

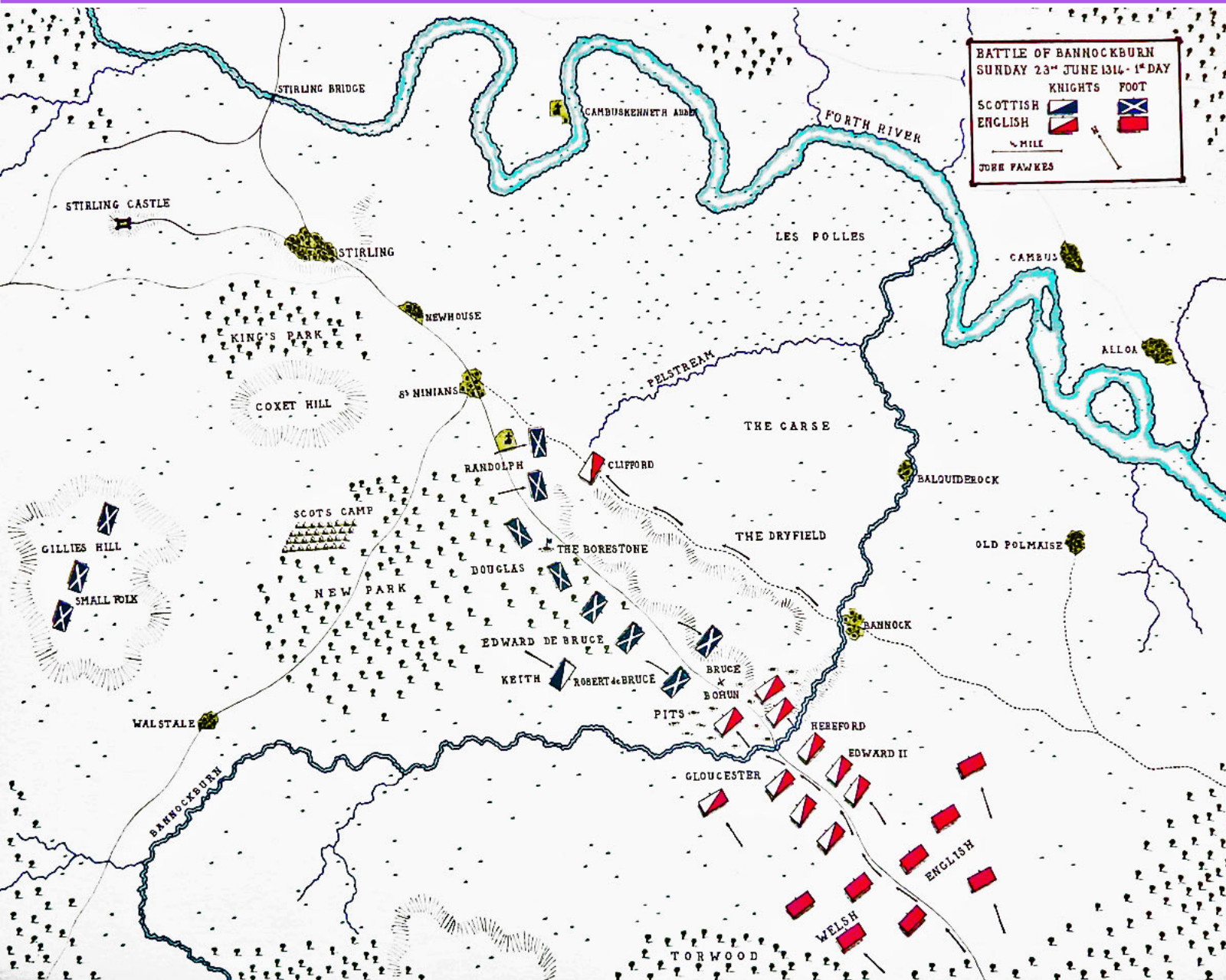


31ST
ANNUAL
FIRST
CONFERENCE

EDINBURGH
JUNE 16-21
2019

CSIRT Schiltron: Training, Techniques, and Talent

Jeff Bollinger
James Sheppard
(Cisco CSIRT)



(1314) Robert the Bruce positioned his army in the New Park with Randolph's schiltron to the fore and his own immediately behind it. The chosen **method** of combat was for each **schiltron** to form a **bristling mass of spears** which the English knights would be **unable to penetrate**.

The Scots dug **concealed pits** across the front of their position and along the bank of the Bannockburn to break up any mounted charge against them.

<https://www.britishbattles.com/scottish-war-of-independence/battle-of-bannockburn/>



<https://www.britishbattles.com/scottish-war-of-independence/battle-of-bannockburn/>

How can an incident response teams enable **readiness** and improve **capabilities** with evolving threat profiles that require new approaches and new skillsets?



- Mail and **phishing** messages have become the primary malware infection vector;
- **Cryptominers** have become an important monetization vector for cyber criminals;
- State-sponsored agents increasingly target banks by using **attack-vectors** utilized in cyber crime;
- The emergence of **IoT environments** will remain a concern due to missing protection mechanisms...
- Cyber **threat intelligence** needs to respond to increasingly automated attacks...
- **Skills and training are the main focus of defenders.**

PRESS RELEASE

Exposure to cyber-attacks in the EU remains high - New ENISA Threat Landscape report analyses the latest cyber threats

In 2018, the cyber threat landscape changed significantly. The most important threat agent groups, namely cyber-criminals and state-sponsored actors have further advanced their motives and tactics. Monetisation motives contributed to the appearance of crypto-miners in the top 15 cyber threats.

Published on January 28, 2019



Tagged with [Cyber Threats](#), [Threat landscape](#)

