https://tinyurl.com/CNCF-Champions



Championing Security:
Scaling Security At Every Level





@mcdwayne
@mcdwayne

The Story Of Leslie





Works at an insurance company

Accountant

Logs into 6 systems a day

MFA enabled 👍

Believes security is important

@mcdwayne



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

@mcdwayne



Tr

Dear valued cu

We have recie
following amou

If this informati
account. As a s
your personal i

http://www.trust

Once you have
discrepency. W

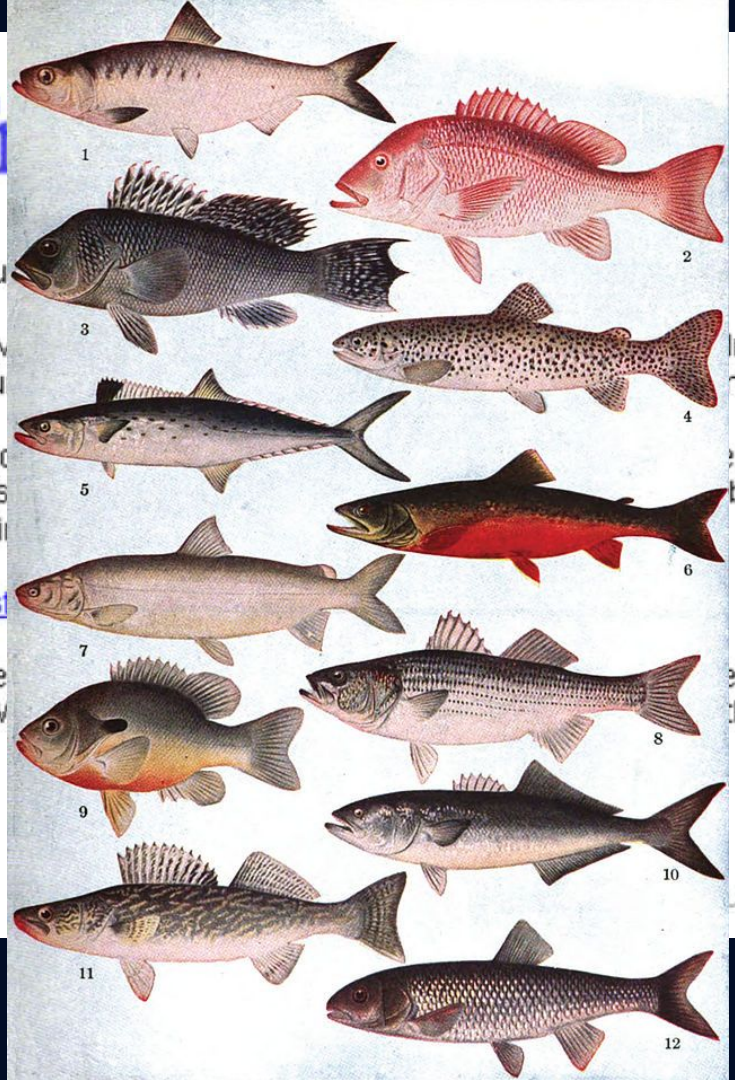
Thank you,
TrustedBank

raw the
ntry: $135.25.

ess to your
below to verify

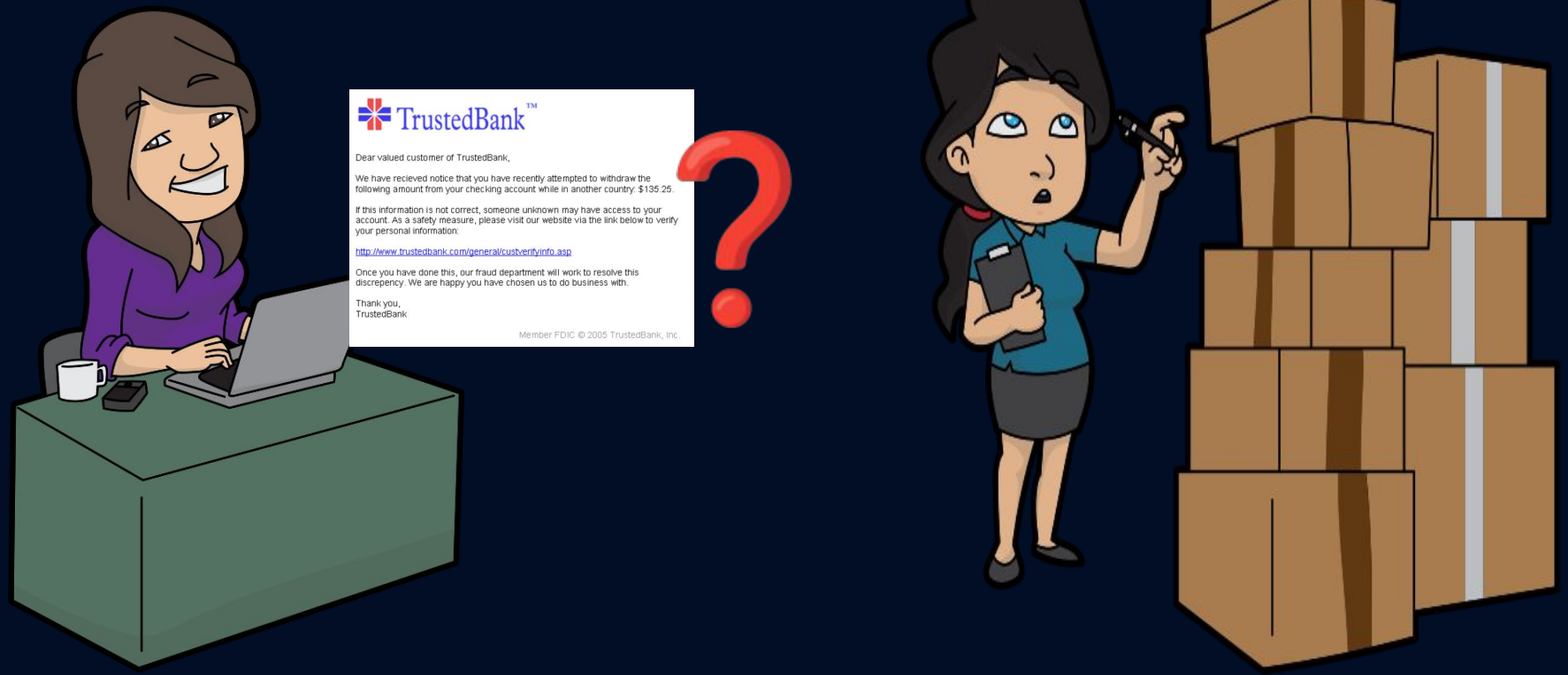
e this
h.

ustedBank, Inc.



