

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

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:

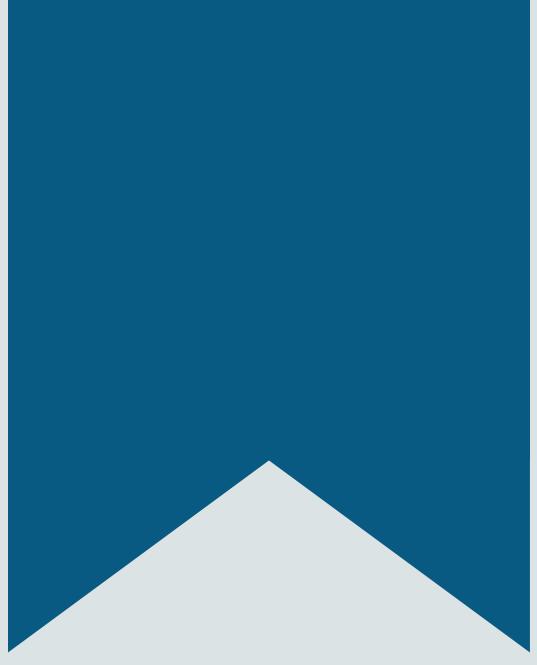
- Security
- Secure and Compliant Development Process
- Application Config Data
- Security and Compliance in a Pipeline
- Code Quality
- Security Policies

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





Introduction to Security

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

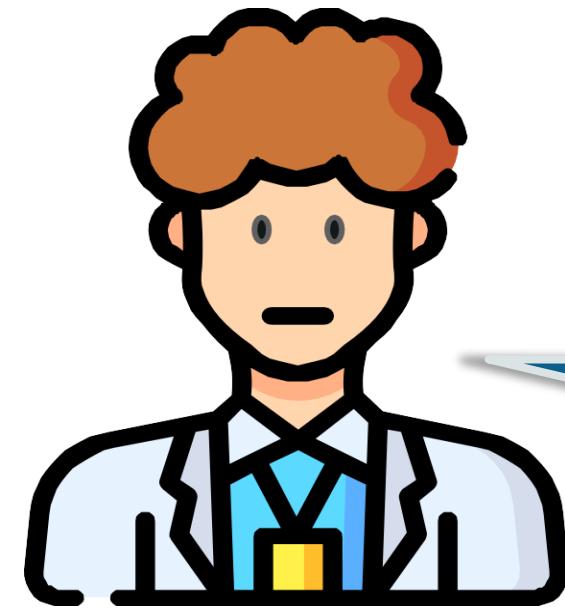
Please go ahead!



Manager
Ethical Team

PayPal has hired Jeff to address this issue

The Research



Jeff
Azure DevOps Engineer

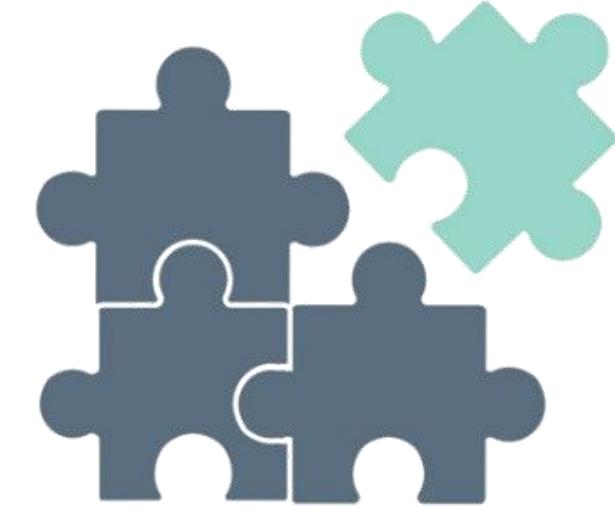
From my research, it is clear that two things need to be addressed

- 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



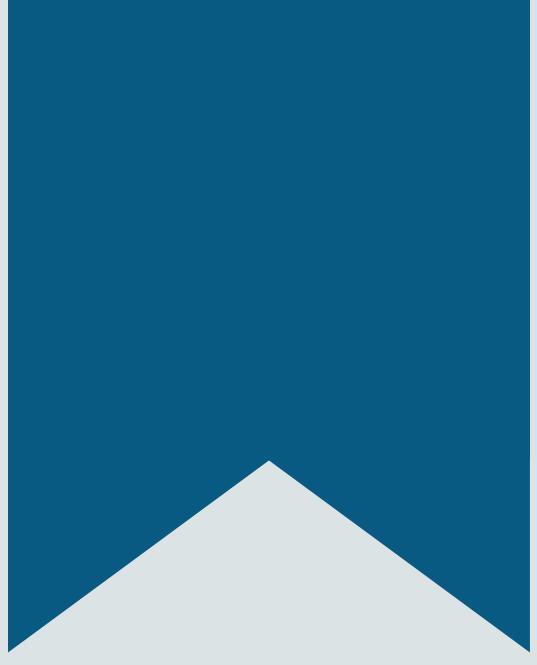
Azure DevOps is a cloud service from Microsoft for collaborating on code development



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

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

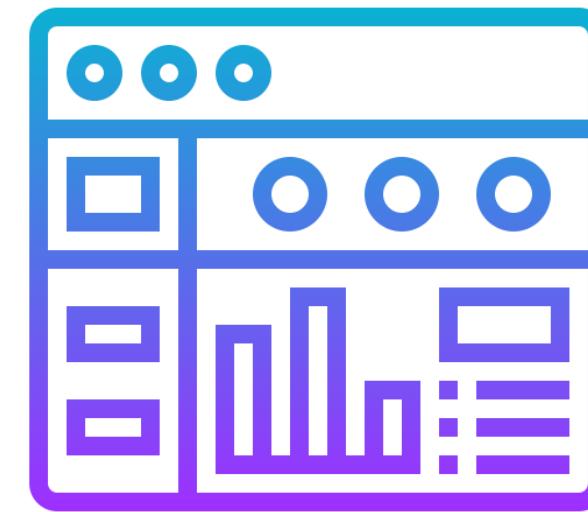
5 Azure Monitor Log

6 Azure Advisor

7 Azure Security Centre

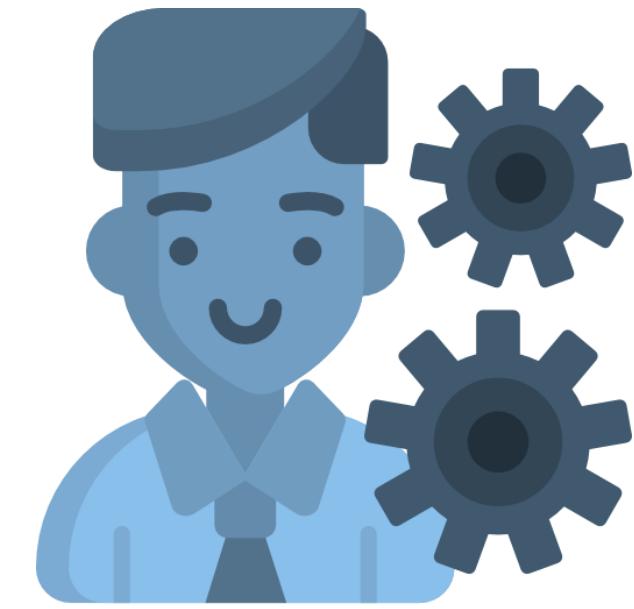
Operations: Security and Audit Dashboard