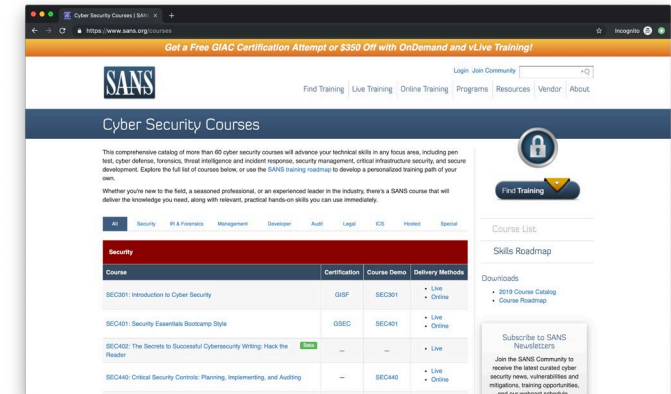
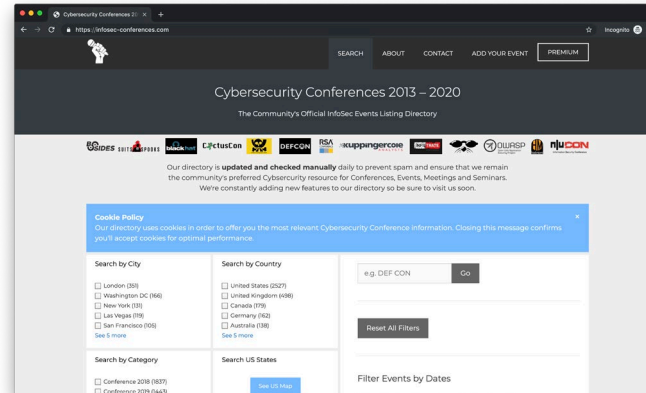
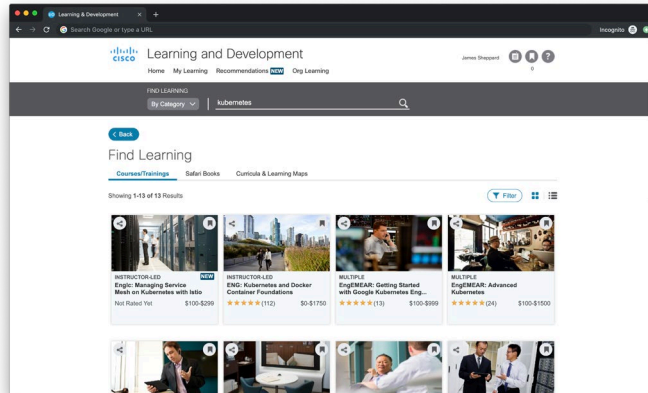
Advances in defence have also been assessed: law enforcement authorities, governments and vendors were able to further develop active defence practices such as threat agent profiling and the combination of cyber threat intelligence (CTI) and traditional intelligence. This led to a more efficient identification of attack practices and malicious artefacts, leading in turn to more efficient defence techniques and attribution rates.

“We are witnessing the development and deployment of new technologies, which are reshaping the cyber landscape and significantly impacting society and national security. The European Union needs to be ready to adapt to and reap the benefits of these technologies to reduce the cyber-attack surface. This report raises awareness of the cyber dangers that citizens and businesses should be conscious of and responsive to. It provides recommendations as to how the digital single market can prepare an adequate response to cyber threats, with certification and standardisation at the forefront”, said ENISA’s Executive Director Udo Helmbrecht.

References

- [ENISA Threat Landscape Report 2018](#)
- <http://www.enisa.europa.eu/media/news-items/news-wires/RSS>
- <http://www.enisa.europa.eu/media/press-releases/press-releases/RSS>

We Value Learning & Development



SANS Courses
Cisco L&D
Conferences
CTFs
Tabletops
Purple Team

We Needed More

- Training based on real cases and real data.
- Useful to newbies and veterans alike.
- Tailored challenges unique to the IR role.
- Teaching on incidents with similar characteristics and techniques.
- Fostering collaboration, camaraderie, and trust.



Team Training Goals

- Security 101
- Case Work
- Data Sources
- Internal Tools



Security 101

- New analysts typically arrive with some domain knowledge
- System and networking basics are crucial to daily work and understanding
- Develops better “hacker mindset” – builds on curiosity
- Evaluates efficacy/comprehension of commercial training programs



Casework

- Pairing operational/technical knowledge with practical security comprehension
- Helps to maintain consistency in response
- Introduces useful tricks/tips that senior teammates have used over the years
- Drawn from *real incidents* to allow replaying a part of an investigation



Data Sources

- We're a *data-centric* team that makes decisions based on evidence in the available data.
- Understanding how to effectively search all the available data sources can take time
- Knowing what data is available and what questions can be answered delivers better analysis and results.



Internal Tools

- Tools get built over the years and often forgotten.
- The time to learn how to use tools is not during an incident.
- Having practice and understanding how to use features saves time and minimizes delays.



Skills Training

Why a Blue Team CTF?

- Certifications and professional training organizations teach security/technology skills – not operations/SOP
- We can tailor the training content to our team goals
- Hands-on training / terminal time
- Several audits (ex. ISO27001) require annual training programs
- People are familiar with the CTF format
- Gamification* removes the dread of boring training/testing/drilling
- Cost – FOSS. Only need a small server and to develop your own training content



Blue Team CTF

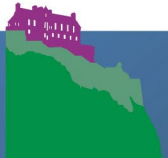
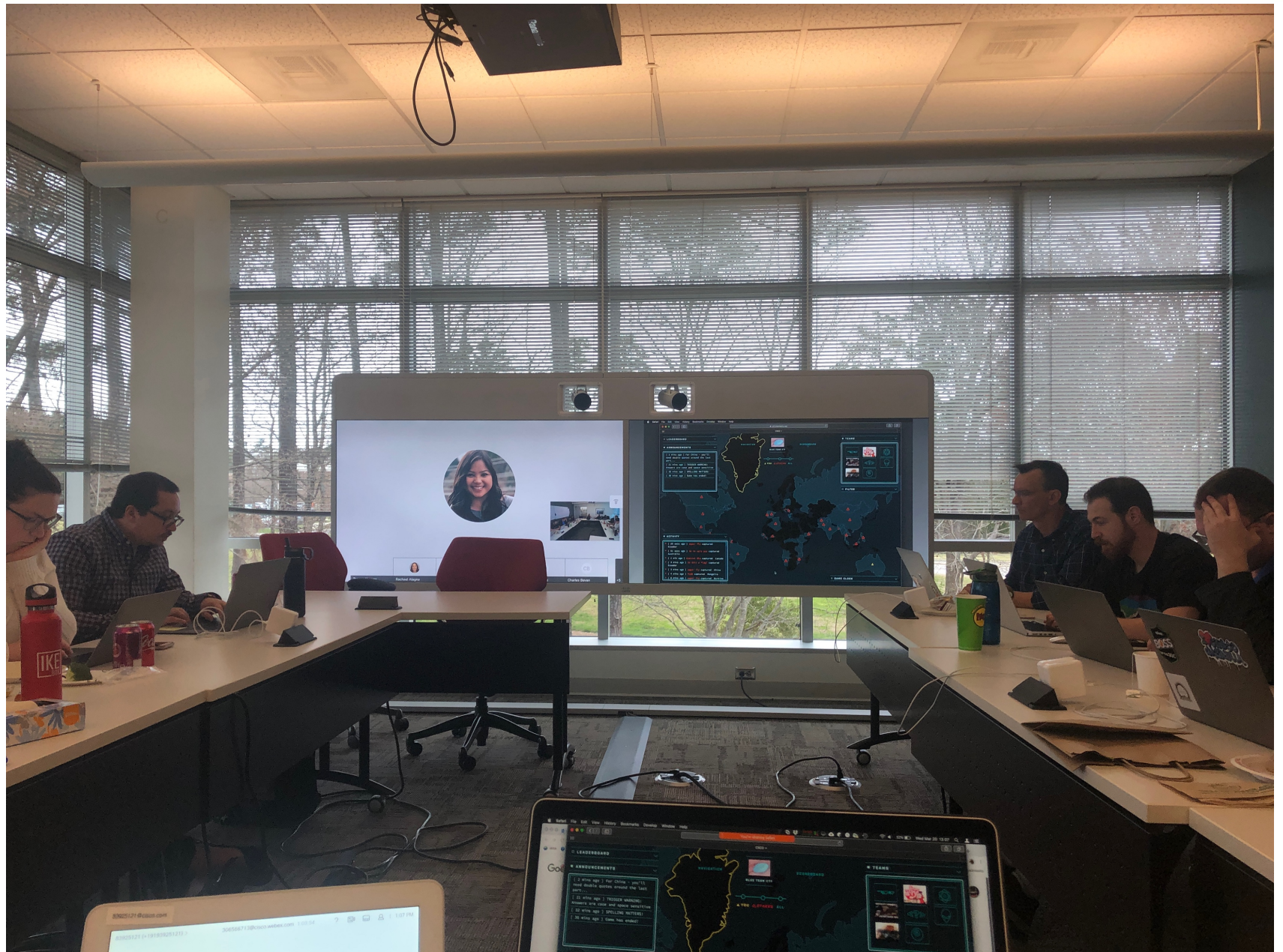
- Must fit the training goals
- Fun
- Interesting interface
- Easy to run/support
- Decent scoring/teaming interface



