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

# Overview

The DevSecOps OpenHack Light is a multi-day experience where attendees learn to add Security oriented tooling into their workflow and CI/CD tasks. Attendees will learn how to leverage available tools/tasks in Azure DevOps to enable best practice oriented scenarios such as:

* Credential Scanning and Secret Management
* Static Analysis and Dependency/Container Scanning
* Automated Penetration testing
* Workflow optimization and automated feedback loops

Attendees will participate in challenges designed to educate them on these scenarios so they can implement as part of their engagement dev sprints with ease. These best practices and concepts were developed by the CSE Strategic Tech – DevOps team through real world engagement with our S400 and Hi-Po partners.

# Technologies

**Microsoft**

[Azure DevOps](https://dev.azure.com/), [Azure Key Vault](https://azure.microsoft.com/en-us/services/key-vault/), [Azure Automation](https://azure.microsoft.com/en-us/services/automation/), [Microsoft Security Code Analysis](https://secdevtools.azurewebsites.net/), [Azure Kubernetes Service](https://azure.microsoft.com/en-us/services/kubernetes-service/), [Azure Container Registry](https://azure.microsoft.com/en-us/services/container-registry/), [Azure Active Directory](https://azure.microsoft.com/en-us/services/active-directory/),

**Third Party**

[Sonar Cloud](https://sonarcloud.io/), [Aqua](https://marketplace.visualstudio.com/items?itemName=aquasec.aquasec), [Fossa](https://marketplace.visualstudio.com/items?itemName=Fossa.fossa-vsts), [White Source](https://marketplace.visualstudio.com/items?itemName=whitesource.whitesource),

# Challenges

**Challenge 1: Managing Secrets**

* Identify the tools and technologies that can help to protect from leaking credentials and secrets while in development
* Create a custom search pattern for secrets in your source code
* Manage/Rotate secrets in dev/test/production environments

**Challenge 2: Keep your code clean and vulnerability free**

* Identify the tools and technologies that you will use find security issues early in your development process
* Design/implement a workflow that eliminates many issues and false positives using static code analysis and dependency scanning
* Analyze dependencies in code and scan containers for known vulnerabilities

**Challenge 3: Automate penetration testing**

* Scan for OWASP top 10 vulnerabilities
* Incorporate pen testing into UI Automation testing
* Adjust scoring algorithm based on your threat model (SMACD)

**Challenge 4: Streamline and integrate workflow**

* Learn techniques/ trade-offs to speed up execution and minimize impact to developer productivity.
* Integrate into PR based workflow to provide effective and timeline feedback from automation
* Enable bot automation to streamline false positive resolution in external systems such as sonarcloud

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

* Make DevSecOps mandatory for all PR merges to master branches for your organization
* Reject a push to repository that contains secrets

At the end of the event, we will provide content and a recommended set of task that can be incorporated into a dev crew engagement to enable some of the practices that are covered during the event.