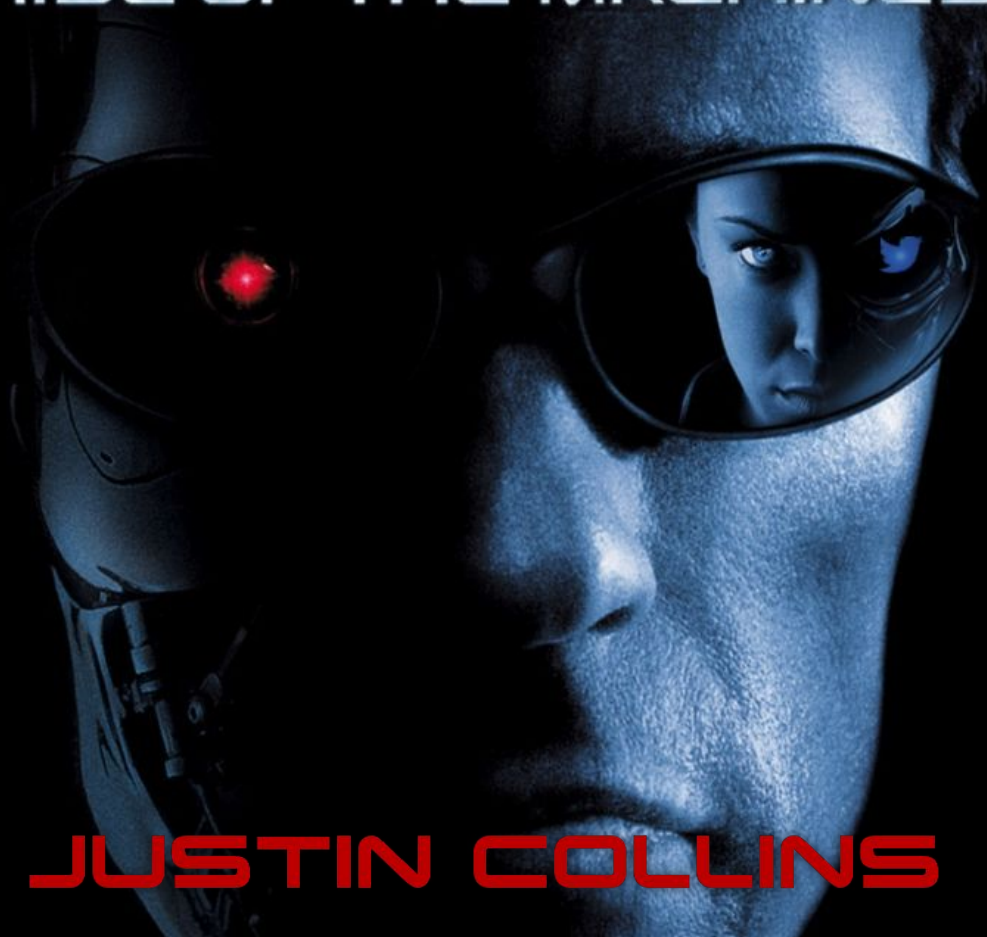
SECURITY AUTOMATION AT TWITTER

RISE OF THE MACHINES



JUSTIN COLLINS


Neil Matatall
Alex Smolen
Nick Green
Me
Putting Your
Robots to Work
Security Automation at Twitter
TOTAL SECURITY
AUTOMATED AUTHORITY

Secure by Default
Detect via Tests

Don't Fix Vulnerabilities Prevent Them

Is Twitter a Unicorn?

2009-2010

092 3093

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Jon Leibowitz, Chairman
William E. Kovacic
J. Thomas Rosch
Edith Ramirez
Julie Brill

In the Matter of	)	
	)	DOCKET NO: C-4316
TWITTER, INC.,	)	
a corporation.	)	

DECISION AND ORDER

No company-provided email accounts

No admin password complexity requirements

No separate administrative login page

No limit on failed admin login attempts

No admin password rotation enforcement

No access controls on admin actions

No IP restrictions on admin logins

Also...

Every employee is an admin!


ANALYSIS:
****
234654 453
654334 450 16
245261 865 26
453665 766 46
382856 863 09
356878 544 04
664217 985 89
254346 958 32
SCAN MODE 43894
SIZE ASSESSMENT
ASSESSMENT COMPLETE
FIT PROBABILITY 0.99
RESET TO ACQUISITION
MODE SPEECH LEVEL 78
PRIORITY OVERRIDE
DEFENSE SYSTEMS SET
ACTIVE STATUS
MAX
MATCH

Incident 01

Employee password brute-forced

Incident 01

Employee password brute-forced

Password:

Incident 01

Employee password brute-forced

Password: happiness


power twitter
Home Profile Find People Settings Help t3? Sign out
FOX NEWS .com
foxnews
Follow
Breaking: Bill O Riley is gay
21 minutes ago from web
Name Fox News
Location New York, NY
Web http://www.foxnew...
0 following
6,311 followers
85,668 updates
only foxnews's updates
Search

power twitter

Home Profile Find People Settings Help t3? Sign out

foxnews

Follow

Name Fox News
Location New York, NY

Breaking: Bill O Riley is gay

21 minutes ago from web

power twitter

Home Profile Find People Settings Help t3? Sign out

ricksanchezcnn

Follow

Name Rick Sanchez
Web http://www.cnn.co...
Bio Join Rick on CNN every weekday at 3pm ET

21,769 following | 39,711 followers | 1,243 updates

only ricksanchezcnn's updates

Search

i am high on crack right now might not be coming into work today

9 minutes ago from web

@kittell e mail it to me *about 13 hours ago from web in reply to kittell*

Updates


power twitter
Home Profile Find People Settings Help t3? Sign out
foxnews
Follow
Name Fox News
Location New York, NY
Breaking: Bill O Riley is gay


power twitter
Home Profile Find People Settings Help t3? Sign out
Name Rick Sanchez
Web http://www.cnn.co...
Join Rick on CNN every weekday at 3pm ET
1,769 following
39,711 followers
1,243 updates
only ricksanchezcnn's updates
Search
updates

BarackObama
What is your opinion on Barack Obama? Take the survey and possibly win $500 in free gas. http://tinyurl.com/9evlne
11 minutes ago from web
We just made history. All of this happened because you gave your time, talent and passion. All of this happened because of you. Thanks 11:34 AM Nov 5th, 2008 from web
Name Barack Obama
Location Chicago, IL
Web http://www.barack...
166,777 following
155,034 followers
264 updates
Updates
Favorites
Following