<https://github.com/facebook/fbctf>



- 4 Hours
- 30 Participants
- All branches of CSIRT
- 8 Randomly selected teams
- 4 Different Sites
- 49 Flags/Quizzes
- 100+ Tacos



LEADERBOARD

ANNOUNCEMENTS

[2 mins ago] TRIGGER WARNING:
Answers are case and space sensitive

[13 mins ago] SPELLING MATTERS!

[18 mins ago] Game has ended!

NAVIGATION



BLUE TEAM CTF



▲ YOU ▲ OTHERS ALL

SCOREBOARD

TEAMS

FILTER

ACTIVITY

- [14 secs ago] TLDR captured Bangladesh
- [36 secs ago] Je ne sais pas captured Brazil
- [1 min ago] D.E.A.D. captured Thailand
- [3 mins ago] super fly captured Bolivia
- [4 mins ago] Gigachads captured Algeria
- [5 mins ago] TLDR captured Philippines
- [6 mins ago] kewl brahs captured Philippines
- [6 mins ago] Eternal Fly captured

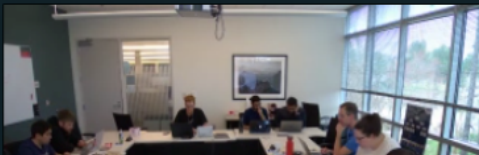
capture_Spain - Don't bro me if you don't know me

What is the only index that includes the field labeled 'applicationName'?

Insert your answer

REQUEST HINT SUBMIT

15 PTS	type	completed_by >	KEWL BRAHS
	flag		D.E.A.D.
	category		SUPER FLY
	Data_Sources		IS THIS A FLAG?
	first_capture		GIGACHADS
	kewl brahs		JE NE SAIS



GAME CLOCK

Prizes!

filter_	rank_	team_name_	quiz_pts_	flag_pts_	base_pts_	total_pts_
<input checked="" type="radio"/>	1	SUPER FLY	255	1220	0	1425
<input checked="" type="radio"/>	2	KEWL BRAHS	135	1005	0	1031
<input checked="" type="radio"/>	3	GIGACHADS	85	955	0	999
<input checked="" type="radio"/>	4	ETERNAL BLU	285	760	0	960
<input checked="" type="radio"/>	5	TLDR	180	820	0	945
<input checked="" type="radio"/>	6	IS THIS A FLAG?	200	740	0	940
<input checked="" type="radio"/>	7	D.E.A.D.	145	685	0	805
<input checked="" type="radio"/>	8	JE NE SAIS PAS	105	575	0	665

10TB!



Security 101

CATEGORY	QUESTION	HINT
Security 101	What networking technique prevented Wannacry from encrypting its victims?	The same technique our DNS RPZ can use...



Security 101

FLAG	TESTS
Sinkhole	How [part of] Wannacry worked
	Common terminology used in takedowns and security research
	Basic understanding of our DNS Response Policy Zone features

<https://tools.ietf.org/id/draft-vixie-dnsop-dns-rpz-00.html>



Case Work

CATEGORY	QUESTION	HINT
Case Work	How many cases have been opened that have references in the case notes to MAC addresses created by <i>“Universal Global Scientific Industrial Co.”</i> ?	note:"00:10:C6:*" OR ...



Case Work

The screenshot shows the GIR CSIRT search interface. At the top, there is a search bar with a query: `note:"00:10:C6:*" OR note:"00:16:41:*" OR note:"00:16:41:*" OR note:"00:1A:6B:*" OR note:"00:1A:6B:*" OR note:"00:1E:37:*" OR note:"00:21:86:*" OR note:"00:24:7E:*" OR note:"00:27:13:*" OR note:"03:3C:CD:*" OR note:"40:2C:F4:*" OR note:"44:39:C4:*" OR note:"6C:0B:84:*" OR note:"70:F3:95:*" OR`. Below the search bar, it says "513 results returned." and provides a permalink. The results table has columns for id, title, modified, playbook_id, agent, status, and categ_type. The table contains several rows of data, with some rows highlighted in green.

id	title	modified	playbook_id	agent	status	categ_type
40	61213-2592	2007-02-08T04:26:27Z			Closed	Compromise Information
39	70402-3166	2007-04-12T06:12:04Z			Closed	Malware
38	70404-3183	2007-10-31T21:36:52Z			Closed	Malware
35	80123-4453	2008-01-23T22:04:04Z			Closed	Policy Violations
33	80219-5237	2008-02-27T13:30:12Z			Closed	Malware

FLAG	TESTS
513	Basic case repository searching
	Case details and typical metadata captured
	Knowledge of MAC Address organizationally unique identifier (OUIs)



Case Work

CATEGORY	QUESTION	HINT
Case Work	Which server (hostname) hosted in the UK triggered the play described in bug 12161?	playbook_id=610002



Case Work

FLAG	TESTS
SRV-GPK12-RS-T	Basic case repository searching
	Connection between Incidents and CSIRT Playbook
	Knowledge of internal host naming
	Experience finding playbooks and detection methods.

Case #
Logged in as: jbolling (CSIRT) [My Cases](#) [Search](#) [Search++](#) [New Case](#)

Search

playbook_id=610002

Results Fields (Redo/reorder results field. Optional.)

search is case-insensitive

Need help? Check out the [Search++ Help Page](#) and the [GIR Data Guide](#).

9 results returned.

