Security Compass

MANAGING APPLICATION SECURITY

2017 Application Security Survey by Security Compass

MARCH 21, 2017

PRESENTED AT:

OWASP
Open Web Application Security Project

CONFIDENTIAL.

ABOUT THE SURVEY

PURPOSE

To discover how large, complex organizations manage application security.

WHO

Most respondents were large multinational companies earning >$1 billion USD in annual earnings (n = 28).

THE RESULT

Aggregated insights, industry trends, and best practices that illuminate how large corporations manage application security.

KEY FINDINGS

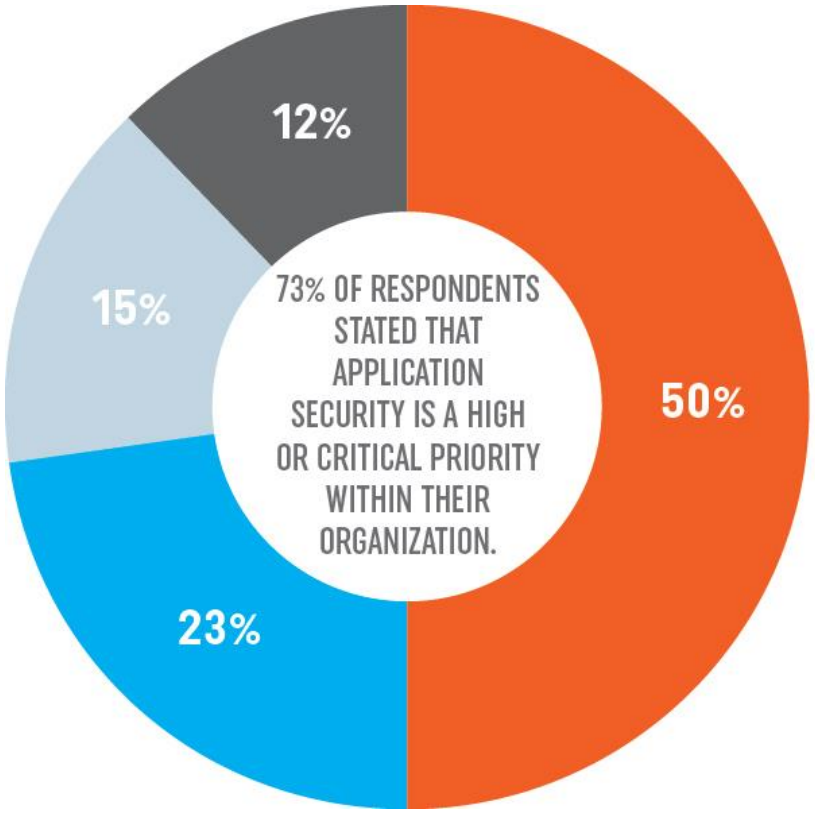
THREE KEY BUSINESS TRENDS

INCREASING SPEED OF BUSINESS

INCREASING SOPHISTICATION OF RISK MANAGEMENT

INCREASING PRESSURE ON COST CONTROL

IMPORTANCE OF APPLICATION SECURITY

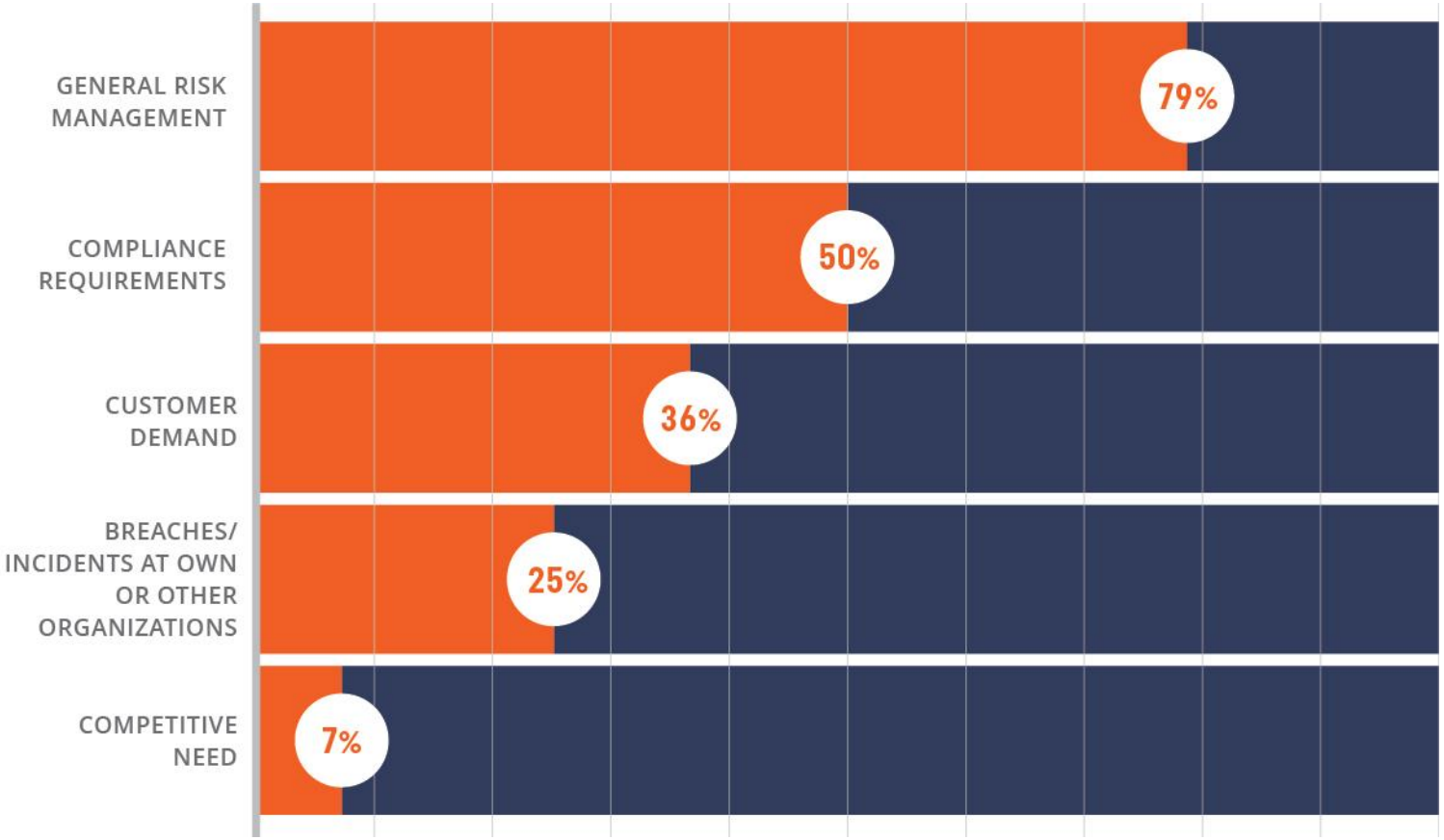


- IT IS CRITICAL/ALWAYS A TOP PRIORITY
- IT IS CURRENTLY A HIGH PRIORITY (E.G. BECAUSE OF AN AUDIT DEFICIENCY)
- IT IS THE SAME PRIORITY AS OTHER PARTS OF INFORMATION SECURITY (E.G. INCIDENT MANAGEMENT, NETWORK SECURITY, ETC.)
- IT IS NOT PARTICULARLY IMPORTANT COMPARED TO OTHER AREAS

73%

of respondents stated that application security is a high or critical priority within their organization.

KEY DRIVERS OF APPLICATION SECURITY



79%

of respondents stated that general risk management was the key driver for their organization's application security.

HOW BROAD IS YOUR ORGANIZATIONAL SUPPORT FOR APPLICATION SECURITY?

