Security Compass
THE SECURITY BY DESIGN COMPANY

Security Compass Overview

Presented By:

James Greenhaw – Account Executive

501.412.4041

jgreenhaw@securitycompass.com

Joseph Rowe – Solutions Engineer

214.592.3596

jrowe@securitycompass.com

Security Compass
THE SECURITY BY DESIGN COMPANY

Agenda:

Introductions

Security By Design with SD Elements

- Workflows
- Integrations
- Support

Customers

Net Net

Demo

SecurityCompass

THE SECURITY BY DESIGN COMPANY

Security By Design with SD Elements

Security Compass

THE SECURITY BY DESIGN COMPANY

Developer-centric software threat, security, and compliance modeling by design

Common Software Security Challenges

CHALLENGE 1:

Manual process to generate an Authority to Operate (ATO) is **slow**

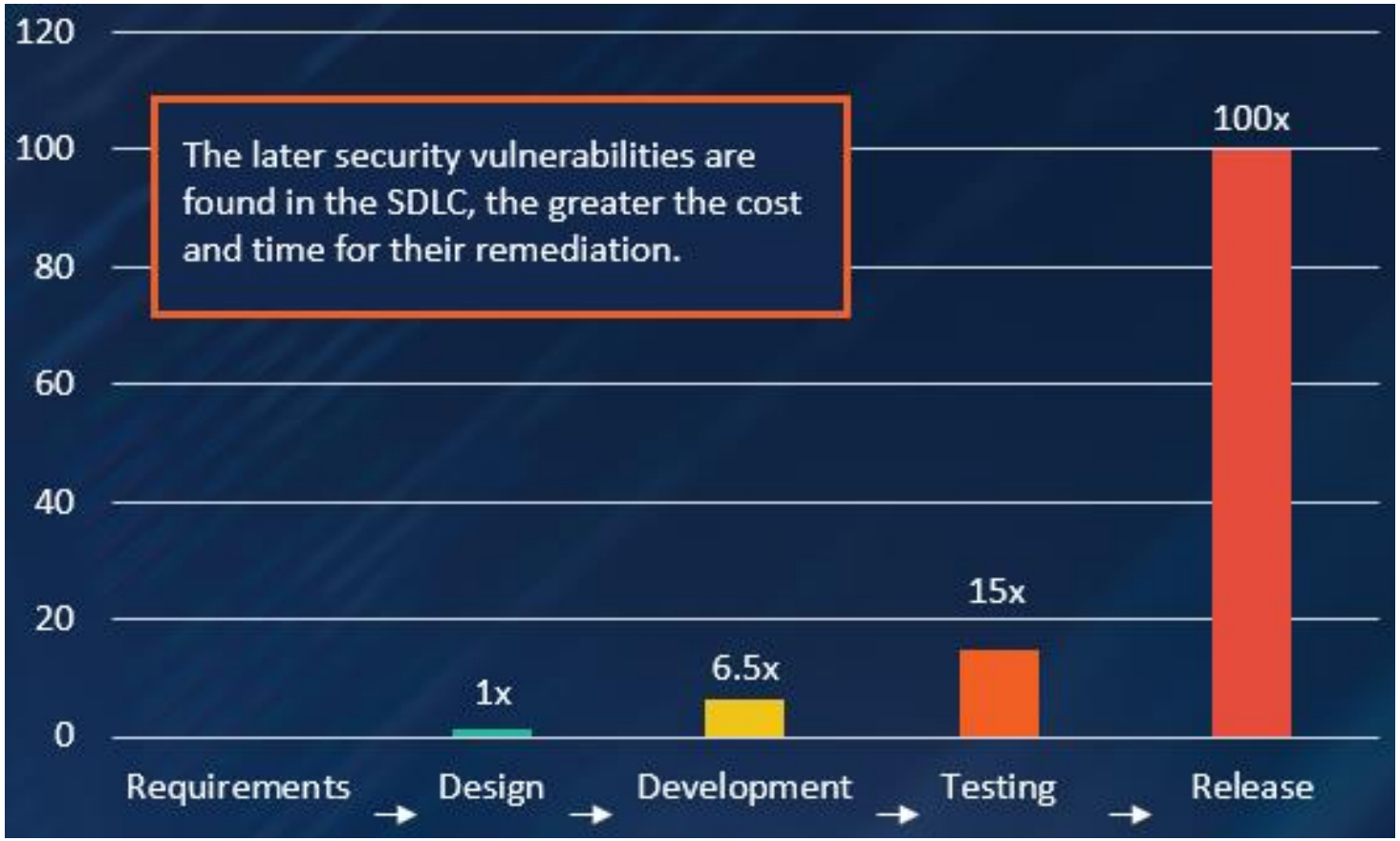
CHALLENGE 2:

Skills **shortage** limits the number of **security** professionals to support the ATO process.

CHALLENGE 3:

Remediation related to SAST/DAST Testing is costly and impacts development timelines/ATO process - **Reactive**

THE PROBLEM:
Software security policy to execution gap
NIST RMF ---> ATO



Role of SD Elements

SD Elements **enables** developers to build or modify software to meet security compliance standards (eg NIST RMF) and prevent the bad.

SD Elements integrates with popular SAST/DAST tools in order to verify compliance.

SD Elements generates auditable and traceable reports for each regulatory standard to verify compliance.

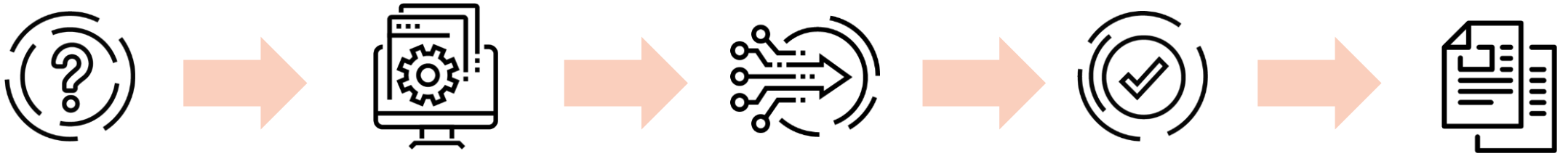
SD Element supports DevSecOps and enables rapid or continuous ATO

Security Compass

THE SECURITY BY DESIGN COMPANY

SD Elements Workflows

SD Elements/ATO Compliance Workflow



Survey

Characterize the project and identify applicable regulatory requirements through a survey.

Translate

SD Elements automatically translates complex regulatory standards (NIST RMF) into easy-to-understand development and IT activities.

Assign

Assigns tasks/activities to practitioners, including sample code, test plans, and Just-in-Time training. **In the task tracking system they use.**

Verify

SD Elements integrates with testing tools to verify task completion.

Report

SD Elements generates auditable and traceable reports for each regulatory standard to verify compliance.

SD Elements Content Library

Web Applications & Services
- Apex for Force.com
- C#, Visual Basic.NET, ASP.NET
- GoLang
- C/C++
- COBOL
- HTML5 and CSP
- Java SE / EE
- Java Libraries and Frameworks: (ESAPI, Struts, Spring, Apache Wicket, Hibernate)
- JavaScript (Angular, React, Node)
- JSP, Servlets
- PHP
- Python (Django)
- Ruby on Rails
- GraphQL
- TypeScript
- OAuth and OIDC
- SOAP & REST APIs
- XML & YAML Security

Cloud
- AWS, Azure, GCP, Terraform, Ansible

Containers
- Docker, Kubernetes, OpenShift

Web Servers
- Apache HTTP, Apache Tomcat, Microsoft IIS, NGINX

Databases
- SQL: MS SQL Server, MySQL, Oracle
- NoSQL: MongoDB
- Cloud databases: AWS (DynamoDB, RDS), Azure, GCP