Permalink: [https://\[redacted\]/gir/search2.php?q=playbook_id%3D610002](https://[redacted]/gir/search2.php?q=playbook_id%3D610002)

Export

Show All entries

	id	title	modified	playbook_id			
1	190209-169694	[redacted]	2019-02-15T17:03:10Z				
2	190106-164677	[redacted]	2019-01-17T10:22:27Z	610002			
3	181213-162774	[redacted]	2018-12-14T06:24:24Z	610002			
4	181117-160108	[redacted]	2018-11-21T06:26:45Z	610002			
5	180305-134600	[redacted]	2018-03-05T08:50:02Z	610002			
6	171229-127006	Remediation for [redacted]	2018-07-26T08:17:06Z	610002		Closed	CAT3
7	170801-111197	[redacted]	2017-08-04T07:37:07Z			Closed	CAT6
8	170412-106015	[redacted]	2017-05-24T08:32:45Z	610002		Closed	CAT3
9	170411-106000	[redacted]	2017-08-04T07:56:03Z	610002		Closed	CAT6

Hostname of only 1 of the 9 results matches the right Cisco site code/naming convention

Showing 1 to 9 of 9 entries

Previous 1 Next

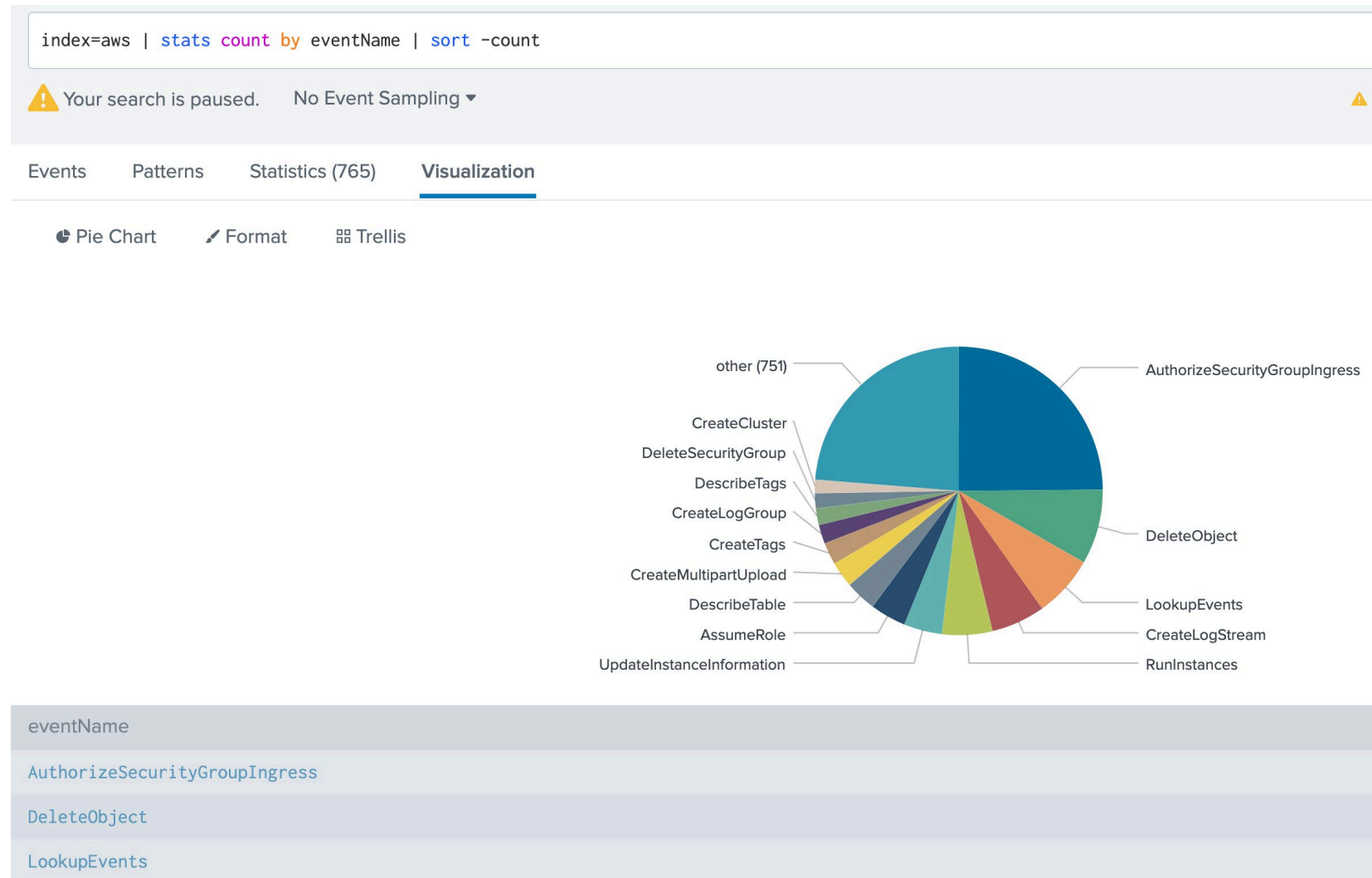
Data Sources

CATEGORY	QUESTION	HINT
Data Sources	What is the most common event name in our AWS data?	index=aws stats count by eventName sort -count



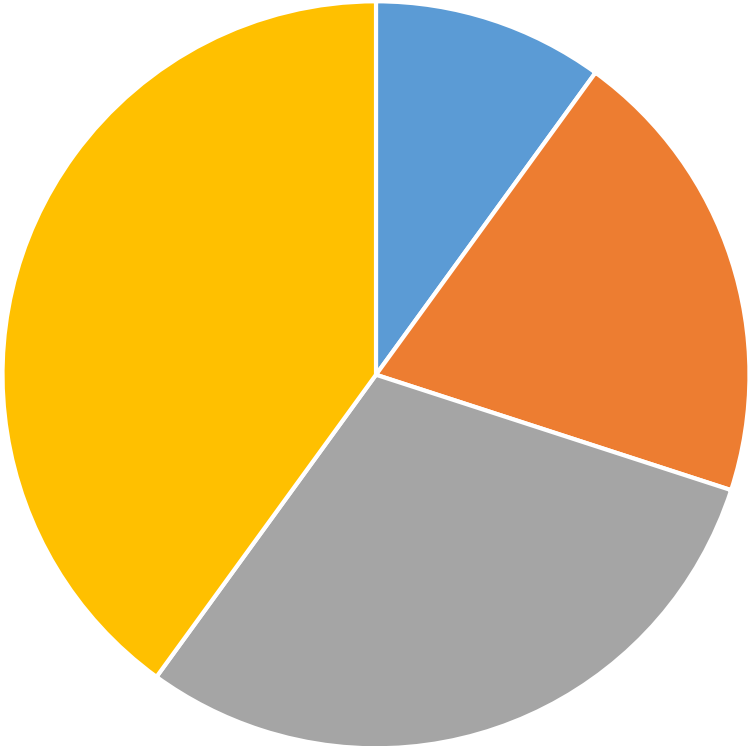
Data Sources

FLAG	TESTS
AuthorizeSecurityGroupIngress	Splunk search/stats
	Type of AWS log events
	Where to find AWS events



