The Security Champion Framework

The Security Champion framework exists as a measuring stick and a roadmap. As a measuring stick, the framework allows leaders to measure how well their champions program performs. As a roadmap, the leader can use the measurements as input and build a plan to improve their program by applying updates towards a higher framework level.

Key terms to know

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

The security community is 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.

What's in a name?

Various names apply to the people that make up a security champion program. For example, organizations use different naming schemes for Champions, Advocates, Guild Members, Ninjas, and Agents.

Names sometimes matter: people may define their roles by their terms. It is vital to choose a name that fits your organization's culture. Some names carry implications on the level of involvement and authority expected: liaisons, champions, advisors, consultants, etc. Choosing the perfect phrase or term to describe the people does **not** define the success of your program! But do give it a thought so that the label specifies the content and expectations correctly.

For purposes of the framework, the word champion is universal.

The need for champions

Security champions are necessary because most security teams must extend their resources to meet security demands. The security department needs more time/energy/people to perform security for all. They have the knowledge and expertise but need scalability.

Each year, BSIMM asks their member companies how many developers and security team members they have. From BSIMM 12, the ratio was one security person to every one hundred and thirty-five developers. This ratio demonstrates the need for security champions. BSIMM members take security seriously enough to spend money on a consultant to analyze their maturity. Non-BSIMM companies are likely at an even higher ratio. The higher percentage is why Security Champions are needed – there need to be more security team members to do all the work.

The successful champion

There are four facets to the successful champion experience.

First, consider foundational knowledge. Foundational is the knowledge about application security, from vocabulary to return on investment and the business case. Foundational knowledge answers the why of application security and the things everyone needs to understand.

Second, a spark of passion. A spark of security passion is vital. Rather than forcing a champion to volunteer, the best case is a champion that steps forward because they have some security interest. The champion program can fan that little interest into a security flame.

Third, understand/acknowledge attacks. Champions must realize the reach of modern attacks and recognize that what they build is under attack.

Fourth, utilize tools and processes. Champions must follow the defined procedures to enhance security, like Secure Development Lifecycle, and be the eyes and ears that execute and interpret the results of the tools. They must also

participate in making the program better over time by giving feedback on tools and processes and how they fit in the organization.

The value for the champion

Many security champion programs focus on the company's value instead of thinking about the champion. Flip the table and consider what's in it for your champions. Make it about them.

Here are some examples of items that can provide value for the champion:

- Advanced training + knowledge and degrees.
- Exclusive learning events.
- Management/Executive visibility and exposure to successful projects that improve security.
- Acknowledgement and recognition as someone who makes company products safer for Customers.
- Cross-organizational collaboration – networking with other like-minded security people.
- Career advancement.
- Career pivot into security.

The company's return on a champion program

The company does receive many benefits from the program. Consider these ideas for the value provided to the organization.

- Specialized security resources without additional headcount investment.
- A population of employees is satisfied with a program dedicated to their interests.
- Integrated security coaches within functional teams.
- Contributes to security ROI.
- Visibility as an organization that takes security seriously.

A few Champion Program Models

[The authors adapted this section from a comment by Brook Schoenefield, based on his brilliance in running multiple Champion programs in various organizations.]

There are three general Champion program forms: central team + security referees, central team + Champions, and fully empowered satellite security people. Each of these forms reaches "maturity" somewhat differently.

Central team and security referees

The central team is responsible for security, and the security referees across the organization spot each need and call in the central resources to perform the security work.

This form is easier to set up and often sits comfortably for security folk since they maintain most control. But this program needs to catch up and has far too much friction.

Central team and security engineer champions

The champions handle basic security tasks, and the complex functions move to the central security team.

Security engineers still keep complex and tricky in the hands of the central team. But, on the other hand, it's less training, requires the central team investment, and is simple for nearly everyone to understand.

Fully empowered satellite security people federated throughout development

Dedicated security resources exist across the business, paid for by their management. Usually, with this, there has to be a central program, but it may be minimal.

While the journey may be much longer, at some point, the security professionals make themselves redundant. As a result, security becomes "how we build software," and the security culture demonstrates an organization that takes security seriously and takes action to improve security.

Overview of the Security Champion Framework

Five high-level areas divide the framework, with one to four sub-areas within each area.

Area	Description
Planning	Planning includes the activities needed to scope and build a strategy.
People	People include recruiting, retaining, capturing commitment, and onboarding new champions.
Marketing	Marketing includes the branding of the program and communication plans.
Execution	Execution includes the program pillars, coaching, education, and globalization efforts.
Measurement	Measurement includes metrics for demonstrating the value generated by the program.

Other Security Champion Resources

- Security Champion Program Success Guide – https://securitychampionsuccessguide.org/
- Security Champions Playbook – https://github.com/c0rdis/security-champions-playbook

Contributors

- Chris Romeo, Project Leader
- Izar Tarandach
- Brook Schoenfield

Scope

Short Description

Scope: how deep is the program?

Long Description

Scope measures the depth of the program within the organization. The deeper the champion program embeds itself, the more significant the impact it can have on the organization.

Overview

Level	Name	Validation
Maturity 0	Developers only	Survey the Champion population, and ask for current role.
Maturity 1	Product adjacent (SCRUM, SRE, DevOps, Cloud)	Survey the Champion population, and ask for current role.
Maturity 2	Product managers	Survey the Champion population, and ask for current role.
Maturity 3	Executives and Managers	Survey the Champion population, and ask for current role.

