RSAConference2022
San Francisco & Digital | February 7 – 10

TRANSFORM

SESSION ID: **DSO-M02**

Elite Security Champions Build Strong Security Culture in a DevSecOps World

Christopher J. Romeo

CEO
Security Journey
@edgeroute

Agenda

- The need for and goal of Security Champions.
- A nightmare on DevSecOps street (without Champions).
- A phased approach to building Security Champions.
- Ten tactics for building a strong program, and strategic actions to guide you in how to launch a successful Security Champion program.


ORDER
CHAOS

My Security Champion Origin Story

Descriptive, not always prescriptive

Key terms to know

Elite Security Champion

A **security-passionate** person engaged with your security team, interested in expanding their knowledge and experience with security.

Security Community

A virtual team of engaged developers, architects, software managers, testers, and similar roles (**product adjacent**) that extends the experience and knowledge of a central security team deeply into product/development teams.

The security champion mindset

The need for security champions

Median ratio of full-time SSG members to developers

Source: BSIMM-12

The goal, part one

Product adjacent
folks that think
like security people.

SECURITY JOURNEY

The goal, part 2

1/8

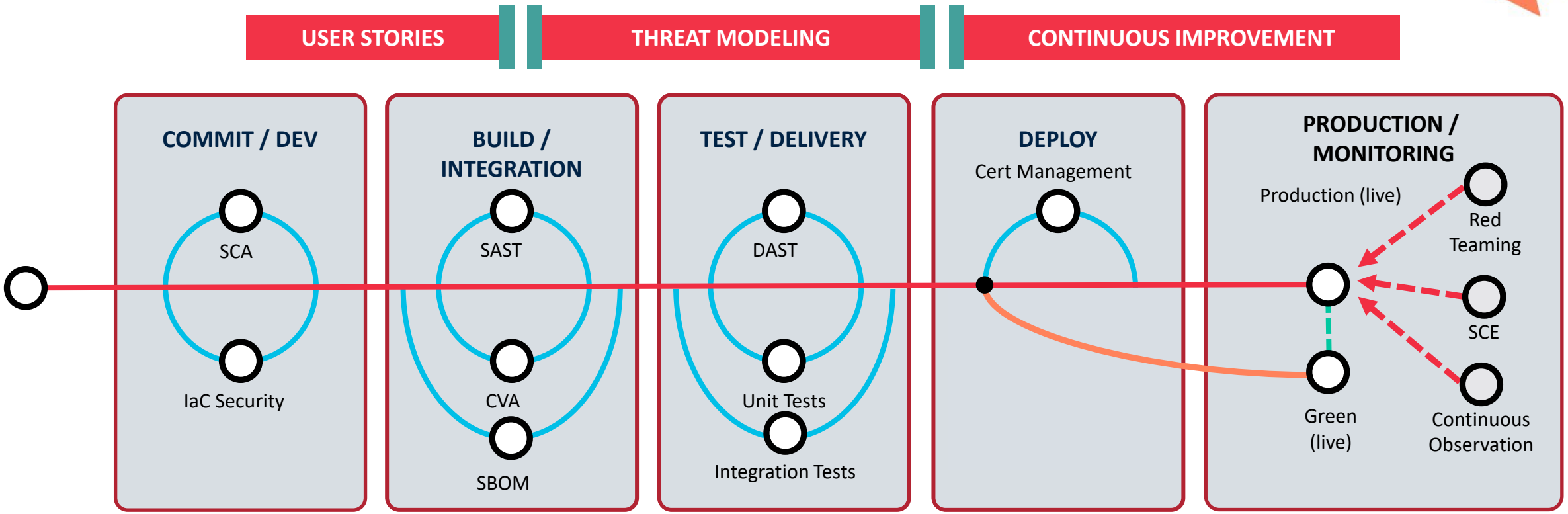
One security champion for every eight developers.