Find the Gaps

% Unanswered or Missed

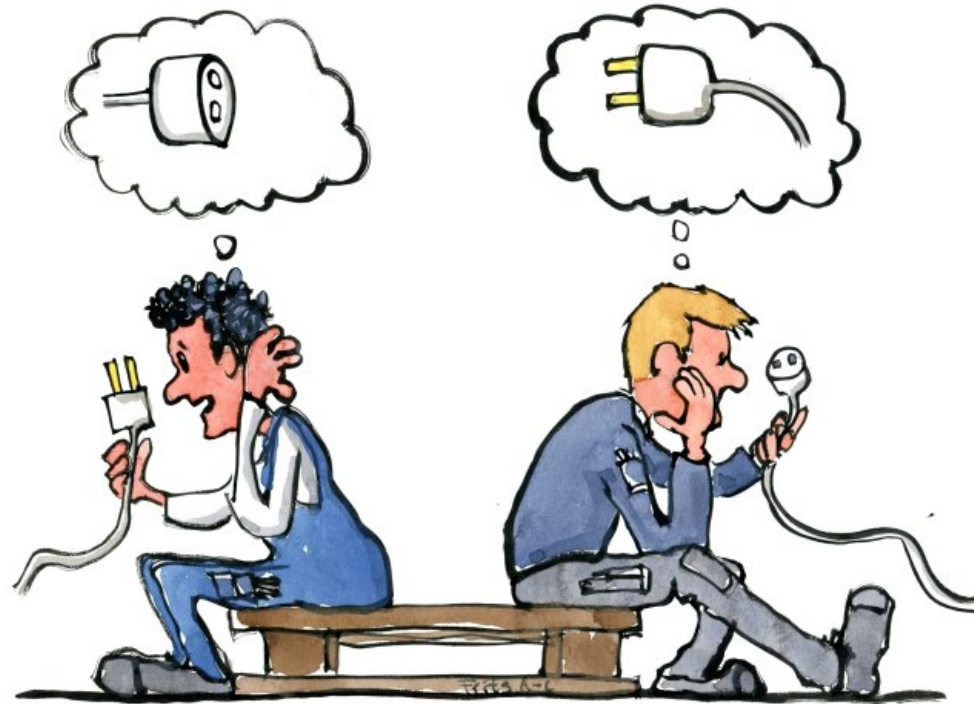


■ Security 101 ■ Casework ■ Data Sources ■ Internal Tools



The Biggest Win?

The social aspect – getting people to work together that typically don't work together.



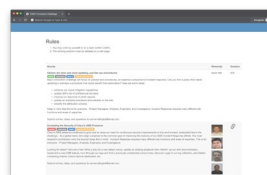
Source: <https://www.flickr.com/photos/hikingartist/28221166901/>

CSIRT Innovation Challenge

Improving **Capabilities**

CSIRT Innovation Challenge

An invitation to use your creativity, talents, and knowledge to improve security at Cisco

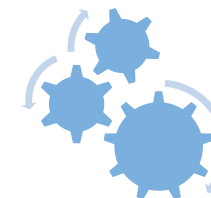


Three...

New challenges are regularly posted to the innovation hub/dashboard, each focusing on a specific area of IR.

Two...

CSIRT Individuals & teams use their creativity and talent to contribute “something” related to the challenge.



One...

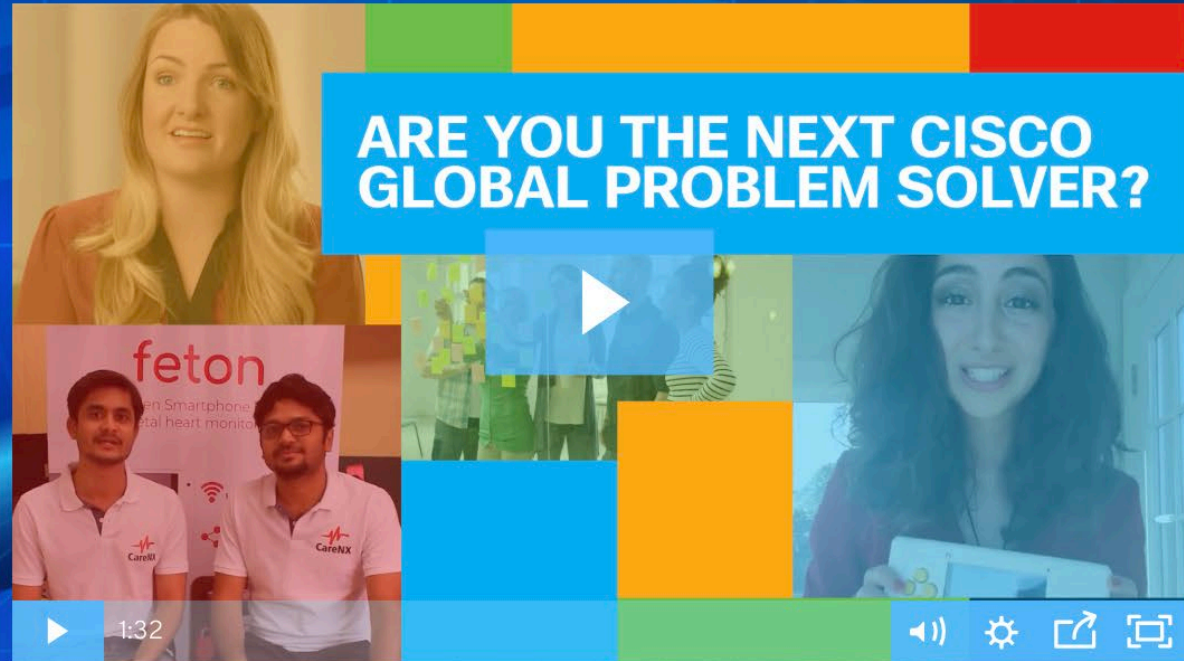
Submissions are reviewed by a panel of stakeholders and the most impactful contribution wins a reward.

Cisco Global Problem Solver Challenge 2019

\$300,000 in Prizes - Calling Students and Recent Grads

How can your innovative technology solution solve the world's most pressing social and environmental problems?

[View the Winners!](#)





\$100,000
Grand Prize

Oorja: Oonnati
PAYG Community
Solar Pumping
Systems

Oorja deploys and operates
PAYG Community Solar
Pumping Systems to provide
affordable pay-per-use
irrigation services to
smallholder farmers.



\$75,000
First Runner Up

Solar Freeze

A one stop turnkey portable
off-grid toolkit for localized
rural food.



\$25,000
Second Runner Up

Calla Imaging

A patient-centric cervical
cancer screening technology
with mHealth communication,
patient data storage and
artificial intelligence
capabilities.

