edureka!

Microsoft Azure DevOps Solutions Certification (AZ-400)

COURSE OUTLINE

Azure AZ-400

MODULE 1: Introduction to Azure DevOps

MODULE 2: Implementing Continuous Integration

MODULE 3: Build Containers with Azure DevOps

MODULE 4: Designing a Dependency Management Strategy and Managing

Artifact Versioning

MODULE 5: Setting up Release Management Workflow

MODULE 6: Implementing Deployment Models and Services

MODULE 7: Implement and Optimize Continuous Feedback Mechanism

MODULE 8: Azure Tools: Infrastructure and Configuration, and Third-Party Tools

MODULE 9: Implementing Compliance and Security

MODULE 10: Azure Case Studies

edureka!

Implementing Compliance and Security

Topics

Following are the topics covered in this module:

- Security
- Secure and Compliant Development Process
- Application Config Data
- Security and Compliance in a Pipeline
- Code Quality
- Security Policies

Objectives

After completing this module, you should be able to:

- Set up secure and compliant development process
- Test code quality
- Design security policies
- Manage technical debt with Azure DevOps and SonarCloud
- Integrate Azure Key Vault with Azure DevOps
- Implement security and compliance in an Azure DevOps pipeline

edureka!

Introduction to Security

edureka!

Managing PayPal's Security

PayPal is an American company operating an online payments system in most countries that supports online money transfers and serves as an electronic alternative to traditional paper methods like checks and money orders

The Issue

Being a payment gateway company, they deal with a lot of financial transactions through their application. So, there are high chances of cyber attacks

PayPal Hires an Azure DevOps Engineer

Mr. CTO
PayPal

The application is vulnerable to attacks. We must provide security to the website

What is the plan?

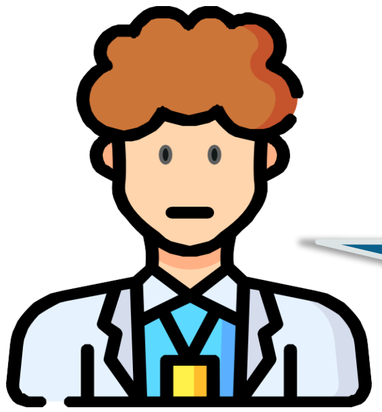
We will have to hire a senior Azure DevOps Engineer to solve this issue

Please go ahead!

Manager
Ethical Team

PayPal has hired Jeff to address this issue

The Research



Jeff
Azure DevOps Engineer

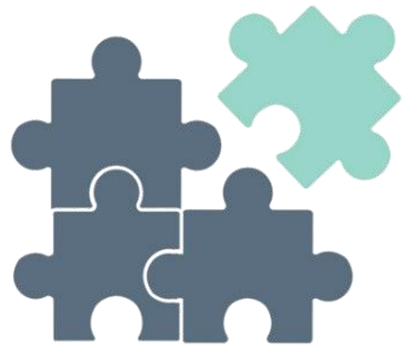
From my research, it is clear that two things need to be addressed

- Technical debts
- Security and compliance

Jeff’s Analysis

According to Jeff

- Technical debts can be managed by using SonarCloud and Azure DevOps
- Security and compliance can be maintained by integrating Azure Key Vault with Azure DevOps and implementing compliance in an Azure DevOps Pipeline



The Solution

Sonarcloud is the leading online service for Code Quality and Code Security

Azure DevOps is a cloud service from Microsoft for collaborating on code development

Azure Key Vault helps teams to securely store and manage sensitive information such as keys, passwords, certificates, etc

Azure DevOps Pipeline lets you build, test and deploy application on Azure cloud and other supported platforms

Introduction to Security

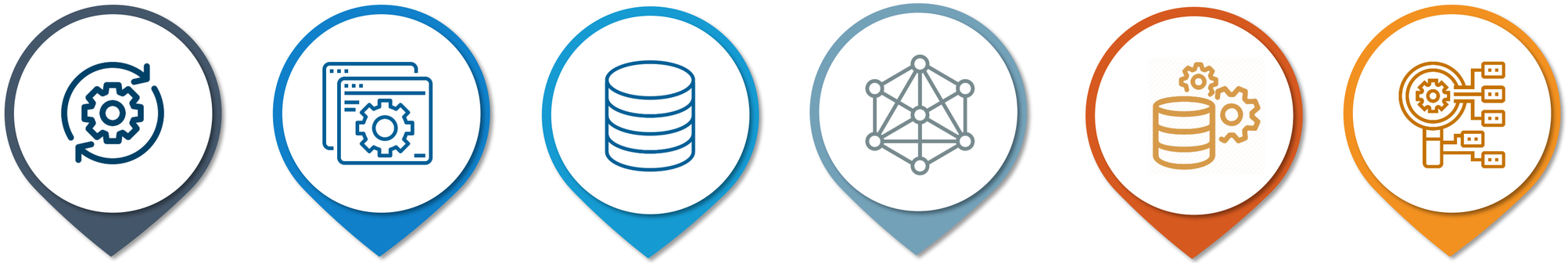
edureka!

Overview of Security

- Security of all the cloud resources is mandatory for any organization
- Security in the cloud is a shared responsibility, meaning it is jointly controlled by Azure and Developer
- Azure provides various tools to design the security system for the application

Built-in Capabilities in Azure

- The capabilities available in the Azure platform help in managing the security of the application or service
- The built-in capabilities in Azure are organized in six functional areas:



Operations | Applications | Storage | Networking | Compute | Identify

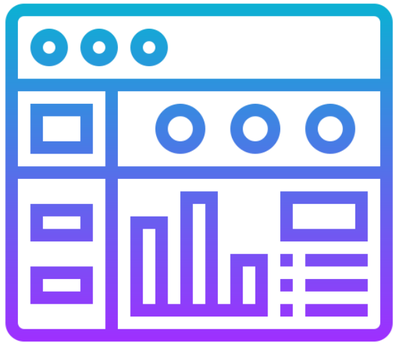
Operations

Operations include:

1. Security and Audit Dashboard
2. Azure Resource Manager
3. Application Insights
4. Azure Monitor
5. Azure Monitor Log
6. Azure Advisor
7. Azure Security Centre

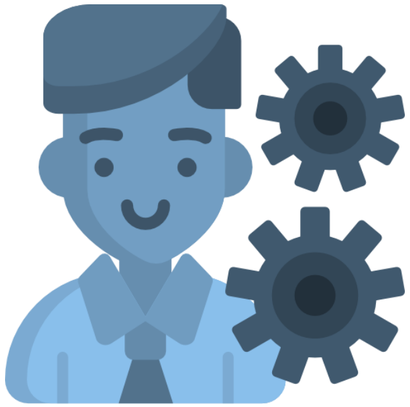
Operations: Security and Audit Dashboard

The security and audit dashboard is a screen related to security in Azure Monitor logs



Operations: Azure Resource Manager

Security can be controlled by creating the resources through ARM Template with Security-related settings



Operations: Application Insights

Application insights provides information about application availability, crashes, etc

Operations: Azure Monitor

Azure Monitor alerts us about any security-related event

Operations: Azure Monitor Log

Azure Monitor logs can be queried, and any security-related information present in the log can be found out

Operations: Azure Advisor

This service scans and analyzes all the resources along with telemetry and recommends ways to improve the security

Operations: Azure Security Center

It provides integrated security monitoring and policy management which helps detect threats

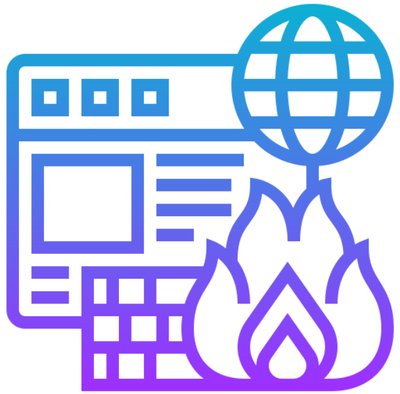
Applications

Applications include:

1. Web Application Firewall (WAF)
2. Authentication and Authorization
3. Layered Security Architecture
4. Diagnostic Log

Applications: Web Application Firewall (WAF)

To safeguard the application from popular web-based attacks, WAF is present in the application gateway



Applications: Authentication and Authorization

Authentication and authorization makes sure that only the right user with the right permission is granted application access

Applications: Layered Security Architecture

It is like a load balancer, where firewall is defined to protect the application in layers like network security group in virtual machine

Applications: Diagnostic Log

Diagnostic logging is a troubleshooting mode. It helps generate:

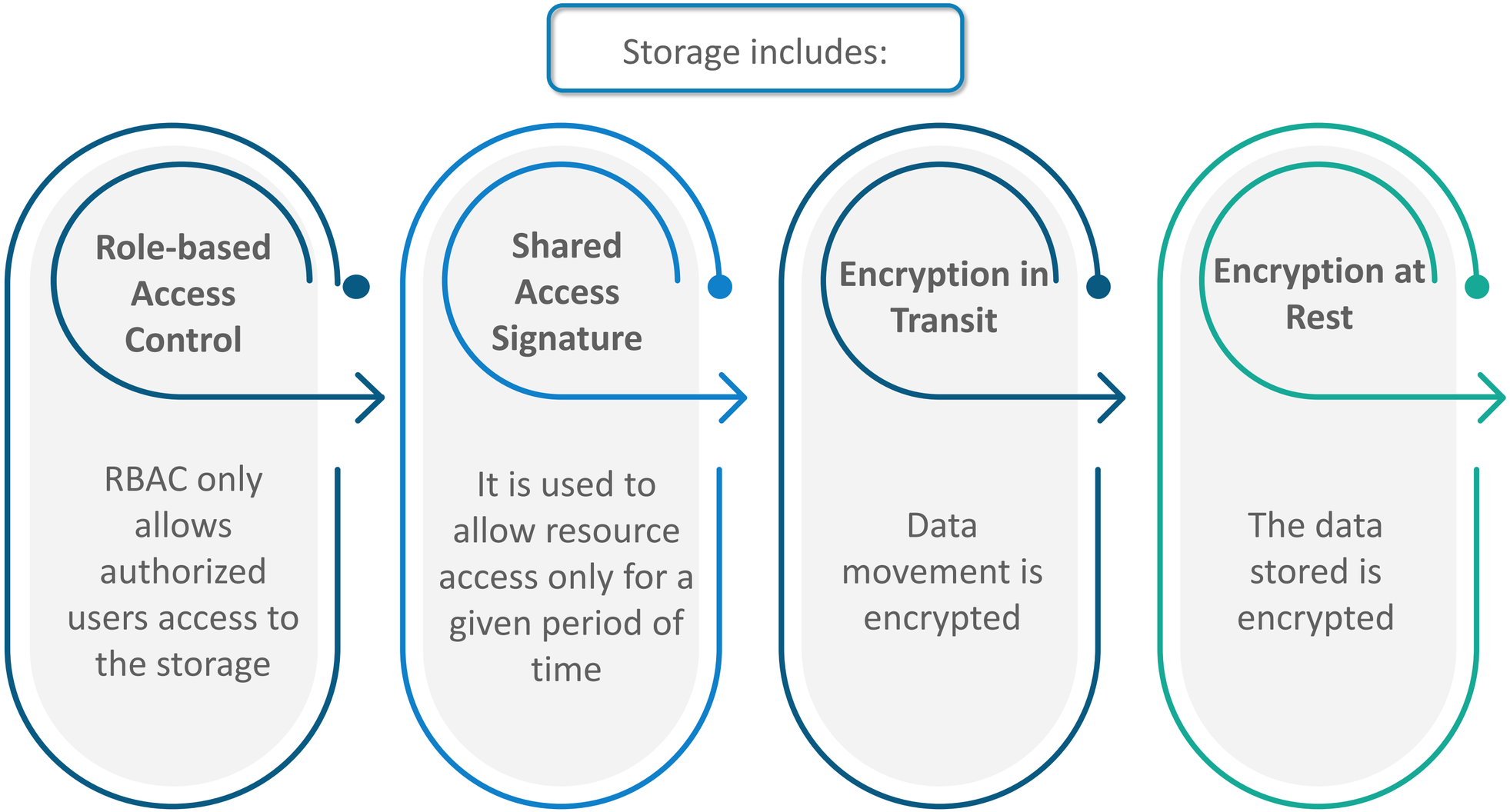
Web Server Log

- Detailed Error Log
- Failed Request Log

Application Diagnostic Log

- Application Error
- Performance Log

Storage



Networking

Networking includes:

Network Security Group	Protects the VM by letting through only allowed traffic
Azure Virtual network	It is used to group a set of resources so that they can communicate with each other by not allowing outside traffic
Security Center	Azure security center continuously analyzes the security state of Azure resources

Compute

Compute includes:

Antimalware and Antivirus	Antimalware and Antivirus must be installed in the virtual machines to protect it
Virtual Machine Backup	Take the back up of virtual machine frequently to protect it
Azure Site Recovery	It is required for the continuity of operations in the event of failure

edureka!

Identity and Access Management

- Securing applications, systems and data begins with identity-based access controls
- Grant user access only to those controls that the user needs

Identity and Access Management: Processes

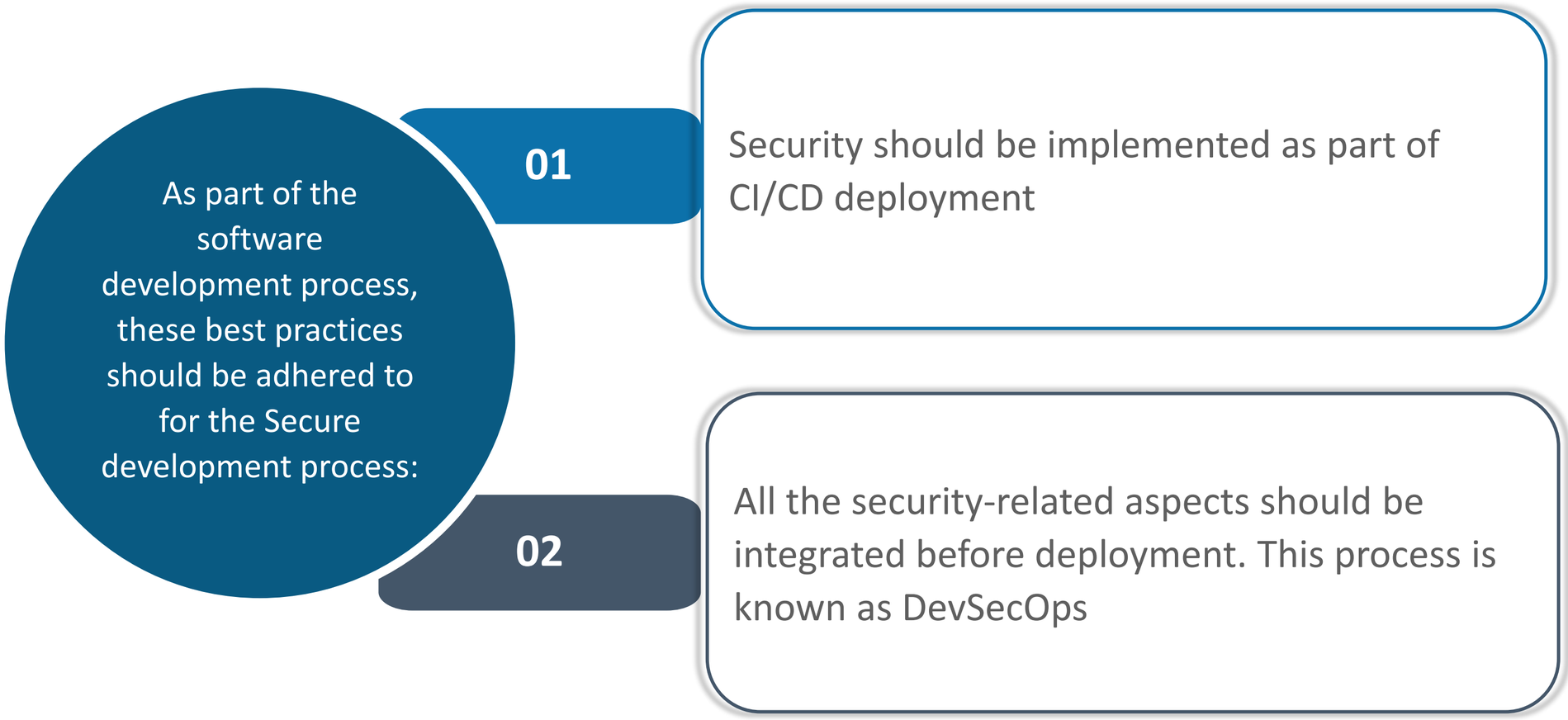
To secure the identity and ensure a safe login, Microsoft has defined several security measures:

Multi-factor authentication	Apart from a user password, it mandates another mode of authentication such as OTP, phone-call
Microsoft Authenticator app	The app provides the token id, which will be required for login
Role-based access	Grants access based on the user's assigned role

Implement Secure and Compliant Development Process

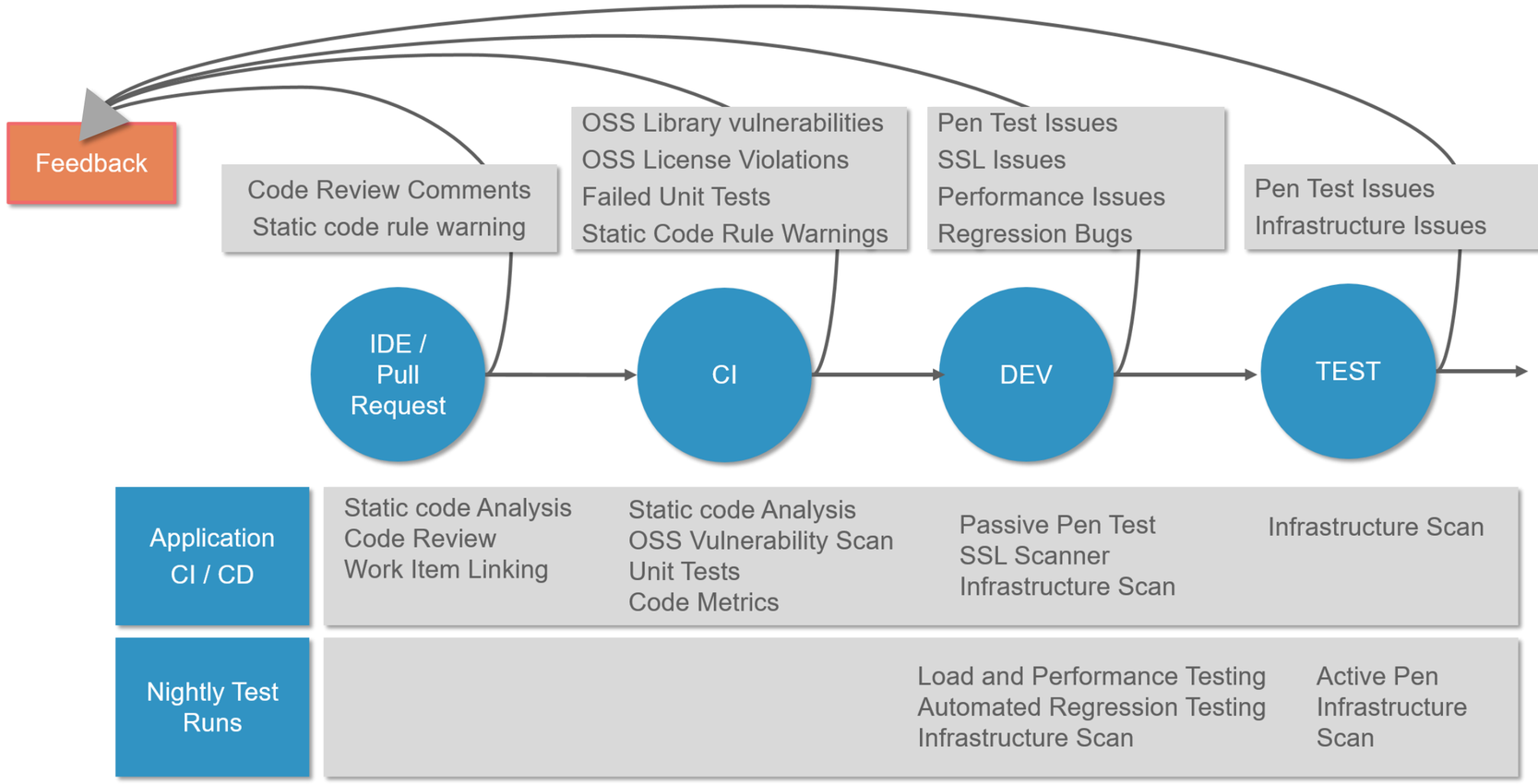
edureka!

