TRAINING

MWR CYBERSEC

Proactive DevSecOps Defence

A three-day training course in Proactive DevSecOps Defence.

PDD is an exercise-driven training course that will guide you through common attack vectors affecting the entire chain of a development pipeline, from code development through to deployment. The purpose being to provide a practical understanding of attacks against these environments, and most importantly the defensive controls required to mitigate them. Through the exercises and discussions held throughout the course, candidates will develop a holistic view of the security model needed to ensure the integrity of all code changes that get deployed. Participants will thus be equipped to create and maintain secure and robust development pipelines.

Who should attend?

The course is orientated around critical phases or activities within the broader Software Development Lifecycle (SDLC); where a lack of security controls could result in opportunities for attackers to affect the integrity of the software project and the dependent business as a whole. It is also aimed at developers and operations teams alike as they are typically involved in the the development, maintenance and deployment of any software project, and the risks posed to the project as a whole span the responsibilities of these teams. The course covers a holistic view of the greater development pipeline, from code changes to release; so anyone involved in the execution, planning and maintenance of such a pipeline would benefit. DevOps engineers would benefit the most from the course as the entire course content would be directly applicable to their role. Content presented is at an intermediate level and would require the candidates to have basic knowledge of Unix systems, and typical development practices. General familiarity is necessary for the concepts of source code management, managing dependency repositories, and configuring build and deployment pipelines.

Course highlights

- ✓ You'll gain an understanding of the risks and attacks affecting software development projects, from code change to deployment.
- ✓ You'll learn how to attack vulnerable development environments by exploiting common misconfigurations, in order to understand them better.
- ✓ You'll learn how following security best practices and using secure configurations can be effectively used to ensure the integrity and accountability of all code changes being deployed.
- ✓ You'll gain an understanding of how to reason about security of the software pipeline, in order to better influence the security of your current and future software development pipelines.

Benefits to your organization

- ✓ An understanding of the necessary technical controls and processes needed to ensure the integrity and accountability for all code changes that get deployed.
- ✓ Tools to improve the general resilience of your software projects against attacks.
- ✓ Understandings of the attack surface and avenues available to compromise critical components within your software-related processes.
- ✓ Promotion of a positive attitude and an understanding of the importance of security.
- ✓ Actionable advice that can be implemented to make direct improvements on a policy level, so that security policies can be informed by the realities of business pressures on software development.
- ✓ A framework that allows evaluation of the evolving needs of your business against models of security best practice, allowing for self-driven, continuous improvement.

How is this course different?

This is a **practical, exercise driven course,** consisting of a number of common configurations of development pipelines for you to attack. The course is **delivered by experienced security professionals**, who have experience performing many of the attacks incorporated into the exercises.

The course **focuses on key security controls** that span across the entire Software Development lifecycle: from code change to deployment. **Focus is placed on teaching offensive security techniques** by providing participants with practical exercises that allow them to exploit weaknesses to achieve a particular goal.

By orientating the course around the attacker mindset, participants are able to **see these environments through the lens of an attacker.** This approach allows us to **tangibly teach you the risks,** so that it becomes evident “why“ and ”how” to protect the pipeline against these threats. With an understanding of the requirements needed to perform an attack, the context needed to enforce effective security controls will allow participants to **proactively secure their environments.**

Topics / Syllabus

Foundation

- Software Development Lifecycle and Models
- Evolution of software development
- Real world compromise examples

Defending the pipeline

- Shifting security left
- Size, scale and complexity of security requirements
- Attack surface and security principles

Development

- The code repository
- Workstation compromise
- Code repository security controls

Dependency Management

- Internal dependencies
- External dependencies

Building and Deployment

- Build technology
- Automatic build triggers
- Secret management
- Shared build infrastructure
- Deployment

Case Study: Pipeline Comparison

- Gitlab pipeline exploitation
- Pipeline Comparison: comparing weak controls, to the ideal environment

For more information visit www.mwrcybersec.com or email us on info@mwrcybersec.com