German OWASP Day 2024

German OWASP Day 2024

Security Inside Out: Developing Security Champions within your Teams

DIANA CALDERON

Agenda

- The need for Security Champions
- Building a Security Champions Program
- Key Takeaways

01

The need for Security Champions

Security & Compliance Challenges

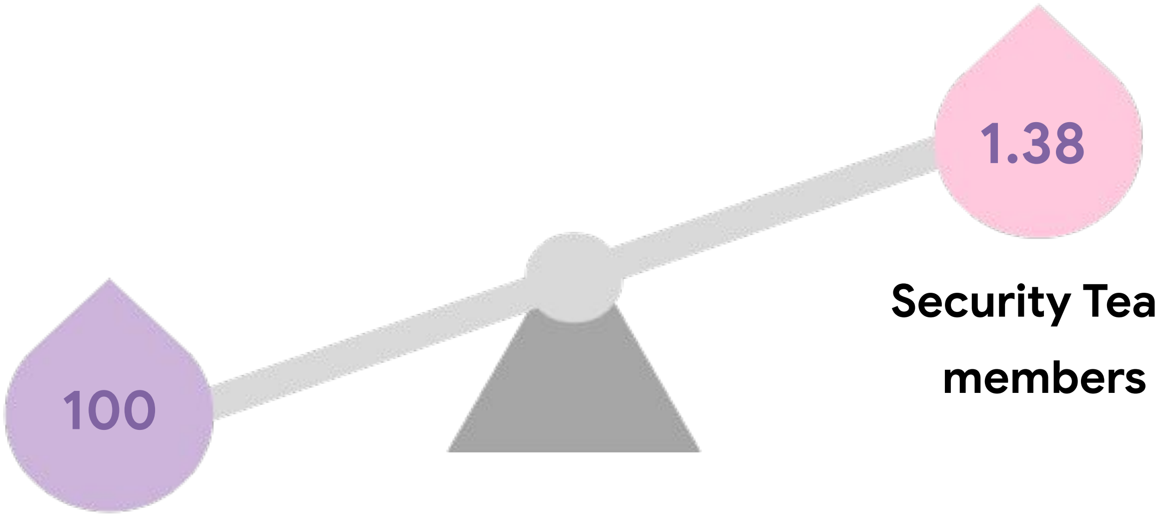
Security teams

- Security ratio disparity
- Lack of Scalability
- Limited Budget

Engineering teams

- Delivery Pressure
- Security is a bottleneck
- Adherence to compliance requirements

