Leveling Up Security @ Riot

2015 v 2018

AGENDA

- Who
- 2015
- 2018
- Getting to the Nexus

Who Am I?

🇮🇪

🐦 @markofu

Older than I'd like to imagine

Do InfoSec stuff

Would rather be 🏄

MORE THAN
100 MILLION

MONTHLY ACTIVE PLAYERS

MORE THAN
27 MILLION

DAILY ACTIVE PLAYERS

7.5 MILLION

PEAK CONCURRENT PLAYERS

eSports

Who Are We?

OUR MISSION

WE ASPIRE
TO BE THE MOST
PLAYER
FOCUSED
GAME COMPANY IN THE
WORLD

AGENDA

- Who
- 2015
- 2018
- Getting to the Nexus

Important Security Update and Password Reset

BY TRYNDAMERE

The security of your information is critically important to us, so we're really sorry to share that a portion of our North American account information was recently compromised.

What we know: usernames, email addresses, salted password hashes, and some first and last names were accessed. This means that the password files are unreadable, but players with easily guessable

Related Content

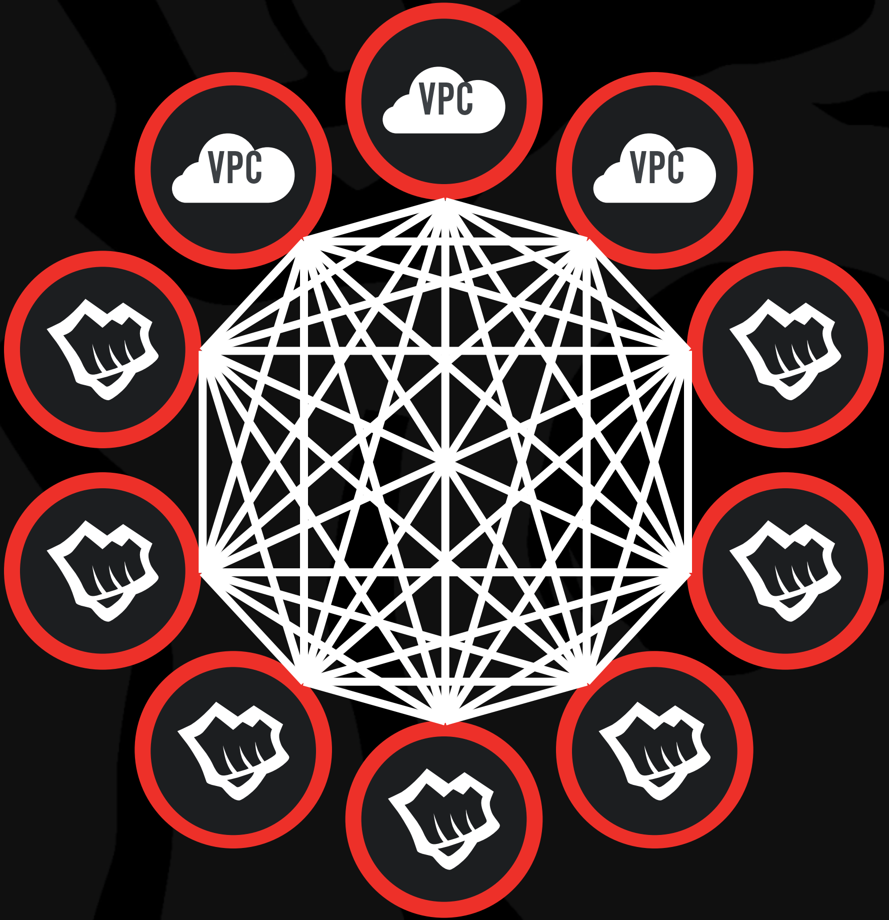
Privacy policy update

Digital RP Codes on Amazon

Riot Games Engineering Blog

IR

AWS



!!

# of VPNs

What brought us agility also brought us the Wild Wild West of Computing

If security introduces **blocking** to the org, it will be **ignored**, not embraced

The first recipients of the reward are Rioters who saw something suspicious, went above and beyond to make their project as secure as possible, or helped Riot as a whole stay secure. These awesome dudes & dudettes will receive a token of our appreciation that matches their mega-sized dedication to security!

Here’s the first batch of Rioters who received our Gnarly Security Award!

RFCs=Tech Design

RFC Feedback

Not an approval process, it’s about receiving advice!

Received comments & iterate through the draft

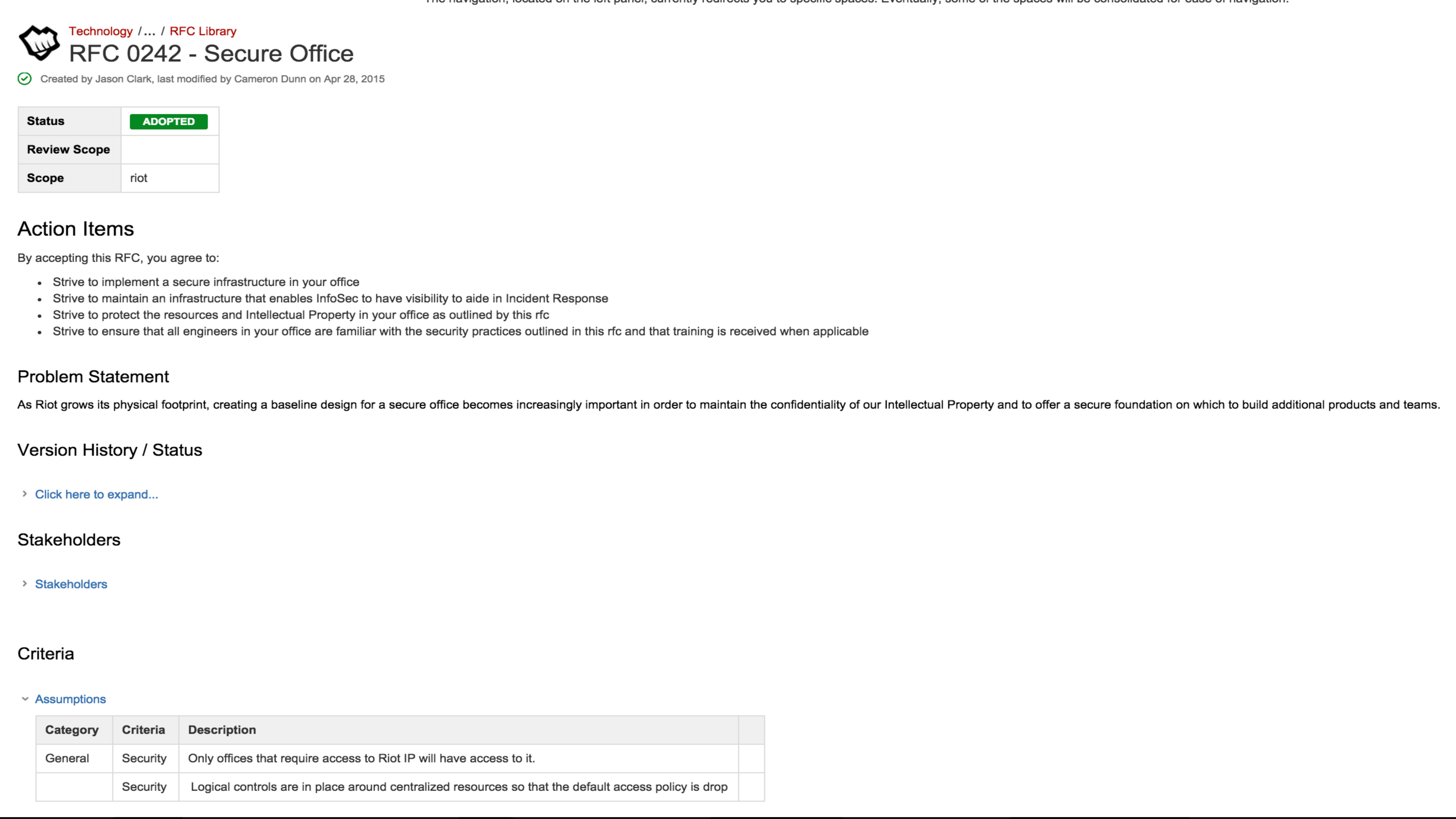
Becomes a standard through adoption @ scopes

RFC0242

Goal :: Alignment with Rioters on a secure standard for our office builds, with our offices being treated as code

Why :: We had no visibility and couldn’t do Incident Response effectively

How :: Document, Receive Feedback, Iterate & ultimately create a defendable network capable of alerting and forensics



The navigation, located on the left panel, currently redirects you to specific spaces. Eventually, some of the spaces will be consolidated for ease of navigation.

Technology / ... / RFC Library

RFC 0242 - Secure Office

Created by Jason Clark, last modified by Cameron Dunn on Apr 28, 2015

Status	ADOPTED
Review Scope	
Scope	riot

Action Items

By accepting this RFC, you agree to:

- Strive to implement a secure infrastructure in your office
- Strive to maintain an infrastructure that enables InfoSec to have visibility to aide in Incident Response
- Strive to protect the resources and Intellectual Property in your office as outlined by this rfc
- Strive to ensure that all engineers in your office are familiar with the security practices outlined in this rfc and that training is received when applicable

Problem Statement

As Riot grows its physical footprint, creating a baseline design for a secure office becomes increasingly important in order to maintain the confidentiality of our Intellectual Property and to offer a secure foundation on which to build additional products and teams.

Version History / Status

› Click here to expand...

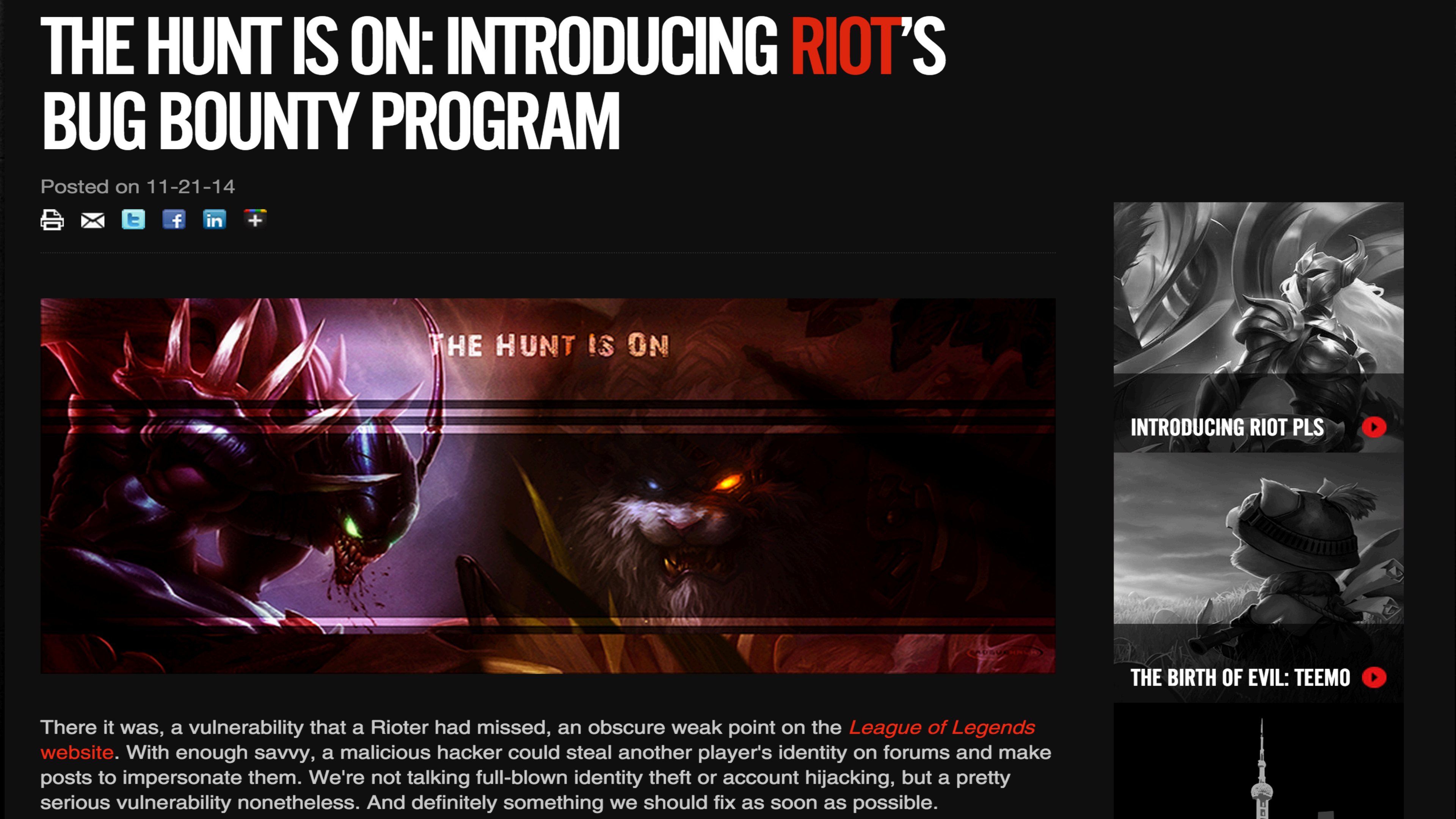
Stakeholders

› Stakeholders

Criteria

⌄ Assumptions

Category	Criteria	Description	
General	Security	Only offices that require access to Riot IP will have access to it.	
	Security	Logical controls are in place around centralized resources so that the default access policy is drop	



THE HUNT IS ON: INTRODUCING RIOT'S BUG BOUNTY PROGRAM

Posted on 11-21-14

There it was, a vulnerability that a Rioter had missed, an obscure weak point on the *League of Legends* website. With enough savvy, a malicious hacker could steal another player's identity on forums and make posts to impersonate them. We're not talking full-blown identity theft or account hijacking, but a pretty serious vulnerability nonetheless. And definitely something we should fix as soon as possible.