Maturity 0 - Developers only

The traditional champion program focuses on the developers. However, developers have the most significant impact through their participation in a program, as they design and implement the products and applications, execute the tools, and take action based on tool results.

Activity

- Create program activities that have value for developers.

Benefit

- Developers are the center and are a great start.

Maturity 1 - Product adjacent

Product adjacent includes all those folks that have visibility and influence over the products and applications. For example, product adjacent includes SCRUM leadership, Site Reliability Engineers (SRE), DevOps, Cloud, and Quality Assurance(QA).

Activity

- Create program activities that have value for the product adjacent.

Benefit

- Expanding to the product adjacent lowers security friction across the business.

Maturity 2 - Product Managers

Product managers create the vision and set priorities for additions to products and applications. When product managers catch a security vision, they prevent security friction and enable the proper security prioritization.

Activity

- Create program activities that have value for product managers.

Benefit

- Product drives what engineering builds and can drastically lower security friction by specifying built-in security.

Maturity 3 - Executives and Managers

Executives and managers have ownership of champion resources. Building a true partnership with this user group protects champions from pushback on their champion activities.

Executives and managers are busy, so having a quarterly approach to meeting with this group can provide the right amount of value while not being a drain.

Activity

- Create program activities that have value for executives and managers.

Benefit

- When the leaders share best practices, the entire culture has changed.

Strategy

Short Description

Strategy answers the questions, "What do you want them to do?" and "What is the big-picture goal?"

Long Description

The Strategy sets the tone for your Security Champions program, identifying the shared vision and goals for participants. Participants want to know where the program is heading and how they can be a part of the solution. Providing this guidance motivates Security Champions to do their best within the program.

Overview

Level	Name	Validation
Maturity 0	No program	Nothing to validate
Maturity 1	Program objective	Visual inspection – review the program objective and determine if it is clear.
Maturity 2	Yearly goals, program vision, and an acceptance/tracking tool.	Visual inspection – review the goals and vision and test the tool.
Maturity 3	Executive Sponsor buy-in.	Interview – meet with the Executive Sponsor and confirm what buy-in means in their words.

Maturity 0 - No Program

Activity

- Get on board and scope a program.

Benefit

- Read this framework to capture the benefits you'll experience by launching a Security Champion program.

Maturity 1 - Program Objective

Activity

- Define and publicize a program objective.

Benefit

- Communicates to everyone what we are trying to achieve.

Examples

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

Maturity 2 - Yearly goals, program vision, and an acceptance and tracking tool.

Activity

- Define and publicize yearly goals.
- Define and prioritize a program vision.
- Provide an acceptance and tracking tool for the Champion and Manager goals.

Benefit

- Yearly goals and opt-ins protect the Champion's resource commitments. Most of the time, Champions perform their security duties with a shared slice of their time. By setting yearly goals and facilitating an opt-in where Champions and the Manager acknowledge the signup, you prevent uncomfortable conversations. Things can be difficult if the Champion and manager are not in sync regarding resources.
- Represent how security champions are business enablers and partner with a strong Executive Sponsor that catches the Champion program vision.

Examples

- Participate in the Security Champion community via monthly meetings.
- Drive the adoption of our SDL.
- Attain a specific security education level.
- Focus on growing expertise in one area of our SDL (Security Controls, Threat Modeling, Static Analysis, Vulnerability Testing)

Maturity 3 - Executive Sponsor buy-in.

Activity

- Achieve Executive Sponsor buy-in for program vision.

Benefit

- When an Executive Sponsor is on board with the Champions program, they can assist with spreading awareness within the Executive Suite and help with any dedicated budget required to execute the program.

Commitment

Short Description

Commitment: how much time are your champions spending on security (average)?

Long Description

Champion resources in most programs need to be dedicated. Champions dedicate a slice of their available time, dedicated to security.

Overview

Level	Name	Validation
Maturity 0	None.	None
Maturity 1	One.	Review the results of a survey of the champion population, asking them the average number of hours per week they spend on champion activities.
Maturity 2	Two to Four.	Review the results of a survey of the champion population, asking them the average number of hours per week they spend on champion activities.
Maturity 3	Eight.	Review the results of a survey of the champion population, asking them the average number of hours per week they spend on champion activities.

Maturity 0 - None

Activity

- None – strictly a measurement sub-area.

Benefit

- There is no benefit to a program where champions spend no time.

Maturity 1 - One

Activity

- None – strictly a measurement sub-area.

Benefit

- One hour per month is a start.

Maturity 2 - Two to four

Activity

- None – strictly a measurement sub-area.

Benefit

- Two to four hours per month give champions a chance to provide actionable results.

Maturity 3 - Eight or more

Activity

- None – strictly a measurement sub-area.

Benefit

- Eight or more hours per month is the sweet spot, allowing champions to become the security expert for their functional area.

Onboarding

Short Description

Onboarding answers the question, "how are you going to get a new, inexperienced Champion embedded into the Champions Program, so they feel at home?".

Long Description

When a new person becomes a Security Champion, they likely have yet to learn what to expect. If you only invite them to a monthly meeting, with no context for what they should expect, you are setting them up for failure. On the other hand, there is an opportunity with onboarding to welcome a new Champion and set them up for a long and successful time within the Program.