Microservices Infrastructure

Mobile
- iOS Swift/ObjC, Android Java/Kotlin

Internet of Things (IoT)
- Authentication and Access Control
- Bluetooth
- Communication Protocols: MQTT, XMPP, AMQP, Thread, HyperCat, ZigBee, Pub/Sub
- Availability and Systems DoS Protection
- RFID Solutions
- WiFi

Regulatory & Compliance
- ANSI/ISA/IEC 62443-3-3
- ANSI/ISA/IEC 62443-4-2
- CMMC v1 & v2
- Cloud Security Alliance CCM
- CNSSI 1253
- DIACAP
- FedRAMP
- GLBA
- HIPAA
- ISO 27001:2013/SOX
- NYDFS
- PCI-DSS
- PCI Secure Software Framework (SSF)
- SOC2 (AICPA TrustServices Criteria)

Privacy
- Anti-Spam Guidelines/CASL
- Brazilian LGPD
- California Consumer Privacy Act (CCPA)
- California Privacy Rights Act (CPRA)
- California Online Privacy (CalOPPA)
- Children's Online Privacy (COPPA)
- Chinese Cybersecurity Law 2020
- EU GDPR
- EU Privacy and Cookie Laws
- GAPP
- New York Shield Act (S5575B)
- NIST 800-53 Privacy Controls
- PIPEDA/ECPA/CAN-SPAM

Industry Standards
- ASD-STIG 5
- CWE 4.3 Software
- CWE 4.3 Hardware
- CWE/SANS Top 25
- MDS2-2013
- OWASP Top 10 2021 & API Top 10 2019
- OWASP ASVS 4.0
- OWASP Mobile ASVS
- NIST 800-171 Non-Federal Systems
- NIST 800-53 Information Systems
- NIST 800-82 Industrial Control Systems
- NIST 800-95 Web Services
- NIST 800-147/800-155 BIOS/FW
- NIST 800-190 Container Security
- NIST 800-218 SSDF
- Executive Order 14028
- UNECE WP29/R155
- ISO 21434
- DISA Control Correlation Identifier (CCI) Framework
- NISTIR 8397 (Verification Req.)

Weaknesses: **833**
Countermeasures: **1929**

How-Tos: **1484**
Additional Req: **3922**

As of April 2023

Regulations/Reports: **89**
Training Videos: **942**

Master Datasheet

Just-In-Time Training: Right Guidance, Right Time

Integrated

- Mapped to security requirements
- Synced to your ALM tools (e.g. JIRA) through SD Elements