Incident 02

Attacker gains access to employee’s email account

Incident 02

Attacker gains access to employee’s email account

Finds two passwords, over six months old

Incident 02

Attacker gains access to employee’s email account

Finds two passwords, over six months old

Infers current password

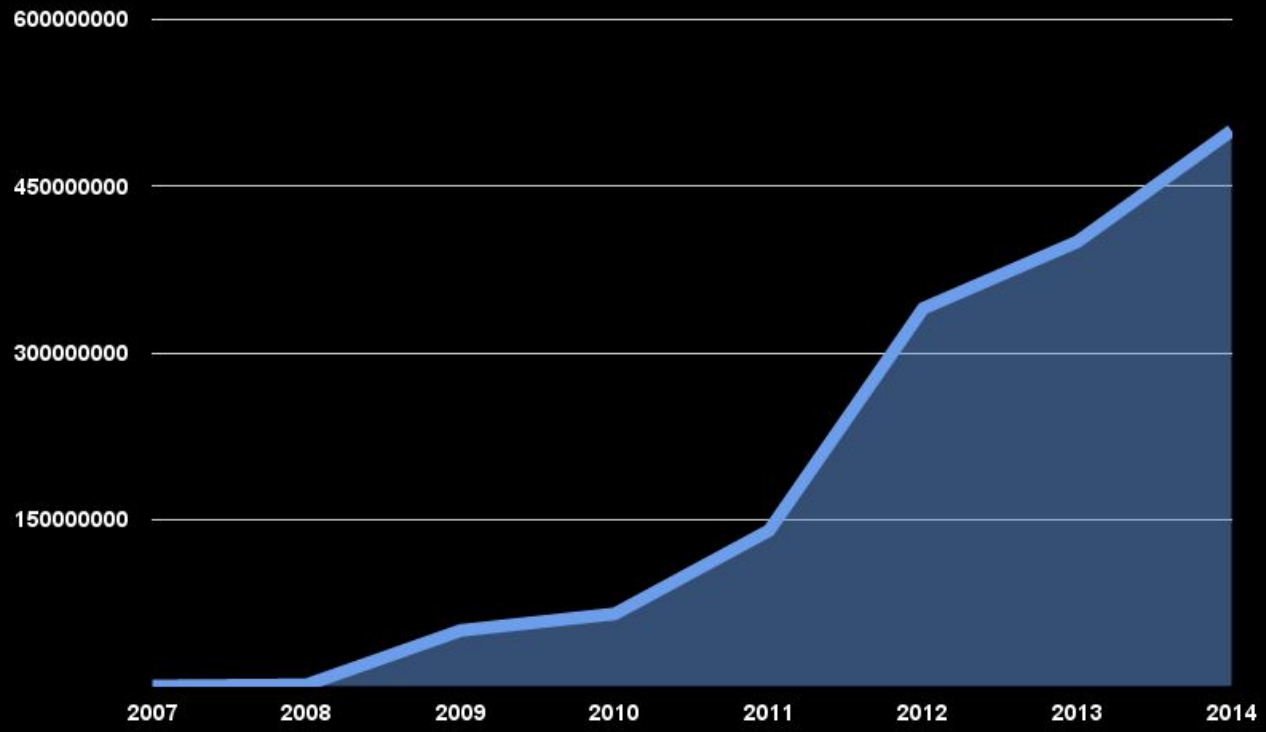
FTC Order

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, website, or other device, in connection with the offering of any product or service, in or affecting commerce, shall, no later than the date or service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the nonpublic consumer information, including:

FTC Order

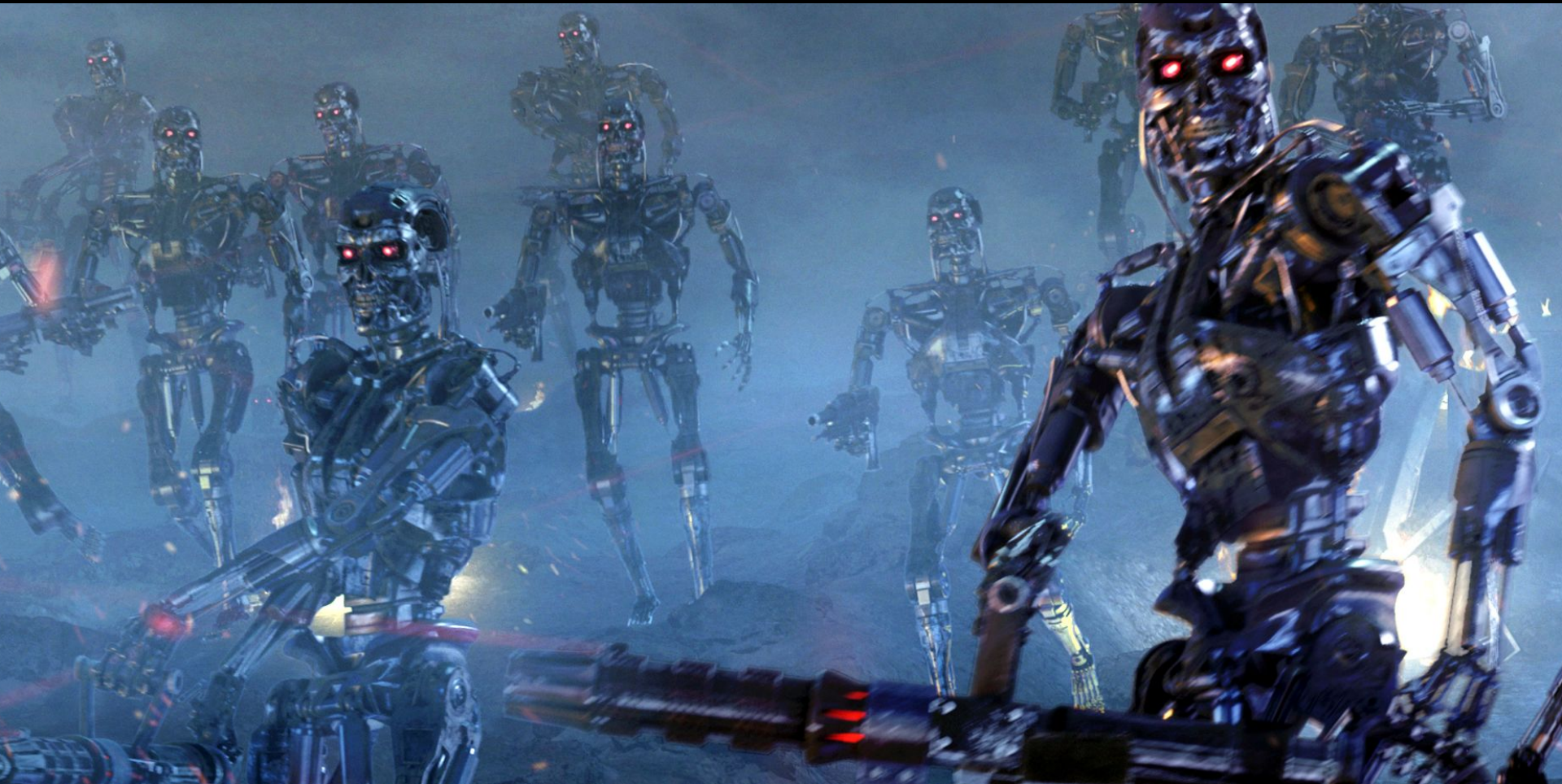
IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, website, or other device, in connection with the offering of any product or service, in or affecting commerce, shall, no later than the date or service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the nonpublic consumer information, including:

Tweets per Day



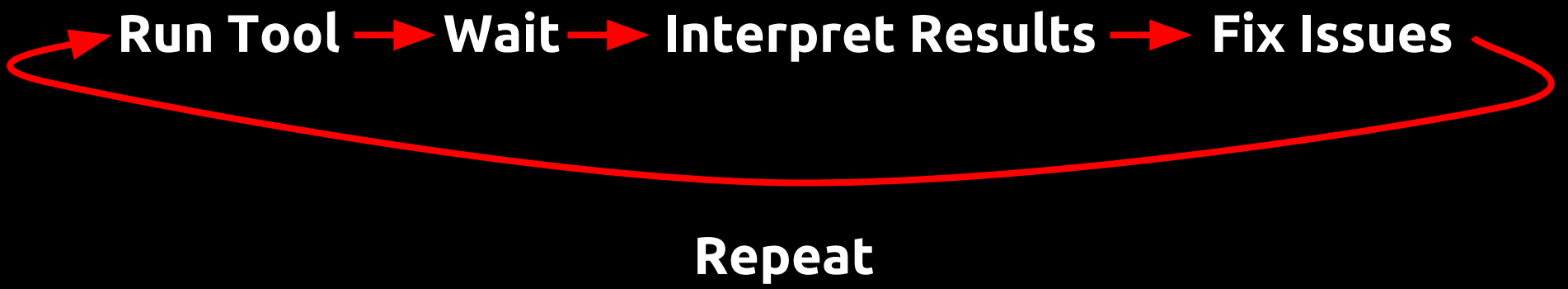
About Me

About Machines

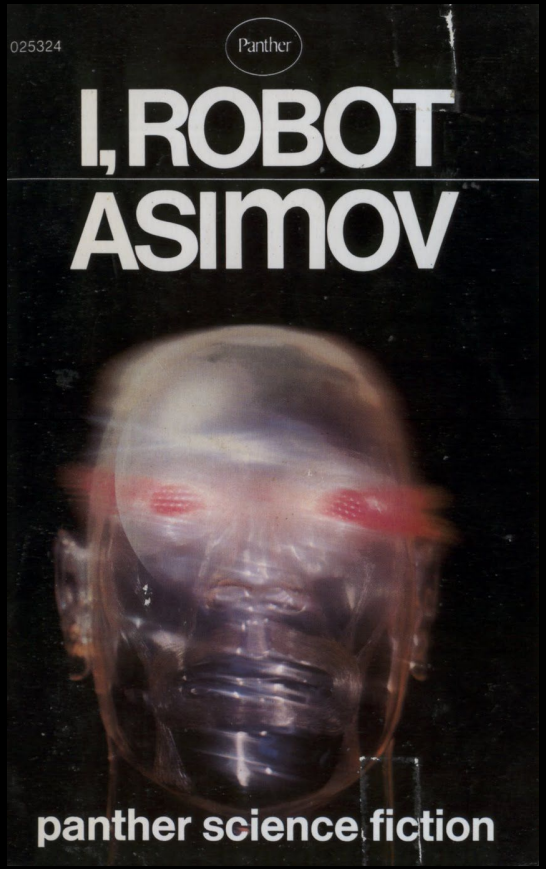


Tool Cycle

Tool Cycle



Philosophy of Automation



Right Information to the Right People

Find Bugs as Quickly as Possible

Don’t Repeat Your Mistakes

Analyze from Many Angles

Let People Prove You Wrong

Help People
Help Themselves

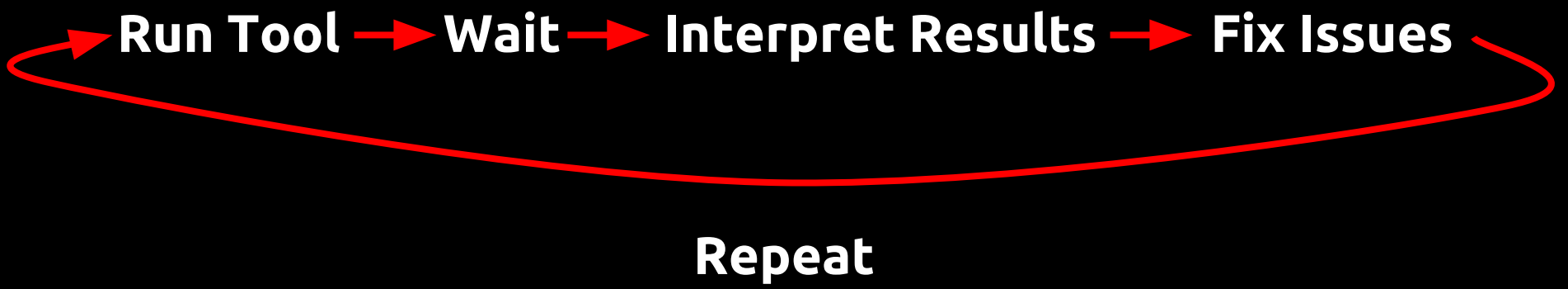