Overview

Level	Name	Validation
Maturity 0	No onboarding process.	Nothing to validate.
Maturity 1	Individual orientation and basic requirements.	Visual inspection – review the simple onboarding process.
Maturity 2	Team-focused orientation and buddy system.	Visual inspection and ad hoc interviews – review the training materials and the champion buddy system.
Maturity 3	Certified Security Champion.	Visual inspection and ad hoc interviews – review the certification process, and discuss the value generated with a selection of certified Champions.

Maturity 0 - No onboarding process.

Activity

- Develop and implement an onboarding process.

Benefit

- An onboarding process sets champions up for success from day one.

Maturity 1 - Individual orientation and basic requirements.

Activity

- Create a set of requirements that Champions must meet or comply with within a specified time.
- Develop an individual orientation agenda and set of content.
- Deliver the individual champion orientation on a set schedule throughout the year.

Benefit

- The individual orientation sets expectations for new champions and points them to where they can get more help.

Maturity 2 - Team-focused orientation, champion buddy system, and manager approval.

Activity

- Develop a team-focused orientation to deliver to entire new teams of champions for a business unit.
- Assign a new champion buddy system, pairing experienced champions with new champions. Encourage champion buddies to meet weekly for the first month, bi-weekly for the second month, and then once in the third month.
- Provide a mechanism for managers to approve the champion commitment.

Benefit

- Providing orientation for champions within a business unit allows the new champions to forge relationships within their functional area.
- When managers approve the champion commitment, they will support the champion throughout their time with the program.

Maturity 3 - Certified Security Champion.

Activity

- Define and assemble the standard body of knowledge.
- Build a training curriculum to deliver the standard body of knowledge.
- Build a testing approach to validate that champions can demonstrate the standard body of knowledge.

Benefit

- A Champion certification provides value to the Champion as they can reference their status at promotion time and take the status with them if they switch companies.
- Certified Champions have proven that they have attained the standard body of knowledge you define for your Program.

Recruitment

Short Description

Recruitment: how are you going to find and sign-up new champions?

Long Description

The job that never ends for the program leadership team is recruiting new champions.

While mandatory assignments and volunteers represent levels two and three, most programs will blend recruitment strategies. Successful Champion programs accept resources from wherever they are available.

Overview

Level	Name	Validation
Maturity 0	None	None
Maturity 1	Ragtag crew.	Review the recruitment approach and the output of the recruitment process.
Maturity 2	Mandatory assignment.	Review the recruitment approach and the output of the recruitment process.
Maturity 3	Volunteer.	Review the recruitment approach and the output of the recruitment process.

Maturity 0 - No active recruitment efforts.

Activity

- Build a recruitment strategy for new champions.

Benefit

- Recruitment develops a pipeline of new champions.

Maturity 1 - Ragtag crew of security-passionate people.

A ragtag crew of people describes a program where you have a core of security and passionate people that raise their hands to participate in a program. These folks are excited by security and want to add their efforts to the security mission.

Activity

- Communicate the program's existence and offer a method for interested members to join.

Benefit

- You have a spark – the start of a robust security community.

Maturity 2 - Mandatory assignment.

With a mandatory assignment, the program defines a minimum number of champions per business unit or product/application and then asks for volunteers to fill the roster.

Activity

- Define the minimum number of champions and how to split up the champion allocation.
- Invite and register new champions.
- Confirm that the minimum number of champions exists.

Benefit

- While the voluntold method where champions participate against their will may bring in some that are not security passionate, the numbers are growing, and the distribution from across the business will be solid.

Maturity 3 - Volunteer opt-in.

The holy grail of the champion program is where potential champions chase down program leadership and ask to be a champion.

Activity

- Provide a method for volunteers to join the program.

Benefit

- Ideal, as people are chasing you to join your program.

Retention

Short Description

Retention: how are you going to keep them coming back for more?

Long Description

The best security champions are volunteers, and volunteers will only continue forward for the love of the game for so long. Retention is how you reward and incentivize champions to continue forward with the program.

Overview

Level	Name	Validation
Maturity 0	No retention efforts.	None
Maturity 1	Simple retention efforts.	Survey the Champion population, and ask what rewards and retention efforts they have experienced.
Maturity 2	Existing rewards and recognition.	Survey the Champion population, and ask what rewards and retention efforts they have experienced.
Maturity 3	Specific budget for Champions.	Survey the Champion population, and ask what rewards and retention efforts they have experienced.

Maturity 0 - No retention efforts

No retention efforts.

Activity

- Build a retention plan.

Benefit

- Dedicated and thoughtful retention ideas will keep champions coming back for years.

Maturity 1 - Simple

Simple retention efforts, including email and Slack/Teams messages.

Activity

- Draft and send regular emails to champions and their management.
- Draft and send Slack / Teams messages affirming the efforts of champions.

Benefit

- Everyone appreciates recognition for what they accomplish; recognition breeds loyalty.

Maturity 2 - Existing rewards and recognition

Tap into your existing company rewards and recognition programs.

Activity

- Recognize champions publicly at all hands meetings or any other available broadcasts.
- If there is a cash reward program, provide cash to champions for various successes.
- Send SWAG (lanyards, t-shirts, and stickers) to champions.

Benefit

- Rewards without new budget allocation.

Maturity 3 - Specific budget

Request and receive a particular budget to retain and reward Security Champions.

Activity

- Request budget according to budget cycles.

Benefit

- With the budget, many new doors are open.

Branding

Short Description

Branding: how to best represent the group to the larger company?

