# DevSecOps

## Understanding Our Eight Step Process

TROLLEYE SECURITY

# Table of Content



# Overview

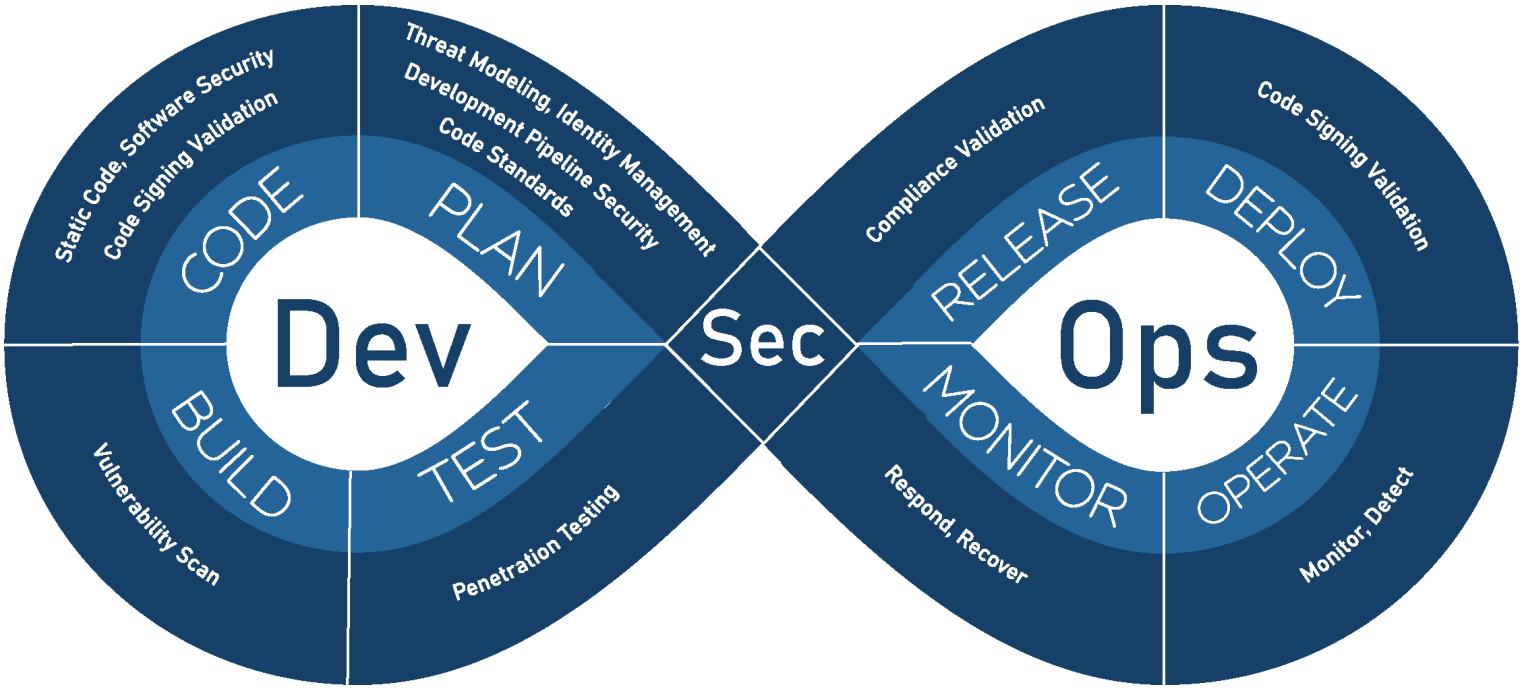
Organizations grapple with relentless cybersecurity threats every day, many of them coming from vulnerabilities that could have easily been remediated in the development process. To combat them organizations can use DevSecOps to seamlessly integrate security into the development process to fortify code and protect it against cybercriminals.

We have prepared this white paper so you can better understand the process of DevSecOps, and how our organization can help you secure your software development process.