AGENDA

- Who
- 2015
- 2018
- Getting to the Nexus

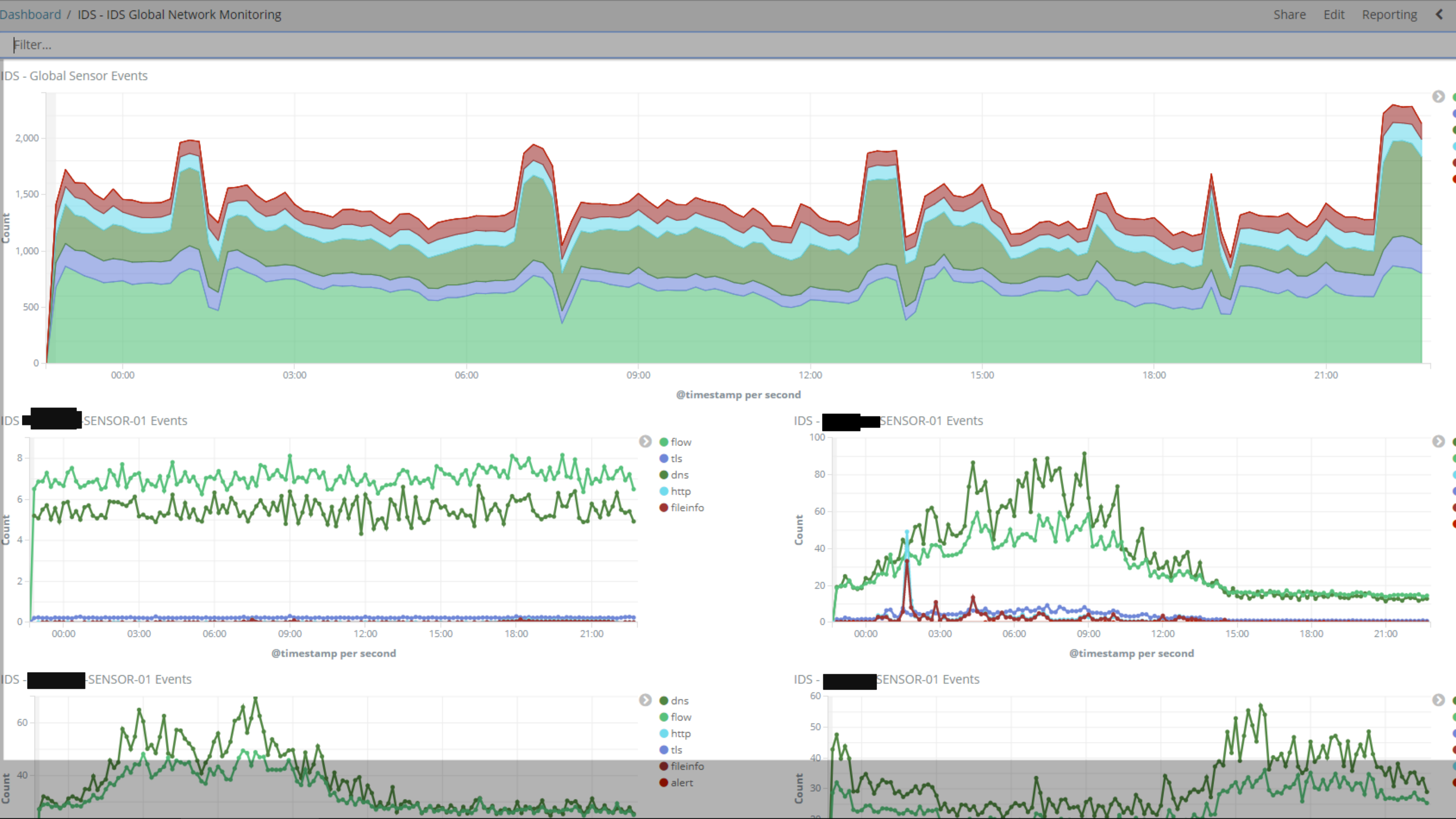
Team

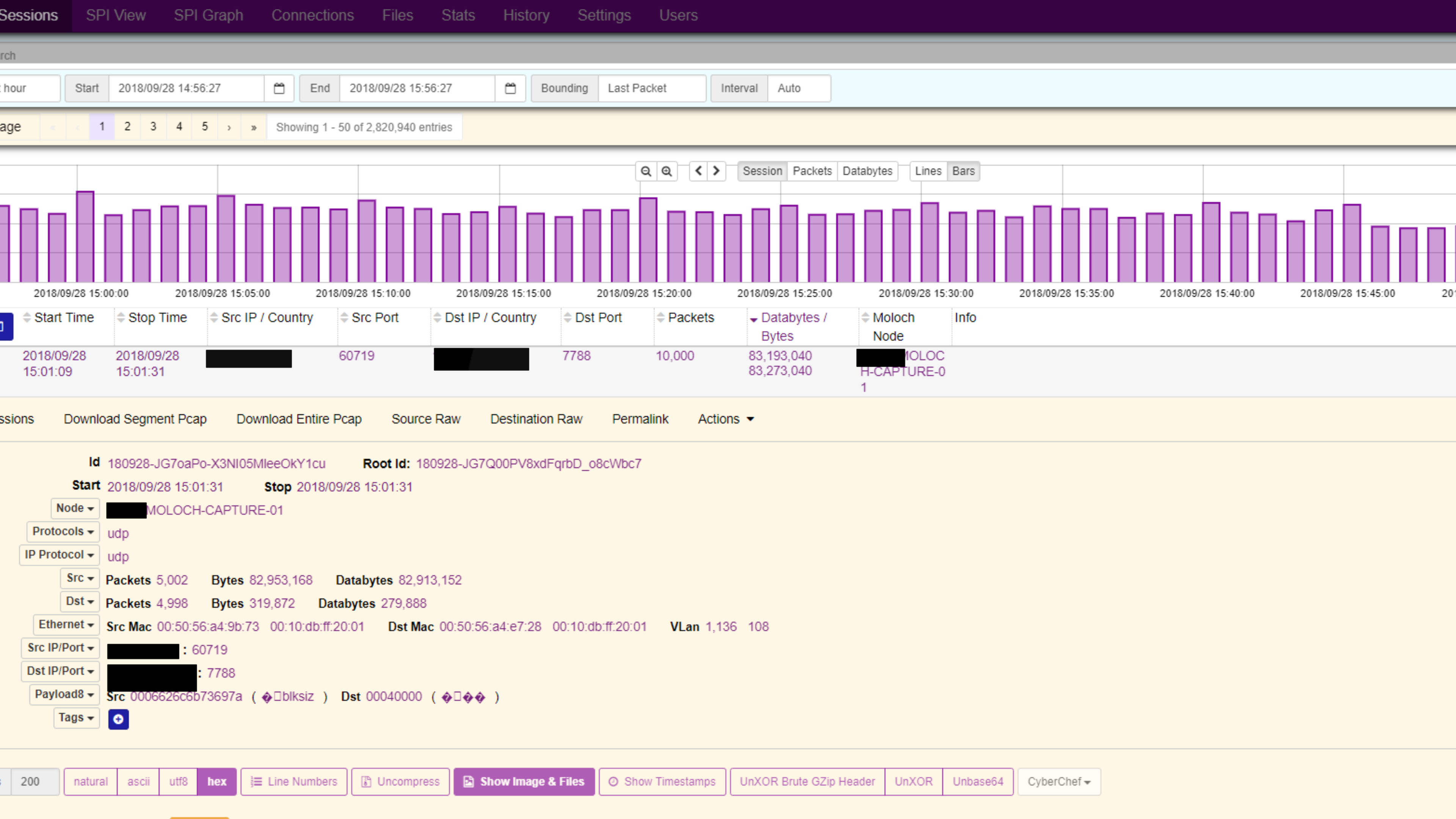
RFC0242

Where :: All offices worldwide (mandatory for code access)

How :: Automation & lots of air miles

What :: Centralised logging, Visibility, “Office as Code” & Threat Intel


Dashboard / IDS - IDS Global Network Monitoring
Share
Edit
Reporting
Filter...
IDS - Global Sensor Events
Count
0
500
1,000
1,500
2,000
00:00
03:00
06:00
09:00
12:00
15:00
18:00
21:00
@timestamp per second
IDS [redacted] SENSOR-01 Events
flow
tls
dns
http
fileinfo
Count
0
2
4
6
8
00:00
03:00
06:00
09:00
12:00
15:00
18:00
21:00
@timestamp per second
IDS - [redacted] SENSOR-01 Events
Count
0
20
40
60
80
100
00:00
03:00
06:00
09:00
12:00
15:00
18:00
21:00
@timestamp per second
IDS - [redacted] SENSOR-01 Events
dns
flow
http
tls
fileinfo
alert
Count
40
60
IDS - [redacted] SENSOR-01 Events
Count
30
40
50
60



Start 2018/09/28 14:56:27

End 2018/09/28 15:56:27

Bounding Last Packet

Interval Auto

Showing 1 - 50 of 2,820,940 entries

Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Moloch Node	Info
2018/09/28 15:01:09	2018/09/28 15:01:31	[redacted]	60719	[redacted]	7788	10,000	83,193,040 83,273,040	[redacted]IOLOCH-CAPTURE-01	