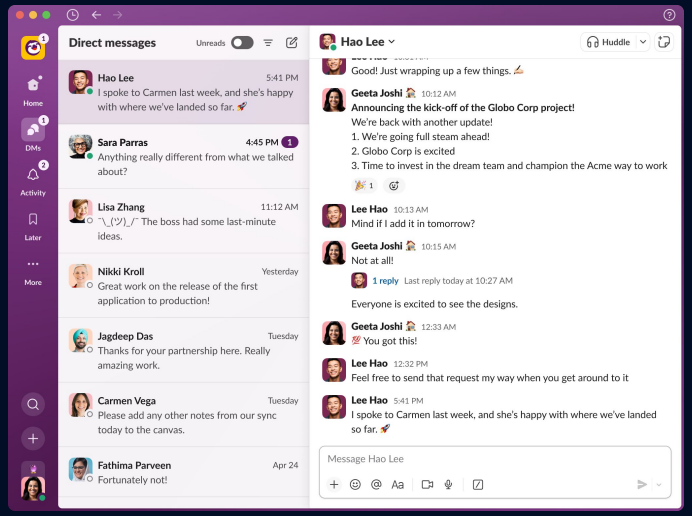


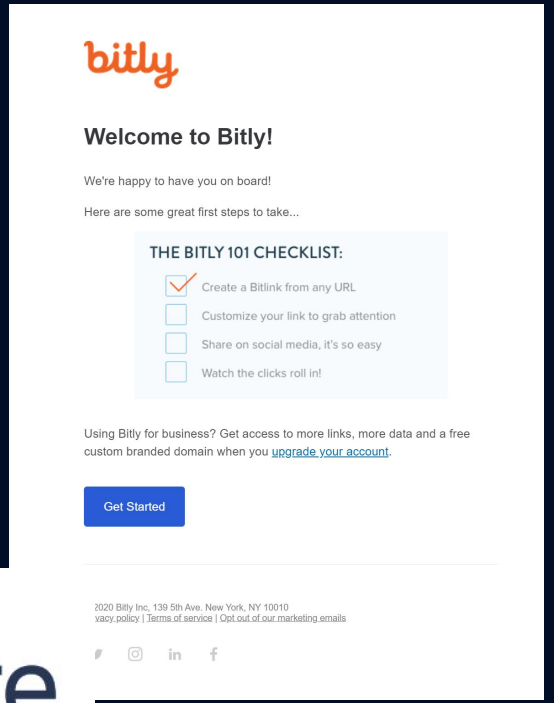
@mcdwayne


TrustedBank™
Dear valued customer of TrustedBank,
We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.
If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information.
http://www.trustedbank.com/general/custverifyinfo.asp
Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.
Thank you,
TrustedBank
Member FDIC © 2005 TrustedBank, Inc.

@mcdwayne







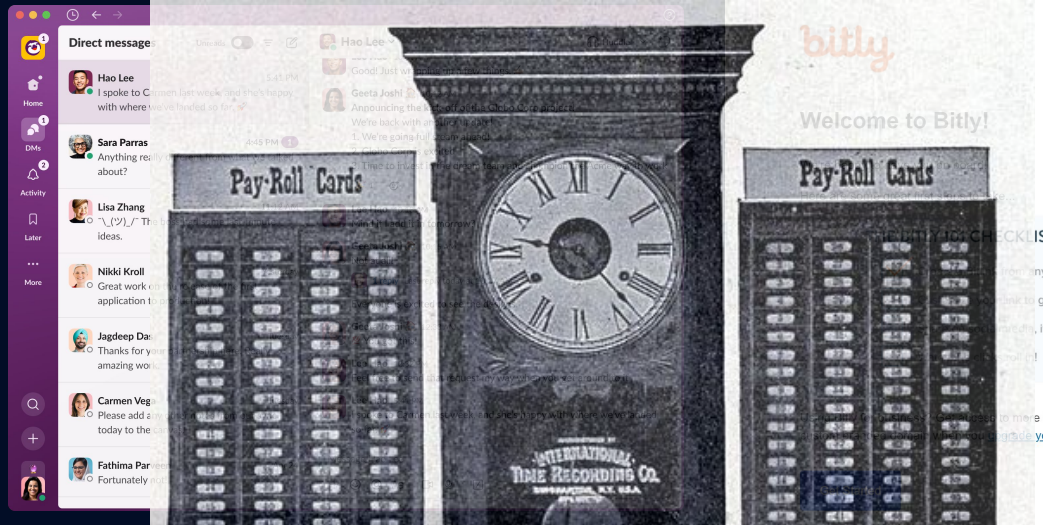




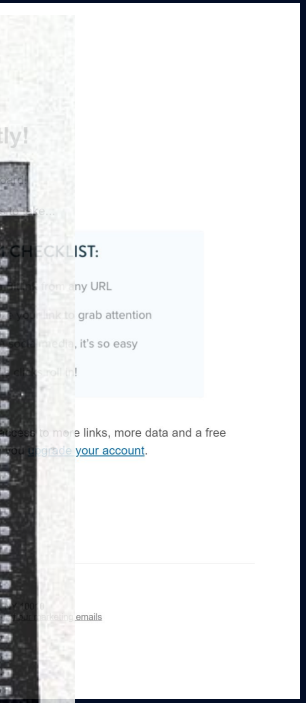


@mcdwayne
@mcdwayne





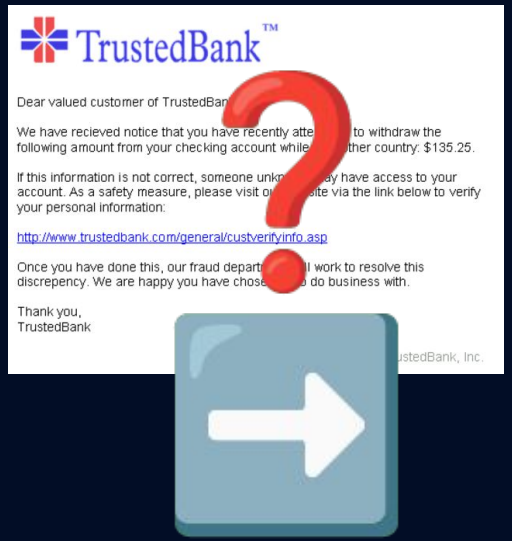






@mcdwayne
@mcdwayne





SEC



@mcdwayne

SEC





@mcdwayne

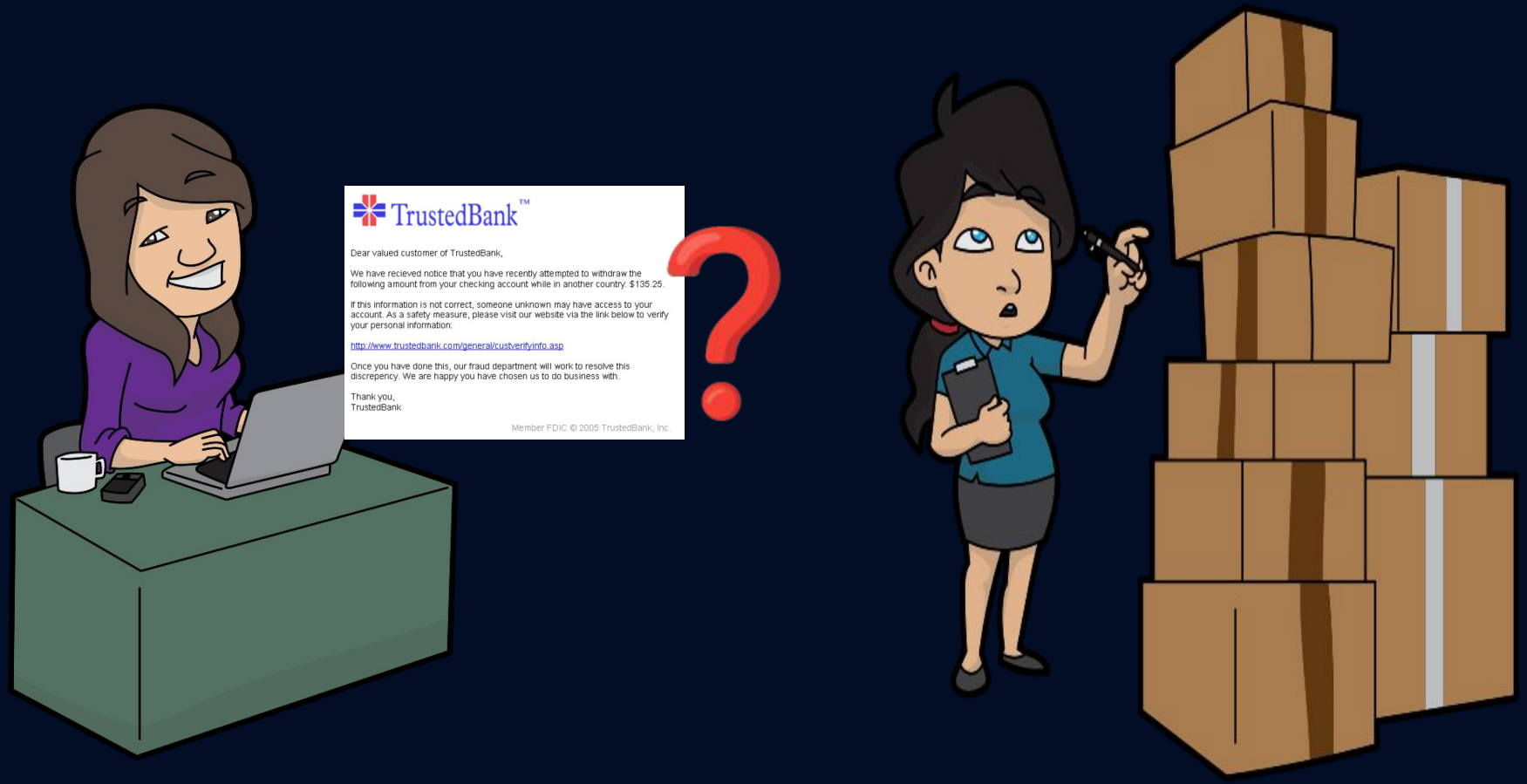




@mcdwayne

But what if?