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



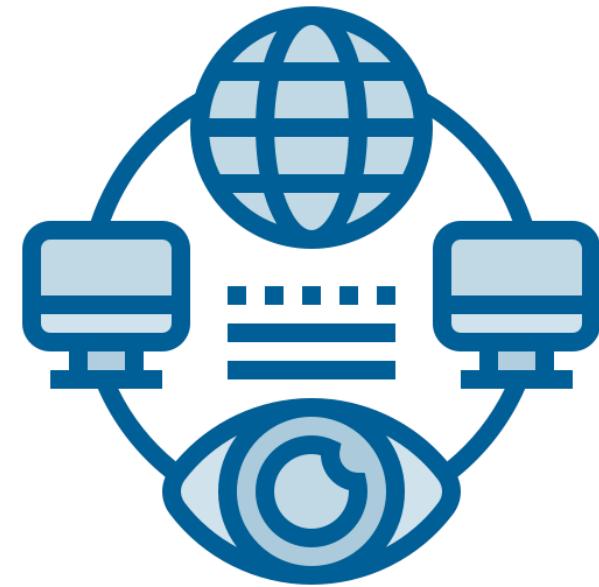
Operations: Application Insights

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

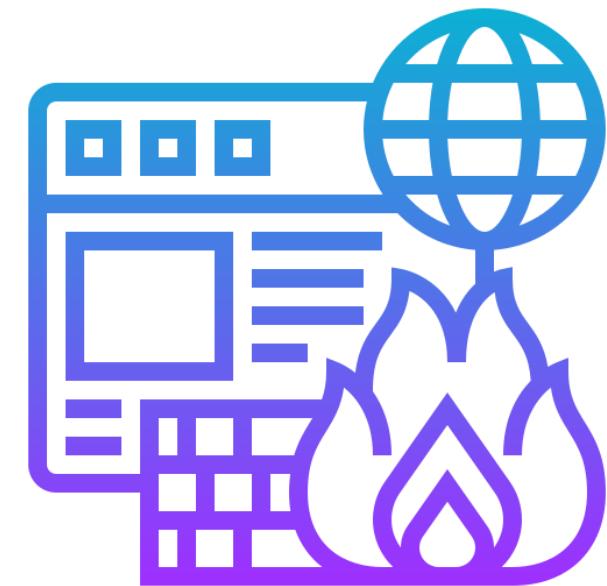
Layered Security Architecture

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:

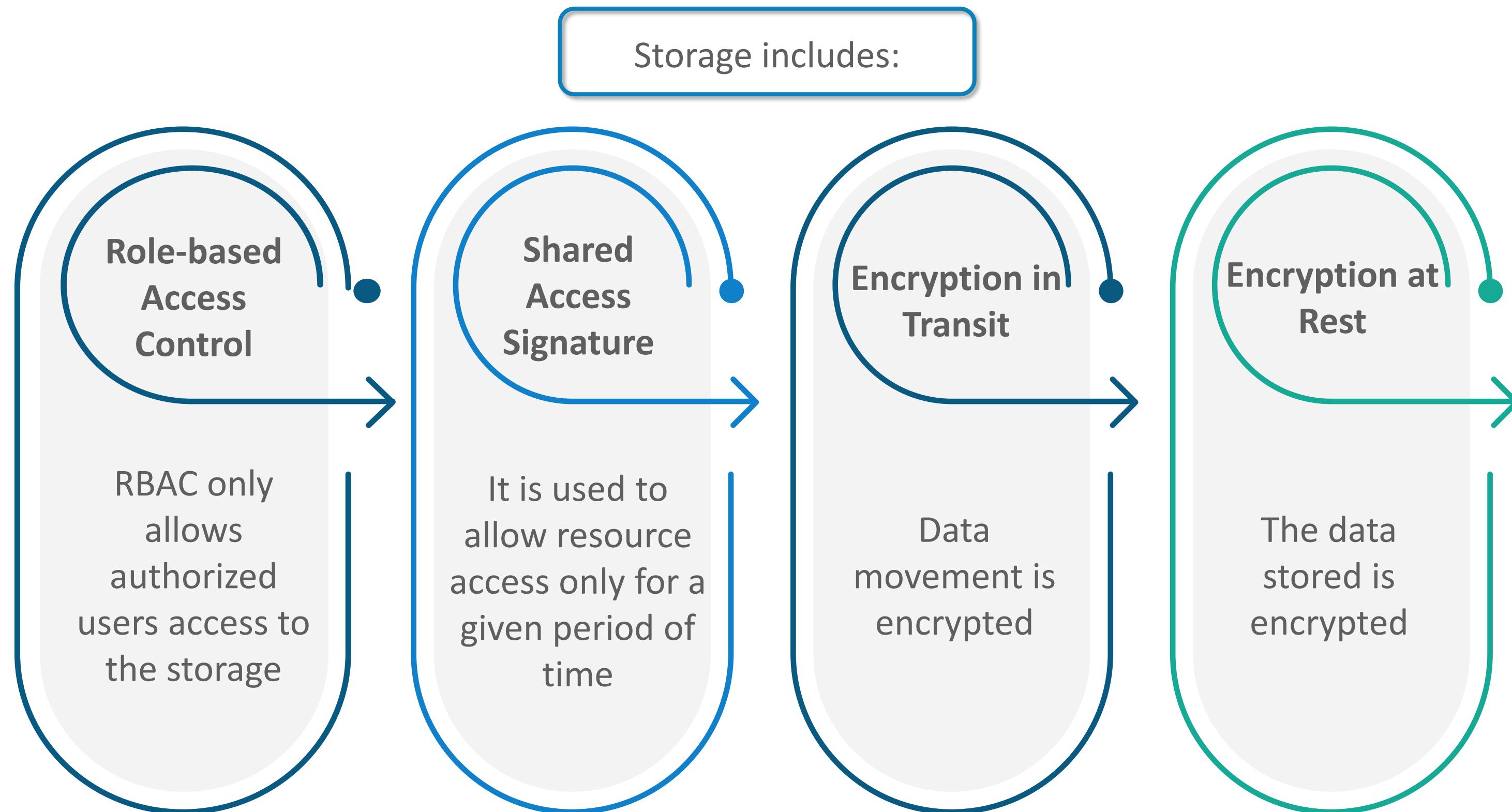
Web Server Log

- 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

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

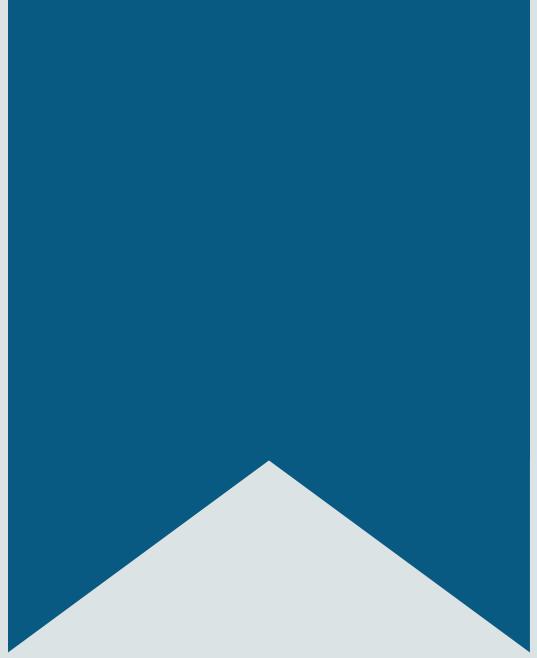
Apart from a user password, it mandates another mode of authentication such as OTP, phone-call

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

Secure Development Process

As part of the software development process, these best practices should be adhered to for the Secure development process:

01

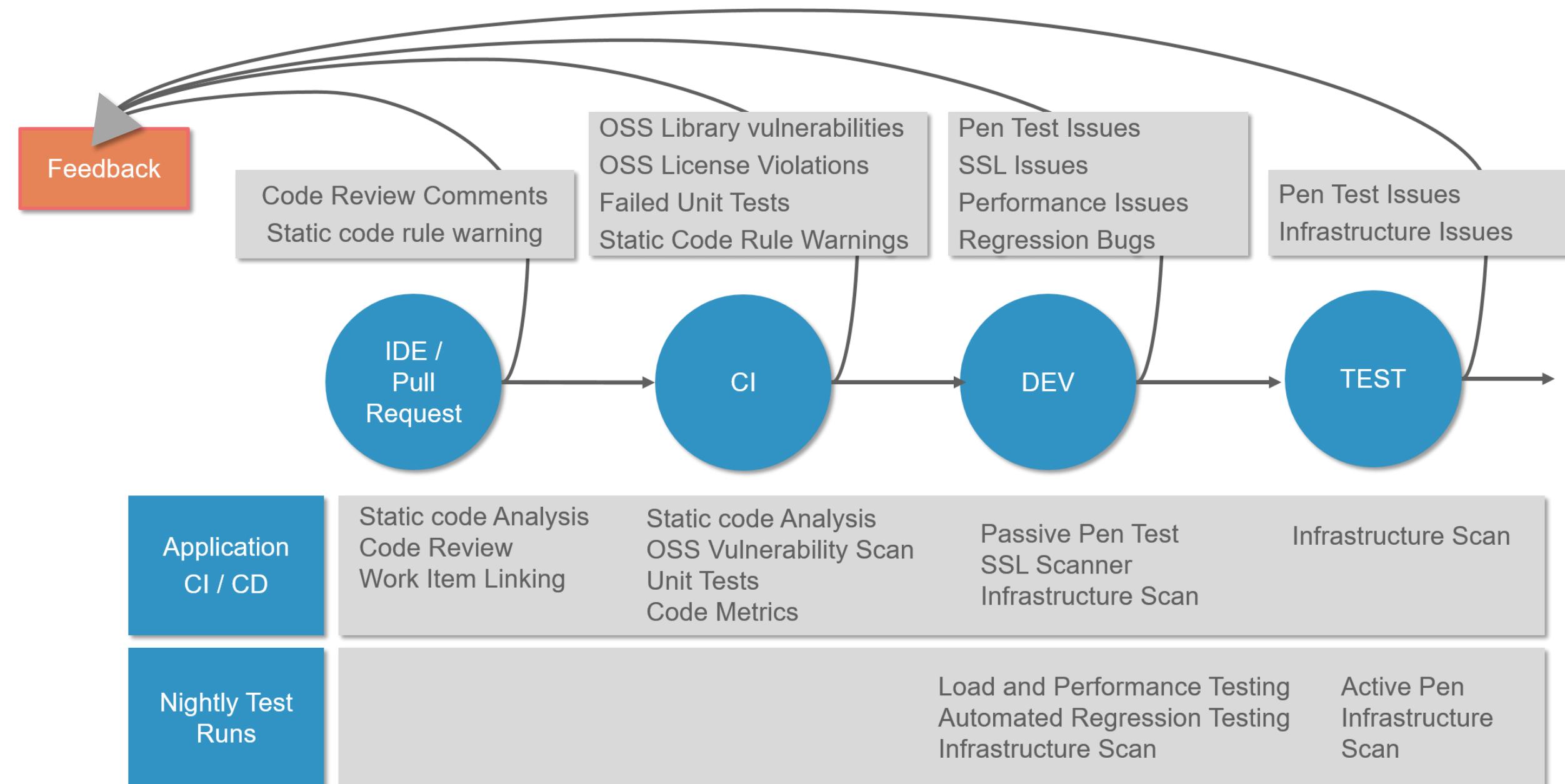
Security should be implemented as part of CI/CD deployment

02

All the security-related aspects should be integrated before deployment. This process is known as DevSecOps