TROLLEYE SECURITY

# The Process of DevSecOps

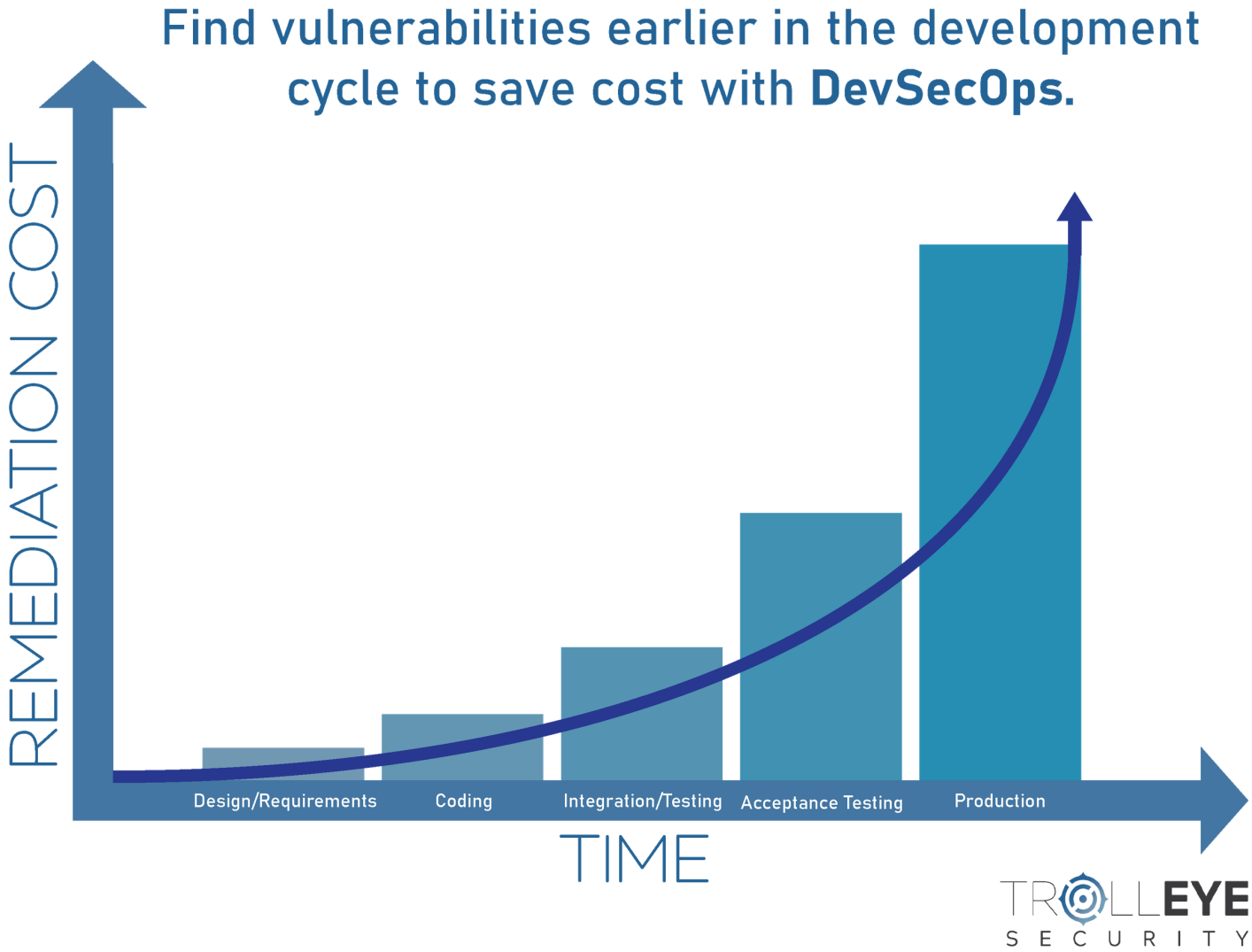
DevSecOps represents the seamless integration of security measures into the software development process, ensuring that security considerations are embedded from the outset and throughout the entire development lifecycle. This methodology is supported by the use of specialized tooling and automation, which underpins a continuous and iterative improvement approach to security practices within development and operational workflows.




DevSecOps is an expansion of the DevOps model, integrating security into the entire development process.