Id 180928-JG7oaPo-X3NI05MleeOkY1cu Root Id: 180928-JG7Q00PV8xdFqrbD_o8cWbc7

Start 2018/09/28 15:01:31 Stop 2018/09/28 15:01:31

Node [redacted]MOLOCH-CAPTURE-01

Protocols udp

IP Protocol udp

Src Packets 5,002 Bytes 82,953,168 Databytes 82,913,152

Dst Packets 4,998 Bytes 319,872 Databytes 279,888

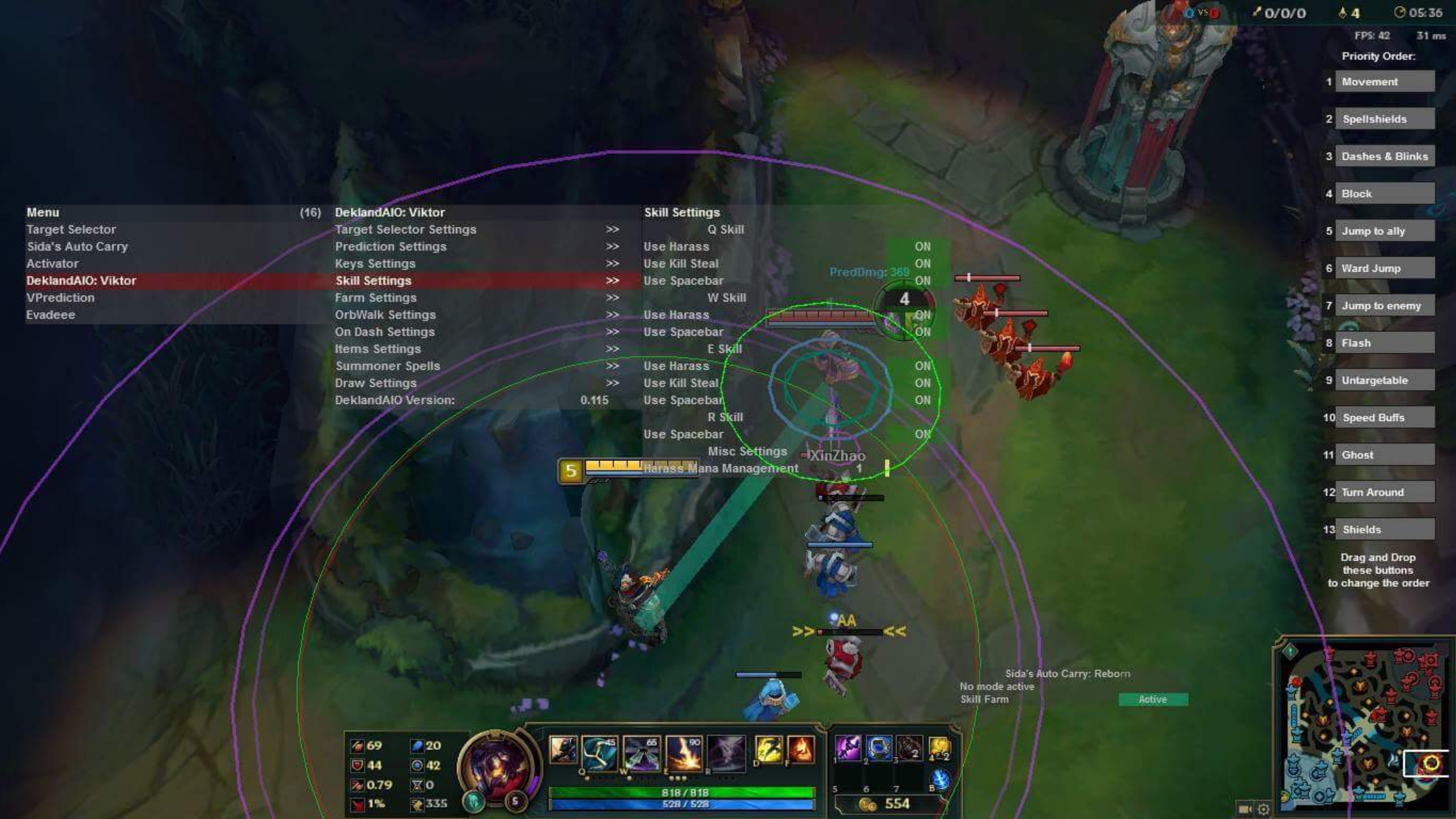
Ethernet Src Mac 00:50:56:a4:9b:73 00:10:db:ff:20:01 Dst Mac 00:50:56:a4:e7:28 00:10:db:ff:20:01 VLan 1,136 108

Src IP/Port [redacted] : 60719

Dst IP/Port [redacted]: 7788

Payload8 Src 0006626c6b73697a (�□blksiz) Dst 00040000 (�□��)

Tags



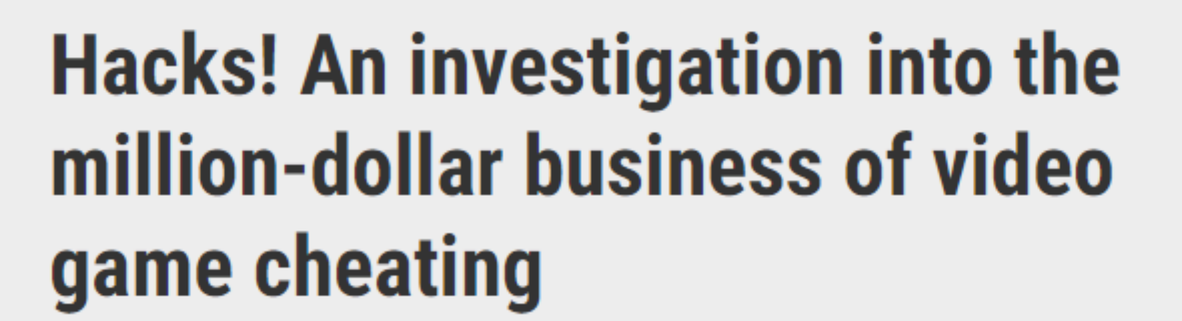
Menu (16)
Target Selector
Sida's Auto Carry
Activator
DeklandAIO: Viktor
VPrediction
Evadeee

DeklandAIO: Viktor
Target Selector Settings >>
Prediction Settings >>
Keys Settings >>
Skill Settings >>
Farm Settings >>
OrbWalk Settings >>
On Dash Settings >>
Items Settings >>
Summoner Spells >>
Draw Settings >>
DeklandAIO Version: 0.115

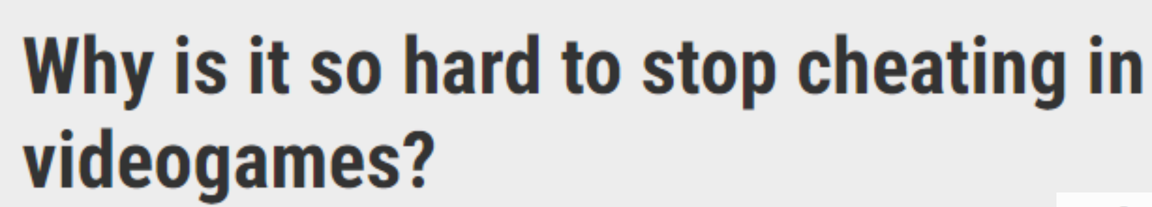
Skill Settings
Q Skill
Use Harass ON
Use Kill Steal ON
Use Spacebar ON
W Skill
Use Harass ON
Use Spacebar ON
E Skill
Use Harass ON
Use Kill Steal ON
Use Spacebar ON
R Skill
Use Spacebar ON
Misc Settings
Harass Mana Management 1

Priority Order:
1 Movement
2 Spellshields
3 Dashes & Blinks
4 Block
5 Jump to ally
6 Ward Jump
7 Jump to enemy
8 Flash
9 Untargetable
10 Speed Buffs
11 Ghost
12 Turn Around
13 Shields
Drag and Drop these buttons to change the order

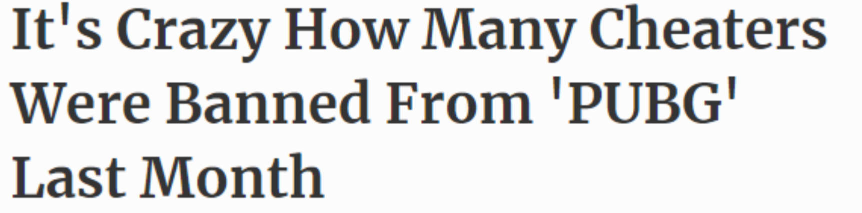
Sida's Auto Carry: Reborn
No mode active
Skill Farm Active



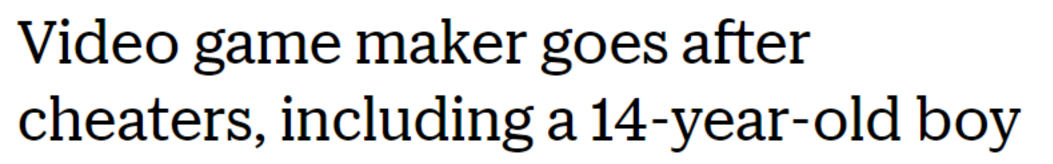
Hacks! An investigation into the million-dollar business of video game cheating



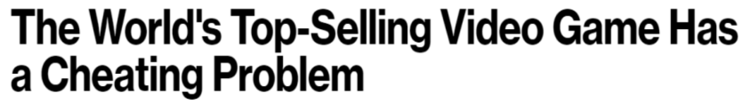
Why is it so hard to stop cheating in videogames?



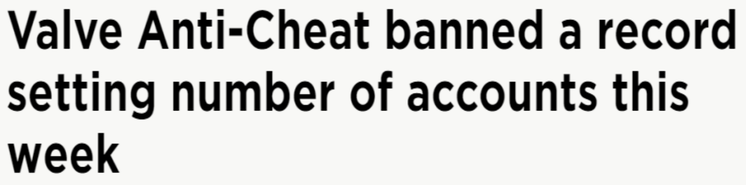
It's Crazy How Many Cheaters Were Banned From 'PUBG' Last Month



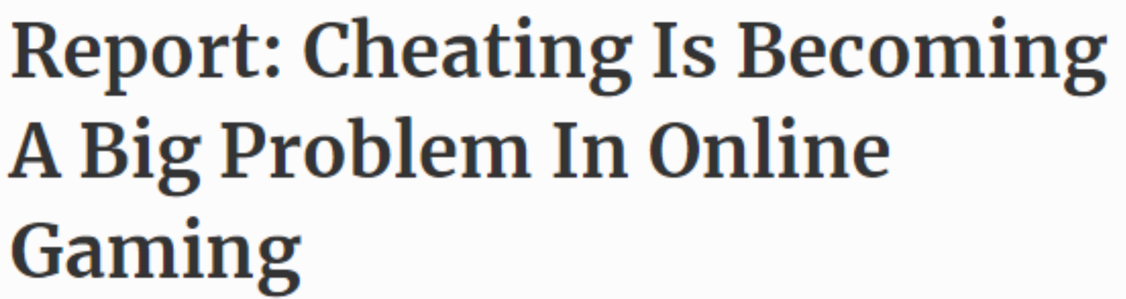
Video game maker goes after cheaters, including a 14-year-old boy