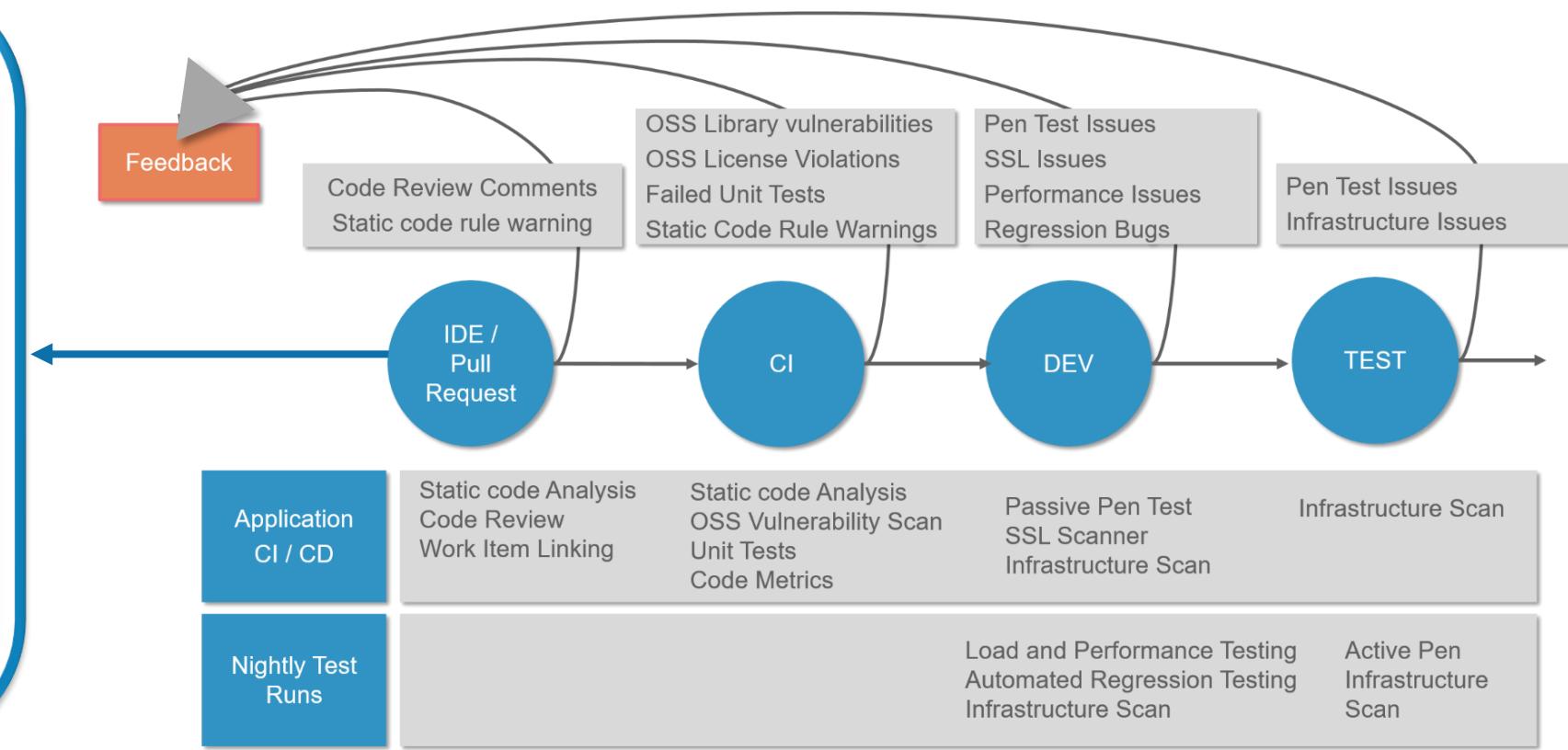
Implementing Security in CI/CD Pipeline

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



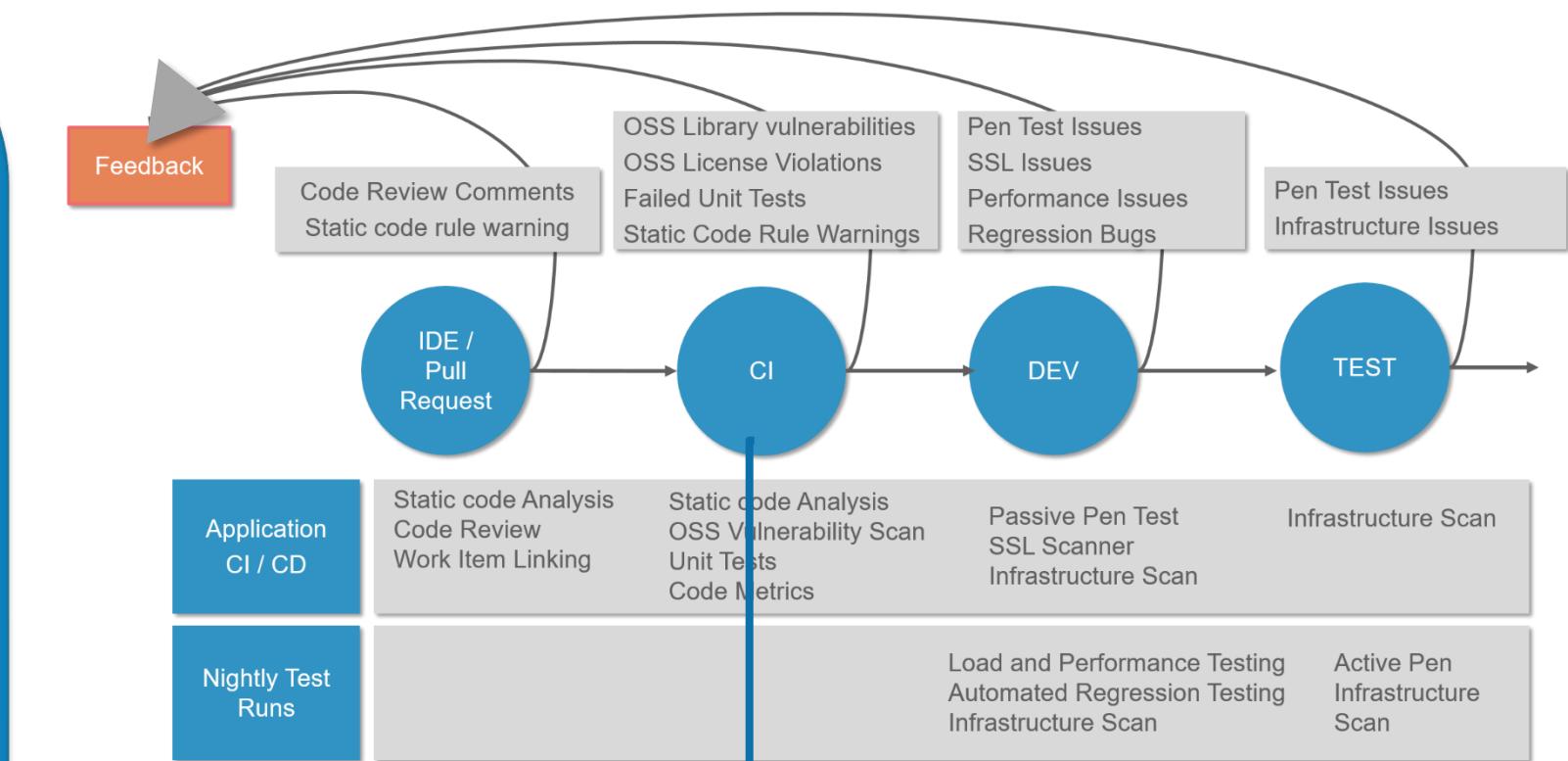
IDE/Pull Request

- 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



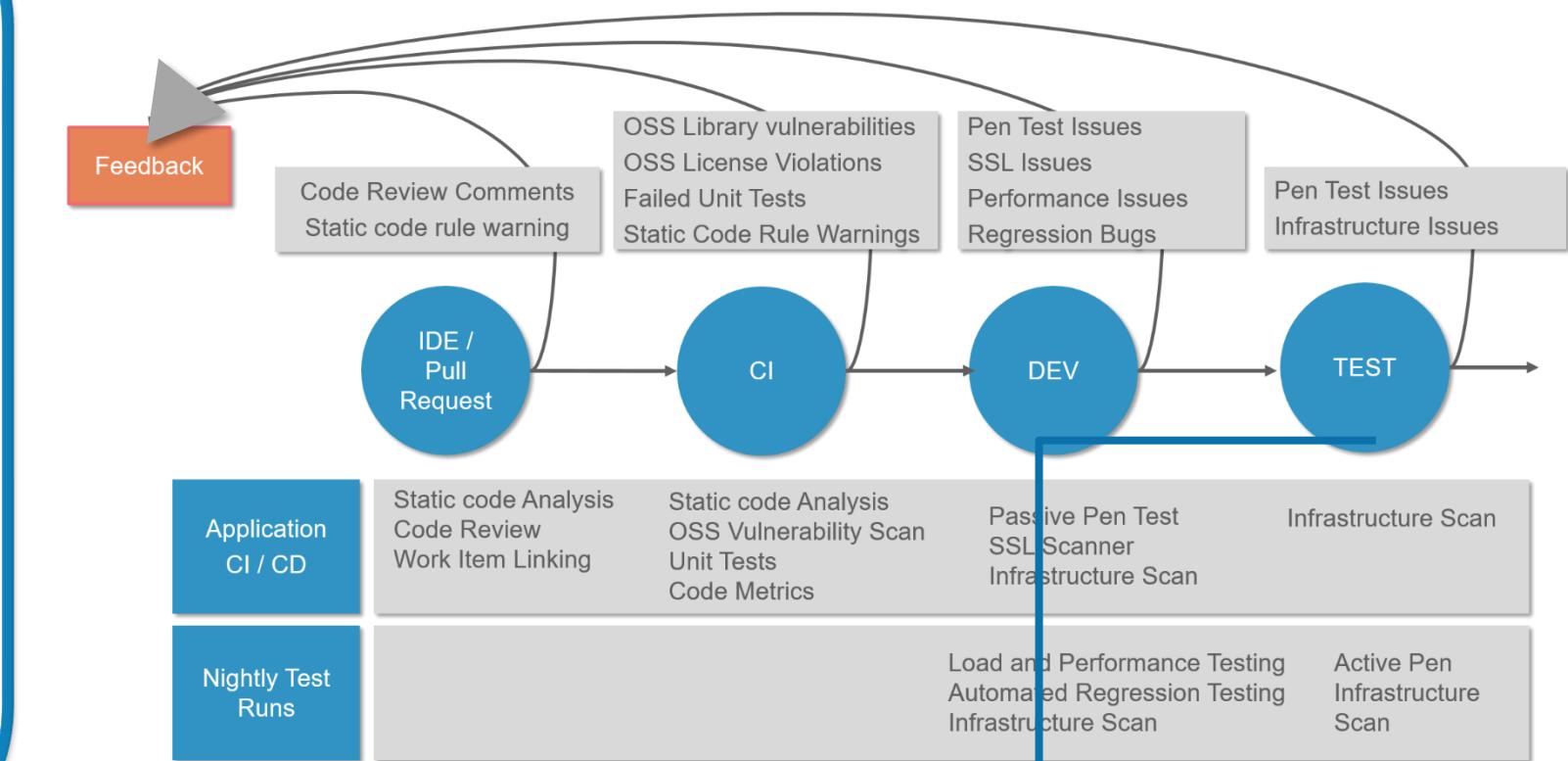
CI (Continuous Integration)