Progress Reports

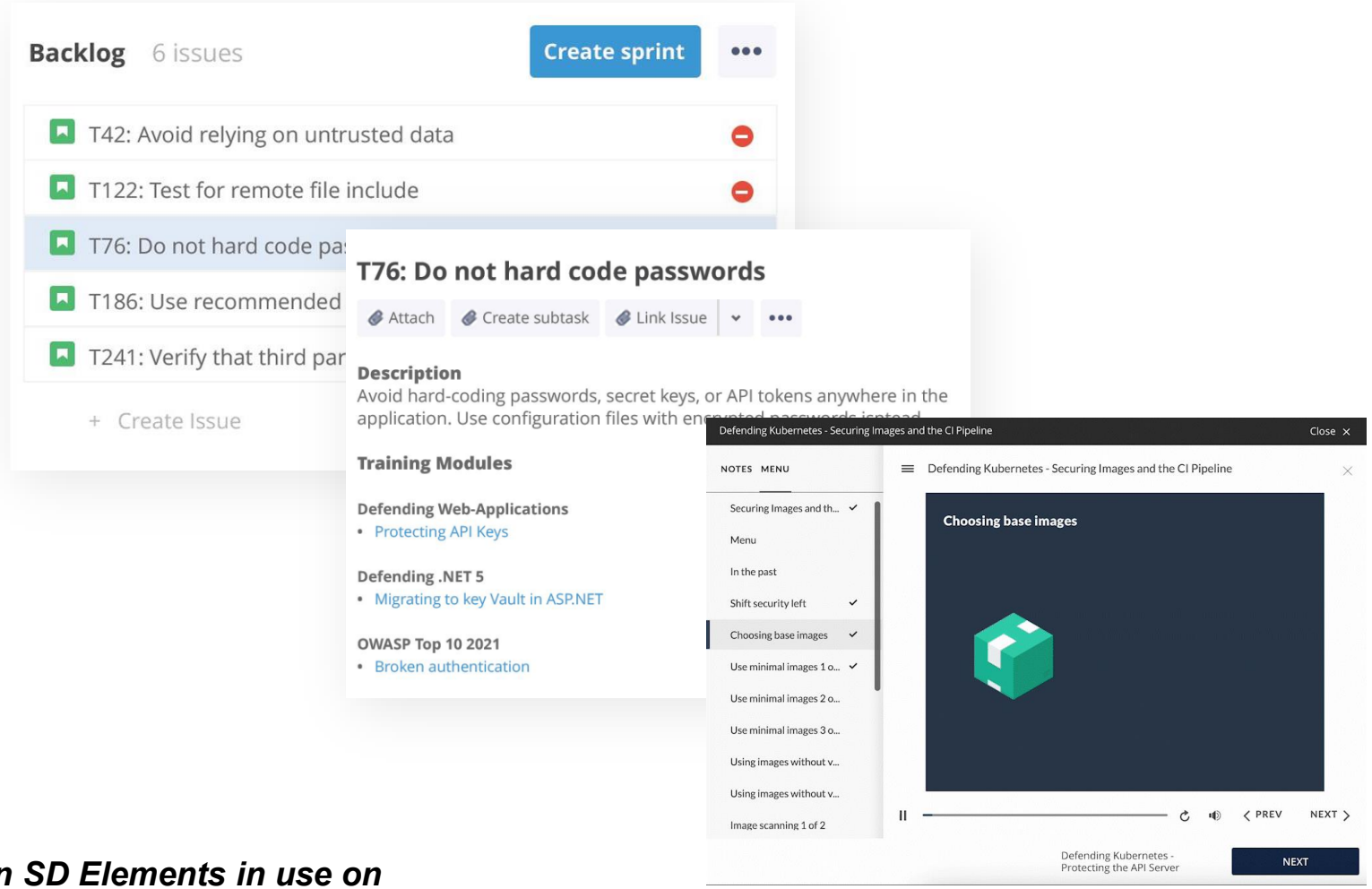
- Track and report progress to encourage continued learning

Contextual Microlearning

- Micromodules & tasks complement written instructions
- Developers understand why & how to implement security requirements

Flexible

- Our researchers manage content
- Address new technologies and custom frameworks



"Having seen SD Elements in use on Kobayashi Maru I can tell you this content is excellent."
-Associate Director – Cyber, Raytheon

Security Compass

THE SECURITY BY DESIGN COMPANY

Integrations

SD Elements: 37+ Integrations to Support DevSecOps Workflows

Issue Tracking

Jira Software

GitHub

GitLab

IBM® Engineering Workflow Management (formerly RTC)

Azure

MICRO FOCUS
ALM/Quality Center

ca technologies A Broadcom Company
Rally

PivotalTracker

servicenow

digital.ai

RSA ARCHER SUITE

Security Code Scanning (SAST/DAST/SCA)

VERACODE
Dynamic Analysis & Static Analysis

MICRO FOCUS
Fortify WebInspect, Static Code Analyzer

HCL

HCL AppScan

SYNOPSYS®
Coverity & WhiteHat

snyk NEW

BLACKDUCK

sonarqube

Checkmarx

klocwork

OWASP Dependency Check & Dependency Track

DevOps Tools (CI/CD)

