Security in Automation

So Before We Begin….

Jamesha Fisher

- Security Operations Engineer at GitHub
- Love Automation, Ops and Security
- Aspires to be Garnet, a badass character from Steven Universe (though I fail with my version of future vision)

Jamesha Fisher

- Security Operations Engineer at GitHub
- Love Automation, Ops and Security
- Aspires to be Garnet, a badass character from Steven Universe (though I fail with my version of future vision)

What we'll Learn:

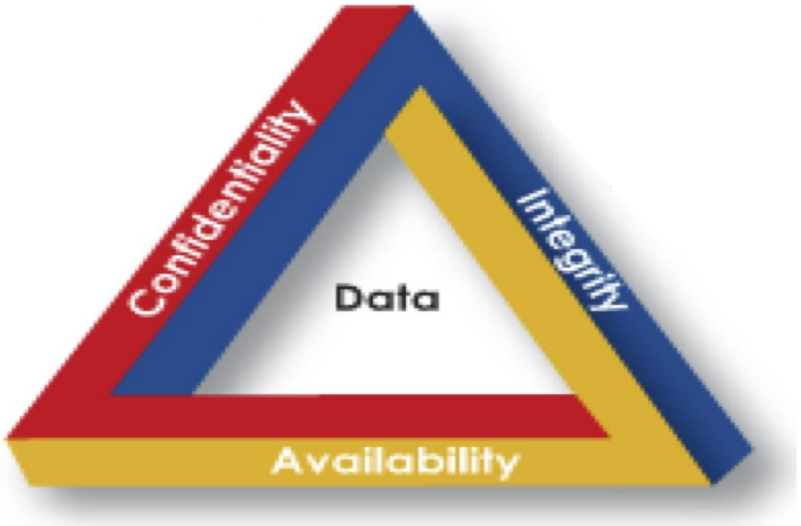
- Why Security Automation?
- What Security Automation Should Do?
- What Security Automation Can Do?
  - How we Can Do It

Why Security Automation?

Why Security?


TL
EV OF RIGHT SECTION ELLIPSE
EV OF CIRCULAR SECTION
TL
TL
GIVEN LINES
SPATIALLY PARALLEL
INFORMATION VIEW ONLY
SOLUTION CONE (ELLIPTICAL)
CIRCULAR SECTION
SOLUTION VIEW
90 000000°
GIVEN TWO SKEW LINES IN GENERAL POSITIONS
DETERMINE A VIEW SUCH THAT THE GIVEN LINES APPEAR PERPENDICULAR

Roll Back a Few Years...



Availability

"For any information system to serve its purpose, the information must be available when it is needed."

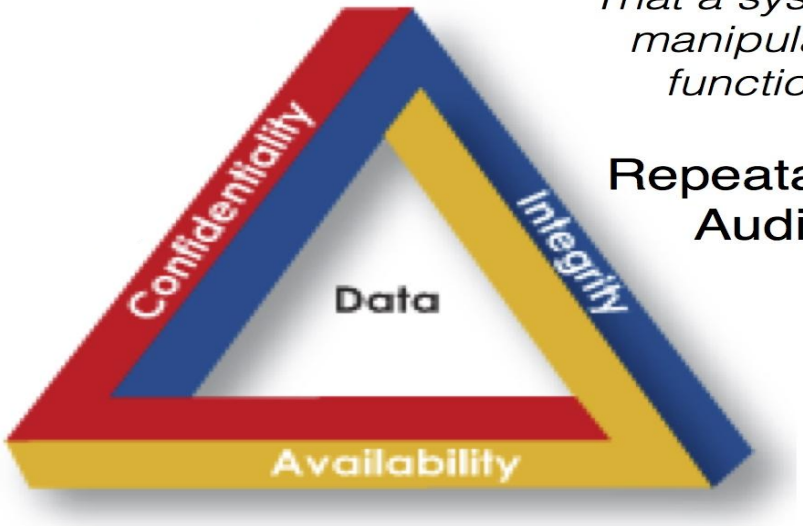
Fast

Ensure Uptime

Integrity

"That a system and its data are not manipulated for unauthorized functionality or alteration."