Long Description

Branding generates words or pictures that everyone inside the company will associate with security champions. A solid brand allows all the goodwill built by champions to accumulate inside a given mark and provides residual value for years to come.

Overview

Level	Name	Validation
Maturity 0	No branding efforts.	None
Maturity 1	Name and tagline.	Visual inspection – review and confirm that the name and slogan exist and are in use.
Maturity 2	Logo and mascot.	Visual inspection – review and ensure that the logo and mascot exist and are in use.
Maturity 3	SWAG	Visual inspection – review the available SWAG and the distribution policy for champions.

Maturity 0 - No branding efforts

No branding occurs.

Activity

- None.

Benefit

- None.

Maturity 1 - Establish a name and tagline for your security community.

Activity

- Partner with folks in marketing to develop a name and tagline, or gather your core group of champions and ask them for help brainstorming.

Benefit

- Your brand is an advertisement and provides attribution for all the cool things the program does and achieves. The name and tagline provide a value capture device for all your efforts towards building the champion program.

Maturity 2 - Build a visual look and a logo/mascot for your security community.

Activity

- Partner with folks in marketing to develop a logo/mascot, or gather your core group of champions and ask them for help brainstorming.

Benefit

- The logo/mascot provides a visual mark to build residual value beyond your name and tagline.
- The logo/mascot are excellent assets to place upon various SWAGs.

Maturity 3 - Distribute SWAG.

Distribute SWAG (Stuff We All Get)to your champions, allowing them to show their commitment and act as a billboard. * Souvenirs, wearables, and gifts * T-shirts, laptop stickers, etc.

Activity

- Build a catalog and roadmap of SWAG items.
- Order SWAG items and distribute them according to your roadmap.

Benefit

- Everyone loves SWAG, and SWAG turns your champions into walking billboards for the program.

Communication

Short Description

Communication: How will you keep the rest of the organization apprised of what the Champions are doing?

Long Description

Communication is critical, and the organization needs to stay abreast with all the champion happenings. In addition, communication connects with key stakeholders, from champions to direct managers and executives.

Overview

Level	Name	Validation
Maturity 0	No communication.	Nothing to validate.
Maturity 1	Champions only.	Visual inspection and survey – review the communication plan, scope of communication, and communication examples, and survey Champions about effectiveness of communication.
Maturity 2	Direct Managers.	Visual inspection and ad hoc interview – review the communication plan, scope of communication, and communication examples.
Maturity 3	Executives.	Visual inspection and ad hoc interview – review the communication plan, scope of communication, and communication examples.

Maturity 0 - No communication

Activity

- Build a communication plan for the program.

Benefit

- Communications keep everyone up to date on the benefits of the champions program.

Maturity 1 - Champions only.

As the primary constituents, champions need a constant communication from the program.

Activity

- Build a communication plan.
- Execute the communication plan.
- Send a newsletter-style e-mail with updates.
- Create a central Slack/Teams channel for questions and encouragement.

Benefit

- Champions are in the loop on how they can participate more deeply in the community.

Maturity 2 - Direct Managers

Direct managers must understand the value their employees provide to the program. Achieve this understanding through communicating actual events to the direct managers.

Activity

- Add direct managers to the communication plans.
- Update direct managers about the impact of individual Champions – over-communicate.

Benefit

- Communicating about the contributions your Champions make demonstrates the return on investment to the Manager for providing resources.

Maturity 3 - Executives

The champion program relies upon participants from various parts of the organization. Executives have direct responsibility for those parts. Keeping executives in the loop allows them to determine what value their people are generating.

Activity

- Add executives to the communication plans.
- Send a high-level report to Executive staff, highlighting the contributions of their organization's Champions.

Benefit

- Executives understand the return on investment, and the more data provided to them, the better they can advocate for the program.

Coaching

Short Description

Coaching: how will you provide consulting and one to training?

Long Description

Security coaches are to developers, as life coaches are to health and wellness. A solid security coach works with a developer one-on-one or one to a few for a short period, assisting and teaching one area or helping to resolve one challenge. Then the security coach moves on to another set of folks to work with and help succeed.

A coach could cover subjects such as threat modeling, using SAST or DAST, and advising on a tough security challenge.

To be a successful security coach, an individual must have a solid development background. Walking a mile in a developer's shoes goes a long way towards showing that developer that the coach cares enough to understand the subject for which they are providing consulting. The coach must also have a solid background in application and product security. The final piece for success is soft skills- communicating with a small group of developers and adapting communication and collaboration styles to make the group successful. Communication is crucial, and the best coaches connect with developers.

Overview

Level	Name	Validation
Maturity 0	No coaching.	None.
Maturity 1	Volunteer coaches.	Visual inspection and survey – review the coach roster, and interview a few coaches to evaluate their efforts, and survey population about total amount of coaching they have received in the past year.
Maturity 2	Staff coaches.	Visual inspection – review the coach roster, and interview a few coaches to evaluate their efforts.
Maturity 3	Dedicated coaches.	Visual inspection – review the coach roster, and interview a few coaches to evaluate their efforts.

Maturity 0 - No coaching

No coaching occurs.

Activity

- Study and understand the value of beginning a security coaching practice.

Benefit

- A security coaching practice provides specialized consulting and training and extends the influence of a central security team across a development organization.

Maturity 1 - Volunteer coaches

Volunteer coaches are available. A volunteer coach is an existing Security Champion or security team member with other responsibilities beyond coaching. They find time in their busy schedules to provide coaching services.