# The Effect of DevSecOps

According to IBM's 2023 Data Breach Report, organizations that experienced a data breach with high levels of DevSecOps adoption saved an average of $1.68 million, compared to those who didn't



# Step 1: Plan

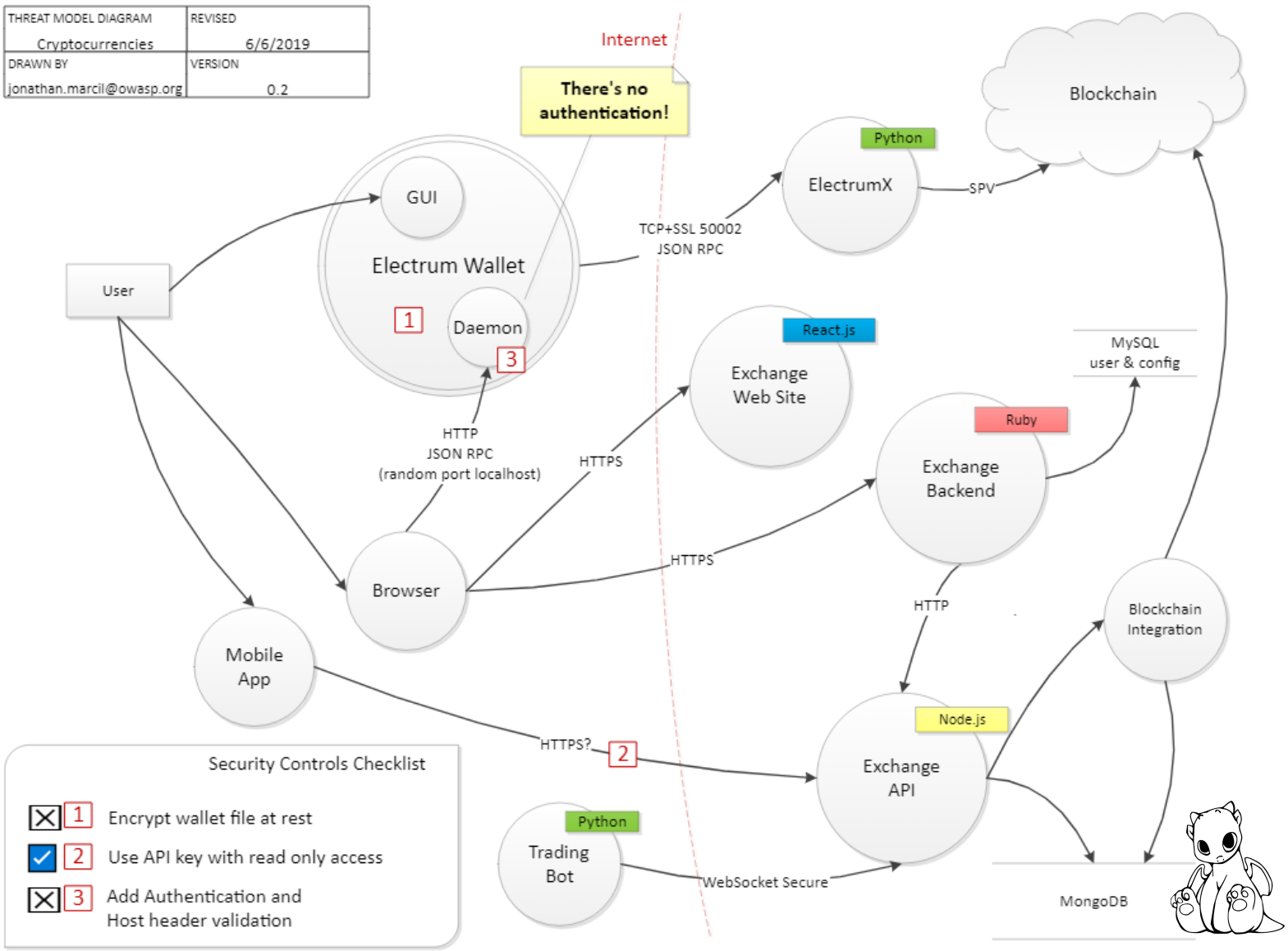
The initial step in our DevSecOps process is the Plan phase. Here, we meticulously lay the groundwork for a secure and robust development process. This phase encompasses several critical components: threat modeling, code standards, identity management, and development pipeline security.

- Threat Modeling: Before a single line of code is written, we invest time in thoroughly understanding potential threats and vulnerabilities. Our experts identify and evaluate potential risks to your application, ensuring that security is a fundamental consideration from the project's inception. One model we use is the OSWAP Threat Dragon.

- Code Standards: Code standards are the guiding principles and rules that govern how software is written. These standards encompass a set of best practices, conventions, and security measures that developers adhere to when crafting code. They serve as a blueprint, ensuring that every line of code is constructed with security, quality, and consistency in mind.

# Threat Modeling Process

The Threat Modeling process shown below is an example of the OSWAP Threat Dragon.