The Need For Security Champions



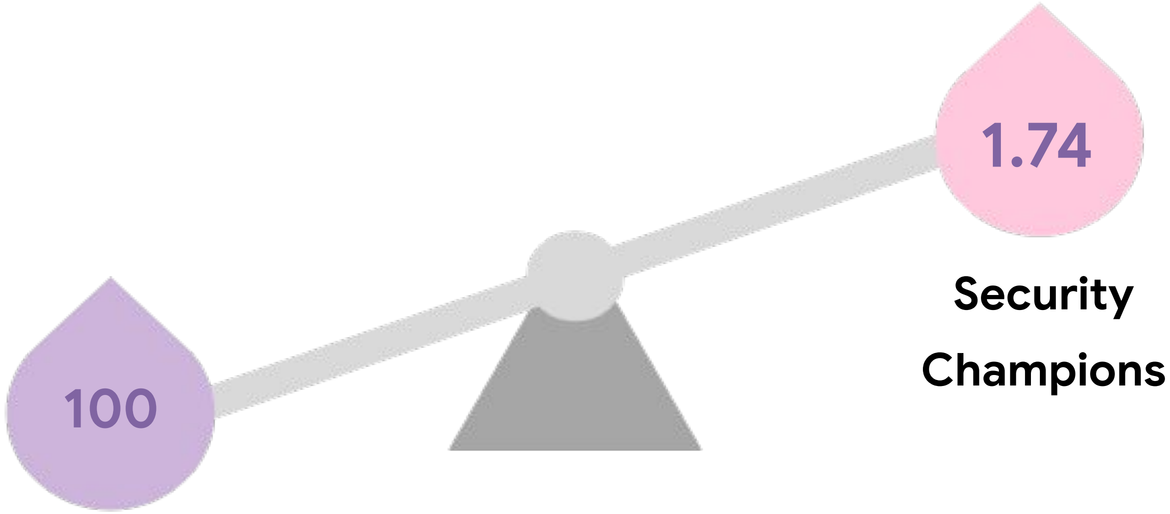
100

Developers

1.38

Security Team members

Median ratio of full-time SSG members to developers
BSSIM - 14



100

Developers

1.74

Security Champions

Median ratio of full-time Satellite members to developers
BSSIM - 14

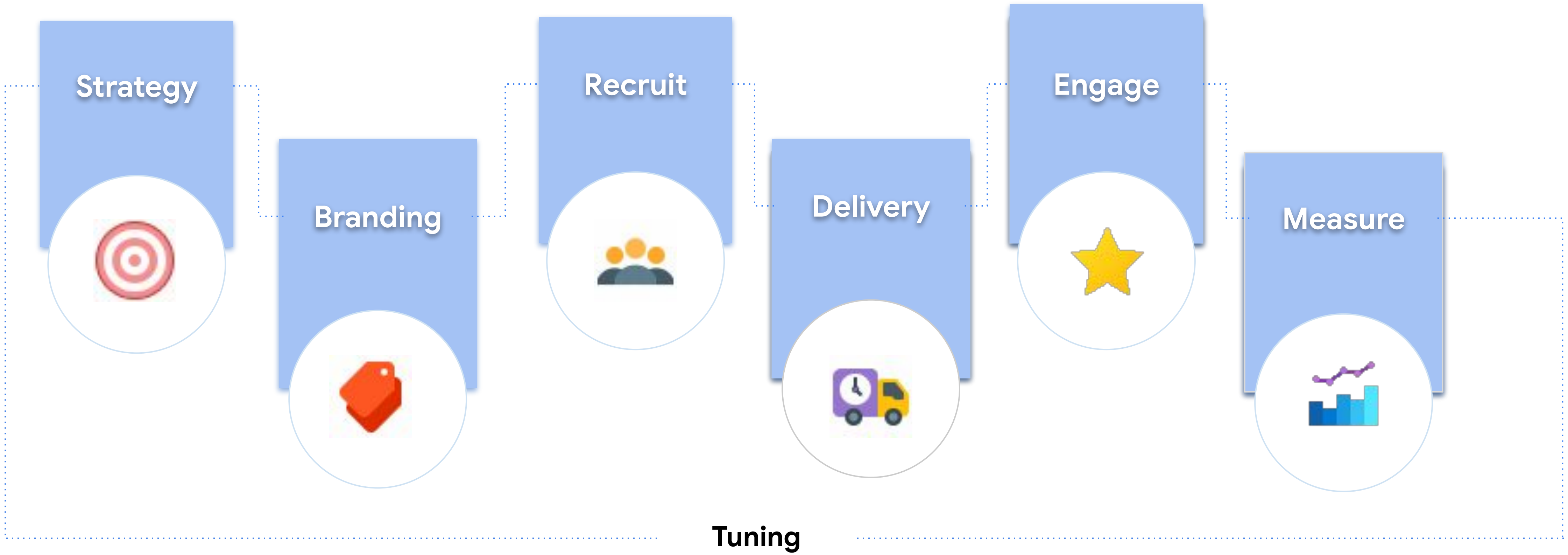
Source: Building Security in Maturity Model (BSIMM) 14 Report

German OWASP Day 2024

02

Building a Security Champions Program

A step-by-step approach



Let’s scale security!

Strategy: Look at the big canvas.

- Get executive buy in & budget
- Develop your Program objective, Mission and Vision
- Set achievable goals for your Security Champions program

BUY IN

Make the business case

GOALS

Set yearly goals

Branding: Make an Impact

- Advertise the existence of the program.
- Branding can help build Trust with the different audiences involved.

BRAND

Invest in a central brand.

VISUAL IDENTITY

Design a Logo/Mascot

SWAG

Merchandise, stickers, posters,

Recruit: Find and sign champions

- Formalize the Security Champion Role
- Ensure managers are on board and will give time to the security champions

START SMALL

Beg in the early days

THINK BIG

At least one champion per "team"

VALUE

Sell the value proposition

Delivery: Partnership in action (I)

- Establish Security Champions Levels
- Set up communication channels & build a knowledge base

LEVELS

Divide the program into multiple competency levels.

TRAINING & UPSKILLING

Basic training to speed up learning and prepare champs for complex scenarios.

KNOWLEDGE BASE

Primary source for answering security-related questions.