Innovate Everywhere Challenge discovers the greatest ideas within Cisco

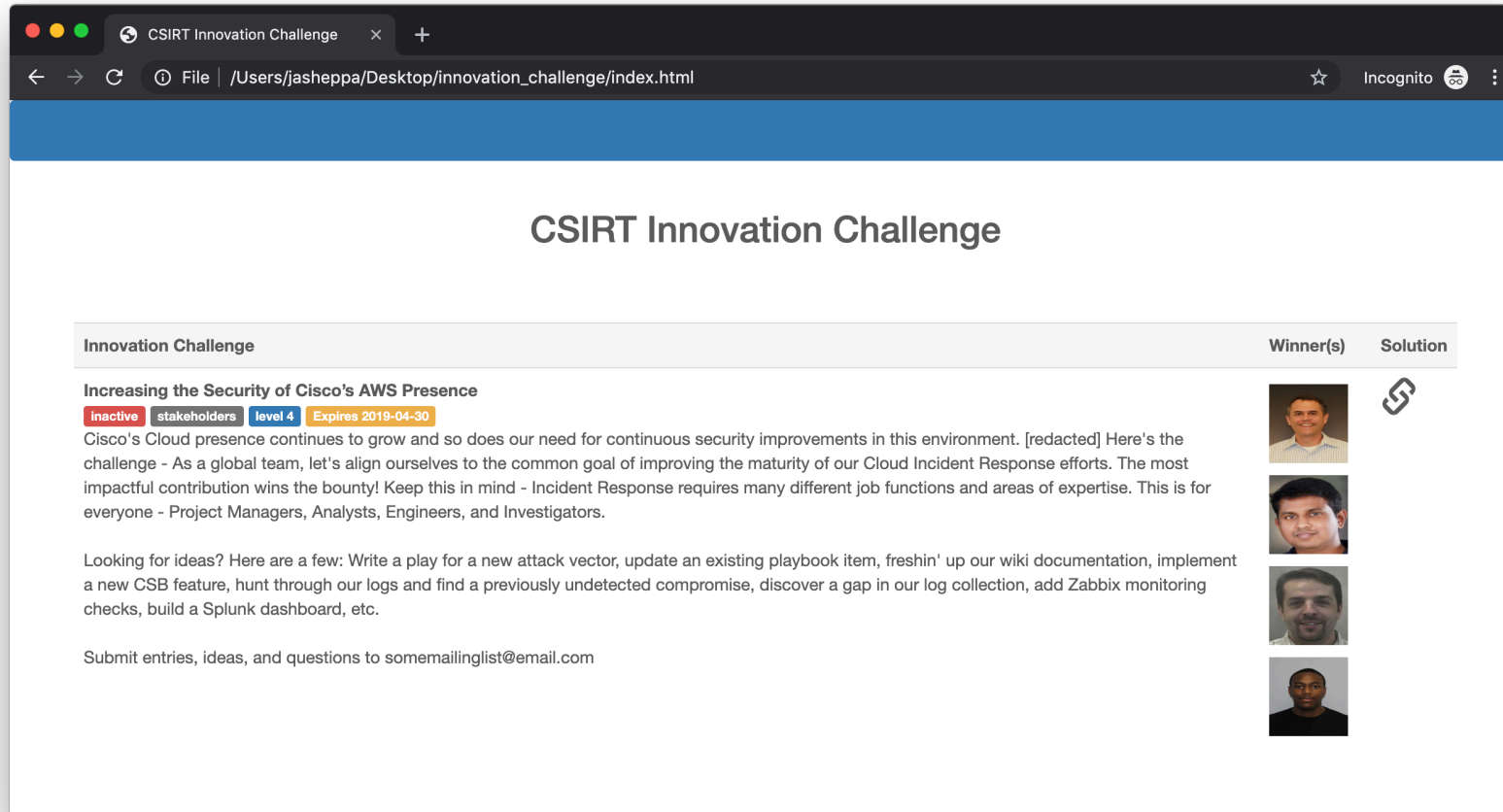


by [Stephanie Chan](#) · June 07, 2017



Cisco's Innovate Everywhere Challenge asks employees to bring their most innovative ideas to the forefront. See the excitement from this year's finalist pitches.



Innovation Hub/Dashboard



The screenshot shows a web browser window with the following details:

- Browser: Incognito
- Address Bar: /Users/jasheppa/Desktop/innovation_challenge/index.html
- Page Title: CSIRT Innovation Challenge

The main content area features a table with the following structure:

Innovation Challenge	Winner(s)	Solution
<p>Increasing the Security of Cisco's AWS Presence</p> <p>inactive stakeholders level 4 Expires 2019-04-30</p> <p>Cisco's Cloud presence continues to grow and so does our need for continuous security improvements in this environment. [redacted] Here's the challenge - As a global team, let's align ourselves to the common goal of improving the maturity of our Cloud Incident Response efforts. The most impactful contribution wins the bounty! Keep this in mind - Incident Response requires many different job functions and areas of expertise. This is for everyone - Project Managers, Analysts, Engineers, and Investigators.</p> <p>Looking for ideas? Here are a few: Write a play for a new attack vector, update an existing playbook item, freshin' up our wiki documentation, implement a new CSB feature, hunt through our logs and find a previously undetected compromise, discover a gap in our log collection, add Zabbix monitoring checks, build a Splunk dashboard, etc.</p> <p>Submit entries, ideas, and questions to somemailinglist@email.com</p>		

Innovation Hub/Dashboard

CSIRT Innovation Challenge

Innovation Challenge	Winner(s)	Solution
<p>Improving the Security of Cisco's AWS Presence</p> <p>inactive Stakeholders level 4 Expires 2019-04-30</p> <p>Cloud presence continues to grow and so does our need for continuous security improvements in this environment. [redacted] Here's the challenge - As a global team, let's align ourselves to the common goal of improving the maturity of our Cloud Incident Response efforts. The most impactful contribution wins the bounty! Keep this in mind - Incident Response requires many different job functions and areas of expertise. This is for everyone - Project Managers, Analysts, Engineers, and Investigators.</p> <p>Looking for ideas? Here are a few: Write a play for a new attack vector, update an existing playbook item, freshin' up our wiki documentation, implement a new CSB feature, hunt through our logs and find a previously undetected compromise, discover a gap in our log collection, add Zabbix monitoring checks, build a Splunk dashboard, etc.</p> <p>Submit entries, ideas, and questions to somemailinglist@email.com</p>	 	

Active/Inactive

- *Is this challenge open for submissions?*

Stakeholders

- *Who sponsored this challenge?*

Difficulty

- *Corresponds to reward level*

Expiration

- *When does this challenge end?*

Description

- *What is the scope of the challenge?*

Winner(s) + Solution

- *Who won? Why? What did they submit?*

Innovation Hub/Dashboard

CSIRT Innovation Challenge

Innovation Challenge	Winner(s)	Solution
Increasing the Security of Cisco's AWS Presence Inactive Stakeholders Expires 2019-04-30 Cisco's Cloud presence continues to grow and so does our need for continuous security improvements in this environment. [redacted] Here's the challenge - As a global team, let's align ourselves to the common goal of improving the maturity of our Cloud Incident Response efforts. The most impactful contribution wins the bounty! Keep this in mind - Incident Response requires many different job functions and areas of expertise. This is for everyone - Project Managers, Analysts, Engineers, and Investigators. Looking for ideas? Here are a few: Write a play for a new attack vector, update an existing playbook item, freshin' up our wiki documentation, implement a new CSB feature, hunt through our logs and find a previously undetected compromise, discover a gap in our log collection, add Zabbix monitoring checks, build a Splunk dashboard, etc. Submit entries, ideas, and questions to somemailinglist@email.com	 	

