mind Hacking Point

CHECK POINT

DevSecOps

2 day class

Specialist training

Keep up with DevOps modernization and widen your career prospects. This practical 2-day course will help you build your own DevSecOps pipeline so you can make products secure by design. Get your hands dirty with our popular virtual labs and learn from experienced, practicing penetration testers with a legacy of training at Black Hat. Learn how to use and automate the most popular and effective security tools and practices, overcome common DevSecOps challenges, instil security culture within your team, and more...

Who it's for

- Developers
- DevOps/DevSecOps engineers
- Application security engineers
- Ops teams
- CISOs

This course is suitable for organizations and teams with a DevOps pipeline already in place, as well as those planning to implement one. The syllabus has been designed to help different key stakeholders improve their skills and knowledge across different security practices and embed "security by design" as the way of working. Putting these learnings to use will lead to improvements in the overall security posture of your applications over time.

Top 3 takeaways

- Hands-on experience with DevSecOps tools to help you learn what they do and how to use them
- Working knowledge of how to implement these security tools and other practices in your DevOps pipeline
- An offline lab setup, which you can replicate on your own computer to create and practice in the same environment in your own time (we will provide a folder and instructions for setup on Linux/MAX or Windows)

What you'll learn

This course uses a Defense by Offence methodology based on real world offensive research (not theory). That means everything we teach has been tried and tested, either on a live environment or in our labs, and can be applied (by you) once the course is over. By the end of the course, you'll know:

- How cyber criminals and penetration testers exploit insecure DevOps practices
- Exactly where to start when shifting from DevOps to DevSecOps
- How to use Talisman to create pre-commit hooks to lower the chance of credentials and other secrets being exposed during development
- How to automate security into a fast-paced DevOps environment using various opensource tools and scripts that don't slow down delivery
- How to secure your methodology for managing and delivering Infrastructure as Code (IaC)
- How to use the Elastic (ELK) Stack to monitor your applications' behaviors with logs and alerts
- How to achieve DevSecOps in cloud native AWS
- What challenges to expect when moving to a DevSecOps model and how to overcome them
- How to mature your DevSecOps approach over time

Why it's relevant

This course was met with an incredible response when we delivered it at OWASP's 2022 AppSec Days Developer

NotSoSecure part of claranet cyber security

Security Summit. Despite growing awareness around the need to shift security left, speed of development is still taking precedent over risk in many organizations, leaving security behind with every deploy. Moving from DevOps to DevSecOps without slowing down is a real challenge. You need to know which tools to use, what processes to put in place and how to govern them, and how change the culture of development at the people level. Maybe most importantly, you need to know where to start.

Our DevSecOps course syllabus responds to that challenge by:

- Covering the most recognized (and effective) DevSecOps tools, so you can put them into practice
- Showing you how you to maintain automation and speed without compromising security
- Addressing the challenges that teams often come up against, so you can prepare to do the same
- Tackling DevSecOps in the cloud to help you adapt your approach for different environments
- Acknowledging and responding to the security skills gap that exists in most development teams
- Covering everything that DevSecOps stakeholders need to know (not just the development aspect)

What you'll be doing

Our interactive course format enables you to get hands on throughout the session, including:

- Running different tools and testing them against realistic use cases in your own dedicated lab
- Automating code reviews to check software for vulnerabilities
- Modelling a Secure by Design environment module by module
- Discussing how to embed the human and cultural aspects of DevSecOps

What's in the syllabus

Note: our syllabuses are subject to change based on new vulnerabilities found and exploits released.

LAB SETUP
- Online lab setup
- Offline lab instructions

INTRODUCTION TO DEVOPS
- What is DevOps?
- Lab: creating a DevOps pipeline

INTRODUCTION TO DEVSECOPS
- Security challenges in DevOps
- Threat modelling for DevOps
- DevSecOps – why you need it, how you use it, and what it is
- Vulnerability management

CONTINUOUS INTEGRATION
- Pre-commit hooks
- Introduction to Talisman
- Lab: Running Talisman
- Lab: Create your own regexes for Talisman
- Secrets management
- Introduction to HashiCorp Vault
- Demo: Vault commands

CONTINUOUS DELIVERY
- Software Composition Analysis (SCA)
- Introduction to OWASP Dependency-Check
- Lab: Run OWASP Dependency-Check pipeline
- Lab: Fix issues reported by Dependency-Check
- Static Analysis Security Testing (SAST)
- Introduction to Semgrep
- Lab: Run Semgrep pipeline
- Lab: Create your own Semgrep rules
- Lab: Fix issues reported by Semgrep
- Dynamic Analysis Security Testing (DAST)
- Introduction to OWASP ZAP
- Demo: Creating OWASP ZAP Context File
- Lab: Run OWASP ZAP in pipeline

INFRASTRUCTURE AS CODE
- Vulnerability Assessment (VA)

- Introduction to OpenVAS
- Lab: Run OpenVAS pipeline
- Container Security (CS)
- Introduction to Trivy
- Lab: Run Trivy in Pipeline
- Lab: Improvise Docker base image
- Compliance as Code (CaC)
- Introduction to Chef Inspec
- Lab: Run Chef Inspec in pipeline
- Lab: Improvise with Docker compliancy controls

CONTINUOUS MONITORING

- Logging – why to do it, how, and what logs to collect.
- Introduction to the ELK Stack
- Lab: View Logs in Kibana
- Alerting – how to create alerts that help you prioritize
- Introduction to ElastAlert and ModSecurity
- Lab: View alerts in Kibana
- Monitoring – how to track and learn from malicious activity
- Lab: Create Attack Dashboards in Kibana

DEVSECOPS IN AWS

- What does DevOps on Cloud Native AWS look like?
- AWS threat landscape
- Shifting to DevSecOps in Cloud Native AWS

DEVSECOPS CHALLENGES AND ENABLERS

- Challenges with DevSecOps
- How to build a DevSecOps culture
- Security champions – how to create DevSecOps advocates across your team
- Case study: how organizations use automation to implement development security best practice
- Where to begin
- DevSecOps maturity model

What you'll get

- Certificate of completion
- Your own offline lab setup to use after the course
- 8 Continuing Professional Education (CPE) credits awarded per day of training fulfilled
- Learning pack: question & answer sheets, setup documents, and command cheat sheets

Course highlights

What delegates love:

- Offensive angle: you'll learn from practicing penetration testers and red teamers with working knowledge of the latest and most common software hacks
- Browser based: the course has no software dependency and requires no installations, making it fast to get set up and easier to get security clearance (all you need is internet access and a GitHub account)
- Multiple mitigations: for every vulnerability covered, you'll explore 3 to 4 remediations, helping you develop a versatile approach
- Technology focus: almost two full days spent testing the industry's preferred DevSecOps tools, for free
- Real-world learning: in an industry where most of the leading cybersecurity training courses are based on theory, our scenario-led, research-based approach ensures you learn how real threat actors think and act.

Outcomes for budget holders

This course is designed to develop web application security testing competency within your organization, helping you:

- Increase the frequency and consistency of secure (vulnerability-free) software releases
- Lower the cost of remediation by identifying vulnerabilities before software is deployed
- Manage the likelihood and impact of security incidents originating from insecure code and development practices
- Identify security issues that need dedicated, in-depth security testing (e.g., business logic issues) to validate the risk they pose and recommend remediation measures
- Develop the organization's competitive advantage for security-conscious customers
- Test the effectiveness of tools before committing to investment
- Nurture and retain passionate, highly skilled, and security conscious employees
- Demonstrate commitment to security through training and change management

NotSoSecure part of claranet cyber security