The World's Top-Selling Video Game Has a Cheating Problem

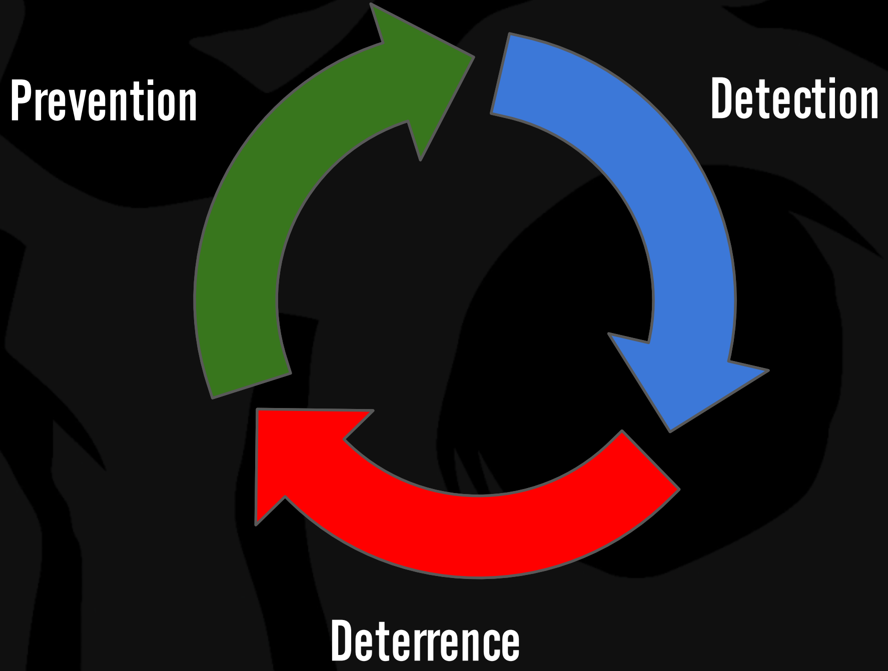


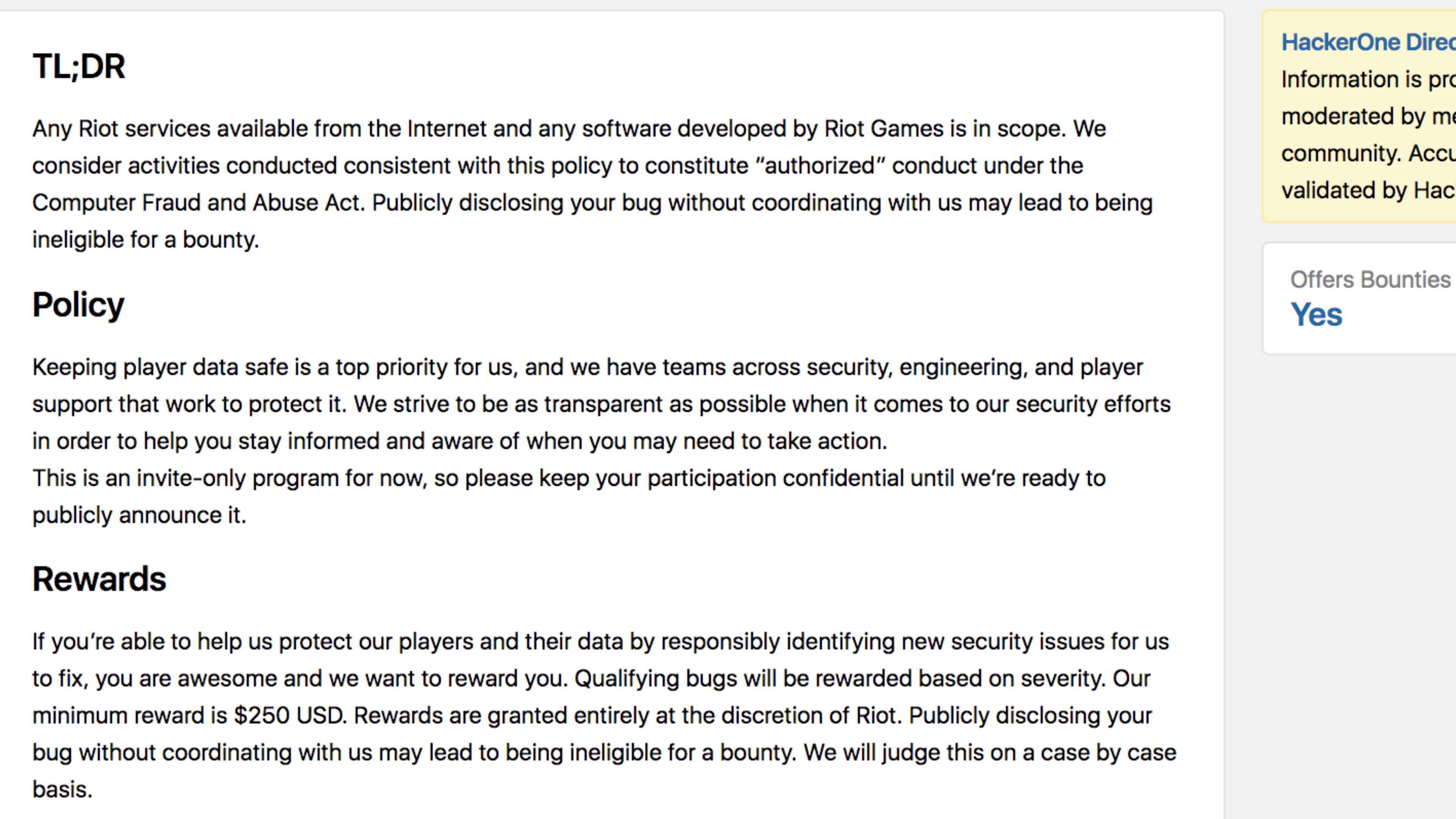
Valve Anti-Cheat banned a record setting number of accounts this week



Report: Cheating Is Becoming A Big Problem In Online Gaming

Strategy





TL;DR

Any Riot services available from the Internet and any software developed by Riot Games is in scope. We consider activities conducted consistent with this policy to constitute "authorized" conduct under the Computer Fraud and Abuse Act. Publicly disclosing your bug without coordinating with us may lead to being ineligible for a bounty.

Policy

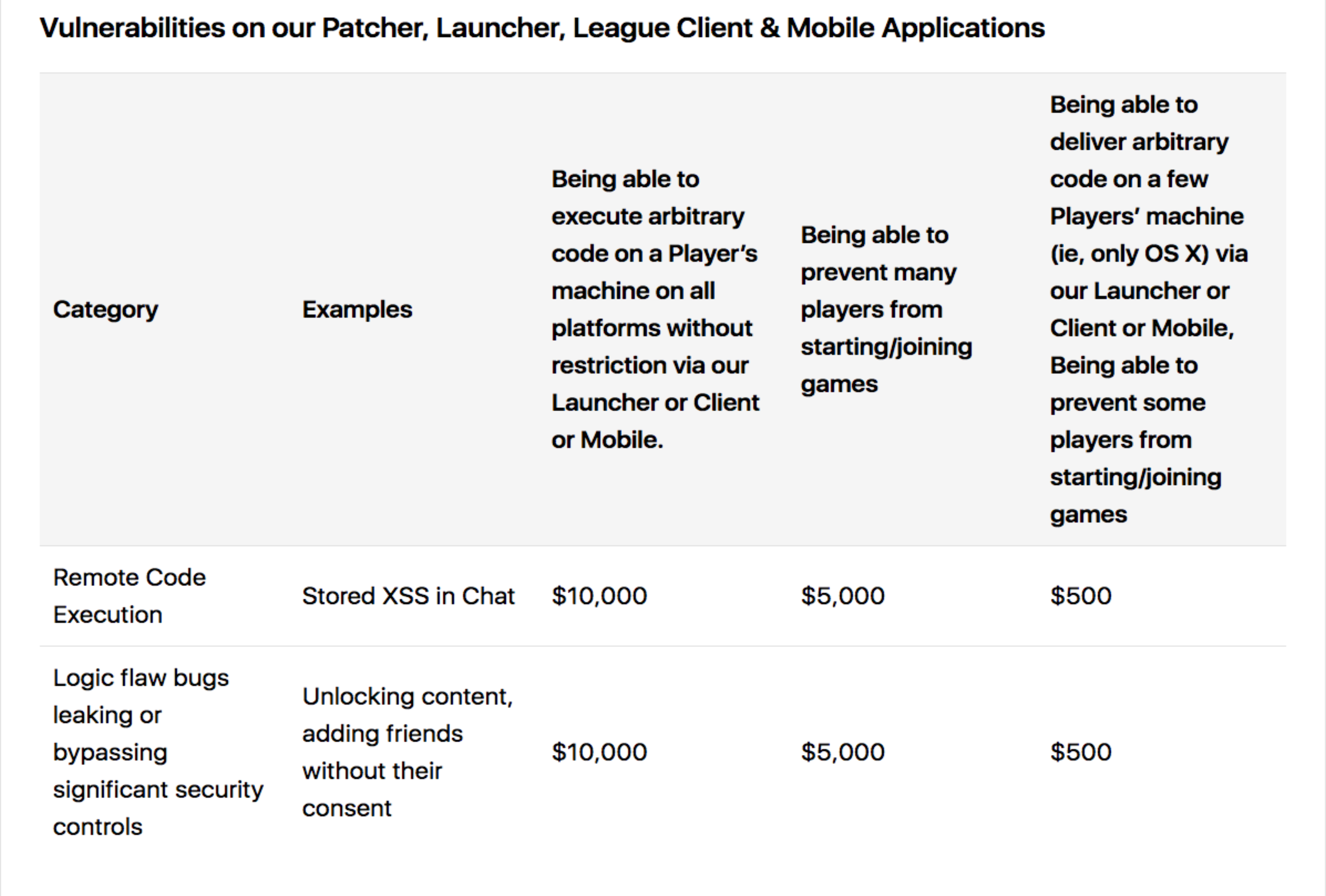
Keeping player data safe is a top priority for us, and we have teams across security, engineering, and player support that work to protect it. We strive to be as transparent as possible when it comes to our security efforts in order to help you stay informed and aware of when you may need to take action.
This is an invite-only program for now, so please keep your participation confidential until we're ready to publicly announce it.

Rewards

If you're able to help us protect our players and their data by responsibly identifying new security issues for us to fix, you are awesome and we want to reward you. Qualifying bugs will be rewarded based on severity. Our minimum reward is $250 USD. Rewards are granted entirely at the discretion of Riot. Publicly disclosing your bug without coordinating with us may lead to being ineligible for a bounty. We will judge this on a case by case basis.

HackerOne Direc
Information is pro
moderated by me
community. Accu
validated by Hac

Offers Bounties
Yes



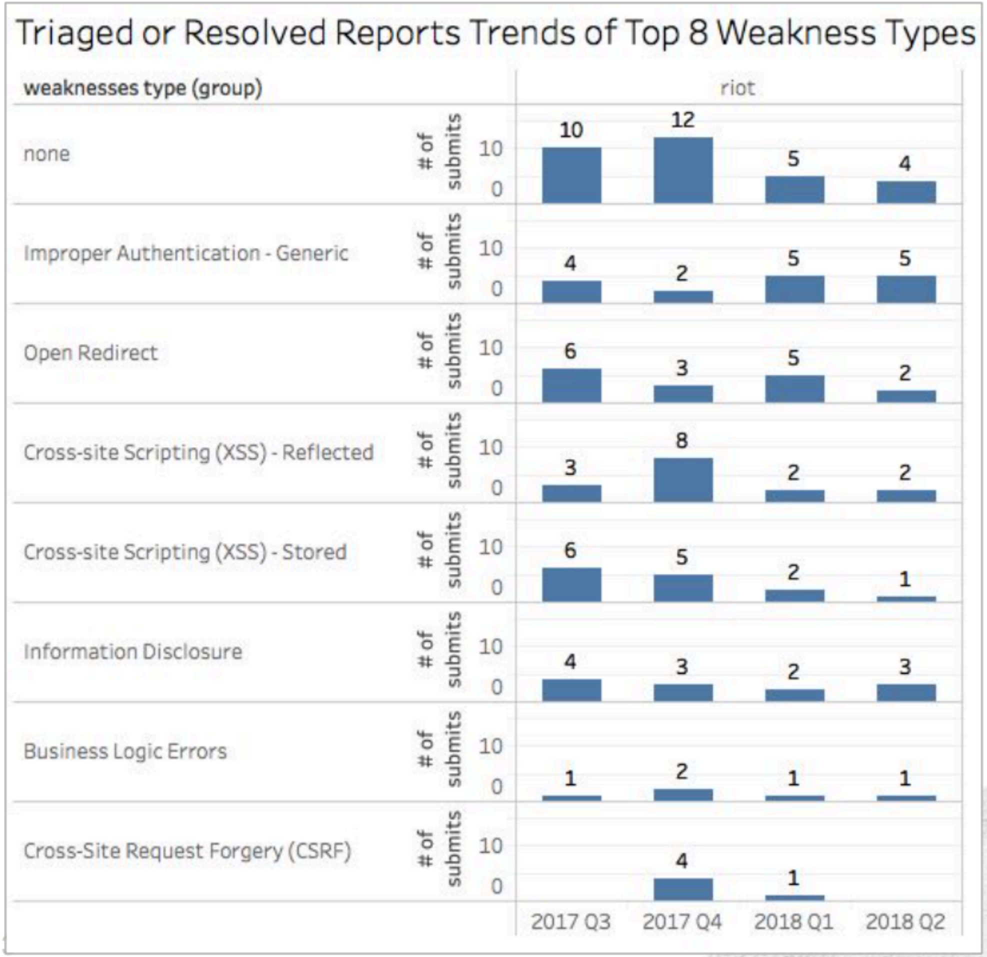
Vulnerabilities on our Patcher, Launcher, League Client & Mobile Applications

Category	Examples	Being able to execute arbitrary code on a Player's machine on all platforms without restriction via our Launcher or Client or Mobile.	Being able to prevent many players from starting/joining games	Being able to deliver arbitrary code on a few Players' machine (ie, only OS X) via our Launcher or Client or Mobile, Being able to prevent some players from starting/joining games
Remote Code Execution	Stored XSS in Chat	$10,000	$5,000	$500
Logic flaw bugs leaking or bypassing significant security controls	Unlocking content, adding friends without their consent	$10,000	$5,000	$500