TrustedBank™
Dear valued customer of TrustedBank,
We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.
If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information.
http://www.trustedbank.com/general/custverifyinfo.asp
Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.
Thank you,
TrustedBank
Member FDIC © 2005 TrustedBank, Inc.



@mcdwayne



GG-Test-Sl...

Upgrade Plan

Threads
Drafts & sent

Channels
general
gg
private-channel
random
security-party
Add channels

Direct messages
1dwayne.mcdaniel you
Add coworkers

Apps
GitGUardianSlack
Honeytoken Alerts
Add apps

security-party

1 Canvas

Today

slack

5:30 GUAC party!!!!

Who wants to learn about SLSA and GUAC? Well, who wants to eat some?
Come to our Security Tuesday 15-minute stand up party this afternoon and show on some guacamole while we tell you why we are adopting GUAC
Graph for Understanding Artifact Composition!

?? Is this something you need to use daily? - NO!
?? How will I need to use it? - This is related to SBOMs -
The more you know.....
More info in the thread

image.png



Message #security-party



@mcdwayne
@mcdwayne



security-party

Get Notifications for All Messages

Huddle

About | Members 1 | Integrations | Settings

Channel name Edit

security-party

Topic Edit

Who has the best Smishing story? Contest ends at end of the month.
LINK TO THREAD

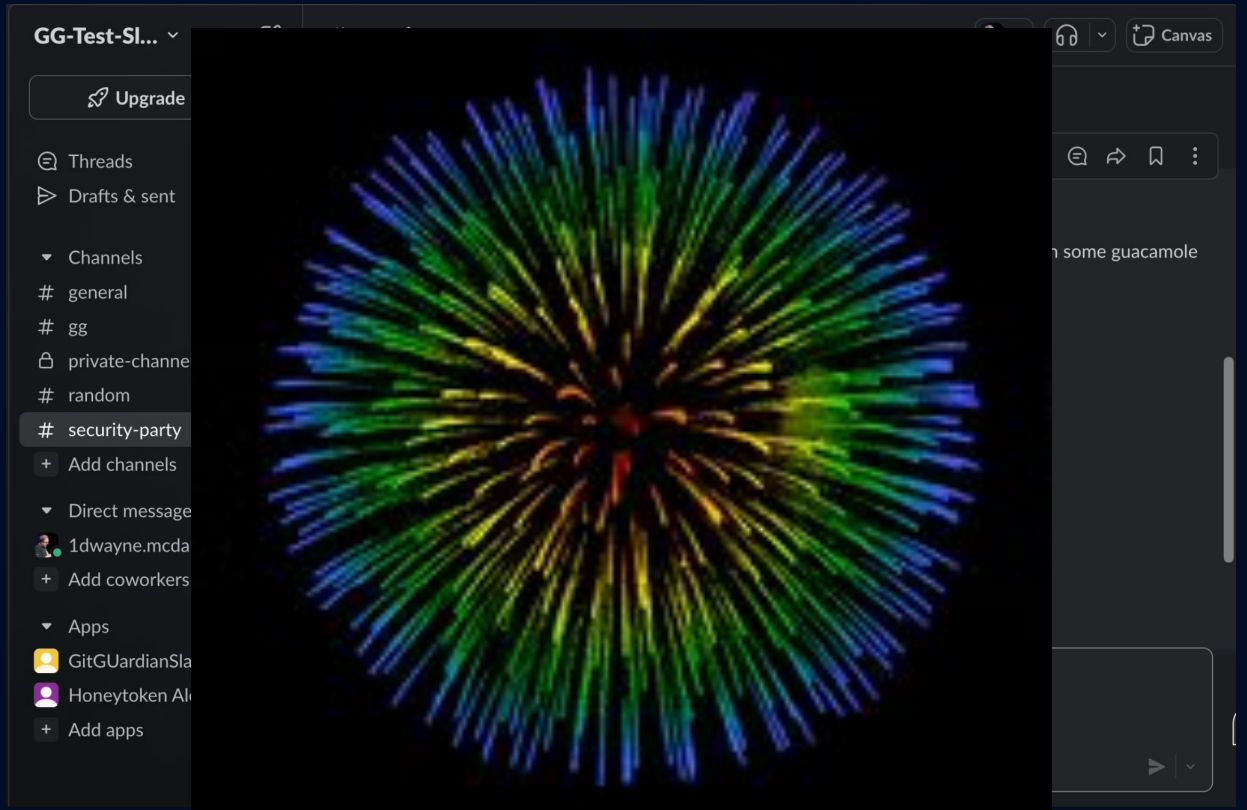
Description Edit

Welcome to the security party!!!
Ask your questions, and let's learn together and have some fun!
Yes, we will also make our company more secure together.



@mcdwayne




GG-Test-Sl...
Upgrade
Threads
Drafts & sent
Channels
general
gg
private-channe
random
security-party
Add channels
Direct message
1dwayne.mcda
Add coworkers
Apps
GitGUardianSla
Honeytoken Al
Add apps
Canvas
some guacamole



@mcdwayne



GG-Test-Sl...
Upg
Threads
Drafts & s
Channels
general
gg
private-ch
random
security-p
Add chan
Direct me
1dwayne.
Add cowo
Apps
GitGUardi
Honeytok
Add apps

security-party

1

Today

Thanks @leslie You ROCK!

We will review and s... already known and get back to you.
In the meantime, please don't open it again. Select it from the inbox or folder it is in and hit the Report Spam button above the subject lines, like we show in the pic:

It's the stop sign looking one.

Thanks again! (edited)

Screenshot 2024-04-04 at 9.31.36 PM.png

Search mail

1 reply Today at 9:35 PM

1dwayne.mcdaniel 9:35 PM
replied to a thread: Reporting a phishing email Autobo...
Congrats @Leslie, this is a new one, so you are now entered into the monthly New Phish drawing for the $25 amazon gift card!

Canvas

cdwayne
cdwayne



She now is curious about this whole “smishing” thing.

She checks the security channel from time to time.

She becomes known as the team member that knows security.

She becomes…

@mcdwayne
@mcdwayne



A Security Champion



@mcdwayne

Hi. I’m Dwayne.



Dwayne McDaniel

- I live in Chicago
- I’ve been a Developer Advocate since 2016
- Co-host of The Security Repo Podcast
- On Twitter @mcdwayne
- mcdwayne@mastodon.social
- LinkedIn @dwaynemcdaniel
- Happy to chat about anything, hit me up
- Outside of tech, I love improv, karaoke and going to rock and roll shows!

@mcdwayne

About GitGuardian



GitGuardian is the code security platform for the DevOps generation.