COMMS

Set up communication channels

Delivery: Partnership in action (II)

- Define clear roles & responsibilities
- Find key partnership areas: Threat Modeling, Testing scope, Pentesting & Finding remediation

Topics For Champions

SECURE CODING & ARCHITECTURE

- Formal training on secure coding & labs.
- Threat modelling training
- Baseline Security controls
- Secure architecture reviews
- Code Reviews
- How to fix the bugs they find

POLICIES

- Policies, standards and guidelines
- Support champs create missing guidelines
- How to be compliant
- Their role during an incident
- Security Consulting

TOOLING

- Custom training on tools they use
- How to install and configure tools
- Help them select the BEST tools
- Lunch and learns or hack-a-thons

Engage: Boosting and motivating retention

- Have fun, be creative and test.
- Champions stay when they feel appreciated, so over-communicate their contributions.

How to keep them engaged?

- **Tournaments, contests, CTFs**
- **Live Streams, webinars**
- **Newsletters, emails, posts.**
- **Security Champions corner**
- **Visibility & Recognition**
- **Networking**
- **Monetary Rewards**

Track & Measure Success

- Determine the ROI of the Security Champions program

CHAMPIONS

- Total Count
- Active Champions
- number of security champions onboarded
- Champions distribution

THREAT MODELLING

- number of threat models or threat modelling activities conducted
- number of findings from threat models