Program Success

Top 8 Vulnerability Type Trends

Triaged & Resolved Reports



Increasing over time

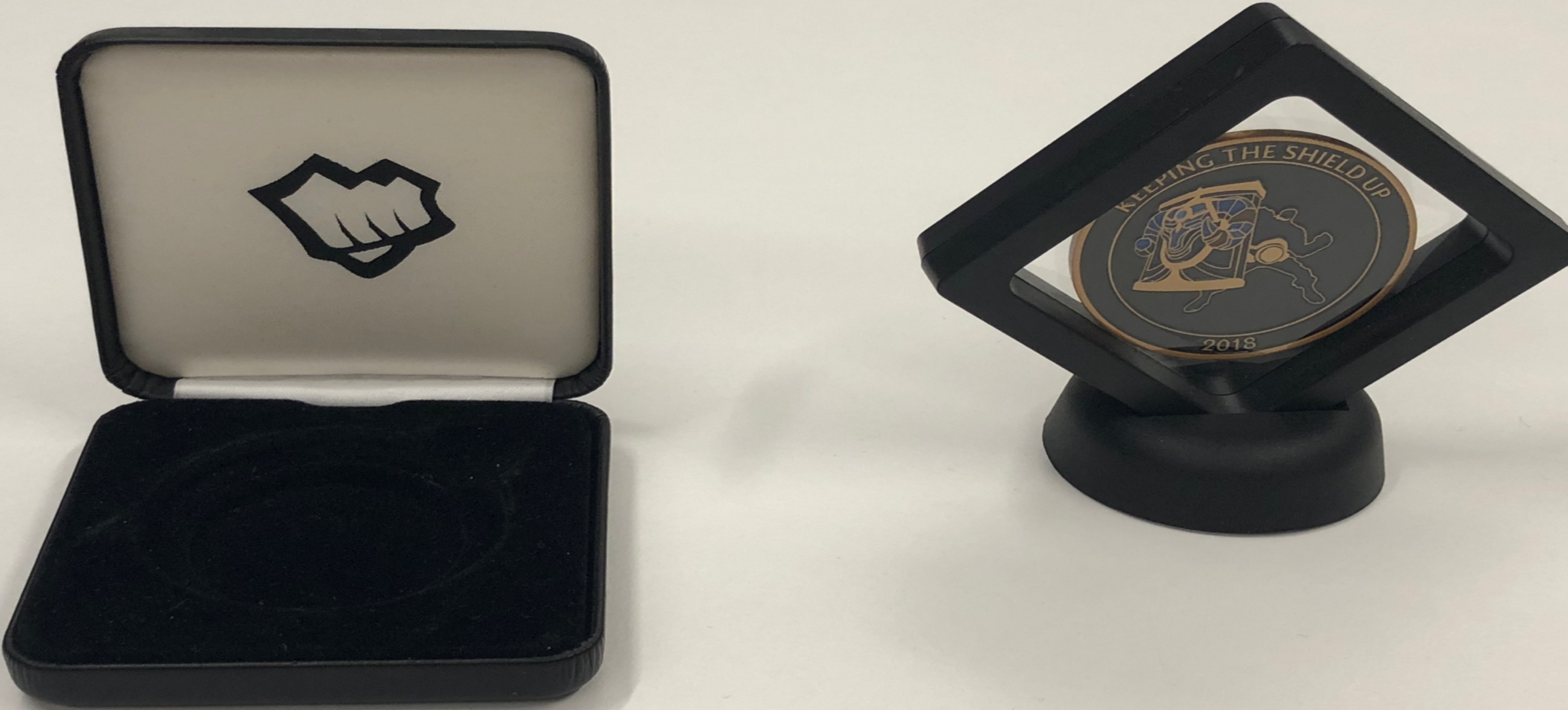
Improper Authentication

Stagnant over time

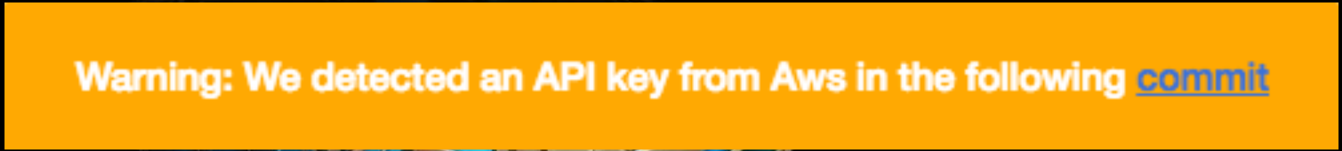
Open Redirect
Information Disclosure
Business Logic Errors

Decreasing over time

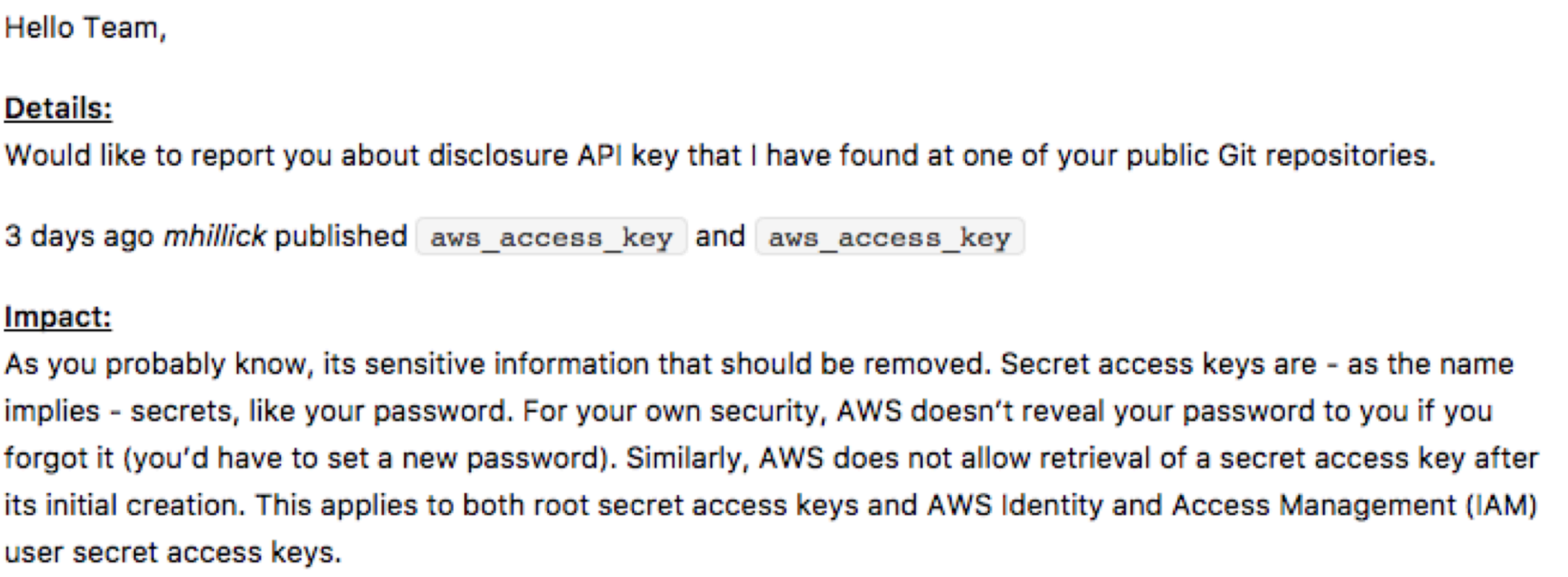
CSRF
XSS-Stored and Reflected


KEEPING THE SHIELD UP
2018

Secrets



Warning: We detected an API key from Aws in the following commit



Hello Team,

Details:

Would like to report you about disclosure API key that I have found at one of your public Git repositories.

3 days ago *mhillick* published `aws_access_key` and `aws_access_key`

Impact:

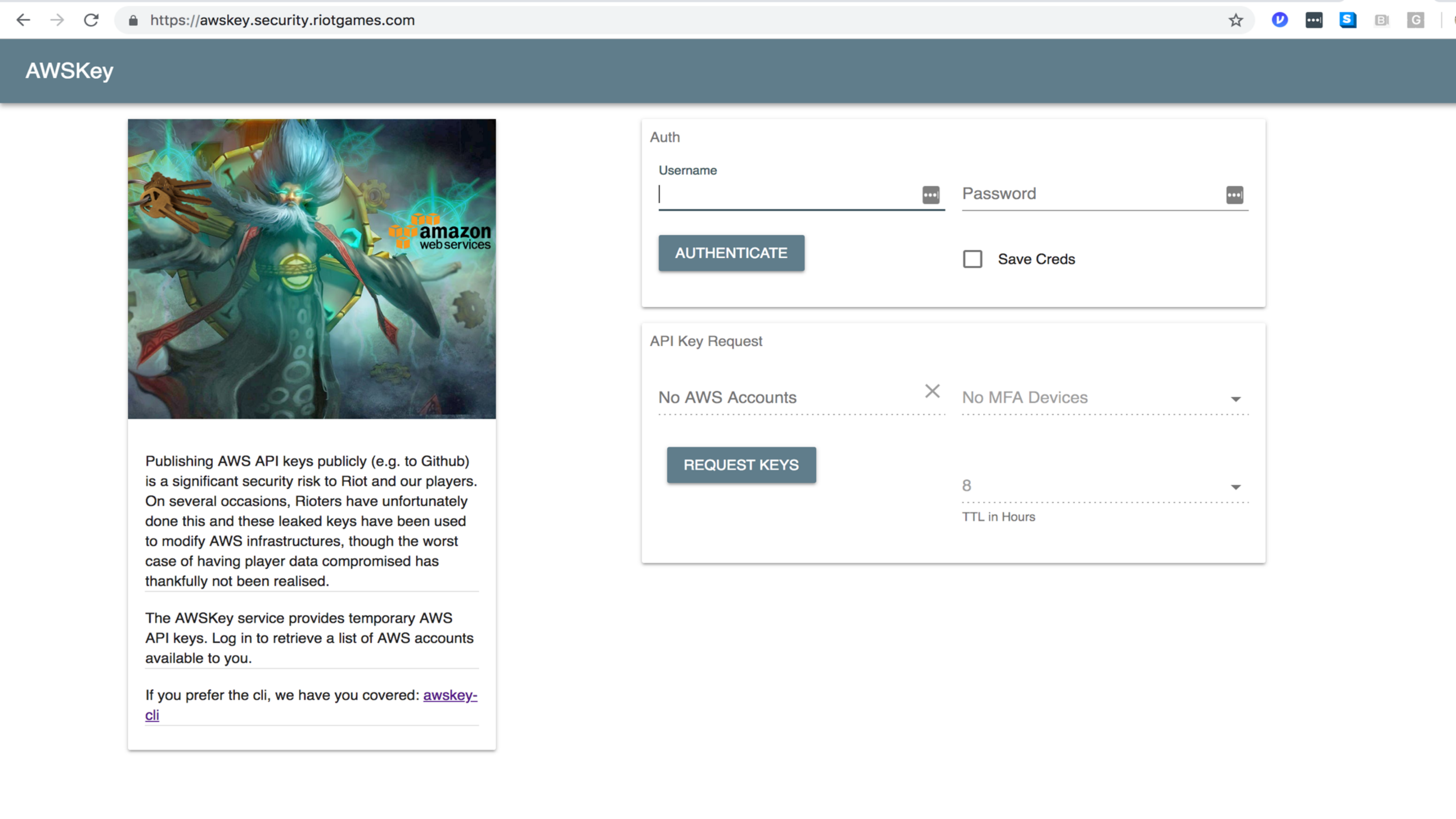
As you probably know, its sensitive information that should be removed. Secret access keys are - as the name implies - secrets, like your password. For your own security, AWS doesn't reveal your password to you if you forgot it (you'd have to set a new password). Similarly, AWS does not allow retrieval of a secret access key after its initial creation. This applies to both root secret access keys and AWS Identity and Access Management (IAM) user secret access keys.

AWSKey

Provides temporary AWS API tokens (via STS) & activity monitoring

~~Minimize~~ Remove the use of long-lived AWS API Keys => Less Impact

Metrics



AWSKey

Auth

Username

Password

AUTHENTICATE

□ Save Creds

API Key Request

No AWS Accounts

No MFA Devices

REQUEST KEYS

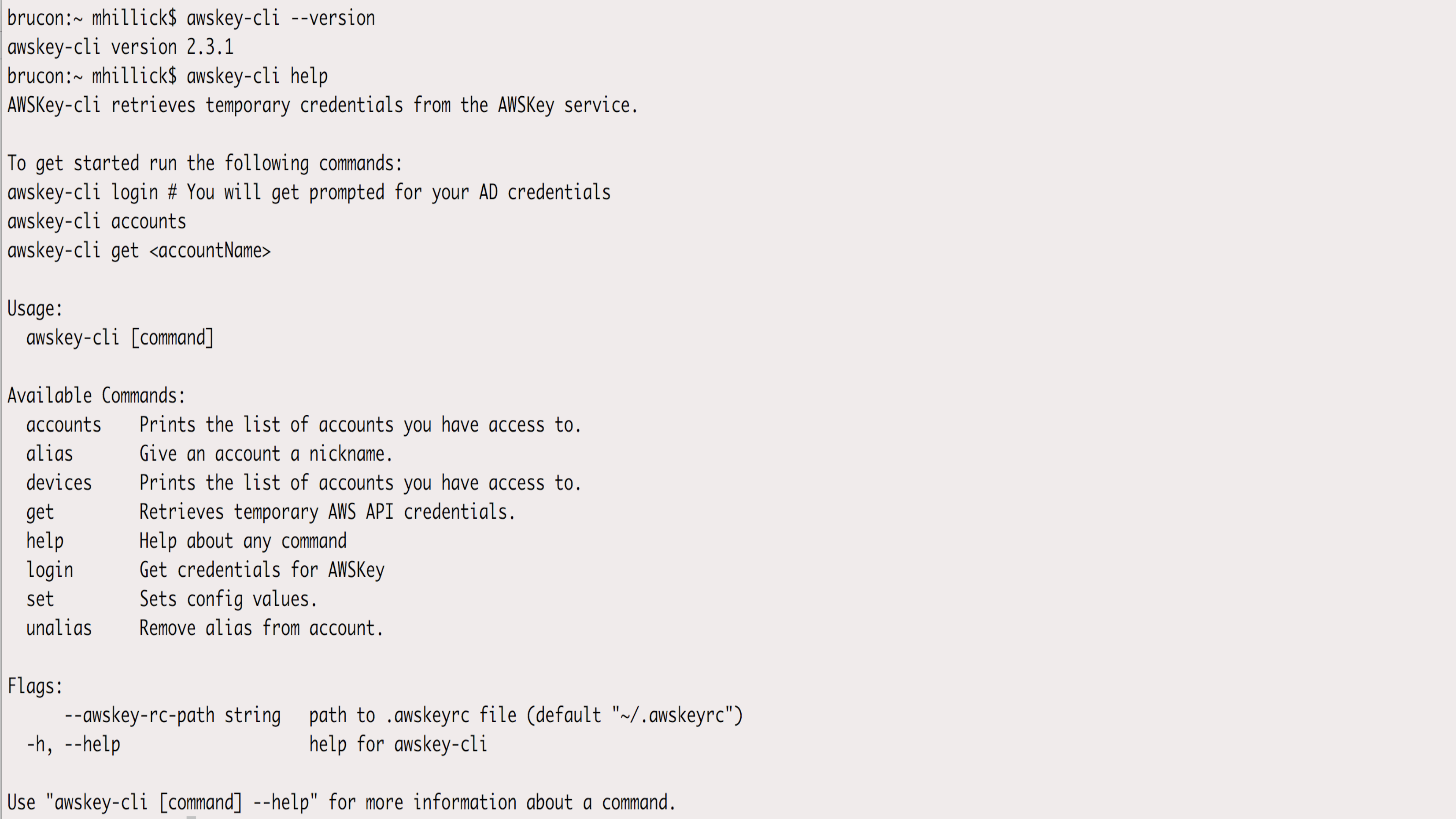
8

TTL in Hours

Publishing AWS API keys publicly (e.g. to Github) is a significant security risk to Riot and our players. On several occasions, Rioters have unfortunately done this and these leaked keys have been used to modify AWS infrastructures, though the worst case of having player data compromised has thankfully not been realised.

