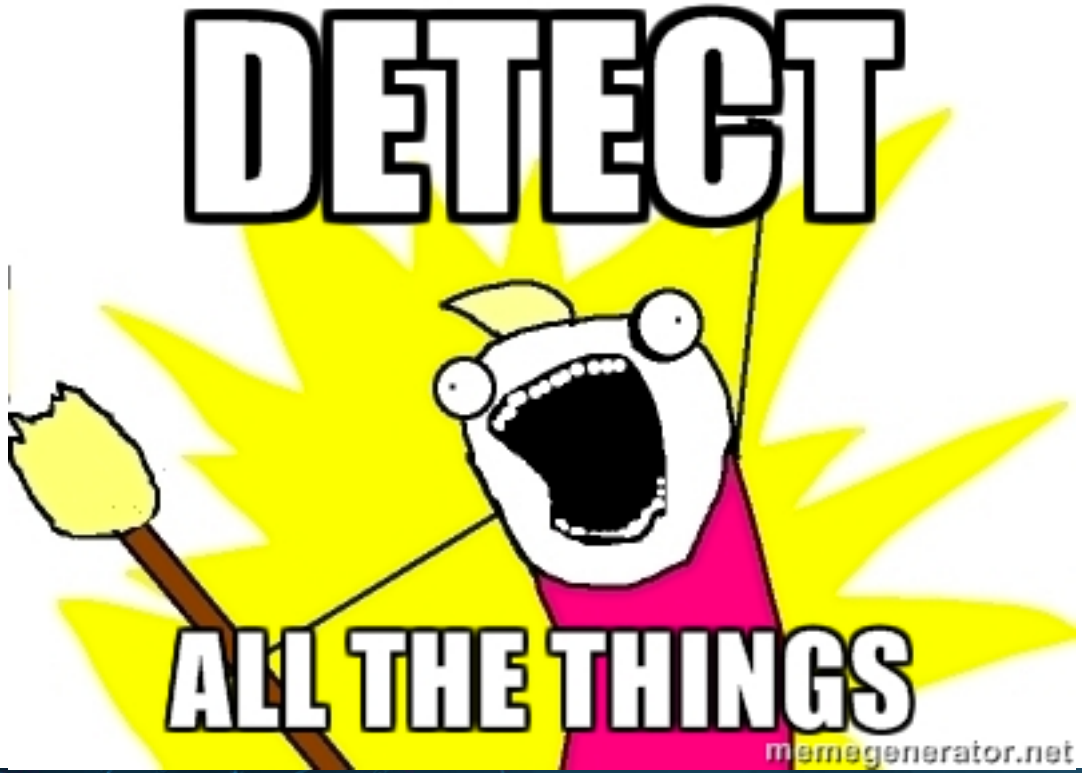
Network/Endpoint Detection!

Investigative Timeline!

Threat Intelligence Framework!

Incident Review!

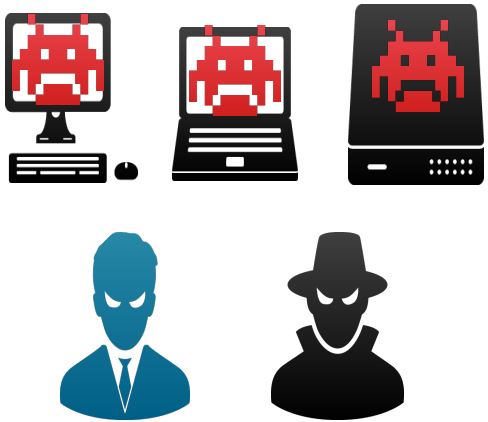
Splunk Enterprise Security



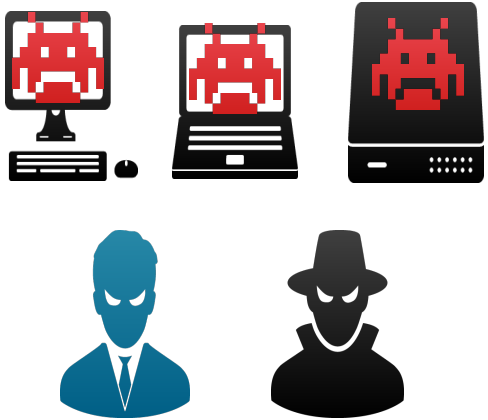
Just Detected a Breach, Now What?

Just Detected a Breach, Now What?

