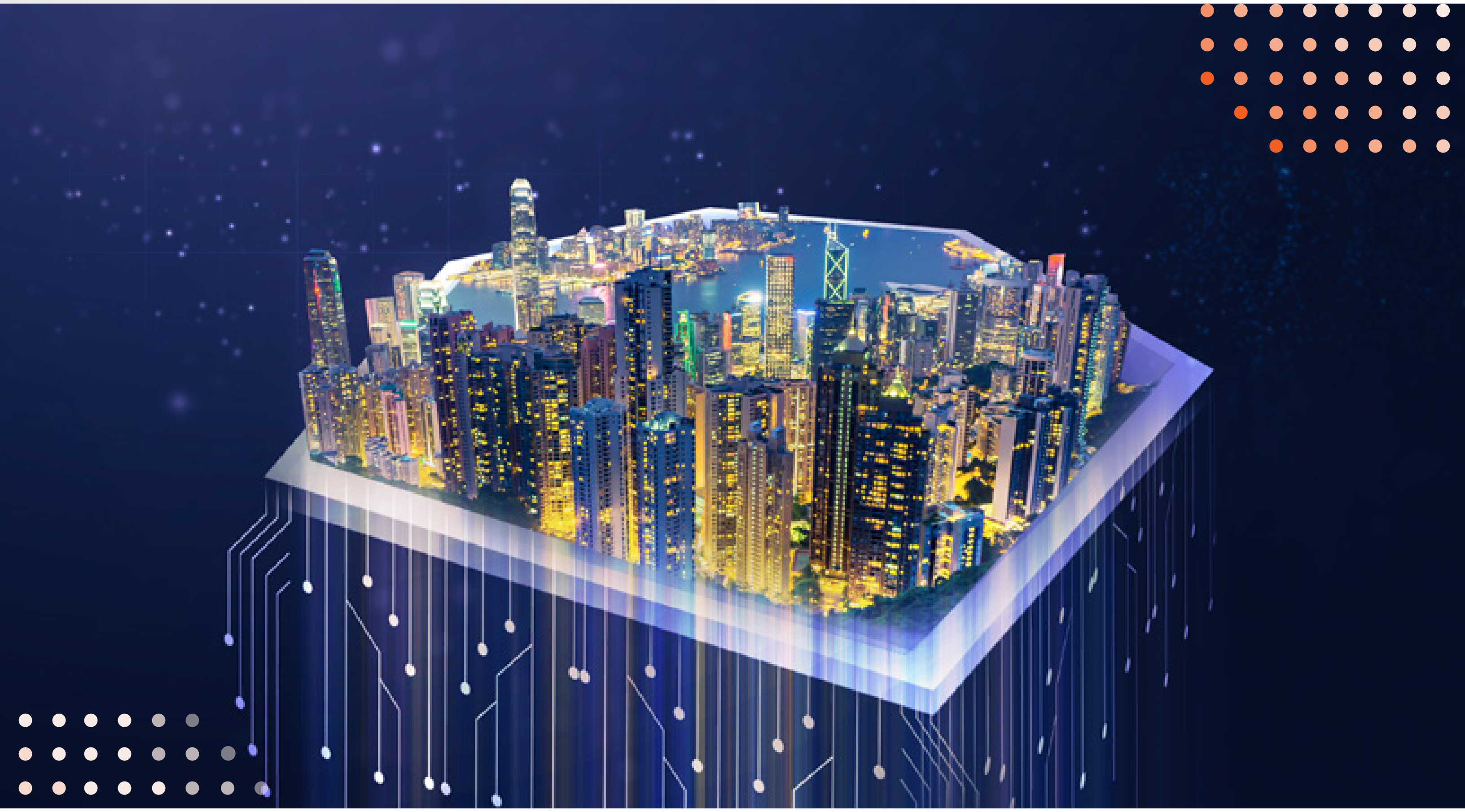
WHITEPAPER

How to Ramp Up Your AppSec Program

(And Keep Your Developers Happy)



Security Compass

Introduction

The news cycle for cyber security breaches seems to be on a continuous loop as bad actors get more and more creative in exploiting vulnerabilities in applications, platforms, and infrastructure.

For many mid-sized companies, growth depends on safeguarding applications, and responding to customer security demands and compliance requirements. But, the increasing volume of projects and business demand for faster releases often hinder the ability of development teams to deliver secure software due to a lack of security resources. The result? There is a tendency to handle security reactively rather than proactively, creating a "security island" that seems disconnected (or worse, oblivious) to the challenges development teams face to innovate and develop products faster.