- 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



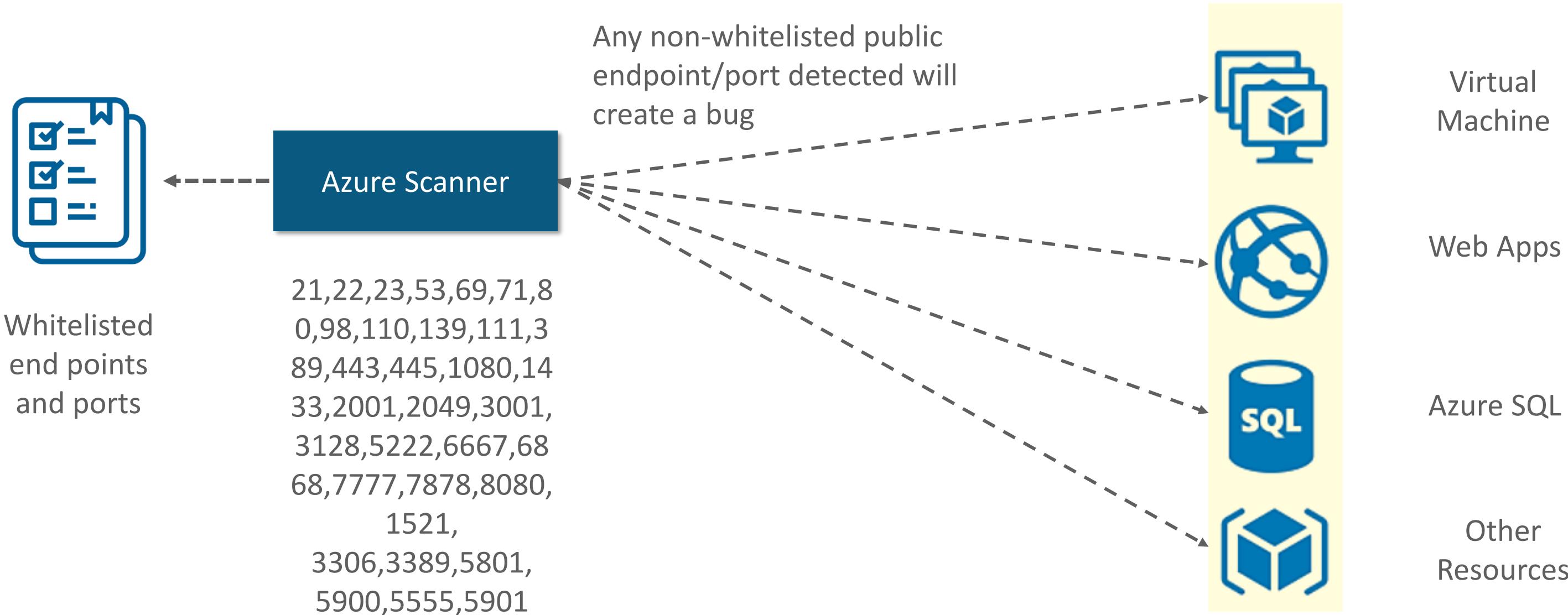
Validating Infrastructure Security

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

Azure Key Vault

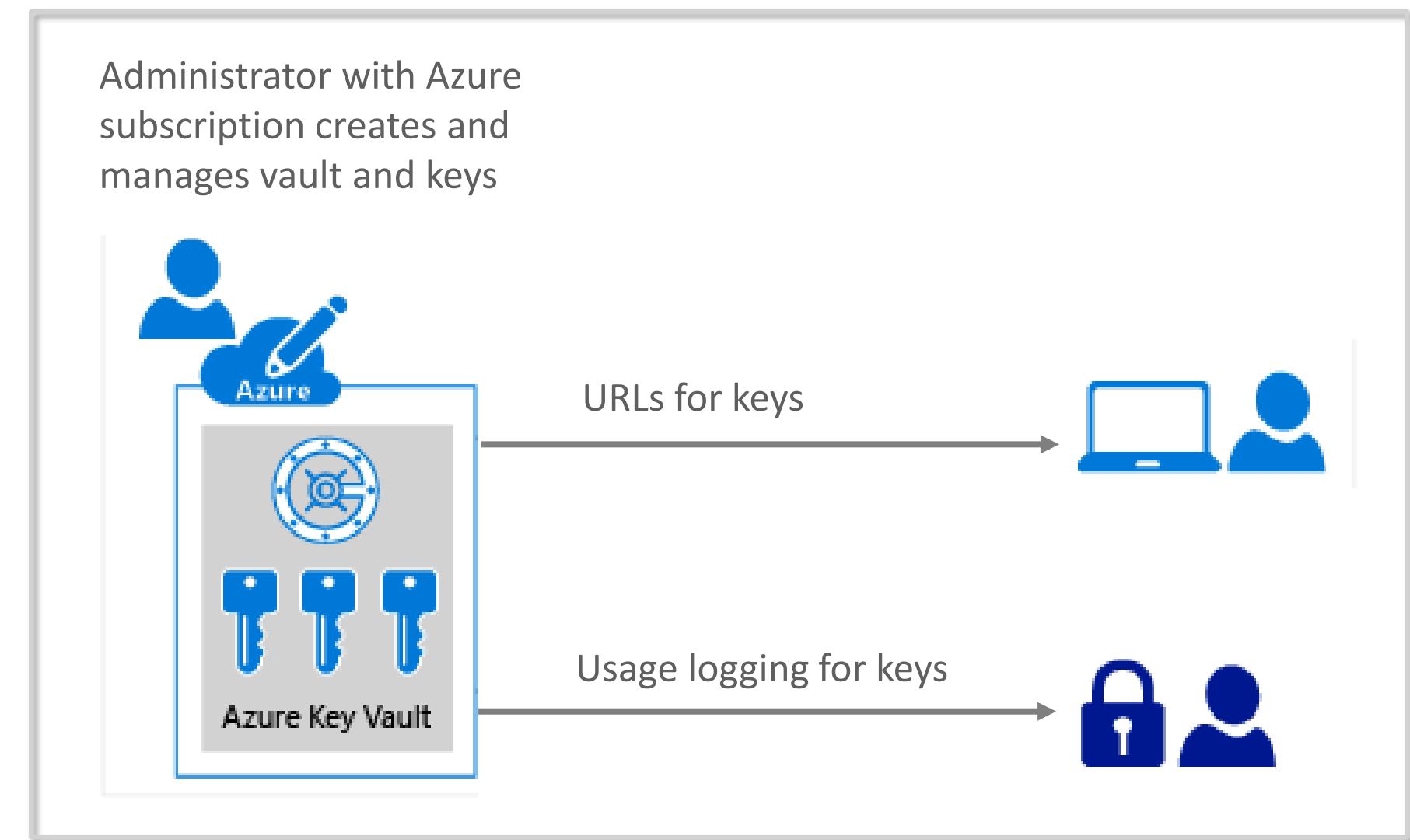
The application depends on configuration data for many of the runtime properties in the configuration file, the data connection strings, certificate, etc.



- 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



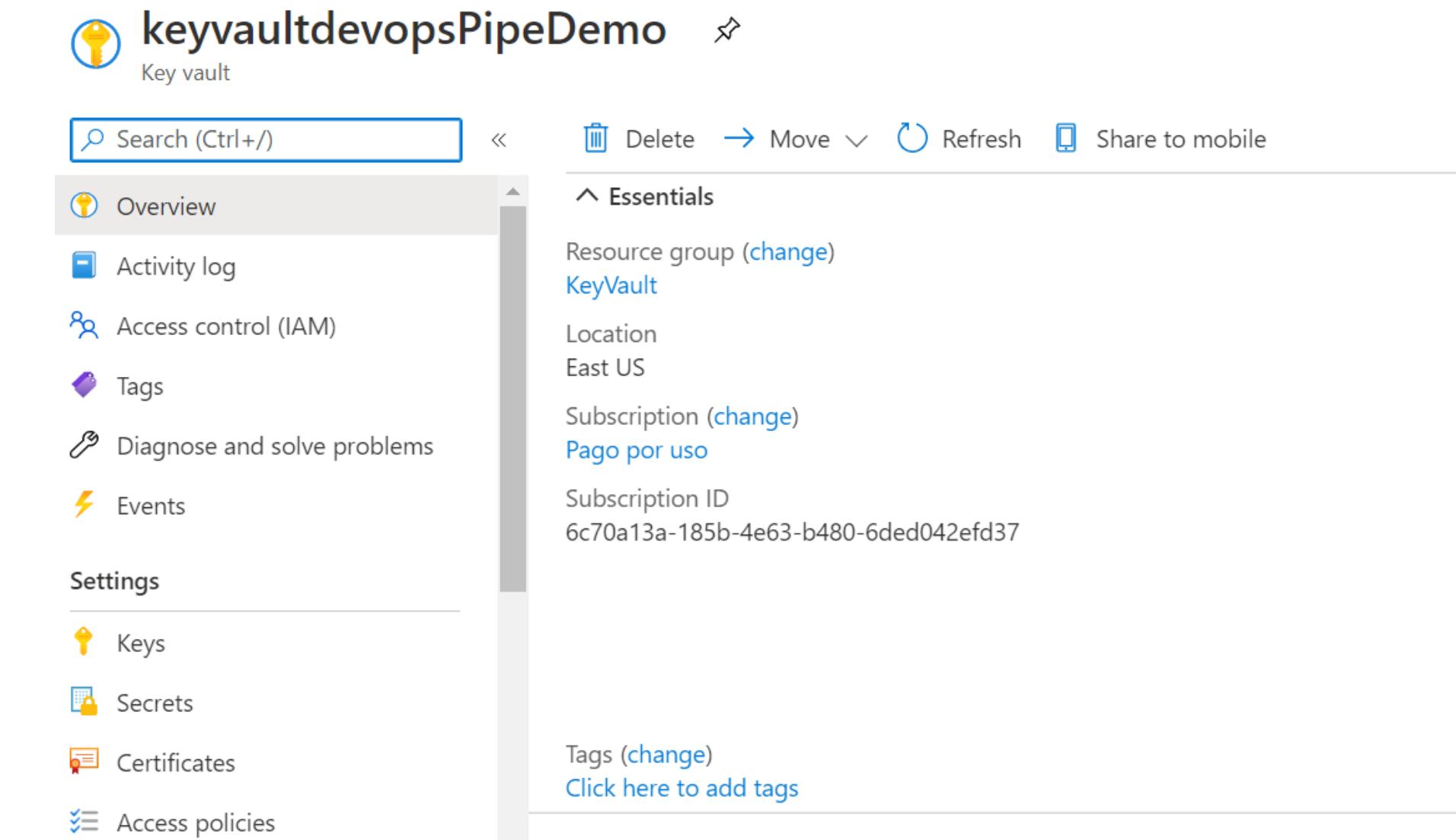
Configuring Secret, Key, and Certificate