Automate Dumb Work

Keep It Tailored

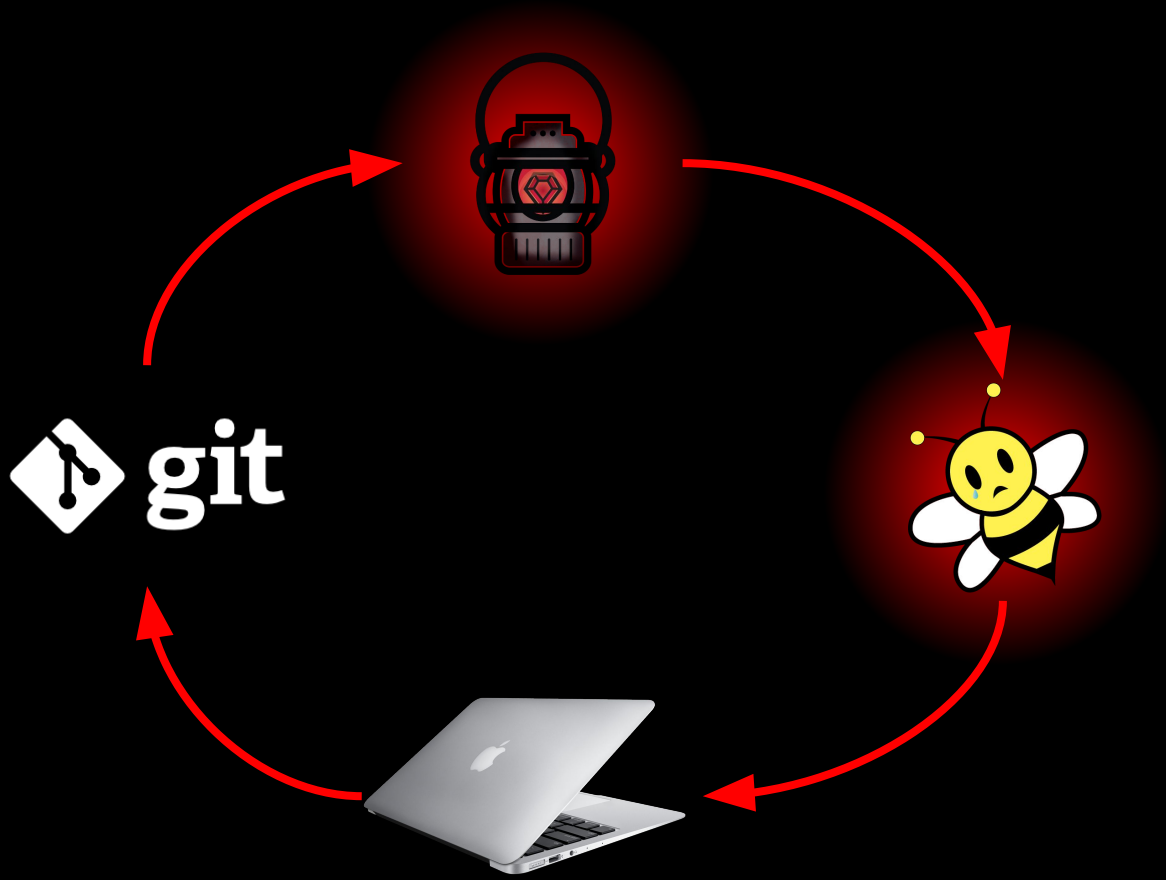
Legend of SADB

Brakeman

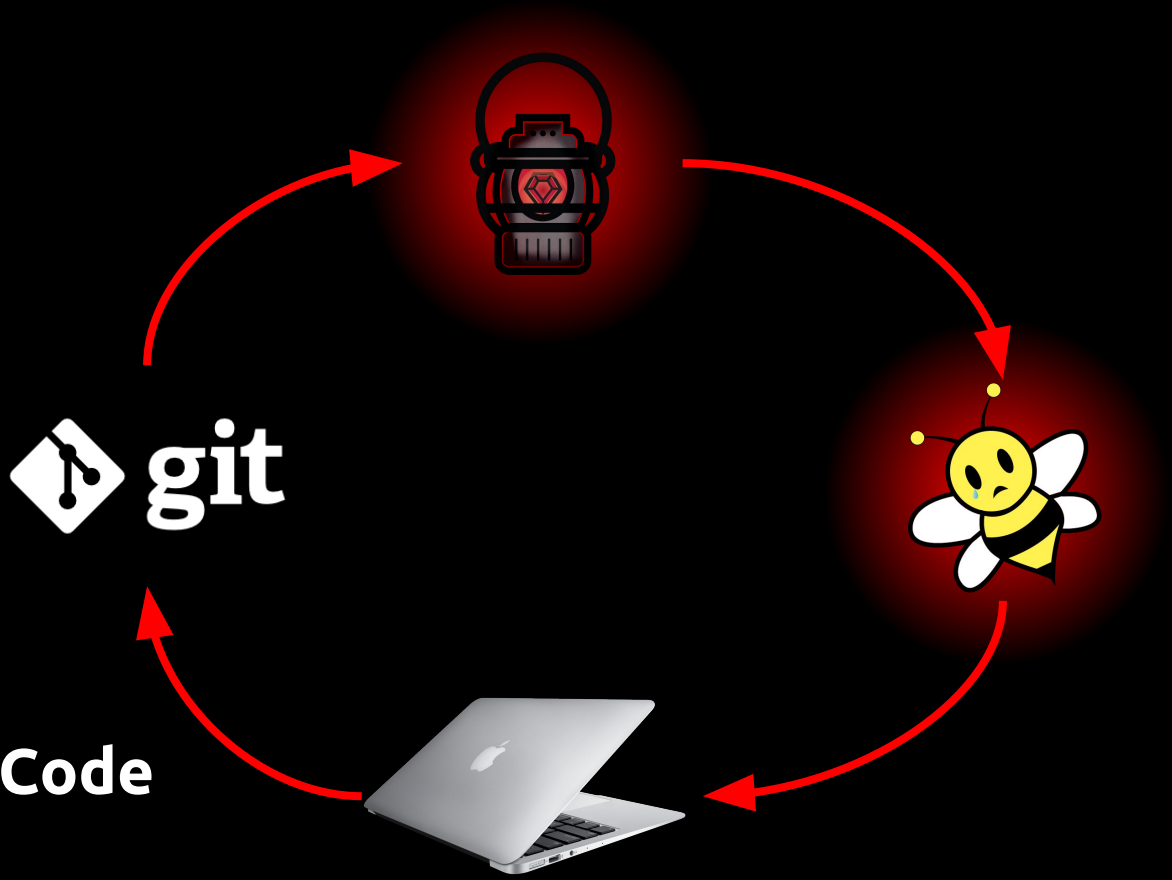
Using Brakeman



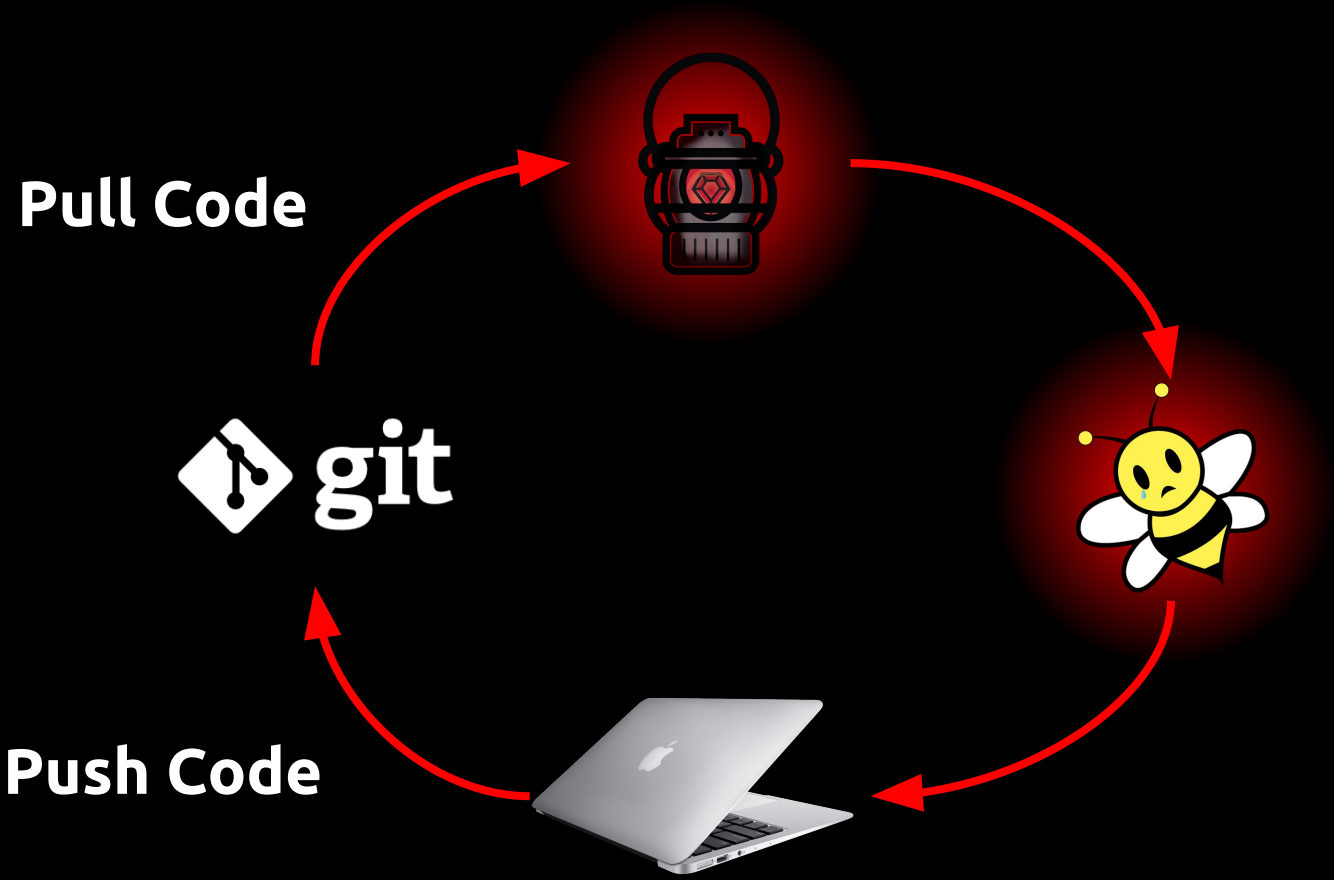
Automated Brakeman



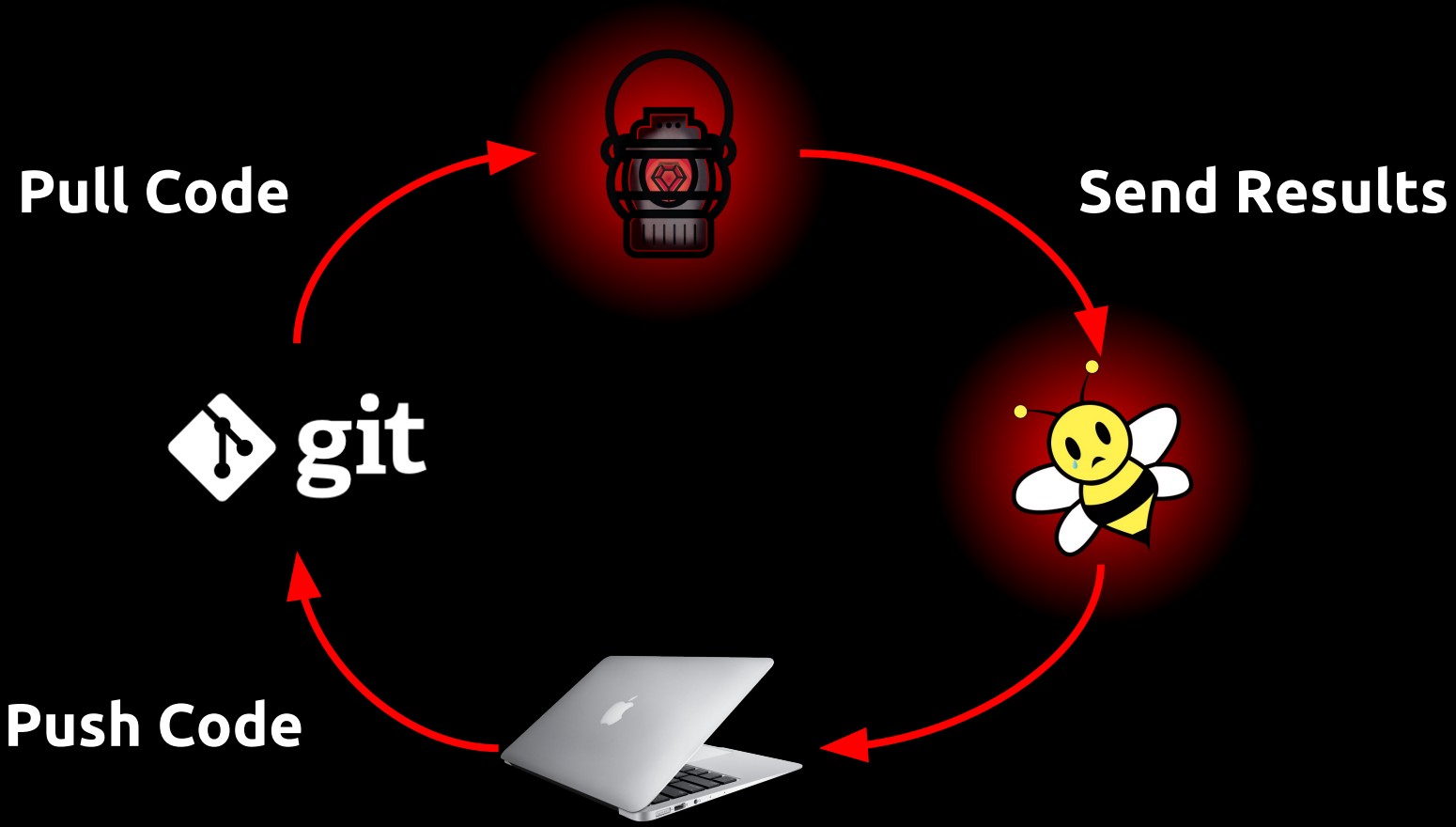
Automated Brakeman



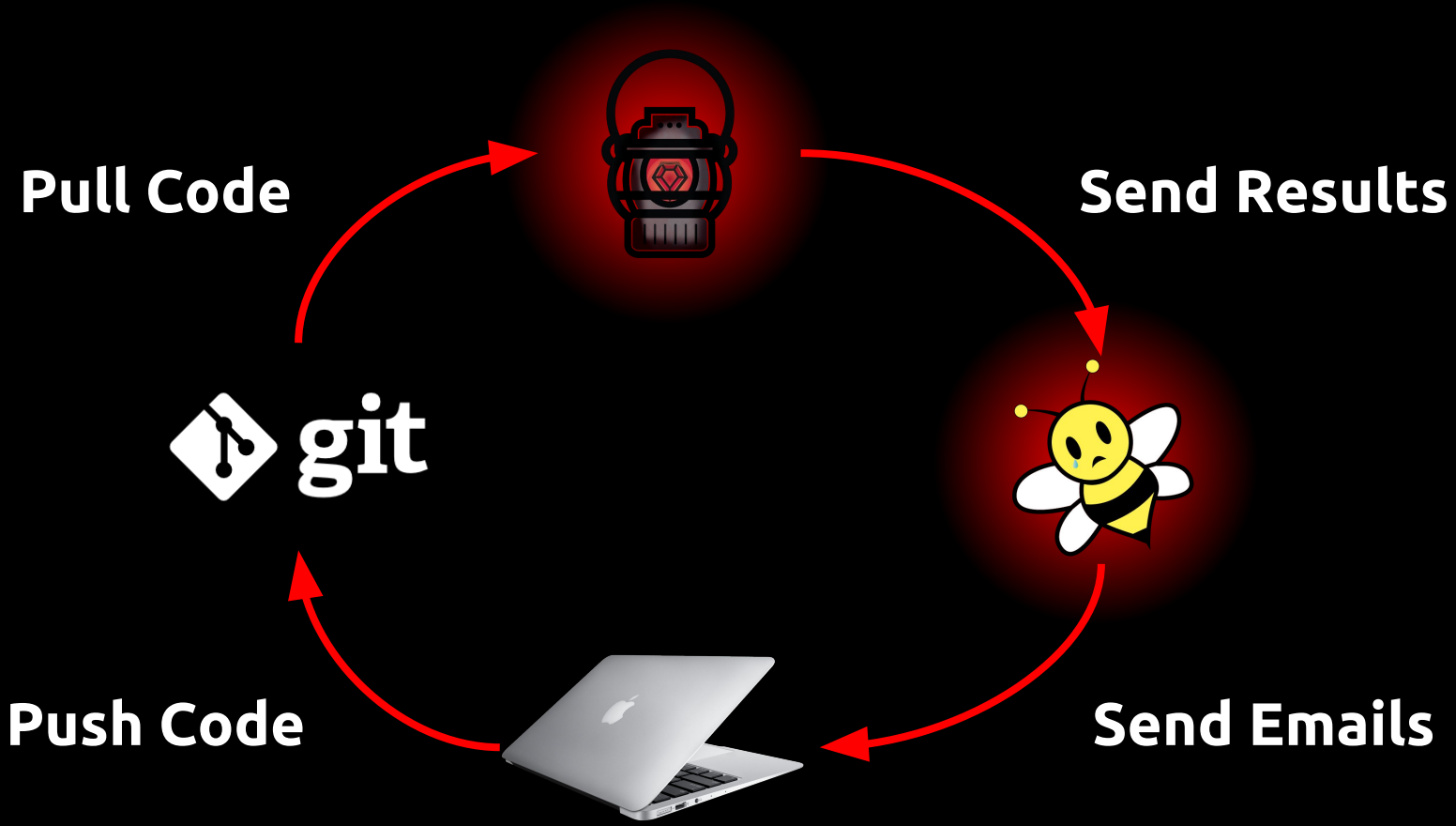
Automated Brakeman



Automated Brakeman



Automated Brakeman



[redacted]

CSP Reports	Brakeman	BundlerAudit
Warnings	[redacted]	[redacted]
Latest Change	[redacted] (over 1 year ago)	[redacted] (25 days ago)
Latest Report	13 days ago	13 days ago
Pending Reports	0	0

[redacted]

CSP Reports	Brakeman	BundlerAudit
Warnings	[redacted]	[redacted]
Latest Change	[redacted] (3 months ago)	[redacted] (4 months ago)
Latest Report	about 1 hour ago	about 22 hours ago
Pending Reports	0	0

[redacted]

CSP Reports	Brakeman	BundlerAudit
Warnings	[redacted]	[redacted]
Latest Change	[redacted] (2 months ago)	[redacted] (20 days ago)
Latest Report	about 1 hour ago	about 1 hour ago
Pending Reports	0	0

Secauto Dashboard

CSP Reports	Brakeman	BundlerAudit
Warnings	4	1
Latest Change	1 new warnings (about 1 month ago)	1 new warnings (about 1 month ago)
Latest Report	1 day ago	1 day ago
Pending Reports	0	0