Active/Inactive

- *Is this challenge open for submissions?*

Stakeholders

- *Who sponsored this challenge?*

Difficulty

- *Corresponds to reward level*

Expiration

- *When does this challenge end?*

Description

- *What is the scope of the challenge?*

Winner(s) + Solution

- *Who won? Why? What did they submit?*



Innovation Hub/Dashboard

CSIRT Innovation Challenge

Innovation Challenge	Winner(s)	Solution
Increasing the Security of Cisco's AWS Presence inactive stakeholder level 4 Expires 2019-04-30 Cisco's Cloud presence continues to grow and so does our need for continuous security improvements in this environment. [redacted] Here's the challenge - As a global team, let's align ourselves to the common goal of improving the maturity of our Cloud Incident Response efforts. The most impactful contribution wins the bounty! Keep this in mind - Incident Response requires many different job functions and areas of expertise. This is for everyone - Project Managers, Analysts, Engineers, and Investigators. Looking for ideas? Here are a few: Write a play for a new attack vector, update an existing playbook item, freshin' up our wiki documentation, implement a new CSB feature, hunt through our logs and find a previously undetected compromise, discover a gap in our log collection, add Zabbix monitoring checks, build a Splunk dashboard, etc. Submit entries, ideas, and questions to somemailinglist@email.com	 	

Active/Inactive

- *Is this challenge open for submissions?*

Stakeholders

- *Who sponsored this challenge?*

Difficulty

- *Corresponds to reward level*

Expiration

- *When does this challenge end?*

Description

- *What is the scope of the challenge?*

Winner(s) + Solution

- *Who won? Why? What did they submit?*

Innovation Hub/Dashboard

CSIRT Innovation Challenge

Innovation Challenge	Winner(s)	Solution
Increasing the Security of Cisco's AWS Presence inactive stakeholders level Expires 2019-04-30 Cisco's Cloud presence continues to grow and so does our need for continuous security improvements in this environment. [redacted] Here's the challenge - As a global team, let's align ourselves to the common goal of improving the maturity of our Cloud Incident Response efforts. The most impactful contribution wins the bounty! Keep this in mind - Incident Response requires many different job functions and areas of expertise. This is for everyone - Project Managers, Analysts, Engineers, and Investigators. Looking for ideas? Here are a few: Write a play for a new attack vector, update an existing playbook item, freshin' up our wiki documentation, implement a new CSB feature, hunt through our logs and find a previously undetected compromise, discover a gap in our log collection, add Zabbix monitoring checks, build a Splunk dashboard, etc. Submit entries, ideas, and questions to somemailinglist@email.com	 	

Active/Inactive

- *Is this challenge open for submissions?*

Stakeholders

- *Who sponsored this challenge?*

Difficulty

- *Corresponds to reward level*

Expiration

- *When does this challenge end?*

Description

- *What is the scope of the challenge?*

Winner(s) + Solution

- *Who won? Why? What did they submit?*

Innovation Hub/Dashboard

CSIRT Innovation Challenge

Innovation Challenge	Winner(s)	Solution
Increasing the Security of Cisco's AWS Presence inactive stakeholders level 4 Expires 2019-04-30 Cisco's Cloud presence continues to grow and so does our need for continuous security improvements in this environment. [redacted] Here's the challenge - As a global team, let's align ourselves to the common goal of improving the maturity of our Cloud Incident Response efforts. The most impactful contribution wins the bounty! Keep this in mind - Incident Response requires many different job functions and areas of expertise. This is for everyone - Project Managers, Analysts, Engineers, and Investigators. Looking for ideas? Here are a few: Write a play for a new attack vector, update an existing playbook item, freshin' up our wiki documentation, implement a new CSB feature, hunt through our logs and find a previously undetected compromise, discover a gap in our log collection, add Zabbix monitoring checks, build a Splunk dashboard, etc. Submit entries, ideas, and questions to somemailinglist@email.com	 	

Active/Inactive

- *Is this challenge open for submissions?*

Stakeholders

- *Who sponsored this challenge?*

Difficulty

- *Corresponds to reward level*

Expiration

- *When does this challenge end?*

Description

- *What is the scope of the challenge?*

Winner(s) + Solution

- *Who won? Why? What did they submit?*



Innovation Hub/Dashboard

CSIRT Innovation Challenge

Innovation Challenge

Increasing the Security of Cisco's AWS Presence

inactive **stakeholders** **level 4** Expires 2019-04-30

Cisco's Cloud presence continues to grow and so does our need for continuous security improvements in this environment. [redacted] Here's the challenge - As a global team, let's align ourselves to the common goal of improving the maturity of our Cloud Incident Response efforts. The most impactful contribution wins the bounty! Keep this in mind - Incident Response requires many different job functions and areas of expertise. This is for everyone - Project Managers, Analysts, Engineers, and Investigators.

Looking for ideas? Here are a few: Write a play for a new attack vector, update an existing playbook item, freshin' up our wiki documentation, implement a new CSB feature, hunt through our logs and find a previously undetected compromise, discover a gap in our log collection, add Zabbix monitoring checks, build a Splunk dashboard, etc.

Submit entries, ideas, and questions to somemailinglist@email.com

Winner(s)	Solution

Active/Inactive

- *Is this challenge open for submissions?*

Stakeholders

- *Who sponsored this challenge?*

Difficulty

- *Corresponds to reward level*

Expiration

- *When does this challenge end?*

Description

- *What is the scope of the challenge?*

Winner(s) + Solution

- *Who won? Why? What did they submit?*



CSIRT Innovation Challenge

Winning contribution from the April 2019 Innovation Challenge

The Challenge

Cisco's Cloud presence continues to grow and so does our need for continuous security improvements in this environment. As a global team, let's align ourselves to the common goal of improving the maturity of our Cloud IR efforts.



1 Winning Solution

A novel detection technique for finding and alerting on API calls coming from unusual IP spaces (typically outside Cisco or AWS). Also includes proposal for proactive enumeration of ACLs attached to programmatic users.



Impact 3...

Automated alerts & reporting directly to tenant owners.

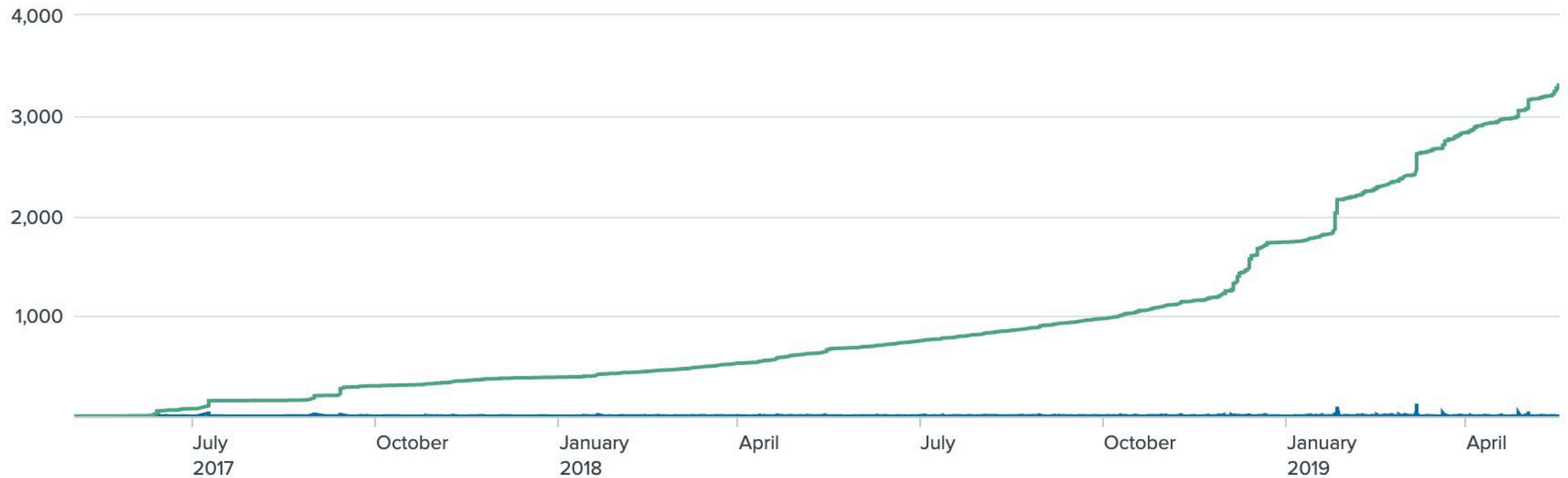
Impact 2...