TROLLEYE SECURITY

# Step 1: Plan (Continued)

- Identity Management: Identity Management refers to a framework of policies and technologies ensuring that the right individuals have the appropriate access to technology resources. IdM systems manage user information, including authentication and authorization levels, to safeguard data and systems by verifying user identities and controlling access to resources within the development pipeline.

- Development Pipeline Security: Development Pipeline Security is a set of practices and tools designed to protect the software delivery process by integrating security measures directly into the development pipeline. This encompasses the entire cycle from code commit to deployment, ensuring that security checks, compliance rules, and vulnerability assessments are an intrinsic part of the continuous integration and continuous delivery (CI/CD) processes.

# Step 2: Code

The "Code" phase of the DevSecOps process represents a pivotal stage where security is deeply integrated into the development workflow. This phase is divided into three critical components: Software Security, Static Application Security Testing, and Code Signing.

- Software Security: Software Security, which includes Software Composition Analysis, is the practice of ensuring that applications are designed, developed, and maintained to protect against vulnerabilities and threats throughout their lifecycle. It encompasses a range of activities from coding and design to configuration and patch management, aimed at minimizing the risk of unauthorized access and manipulation.
- Static Application Security Testing: SAST is a vital practice for reinforcing code security right from the outset of the development process. SAST represents a proactive approach to identifying and mitigating security vulnerabilities before they manifest into critical issues.
- Code Signing Validation: Code Signing Validation is a security measure that verifies the authenticity and integrity of software by confirming that the code has been digitally signed by a legitimate source.

TROLLEYE SECURITY

# Step 3: Build

In the Build phase of the DevSecOps process, vulnerability scanning takes center stage. This critical step involves the systematic assessment of the software codebase and its dependencies to uncover any known security vulnerabilities, weaknesses, or compliance issues.

Dynamic Application Security Testing: DAST, plays a vital role in ensuring the security and resilience of our software applications. DAST is a dynamic testing method that involves evaluating an application while it's running.

TROLLEYE SECURITY

# Step 4: Test

We take the critical testing phase in the DevSecOps pipeline to a new level with our Penetration Testing as a Service (PTaaS) offering. Leveraging heavily automated weekly testing, PTaaS integrates seamlessly into the development lifecycle, ensuring that every application is scrutinized for vulnerabilities. This continuous and automated approach not only aligns with agile methodologies but also elevates security testing to a proactive and preventive measure rather than a reactive one.

TROLLEYE SECURITY

# Step 5: Release

In the Release phase of the DevSecOps process, organizations move forward with the utmost confidence in their application's compliance with stringent regulations such as PCI-DSS, GDPR, and CCPA. By embracing a DevSecOps approach, organizations can confidently release their applications, knowing that they have proactively addressed compliance concerns, minimized risks, and upheld the highest standards of data security and integrity.

With the recent release of PCI-DSS 4.0, it is important for organizations to implement DevSecOps to ensure compliance with these regulatory standards. These new standards:

- Place a greater emphasis on security as a continuous process.
- Introduce new requirements for software security and vulnerability management.
- Require additional focus on supply chain security.
- Include new requirements to protect against attacks exploiting software vulnerabilities.

TROLLEYE SECURITY

# Step 6: Deploy

Within the deployment phase of the DevSecOps process, organizations prioritize code signing validation as a crucial step to fortify the integrity and security of their software deployments. Code signing serves as a digital seal of authenticity, ensuring that the deployed code has not been tampered with or compromised.

By rigorously validating these signatures during the deployment process, organizations can mitigate the risks associated with compromised or altered code, ensuring that only trusted and unaltered applications are delivered to end-users. This practice not only bolsters the integrity of software deployments but also enhances user trust, as they can confidently engage with applications knowing they are free from malicious modifications.

TROLLEYE SECURITY

# Step 7: Operate

In the operation phase of the DevSecOps process, the focus shifts to continuous monitoring and vigilant detection of security threats. This phase involves the implementation of robust monitoring systems and security controls to actively scrutinize the environment for any signs of suspicious activities, vulnerabilities, or anomalies.