SECURITY JOURNEY

Extrapolating the need for champions

Profile	Size of engineering team	Estimated # of software engineers	Estimated size of software security team	Goal for number of champions (1 to 8)
Large online retailer	70,814	40,000	296	5,000
Ride sharing	4,817	3,000	22	375
Insurance / Financial Services	1,509	414	3	52
Auto maker	28,357	2,500	19	313

A nightmare on DevSecOps street



- Threat model all the features.
- Write the security user stories.
- Review and remediate:
  - 1-5 SCA results
  - 5-25 SAST findings
  - 1-5 CVA findings
  - 5-10 DAST findings

- Failed security unit or integration tests
- Broken cert
- Pen test results
- Security Chaos Engineering experiment failures.

A common champion problem

"Our Champions program isn't really one I'd talk about at the moment. …

I've heard a common theme that champions programs aren't working well in many companies this past year. The champions are not being allocated enough time to really take on the role, resulting in missed expectations."

-- Anonymous AppSec Director at a Large Company

A phased approach to champions

Top growth

Mid growth

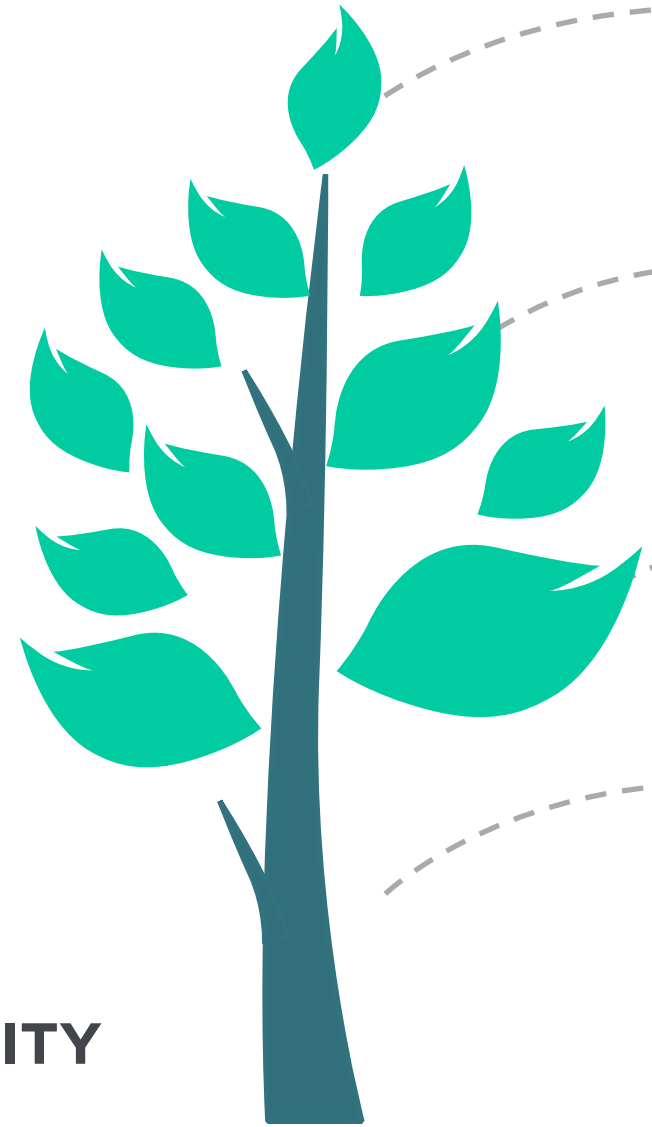
Starting out

Security people
Passionate, die-hard product adjacent folks that do security in their spare time.

Security voluntold
Mandatory assignments, per product / application team.

Security volunteers
Breaking down the doors to join up.

Security community and the mind of the Champion



Deliberate and disruptive
We are okay with breaking some eggs.

Engaging and fun
Make it fun if you want us to stick around.

Rewarding
Provide us with recognition as well.

Return on investment
Demonstrate to our boss how our time made things better.

SECURITY JOURNEY

Two other models – similar results

Security coaching

Product security leads

Tactics for building a Champions Program

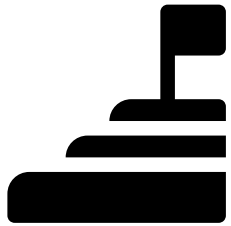
Think big picture via strategy.