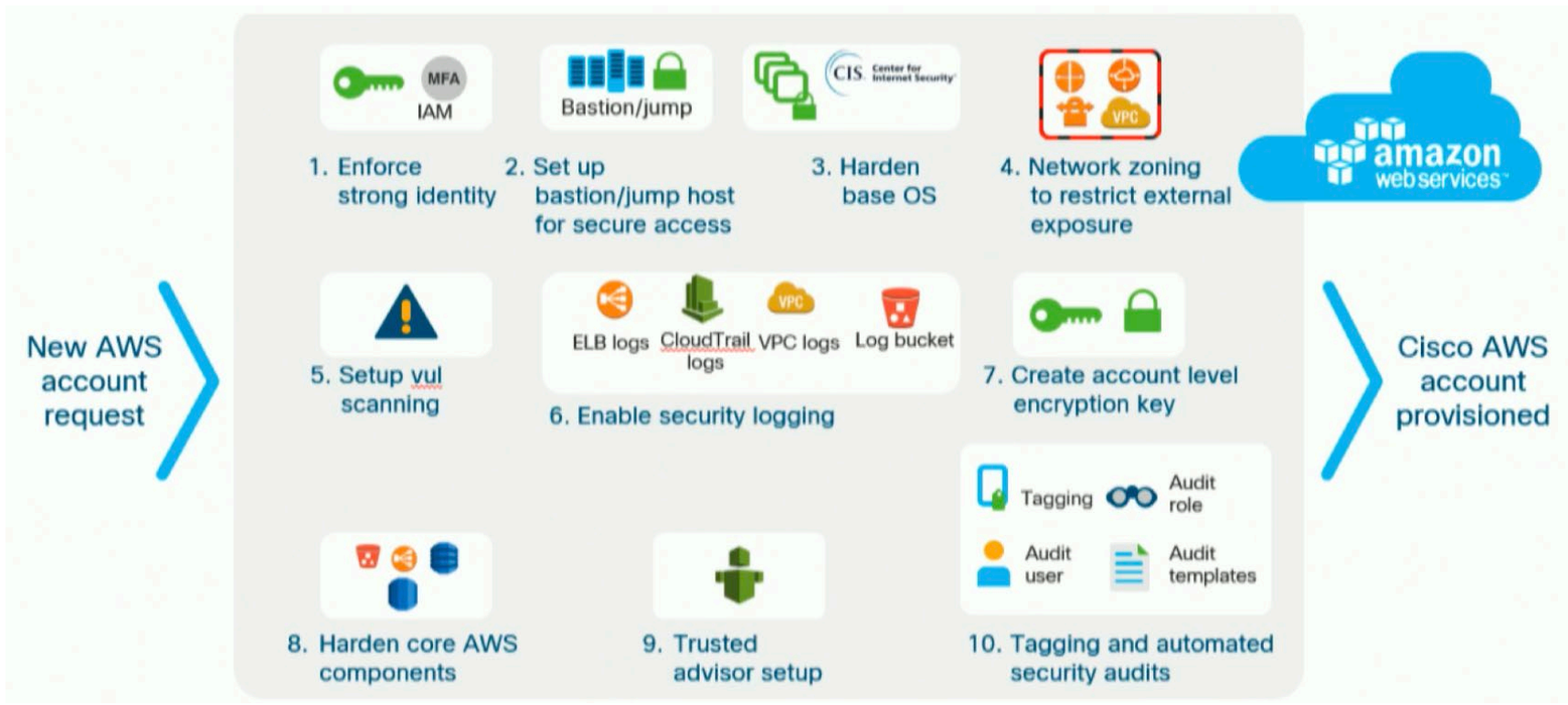
Provides additional visibility into our Cloud "API Footprint".

Impact 1...

This contribution was a direct result of an incident.

Growing Cloud Presence







Overall Risk Score:



Security Metrics



Section	Section Score
1. Identity and Access Management	- 100/100
2. Network Security	- 90/100
3. Storage (S3 buckets)	- 100/100
4. Tagging	- 90/100
5. External Vulnerabilities	- 100/100
6. CIS AWS Benchmarks	- 100/100
7. Trusted Advisor Checks	- Not Scored

CSIRT Innovation Challenge

Winning contribution from the April 2019 Innovation Challenge

The Challenge

Cisco's Cloud presence continues to grow and so does our need for continuous security improvements in this environment. As a global team, let's align ourselves to the common goal of improving the maturity of our Cloud IR efforts.



Impact 3...

Automated alerts & reporting directly to tenant owners.

Impact 2...

Provides additional visibility into our Cloud "API Footprint".

Impact 1...

This contribution was a direct result of an incident.

1 Winning Solution

A novel detection technique for finding and alerting on API calls coming from unusual IP spaces (typically outside Cisco or AWS). Also includes proposal for proactive enumeration of ACLs attached to programmatic users.

Over a period of 90 days, there were **84,751,672** 'AwsApiCall' events originating from 1400+ AWS accounts, sourced from **3,155** different ip addresses. **353** of those IP addresses originate from outside Cisco and Amazon.



CSIRT Innovation Challenge

Winning contribution from the April 2019 Innovation Challenge

The Challenge

Cisco's Cloud presence continues to grow and so does our need for continuous security improvements in this environment. As a global team, let's align ourselves to the common goal of improving the maturity of our Cloud IR efforts.



Impact 3...

Automated alerts & reporting directly to tenant owners.

Impact 2...

Provides additional visibility into our Cloud "API Footprint".

Impact 1...

This contribution was a direct result of an incident.

1 Winning Solution

A novel detection technique for finding and alerting on API calls coming from unusual IP spaces (typically outside Cisco or AWS). Also includes proposal for proactive enumeration of ACLs attached to programmatic users.

CSIRT Innovation Challenge

*Here's what we've **learned** from implementing and running the challenge*



Three...

Motivating people is hard, and people are motivated by different things.

Two...

We have existing momentum we must overcome and this will take time.

One...

Ideas are (mostly) useless without execution.



INNOVATION

JUST BECAUSE SOMETHING IS INNOVATIVE,
DOESN'T MEAN IT'S A GOOD IDEA.



How do *you* address the challenges of training
& development?