OWASP Open Web Application Security Project

Security Compass

FINANCIAL INSTITUTIONS

INDEPENDENT SOFTWARE VENDORS

1 = NO SUPPORT

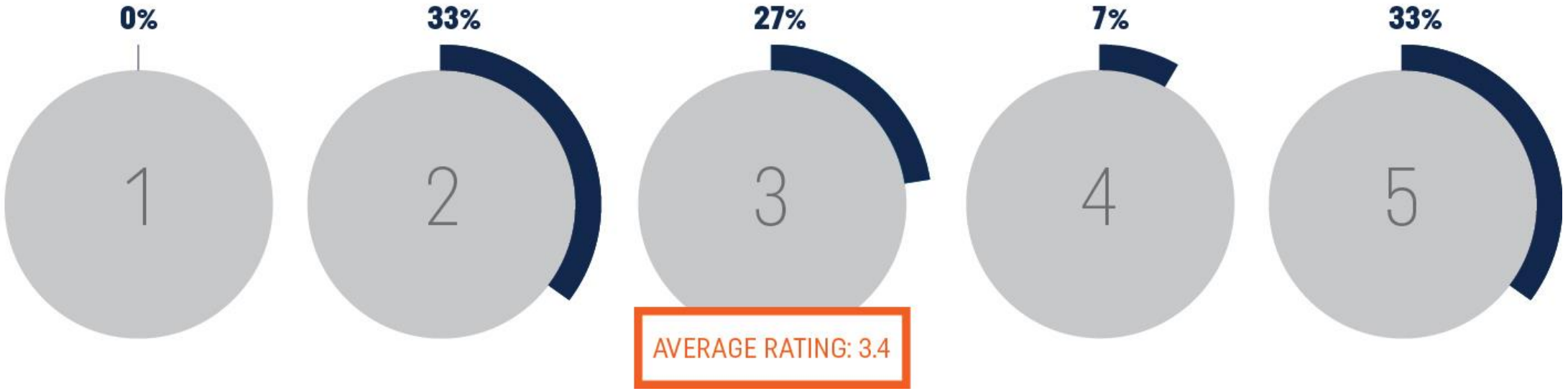
5 = SUPPORT ACROSS THE BOARD

OIL & GAS

ALL OTHERS

SECURITY AWARENESS TRAINING ADOPTION BY DEVELOPERS ACROSS THE ORGANIZATION

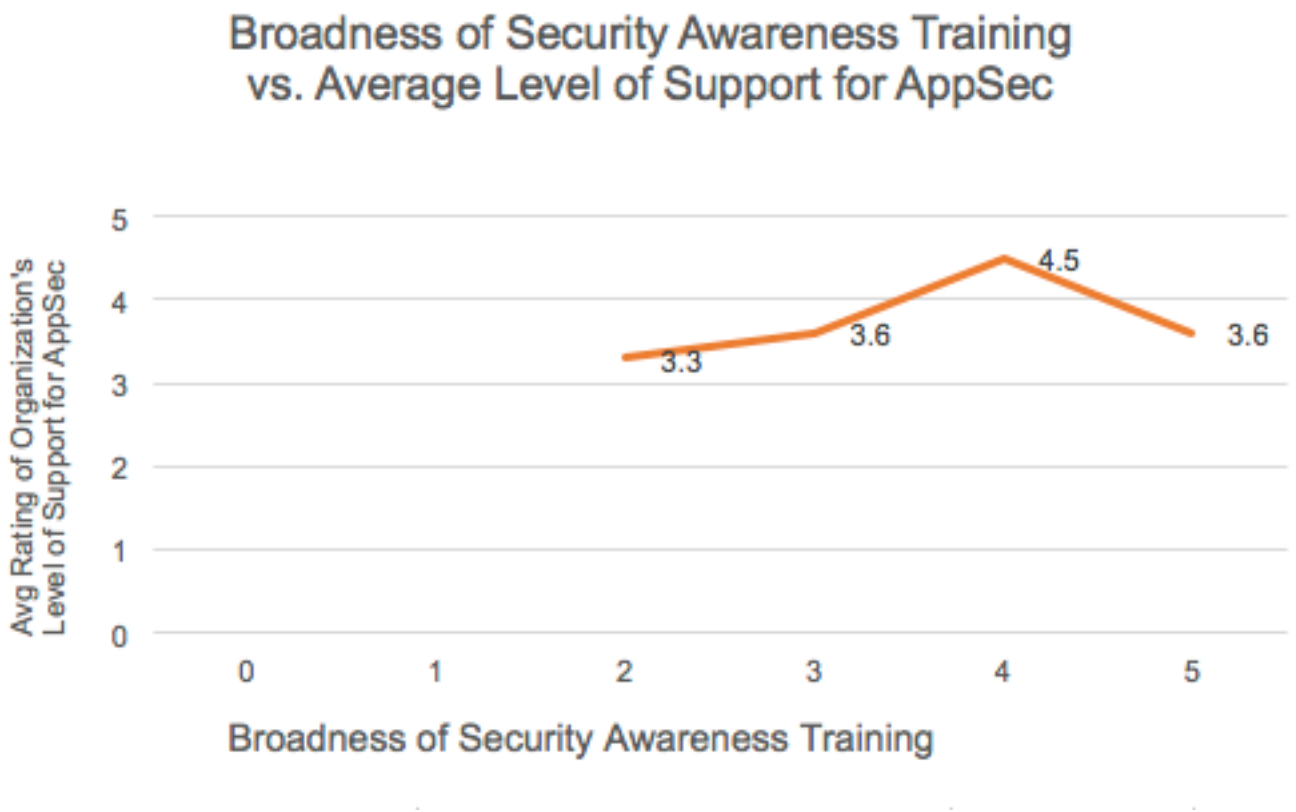
(1 = NO TRAINING, 5 = ALL DEVELOPERS ARE TRAINED)