- Secrets Detection and Remediation
- Honeytokens
- Source Composition Analysis
- IaC Misconfiguration Scanning
- Public Monitoring of GitHub

@mcdwayne
@mcdwayne















@mcdwayne
@mcdwayne



All You Need is Guest - https://www.youtube.com/watch?v=dmbRpwP5L9s



@mcdwayne







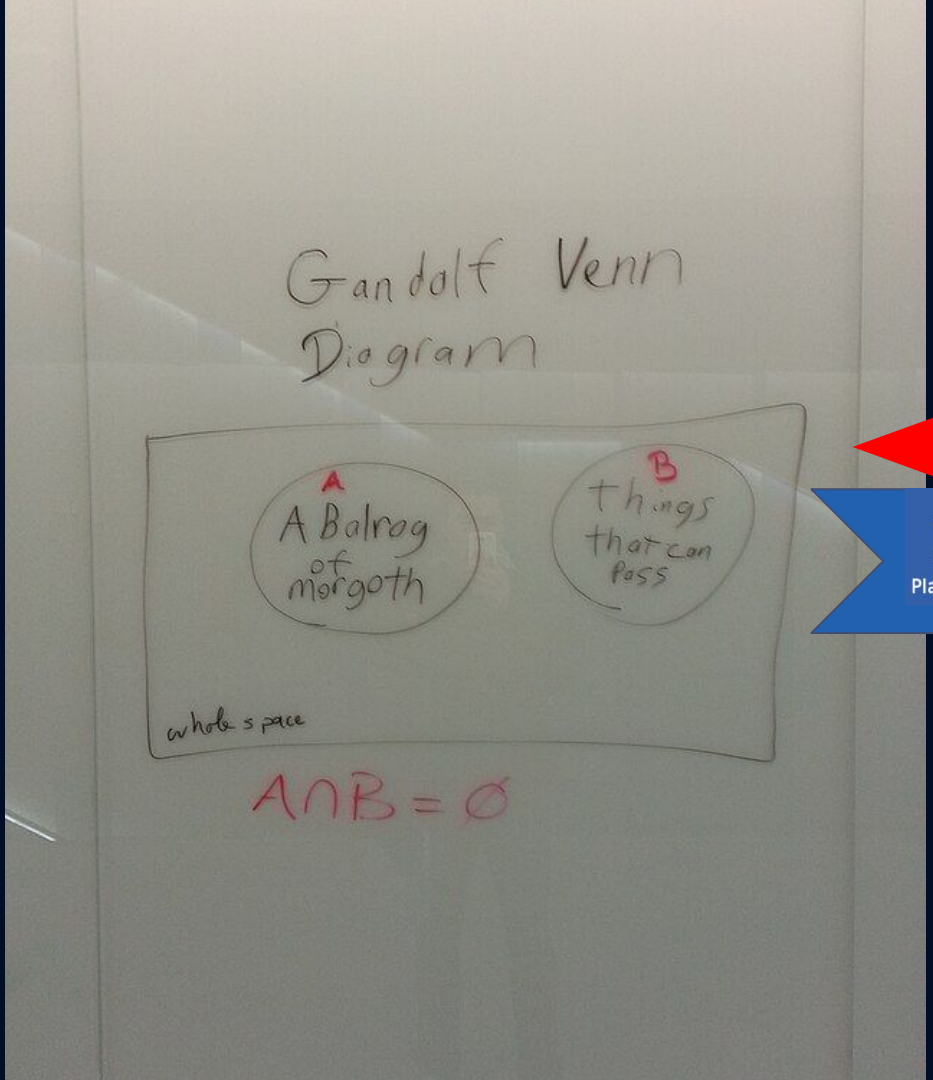








@mcdwayne
@mcdwayne



1 Planning
2 Analysis
3 Design
4 Implementation
5 Testing & Integration

@mcdwayne
@mcdwayne



1
lanning

2
Analysis

@mcdwayne

Creating A Security Campions Program





SECURITY CHAMPION
PROGRAM SUCCESS GUIDE

Building Security Champions

By Tanya Janca (SheHacksPurple) on October 13, 2021

OWASP®

OWASP
SECURITY CHAMPIONS
GUIDE

OWASP Security Champions Guide

@mcdwayne

What Is A Campions Program?



@mcdwayne

A Security Champion program spreads awareness of best practices by influencing organizational behavior toward better habits to reduce overall security risk.

Security Champions are non-security volunteers who receive additional training and incentives to represent security on their teams.

They act as liaisons, or points of contact, in both directions: from security to their team, and from their team to security.



@mcdwayne

Recipe:

- *Recruit*
- *Engage*
- *Teach*
- *Recognize*
- *Reward*
- *(Over)Communication*
- *Metrics & Data*
- *Don’t Stop!*



@mcdwayne

The Ten Key Principles for a Successful Security Champions Program

1. Be passionate about security
2. Start with a clear vision for your program
3. Secure management support
4. Nominate a dedicated captain
5. Trust your champions
6. Create a community
7. Promote knowledge sharing
8. Reward responsibility
9. Invest in your champions
10. Anticipate personnel changes





@mcdwayne

Some things to keep in mind before we go any further…





@mcdwayne





@mcdwayne





@mcdwayne



We will never have the staff, budget or time to do all the security work we want to do.

– Janca's law



@mcdwayne

1. Be passionate about security





@mcdwayne





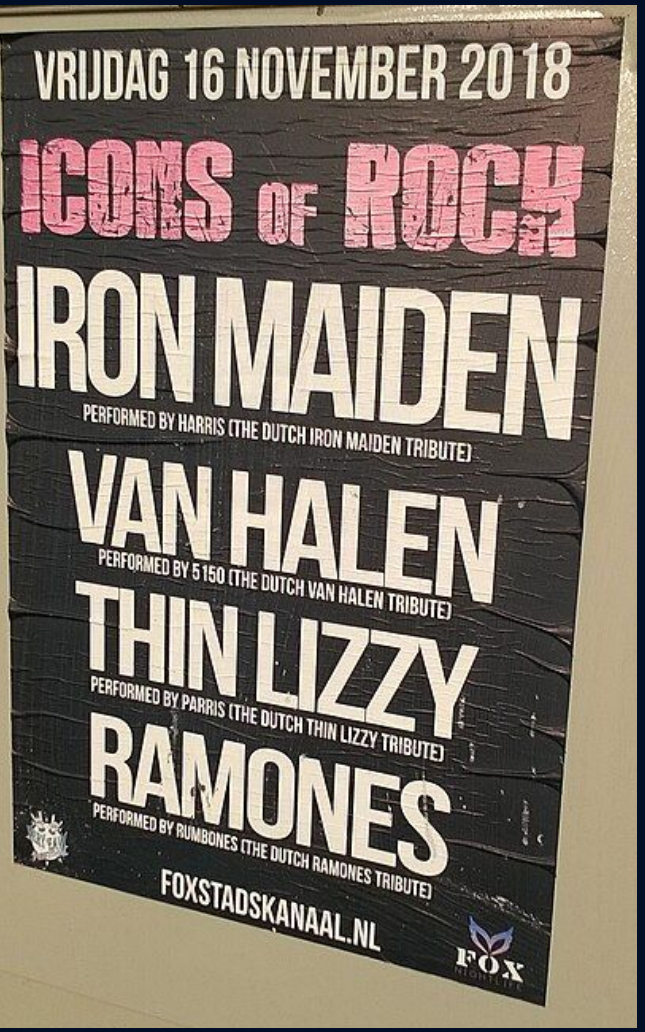
@mcdwayne

2. Start with a clear vision for your program





@mcdwayne



MAKE THE POSTER FIRST

- *When?*
- *What?*
- *Where?*
- *Why?*
- *Who?*
- *How?*

@mcdwayne
@mcdwayne

Write an internal blog post that defines how you succeeded.

Start with your ideal conclusion:

“This year, our Champions Program gained 30 members and boasts an active slack channel 40% of the company has used. Lead by Persons X and Y, we have helped 75% of all team members adopt MFA for critical tools and caught 100 attacks.”



@mcdwayne

3. Secure management support





@mcdwayne

Talk In Terms Of Risk

Risks are NOT threats.
Risks are NOT vulns.
Risks are NOT exploits.

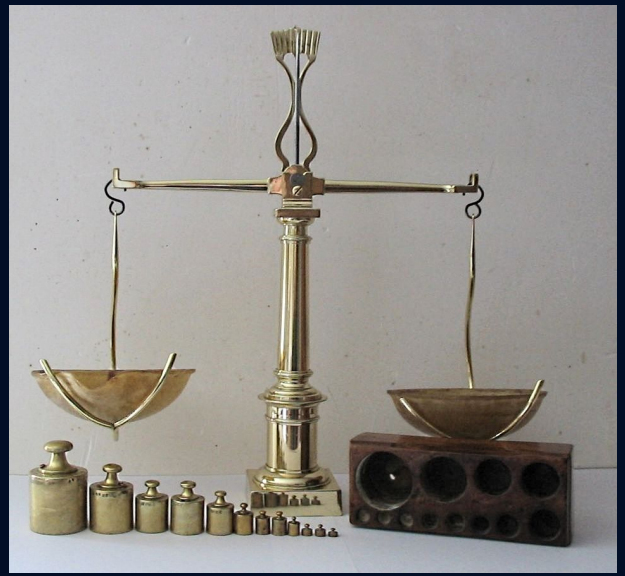
Risks are what you are set to lose if things go bad.