Secure Development Process



Implementing Security in CI/CD Pipeline

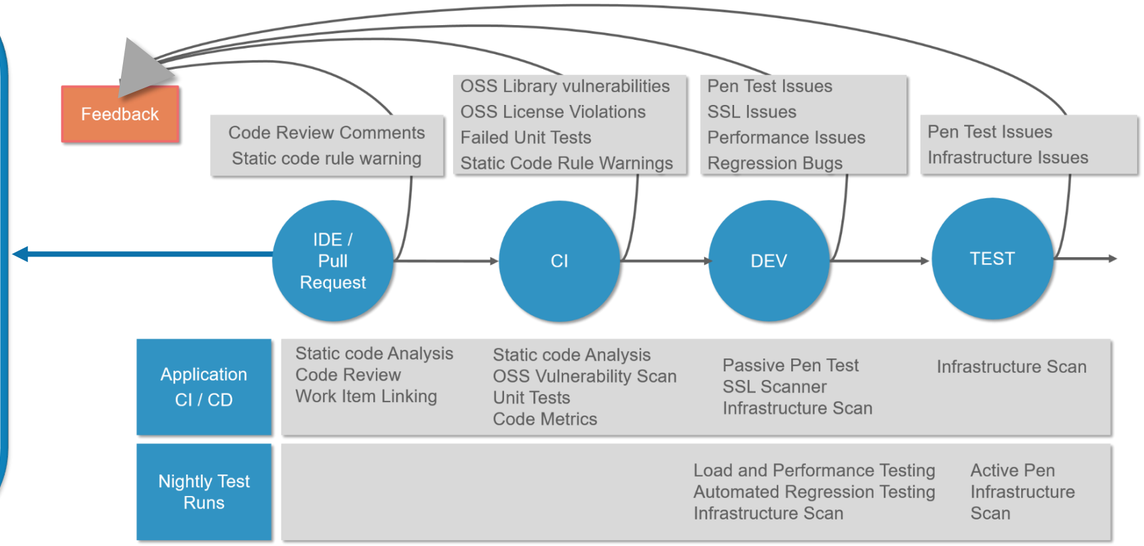
Below diagram shows the various parts of implementing security in the CI/CD pipeline:



edureka!

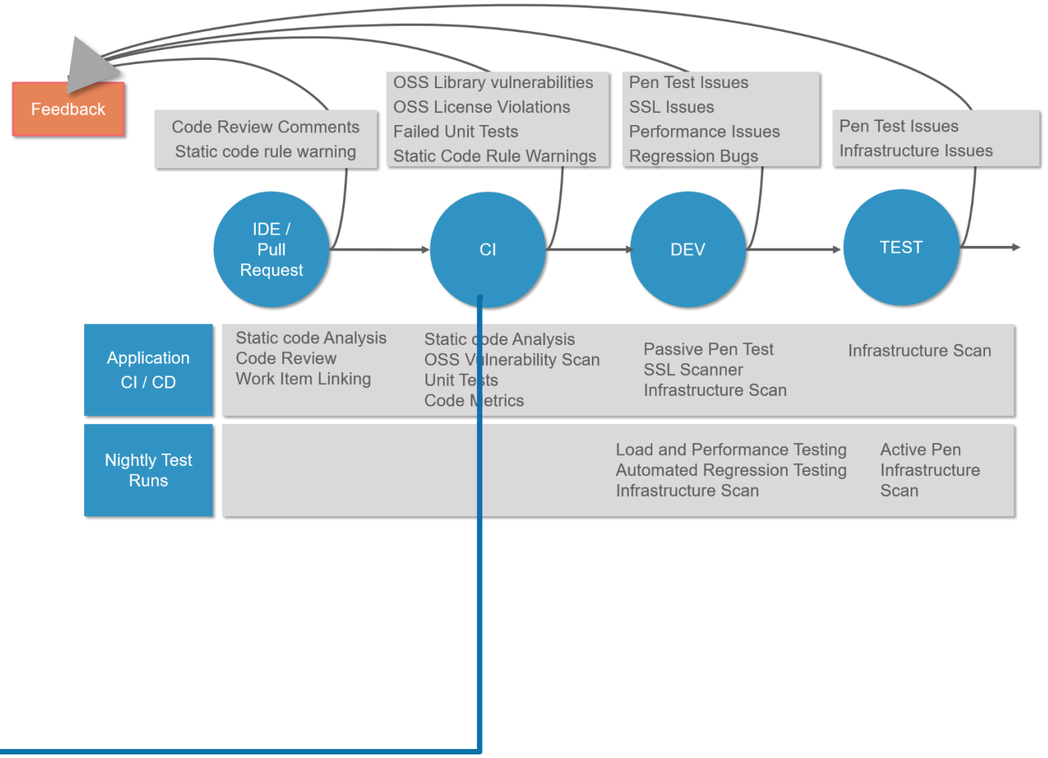
IDE/Pull Request

- Security validation in the CI/CD begins when the developer commits his or her code
- Code analysis tools provide the first level of security check



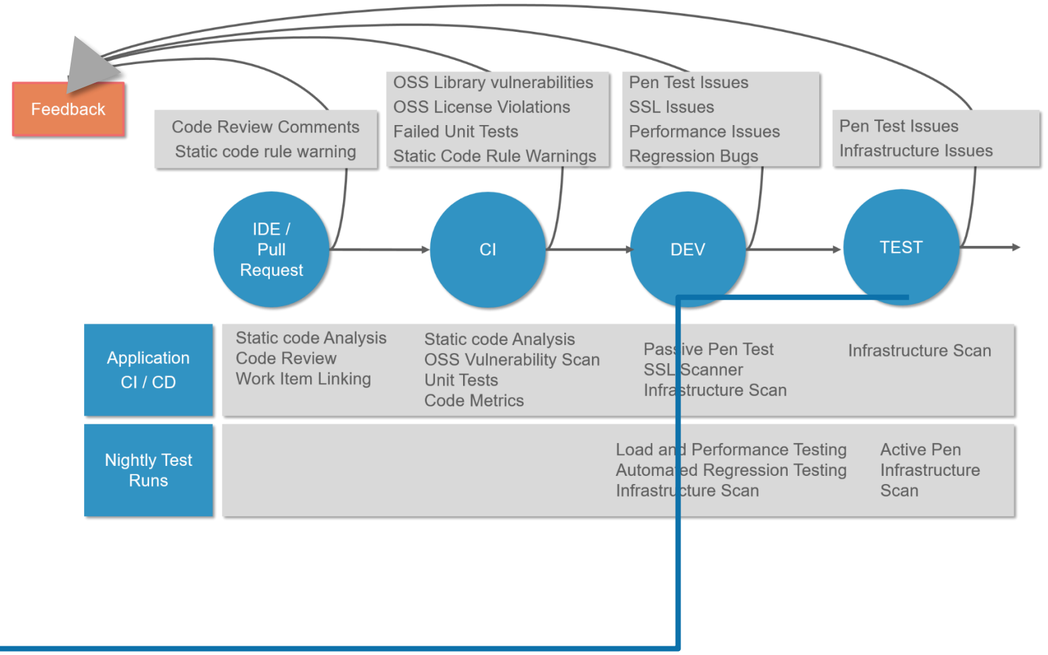
CI (Continuous Integration)

- In the continuous integration process, static code analysis should be done before initiating
- For the 3rd party libraries, WhiteSource Software should be used as part of the CI/CD pipeline to check that 3rd party software is secure



Dev and Test

- After the application is deployed, make sure there aren't any security vulnerabilities
- This is achieved by executing an automated Penetration test. **OWASP ZAP** tool can be used for Penetration testing

