SECURITY COMPASS WHITEPAPER

Cybersecurity Talent Shortage: Combining In-House Expertise With Automation

SecurityCompass

Shortage of security professionals

Sometimes it seems like the white hats will never get ahead. Security talent is scarce in organizations of all sizes.

ISACA's State of Cybersecurity 2020 research reports that 62 percent of the respondents believe their organizations' cybersecurity teams are understaffed and 70 percent said fewer than half of cybersecurity applicants are well qualified.

When security roles can be filled, it is increasingly expensive.

62% of cybersecurity teams are understaffed

70% believe fewer than half of cybersecurity applicants are well qualified

Rapid application development challenges cybersecurity

A shortage of security talent comes at a time where defending against cyberattacks has never been more difficult and data breaches happen continuously.

With businesses increasingly moving to online platforms, perimeter defenses lose meaning. Each application, user, server, and IoT device provides an attack vector that must be defended. This is happening in a rapidly changing environment; a condition that favors the attackers over the defenders.

DevOps and CI/CD strains security resources: The ability to deliver features to users faster than competitors is a market differentiator. Rapid development and deployment methodologies like DevOps and Continuous Integration and Continuous Delivery (CI/CD) help organizations win business but present challenges with product security.

Traditional testing tools like static and dynamic analysis can take several hours to scan an application, then those results must be analyzed and prioritized. This model of testing for security is a poor fit when teams are pushing dozens of releases to production each day.

DevOps environments can also add another security consideration — containers. Containers like Docker allow organizations to deploy and update applications more quickly and easily. Containers also may have more people involved in management and deployment, leading to more opportunities for errors. In addition, an error in one container can quickly propagate to dozens or hundreds of containers as administrators clone images.

Cloud migrations: Organizations are moving their applications from in-house data centers to Cloud Service Providers (CSP) like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. These providers can provide everything from hosted environments managed by users to full Platform-as-a-Service offerings.

The benefits of moving to the cloud can be significant. Shared cloud resources are efficient and provide the ability for organizations to rapidly scale resources up or down as required without investing in fixed assets.

Cloud computing is not necessarily less (or more) secure than in-house data centers. They are different because of the “shared responsibility” model used by CSP. Under this model, the responsibility for each aspect of the application deployment changes depending on the deployment model selected. Understanding which entity is responsible for the infrastructure, metastructure, infostructure, and applistructure layers of the environment is critical and can challenge organizations.

Regulatory standards are multiplying: The regulatory landscape continues to grow each year, as do penalties for non-compliance. In addition, application security is now a board-level issue, and security and development teams need to comply with additional internal requirements. The result is that already stretched cybersecurity professionals need to account for new requirements each day and provide compliance reports in the event of an audit.

Cybersecurity skills shortage is not a people problem

Everyone knows you should validate application inputs, follow the principle of least privilege in critical applications.

While more security professionals are always welcome, simply adding people doesn’t solve problems like misconfigured AWS buckets and cloud resources left open to the world. These are errors made by people with too many things to keep track of.

With more and more applications to defend, security teams are turning to automation to scale their strategies and ensure that critical tasks are not overlooked.

Automation expands in-house security expertise

Automation is not about replacing humans.

It is about leveraging their expertise, particularly across repetitive tasks. Automation delivers to engineering and operations the information they need to build more secure applications from the beginning.

These security teams are expected to remember the hundreds of different items listed in their policy manuals and regulatory standards they “should do” for every project. Automation excels at these repetitive tasks, including translating policies and regulatory requirements into actionable tasks for engineering and development, and validating that each task is completed. This frees up scarce security resources and allows them to focus on critical applications.

Use automation to scale threat identification and mitigation

Automation has transformed security testing from expensive manual code reviews and infrequent penetration tests to scans initiated with every build. Unfortunately, these are often the first security activities performed on an application and are expensive. The remediation costs of security vulnerabilities are quite high at this stage of the SDLC.

The key to build secure applications is to anticipate risks using proactive approaches like threat modeling. While manual threat modeling requires weeks of effort from scarce security leaders, most of these activities can be automated.

Since over 90 percent of the threats can be derived from an applications' development stack, automating threat modeling eliminates inconsistent assessments and controls. By identifying and assigning controls as part of a developer's tasks, security testing becomes a validation exercise to ensure that assigned actions were completed correctly

How to fill the cybersecurity skills gap

Get rid of spreadsheets: The first step in automating security processes is adopting a centralized platform for policies and controls. Discrete spreadsheets for each project are difficult to manage, easy to ignore, and subject to untraceable changes. A centralized repository of rules and standard risk mitigation controls ensures that all security, development, operations, and compliance personnel have the information they need at all times.

Adopt policies and standards: Many organizations have secure software development policies. For those that do not, there are several external standards available to help organizations build more secure software. The US National Institute of Standards and Technologies (NIST) publishes SP800-53, a database of security controls and SP 800-95 Guide to Secure Web Services.

The Open Web Application Security Project (OWASP) provides an Application Security Verification Standard (ASVS) to help organizations test application security controls and the Cloud Security Alliance provides help for those organizations migrating to the cloud. Mapping these standards to corresponding security controls enables organizations to automate assignments of tasks based on the required policies and standards.

Automate threat identification and guidance: Attackers want to use the simplest approach possible and therefore focus on common weaknesses in applications. By translating an application's frameworks and deployment environment into actionable controls for developers, teams can eliminate a hacker's most common approaches.

Build secure applications through automation

The push to move businesses online keeps security professionals busy. While growing a team can help, automation is required to stay ahead of adversaries. Automation "stretches" security resources by covering repetitive tasks for which there are established policies and controls.

Automation ensures that organizational policies are followed for every application — not just the few most critical projects. Automation centralizes policy controls and allows organizations to standardize controls. It also provides a record of every activity used to secure applications, simplifying management reporting, and external audits.

SD Elements is the world's first Balanced Development Automation platform that enables you to automate proactive security processes for rapid application development.

Security Compass

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to adopt balanced development automation for rapid and secure application development. With their flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. In addition, they offer advisory services on how organizations can embrace emerging technologies like 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.

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
995 Market St,
2nd Floor
San Francisco, CA
USA 94103

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