Average Rating by Industry:

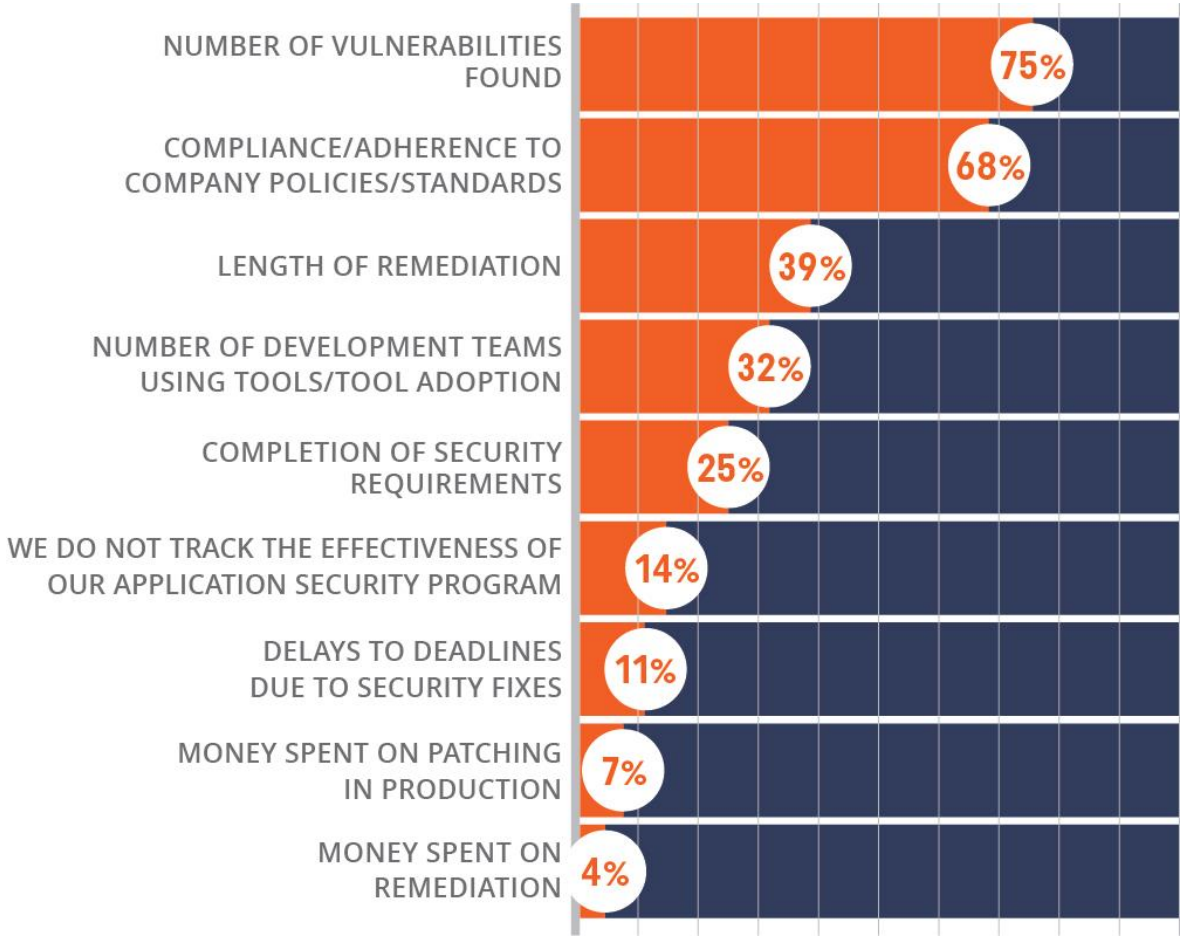
Financial Institutions	3.5
Independent Software Vendors	3.5
Oil & Gas	3.3

CORRELATION BETWEEN SECURITY AWARENESS TRAINING & SUPPORT FOR APPSEC



In general, respondents with a higher level of support for AppSec across the organization show a broader adoption rate of security awareness training, although a larger sample size can confirm this.