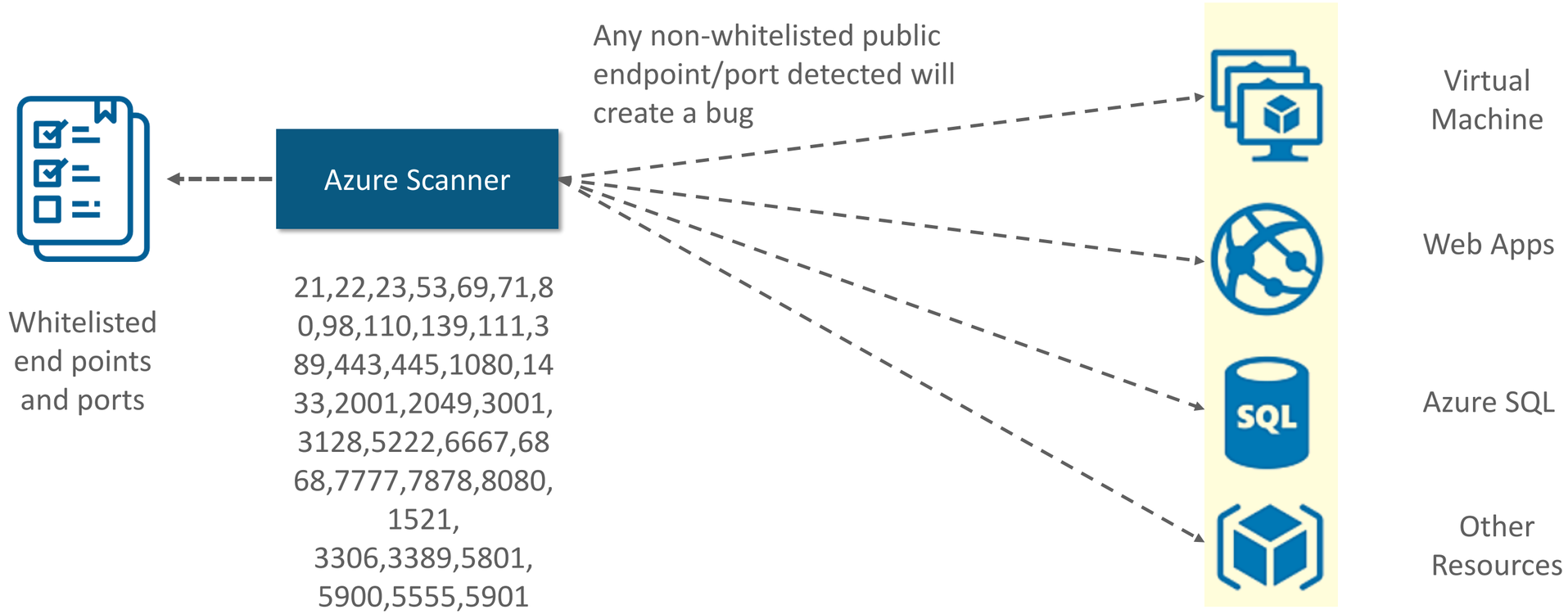


Validating Infrastructure Security

Azure provides Azure Security Center and Azure Policy to validate the security

Azure Scanner

Azure scanner scans the resources and checks if any internet-facing endpoint or port is available in the Allow list of endpoints and port.



Azure Scanner (Cont.)

- After the scan is completed, Azure Pipelines release is updated with a result report, and bugs are created in the team's backlog
- Resolved bugs will be closed if the vulnerability has been fixed

Managing Application Config Data

edureka!

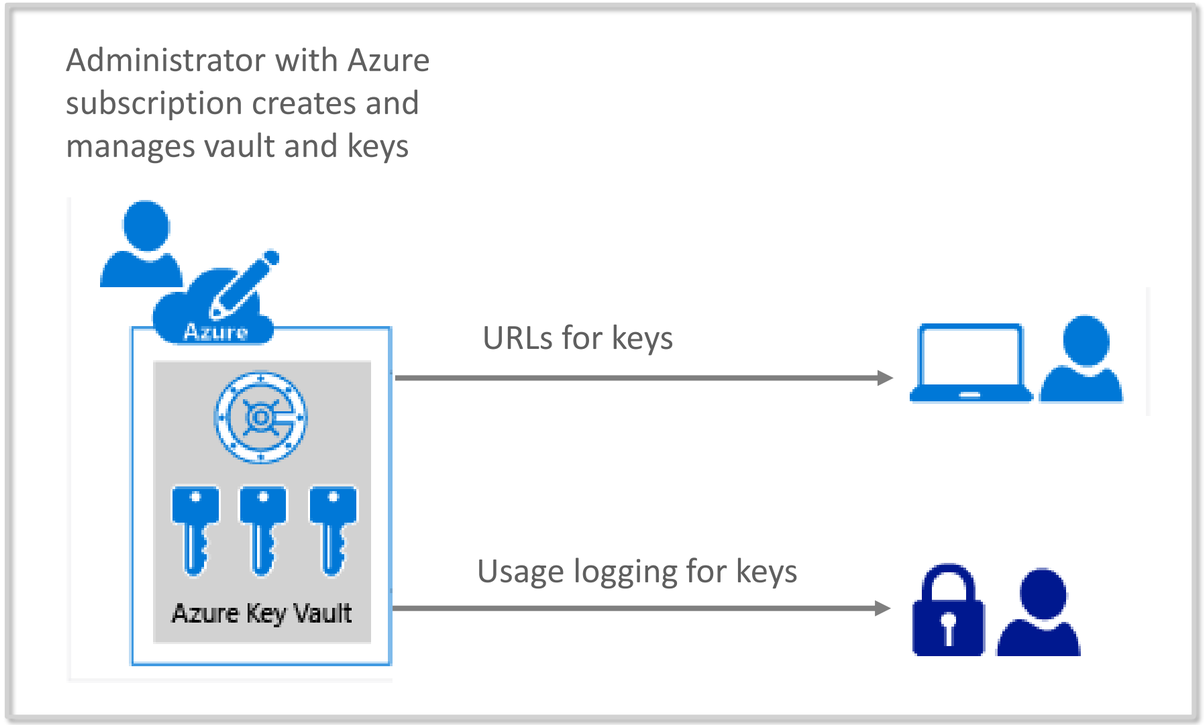
Azure Key Vault

The application depends on configuration data for many of the runtime properties in the configuration file, the data connection strings, certificate, etc.

- This file can be exposed to client users due to which there can be potential security issues
- To resolve this, Azure came with the concept of the Azure Key Vault

Azure Key Vault (Cont.)

- The key can be used for retrieving the value
- The advantage is that no one can see these values
- To access these keys, the application should first authenticate with key vault



Secret Management

Azure Key Vault can securely store and control access to tokens, passwords, certificates, API keys, and other secrets.

Key Management

- Azure Key Vault makes it easier to create and control the encryption keys used to encrypt your data
- Azure services such as App Service integrate directly with Azure Key Vault and can decrypt secrets

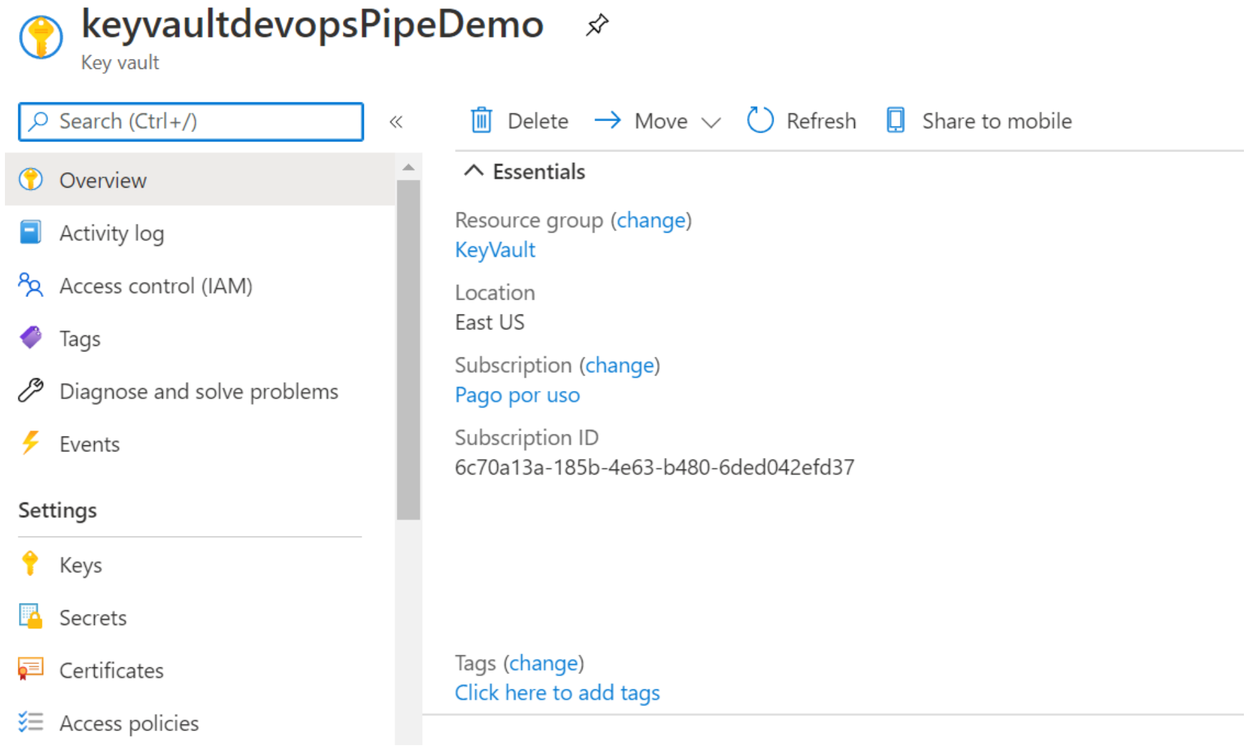
Certificate Management

Azure Key Vault provides the capability to provision, manage, and deploy public and private SSL/TLS certificates

Configuring Secret, Key, and Certificate

The secret, key and certificate can be configured from Azure portal.

- Go to Azure portal
- Create Key vault
- Configure the keys, secrets and certificate through the left side menu in Key vault



edureka!

Managing Security and Compliance in a Pipeline

edureka!

Security and Compliance

Security and Compliance are required for a successful and secure deployment.