– [Walt Powell - Field CISO, CDW]



@mcdwayne

Lay out benefits vs low cost



This should be a win/win situation



@mcdwayne
@mcdwayne

4. Nominate a dedicated captain(s)





@mcdwayne





Example of a Kanban Board

Backlog	In Progress (3)	Peer Review (3)	In Test (1)	Done	Blocked
Fast Track/ Defect					

@mcdwayne

@mcdwayne

5. Trust your champions



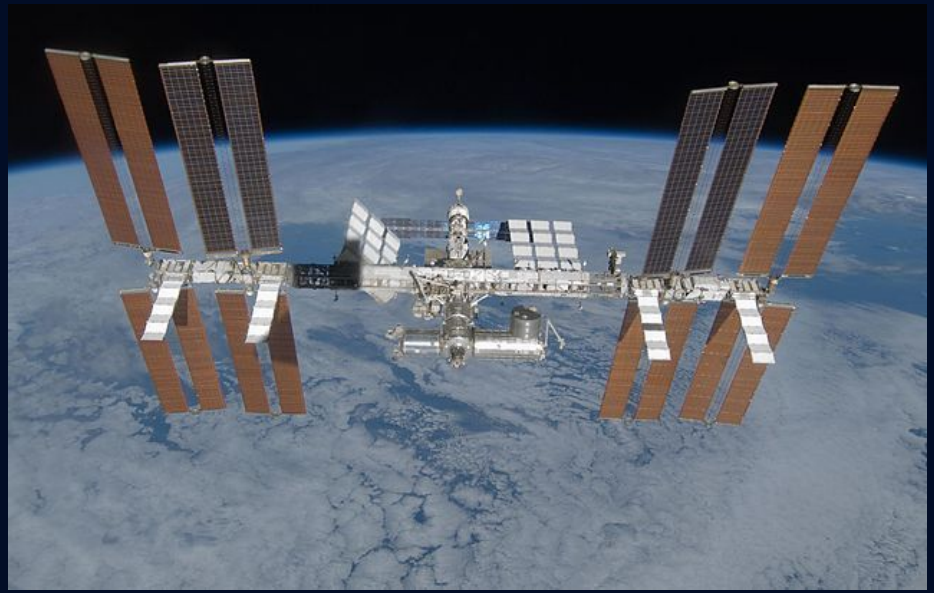


@mcdwayne

Active Listening



The Power Of “Yes, And…”