TRACKING THE EFFECTIVENESS OF AN APPLICATION SECURITY PROGRAM



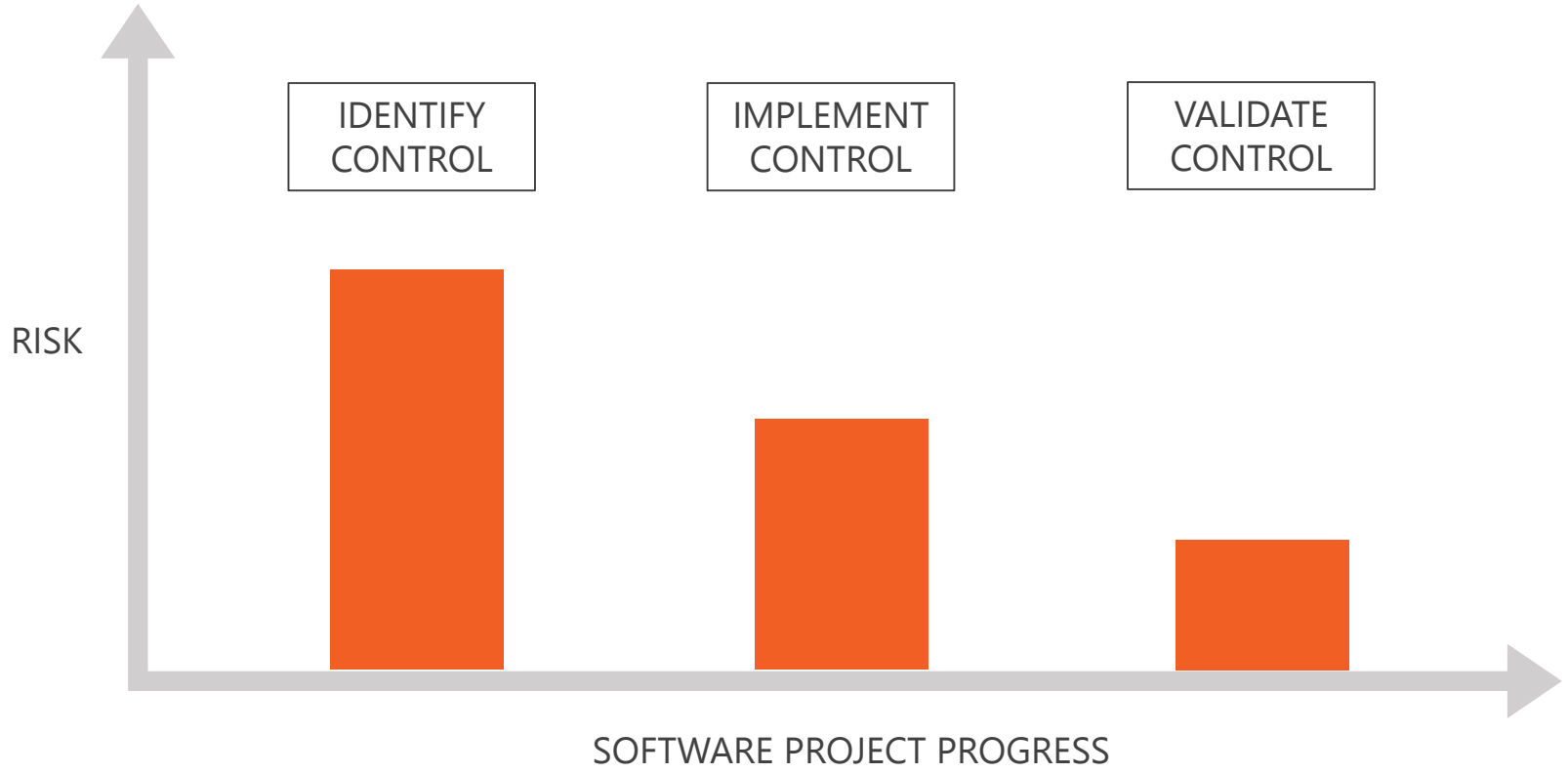
75%

of respondents stated that the number of vulnerabilities found was a key metric used to track the effectiveness of their application security program.

ONLY 4%

of respondents stated that they used the amount of money spent on remediating vulnerabilities as a key metric to track the effectiveness of their application security program.