Activity

- Write a job description for the Security Coach.
- Provide training sessions explaining successful approaches in coaching for those with a full scope of work in their day jobs.

Benefit

Voluntary coaching is better than no coaching at all. In addition, voluntary coaches can contribute on an as-available basis and positively impact a program.

Maturity 2 - Staff coaches

Staff coaches are available. A Staff Coach is a dedicated headcount resource, reporting to the Security Team. Their focus is to connect with developers and provide security consulting and teaching on a reliable basis.

Activity

- Determine the engagement model for Staff Coaches. How will developers connect with the Coaches if they make an inbound request?

Benefit

- A dedicated Staff Coach focuses on consulting and teaching developers about security. They have no tug of a day job, as this is their day job.
- A dedicated Staff Coach is more efficient and can better serve a larger contingent of developers.

Maturity 3 - Dedicated coaches

Coaches are dedicated and assigned to specific business areas.

Activity

- Determine the breakdown of Coaches to business areas.
- Staff accordingly to provide a standard level of service across the business areas.

Benefit

- Assigned coaches provide more time and coverage for the entire team.

Education

Short Description

Education: how will you train the community at scale?

Long Description

Security education is the approach, tools, and techniques to educate security champions about the most critical pieces of security.

Security education consists of different modalities. The two most popular approaches are online security education platforms and in-person classroom training. Both of these modalities have their advantages and disadvantages. Platforms provide a solution to impact a large percentage of the Champions, no matter their global distribution. Classroom training provides a personal touch, with closer instruction on the finer points, but is expensive to provide for a large organization, both in resource time and cost.

Overview

Level	Name	Validation
Maturity 0	No Security Education.	Nothing to validate.
Maturity 1	Ad hoc security training.	Visual inspection – review training plans, feedback, and metrics/records of training.
Maturity 2	Regular training.	Visual inspection – review training plans, feedback, metrics/records of training, and survey population.
Maturity 3	Creative training.	Visual inspection and ad hoc interviews – review training plans, feedback; interview a cross-section of those trained, and metrics/records of training.

Maturity 0 - No security education.

No security education for Champions.

Activity

- Start an education program for your champions.

Benefit

- Security education lays a foundation for a strong security champion. When the champion learns the essential pieces of security, from fundamentals to deep dives to secure coding, they design and implement more secure applications.

Maturity 1 - Ad hoc security training

Ad hoc security training occurs with no regular schedule. For example, this training could be a short webinar on the OWASP Top 10, a classroom session, or a pointer to an online course. The point of ad hoc is that no regular schedule applies to the champions.

Activity

- Scope an ad hoc training, find a teacher, and advertise it to your champions.
- Execute the training.

Benefit

- Some training is occurring, but we aren't catching everyone. There is a baseline set for all champions.

Maturity 2 - Regular training

Regular security training for all champions sets the baseline of knowledge for all.

Activity

- Evaluate various training offerings, and choose a solution that fits your budget and will touch all the developers.
- Choose a training offering and build a programmatic approach to roll it out.
- Generate metrics for training completion, per Champion.

Benefit

- Spreading education across the community provides base levels of knowledge and experience.

Maturity 3 - Creative training

Creative training goes beyond regular, utilizing techniques such as Hack-a-thons and build/break/fix contests.

Activity

- Brainstorm creative ideas throughout the year that are creative and beyond your regular training.

Benefit

- Collaborative experiences allow champions to learn from each other.

Globalization

Short Description

Globalization: how do you build a program if you're a worldwide company?

Long Description

Globalization is a hurdle that you must clear as you build up your program. Most large companies have offices all over the world. Globalization provides opportunities to engage your global community, providing programmatic efforts aimed at their local time zone. Instead of thinking of champions as only mattering in your local time zone, engage your champions worldwide with a solid globalization strategy.

Overview

Level	Name	Validation
Maturity 0	No consideration for globalization.	Nothing
Maturity 1	Comfortable schedule.	Visual inspection and survey – review the meeting schedule, and confirm that meetings are in a reasonable time zone for global citizens. Add a question to the survey about globalization of Champions.
Maturity 2	Local events across the globe.	Visual inspection and survey – review the meeting schedule, and confirm that there are separate events across the globe. Attend a global event to confirm its format and popularity.
Maturity 3	Boots on the ground.	Visual inspection and survey – meet with the local security champion team members around the globe and confirm their scope and efforts.

Maturity 0 - No consideration

There needs to be a consideration for different parts of the globe.

Activity

- Interview various global champions, and understand the impact on them personally for working with a champions program pointing to your local time zone.

Benefit

- By creating a globalization strategy, the global champion citizens will stay as champions for a longer time, as they will feel more appreciated that you are creating a program that fits into their local time zone.

Maturity 1 - Comfortable schedule.

Create your meeting and activity schedule comfortable for global citizens.

Activity

- Inventory global champion citizens, and know the time zones that require coverage.

Benefit

- Allows the global team to participate as a single community.

Maturity 2 - Local events across the globe.

Create special global events that encompass the local time zones of your international champion citizens.

Activity

- Schedule global events, and realize you'll likely be staying late in your local time zone. It's okay; you're sacrificing for your global champion citizens.

Benefit

- Demonstrates the importance of global champions.

Maturity 3 - Boots on the ground

Install local security team members in global locations that can provide local events, coaching, and instruction.