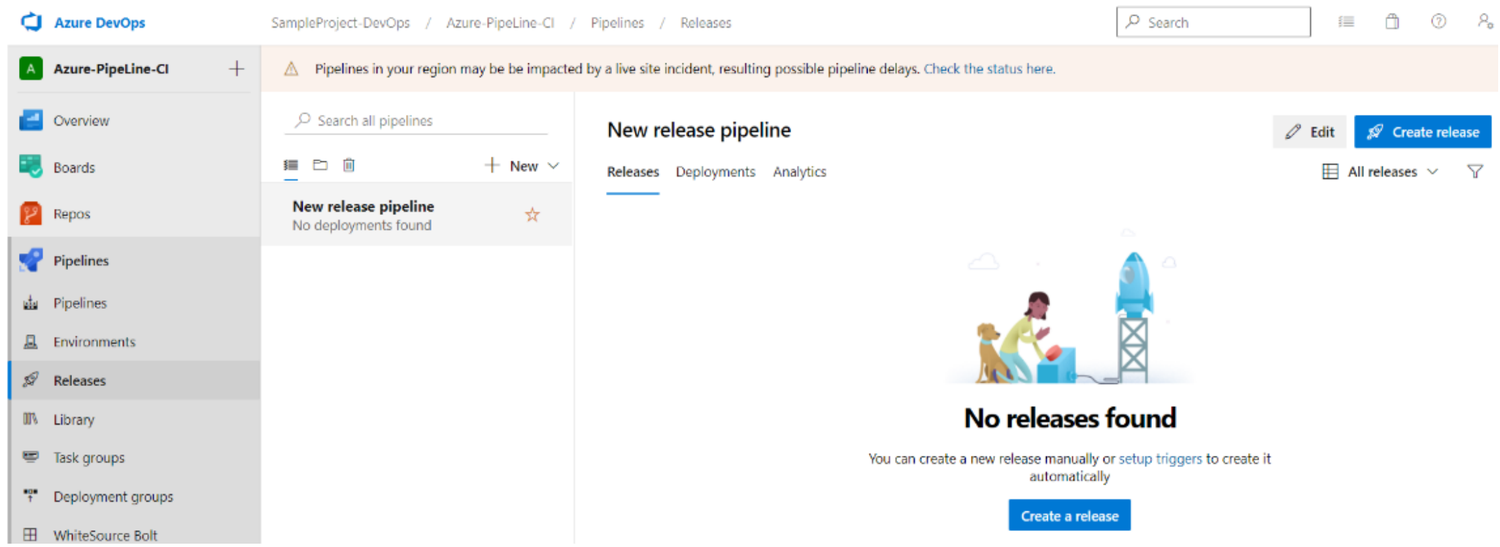
Implementing Security and Compliance

All compliance can be defined in Azure policy and used as part of pre-deployment in Azure Pipeline.

Go to Azure DevOps

Go to any working project

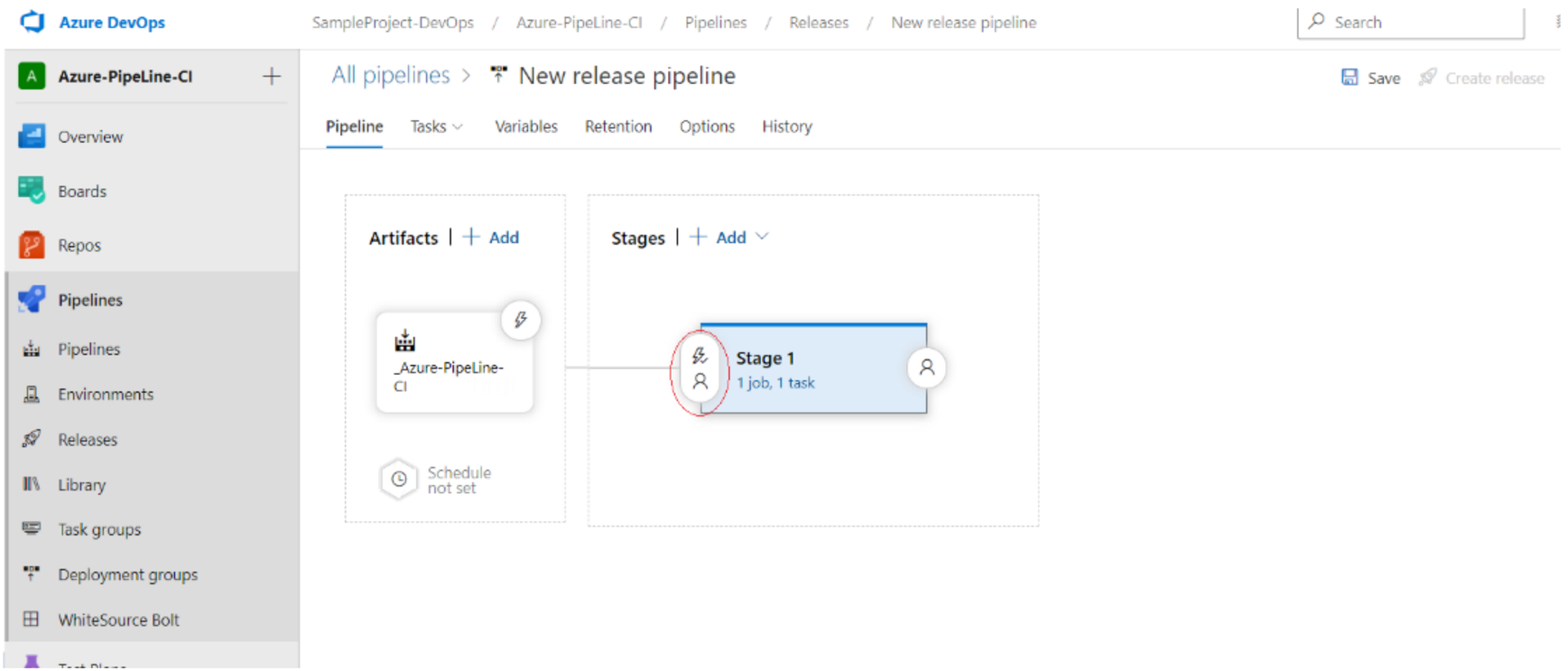
In the Pipeline menu on the left side, click on Releases



edureka!

Implementing Security and Compliance (Cont.)

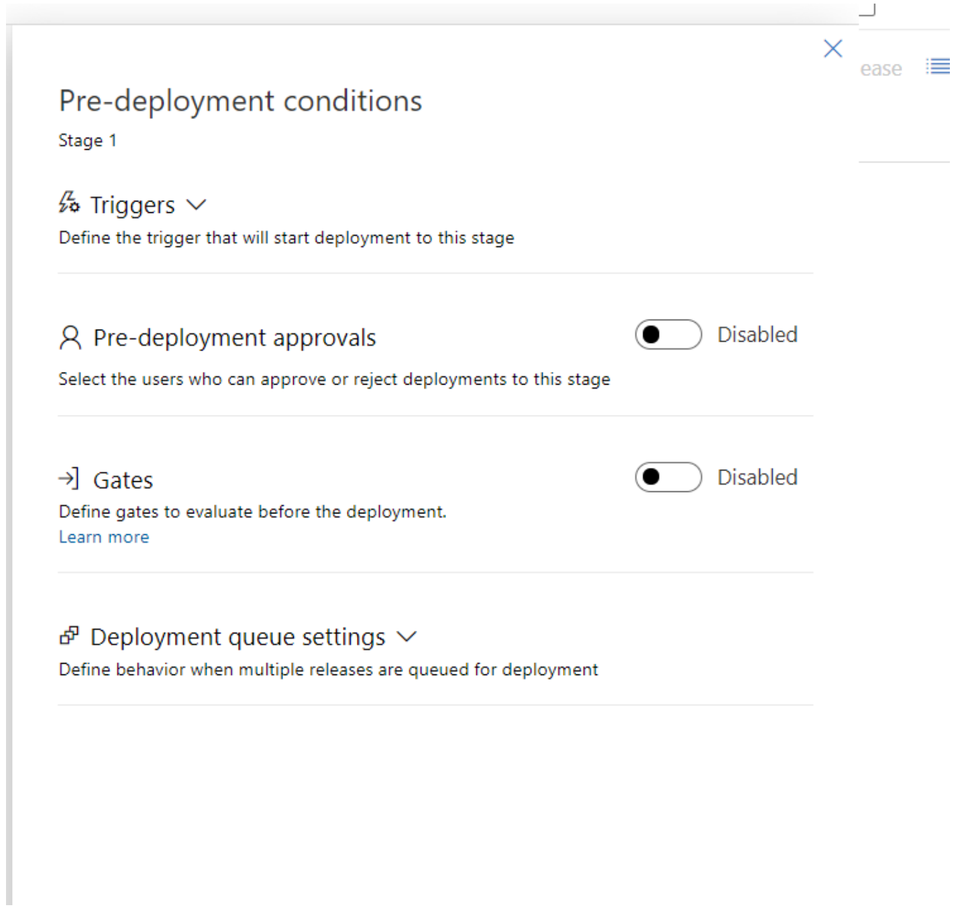
- Create a new release. The below screen will pop up
- Click on the encircled icon as shown below



edureka!