The AWSKey service provides temporary AWS API keys. Log in to retrieve a list of AWS accounts available to you.

If you prefer the cli, we have you covered: awskey-cli



```
brucon:~ mhillick$ awskey-cli --version
awskey-cli version 2.3.1
brucon:~ mhillick$ awskey-cli help
AWSKey-cli retrieves temporary credentials from the AWSKey service.

To get started run the following commands:
awskey-cli login # You will get prompted for your AD credentials
awskey-cli accounts
awskey-cli get <accountName>

Usage:
  awskey-cli [command]

Available Commands:
  accounts    Prints the list of accounts you have access to.
  alias       Give an account a nickname.
  devices     Prints the list of accounts you have access to.
  get         Retrieves temporary AWS API credentials.
  help        Help about any command
  login       Get credentials for AWSKey
  set         Sets config values.
  unalias     Remove alias from account.

Flags:
      --awskey-rc-path string   path to .awskeyrc file (default "~/.awskeyrc")
  -h, --help                    help for awskey-cli

Use "awskey-cli [command] --help" for more information about a command.
```

AWSKey Unique User Count

201

Unique Users

AWSKey Num Push Requests

4,372

Number of Push requests

AWSKey Num OTP Requests

75

Number of OTP requests

AWSKey Keys Generated

4,447

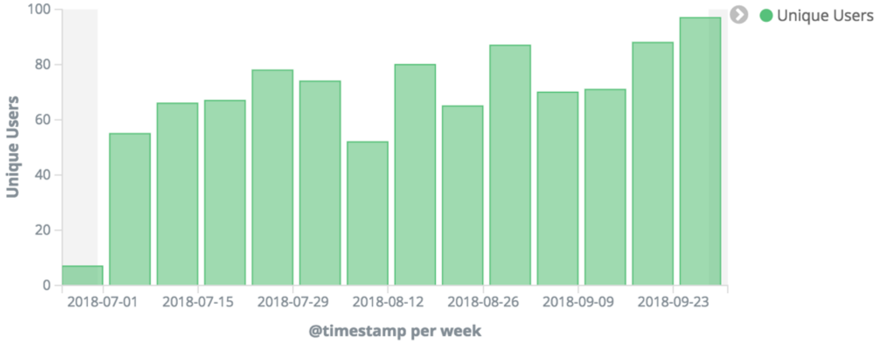
Keys Generated

AWSKey Total Logs

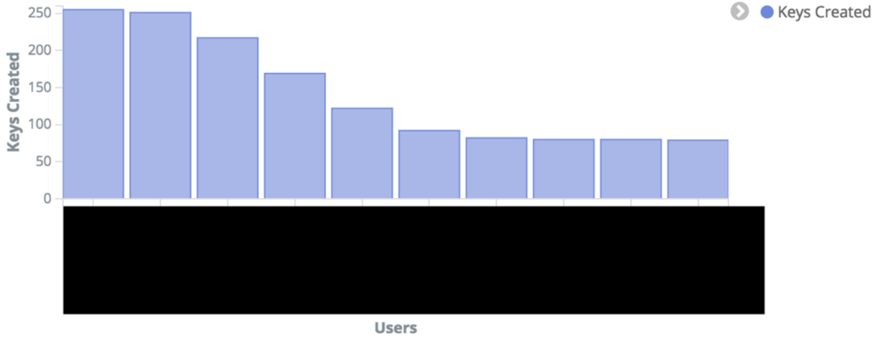
39,425

Total Logs

AWSKey Unique Users per Week

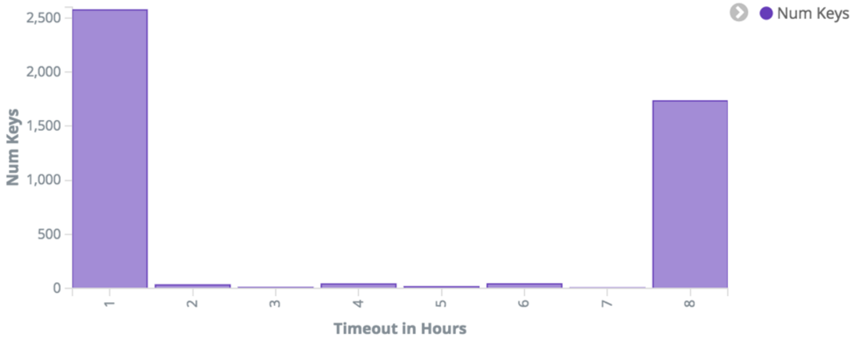


AWSKey Key Created

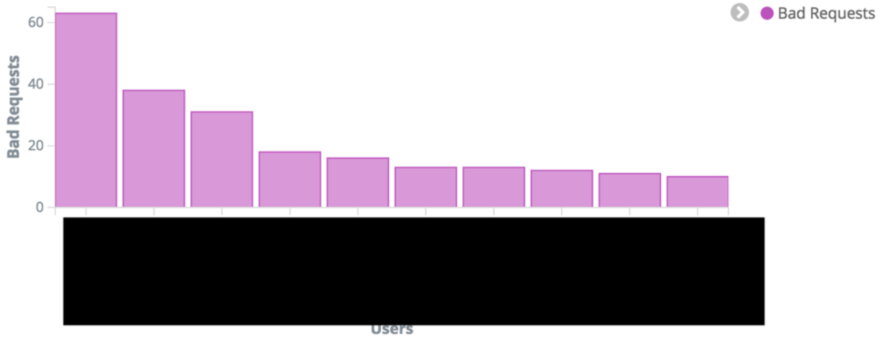


[redacted]

AWSKey KeyTimeouts



AWSKey Bad Requests



[redacted]

AWSKey User List

[redacted]

Cloud is Magic

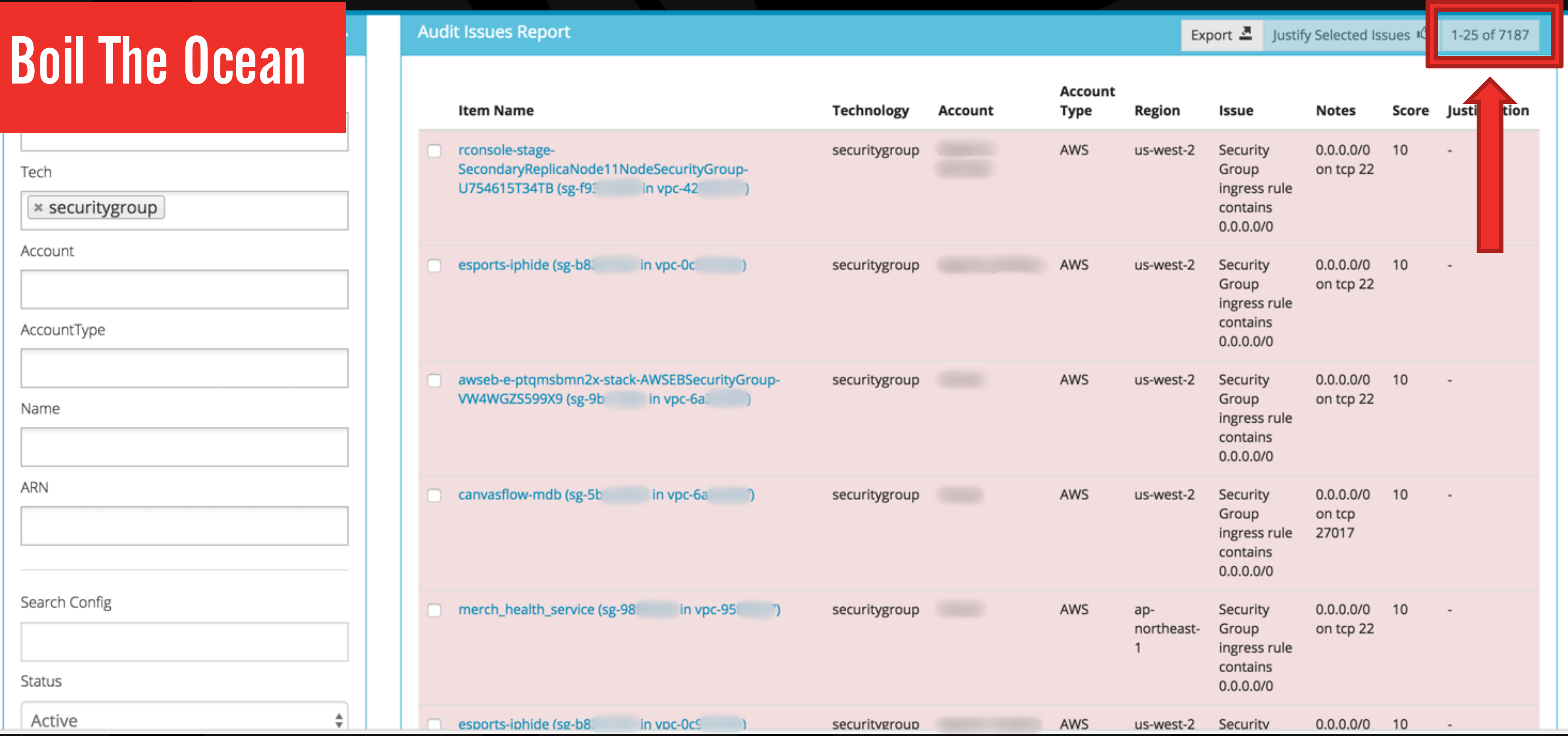
Storytime

Ownership

Problem Statement

While AWS is a great place to rapidly iterate and test new features, the vast number of accounts, instances and usage has no easy way of attributing a running instance back to an owner or feature.