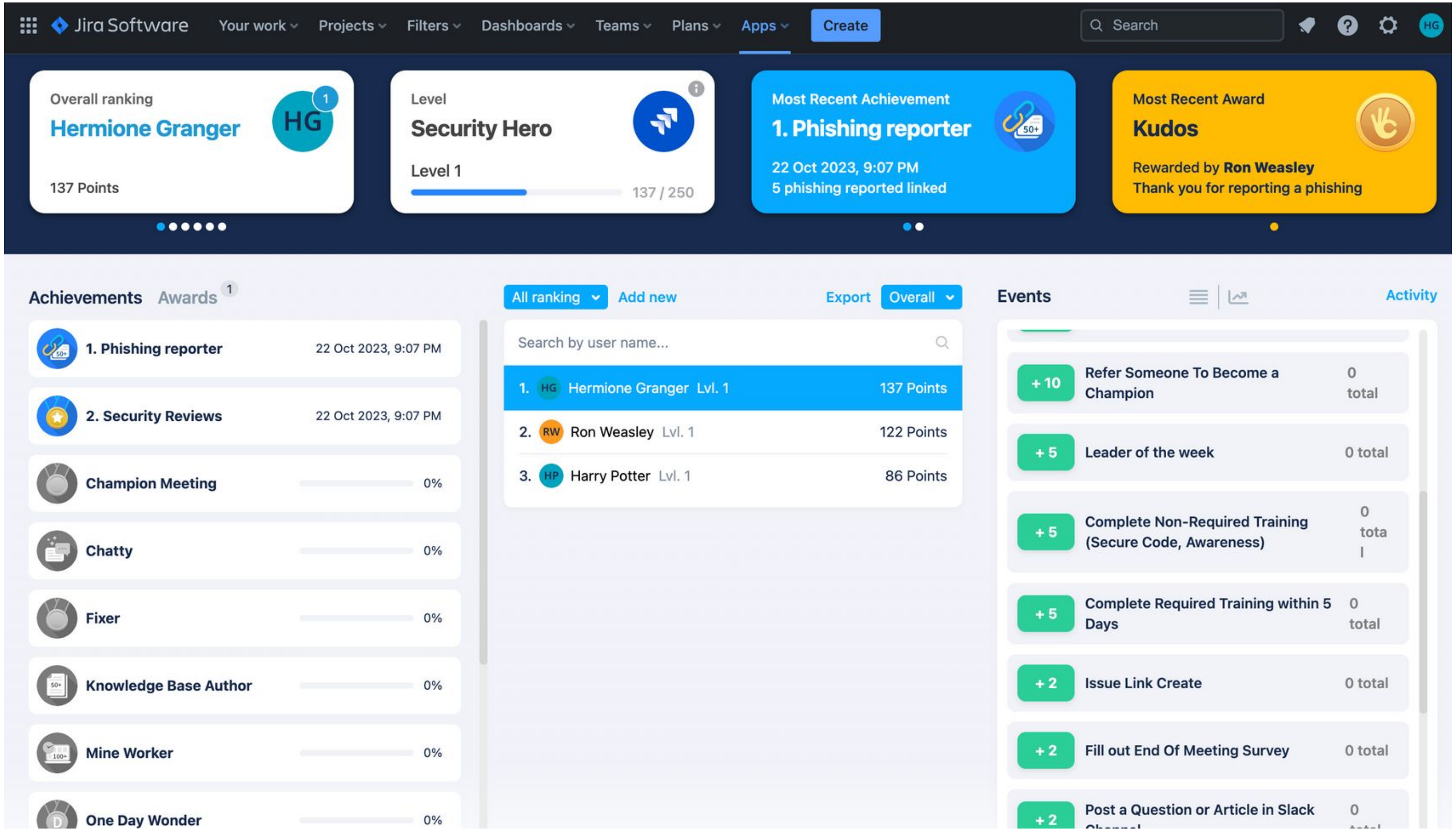
CODE REVIEWS

- number of code reviews conducted
- number of findings from code reviews

SECURITY TESTING

- # of findings remediated from penetration testing
- # of findings solved from vulnerability scanning
- number of findings remediated
- time taken to remediate a vulnerability

Dashboard examples (I)



Overall ranking
Hermione Granger HG 1
137 Points

Level
Security Hero
Level 1
137 / 250

Most Recent Achievement
1. Phishing reporter
22 Oct 2023, 9:07 PM
5 phishing reported linked

Most Recent Award
Kudos
Rewarded by **Ron Weasley**
Thank you for reporting a phishing

Achievements Awards 1

1. Phishing reporter	22 Oct 2023, 9:07 PM
2. Security Reviews	22 Oct 2023, 9:07 PM
Champion Meeting	0%
Chatty	0%
Fixer	0%
Knowledge Base Author	0%
Mine Worker	0%
One Day Wonder	0%

All ranking · Add new · Export · Overall

Search by user name...

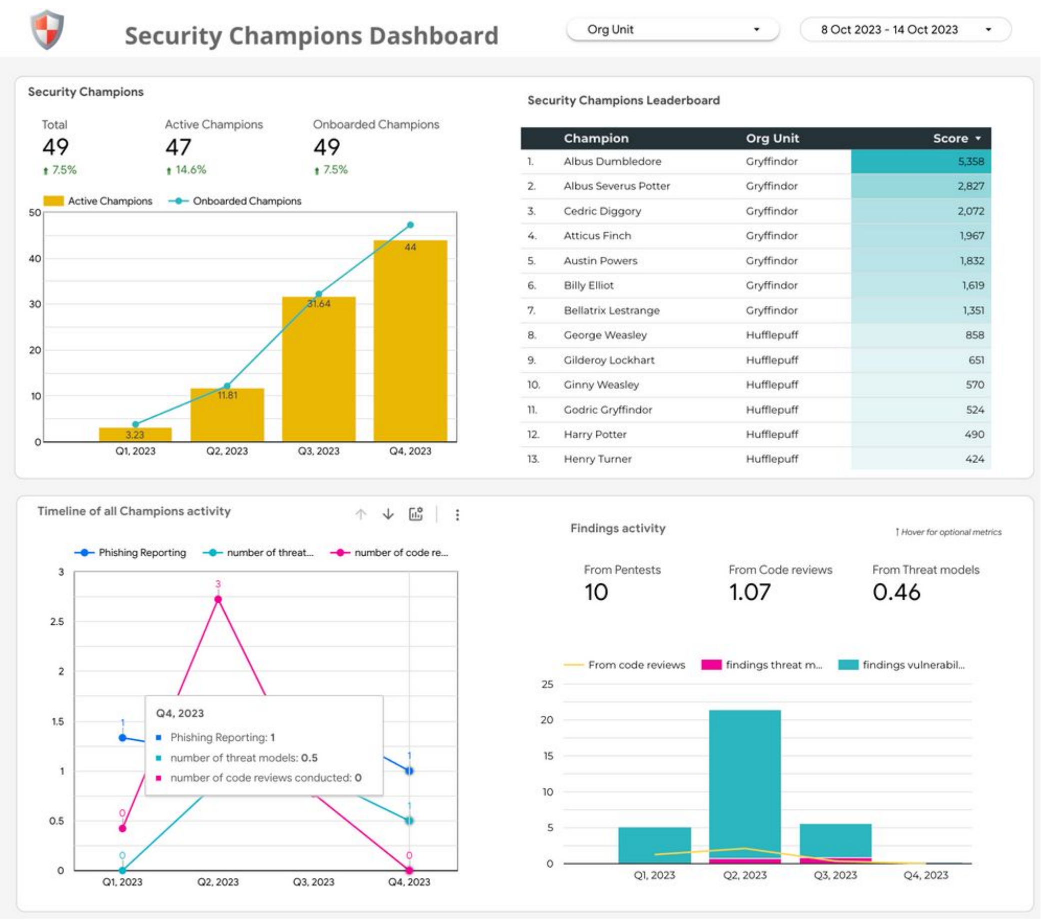
1.	HG Hermione Granger	Lvl. 1	137 Points
2.	RW Ron Weasley	Lvl. 1	122 Points
3.	HP Harry Potter	Lvl. 1	86 Points