Activity

- Hire new security team members to run your global champion group. Search within your global champions for candidates.

Benefit

- Local security team members can more easily pour into the local champions around the globe. Local security coaches understand the culture and can be more effective in coaching by accessing shared values and language.

Program

Short Description

Program: what do the champions receive?

Long Description

The program is the core component of the effort. The program includes all the pieces that provide value for the champion experience. From simple things like monthly meetings to advanced training or internal champion conferences, the program drives the value proposition for the champions.

Overview

Level	Name	Validation
Maturity 0	Nothing.	None
Maturity 1	Monthly training.	Visual inspection and survey – review the recent and future monthly training meetings, and review participation statistics, and ask Champions what they have experienced.
Maturity 2	Special events.	Visual inspection and ad hoc interviews – review the list of special events and meet with a cross-section of champions to understand the events' value.
Maturity 3	Deep effort.	Visual inspection and ad hoc interviews – review the list of deep events and meet with a cross-section of champions to understand the value the events provide.

Maturity 0 - Nothing

No programmatic elements; everything is ad hoc.

Activity

- Start planning a monthly training session to move to maturity level one.

Benefit

- Ad hoc champion programs are chaos for the participants and cause people to drift away. Build an agenda to breed stability in your environment.

Maturity 1 - Monthly training

Monthly training is the core piece of the program. It provides an environment for learning and connection amongst the champion population.

Every Champion meeting should focus on providing insight/educative material and working through whatever needs group input. Every group event is a teaching opportunity.

Activity

- Plan monthly meetings up to twelve months in advance, and add them to champion calendars.
- Provide a mechanism for champions to sign up to speak at a future monthly meeting.
- Reach out to various industry folks and invite them to join a monthly meeting to deliver a talk they have in the bag.

Benefit

- Monthly training builds a cadence within the community and provides champion learning.

Maturity 2 - Special events

Develop special training webinars, internal CTFs, and security days.

Activity

- Scope and schedule special, champion-only training webinars.
- Create internal capture-the-flag experiences only for the champions.
- Schedule and execute security days, as champion only four or eight-hour events.
- Have champion-only deep-dives into the security of the product and identify security debt, giving champions an opportunity to collectively strategize how to lower the debt.

Benefit

- Special events grow the knowledge and connection of the community.

Maturity 3 - Deep effort

Profound events provide value to the champions that allow them to advance their careers.

Activity

- Schedule and execute multi-day internal champion security conferences.
- Pay for and provide special champion certification training. The ISC2 CSSLP is a nice companion certification for champions. To provide true value, ensure the champion does not pay anything out of pocket for the class or the certification exam.
- Send a selection of champions to a regional or national security conference, covering all expenses.
- Develop an advanced degree focusing on cybersecurity, and provide this to your champions with no out-of-pocket expense.

Benefit

- Provides true rewards to those that dedicate their time to building a security community.

Metrics

Short Description

Metrics and measurement: how do you demonstrate program return on investment?

Long Description

Metrics and measurements demonstrate the value that a program generates with data. Metrics track various statistics. Program leadership can track statistics across multiple quarters and years to measure program value over some time.

Overview

Level	Name	Validation
Maturity 0	No metrics.	None.
Maturity 1	Basic metrics.	Visual inspection – review the metric plan and the metric data.
Maturity 2	Intermediate metrics and dashboards.	Visual inspection and survey – review the metric plan and the metric data. Add a question to the survey for scNPS.
Maturity 3	Action-based metrics.	Visual inspection – review the metric plan and the metric data.

Maturity 0 - No metrics

Activity

- Build a metrics plan.
- Execute the metrics plan.

Benefit

- Without measurement, nothing ever changes.

Maturity 1 - Basic metrics

Basic metrics are bulk metrics – items that count various measurable points with the champion program.

Example basic metrics: * Total count of champions * Business unit/product distribution * Champion education levels * Champion flaw density, measuring the number of flaws created per person per one-thousand lines of code.

Activity

- Incorporate the basic set of metrics into the metrics plan.

Benefit

- Basic measurement shows program impact.

Maturity 2 - Intermediate metrics and dashboards.

Intermediate metrics extend the basic metrics, adding champion/employee NPS (eNPS). eNPS is a methodology for applying Net Promoter Score to an employee population. Extend this directly to champions to measure scNPS or Security Champion Net Promoter Score. scNPS measures how likely a champion is to recommend a colleague join the program.

A dashboard is an information system that correlates and displays various metrics.

Activity

- Add scNPS to the metrics plan.
- Send out and report on scNPS according to a schedule laid out in the metrics plan.
- Build a dashboard to record and report on champion metrics.

Benefit

- Intermediate metrics demonstrate the community's impact on the Champions themselves, based on how likely they are to recommend a colleague join the program.
- A dashboard provides visibility into all the metrics tracked.

Maturity 3 - Action-based metrics

Action-based planning takes the output of metrics and creates and executes improvement plans, improving security and the program with the results of champion metrics and measurement.

Activity

- Create plans of action based on output metrics.
- Execute the action plans.

Benefit

- Taking action to improve security as a result of the community improves the organization.

Creative Commons Attribution-ShareAlike 4.0 International Public License

By exercising the Licensed Rights (defined below), You accept and agree to be bound by the terms and conditions of this Creative Commons Attribution-ShareAlike 4.0 International Public License ("Public License"). To the extent this Public License may be interpreted as a contract, You are granted the Licensed Rights in consideration of Your acceptance of these terms and conditions, and the Licensor grants You such rights in consideration of benefits the Licensor receives from making the Licensed Material available under these terms and conditions.