Repeatable & Standardized
Auditable/Processed



Availability

"For any information system to serve its purpose, the information must be available when it is needed."

Fast
Ensure Uptime

Confidentiality

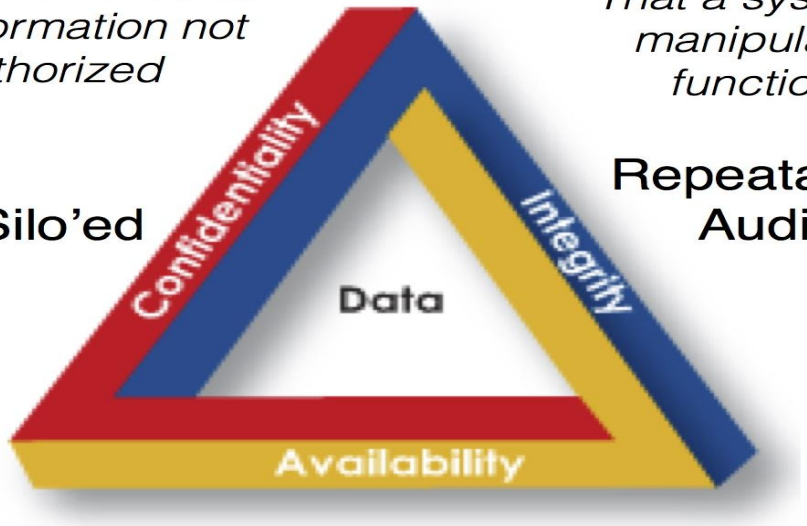
"Confidentiality is the requirement that private or confidential information not be disclosed to unauthorized individuals. "

Collaborative
Controlled, but not Silo'ed

Integrity

"That a system and its data are not manipulated for unauthorized functionality or alteration."

