



SecurityCompass

DevSecOps by Design

How to Incorporate Security & Compliance earlier than Testing and Scanning.

Trevor Young
Chief Product Officer
Security Compass



About Security Compass



Trevor Young

Chief Product Officer, Security Compass

founded in

2004

by security
professionals

15%

of Fortune 100 are
our customers

Developer Centric

**Threat
Modeling**

platform

Application

**Security
Training**

& ISC² Certification

DevSecOps By Design

Products are built in a way that protects against malicious cyber actors gaining access to devices, data & connected infrastructure. Key activities include:

- Training & Awareness
- Coding Practices, Policies & Controls
- Secure Architecture Design & Requirements
- Threat Modeling

WH.GOV 

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM

PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect


NIST Special Publication 800-218

Secure Software Development Framework (SSDF) Version 1.1:

Recommendations for Mitigating the Risk of Software Vulnerabilities


Murugiah Souppaya
Karen Scarfone
Donna Dodson

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-218>


National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY STRATEGY

MARCH 2023


THE WHITE HOUSE
WASHINGTON



Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default

Publication: April 13, 2023
Cybersecurity and Infrastructure Security Agency
NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-AZ

Traditional Approach to Security



Typical Organizations Focus on Testing & Patching

UNCLASSIFIED

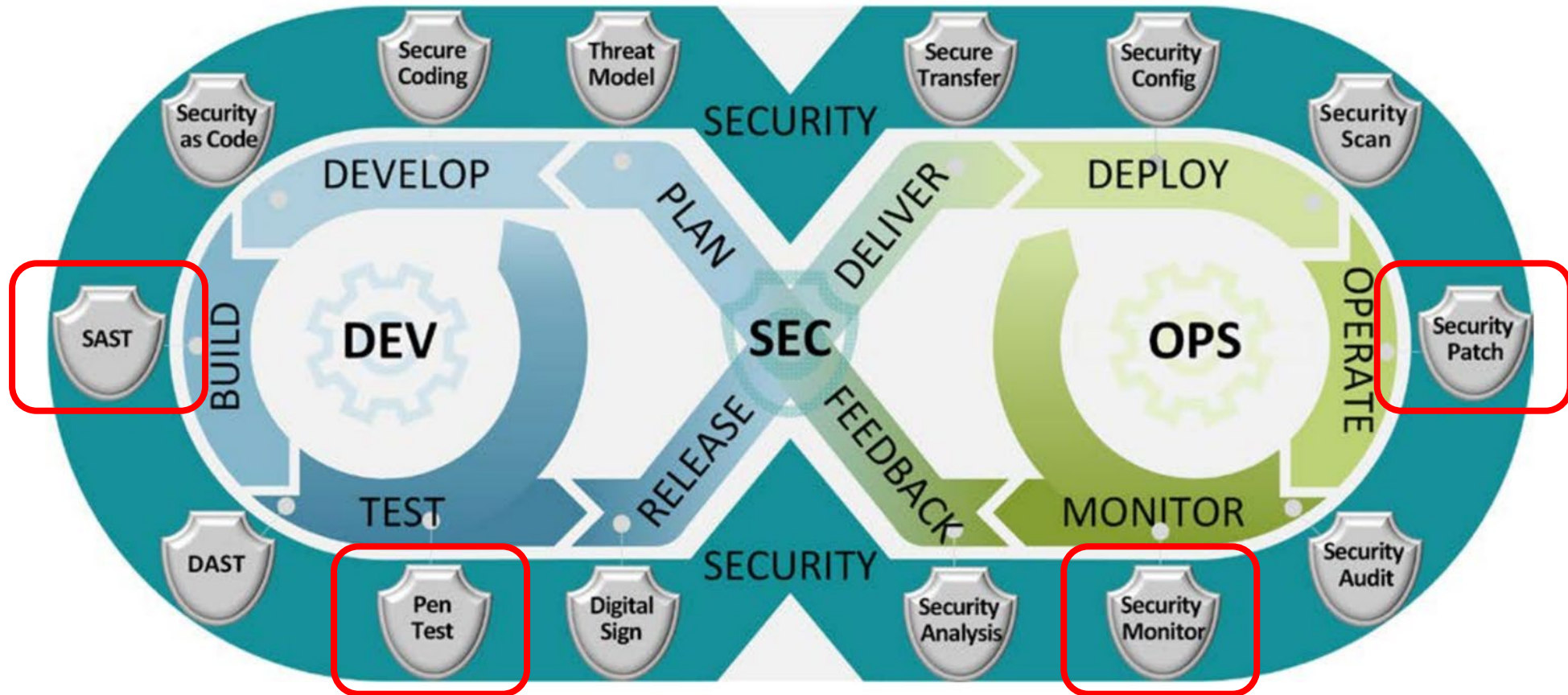
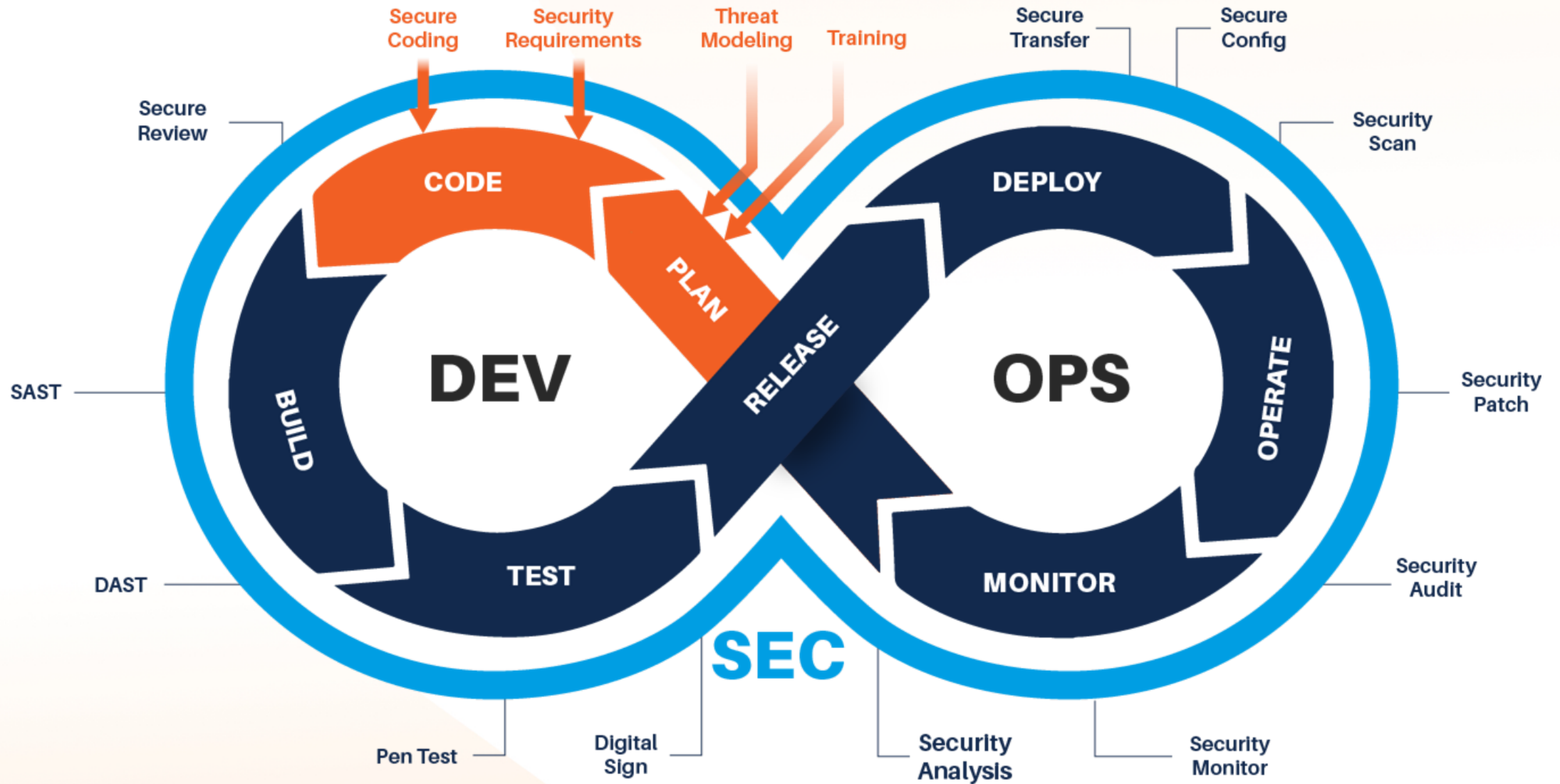


Figure 3: DevSecOps Software Lifecycle

Design Stages in a DevSecOps Lifecycle



What Is Driving DevSecOps By Design?

HIGH PRIORITY for US Fed

Expansion of mandated or recommended security and compliance best practices

50%

Federal Agencies surveyed indicate shifting left is a Top 3 priority

Source: 2023 Federal DoD Perspectives on Application Security (Golfdale / Security Compass)

CUSTOMER DEMAND

Very time consuming to fix security vulnerabilities discovered later in the SDLC

149 DAYS

to fix critical issues

Source: AppSec Stats Flash Report (NTT Security)

TIME & MONEY

Increasingly customers and regulators are demanding secure software practices.

\$4.35M
(\$9.4M US)

Global average total cost of data breach

IBM Data Breach Report 2022

What's Preventing Adoption of DevSecOps by Design?