RISK REDUCTION

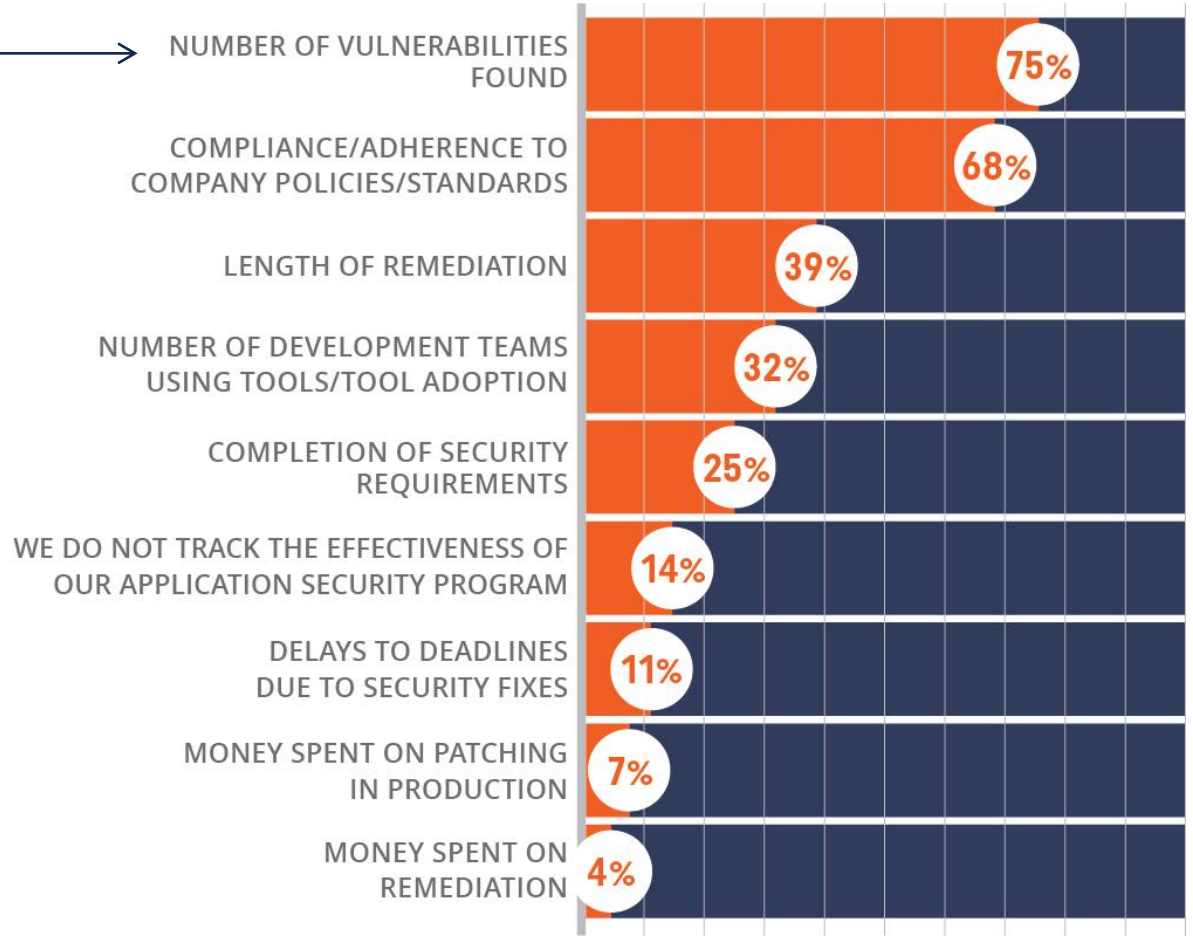


TRACKING THE EFFECTIVENESS OF AN APPLICATION SECURITY PROGRAM

OWASP Open Web Application Security Project

Security Compass

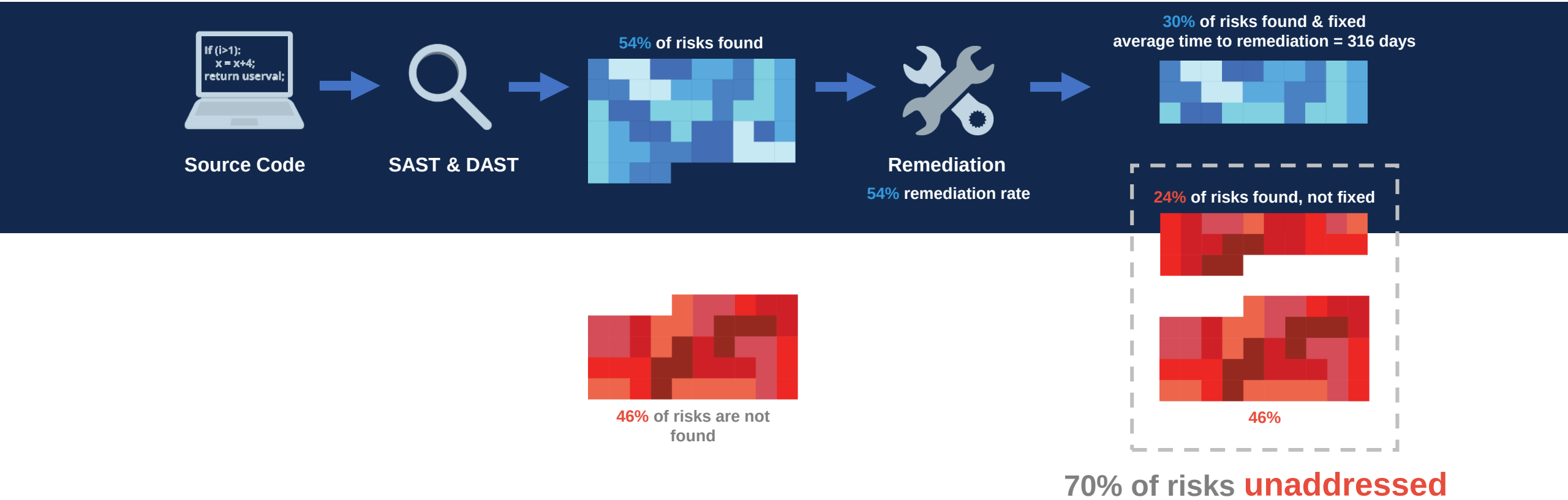
VALIDATE CONTROL →



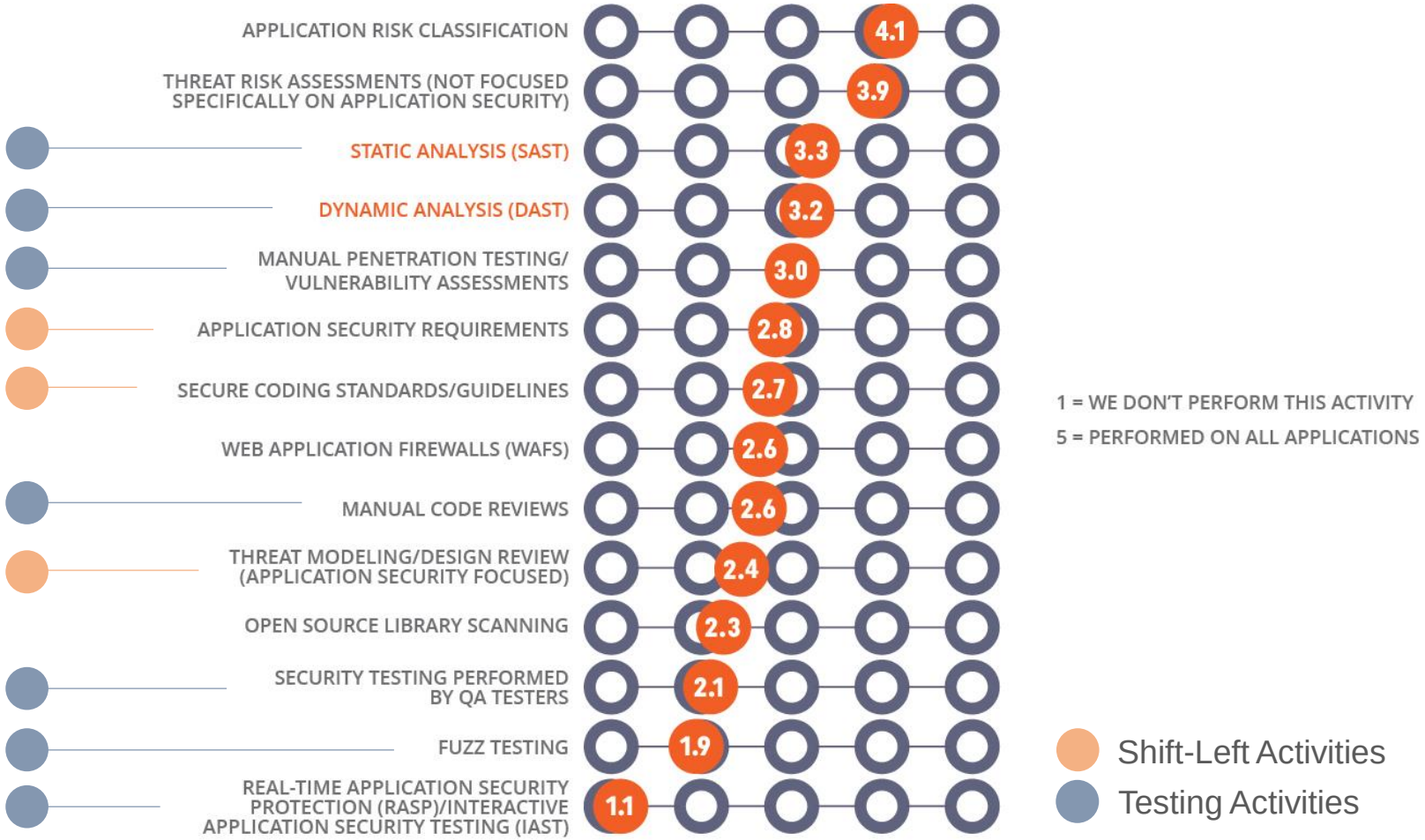