ES Breach Management App

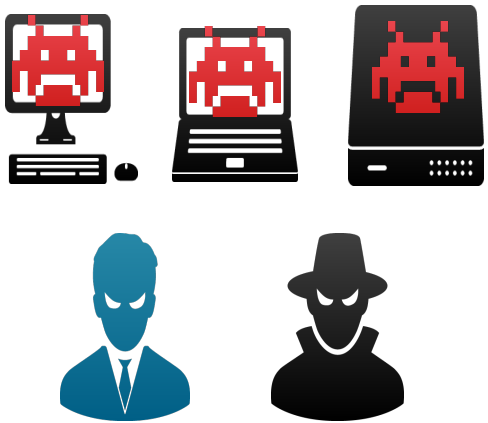


ES Breach Management App



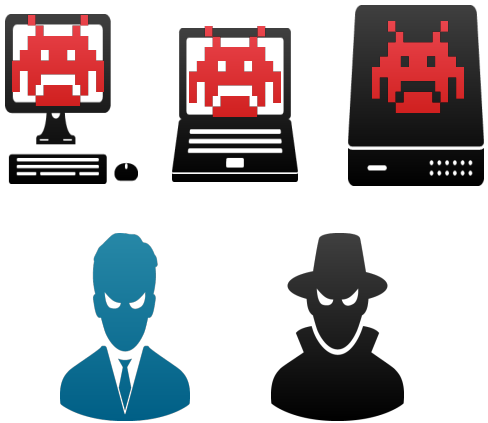
Asset/Identity Framework

ES Breach Management App



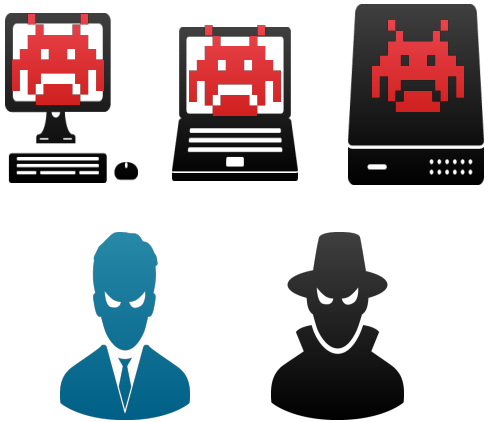
- Asset/Identity Framework
- Threat Intelligence Framework