MANUAL WORK

Developers are struggling to keep up with security and compliance requirements

42%

staying up to date

SCALING CHALLENGES

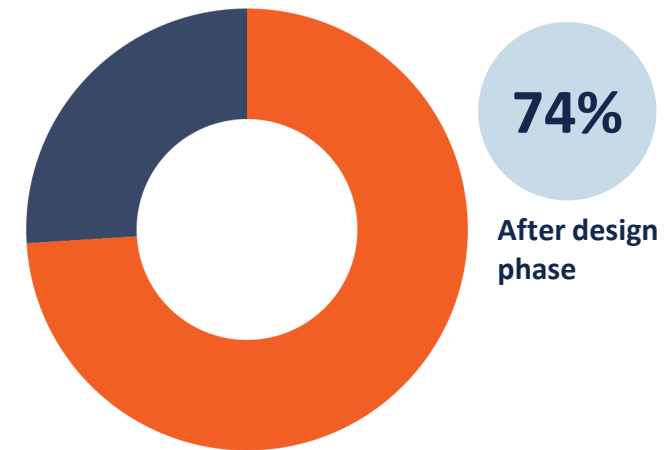
There aren't enough experts to scale application security activities.

1:100

AppSec to Developer Ratio

COLLABORATION CHALLENGES

74% of developers first engage with security after the design phase



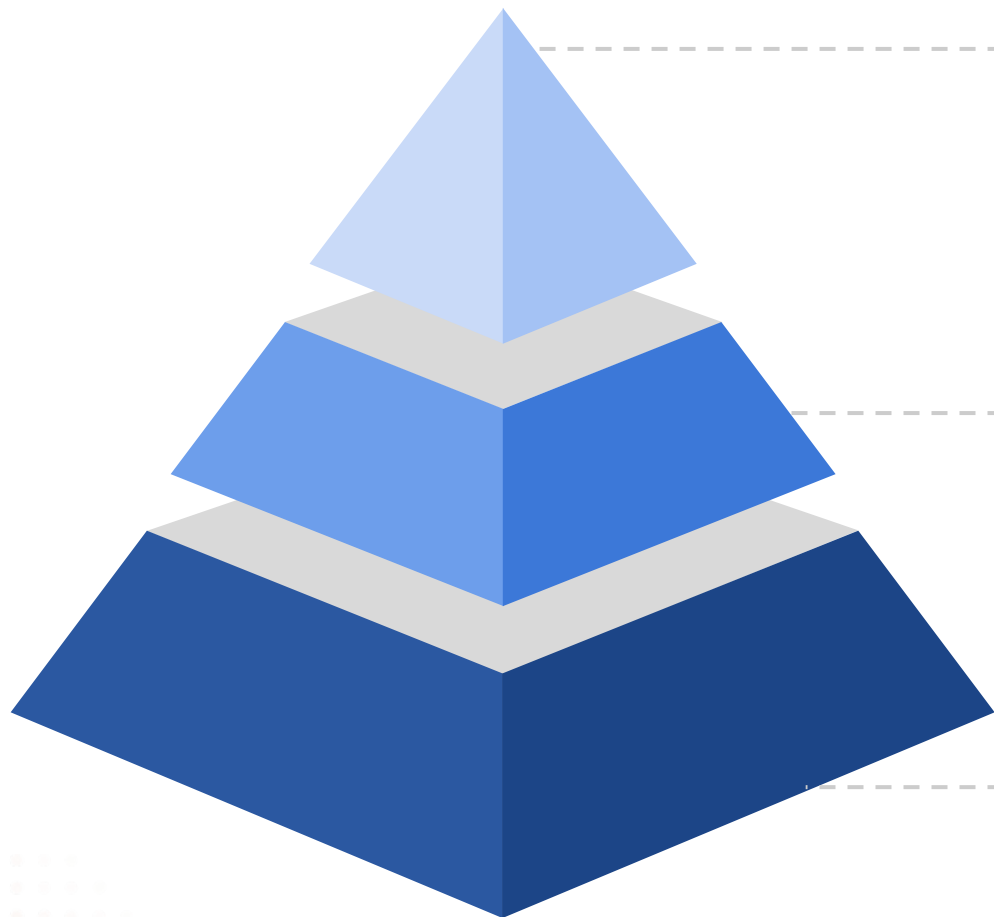
Source: 2022 Developer Perspectives on Application Security (Golfdale / Security Compass)

Source: Stop Checking Boxes And Start Effectively Securing Development Pipelines (Forbes)

Sources: 2021 State of Threat Modeling, 2022 Developer Perspectives on Application Security (Golfdale / Security Compass)

A '**DevSecOps by Design**' culture with executive support, motivated teams and a phased adoption can overcome these challenges