Boil The Ocean



Tech

× securitygroup

Account

AccountType

Name

ARN

Search Config

Status

Active

Audit Issues Report

Export | Justify Selected Issues | 1-25 of 7187

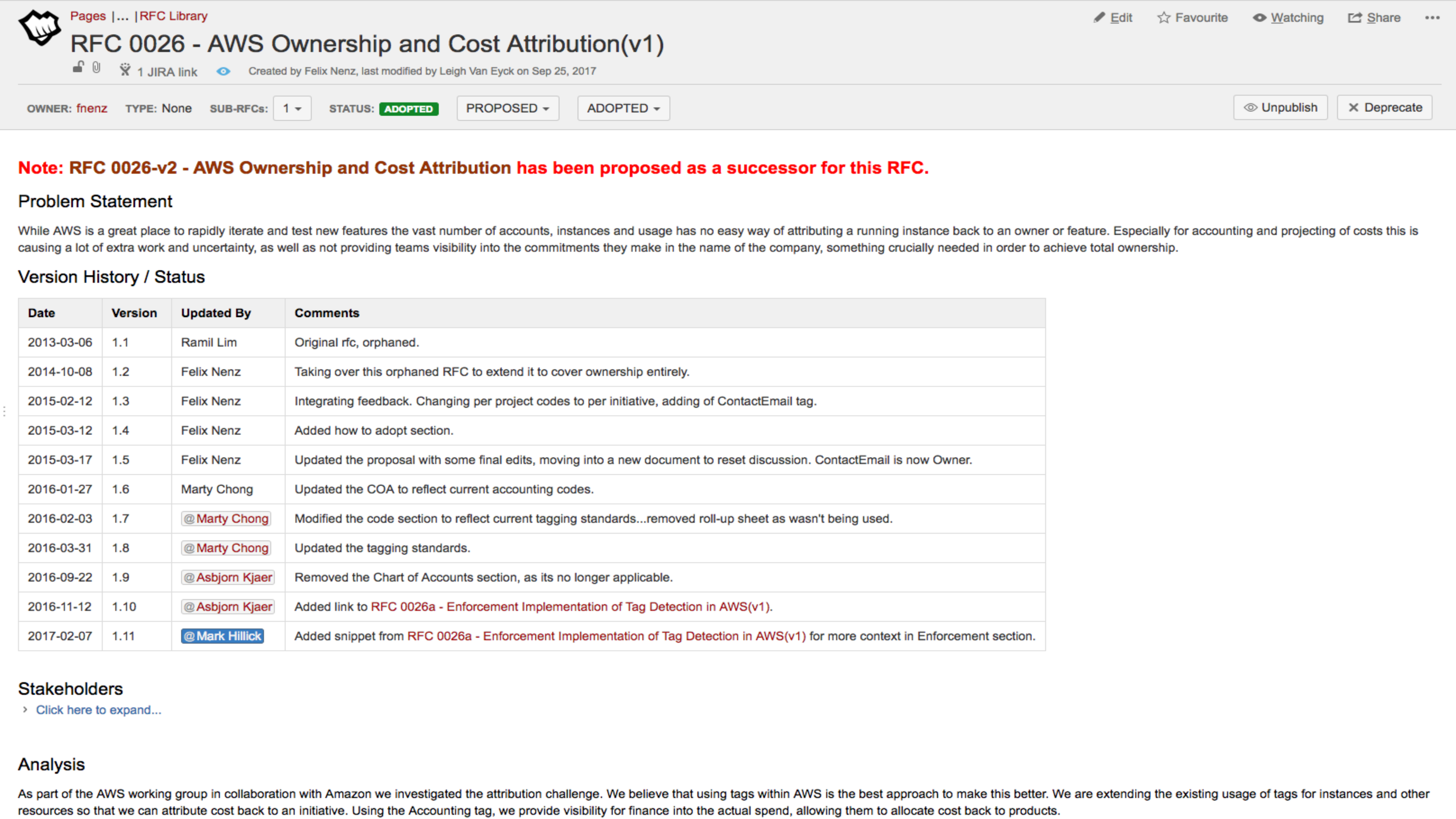
	Item Name	Technology	Account	Account Type	Region	Issue	Notes	Score	Justification
□	rconsole-stage-SecondaryReplicaNode11NodeSecurityGroup-U754615T34TB (sg-f93[redacted] in vpc-42[redacted])	securitygroup	[redacted]	AWS	us-west-2	Security Group ingress rule contains 0.0.0.0/0	0.0.0.0/0 on tcp 22	10	-
□	esports-iphide (sg-b8[redacted] in vpc-0c[redacted])	securitygroup	[redacted]	AWS	us-west-2	Security Group ingress rule contains 0.0.0.0/0	0.0.0.0/0 on tcp 22	10	-
□	awseb-e-ptqmsbmn2x-stack-AWSEBSecurityGroup-VW4WGZS599X9 (sg-9b[redacted] in vpc-6a[redacted])	securitygroup	[redacted]	AWS	us-west-2	Security Group ingress rule contains 0.0.0.0/0	0.0.0.0/0 on tcp 22	10	-
□	canvasflow-mdb (sg-5b[redacted] in vpc-6a[redacted])	securitygroup	[redacted]	AWS	us-west-2	Security Group ingress rule contains 0.0.0.0/0	0.0.0.0/0 on tcp 27017	10	-
□	merch_health_service (sg-98[redacted] in vpc-95[redacted])	securitygroup	[redacted]	AWS	ap-northeast-1	Security Group ingress rule contains 0.0.0.0/0	0.0.0.0/0 on tcp 22	10	-
□	esports-iphide (sg-b8[redacted] in vpc-0c[redacted])	securitygroup	[redacted]	AWS	us-west-2	Security	0.0.0.0/0	10	-

What, where, who?

Why :: Incident Response is hard when you don’t know who owns what

Why :: If you don’t need it, why is it running?

What :: Tagging is incredibly easy to use to identify ownership



RFC 0026 - AWS Ownership and Cost Attribution(v1)

Created by Felix Nenz, last modified by Leigh Van Eyck on Sep 25, 2017

OWNER: fnenz TYPE: None SUB-RFCs: 1 STATUS: ADOPTED PROPOSED ADOPTED

Note: RFC 0026-v2 - AWS Ownership and Cost Attribution has been proposed as a successor for this RFC.

Problem Statement

While AWS is a great place to rapidly iterate and test new features the vast number of accounts, instances and usage has no easy way of attributing a running instance back to an owner or feature. Especially for accounting and projecting of costs this is causing a lot of extra work and uncertainty, as well as not providing teams visibility into the commitments they make in the name of the company, something crucially needed in order to achieve total ownership.

Version History / Status

Date	Version	Updated By	Comments
2013-03-06	1.1	Ramil Lim	Original rfc, orphaned.
2014-10-08	1.2	Felix Nenz	Taking over this orphaned RFC to extend it to cover ownership entirely.
2015-02-12	1.3	Felix Nenz	Integrating feedback. Changing per project codes to per initiative, adding of ContactEmail tag.
2015-03-12	1.4	Felix Nenz	Added how to adopt section.
2015-03-17	1.5	Felix Nenz	Updated the proposal with some final edits, moving into a new document to reset discussion. ContactEmail is now Owner.
2016-01-27	1.6	Marty Chong	Updated the COA to reflect current accounting codes.
2016-02-03	1.7	@Marty Chong	Modified the code section to reflect current tagging standards...removed roll-up sheet as wasn't being used.
2016-03-31	1.8	@Marty Chong	Updated the tagging standards.
2016-09-22	1.9	@Asbjorn Kjaer	Removed the Chart of Accounts section, as its no longer applicable.
2016-11-12	1.10	@Asbjorn Kjaer	Added link to RFC 0026a - Enforcement Implementation of Tag Detection in AWS(v1).
2017-02-07	1.11	@Mark Hillick	Added snippet from RFC 0026a - Enforcement Implementation of Tag Detection in AWS(v1) for more context in Enforcement section.

Stakeholders

› Click here to expand...

Analysis

As part of the AWS working group in collaboration with Amazon we investigated the attribution challenge. We believe that using tags within AWS is the best approach to make this better. We are extending the existing usage of tags for instances and other resources so that we can attribute cost back to an initiative. Using the Accounting tag, we provide visibility for finance into the actual spend, allowing them to allocate cost back to products.

Solution

Shrink the change => No decision paralysis

Feedback & moved to the adoption stage

Standard across Riot

Tagging Details

Required Tags :: Name, Owner & Accounting

Schedule

At 0, 21 and 27 days => Notify Gatekeeper and owner (if possible)

At 4 weeks => Shutdown Instance

At 12 weeks => Terminate Instance

Cinq Features

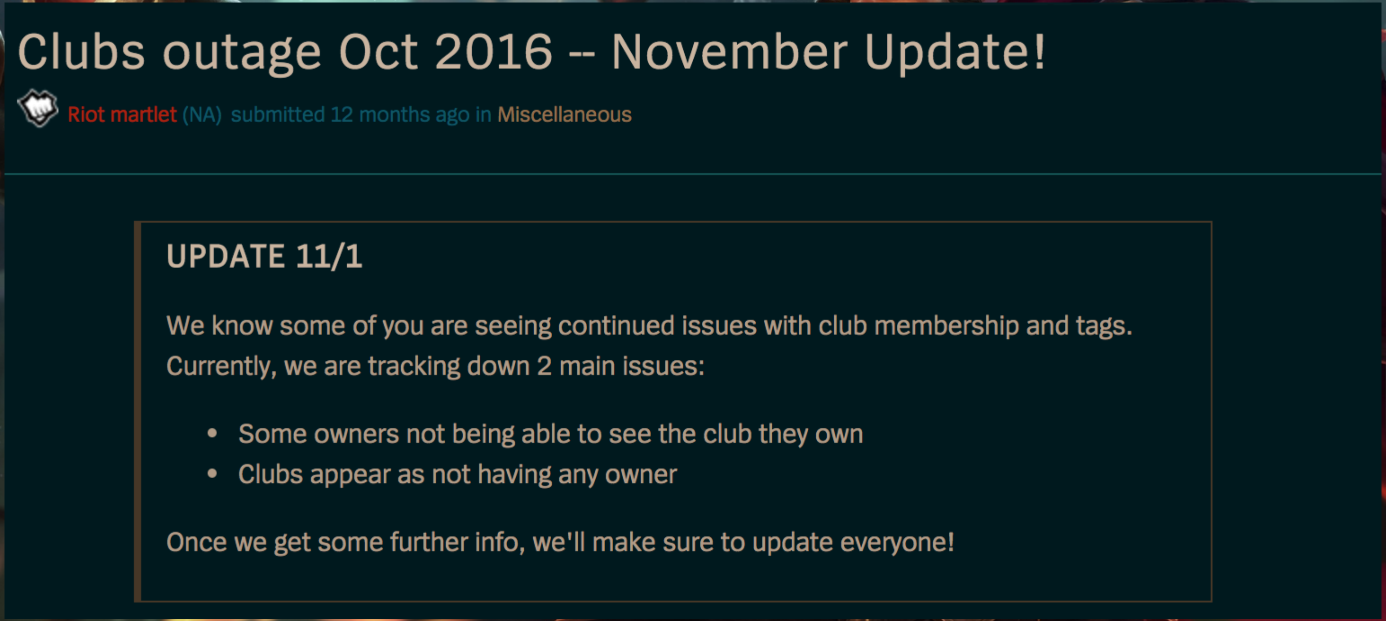
Removes incorrectly tagged & un-owned AWS objects

Checks that security features are turned on throughout our AWS Infra

DNS hijacking & IAM policy management

Code Time

MurderBot



Clubs outage Oct 2016 -- November Update!

Riot martlet (NA) submitted 12 months ago in Miscellaneous

UPDATE 11/1

We know some of you are seeing continued issues with club membership and tags. Currently, we are tracking down 2 main issues:

- Some owners not being able to see the club they own
- Clubs appear as not having any owner

Once we get some further info, we'll make sure to update everyone!

Sad

Learnings

Our communications & planning had gaps

Confusion around RFC Adoption

Our notification code had bugs

Feedback

"By doing a RCA, the team has truly showed themselves to be part of Engineering. We all make mistakes - this is how we learn and improve. /fistbump "

Cam Dunn (Tech Director), Dec. 2016

2nd Adoption, Yay!

