|  |
| --- |
| OpenHack Light – DevSecOps |

# Overview

* The DevSecOps OpenHack Light is a multi-day experience where attendees automate the security best practices to their CI/CD pipeline. This OpenHack simulates a real-world scenario that developers encounter day to day in their jobs wrt security. The content helps them solve the issues to implement Security Best Practices to the workflow and the CI/CD pipeline. "Crackers," who attack the vulnerabilities, validate all challenges by attacking. Attendees can also learn how cracker works to the vulnerabilities. Besides, attendees can learn the case study of security breaches and the threat of cracking by the live demo through the lunchtime presentation. It helps to gain the motivation of causing interest in security incidents for developers.

# Technologies

Azure DevOps, Azure Key Vault, Azure Automation, Microsoft Security Toolkit, Sonar Cloud, Aqua, Fossa, White Source, Azure Kubernetes Service, Azure Container Registry, Azure Active Directory

# Challenges

**Challenge 1: Protect from credential leaks**

* Identify the tools and technologies that you will use to protect from credential leaks
* Identify the tools and technologies that you will use to find SSN, Credit Card numbers in your code
* Implement CI pipeline to identify the credentials, SSN, credit card information.

**Challenge 2: Keep your code clean**

* Identify the tools and technologies that you will use for static code analysis
* Design a workflow that eliminates many issues and false positives from static code analysis
* Design a workflow that eliminates credential leaks never included in the master branch.
* Develop CI pipeline that implements workflow with Static Code analysis

**Challenge 3: Detect Vulnerability of Container**

* Identify the top 10 OWASP vulnerability for the target docker container images
* Identify the Licensing issue through the CI pipeline
* Develop CD pipeline that deploy container-based microservices to an AKS cluster with Vulnerability / Licensing detection

**Challenge 4: Secret Rotation**

* Automate the Database Secret Rotation for existing microservices on the AKS cluster
* Avoid the downtime with rotating the secrets
* Automate the Service Principal rotation for AKS cluster

**Challenge 5: Apply policy to your organization**

* Make credential scanning mandatory to all pipelines among the organization
* Shorten the execution time of the pipeline
* Create a Work Item when the pipeline found vulnerabilities

**Challenge 6: Continuous Delivery with Penetration Testing**

* Develop Continuous Delivery pipeline with Security Approval
* Identify and execute Penetration Testing to the target microservices on AKS cluster
* Add Automate Penetration testing to the Continuous Delivery process

**Challenge 7: Detect vulnerability in one place**

* Centralize the issue detection among the 3rd party tools for developers
* Visualize the vulnerability on a centralized dashboard that the management can monitor
* Enabling centralized false positives suppression in one place