Events · Activity

+ 10	Refer Someone To Become a Champion	0 total
+ 5	Leader of the week	0 total
+ 5	Complete Non-Required Training (Secure Code, Awareness)	0 total
+ 5	Complete Required Training within 5 Days	0 total
+ 2	Issue Link Create	0 total
+ 2	Fill out End Of Meeting Survey	0 total
+ 2	Post a Question or Article in Slack Channel	0 total

Leaderboard dashboard in Jira (Cloud)

Dashboard examples (II)



Security Champions Dashboard

Security Champions

Total	Active Champions	Onboarded Champions
49	47	49
↑ 7.5%	↑ 14.6%	↑ 7.5%

Security Champions Leaderboard

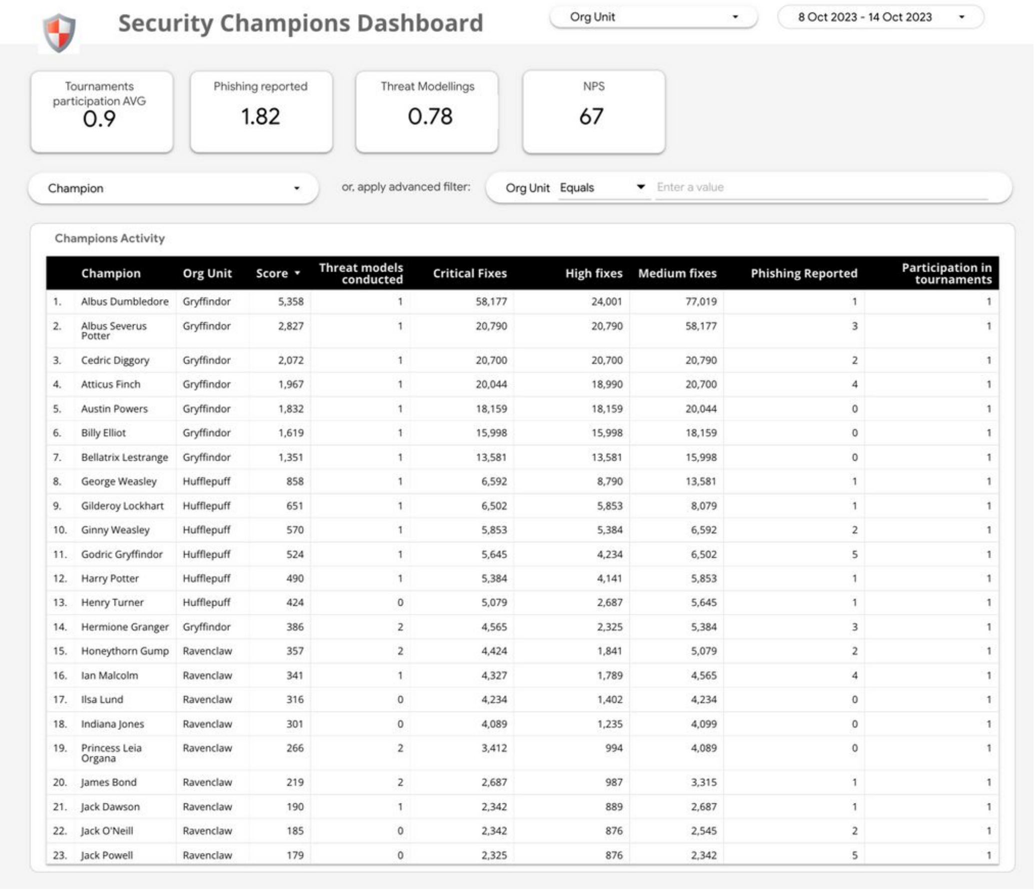
	Champion	Org Unit	Score ▾
1.	Albus Dumbledore	Gryffindor	5,358
2.	Albus Severus Potter	Gryffindor	2,827
3.	Cedric Diggory	Gryffindor	2,072
4.	Atticus Finch	Gryffindor	1,967
5.	Austin Powers	Gryffindor	1,832
6.	Billy Elliot	Gryffindor	1,619
7.	Bellatrix Lestrange	Gryffindor	1,351
8.	George Weasley	Hufflepuff	858
9.	Gilderoy Lockhart	Hufflepuff	651
10.	Ginny Weasley	Hufflepuff	570
11.	Godric Gryffindor	Hufflepuff	524
12.	Harry Potter	Hufflepuff	490
13.	Henry Turner	Hufflepuff	424