Three Step Framework for Security by Design



③ **EMPOWER**

Implement security requirements, threat modeling, and personalized training to realize Security by Design

② **EMBED**

Cultivate depth of security knowledge through coaching, to advocate for a Security by Design culture

① **EDUCATE**

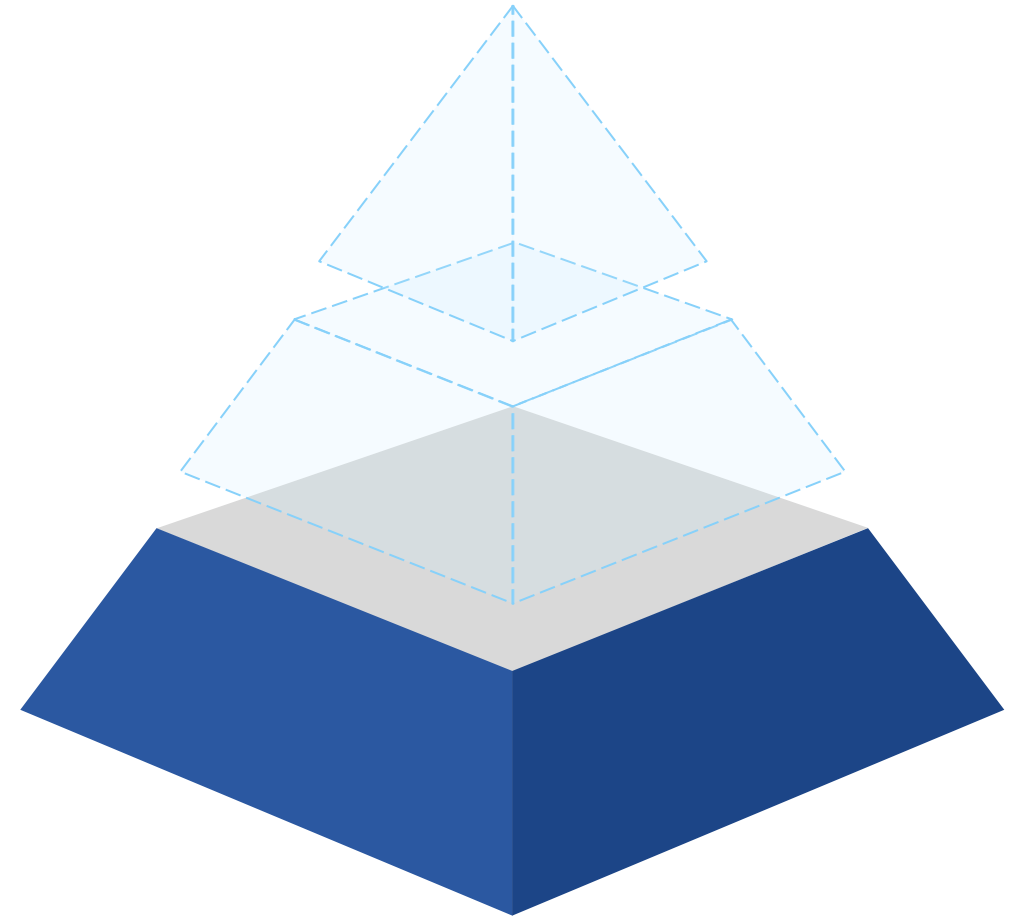
Provide foundational role-specific security awareness training for development teams



EDUCATE

Provide foundational knowledge with **Application Security Training**

- ▶ In this step, organizations lay the foundation for security by design by raising awareness of security in software development teams.
- ▶ With a foundation of basic awareness, development teams will be ready to tackle more advanced security concepts, and become ready to embrace process change necessary for security-by-design
- ▶ Key outcomes:
 - **Risk reduction through developer education**
 - **Increased security awareness**



Example Course Modules to Secure and Defend Against Costly and Damaging Vulnerabilities

Fundamentals



Secure Design
Coding
Testing

Secure Coding

Defending Web APIs



Secure Mobile

Mobile Security Fundamentals

iOS



Operational Security

OpSec, DevSecOps, Defending Databases,
Defending Containers



Compliance

Privacy Fundamentals,
CCPA
HIPAA
GDPR
PCI-DSS
PCI Secure Software Lifecycle
PCI SSF