Repeatable & Standardized
Auditable/Processed

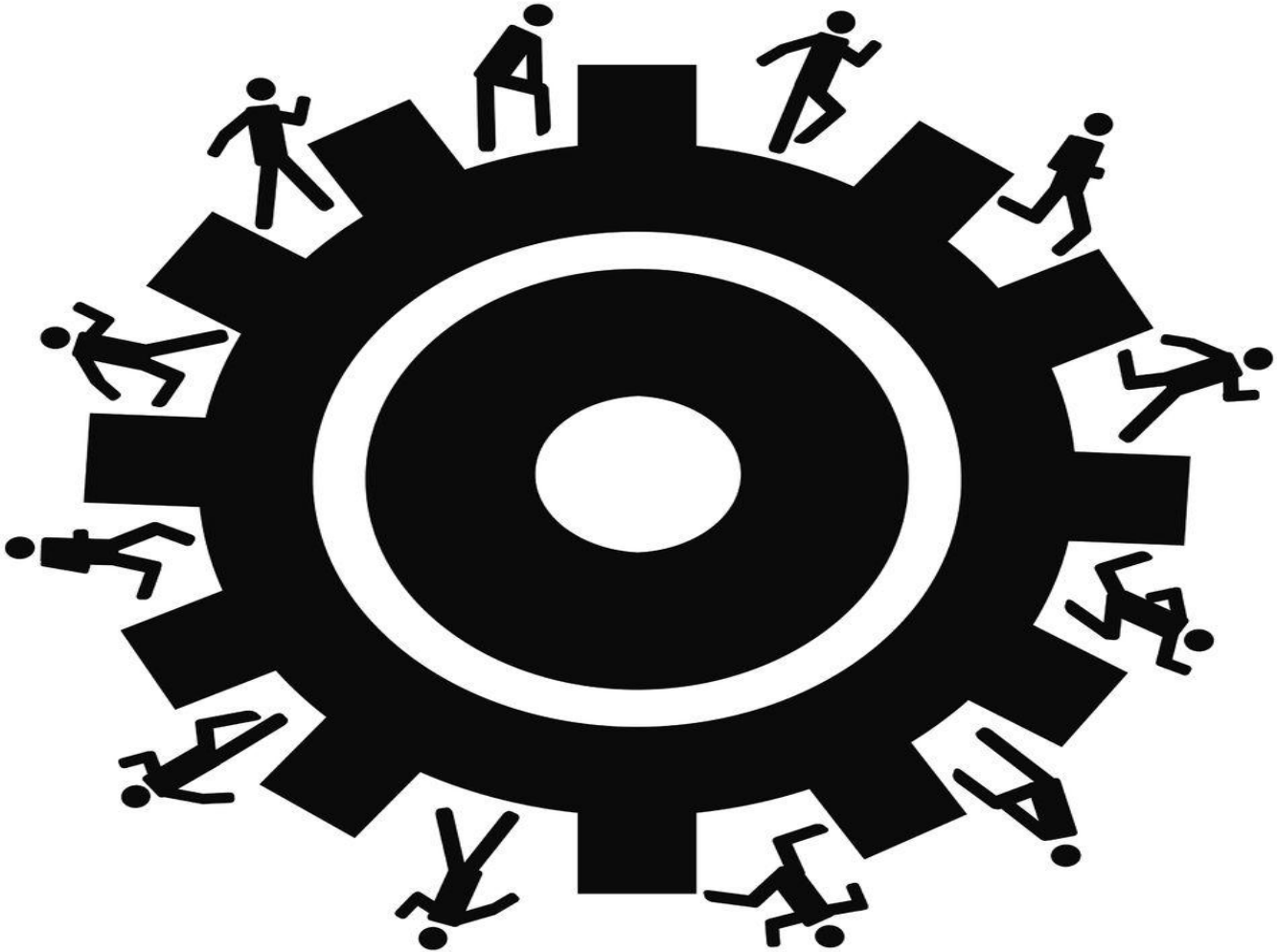


Availability

"For any information system to serve its purpose, the information must be available when it is needed."

Fast
Ensure Uptime

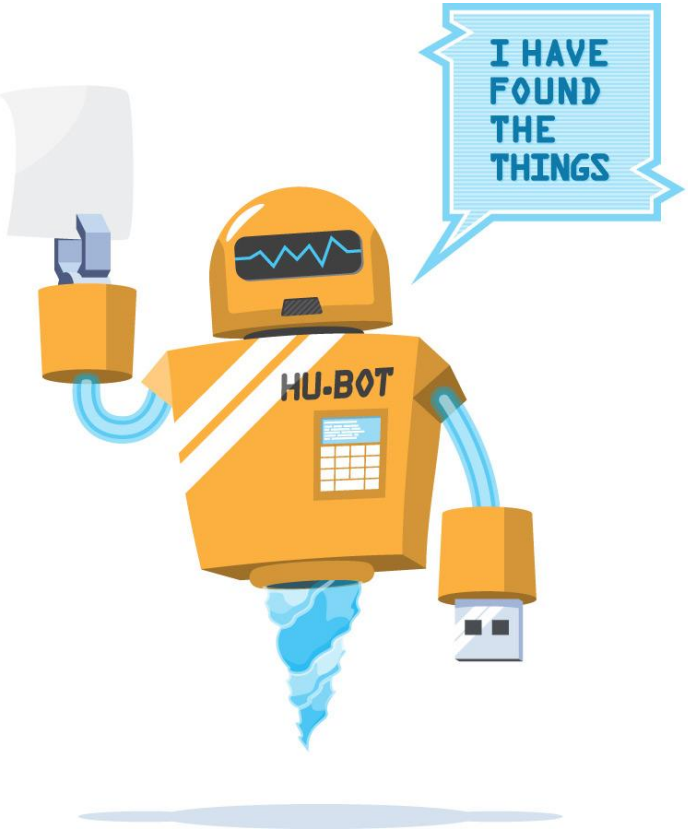
What Should Security Automation Do?