46% OF APPLICATION-LEVEL RISKS ARE NOT COVERED BY SAST & DAST TOOLS

OWASP Open Web Application Security Project

Security Compass

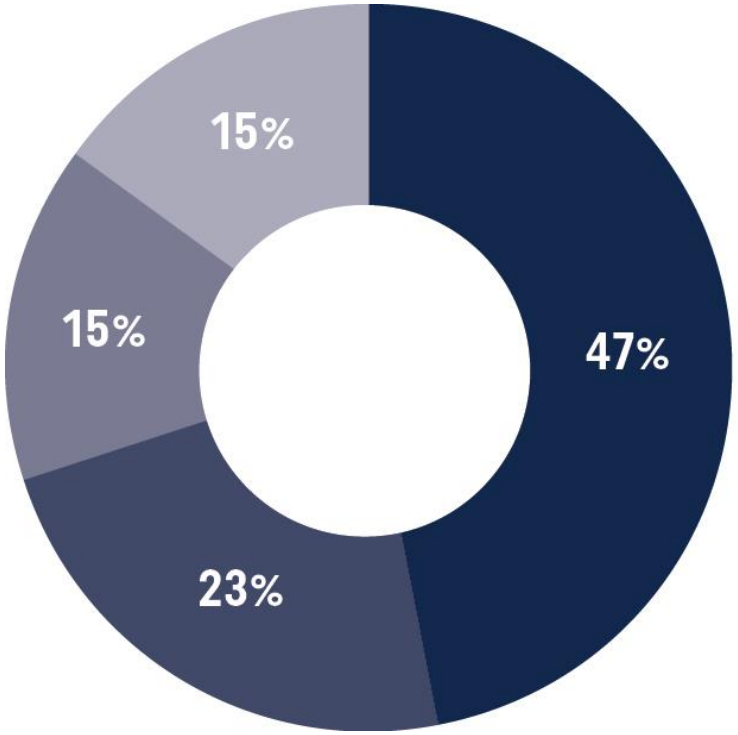


KEY SECURITY ACTIVITIES PERFORMED



What activities are you doing that are not listed here?