General Awareness

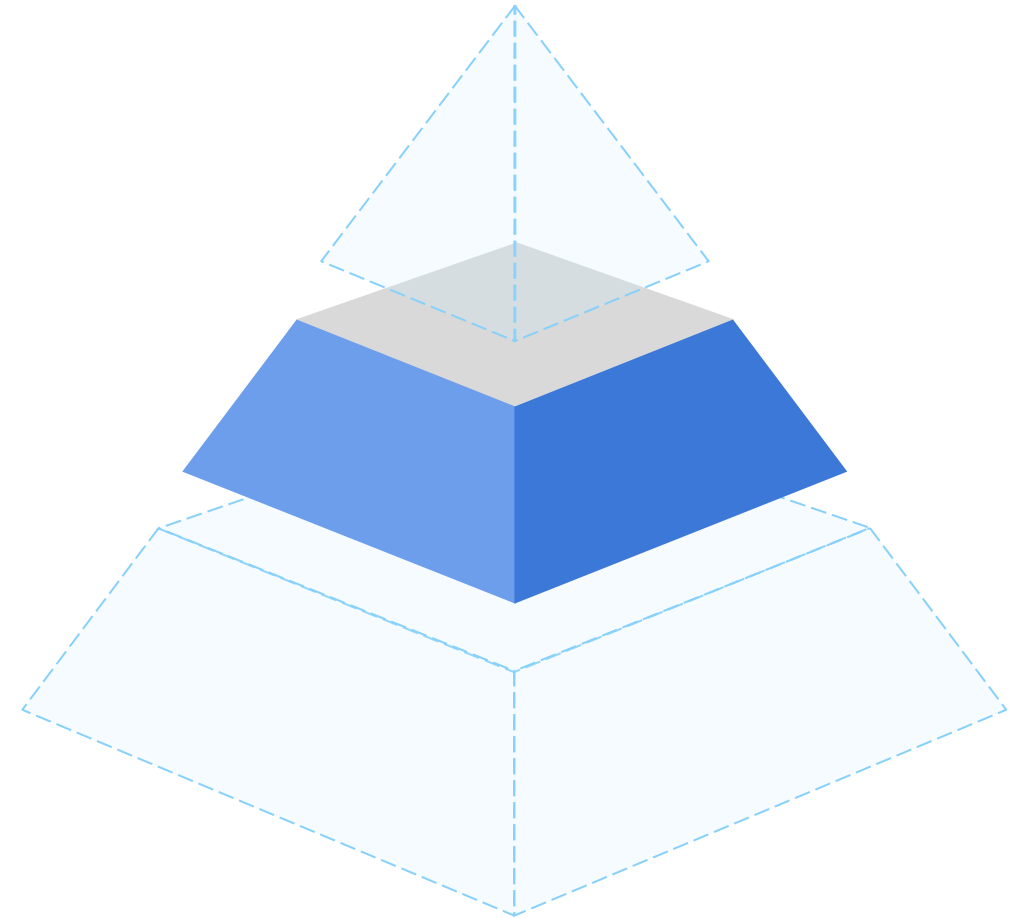
Security Awareness
DevSecOps for Managers
+ new courses planned.



EMBED

Support Implementation and Process change with Security Champions or Coaches

- Begin change management process for embracing more comprehensive security by design
- Assign champions on scrum teams for advanced training and best practices
- Allow AppSec team to focus on policy, critical monitoring, opportunities to scale
- Start small - Setup a few teams to iterate until it's effective before rolling out across departments
- Leverage vendors (ie. expertise, service & support plans etc.)