ES Breach Management App



- Asset/Identity Framework
- Threat Intelligence Framework
- Incident Review

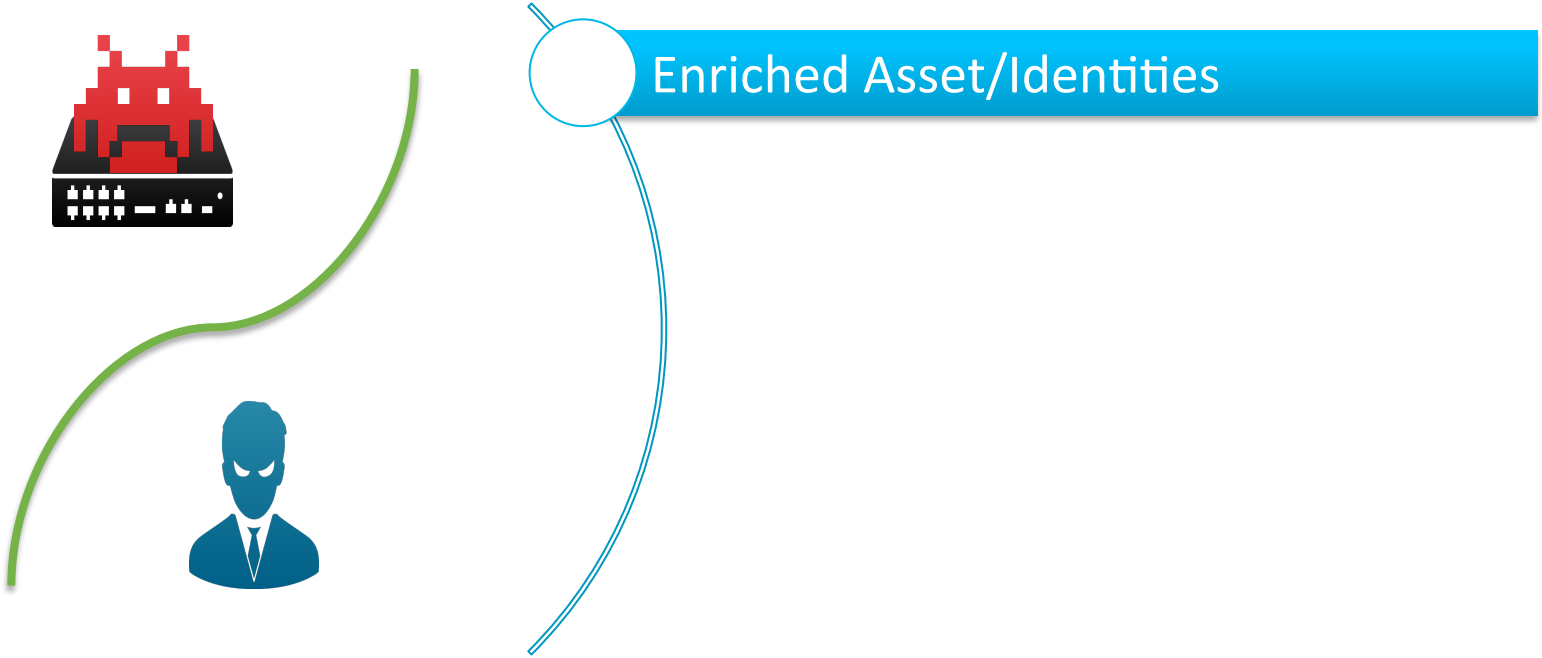
ES Breach Management App



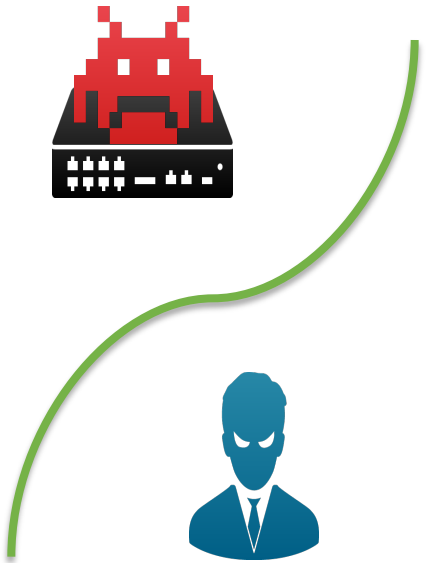
- Asset/Identity Framework
- Threat Intelligence Framework
- Incident Review
- Investigative Timeline

Track Compromised Assets/Identities

Track Compromised Assets/Identities

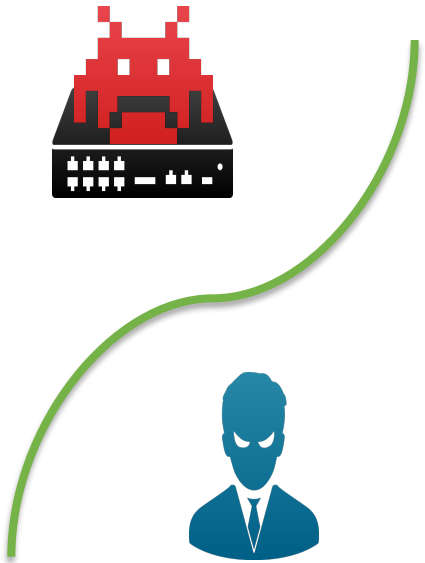


Track Compromised Assets/Identities



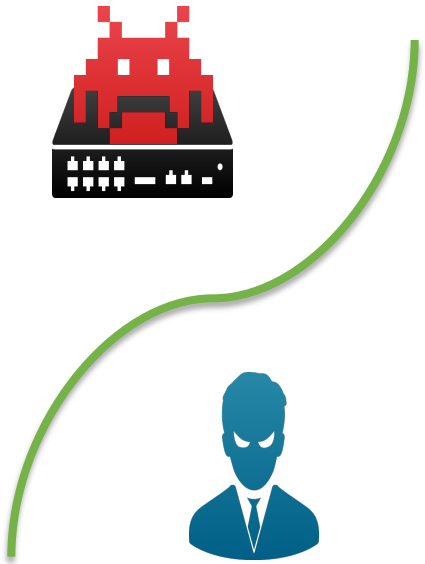
- Enriched Asset/Identities
- Initial/Last Known Activity Tracking