Starting point: develop a program objective

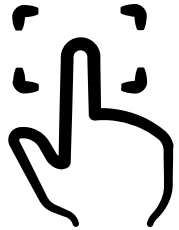
Individual	Establish a growth path for developers to transform into security engineers.
Organizational	Serve as the leadership and catalyst for secure product development using our SDL.
Industry	Industry leading program to improve corporate image as a security company; an organization full of leading security engineers.

Strategic actions

1. Set yearly goals for your community.



2. Yearly strategy opt-in.



EXECUTION TIP

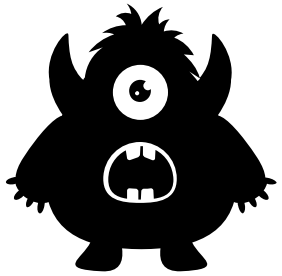
Yearly goals and opt-in protect against Managers claiming they did not realize the commitment they were making.

Make a mark with the brand.

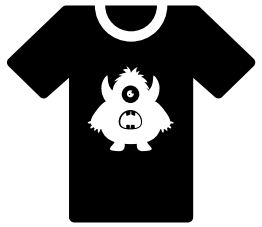
Branding actions

1. Invest in a central brand.

2. Design a logo/mascot.



3. Distribute SWAG.



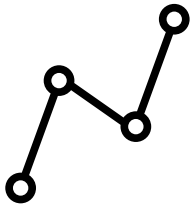
EXECUTION TIP

Your brand is an advertisement and provides attribution for all the cool things the program does and achieves.

Sell the vision to gain buy-in.

Executive buy-in

1. Share the statistics.



2. Make the business case.

3. Ask for the sale.

EXECUTION TIP

Represent how security champions are a business enabler, and partner with a strong Executive Sponsor that catches the Champion vision.

Expose what is hidden as value prop.

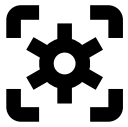
Their value proposition

What's in it for them

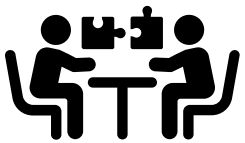
Advanced training, knowledge, and degrees.

Exclusive learning events.

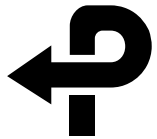
Acknowledgement and recognition



Management/Executive exposure.



Cross organizational collaboration



Career advancement or a pivot into security.

EXECUTION TIP

Flip the table and consider what's in it for your Champions. Make it about them.

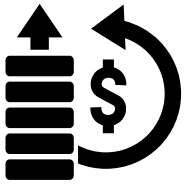
Your value proposition

What's in it for YOU

Resources without headcount.

Employee satisfaction.

Security coaches.



Security ROI.

Industry visibility.

EXECUTION TIP

Achieve and play your cards right, and
you'll be seen as an organizational and external security leader.

Find and sign new champions via recruitment.

Recruitment

1 Beg in the early days.

2 Volunteer or voluntold; mandatory?

3 Sell the value prop.

EXECUTION TIP

Advertise the existence of the program; leave no stone unturned.

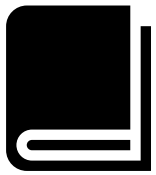
Build a program of value.

Program

Your offering

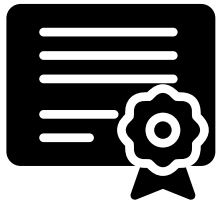
Monthly training / live streams.

Tournaments / internal CTF.

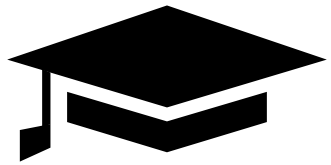


Book of the month club.

Security days or conferences.



CSSLP training.



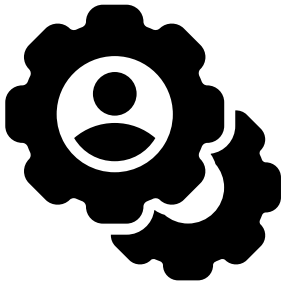
Master's degree.

EXECUTION TIP

Focus on adding value in the lives of the Champions, and they will add value to your security bottom line.

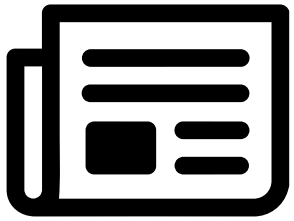
Keep everyone in the loop via communication.