In this phase we employ a multifaceted approach to continuous monitoring and vigilant threat detection, leveraging an array of sophisticated tools along with several of our other services:

- WAF
- RASP
- IPS with SSL Decryption
- EDR
- SIEM / Managed SIEM / Open XDR
- SOAR
- Attack Simulation / Purple Teaming
- Dark Web Analysis

TROLLEYE SECURITY

# Step 8: Monitor

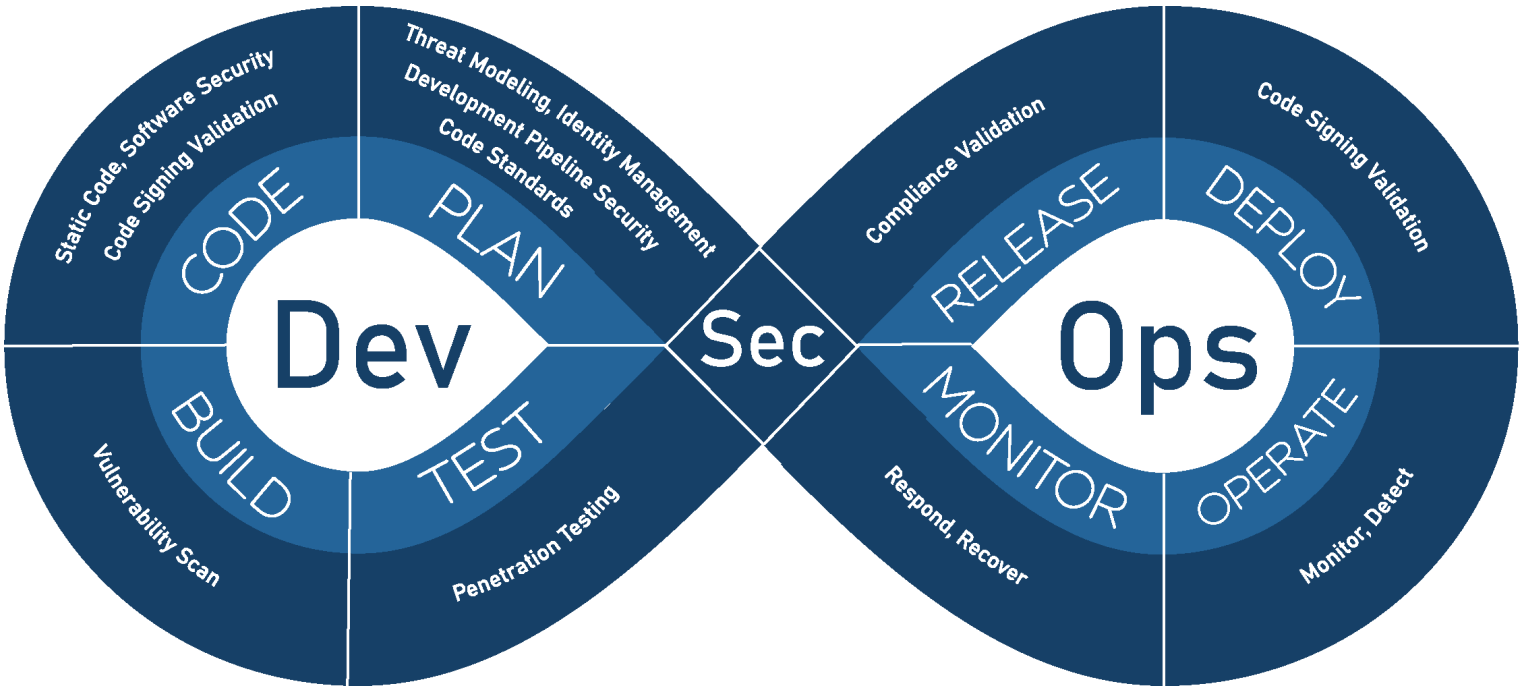
In the final phase of the DevSecOps process, the focus is on continuous monitoring, swift response, and effective recovery in the event of a security incident. This phase is instrumental in ensuring that an organization's security posture remains robust and resilient.

At TrollEye Security we use our Managed SIEM (Purple Teaming) service to monitor your systems, and if an incident happens we call in our First Responders Team.

TROLLEYE SECURITY

# What to Expect.

When you use TrollEye Security for DevSecOps, we will take care of the security aspect outlined in the dark blue, while in most scenarios you will be responsible for the DevOps part of the equation. However, if you do not have a DevOps team, we will happily take on that role too. We strongly encourage you to reach out to us today for a demo and quote, so you can start securing your software today.




Secure Your Software Development Cycle Today!

# Find Out How We Can Help Your Organization

## Schedule a Free Demo Today

(833) 901-0971

trolleyesecurity.com/contact/

TROLLEYE SECURITY