How do resource-constrained security professionals build a metaphoric bridge to security island where security is addressed earlier in the software development lifecycle (SDLC) without facing the ire of development teams? In this whitepaper, we'll offer some practical steps growing companies can take to mature their security program in a scalable and sustainable way, as they convert developers into security champions.

How mature is your security program today?

The maturity of a security program can look very different across companies of various sizes. Some are just getting started with their application security program. Others may be moving along the path of having a programmatic security program, releasing secure software faster. Still, others may be feeling stuck or facing resistance from their development and DevOps teams.

Mid-size or growth companies with limited security and development resources need to focus on where teams are today and map out a strategy to build on those fundamentals in a way that is achievable and scalable. We typically see three categories:

BEGINNER

If you are just starting your program, you have probably done some training, maybe some code review, and perhaps hired a third party to conduct some penetration testing. In addition, you may be thinking about building out a DevOps team to help deploy code more efficiently and effectively. The good news is these are essential activities to building a security program. The bad news is that annual training is often typically done only to demonstrate compliance and is viewed as inconvenient rather than an opportunity to build knowledge and behaviors to build a culture of security. Similarly, while periodic code reviews and penetration testing will give some insights into vulnerabilities, they leave companies open to vulnerabilities and create additional backlog in the development cycle.

Mid-size or growth companies with limited security and development resources need to focus on where teams are today and map out a strategy to build on those fundamentals in a way that is achievable and scalable.

INTERMEDIATE

Many growing mid-sized companies have started building a DevOps function, are adding more regular penetration testing, and have started code scanning. Security vulnerabilities are being identified more frequently, but late in the development cycle during testing. DevOps is not integrated with security, and a "security island" disconnected from the development team and process is starting to emerge. Developers have begun to feel that security testing bottlenecks and backlogs are growing obstacles to meeting the product delivery demands of the business.

ADVANCED

As companies grow and mature, having a fully integrated DevSecOps infrastructure becomes more common. DevSecOps is an approach that puts security in the middle of software development and operations/deployment processes to enable rapid development balanced with security. While this level may seem out of reach for mid-size companies, a 2021 GitHub survey shows that most small and medium-size companies are developing software using DevOps or DevSecOps frameworks.

Beware of "Security Island"

Regardless of where you are in your security program development, beware of "Security Island." Security Island is the term used for a security team or professionals who are disconnected from the day-to-day activities of the development team; who seem like they live on a distant island.

In many mid-sized companies, the security team may consist of only one person. Though they are highly skilled, they typically have limited resources and smaller budgets than the development team. As the company continues to grow, silos often begin to develop between the security team and developers, and relationships can become increasingly contentious.

Combine this with the reality that developers don't typically receive formal training in security (beyond perhaps an annual training for compliance purposes) and you can see how easy it is for Security Island to establish itself.

Often, members of Security Island are perceived as the bad guys, with their sole mission being to tell the "Mainland" (the development team) what went wrong. By reporting failed code scans, issues uncovered during penetration testing, and not allowing code to go into production, Security Island quickly gets the reputation of being a blocker rather than an enabler. This reputation can feed into an unproductive "us versus them" culture, which can slow down the release cycle.

There is a tremendous opportunity for growth companies to avoid inadvertently building Security Island and build an AppSec program that embeds security into development, creating a collaborative and scalable culture of security.

Building a Bridge to Security Island

Your customers (and potential customers) increasingly demand assurance that you will meet their information security requirements. But how secure do you need to be?

Based on the markets you serve, software security requirements may vary widely. For example, if you produce software used by U.S. federal government agencies, your software should meet NIST standards. If you produce software for financial services companies such as banks, insurance, or investment companies, your software may need to be SOC 2 or ISO 27001 certified. Your customer may also demand that your software meet specific supply chain security and compliance requirements.

We often talk about "shifting left," "building security in," and more proactively managing security by injecting security requirements early in the application development lifecycle and tracing their implementation all the way through to the production environment. This is in direct contrast with the traditional approach to testing security only after software or a product has been built.

First things first. Focus on where your teams are today. For mid-sized or growth companies, this could mean you are at the beginner stage or maybe moving into the intermediate stage. When building out and scaling a security program, we advise companies to focus on fundamentals.

Although there are many ways mid-sized companies can create or advance a security program, we've identified three of the most critical steps.

Security champions

One of the most important things you can do, regardless of your current state of maturity, and especially if you are rapidly growing, is to build a security champions program. Security champions are developers who take accountability for the security of their projects and act as security mentors for their peers. Successful security champions are also able to articulate what does and does not work in an existing process and collaboratively work towards solutions that both satisfy security and engineering requirements and foster mutual understanding and respect.