DO YOU PRIMARILY BUILD IN-HOUSE OR BUY THIRD-PARTY SOFTWARE?



- BUILD IN-HOUSE
- (ROUGHLY) EQUAL MIX OF ALL THREE
- BUY & CONFIGURE COTS
- (ROUGHLY) EQUAL MIX OF BUILD IN-HOUSE AND COTS

ENSURING THE SECURITY OF THIRD-PARTY VENDORS

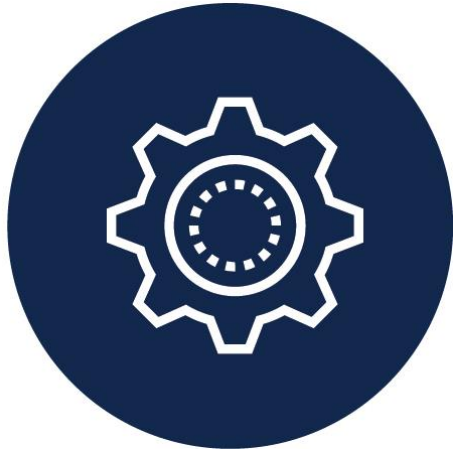
of respondents stated that they provide detailed application security requirements as part of their contracts with third-party software vendors.

of respondents stated that they perform threat modelling or other design-level analysis of third-party software.

A FRAMEWORK FOR APPLICATION SECURITY

STRATEGY

- DRIVERS & GOALS
- METRICS & GOVERNANCE
- ORGANIZATIONAL STRUCTURE



EXECUTION

IN-HOUSE

- TRAINING
- REQUIREMENTS & DESIGN
- TESTING

THIRD PARTY

- PROCUREMENT
- SECURITY QUESTIONNAIRES
- REQUIREMENTS
- TESTING

KEY

- RESPONDENTS NEED IMPROVEMENT
- RESPONDENTS ARE AVERAGE
- RESPONDENTS ARE STRONG

KEY TAKEAWAYS

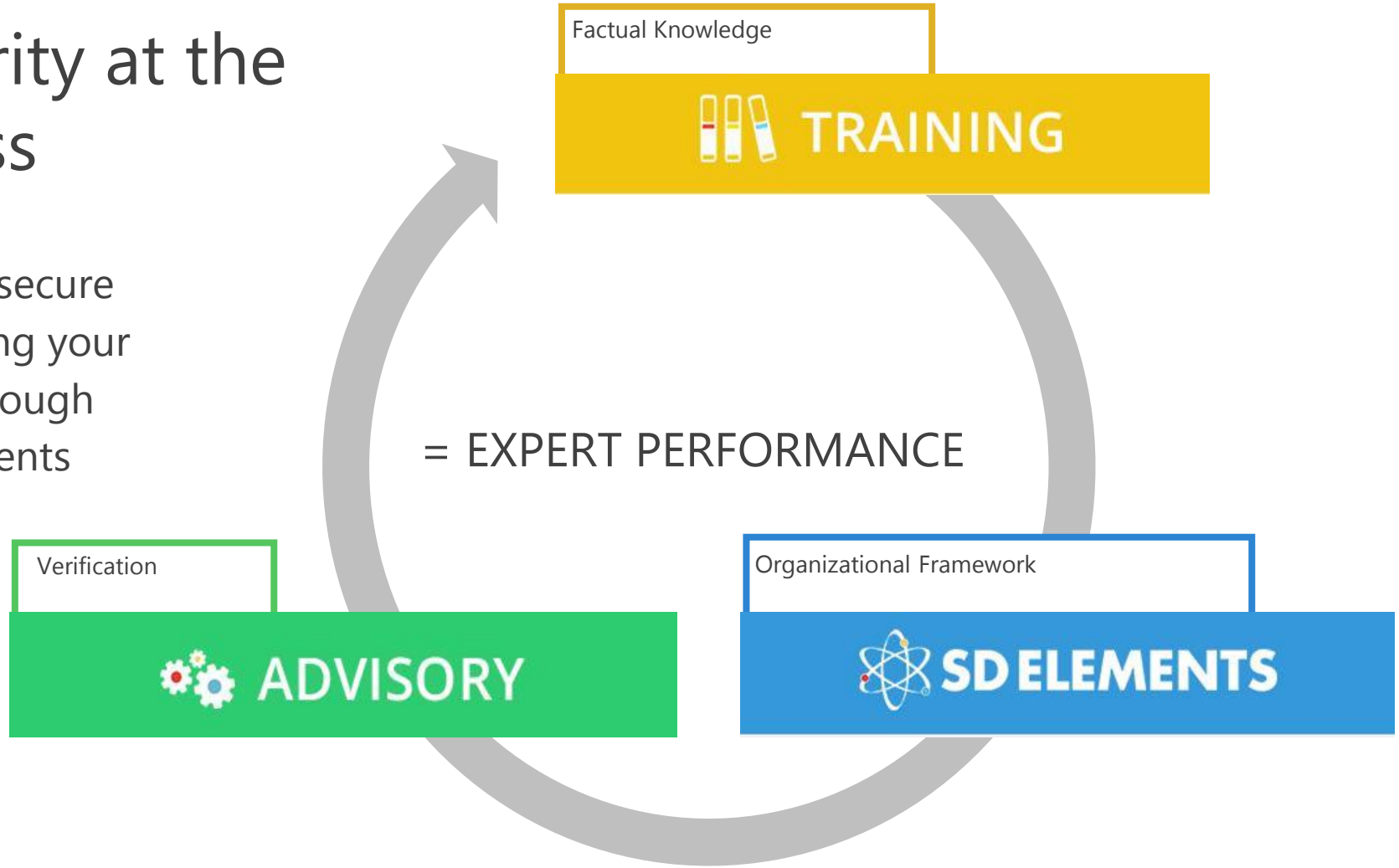
1. Require your vendors to have a higher standard for secure SDLC (e.g. ISO 27034 or vBSIMM or Microsoft's SDL)