CHANGE
START

Story Time: Should in Action

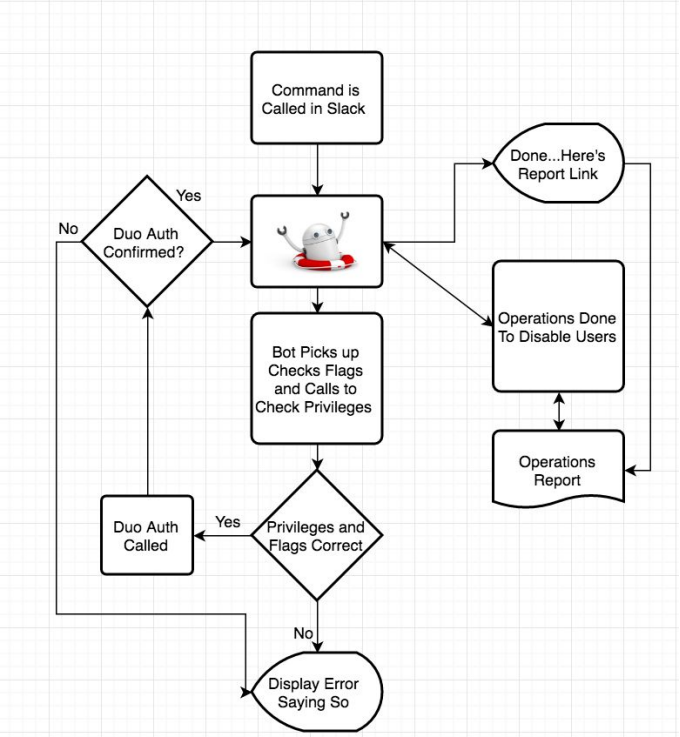

SaasyTech


I HAVE FOUND THE THINGS
HU-BOT


PASSWORD
VERIFY
Username
****
Login

BoardBoat - What It Does

- Listens for Command to Onboard or Offboard
- After some checks, Duo Authentication Request is made (which must be confirmed on caller's phone) before command execution continues.
- For Offboarding, command disables/removes access for a set of users leaving the company.
- Results of this are written to a log that's linked, and the link is returned to the slack channel when the command is finished.



Skyler Wilson 1:10 PM
/offboat 21817 duo

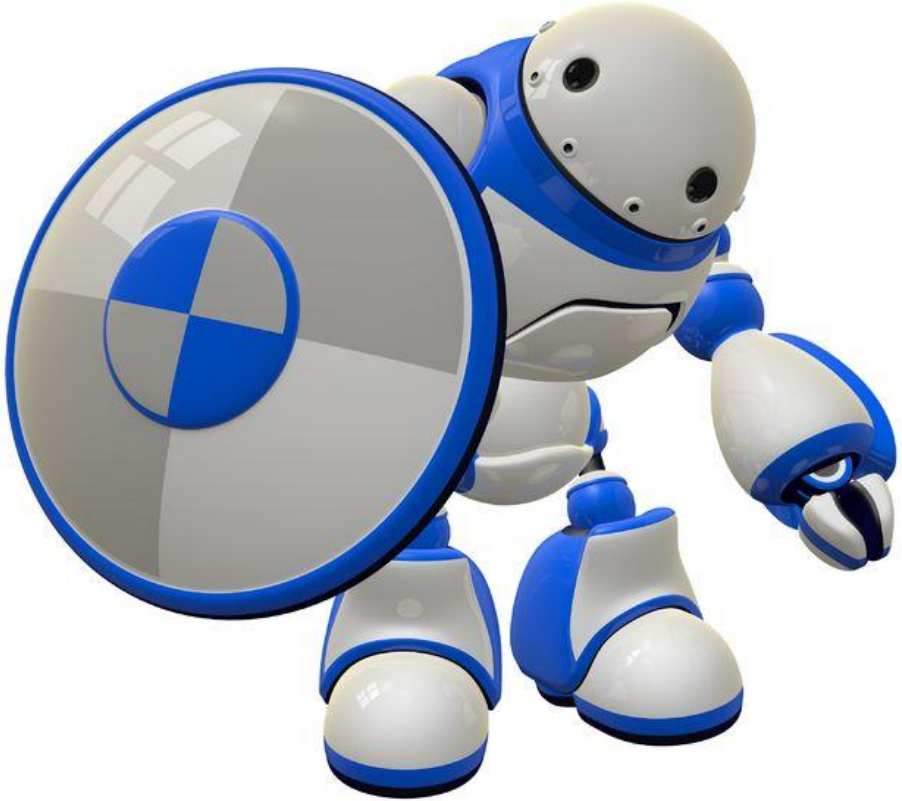
Jim Grey 1:11 PM
Finishing those off for the week?