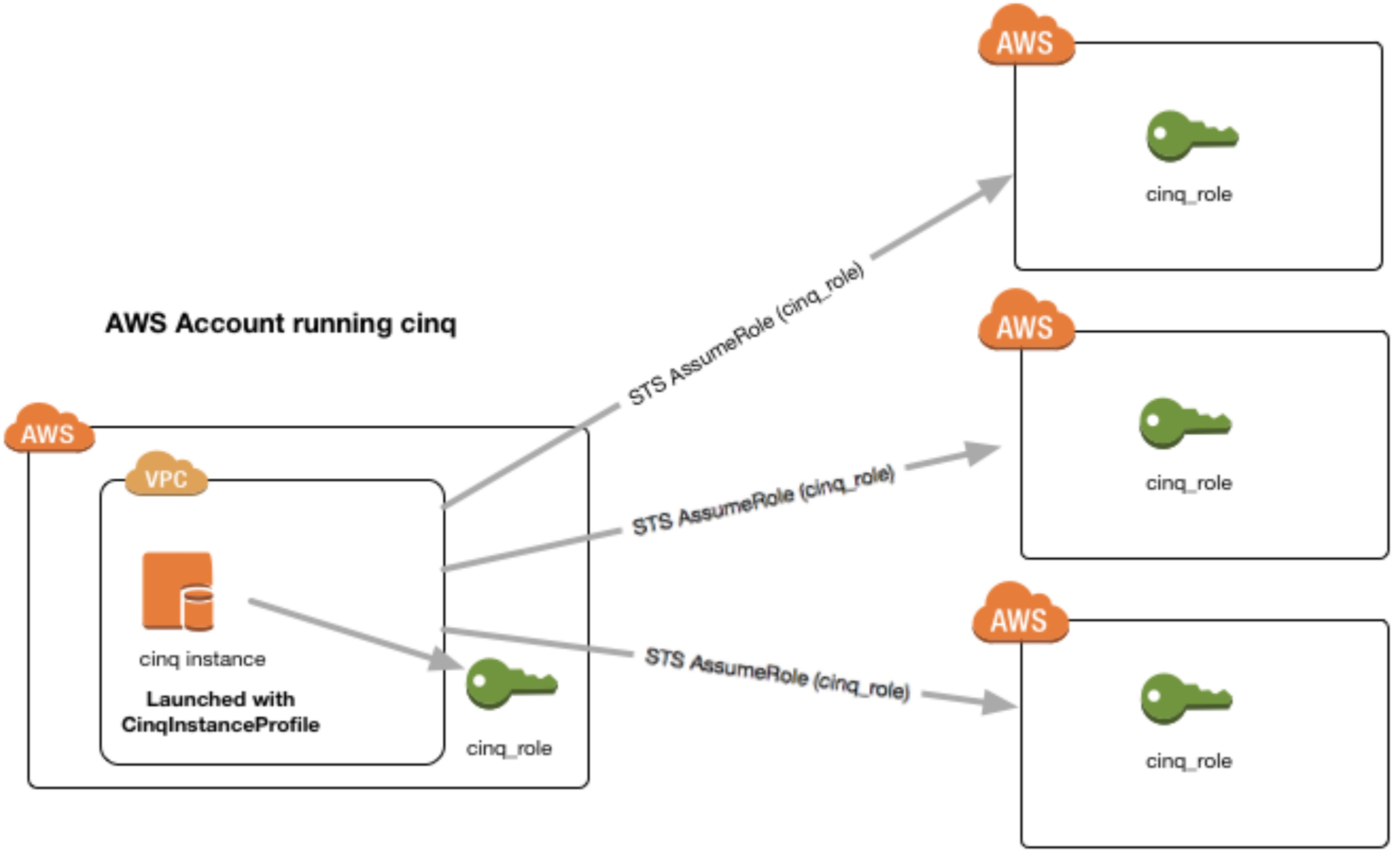
bcc Engineering

“Thanks for everyone's input and consideration for RFC0026, aka MurderBot, over the last several weeks. This is now adopted at Riot scope.”

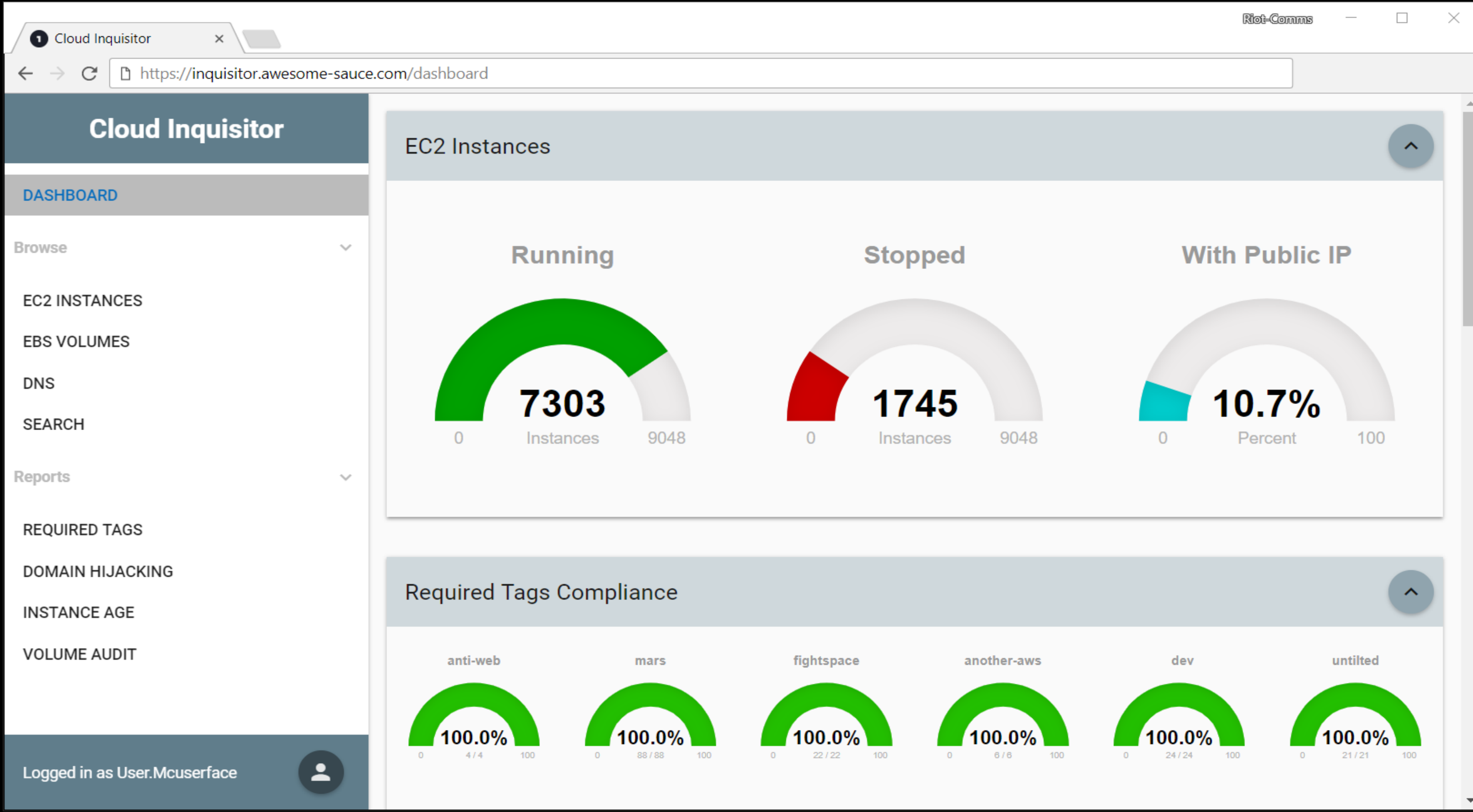
Mike Seavers (Director of Engineering), Feb. 2017

AWS Target Accounts monitored by cinq

AWS Account running cinq



IAM Role called ‘cinq_role’ configured with policy that trusts AWS Instance Profile from cinq AWS Account


Cloud Inquisitor
Riot-Comms
https://inquisitor.awesome-sauce.com/dashboard
Cloud Inquisitor
DASHBOARD
Browse
EC2 INSTANCES
EBS VOLUMES
DNS
SEARCH
Reports
REQUIRED TAGS
DOMAIN HIJACKING
INSTANCE AGE
VOLUME AUDIT
Logged in as User.Mcuserface
EC2 Instances
Running
7303
0
Instances
9048
Stopped
1745
0
Instances
9048
With Public IP
10.7%
0
Percent
100
Required Tags Compliance
anti-web
100.0%
0
4 / 4
100
mars
100.0%
0
88 / 88
100
fightspace
100.0%
0
22 / 22
100
another-aws
100.0%
0
6 / 6
100
dev
100.0%
0
24 / 24
100
untilted
100.0%
0
21 / 21
100

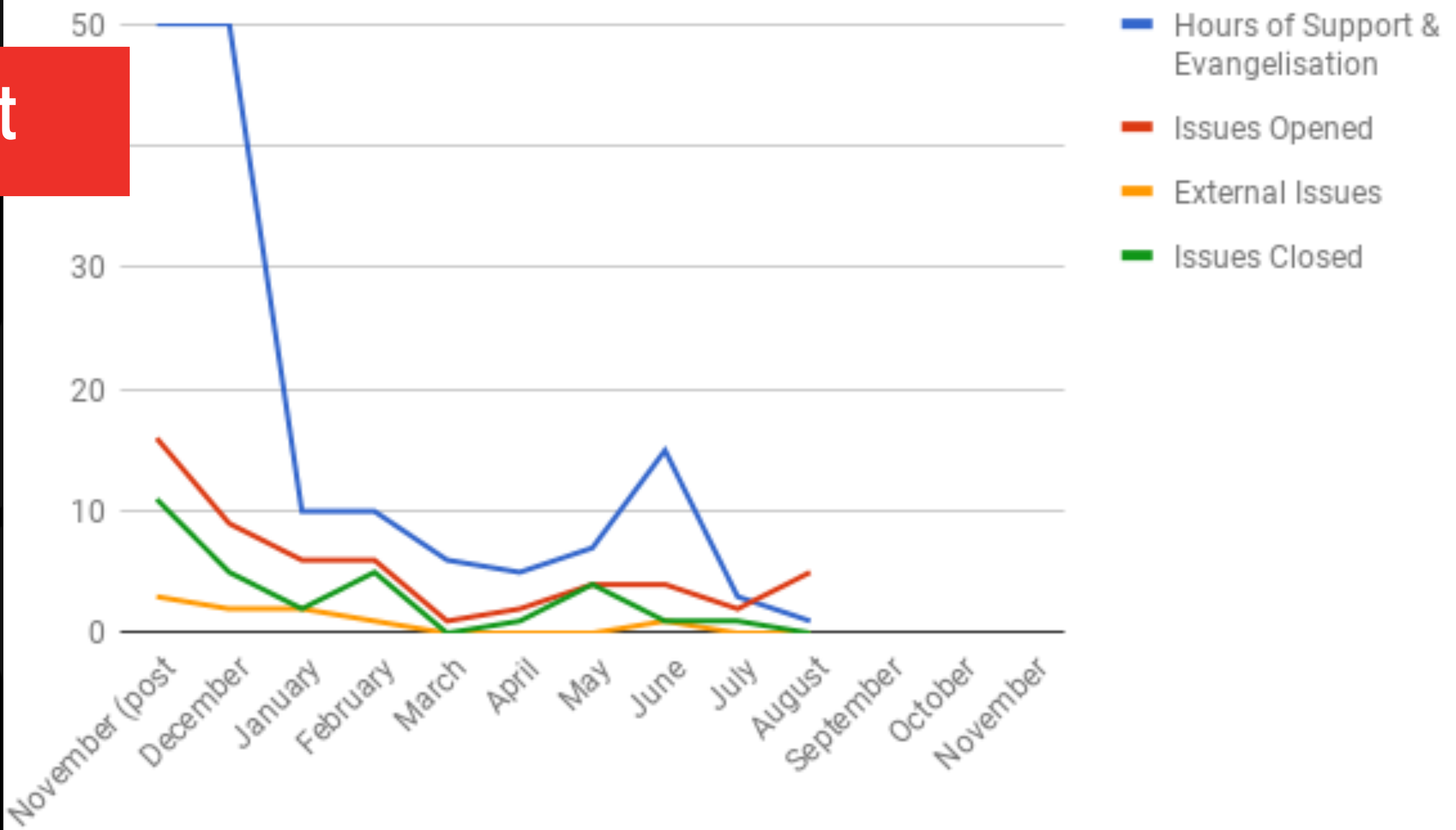
Email Notify

The following resources are not compliant with the Required Tagging standards........

Issues

Resource	Resource Type	Account	Region	Missing tags	Notes	Alert Info
i-0xyz	EC2 Instance	marky-mark	us-west-2	owner, accounting	No Notes	27 days alert
i-1xyz	EC2 Instance	marky-mark	us-west-2	owner, accounting	No Note	Resource stopped
i-2xyz	EC2 Instance	marky-mark	us-west-2	owner	Owner tag is not valid	Resource removed
i-3xyz	EC2 Instance	marky-mark	us-west-2	name	No Notes	0 seconds

OSS Cost


50
30
20
10
0
November (post
December
January
February
March
April
May
June
July
August
September
October
November
Hours of Support & Evangelisation
Issues Opened
External Issues
Issues Closed

AGENDA

- Who
- 2015
- 2018
- Getting to the Nexus

Futures (1)

RFC0242 :: Our focus is changing from Riot to Rioter

Auth :: No permanent credentials & enforced dynamic access policies

Everywhere :: More attribution & platform-independent solutions

Futures (2)

New & Shared :: Work with new products & try to solve with solutions that can be leveraged by many

Measure :: Are we doing any good? If so, how and where?

Collaboration :: Bug Bounty++, OSS++ , Tools & Blogs (Int & Ext)

Evolution

Started :: DFIR & Emergent

Next :: Visibility, Being Embraced, Collaboration & Tools

Now :: Tools within Workflows, Occasional Blocking & Measurement

Thank You

How to Carry your Team
Z-G
S3 BLITZ UPGRADE !
ULTRA HEX BOMB!
KABOOM!
HEX NUKE
HEX DYNAMITE BELT
BLITZ V.2.0!