Step-by-Step Guide for Setting Up a Software Security Group

Table of contents

Why have a software security group? 1

What does a software security group do? 1

Gain executive support 2

Pick a team lead 2

Define an organizational structure 3

Pick the right people 3

Equip them with the right skills 4

Add satellite support 4

What every software security program needs for a successful journey

Traveling with a group will motivate you to pick up the pace. Working together, a team will share the load and make everyone's pack lighter. The right team can make the difference between a painful slog and an incredible adventure.

This step-by-step guide will help you set up your own team so you'll be well-prepared to face the software security journey.

Meet your hiking party—the software security group.

Why have a software security group?

In many organizations, security leaders are balancing network, software, endpoint, even physical security as part of their responsibilities. They are pulled in many directions and must balance budget and resources across all areas. Most do not have specific expertise in the evolving requirements of software security—nor are they expected to.

Having an SSG—an assigned group with full-time responsibility—identifies software security as a specific area of cyber risk, managed by a team who understands the unique challenges of acquiring, creating, deploying, and managing secure software.

Having an SSG is a clear indicator of software security maturity, according to the Building Security In Maturity Model (BSIMM). All participants in the BSIMM organization that implement the most advanced risk management activities have an SSG.

A well-functioning SSG can lower the cost of a cyber attack. Companies that employ expert security staff can reduce cyber crime costs by an average of $1.5 million. Those that appoint a high-level security leader reduce costs by an average of $1.3 million.

What does a software security group do?

The SSG is ultimately responsible for finding and fixing software security defects in software you develop, license, or manage. It also helps ensure the vendors with whom you share data have adequate software security initiatives of their own.

An SSG is unique because it sits at the crossroads of security and development functions and looks for interaction points between the two groups.

It manages the process of introducing software security into the software development life cycle and, on the flip side, integrates the development perspective and process into security policies.

The SSG serves as a "center of excellence" for all software security needs, such as policy, standards, tools, experts, training, and so on, so that people have a place to get answers and improve their skills.

To increase awareness and knowledge of software security, the SSG reports on software security metrics, communicates results to executives and the organization at large, and makes the business case for needed resources.

6 steps to setting up a software security group

STEP 1 Gain executive support

You won’t make much progress on your journey without the backing of your executive team. You’ll need resources to build your SSG, as well as ongoing support to reinforce your policies and decisions within the organization.

Security awareness among boards of directors and executives is at an all-time high, but that doesn’t mean that your leadership team understands the nuances of putting together a software security initiative. Most execs don’t have a security background and won’t appreciate technical jargon.

To maintain management support for your SSG, you need to share your successes—in terms your audience understands and values.

- Explain how a software security initiative developed and managed by an SSG supports broader business goals, such as cost savings, competitive advantage, and customer satisfaction.
- In particular, focus on how the unique approach of an SSG can be a model for cross-functional cooperation to achieve the goals of both the security team and the development organization. By moving security “left” in the software development life cycle, you should be able to identify issues early and launch secure software products more quickly.
- Set up a regular reporting cadence so you can demonstrate how investment in an SSG yields continued progress.

STEP 2 Pick a team lead

An experienced team lead knows the best spots along the journey and can spot the dangers.

Depending on the organization, the SSG could sit under a variety of executives. For example, it could be under the CIO or CSO—as a key part of security strategy, along with network, endpoint, and physical security. It could be under the CTO as a key part of technology or under the CRO as a key part of risk management. On the other hand, it could be embedded as a senior position within a product development organization.

In any case, the team lead needs to be someone with the vision, management skills, authority, and resources to lead the organization on the journey toward software security maturity.

STEP 3

Define an organizational structure

The organizational structure of an SSG should encourage maximum communication and teamwork between the security and development functions. It's essential to clarify roles and responsibilities, decision-making power, and budget authority. The more clearly you outline these points, the more smoothly your SSG will run.

There is no "right way" to organize your team. Your structure should fit the culture of your organization. Among BSIMM organizations, there are five different models for structuring an SSG.

1. **Service Model.** This SSG offers software security activities such as pen testing, SAST, DAST, and so on "as a service" from a central hub. All work must go through the central group and follow standard processes. This model requires the SSG to sign off before products are released.

   Pros: Ensures consistent security protections.

   Cons: Product groups may need to wait to book resources, depending on demand. Developers may feel they have less responsibility for the security of their products.

2. **Policy Model.** A central team sets standard guidelines, but doesn't do actual execution. Policies include risk ranking and classification, creating knowledge bases and security frameworks, managing vendor compliance, and employee training.

   Pro: Fewer people considered "overhead" in a central team.

   Con: May be difficult to enforce policies.

3. **Hybrid Model.** This SSG offers both services and policy as explained above.

   Pro: A full-service SSG makes it easier to measure which policies are carried out and their level of impact.

   Con: Requires a full range of strategy and tactical skills.

4. **Business Unit Model.** This model distributes SSG members to individual business units to serve their specific needs, report within a business unit, and adapt policies and processes as needed.

   Pro: If it works well, more people within an organization are well-versed in security.

   Con: If there is poor coordination or communication, success can be difficult to maintain and measure.

5. **Management Model.** Product leaders manage security as a business process, along with product design, quality assurance, and so on.

   Pro: Security is truly embedded in the culture of the organization.

   Con: Business leaders must continue to prioritize security as they face pressure to release products quickly.

> There is no "right way" to organize your team. Your structure should fit the culture of your organization.

STEP 4

Pick the right people

An SSG doesn't have to be large. In fact, current BSIMM data show an average of about one SSG member per 75 developers for many organizations, with somewhat smaller ratios for organizations with thousands of developers.

An SSG is best composed of people with mixed backgrounds, who understand both security and development. Ideally, this should include people from:

- Security, including penetration testers and threat modelers
- Development, including software security architects, coders, and quality testers
- Risk, including people who specialize in compliance, audit, data governance, and privacy

STEP 5 Equip them with the right skills

Your chances of prospering in the wilderness are greatly improved when you equip your SSG with the necessary skills. The SSG must collectively have a broad and advanced understanding of software security activities that prepare you to deal with whatever hazards you encounter.

Look for opportunities to refuel and refresh your team's skills whenever possible, with training and experienced experts to guide the way. SSG members may rely on external partners for execution of security tests or other activities, but it is important that they have the knowledge to manage those partners effectively.

Soft skills are essential to create a resilient group that can work together toward a common goal. SSG members must be:

- Communicators who can work with people in different roles, executives, vendors, and partners to evangelize software security
- Collaborators who can build bridges across departments and balance competing priorities and goals
- Analysts who can use their knowledge and creativity to prioritize and recommend actions
- Teachers who can increase the skill levels of others in the organization

STEP 6 Add satellite support

In addition to the core team members, the SSG relies on support from other security stakeholders within the organization. This support allows the SSG to scale its reach and influence to all those stakeholders—application owners, development teams, QA groups, test teams, threat/intelligence teams, and so on.

We call this team a "satellite." It creates a social network that drives timely, grassroots efforts to accelerate the adoption of software security best practices. Having a strong satellite is a sign of a mature software security initiative.

How do you find people for your satellite?

- Identify people who stand out during introductory training courses.
- Ask for volunteers. Cyber security is a hot topic and a good career path many want to pursue.
- In a more top-down approach, you can assign qualified people within development or product groups to ensure coverage.

It's time to take the first step

Need help gaining executive support for your SSG?

Read Top 6 Application Security Hurdles and the Secret to Overcoming Them, and begin building the business case for your software security journey.

GET STARTED

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com