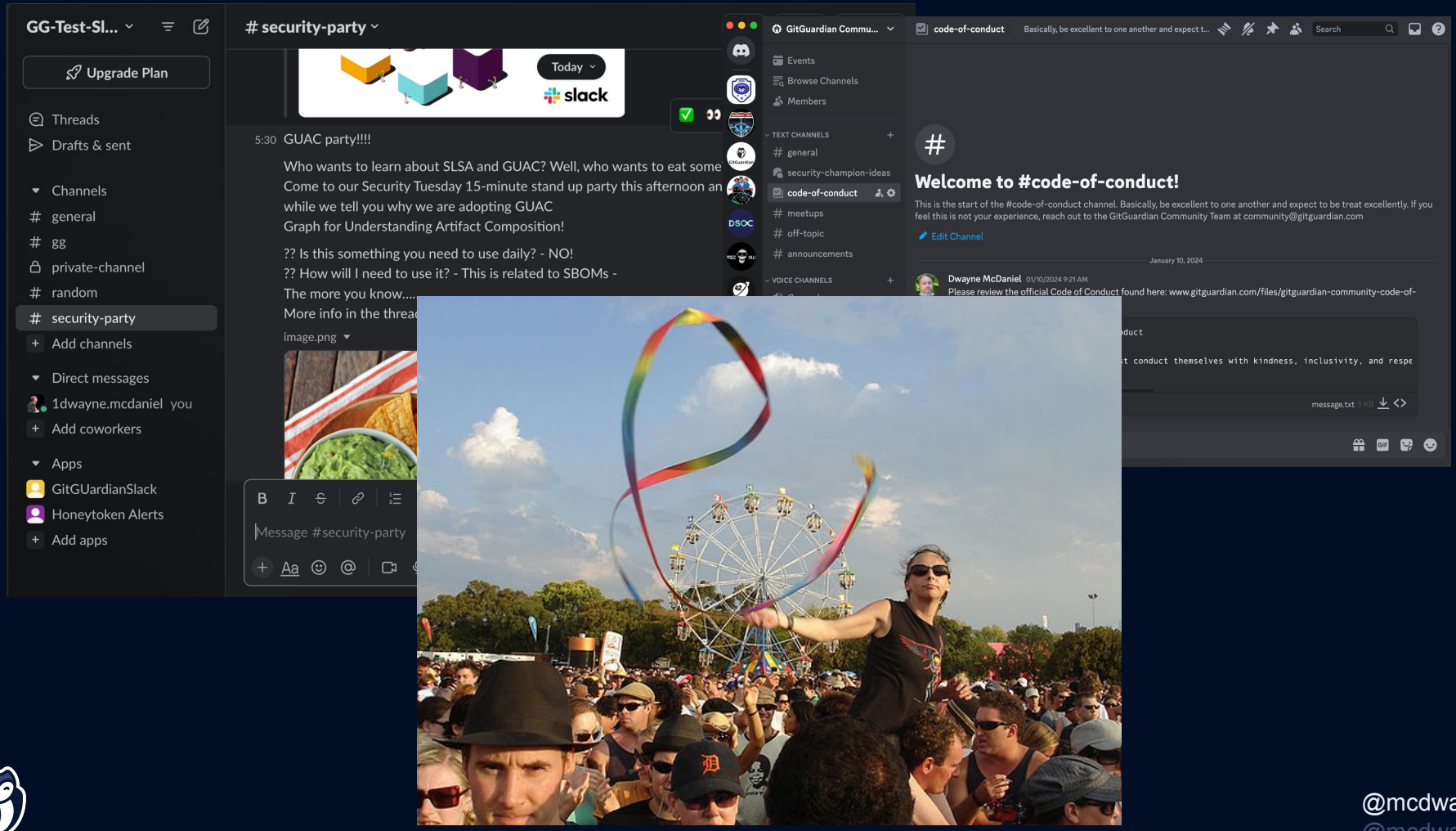
@mcdwayne

6. Create a community



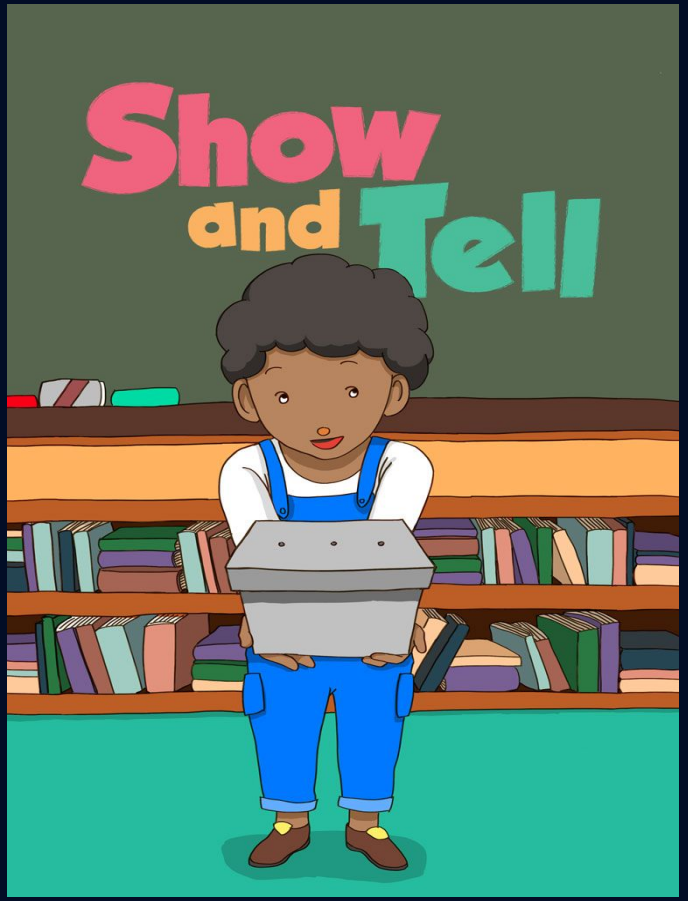


@mcdwayne


GG-Test-Sl...
Upgrade Plan
Threads
Drafts & sent
Channels
general
gg
private-channel
random
security-party
Add channels
Direct messages
1dwayne.mcdaniel you
Add coworkers
Apps
GitGUardianSlack
Honeytoken Alerts
Add apps
security-party
Today
slack
5:30 GUAC party!!!!
Who wants to learn about SLSA and GUAC? Well, who wants to eat some
Come to our Security Tuesday 15-minute stand up party this afternoon an
while we tell you why we are adopting GUAC
Graph for Understanding Artifact Composition!
?? Is this something you need to use daily? - NO!
?? How will I need to use it? - This is related to SBOMs -
The more you know....
More info in the threa
image.png
Message #security-party
GitGuardian Commu...
Events
Browse Channels
Members
TEXT CHANNELS
general
security-champion-ideas
code-of-conduct
meetups
off-topic
announcements
VOICE CHANNELS
code-of-conduct
Basically, be excellent to one another and expect t...
Search
Welcome to #code-of-conduct!
This is the start of the #code-of-conduct channel. Basically, be excellent to one another and expect to be treat excellently. If you feel this is not your experience, reach out to the GitGuardian Community Team at community@gitguardian.com
Edit Channel
January 10, 2024
Dwayne McDaniel 01/10/2024 9:21 AM
Please review the official Code of Conduct found here: www.gitguardian.com/files/gitguardian-community-code-of-
conduct themselves with kindness, inclusivity, and respe
message.txt

@mcdwayne







@mcdwayne





@mcdwayne

“You can’t pay someone enough to really care about your data. You can convince people to work to improve security for their bank accounts and kids.”

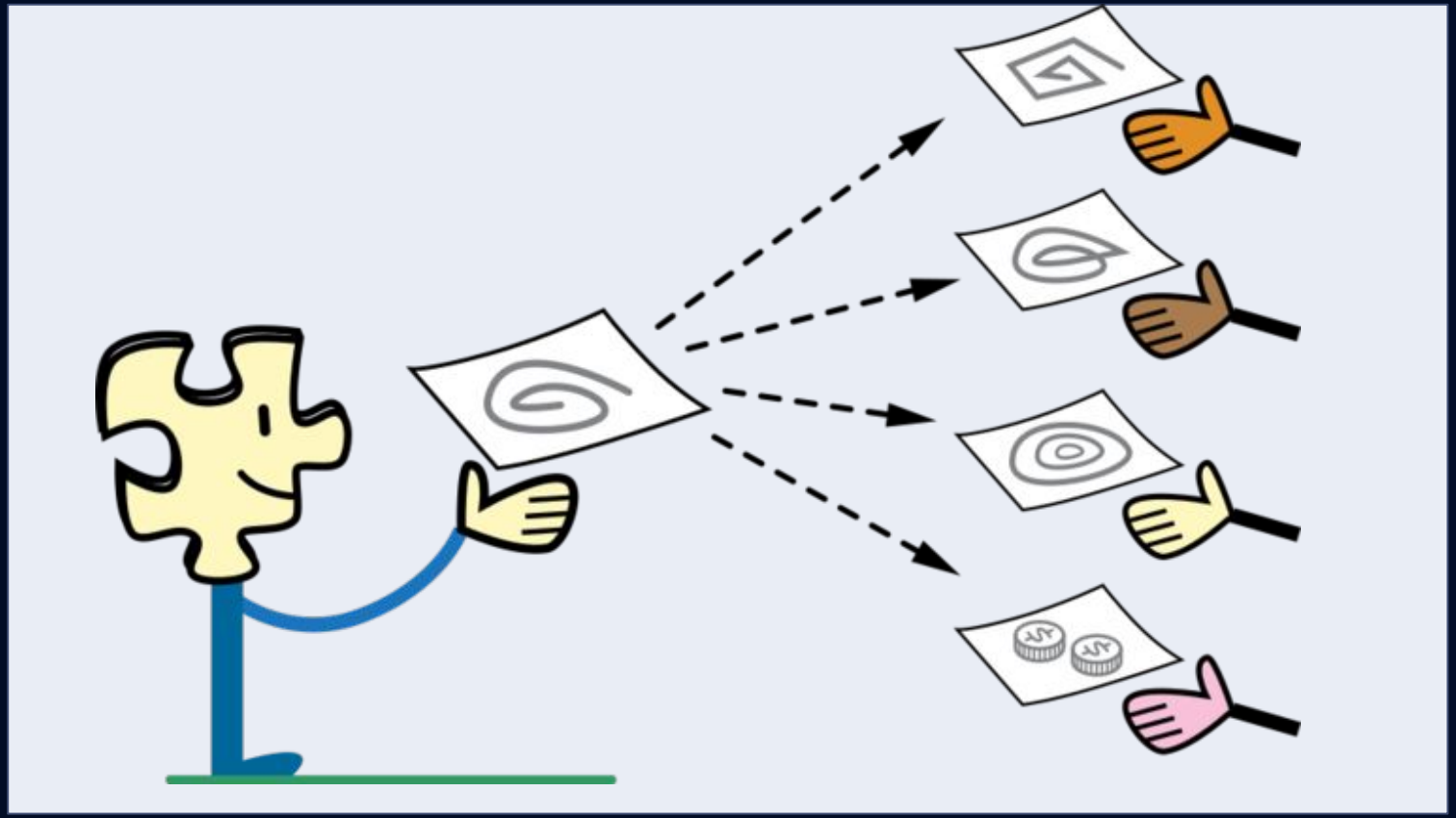
- Jayson E. Street

If MFA is a way of life, they will always embrace it across your system too.



@mcdwayne

7. Promote knowledge sharing



@mcdwayne

Security is CONSTANTLY shifting





@mcdwayne

Encourage link sharing and discussion

DARKREADING

KrebsonSecurity
In-depth security news and investigation

BLEEPINGCOMPUTER



@mcdwayne

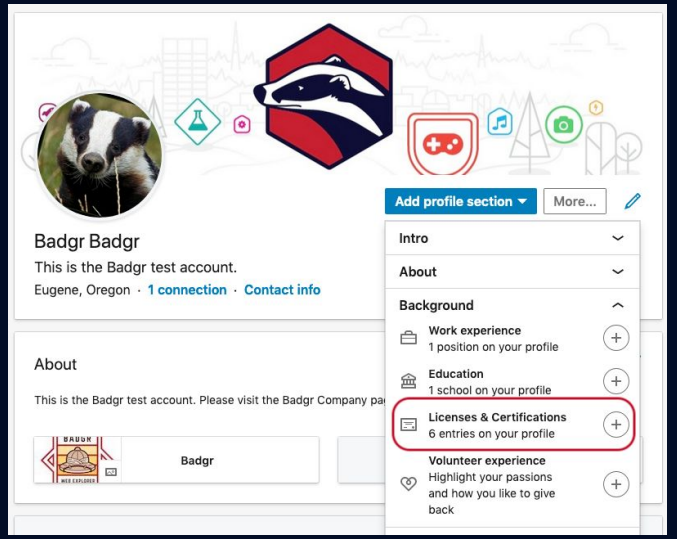
8. Reward responsibility



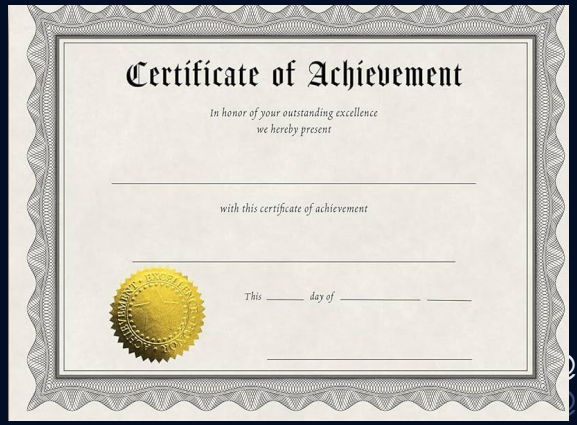
@mcdwayne











@mcdwayne
@mcdwayne



ANNUAL REVIEWS



@mcdwayne
@mcdwayne

9. Invest in your champions





@mcdwayne

- Send them to conferences!