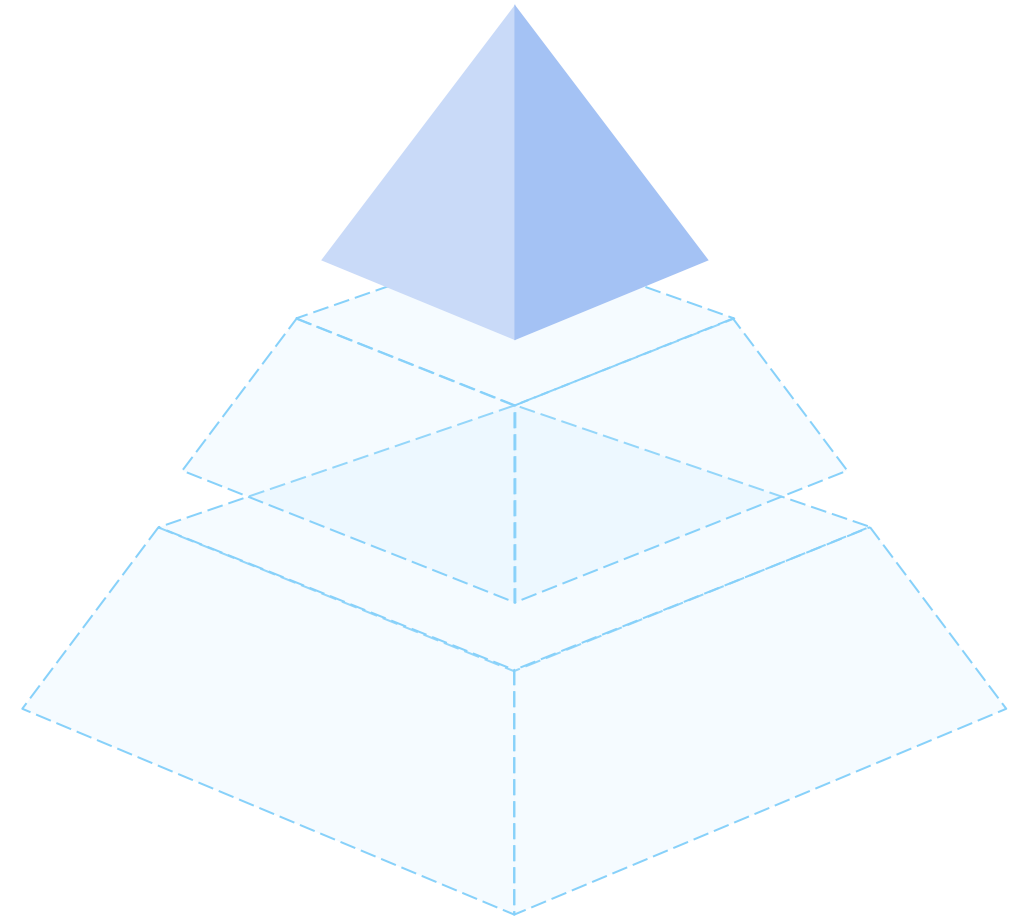




EMPOWER

Allow Development and DevOps teams to be Self-Serving with **Automated, Developer-Centric processes** to scale a secure-by-design approach

- ▶ Automate security by design through Developer Centric tools and processes to reduce disruption
 - API's & SDKs are great (if you have the time)
 - Personalized Just-In-Time Training and Hands-On learning
 - Start small (critical items only) to reduce burden
- ▶ Key outcomes:
 - Faster time to market for secure software
 - Lower risk from software
 - Security-by-design fully integrated into existing development processes



Case Study

MEET OUR SOFTWARE SOLUTIONS COMPANY

215

APPLICATIONS
APPLICATIONS
APPLICATIONS

1 → 250 

APPSEC
EXPERT
TO DEVELOPER



REQUIREMENTS

- OWASP SAMM
- FEDRAMP
- NIST
- PCI-DSS
- HIPAA
- CJIS
(CRIMINAL JUSTICE
INFORMATION SYSTEMS)
- CMMC

BEFORE



Meetings &
Spreadsheets

[Hours]



Manual
Analysis

[Days to weeks]



Security Control
Implementation

[Days to weeks]



Often not
in Scope

What Are We
Working On?



What Could
Go Wrong?



What Do We Do
About It?



Did We Do A
Good Job?

SECURITY BY DESIGN



EMPOWER

Implement security requirements, threat modeling, and just in time training to realize Security by Design



EMBED

Cultivate depth of security knowledge to advocate for a Security by Design culture



EDUCATE

Provide foundational role-specific security awareness training for development teams