Track Compromised Assets/Identities



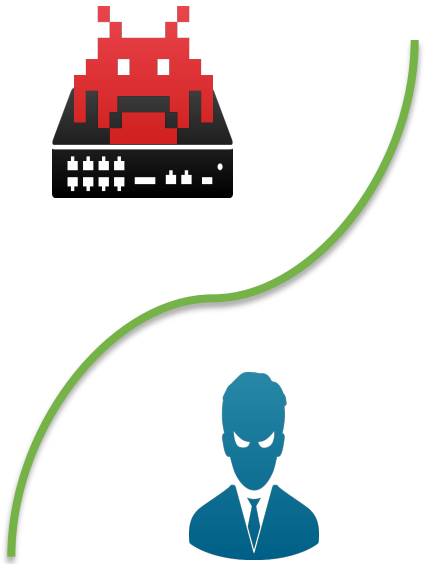
- Enriched Asset/Identities
- Initial/Last Known Activity Tracking
- Asset/Identity Timeline Drilldown

Track Compromised Assets/Identities



- Enriched Asset/Identities
- Initial/Last Known Activity Tracking
- Asset/Identity Timeline Drilldown
- Malicious Activity Tracking

Track Compromised Assets/Identities



- Enriched Asset/Identities
- Initial/Last Known Activity Tracking
- Asset/Identity Timeline Drilldown
- Malicious Activity Tracking
- Post Remediation Tracking

Track Attacker Infrastructure/Intelligence

Track Attacker Infrastructure/Intelligence

Network Intelligence

Track Attacker Infrastructure/Intelligence

- Network Intelligence
- Endpoint Intelligence

Track Attacker Infrastructure/Intelligence

- Network Intelligence
- Endpoint Intelligence
- Initial/Last Know Activity Times

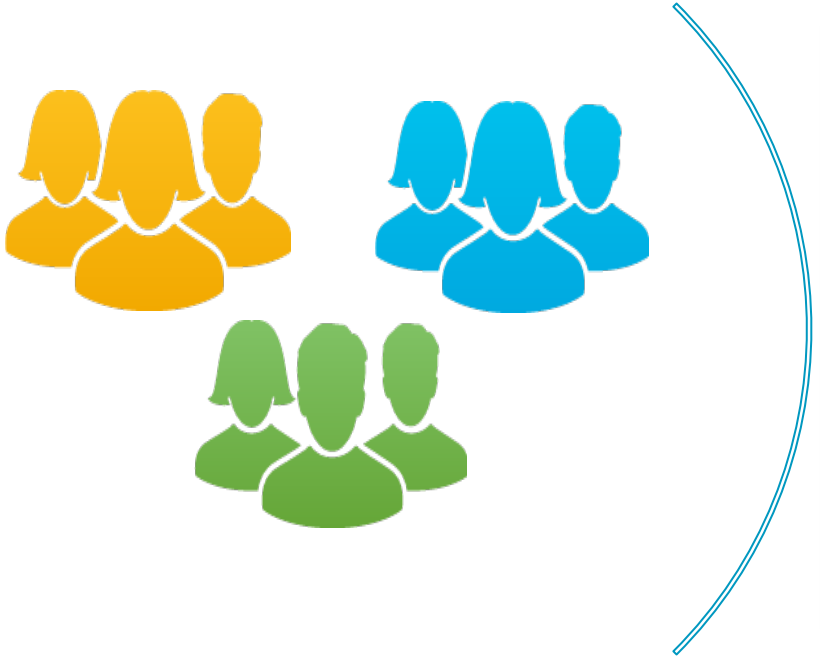
Track Attacker Infrastructure/Intelligence

- Network Intelligence
- Endpoint Intelligence
- Initial/Last Know Activity Times
- TTPs

Track Attacker Infrastructure/Intelligence

- Network Intelligence
- Endpoint Intelligence
- Initial/Last Know Activity Times
- TTPs
- Automatically Pushed to ES Threat Intel Framework