- Vendor Lunch and Learns



- Certifications/
  Continuing Education Units



@mcdwayne

10. Anticipate personnel changes



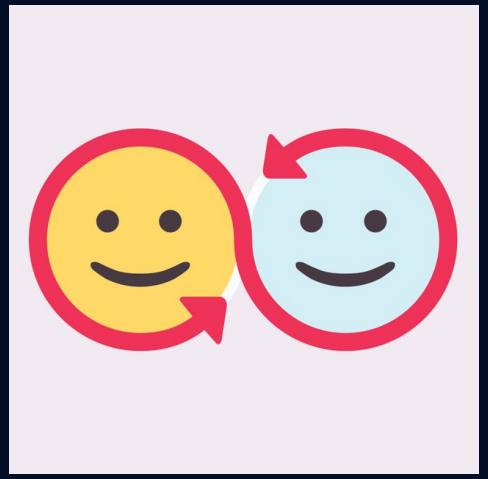


@mcdwayne



@mcdwayne

Rotate captains at regular intervals





Listen to the feedback

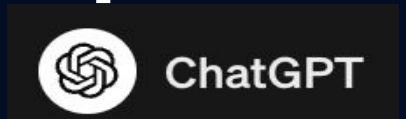
@mcdwayne

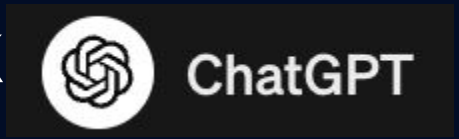
Bonus Advice



LEVERAGE AI!!!

- Need an opinion? Ask 

- Need jumping off point for a description for a lunch and learn? Ask 

- Need some art ideas for part of the project? Ask 



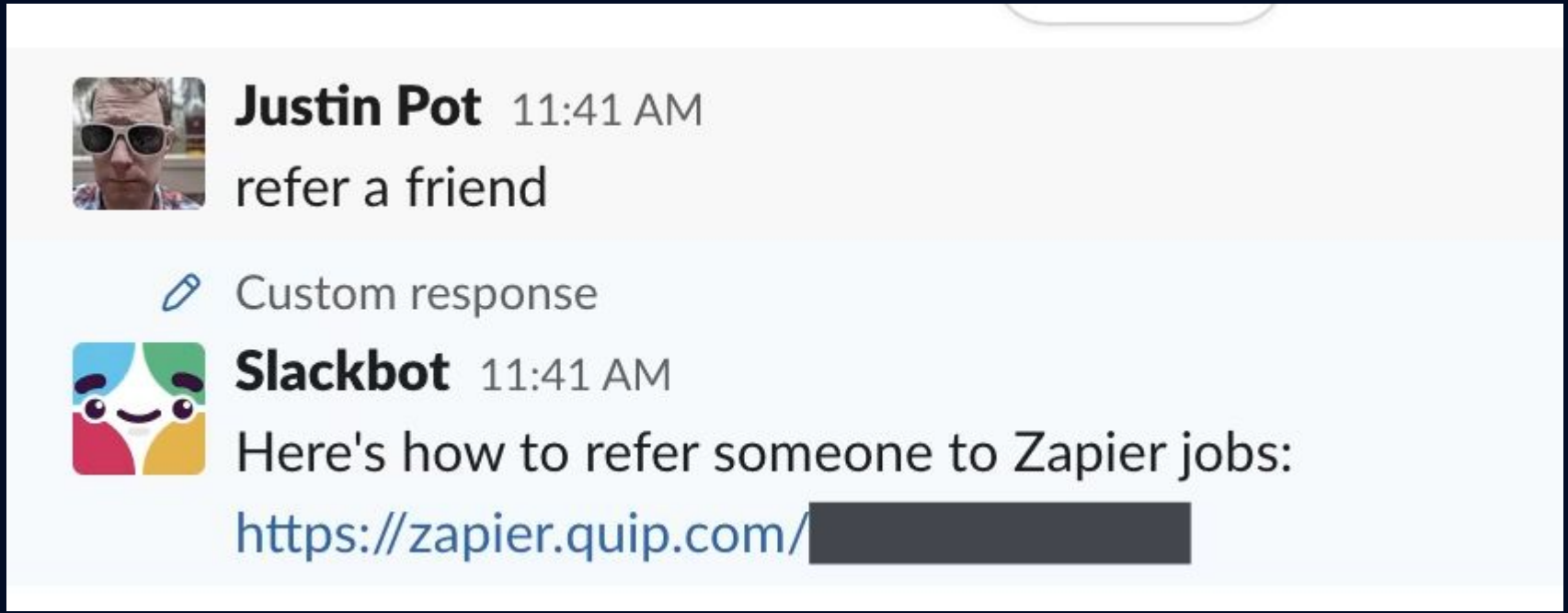
@mcdwayne

Enlist designers



@mcdwayne

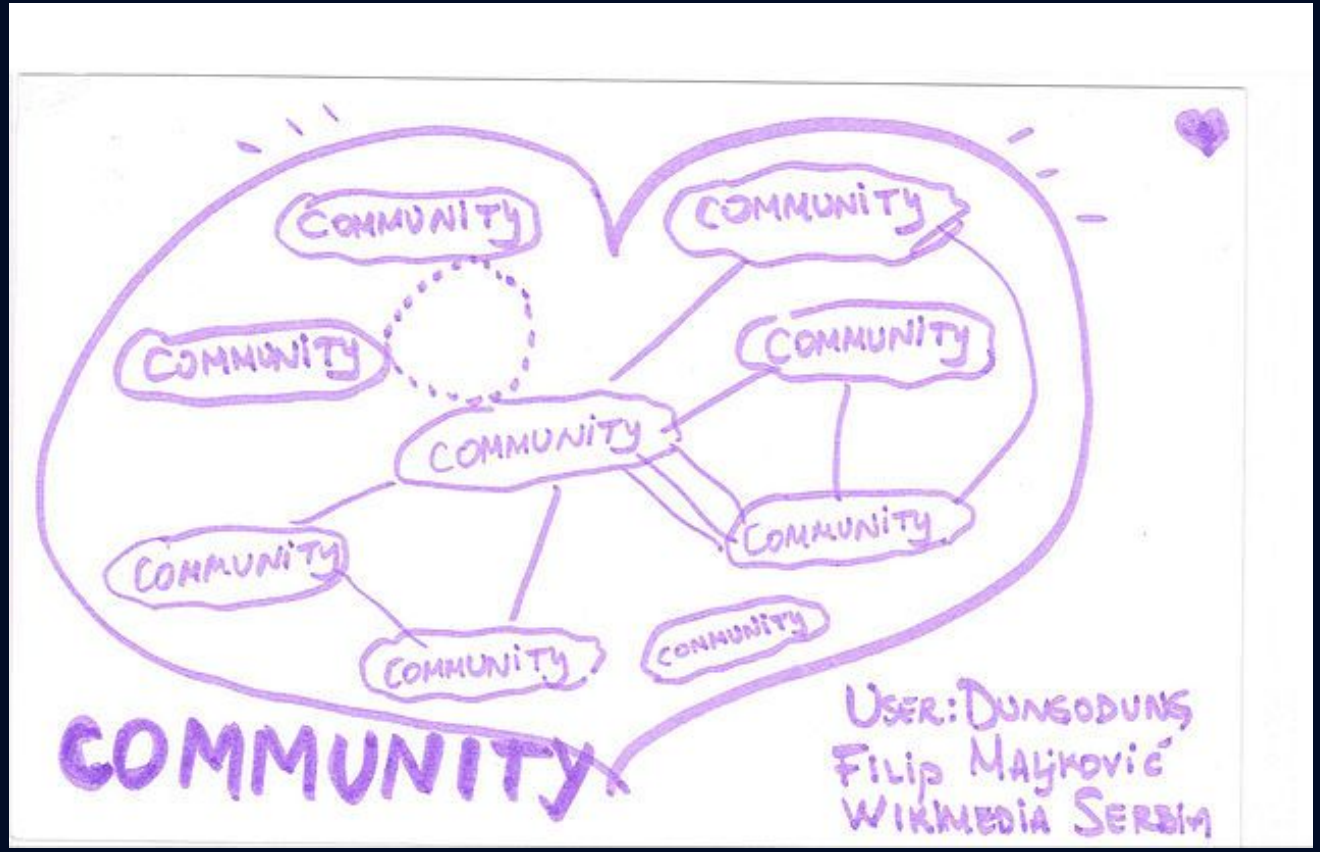
Automate the automatable with Chatbots/Knowledge bots