Communication

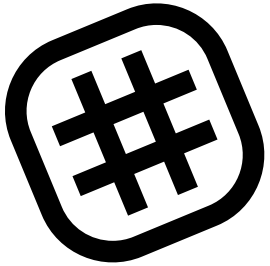


1 Update direct Managers.

2 Send high-level Reports.



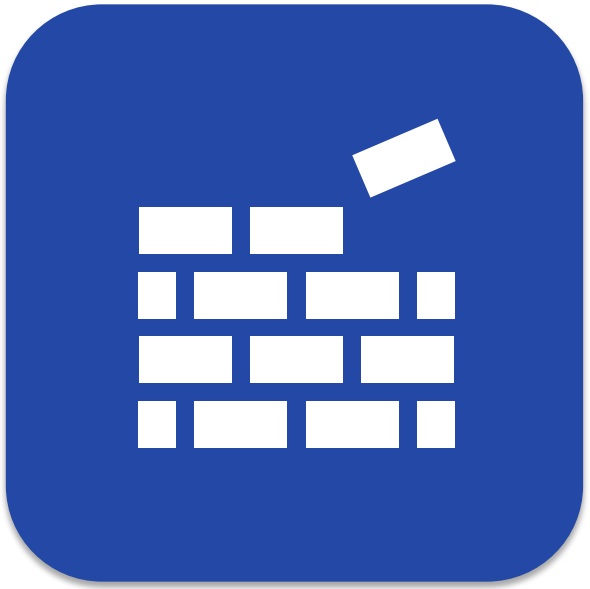
3 Send a newsletter.



4 Create a Slack/ Teams channel.

EXECUTION TIP

Over communicate about the contributions your Champions make.



Keep them coming back for more via retention.

Retention


Email message.


Cash reward.


Public recognition.


Printed certificates.


Lanyards.


T-shirts.


Stickers.


Slack/Teams message.

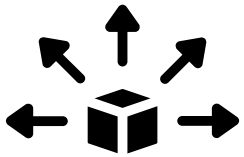
EXECUTION TIP

Champions stick around because they feel valued.

Measure what matters with metrics.

Metrics and measurement

Total count of Champions.



Champion distribution.

Champion education.

Champion flaw density.

EXECUTION TIP

Measure the efficacy of your Champions program as a true ROI.

See the world with globalization.

Globalization

1 Adapt to the world stage.

2 Dedicate local time.

3 Security boots on the ground.

EXECUTION TIP

Security Champions must exist everyplace your company has team members.

Beyond the developer…

Product Managers

Program Managers

Execs and Managers

Hardware Engineers

Extending to other product adjacent roles

“Apply” Slide

- Next week you should:
  - Assess the current success of your Security Champions program and measure its effectiveness.
- In the first three months following this presentation you should:
  - Craft a business case for a Champion program.
  - Build a Champion plan of action, using the tactics that make sense for your new program.
- Within six months you should:
  - Launch or re-launch your program.

Summary of tactics

1. Think big picture via strategy.
2. Make a mark with the brand.
3. Sell the vision to gain buy-in.
4. Expose what is hidden as value prop.
5. Find and sign new champions via recruitment.
6. Build a program of value.
7. Keep everyone in the loop via communication.
8. Keep them coming back for more via retention.
9. Measure what matters with metrics.
10. See the world with globalization.

Key takeaways

- Your company needs Security Champions.
- The goal is product adjacent people that think like security people, and one Champion for every eight developers.
- Embrace the big issues as you build out your strategy.
- Build a Champion plan of action to launch or re-launch your Security Champion program!

Resources

- https://www.securityjourney.com/post/security-rewards-and-recognition
- https://www.securityjourney.com/post/security-coaches
- https://www.securityjourney.com/post/information-security-needs-community-6-ways-to-build-up-your-teams
- https://www.securityjourney.com/post/4-steps-to-transforming-developers-into-security-people

Questions and contact information

EMAIL: chris_romeo@securityjourney.com

SOCIAL: @edgeroute @SecurityJourney

LISTEN: The Application Security Podcast

READ, WATCH, or LISTEN: 5 security articles that are worth your time
https://www.securityjourney.com/resources/hi5

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA® Conference, RSA Security LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.