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





Managing Security and Compliance in a Pipeline

Security and Compliance

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



Code Quality



Securing
third Party
Software



Access to Right
Stakeholders

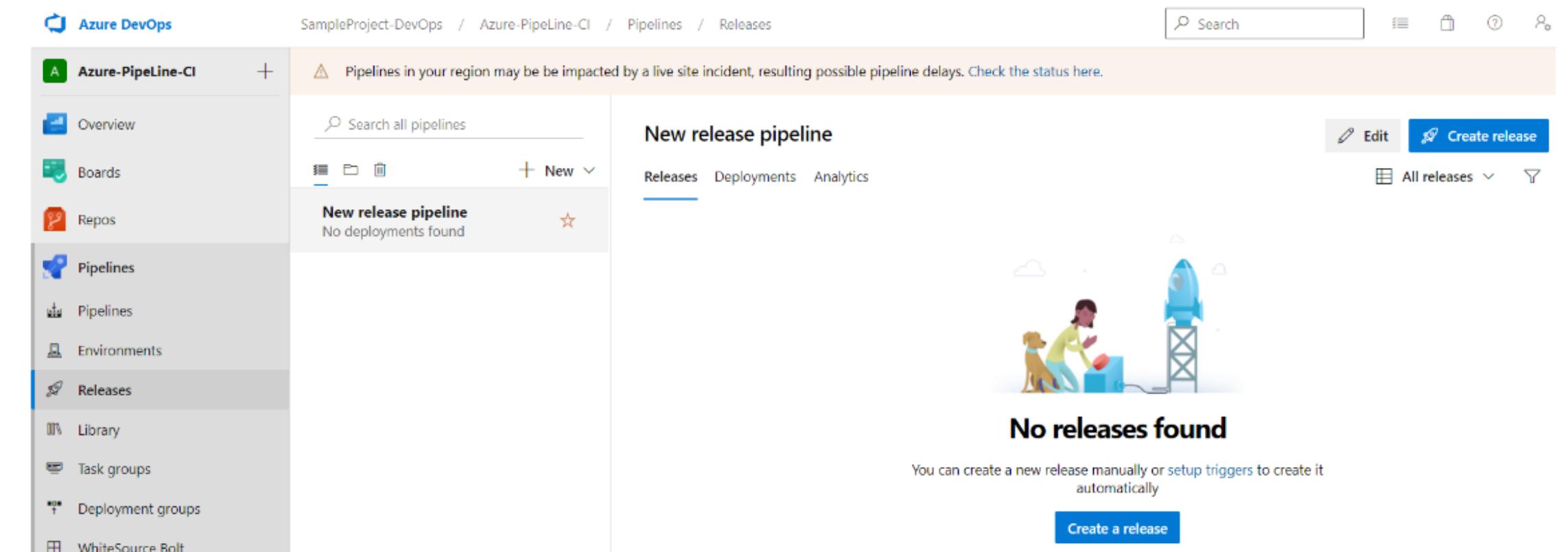
Implementing Security and Compliance

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

Go to Azure DevOps

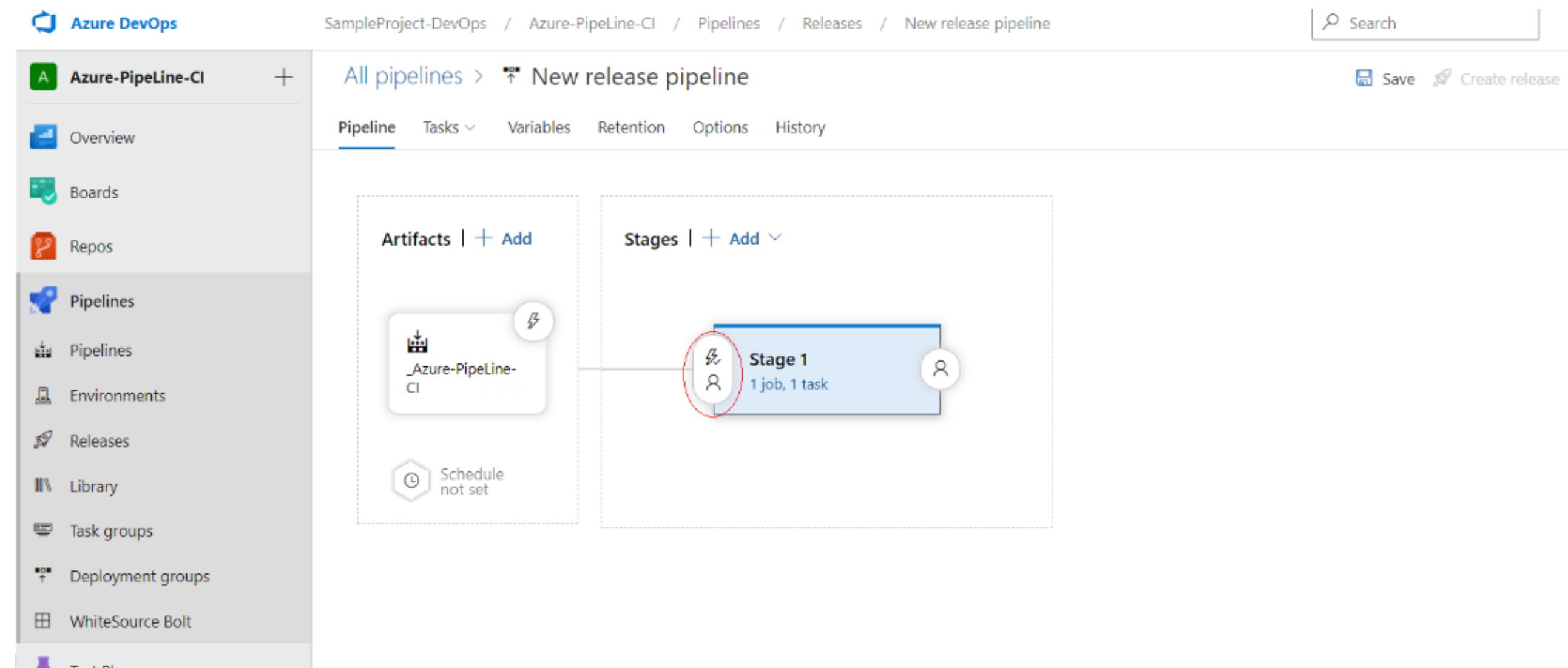
Go to any working project

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



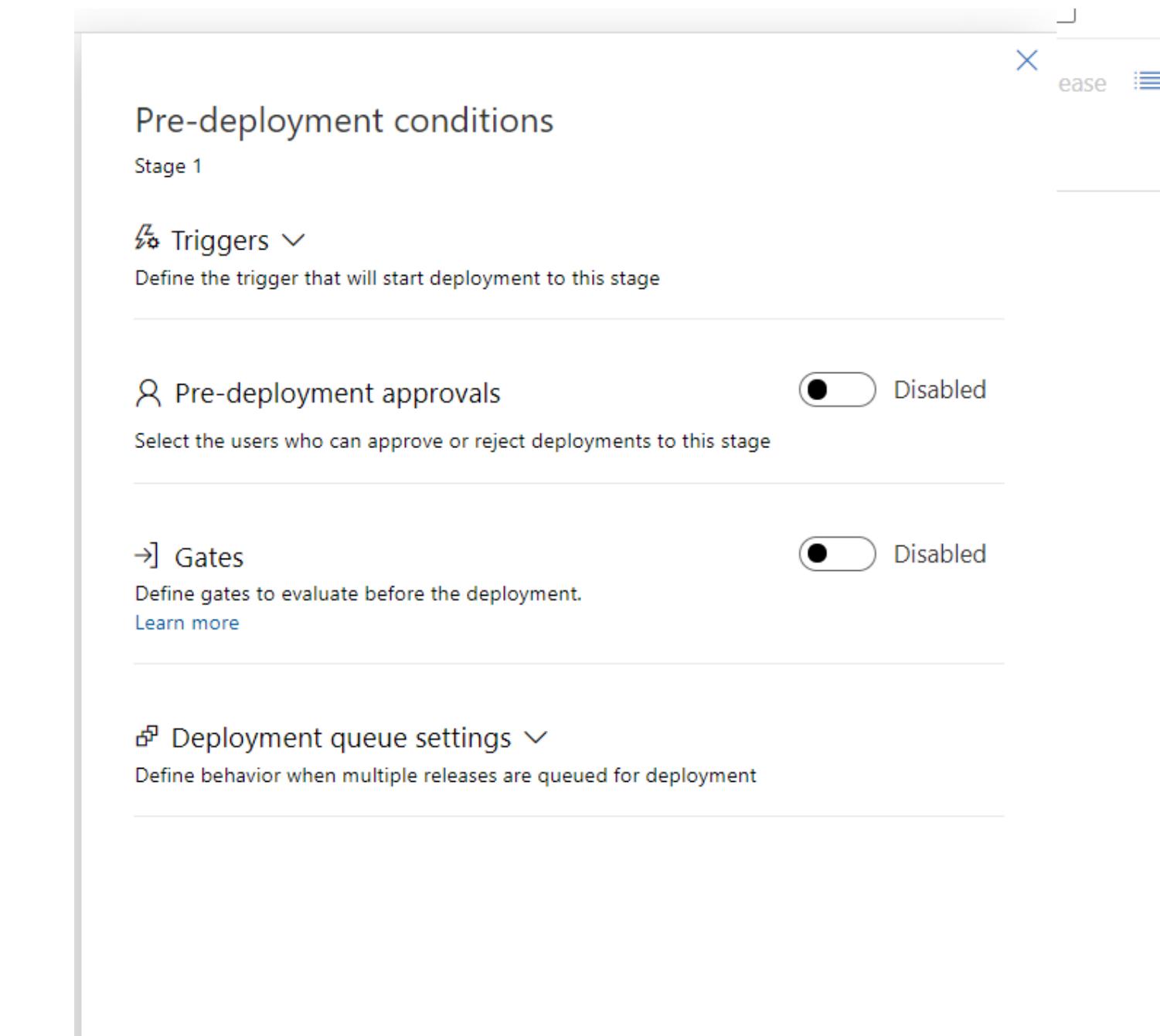
Implementing Security and Compliance (Cont.)