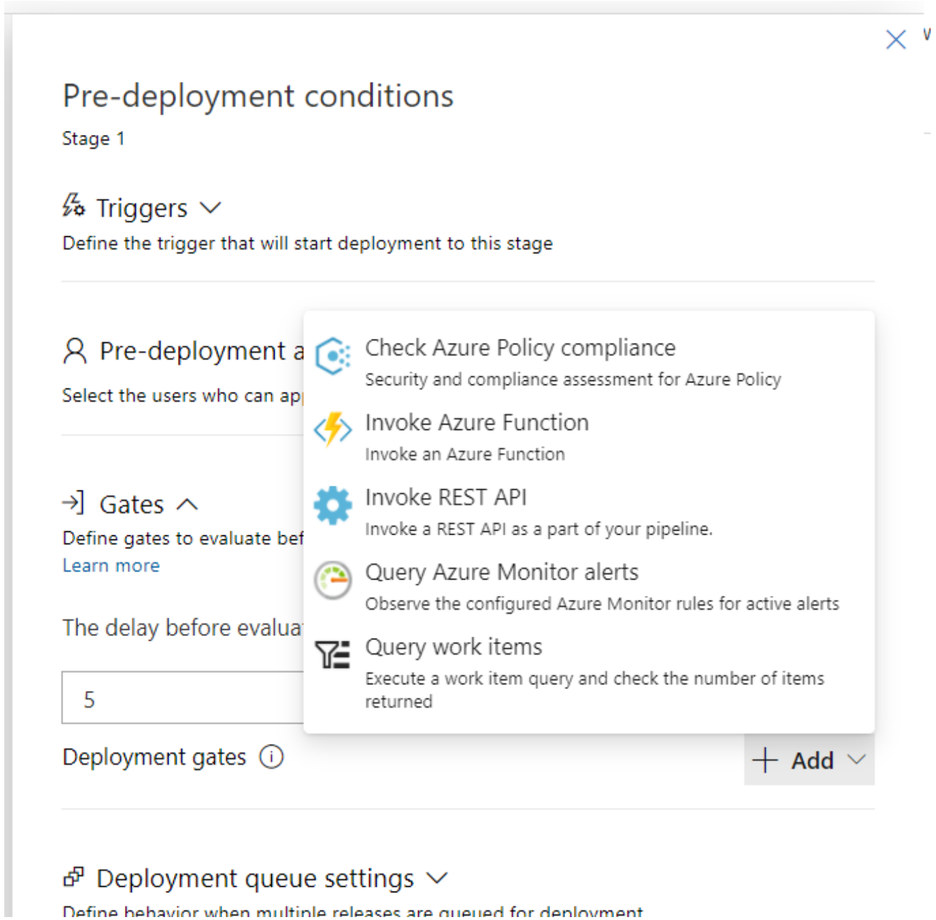
Implementing Security and Compliance (Cont.)

- Now, the below screen will pop up
- Enable the gates here



Implementing Security and Compliance (Cont.)

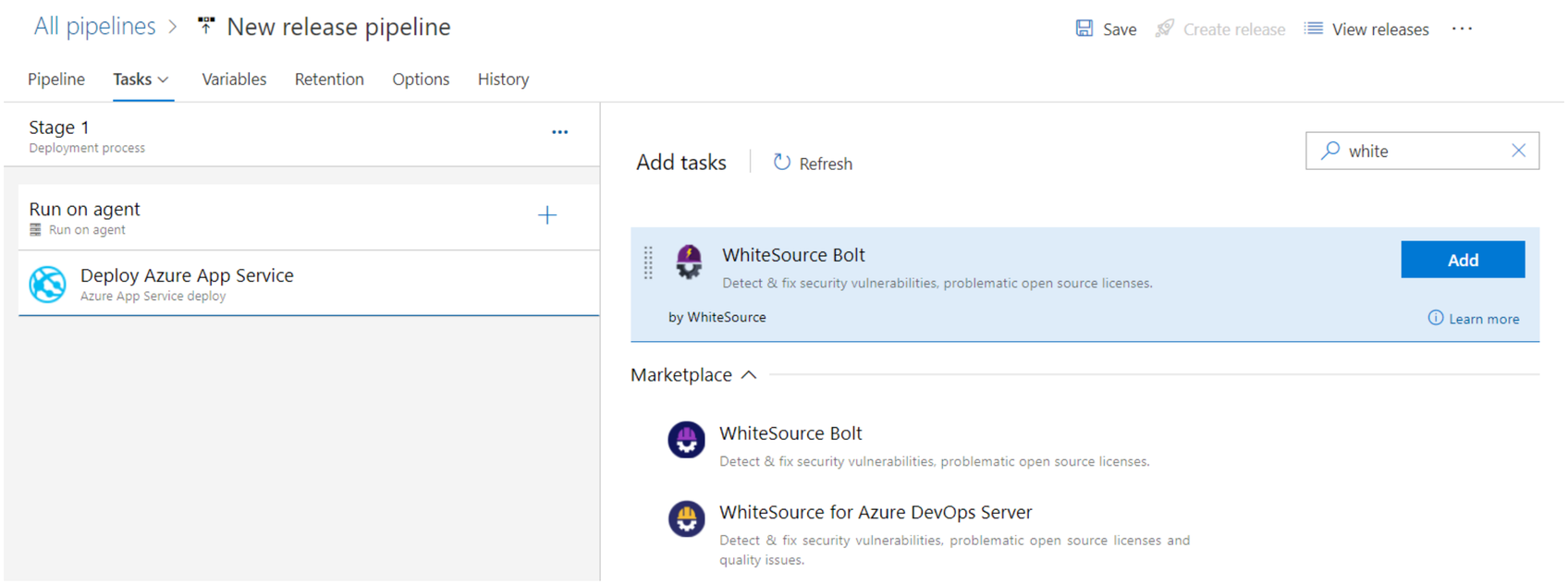
- Select the Check Azure Policy Compliance
- Configure it and connect with the Azure Policy
- This way, compliance will be maintained in the release pipeline



edureka!

Adding Compliance as a Part of Release Pipeline

Security can be maintained by scanning the 3rd party software and license validity through WhiteSource.



edureka!

Managing Code Quality

edureka!

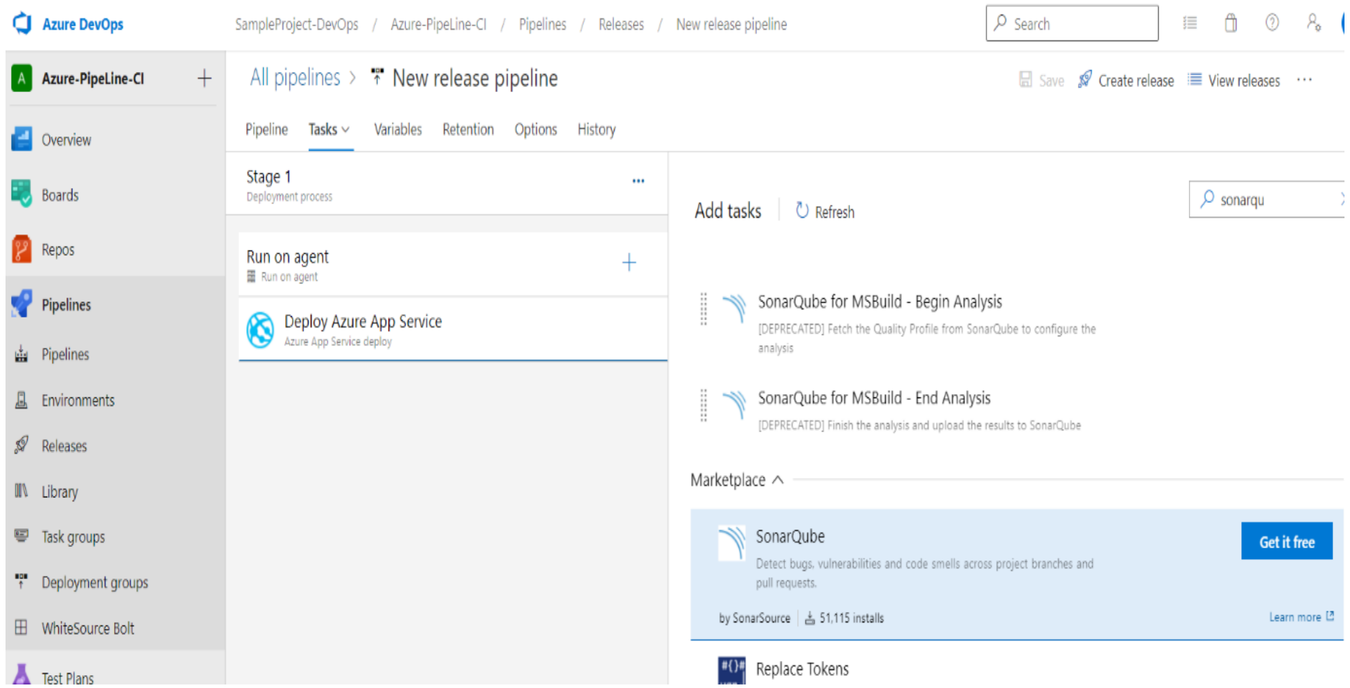
Code Quality

The code quality can be analyzed by using tools such as SonarQube or SonarCloud.

Code Quality: SonarQube

- SonarQube analyzes branches and pulls requests to spot and resolve issues before the user merges to master
- SonarQube dives directly into detected issues and offers contextual help to the users

Code Quality: SonarQube (Cont.)



With SonarQube, it is easy to ensure that the code is up to standards.

edureka!

Code Quality: SonarCloud

The main features of SonarCloud are:

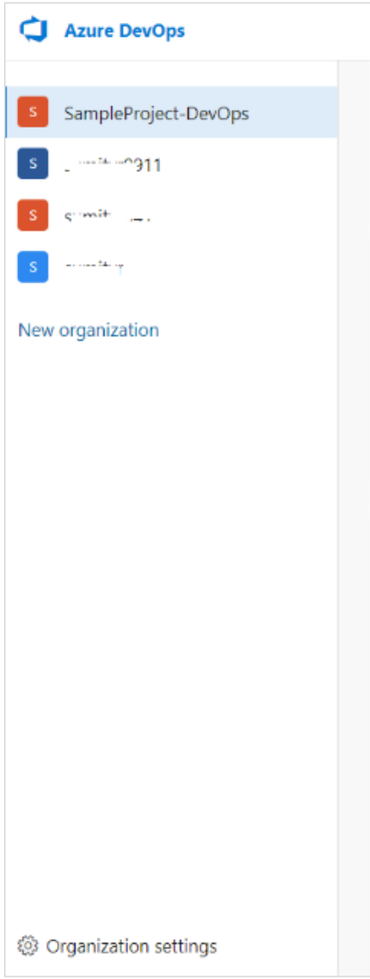
- It supports 16 languages, including Java, JS, C#, C/C++, Objective-C, among others
- It contains thousands of rules to track down hard-to-find bugs and quality issues
- Cloud CI Integrations with VSTS
- It helps in deep code analysis to reach a green quality gate and promote the build
- It is fast and scalable

Managing Security Policies

edureka!