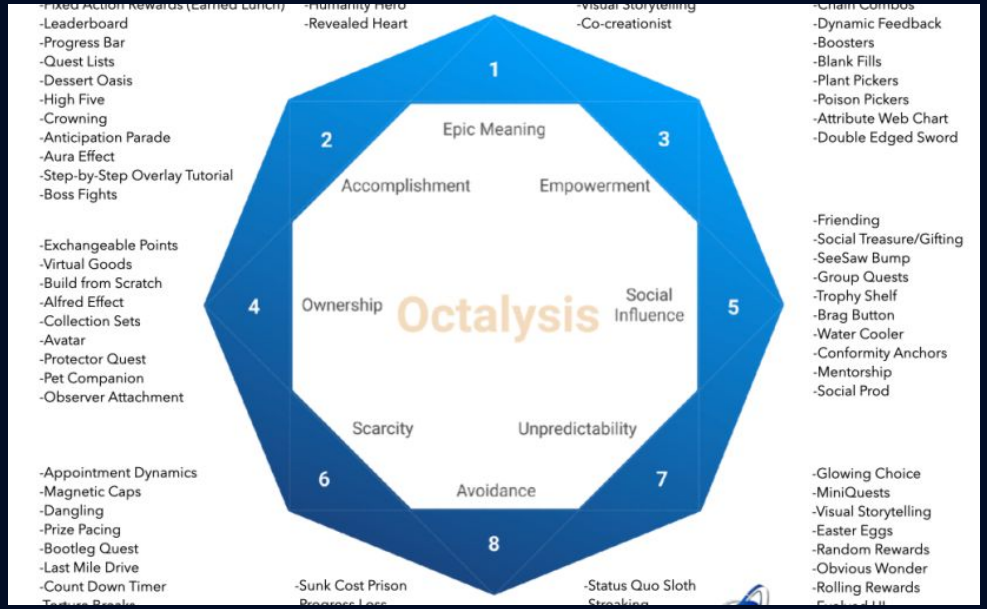
@mcdwayne

Make it personal



@mcdwayne

Work to understand what motivates each Champion



The Octalysis Framework for Gamification & Behavioral Design

Props to Dustin Lehr for introducing me to this

@mcdwayne
@mcdwayne

Remember Be inclusive!





@mcdwayne

Let’s Write The First Email RIGHT NOW!!!



“Hey <POTENTIAL CAPTAIN>,

I want to start a Security Champion Program. Basically, let’s get team members across the whole company to speak up about security and excited to learn more.

<Describe broad goals here>

Can we meet about this <Specific Time>?
I just added it to the calendar.

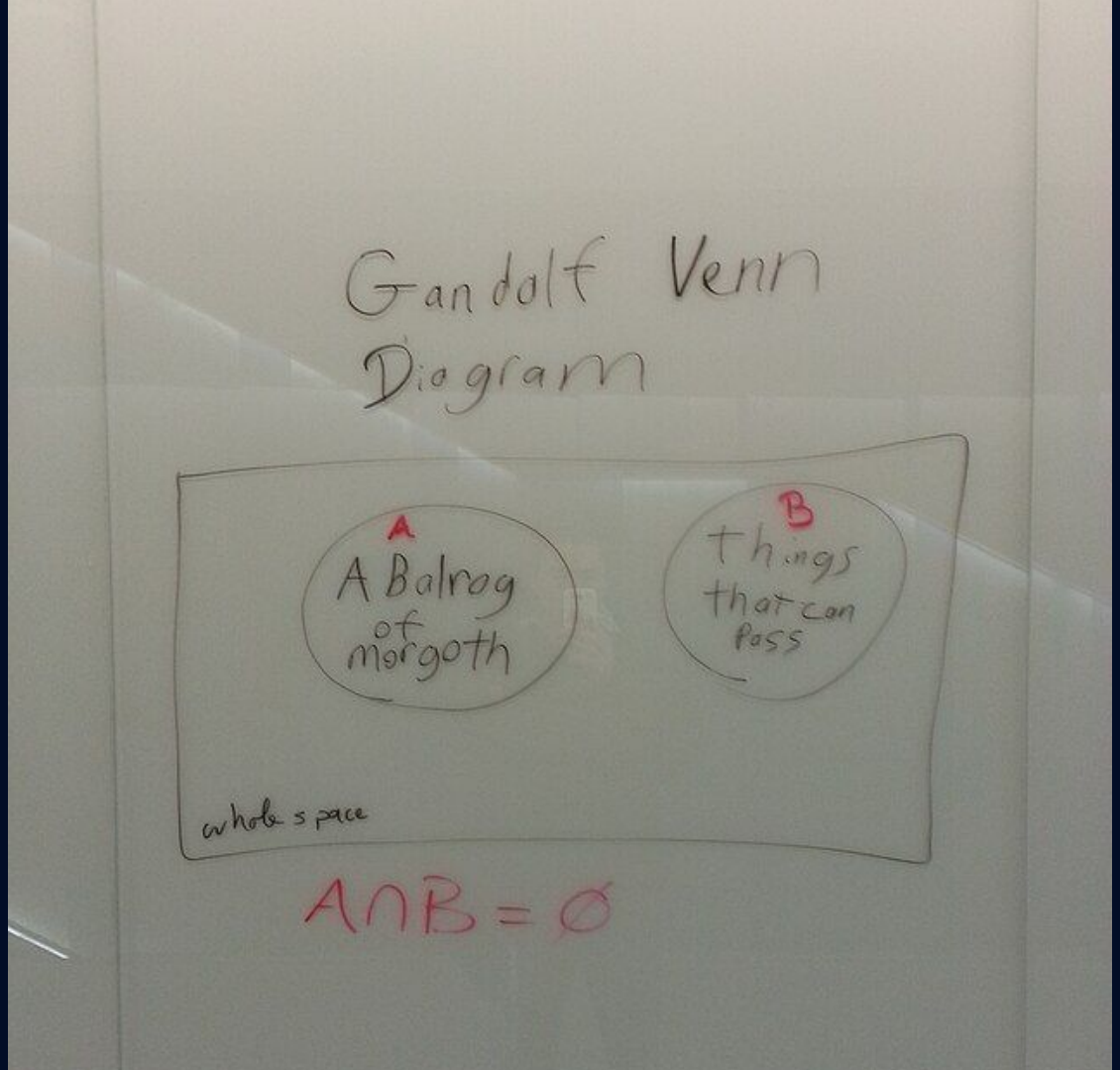
Signed
<me>
“



@mcdwayne

In Conclusion





1 Planning

2 Analysis

@mcdwayne

Every Team Deserves A Champion Security





@mcdwayne
@mcdwayne

MAKE THE POSTER FIRST

- *When?*
- *What?*
- *Where?*
- *Why?*
- *Who?*
- *How?*



@mcdwayne





@mcdwayne

Hi. I’m Dwayne.



Dwayne McDaniel

- I live in Chicago
- I’ve been a Developer Advocate since 2016
- Co-host of The Security Repo Podcast
- On Twitter @mcdwayne
- mcdwayne@mastodon.social
- LinkedIn @dwaynemcdaniel
- Happy to chat about anything, hit me up
- Outside of tech, I love improv, karaoke and going to rock and roll shows!

@mcdwayne

https://tinyurl.com/CNCF-Champions



Championing Security:
Scaling Security At Every Level





@mcdwayne
@mcdwayne



@mcdwayne