EDUCATE

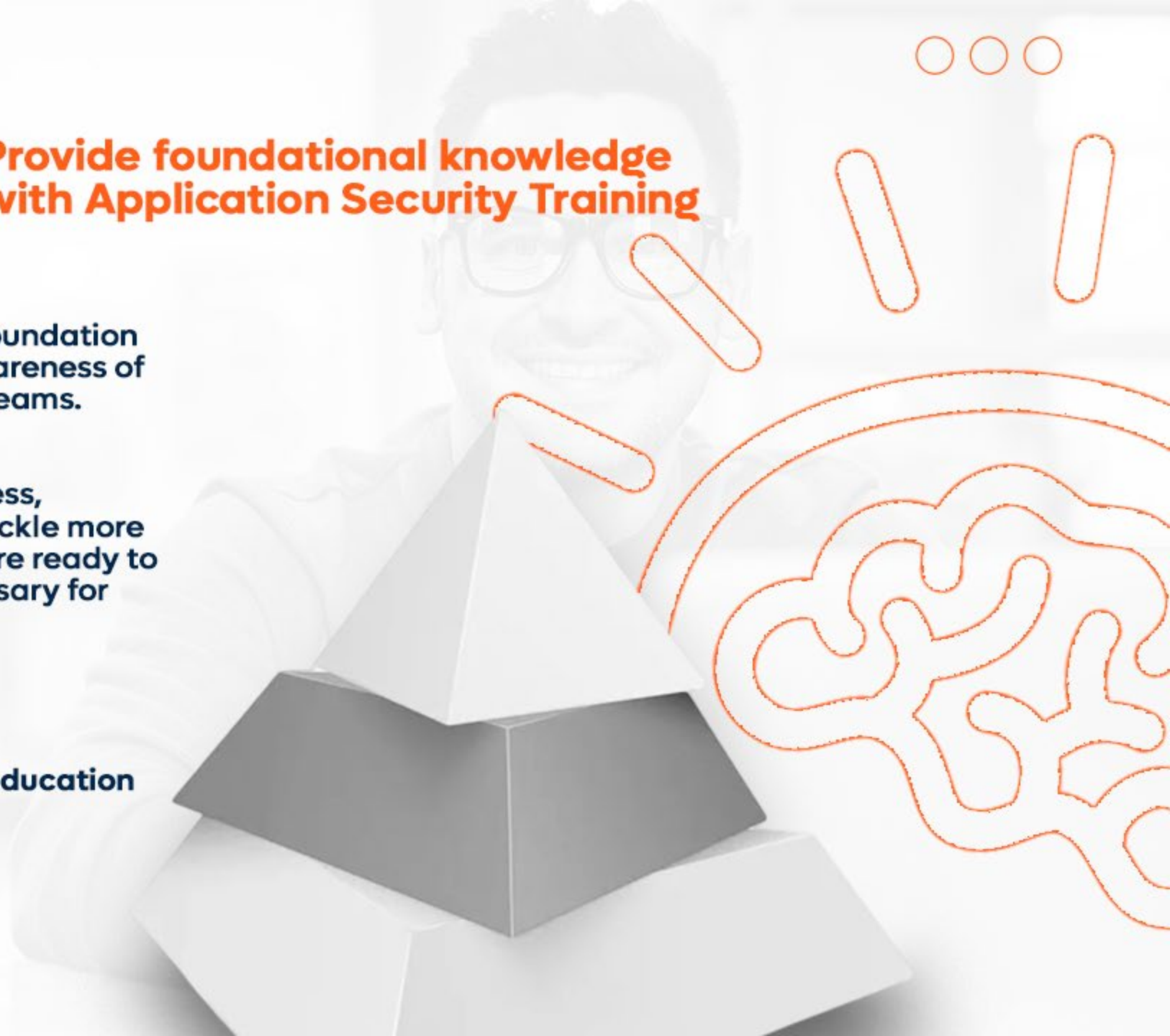
**Provide foundational knowledge
with Application Security Training**

In this step, our customer laid the foundation for security by design by raising awareness of security in software development teams.

With a foundation of basic awareness, development teams are ready to tackle more advanced security concepts, and are ready to embrace the process change necessary for security-by-design

Key outcomes:

- Risk reduction through developer education
- Increased security awareness



- ▶ Transition from basic developer security awareness to fostering security expertise with breadth & depth of training
- ▶ Incorporate basic program design and workflow for adopting Developer Centric Threat Modeling
- ▶ Begin change management process for embracing more comprehensive security by design

Key outcomes:

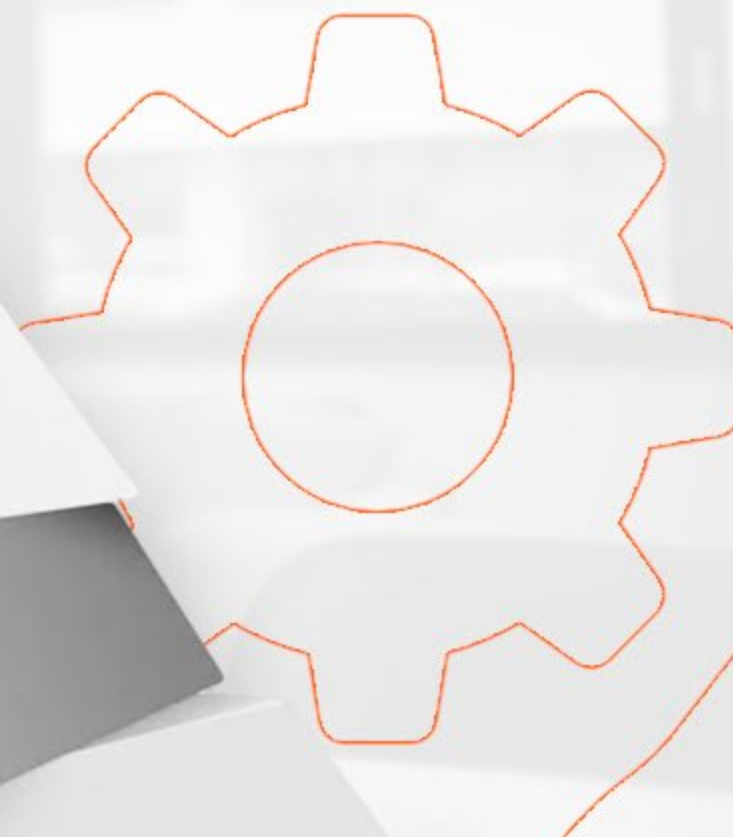
- Increased security expertise in development teams, reduce burden on central security teams
- Visibility of current state risk and cost metrics and quantified goals for security-by-design program
- Increase chances of success of adopting security by design by beginning a change management process