Analyst Assignment



Analyst Assignment

Add Analysts to a Breach

Analyst Assignment

- Add Analysts to a Breach
- Track Amount of Work Performed

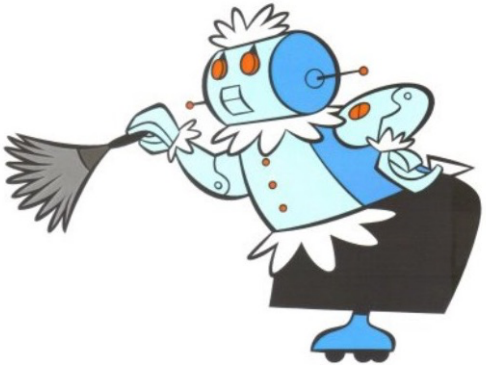
Analyst Assignment

- Add Analysts to a Breach
- Track Amount of Work Performed
- Annotate Breaches

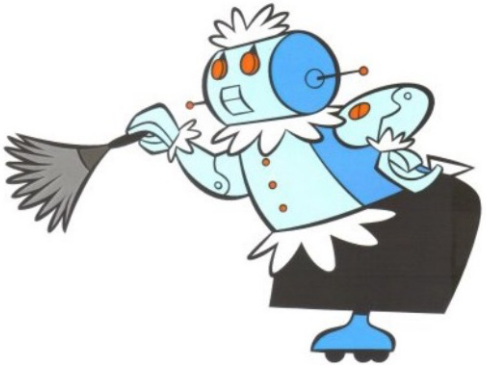
Analyst Assignment

- Add Analysts to a Breach
- Track Amount of Work Performed
- Annotate Breaches
- Fully Integrated with Investigative Timeline

Track Remediation Progress

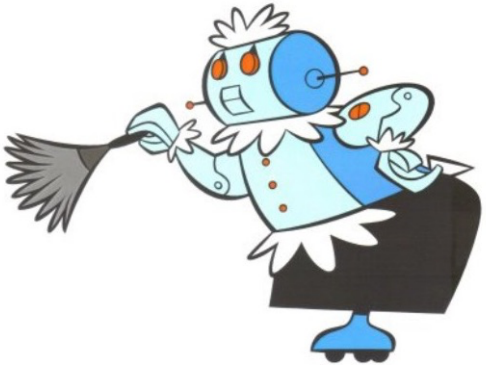


Track Remediation Progress



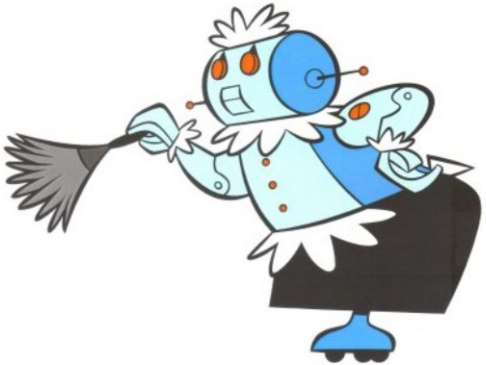
Assets

Track Remediation Progress



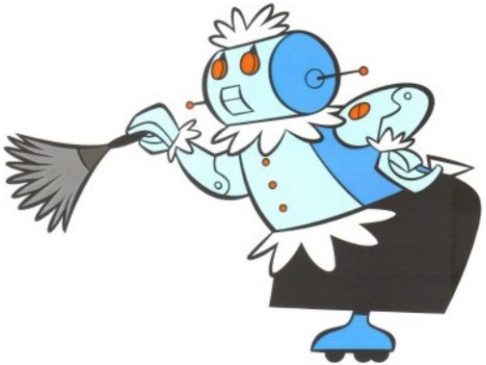
- Assets
- Identities

Track Remediation Progress



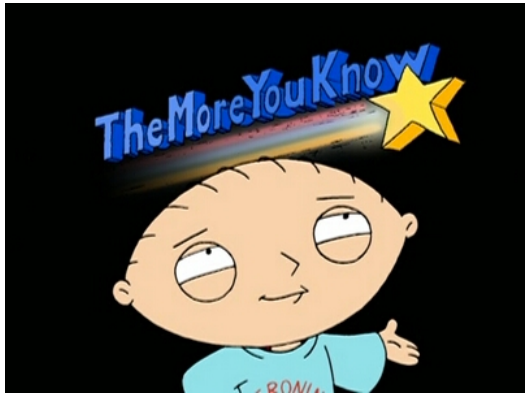
- Assets
- Identities
- Remediation Metrics