Configuring Security Policies

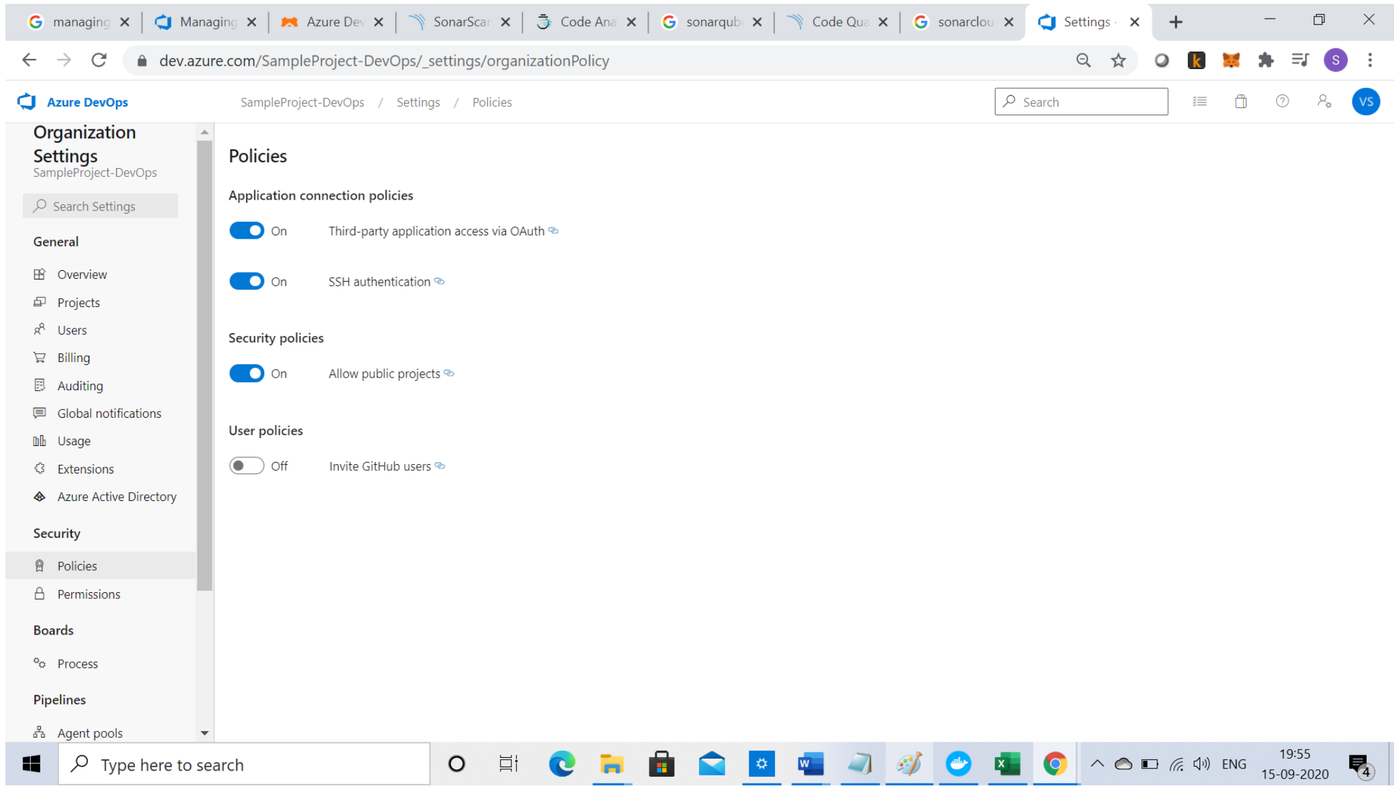
- Security policies for Azure DevOps organization can be set through Azure DevOps
- Click on the Organization settings of the Azure DevOps Organization



Configuring Security Policies (Cont.)

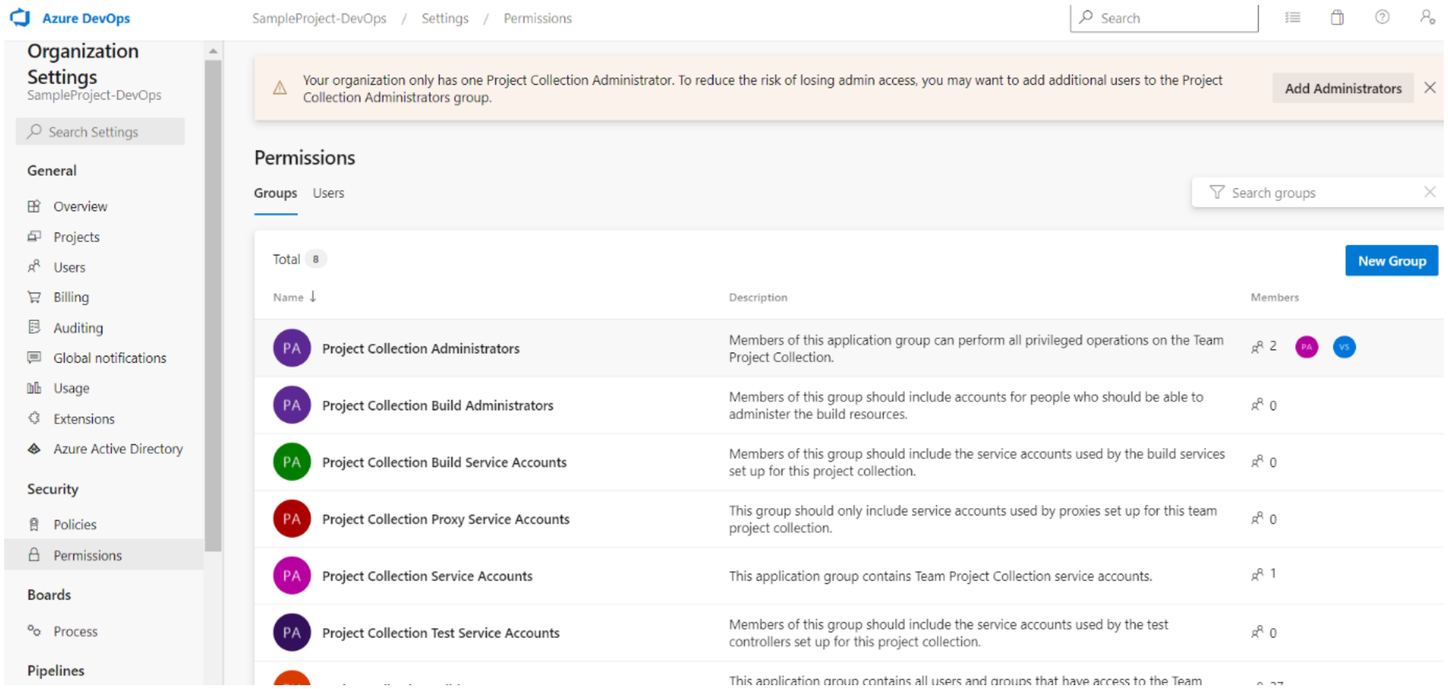
Now, click on Policies and the below screen will pop up. Appropriate settings can be defined here.

This way, security policies can be configured.



Defining Permissions

Permission for users can be defined in the Permissions section, as shown below. Select any group and add the user.



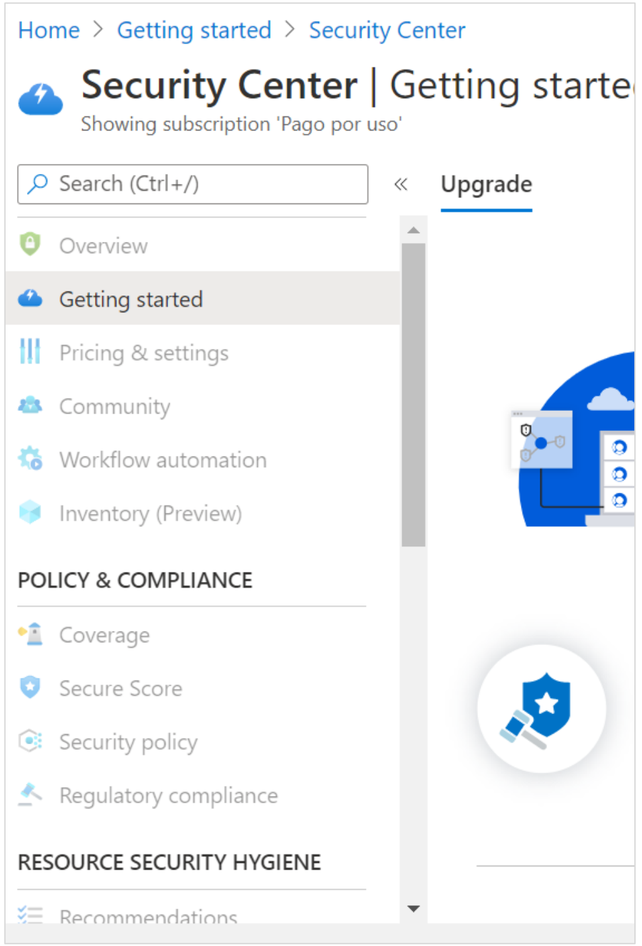
edureka!

What is Azure Security Center?