2. Data about vulnerabilities is being unaddressed - keep this data in mind, communicate this to emphasize secure SDLC

3. Follow 3 steps for assurance - identify, implement & validate

Application Security at the Speed Of Business

Our goal is to help you build secure software by seamlessly unifying your application security needs through eLearning, Security Requirements and Verification.



Security Compass BU Overview

TRAINING

Our Secure Software Professional Suites provide business relevant security courses to help your staff champion security and defend your organization's most valuable software.

SD ELEMENTS

SD Elements automates software security requirements based on your project's technology, business and compliance drivers. SD Elements eliminates security vulnerabilities in the most cost effective way, before scanning begins.

ADVISORY

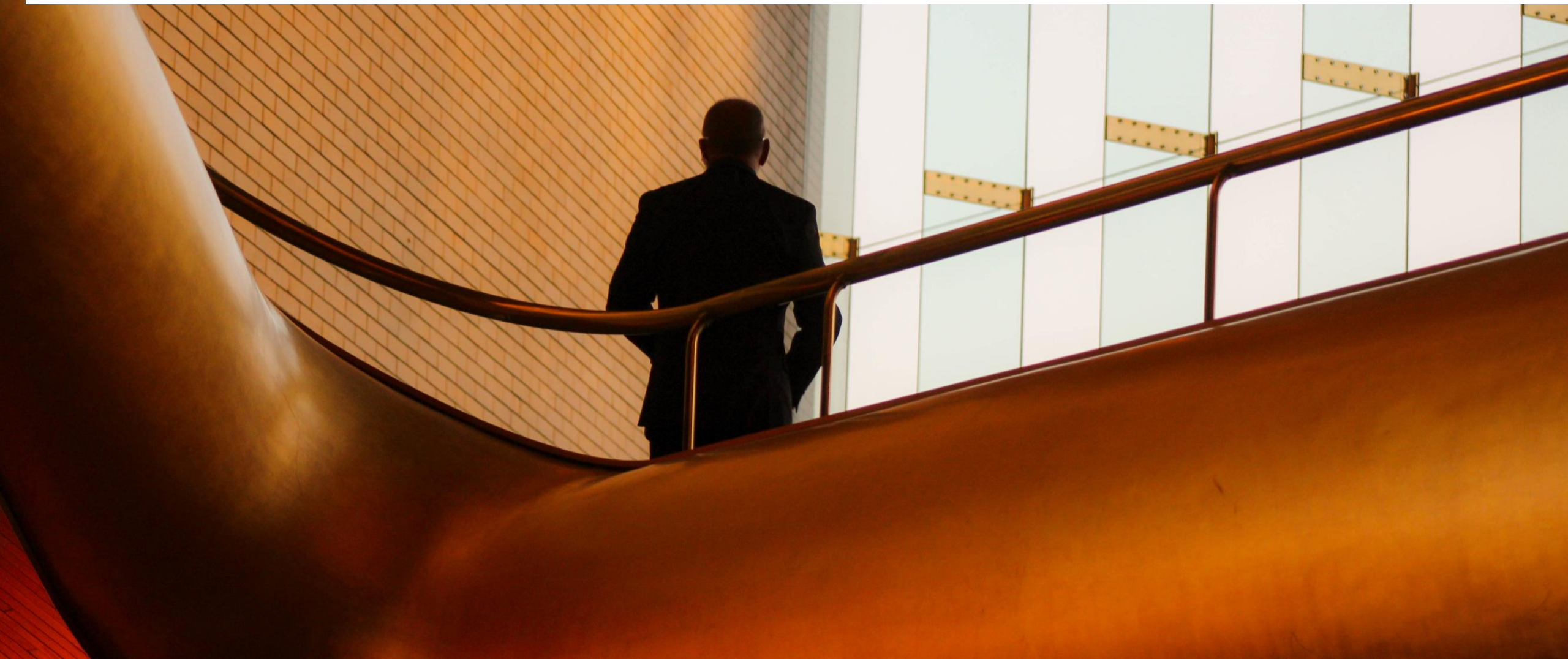
Our advisors understand your unique business requirements and provide services that advise on unique needs while focusing on driving strategic security goals.

For a copy of the full report, please visit:
https://www.securitycompass.com/managingapplicationsecurity2017/

Or email us at info@securitycompass.com

Security Compass

OWASP
Open Web Application Security Project



Security Compass

OWASP Open Web Application Security Project

Security Compass is a leading application security firm specializing in solving root application security problems for Fortune 500 companies. Our goal is to help clients build secure software by seamlessly unifying their application security needs through advisory services, training products, and security requirement software.

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

257 Adelaide Street West

Suite 500

Toronto, Ontario

Canada M5H 1X9

CALIFORNIA

1001 Bayhill Drive

2nd Floor

San Bruno, California

USA 94066

NEW JERSEY

621 Shrewsbury Avenue

Suite 215

Shrewsbury, New Jersey

USA 07702

INDIA

#4.07

4th Floor, Statesman House

Barakhamba Road, New Delhi

India 110001