Track Remediation Progress

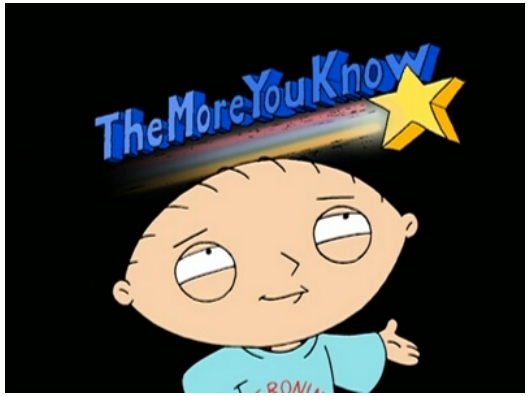


- Assets
- Identities
- Remediation Metrics
- Post-Remediation Compromises

Takeaways

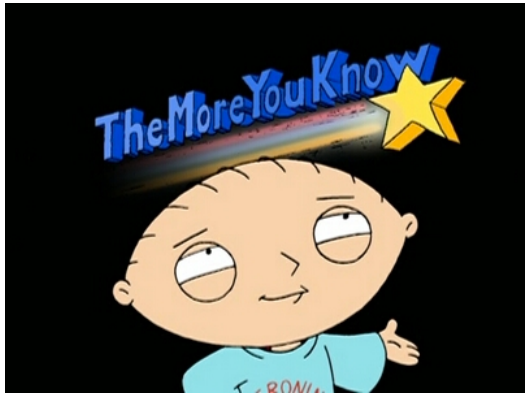


Takeaways



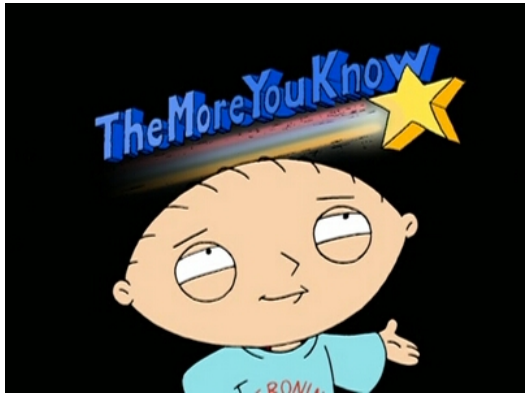
- Compromised Asset/Identity Tracking

Takeaways



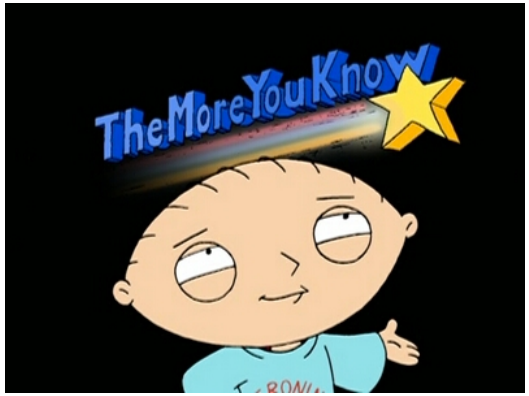
- Compromised Asset/Identity Tracking
- Asset/Identity Specific Timeline Drilldowns

Takeaways



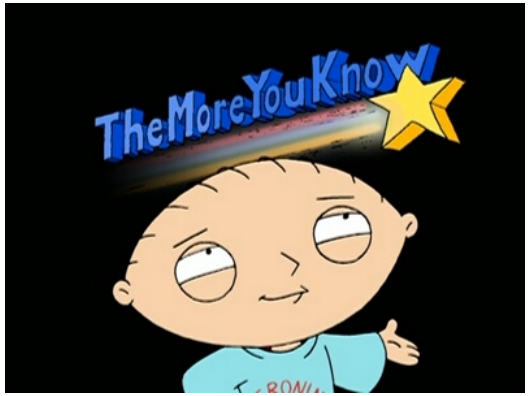
- Compromised Asset/Identity Tracking
- Asset/Identity Specific Timeline Drilldowns
- Threat Infrastructure Tracking

Takeaways



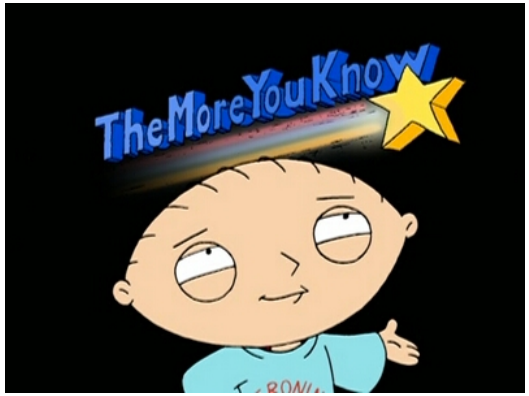
- Compromised Asset/Identity Tracking
- Asset/Identity Specific Timeline Drilldowns
- Threat Infrastructure Tracking
- Remediation Tracking

Takeaways



- Compromised Asset/Identity Tracking
- Asset/Identity Specific Timeline Drilldowns
- Threat Infrastructure Tracking
- Remediation Tracking
- One-Stop Breach Management Solution

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 ☺

THANK YOU

splunk>