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



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

The screenshot shows the 'Pre-deployment conditions' section of an Azure DevOps pipeline configuration. It is set to 'Stage 1'. A dropdown menu is open under the 'Triggers' section, showing the following options:

- Pre-deployment a [Check Azure Policy compliance] Security and compliance assessment for Azure Policy
- [Invoke Azure Function] Invoke an Azure Function
- [Invoke REST API] Invoke a REST API as a part of your pipeline.
- [Query Azure Monitor alerts] Observe the configured Azure Monitor rules for active alerts
- [Query work items] Execute a work item query and check the number of items returned

Below the triggers, there is a 'Gates' section with a delay of 5 minutes. The deployment queue settings are also visible at the bottom.

Adding Compliance as a Part of Release Pipeline

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

The screenshot shows the 'New release pipeline' configuration screen in Azure DevOps. On the left, the pipeline structure is visible with 'Stage 1' containing 'Run on agent' and 'Deploy Azure App Service'. A search bar at the top right contains the text 'white'. In the center, the 'Tasks' tab is selected, showing the 'Add tasks' section. A card for 'WhiteSource Bolt' is displayed, featuring its icon, name, description ('Detect & fix security vulnerabilities, problematic open source licenses.'), and an 'Add' button. Below this, the 'Marketplace' section lists two more entries: 'WhiteSource Bolt' and 'WhiteSource for Azure DevOps Server', both with their respective icons and brief descriptions.



Managing Code Quality

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.)

The screenshot shows the Azure DevOps Pipelines interface for a project named "SampleProject-DevOps". The pipeline is titled "New release pipeline". On the left, there's a sidebar with options like Overview, Boards, Repos, Pipelines (which is selected), Environments, Releases, Library, Task groups, Deployment groups, WhiteSource Bolt, and Test Plans. The main area shows a "Stage 1" deployment process with two tasks: "Run on agent" and "Deploy Azure App Service". Below these tasks, there's a search bar with "sonarq" typed in, and a list of Marketplace items related to SonarQube, including "SonarQube for MSBuild - Begin Analysis" and "SonarQube for MSBuild - End Analysis". A "Marketplace" section also displays the "SonarQube" extension, which is described as detecting bugs, vulnerabilities, and code smells across project branches and pull requests, with 51,115 installs.

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

Code Quality: SonarCloud



The main features of SonarCloud are:

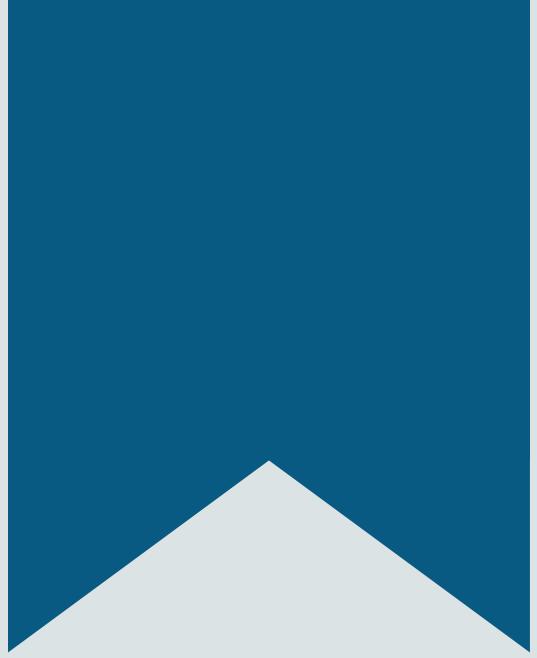
It supports 16 languages, including Java, JS, C#, C/C++, Objective-C, among others