Sad Bee Food

	Brakeman	BundlerAudit
Warnings	4	6
Latest Change	1 new warnings (4 months ago)	1 new warnings (3 months ago)
Latest Report	3 months ago	3 months ago
Pending Reports	0	0

[redacted]

CSP Reports	Brakeman	BundlerAudit
Warnings	[redacted]	[redacted]
Latest Change	[redacted] (7 days ago)	[redacted] (1 day ago)
Latest Report	3 minutes ago	3 minutes ago
Pending Reports	1	2

[redacted]

	Brakeman	BundlerAudit
Warnings	[redacted]	[redacted]
Latest Change	[redacted]	[redacted]

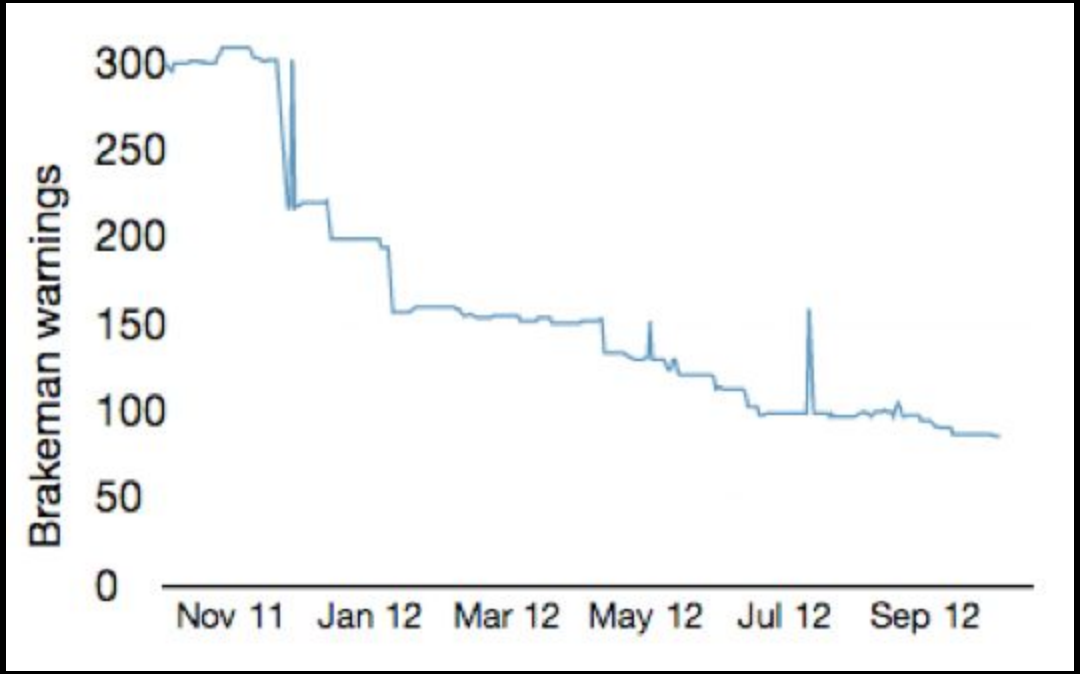
[redacted]

	Brakeman	BundlerAudit
Warnings	[redacted]	[redacted]
Latest Change	[redacted]	[redacted]

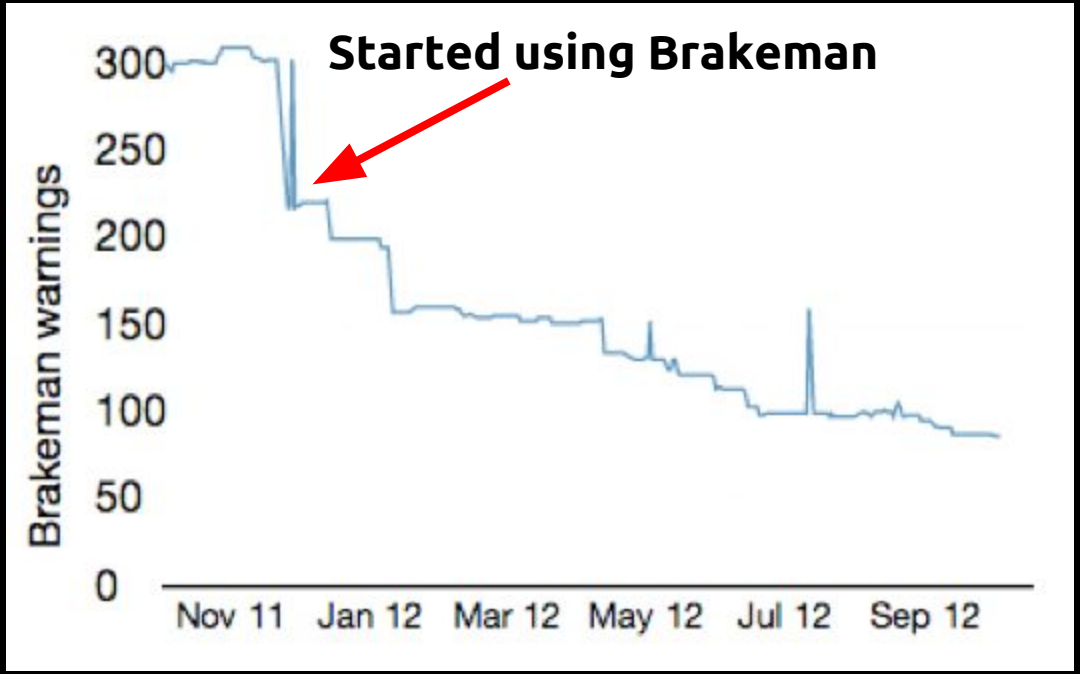
[redacted]

	Brakeman	BundlerAudit
Warnings	[redacted]	[redacted]
Latest Change	[redacted]	[redacted]

Warnings Over Time



Warnings Over Time



project **Sad Bee Food** | branch **master** | **8 months** ago

Go to branch:

Issues

Criticality

10 records per page

Search:

Criticality	Identifier	Issue	Time introduced
High	OSVDB-104080	rbovirt Gem for Ruby contains a flaw	9 months ago
High	OSVDB-105971	sfpagent Gem for Ruby Remote Command Injection	9 months ago
Unknown	OSVDB-103439	XSS Vulnerability in number_to_currency, number_to_percentage and number_to_human	10 months ago
Unknown	CVE-2014-0130	Directory Traversal Vulnerability With Certain Route Configurations	8 months ago
Unknown	OSVDB-103440	Denial of Service Vulnerability in Action View when using render :text	10 months ago
Unknown	OSVDB-98270	Wicked Gem for Ruby contains a flaw	10 months ago

