DevSecOps

Overview

Traditionally, companies doing in-house software development include at least one security review to verify the conformity of the application with the company policies. The adoption of the DevOps development methodology has raised concerns among some Azure customers. Often an automated release management or deployment part of the process is not implemented because of such concerns.

Our goal is to address our customers' concerns in terms of security regarding the implementation of DevOps practices with Azure DevOps and Azure Services.

Customer identification

Qualified customers are expected to have identified Azure as their deployment target and defined security requirement for the application. It is expected that the customer has already implemented a CI/CD pipeline and are willing to evolve it in order to meet their security requirements.

Key Scenarios

Credential Theft

This scenario has a focus on the implementation of proper authentication and permissions on the DevOps pipeline as well as identifying any keys, passwords, sql connection string or certificates that may be in the source code.

Identifying known vulnerabilities

Customers are facing the challenge of identifying early when they are using OSS packages. We aim at helping them identify early any packages or containers with vulnerabilities that they may be using.

Secure and compliant pipeline

Apply best practices for secrets managements, for example using Keyvault for storing keys and passwords and reducing the duplication of secrets using a herachy of vaults.

Implementing gates validating security configuration like ssl configuration or cross-site scripting issues throughout the release process.

Supporting technologies

- Azure DevOps
- Azure AD
- Key Vault
- 3rd party solutions like Appspider from rapid7 or ssltest from Qualys