Section 1 – Definitions.

a. Adapted Material means material subject to Copyright and Similar Rights that is derived from or based upon the Licensed Material and in which the Licensed Material is translated, altered, arranged, transformed, or otherwise modified in a manner requiring permission under the Copyright and Similar Rights held by the Licensor. For purposes of this Public License, where the Licensed Material is a musical work, performance, or sound recording, Adapted Material is always produced where the Licensed Material is synched in timed relation with a moving image.

b. Adapter's License means the license You apply to Your Copyright and Similar Rights in Your contributions to Adapted Material in accordance with the terms and conditions of this Public License.

c. BY-SA Compatible License means a license listed at creativecommons.org/compatiblelicenses, approved by Creative Commons as essentially the equivalent of this Public License.

d. Copyright and Similar Rights means copyright and/or similar rights closely related to copyright including, without limitation, performance, broadcast, sound recording, and Sui Generis Database Rights, without regard to how the rights are labeled or categorized. For purposes of this Public License, the rights specified in Section 2(b)(1)-(2) are not Copyright and Similar Rights.

e. Effective Technological Measures means those measures that, in the absence of proper authority, may not be circumvented under laws fulfilling obligations under Article 11 of the WIPO Copyright Treaty adopted on December 20, 1996, and/or similar international agreements.

f. Exceptions and Limitations means fair use, fair dealing, and/or any other exception or limitation to Copyright and Similar Rights that applies to Your use of the Licensed Material.

g. License Elements means the license attributes listed in the name of a Creative Commons Public License. The License Elements of this Public License are Attribution and ShareAlike.

h. Licensed Material means the artistic or literary work, database, or other material to which the Licensor applied this Public License.

i. Licensed Rights means the rights granted to You subject to the terms and conditions of this Public License, which are limited to all Copyright and Similar Rights that apply to Your use of the Licensed Material and that the Licensor has authority to license.

j. Licensor means the individual(s) or entity(ies) granting rights under this Public License.

k. Share means to provide material to the public by any means or process that requires permission under the Licensed Rights, such as reproduction, public display, public performance, distribution, dissemination, communication, or importation, and to make material available to the public including in ways that members of the public may access the material from a place and at a time individually chosen by them.

l. Sui Generis Database Rights means rights other than copyright resulting from Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, as amended and/or succeeded, as well as other essentially equivalent rights anywhere in the world.

m. You means the individual or entity exercising the Licensed Rights under this Public License. Your has a corresponding meaning.

Section 2 – Scope.

License grant.

1. Subject to the terms and conditions of this Public License, the Licensor hereby grants You a worldwide, royalty-free, non-sublicensable, non-exclusive, irrevocable license to exercise the Licensed Rights in the Licensed Material to: reproduce and Share the Licensed Material, in whole or in part; and produce, reproduce, and Share Adapted Material.

2. Exceptions and Limitations. For the avoidance of doubt, where Exceptions and Limitations apply to Your use, this Public License does not apply, and You do not need to comply with its terms and conditions.

3. Term. The term of this Public License is specified in Section 6(a).

4. Media and formats; technical modifications allowed. The Licensor authorizes You to exercise the Licensed Rights in all media and formats whether now known or hereafter created, and to make technical modifications necessary to do so. The Licensor waives and/or agrees not to assert any right or authority to forbid You from making technical modifications necessary to exercise the Licensed Rights, including technical modifications necessary to circumvent Effective Technological Measures. For purposes of this Public License, simply making modifications authorized by this Section 2(a)(4) never produces Adapted Material.

5. Downstream recipients.

A. Offer from the Licensor – Licensed Material. Every recipient of the Licensed Material automatically receives an offer from the Licensor to exercise the Licensed Rights under the terms and conditions of this Public License.

B. Additional offer from the Licensor – Adapted Material. Every recipient of Adapted Material from You automatically receives an offer from the Licensor to exercise the Licensed Rights in the Adapted Material under the conditions of the Adapter's License You apply.

C. No downstream restrictions. You may not offer or impose any additional or different terms or conditions on, or apply any Effective Technological Measures to, the Licensed Material if doing so restricts exercise of the Licensed Rights by any recipient of the Licensed Material.

6. No endorsement. Nothing in this Public License constitutes or may be construed as permission to assert or imply that You are, or that Your use of the Licensed Material is, connected with, or sponsored, endorsed, or granted official status by, the Licensor or others designated to receive attribution as provided in Section 3(a)(1)(A)(i).

b. Other rights.

1. Moral rights, such as the right of integrity, are not licensed under this Public License, nor are publicity, privacy, and/or other similar personality rights; however, to the extent possible, the Licensor waives and/or agrees not to assert any such rights held by the Licensor to the limited extent necessary to allow You to exercise the Licensed Rights, but not otherwise.

2. Patent and trademark rights are not licensed under this Public License.

3. To the extent possible, the Licensor waives any right to collect royalties from You for the exercise of the Licensed Rights, whether directly or through a collecting society under any voluntary or waivable statutory or compulsory licensing scheme. In all other cases the Licensor expressly reserves any right to collect such royalties.

Section 3 – License Conditions.

Your exercise of the Licensed Rights is expressly made subject to the following conditions.

a. Attribution.