Skyler Wilson 1:11 PM
Yup!

BoardBoat APP 1:12 PM
@skylerwilson done with offboarding. Here's link in case there were any errors: http://offboard.saasytech.com/21817

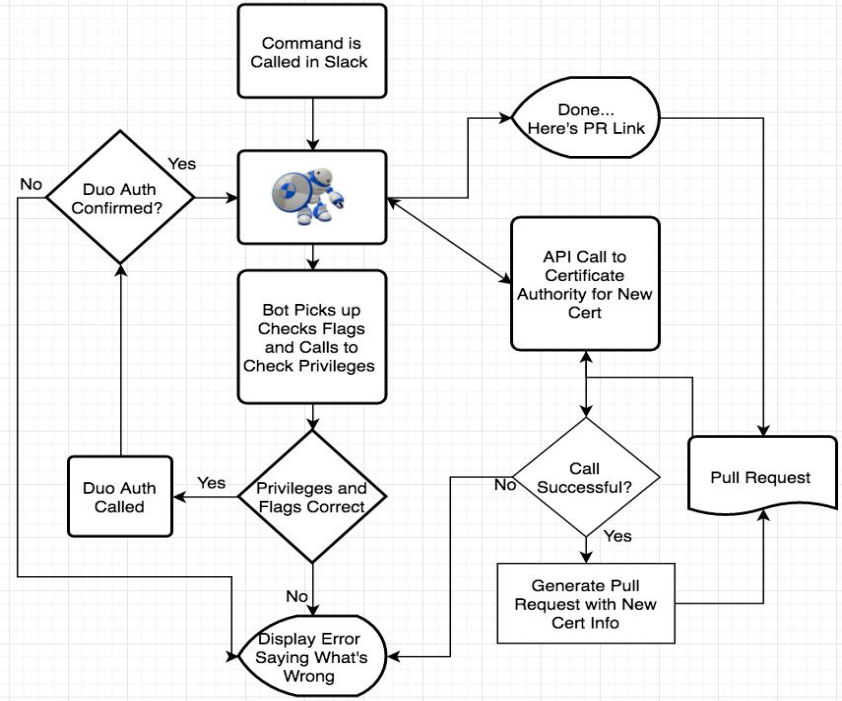
Skyler Wilson 1:14 PM
Sweet! No errors. Happy Friday @jimgrey!

Message #userboarding



Aegis - What it Does

- Listens for Command to Change Secret (if prod, requires Duo flag for Auth)
- After perm checks, Duo Authentication Request is made (which must be confirmed on caller's phone) before command execution continues.
- Certificate is renewed via calls to Certificate Vendor's API, and committed to a data repo with a pull request.
- Pull request link is returned to slack channel for review.



Tatum Scott 1:03 PM
Hey @jimgrey, looks like somebody deployed a frontend outside the firewall. Can you get the frontend baha tech cert renewed ASAP?

Jim Grey 1:03 PM
Sure! One sec.

Jim Grey 1:04 PM
/cert renew frontend baha

Aegis APP 1:04 PM
You're allowed, but forgot a duo token.

Jim Grey 1:05 PM
/cert renew frontend baha duo

Aegis APP 1:06 PM
Cert renewed! Here's link for review: http://cote.saasytech.com/saasytech/aegis_lock/pull/10

Tatum Scott 1:06 PM
Awesome!! Will get the reviewed right away.