Jenkins

Azure Pipelines

XebiaLabs XL RELEASE

Infrastructure

nessus Professional

PRISMA BY PALO ALTO NETWORKS

Security Tools

ThreadFix

MICRO FOCUS
Fortify on Demand & Fortify Software Security Center

Security Compass

THE SECURITY BY DESIGN COMPANY

Support

Your Customer Journey with SD Elements Support w/ Dedicated CSM

ALIGN

Program Kickoff

Align for success with kickoff activities

Milestone and Goal Planning

Define SMART goals and key milestones
* People * Process * Technology

EXECUTE

Program Management Consultation

Participate in a discovery session

Rollout Plan

Support the cross-functional adoption of SD Elements

Instructor-Led Training

Learn from initial product training

REALIZE

Guided Rollout

Partner with us to execute your rollout plan and continue for healthy adoption

Advanced Automation and API Support

Receive advanced support for more complex projects and requirements

ADVOCATE

Advanced Product Feature Enablement

Stay up to date on latest Product feature updates from Security Compass as well as industry developments and trends

Product Usage Analytics

Receive our analysis of anonymized, encrypted and aggregated data to monitor product usage

Security Compass

THE SECURITY BY DESIGN COMPANY

Customers

Organizations Using SD Elements

***USAF Kessel Run** *Software Factory*

***Platform One** *Organization that manages/supports Software Factories for DOD Development teams*

Including: Kobayashi Maru, TRON, Army INSCOM, CYBERCOM's Unified Platform, and others

USAF ABMS CBC2 (Cloud Based Command & Control)

US Air Force Space and Missile Systems Center

The Securities and Exchange Commission

Joint Strike Fighter (JSF) F-35 Program

***USAF Business and Enterprise Systems Product Innovation (BESPIN) Office**

USAF Weather Program

The Federal Bureau of Investigation

***The Department of Veterans Affairs**

***TRANSCOM – TCODE**

SD Elements has been selected as part of the DoD Enterprise DevSecOps Platform Stack (security tools) to drive RMF documentation and controls management

SD Elements is listed on the USAF DevSecOps Tools, Pipeline and Platform Integration and Licensing Basic Ordering Agreement

-The SD Elements hardened container is DOD Iron Bank Approved

--15 of the Fortune 500 commercial companies use SD Elements (ex: Intel, Cisco, PayPal, Adobe)

*** = Software Factory**

WHY SECURITY BY DESIGN

U.S. Government agencies obtain ATO faster & deliver secure software at scale with SD Elements

KESSELRUN

Challenge
Disconnected development tools, vulnerability scanning process, and manual practices slowed time to ATO

Goal
Streamline processes to obtain obtain ATO and continuous cATO

Solution
- Tailored, task-based guidance
- Embedded just-in-time training so developers could write secure code faster

Platform One

Challenge
Demonstrate compliance with NIST 800-53 with manual, labor-intensive processes

Goal
Accelerate secure software delivery by translating security requirements & tracking implementation for developers

Solution
- Reduced time to obtain & maintain cATO from MONTHS/YEARS TO DAYS/WEEKS

BESPIN

Challenge
Needed to automate security requirements generation and compliance traceability early in the dev cycle

Goal
Reduce time to obtain ATO and maintain cATO for applications

Solution
- Automated compliance artifact creation, used SDE threat modeling to ID and remediate vuls early, leveraged our experts to ensure their IA pros were trainged in sw dev best practices

Security Compass

THE SECURITY BY DESIGN COMPANY

Net Net

Net Net: Why SD Elements?

Upskill Developers W/ In Context Training

Significantly Reduce False Positive/Negative Adjudication Activities

Double Check SAST Findings On A Per Tool Basis

100% Automation of Compliance Documentation

Enterprise Continuous Compliance Monitoring

Dedicated Support Rep

Thank you!

Security Compass

For more information please contact:

James Greenhaw

jgreenhaw@securitycompass.com

501.412.4041

1.888.777.2211

info@securitycompass.com

www.securitycompass.com

@securityCompass

Security Compass

Security Compass

THE SECURITY BY DESIGN COMPANY

Demo