1. If You Share the Licensed Material (including in modified form), You must:

A. retain the following if it is supplied by the Licensor with the Licensed Material:

i. identification of the creator(s) of the Licensed Material and any others designated to receive attribution, in any reasonable manner requested by the Licensor (including by pseudonym if designated);
ii. a copyright notice;
iii. a notice that refers to this Public License;
iv. a notice that refers to the disclaimer of warranties;
v. a URI or hyperlink to the Licensed Material to the extent reasonably practicable;

B. indicate if You modified the Licensed Material and retain an indication of any previous modifications; and

C. indicate the Licensed Material is licensed under this Public License, and include the text of, or the URI or hyperlink to, this Public License.

2. You may satisfy the conditions in Section 3(a)(1) in any reasonable manner based on the medium, means, and context in which You Share the Licensed Material. For example, it may be reasonable to satisfy the conditions by providing a URI or hyperlink to a resource that includes the required information.

3. If requested by the Licensor, You must remove any of the information required by Section 3(a)(1)(A) to the extent reasonably practicable.

b. ShareAlike.

In addition to the conditions in Section 3(a), if You Share Adapted Material You produce, the following conditions also apply.

1. The Adapter's License You apply must be a Creative Commons license with the same License Elements, this version or later, or a BY-SA Compatible License.
2. You must include the text of, or the URI or hyperlink to, the Adapter's License You apply. You may satisfy this condition in any reasonable manner based on the medium, means, and context in which You Share Adapted Material.
3. You may not offer or impose any additional or different terms or conditions on, or apply any Effective Technological Measures to, Adapted Material that restrict exercise of the rights granted under the Adapter's License You apply.

Section 4 – Sui Generis Database Rights.

Where the Licensed Rights include Sui Generis Database Rights that apply to Your use of the Licensed Material:

a. for the avoidance of doubt, Section 2(a)(1) grants You the right to extract, reuse, reproduce, and Share all or a substantial portion of the contents of the database;

b. if You include all or a substantial portion of the database contents in a database in which You have Sui Generis Database Rights, then the database in which You have Sui Generis Database Rights (but not its individual contents) is Adapted Material, including for purposes of Section 3(b); and

c. You must comply with the conditions in Section 3(a) if You Share all or a substantial portion of the contents of the database. For the avoidance of doubt, this Section 4 supplements and does not replace Your obligations under this Public License where the Licensed Rights include other Copyright and Similar Rights.

Section 5 – Disclaimer of Warranties and Limitation of Liability.

a. Unless otherwise separately undertaken by the Licensor, to the extent possible, the Licensor offers the Licensed Material as-is and as-available, and makes no representations or warranties of any kind concerning the Licensed Material, whether express, implied, statutory, or other. This includes, without limitation, warranties of title, merchantability, fitness for a particular purpose, non-infringement, absence of latent or other defects, accuracy, or the presence or absence of errors, whether or not known or discoverable. Where disclaimers of warranties are not allowed in full or in part, this disclaimer may not apply to You.

b. To the extent possible, in no event will the Licensor be liable to You on any legal theory (including, without limitation, negligence) or otherwise for any direct, special, indirect, incidental, consequential, punitive, exemplary, or other losses, costs, expenses, or damages arising out of this Public License or use of the Licensed Material, even if the Licensor has been advised of the possibility of such losses, costs, expenses, or damages. Where a limitation of liability is not allowed in full or in part, this limitation may not apply to You.

c. The disclaimer of warranties and limitation of liability provided above shall be interpreted in a manner that, to the extent possible, most closely approximates an absolute disclaimer and waiver of all liability.

Section 6 – Term and Termination.

a. This Public License applies for the term of the Copyright and Similar Rights licensed here. However, if You fail to comply with this Public License, then Your rights under this Public License terminate automatically.

b. Where Your right to use the Licensed Material has terminated under Section 6(a), it reinstates:

1. automatically as of the date the violation is cured, provided it is cured within 30 days of Your discovery of the violation; or
2. upon express reinstatement by the Licensor. For the avoidance of doubt, this Section 6(b) does not affect any right the Licensor may have to seek remedies for Your violations of this Public License.

c. For the avoidance of doubt, the Licensor may also offer the Licensed Material under separate terms or conditions or stop distributing the Licensed Material at any time; however, doing so will not terminate this Public License.

d. Sections 1, 5, 6, 7, and 8 survive termination of this Public License.

Section 7 – Other Terms and Conditions.

a. The Licensor shall not be bound by any additional or different terms or conditions communicated by You unless expressly agreed.

b. Any arrangements, understandings, or agreements regarding the Licensed Material not stated herein are separate from and independent of the terms and conditions of this Public License.

Section 8 – Interpretation.

a. For the avoidance of doubt, this Public License does not, and shall not be interpreted to, reduce, limit, restrict, or impose conditions on any use of the Licensed Material that could lawfully be made without permission under this Public License.

b. To the extent possible, if any provision of this Public License is deemed unenforceable, it shall be automatically reformed to the minimum extent necessary to make it enforceable. If the provision cannot be reformed, it shall be severed from this Public License without affecting the enforceability of the remaining terms and conditions.

c. No term or condition of this Public License will be waived and no failure to comply consented to unless expressly agreed to by the Licensor.

d. Nothing in this Public License constitutes or may be interpreted as a limitation upon, or waiver of, any privileges and immunities that apply to the Licensor or You, including from the legal processes of any jurisdiction or authority.