Azure Security Center is a centralized security management framework for infrastructure that offers advanced threat defense through the hybrid cloud workloads

Azure Security Center

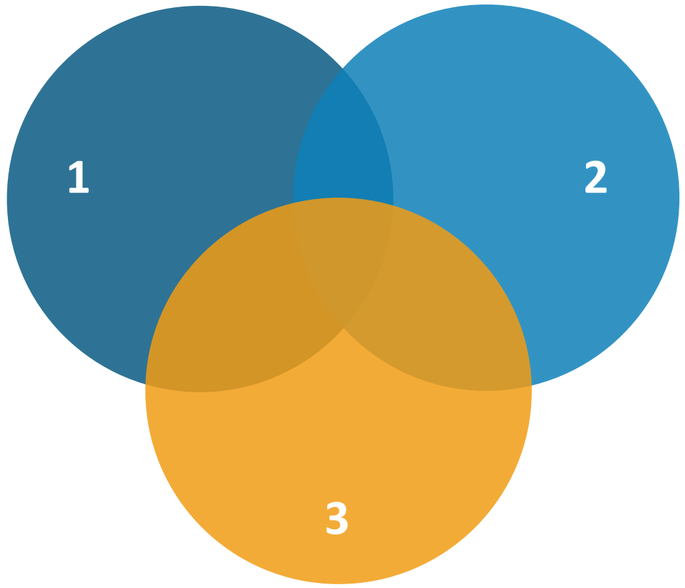
Azure Security Center can be enabled in the Azure Portal



Azure Security Center (Cont.)

Azure security center provides you with the tools to:

Strengthen security posture

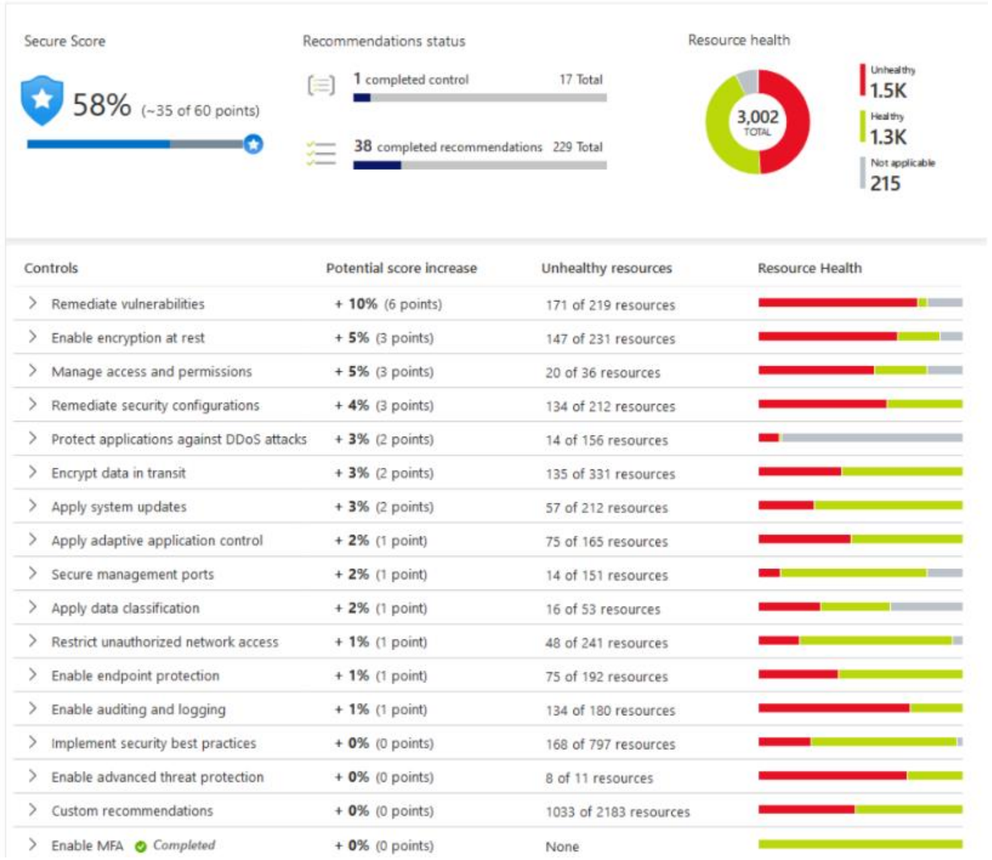


Protect against threats

Get secured faster

Continuous Assessment

As shown here, the Azure Security Center conducts ongoing evaluations of all Azure tools and offers a dashboard with all the recommendations



edureka!

Demo: Manage Technical Debt with Azure DevOps and SonarCloud

edureka!

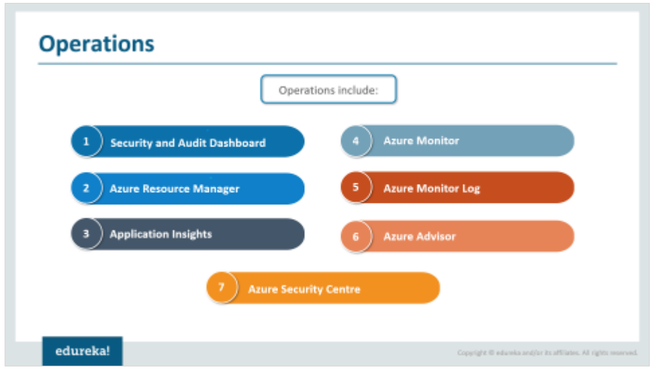
Demo: Integrate Azure Key Vault with Azure DevOps

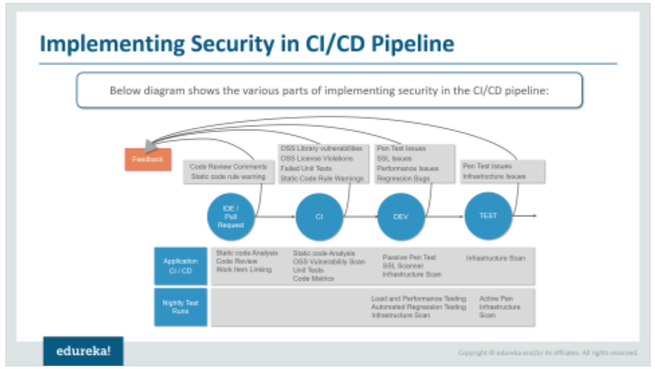
edureka!

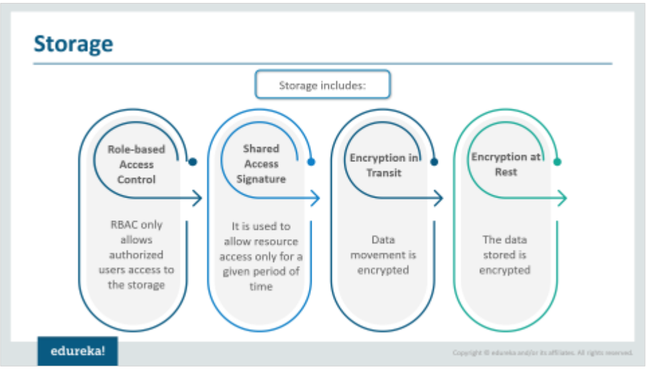
Demo: Implement Security and Compliance in an Azure DevOps Pipeline

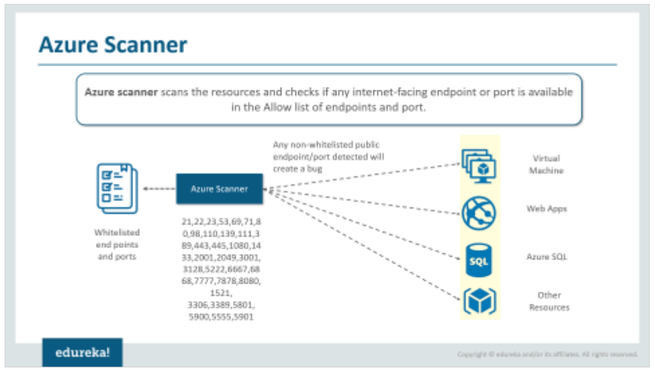
edureka!

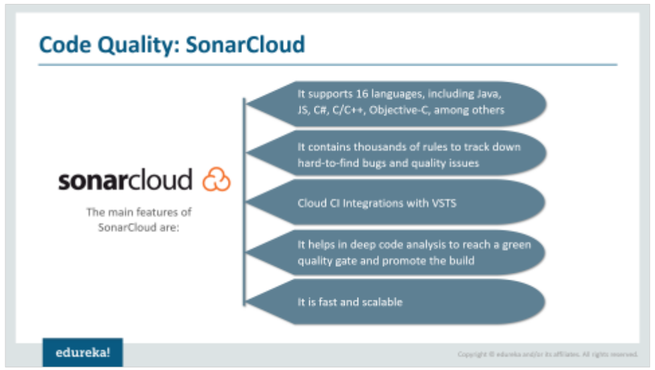
Summary

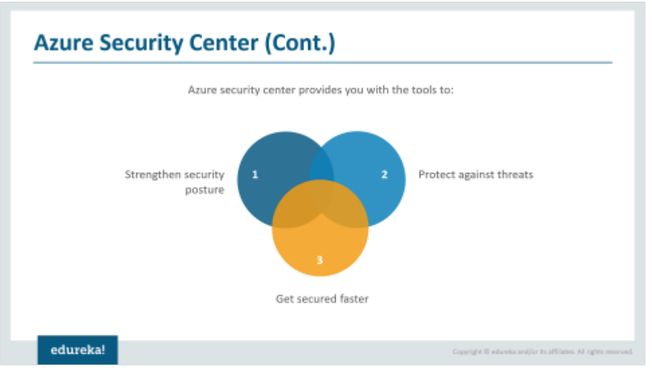












edureka!

edureka!

edureka!

Thank You

For more information please visit our website
www.edureka.co