Checkmarx Business Partner Training

Advanced Certified Engineer

CxSAST Architecture and Installation

CxSAST Setup and Configuration

Threat Modelling and Onboarding

CxQL Training and Workshop

Amot Atrium Tower, 2 Jabotinsky St, Ramat Gan 5250501, Israel | Tel: +972-3-7581800 | Fax: +972-3-7581812 | contact@checkmarx.com | www.checkmarx.com

Prerequisites

1. Participants need their laptops with an an RDP client is installed (this is a default for Windows, but not for Linux and OS/X)
2. The timetable is 9:30AM to 5:30PM Monday to Thursday with 1 hour for lunch each day.

[Day 1]

Module	Duration	Content	Goals
Checkmarx Overview	1 hours	• Static code analysis state in IT. What is the general approach, history, what companies offering products in this area, etc • A little bit about Checkmarx. Who we are, where we have offices • What do we offer as a product, CxSAST, OSA, IAST, Code Bashing, CxARM • Small discussion with group to enable conversation – if anyone has any experience with SAST, ever tried to integrate it – know your audience should come first.	• Learn about the latest in Checkmarx products • Understand the benefits of SAST
SDLC Integration	2 hours	• SDLC stages overview, cost of fixing security bugs • Open discussion on where people see Security and SAST place in SDLC (planning, requirements, implementation, testing) • CxSAST architecture overview (components, DB, portal, IDE plugins, CLI, CI plugins). Types of installations • Hands on session to install Checkmarx, small talks – Why? • Checkmarx SDLC Integration overview (CI, branches scanning, merges, results processing) • Open discussion on results review, FPs, development reluctance to the tool, ways to solve it • Onboarding process overview	• Understand CxSAST in the SDLC • Learn about CxSAST architectureand installation • Know where to find information on integrations and understand the advantages for the SDLC
Lunch Break	1 hour		
Workshop	3 hours	• Practice and discuss result review on a test project • Practice setting up Checkmarx plugs-ins and running a scan	• Get some practice with using Checkmarx plug-ins • Complete the workshop tasks
Q&A	1 hour	• Q&A	• Answer any questions

[Day 2]

Module	Duration	Content	Goals
CxAudit and CxQL	3 hours	• Introduction to CxAudit • False Postivies and False Negatives • Live demo	• Understand how to use CxAudit and CxQL basics • CxQL examples
Lunch Break	1 hour		
Query Customizations	1 hour	• Learn query customizations by looking at the 3-4 most common customizations: ○ Changing the severity of a rule ○ Exposing internal rule (such as Find_Personal_info) ○ Adding a method to sanitizer list	• Get a general idea of common customizations
CxQL Workshop	3 hours	• Hands on exercises on the training machines	• Start the CxQL exercises • Learn the basics of CxQL

[Day 3]

Module	Duration	Content	Goals
Threat Modelling and Onboarding	3 hours	• Threat Modelling Prerequisites, interview and results • Onboading process	• Explain the purpose of TM and Onboarding Understand how this leads to analysis and customizations using CxAudit
Lunch Break	1 hour		
CxQL Workshop (continued)	2 hours	• Complete the exercises on the training machines	• Complete the CxQL exercises
Threat Modeling worked example	2 hours	• Example project to go through Threat Modelling (“Easy Leave”)	• Learn how to do a real Threat Modeling

[Day 4]

Module	Duration	Content	Goals
Onboarding Workshop.	3 hours	Real world example project, looking at reviewing results and doing query modifications	• Learn how to use CxQL in a real project. • Understand onboarding and query customization • Leverage AppSec skills to reduce false-positive and false-negative
Lunch Break			
Onboarding Workshop (continued)	3 hours	• Real world example project, looking at reviewing results and doing query modifications	• Learn how to use CxQL in a real project. • Understand onboarding and query customization • Leverage AppSec skills to reduce false-positive and false-negative
Final Test	1 hour	• Online test based on training content	• Confirm that all candidates are ready for the field

Workshop Details

- ✓ Onboarding an example project (“Easy Leave”)
- ✓ Tune existing Checkmarx queries to specific requirements
- ✓ Discussion on mitigation options for each vulnerability category
- ✓ Review of optimal fix locations for the issues found
- ✓ Add comments for the chosen remediation option
- ✓ Triage and prioritize vulnerabilities
- ✓ Build up a summary report from the workshop