Showing 1 to 6 of 6 entries

Projects affected by CVE-2014-7818

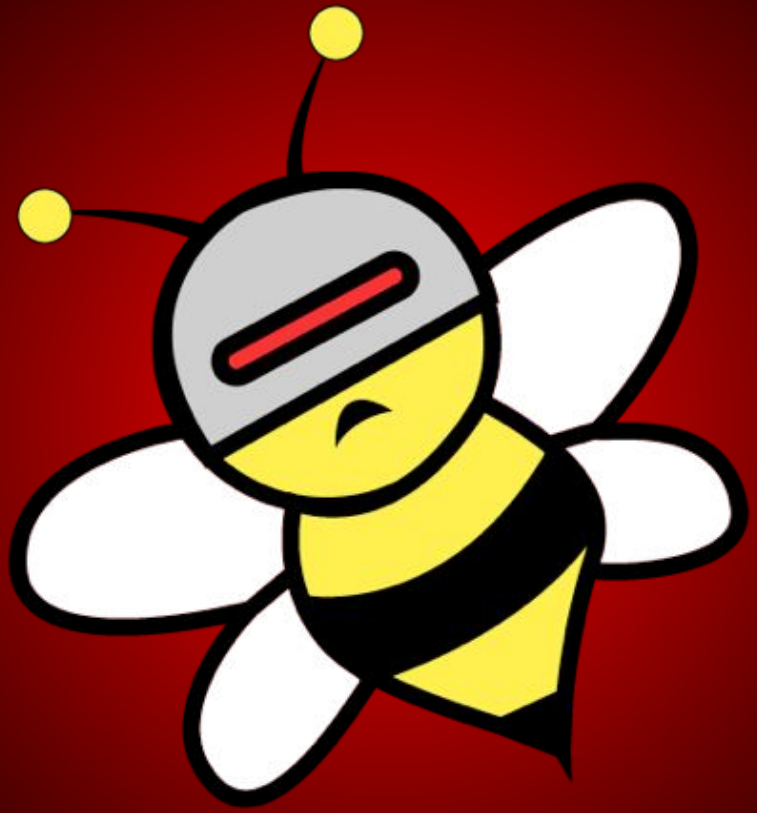
10 records per page

Search:

Project
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

Showing 1 to 8 of 8 entries

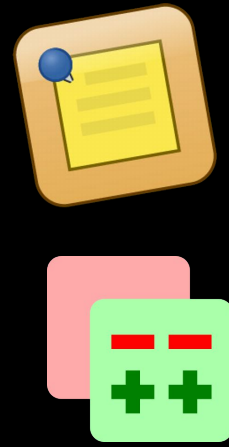
Legacy of SADB



Automated Reviews

Pattern Match

Comment on Review



01 Identify Problem

Repeated incident?

Opt-in code security?

Repetitive work?

02 Solve In Code

Write a library

Make it safe by default

Enforce library use in CI

04 Detect Statically

Determine fingerprint of issue

Identify suspect code

Alert during code review

05 Detect Dynamically

Write Selenium tests

Write a crawler

06 Use Browser Security

Content Security Policy

Strict Transport Security

Public Key Pinning

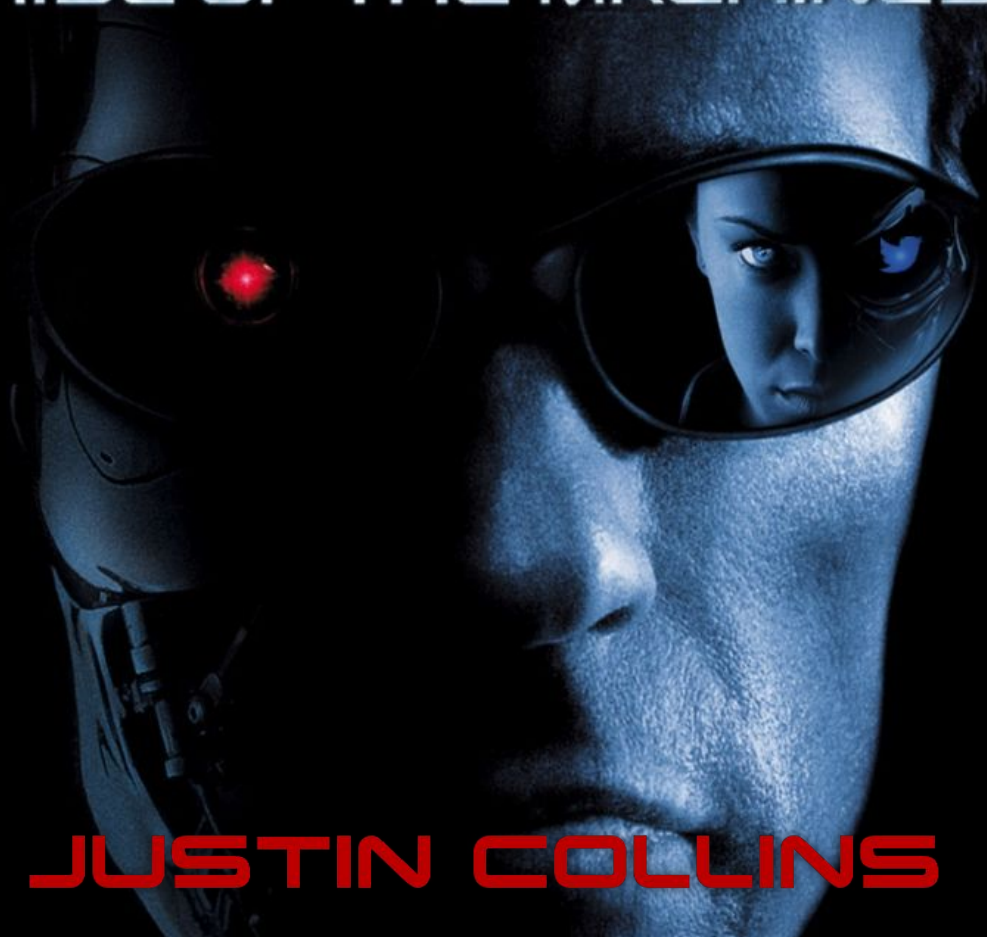
Subresource Integrity

Secure by Default
Detect via Tests

Don't Fix Vulnerabilities Prevent Them

SECURITY AUTOMATION AT TWITTER

RISE OF THE MACHINES



JUSTIN COLLINS