Security champion programs tend to be highly effective within software development organizations, as developers are more likely to ask a teammate or listen to advice from a peer who understands how their projects work. And, because the champions are developers themselves, they more naturally connect the dots between what is needed for security and the business and engineering requirements. In addition, security champions are interested in security and developing those skills and can act as a "bridge-builder" to Security Island. When building a security champion program, it is vital to offer meaningful incentives to encourage developers to take on this role. Incentives could be small, such as company swag, or more significant, such as investment in training and certifications. In the long term this investment in people pays off as a far better and more cost-effective solution than continuing the never-ending cycle of trying to fix code while the backlog grows and releases are delayed.

Security champion programs tend to be highly effective within software development organizations, as developers are more likely to ask a teammate or listen to advice from a peer who understands how their projects work.

Awareness and education

Security champions help advance security culture and embed security awareness and expertise in development teams earlier in the SDLC. For example, let's assume that a development team's knowledge of security has been limited to periodic compliance-based training. As a result, they often don't know what type of security weaknesses they need to guard against in the code, or how to code securely to avoid vulnerabilities. It is important to create awareness programs and an environment where the development team can talk as peers with other teams. Once your development and DevOps teams understand the fundamentals of security awareness and have a bit of experience applying that to their work, you can start introducing increasingly mature concepts. For example, introduce DevOps teams to public material made by OWASP, NIST, and ISO once they understand security terminology.

Threat modeling

Software threat modeling is the ultimate shift left. When performed proactively and consistently, threat modeling can serve as an ounce of prevention that can help prevent a pound of breaches by enabling teams to identify and eliminate potential vulnerabilities before writing a single line of code. Traditionally, smaller software development organizations have viewed threat modeling as a luxury due to the need for staff to have a highly specialized skill set and highly manual, lengthy processes associated with most threat modeling methodologies. Increasingly, however, automation is making threat modeling more accessible and scalable, enabling growing companies to start to get ahead of potential vulnerabilities. Today, a relatively small investment in threat modeling upfront can result in significant time and money savings, as it helps avoid the need to spend large amounts of time and money recovering from an attack and repairing your corporate brand after a breach.

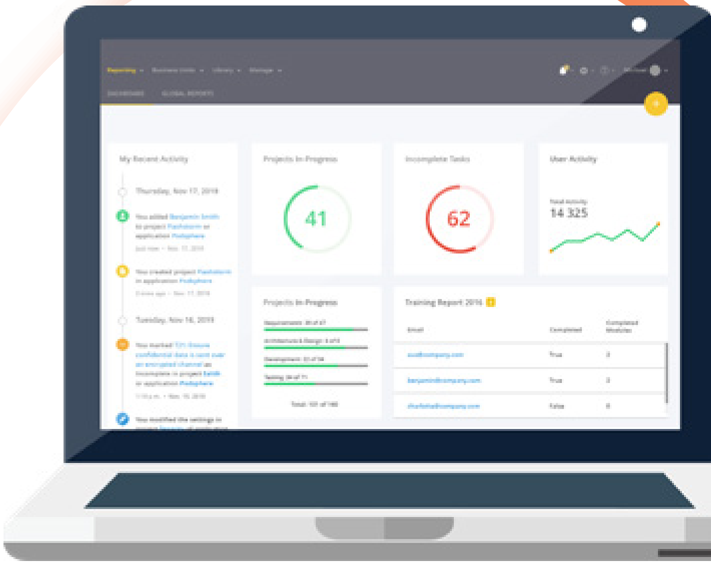
> **When performed proactively and consistently, threat modeling can serve as an ounce of prevention that can help prevent a pound of breaches by enabling teams to identify and eliminate potential vulnerabilities before writing a single line of code.**

Security Compass can help

SD Elements from Security Compass is a cost-effective, scalable, sustainable application security platform for growing companies. Our experienced team of DevSecOps professionals helps you assess where you are in your security journey. Then we work with you to help build out your application security program and improve your software time to market by embedding proactive security into your SDLC from the start.

Learn More

Contact us to learn how SD Elements can enable collaboration among compliance, security, privacy, and engineering teams.



Security Compass

Go Fast. Stay Safe.

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations of all sizes and stages to adopt Balanced Development Automation for rapid and secure application development. SD Elements helps automate significant portions of proactive manual processes for security and compliance that improve time to market for new technology. In addition, we offer advisory services on how organizations can embrace emerging technologies like the cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @securitycompass or visit them at securitycompass.com to learn more.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
600 California Street
San Francisco, California
USA 94108

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001