Timeline of all Champions activity

Q4, 2023
- Phishing Reporting: 1
- number of threat models: 0.5
- number of code reviews conducted: 0

Findings activity

From Pentests	From Code reviews	From Threat models
10	1.07	0.46



Security Champions Dashboard

Tournaments participation AVG	Phishing reported	Threat Modellings	NPS
0.9	1.82	0.78	67

Champions Activity

	Champion	Org Unit	Score ▾	Threat models conducted	Critical Fixes	High fixes	Medium fixes	Phishing Reported	Participation in tournaments
1.	Albus Dumbledore	Gryffindor	5,358	1	58,177	24,001	77,019	1	1
2.	Albus Severus Potter	Gryffindor	2,827	1	20,790	20,790	58,177	3	1
3.	Cedric Diggory	Gryffindor	2,072	1	20,700	20,700	20,790	2	1
4.	Atticus Finch	Gryffindor	1,967	1	20,044	18,990	20,700	4	1
5.	Austin Powers	Gryffindor	1,832	1	18,159	18,159	20,044	0	1
6.	Billy Elliot	Gryffindor	1,619	1	15,998	15,998	18,159	0	1
7.	Bellatrix Lestrange	Gryffindor	1,351	1	13,581	13,581	15,998	0	1
8.	George Weasley	Hufflepuff	858	1	6,592	8,790	13,581	1	1
9.	Gilderoy Lockhart	Hufflepuff	651	1	6,502	5,853	8,079	1	1
10.	Ginny Weasley	Hufflepuff	570	1	5,853	5,384	6,592	2	1
11.	Godric Gryffindor	Hufflepuff	524	1	5,645	4,234	6,502	5	1
12.	Harry Potter	Hufflepuff	490	1	5,384	4,141	5,853	1	1
13.	Henry Turner	Hufflepuff	424	0	5,079	2,687	5,645	1	1
14.	Hermione Granger	Gryffindor	386	2	4,565	2,325	5,384	3	1
15.	Honeythorn Gump	Ravenclaw	357	2	4,424	1,841	5,079	2	1
16.	Ian Malcolm	Ravenclaw	341	1	4,327	1,789	4,565	4	1
17.	Ilsa Lund	Ravenclaw	316	0	4,234	1,402	4,234	0	1
18.	Indiana Jones	Ravenclaw	301	0	4,089	1,235	4,099	0	1
19.	Princess Leia Organa	Ravenclaw	266	2	3,412	994	4,089	0	1
20.	James Bond	Ravenclaw	219	2	2,687	987	3,315	1	1
21.	Jack Dawson	Ravenclaw	190	1	2,342	889	2,687	1	1
22.	Jack O'Neill	Ravenclaw	185	0	2,342	876	2,545	2	1
23.	Jack Powell	Ravenclaw	179	0	2,325	876	2,342	5	1

Security Champions dashboard example

https://lookerstudio.google.com/s/vprIq1lm5AY

03

Key Takeaways

- Get leadership buy in and budget.
- Gamify wherever possible.
- Integrate Champions Program with HR, People & Culture processes.
- You don’t need to buy more tools.
- Automate program activities (Onboarding, etc.)
- Have fun, be creative and enjoy the process :)

Thank you!

Do you have any questions?

in www.linkedin.com/in/dianacalderon

Resources

https://owasp.org/www-project-security-champions-guidebook/

https://www.synopsys.com/software-integrity/resources/analyst-reports/bsimm.html

German OWASP Day 2024

THANK YOU!