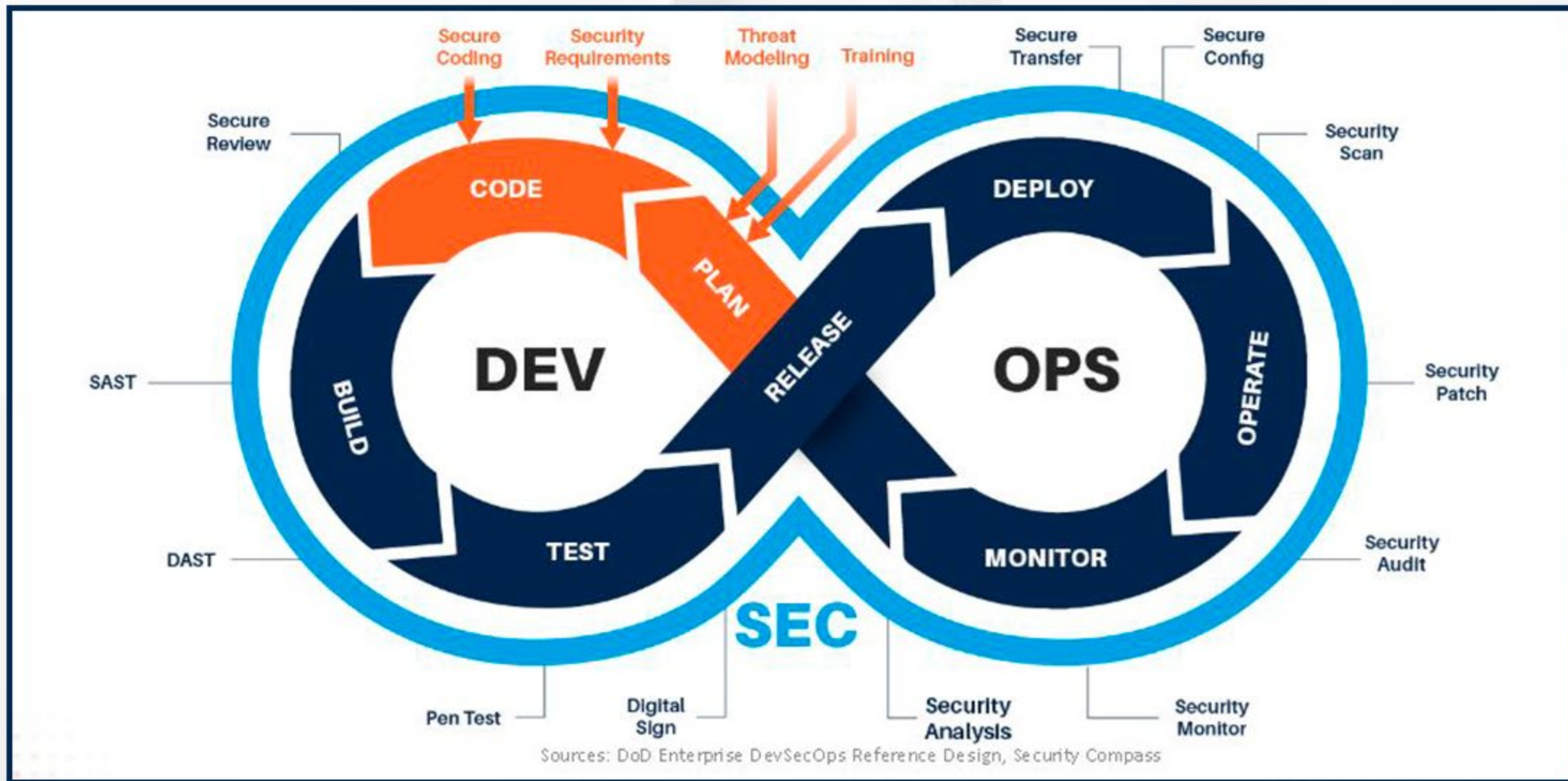
EMPOWER

Implement a Developer-Centric
Threat Modeling Solution to complete
secure-by-design approach

- ▶ Fully embrace security by design through Developer Centric Threat Modeling
- ▶ **Key outcomes:**
 - Faster time to market for secure software
 - Lower risk from software
 - Security-by-design fully integrated into existing development processes



AFTER



Your developers

are not security or compliance experts... and you can't expect them to be.



**But with the right tools and
processes you can protect your
brand and deliver secure
products faster than you ever
thought possible!**

PROTECT
PROTECT
PROTECT

Thank You

For more information, contact us at www.securitycompass.com

SecurityCompass