Message #my-first-story

What Security Automation Can Do?


Research
-Marketing
-Customer
JANUARY
FEBRUARY
MARCH
APRIL
MAY
30%
IDEAS
ACTION
PLAN
Tel 1011 3
Send E-mail

How?

How? Who?

How? Who? With What Resources?

How? Who? With What Resources?

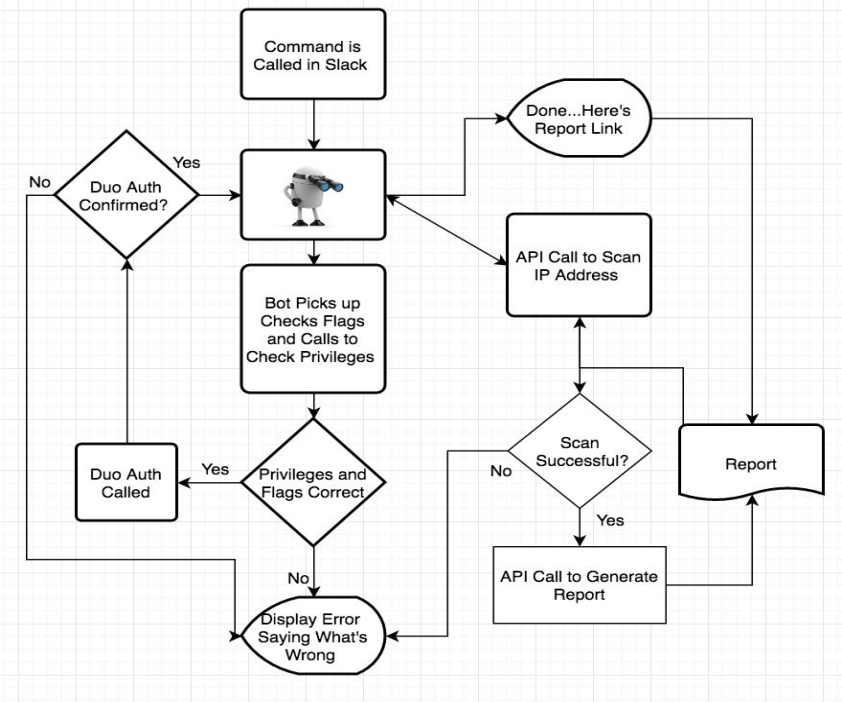
Starting from Scratch

Story Time: The “Should” from Scratch


GOD
IS DOPE.

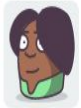
Bino - What it Does

- Listens for Commands to Scan IP
- Does Checks & Duo Auth (same as the others)
- Post checks, Bino makes an API call to scan the specified IP, then an API call for the results if the scan succeeds
- Bino then calls to generate report and returns the url for review and triage.



Bessie Mitchell 1:25 PM

So here's the demo of the bot running a scan and report on a single IP.



Bessie Mitchell 1:26 PM

/scan 192.168.3.24

Bino APP 1:29 PM

@bessiemitchell Done with your scan on 192.168.3.24. Report for review can be found here:
http://cote.saasytech.com/saasytech/vuln/pull/10

Message #demospace


0%
100%


KEEP
CALM
AND
ITERATE
OFTEN

In Conclusion..

Things to Keep in Mind

This is the slide to photograph….

- **Security is the future and it WILL need to be an automated and cross-collaborative effort.**
- **Security Automation that we Can Do:**
  - **User Management**
  - **Quickly Changing (or Rolling) Secrets**
- **Security Automation We Should be Doing :**
  - **Proactive and data-driven**
  - **Using present tools we have with a security context, and visa versa.**
  - **How?**
    - **Cross-team Collaboration**
    - **Input, Iteration (aka Change)**

Thank You!

Jamesha Fisher
Twitter/LinkedIn: jamfish728 **Mail:** me@jam.fish