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

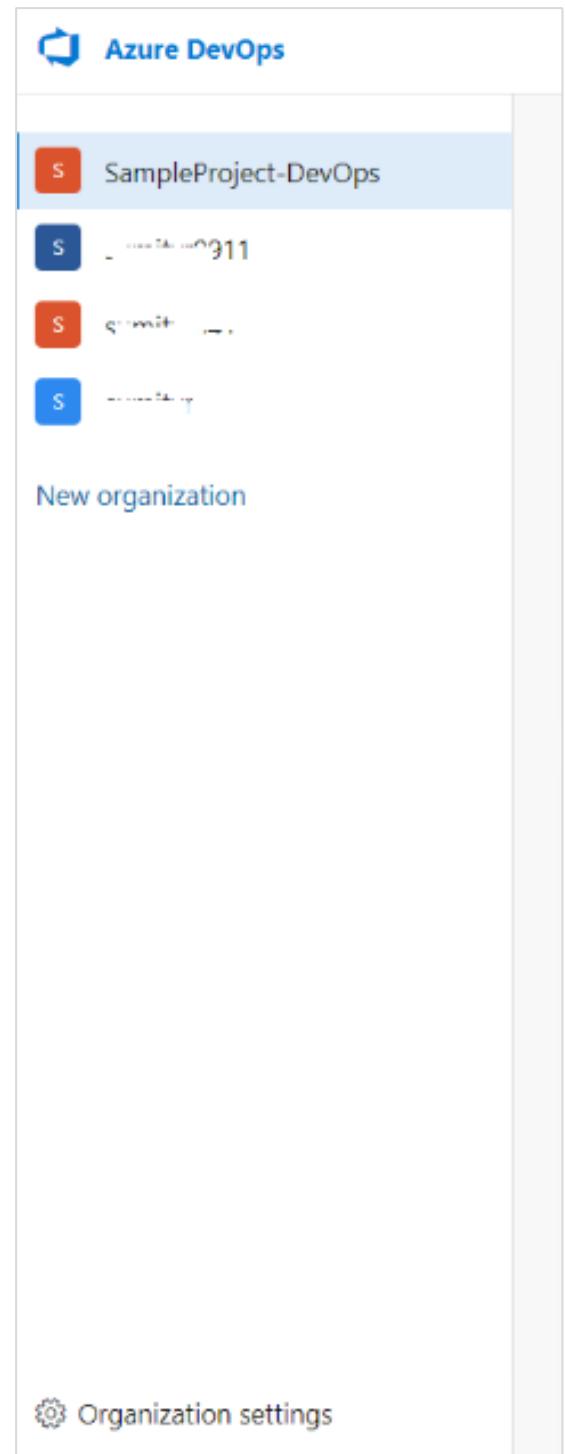
It is fast and scalable



Managing Security Policies

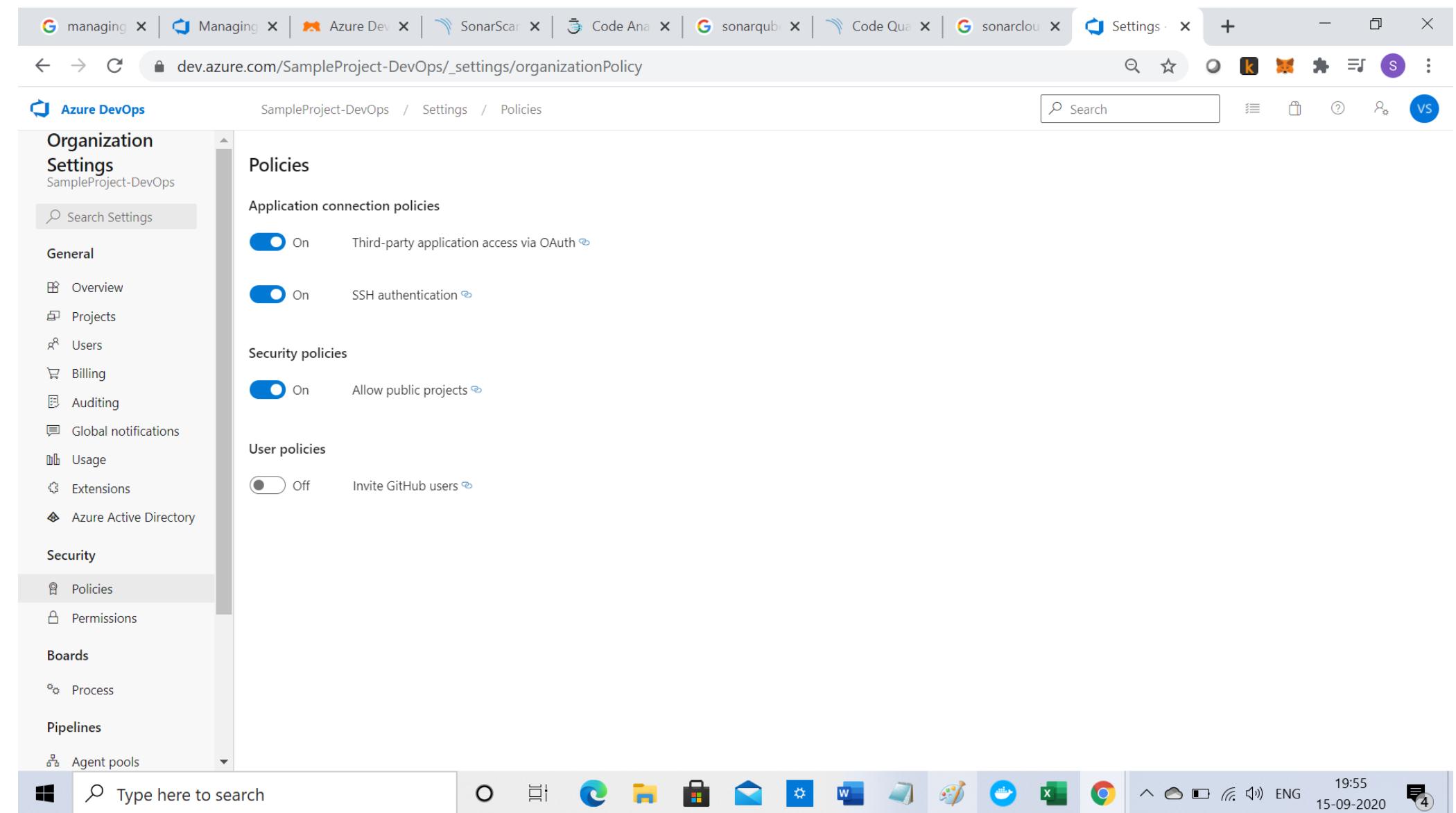
Configuring Security Policies

- 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.

The screenshot shows the 'Permissions' section within the 'Organization Settings' of a project collection named 'SampleProject-DevOps'. The left sidebar includes 'General' (Overview, Projects, Users, Billing, Auditing, Global notifications, Usage, Extensions, Azure Active Directory), 'Security' (Policies, Permissions - selected), 'Boards', 'Process', and 'Pipelines'. The main area displays a table of application groups:

Name	Description	Members
Project Collection Administrators	Members of this application group can perform all privileged operations on the Team Project Collection.	2 (PA, VS)
Project Collection Build Administrators	Members of this group should include accounts for people who should be able to administer the build resources.	0
Project Collection Build Service Accounts	Members of this group should include the service accounts used by the build services set up for this project collection.	0
Project Collection Proxy Service Accounts	This group should only include service accounts used by proxies set up for this team project collection.	0
Project Collection Service Accounts	This application group contains Team Project Collection service accounts.	1
Project Collection Test Service Accounts	Members of this group should include the service accounts used by the test controllers set up for this project collection.	0
(...)	This application group contains all users and groups that have access to the Team	27

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



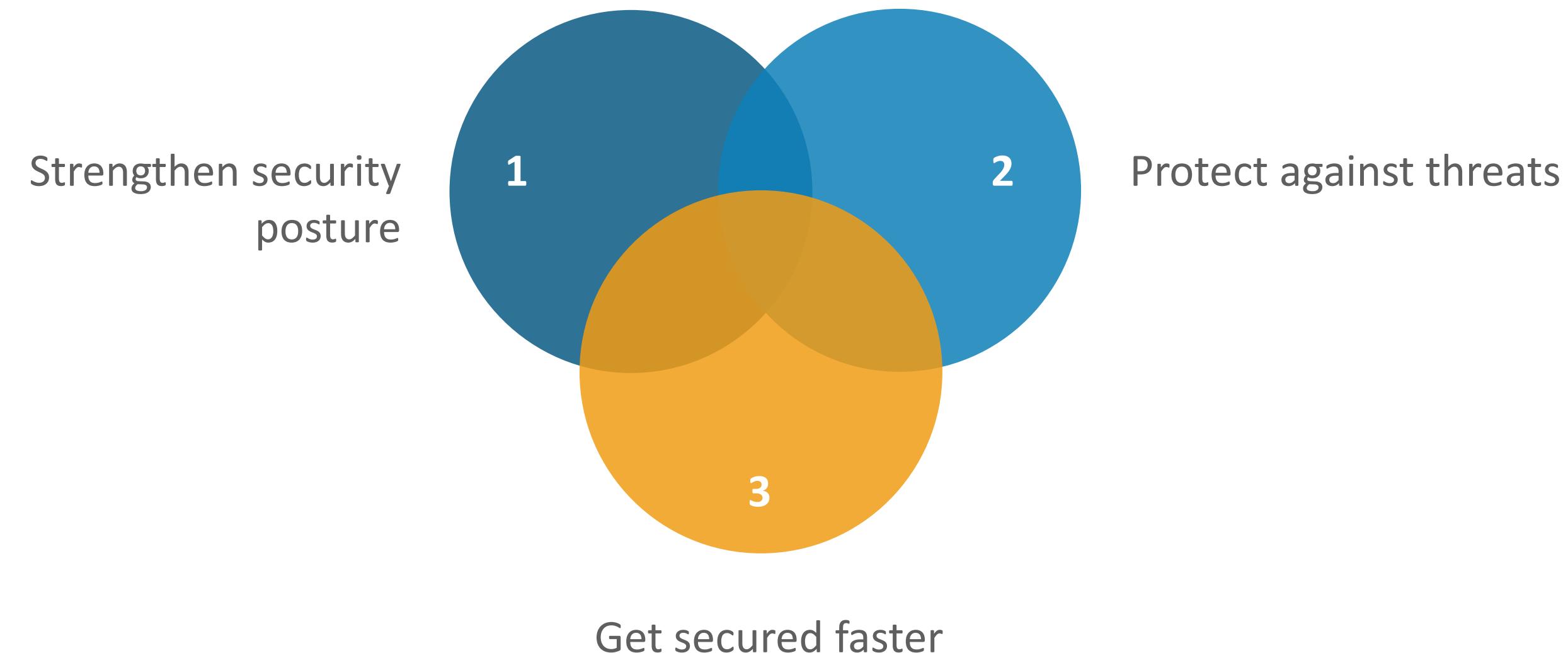
Azure Security Center

Azure Security Center can be enabled in the Azure Portal

The screenshot shows the 'Getting started' section of the Azure Security Center. At the top, there's a breadcrumb navigation: Home > Getting started > Security Center. Below that is the title 'Security Center | Getting started' with a subtitle 'Showing subscription 'Pago por uso''. A search bar labeled 'Search (Ctrl+/' is on the left, and an 'Upgrade' button is on the right. The main content area has several sections: 'Overview' (with a shield icon), 'Getting started' (which is selected and highlighted in grey), 'Pricing & settings', 'Community', 'Workflow automation', and 'Inventory (Preview)'. On the right side, there's a vertical sidebar with sections for 'POLICY & COMPLIANCE' (Coverage, Secure Score, Security policy, Regulatory compliance) and 'RESOURCE SECURITY HYGIENE' (Recommendations). A circular icon with a shield and a checkmark is also visible.

Azure Security Center (Cont.)

Azure security center provides you with the tools to:



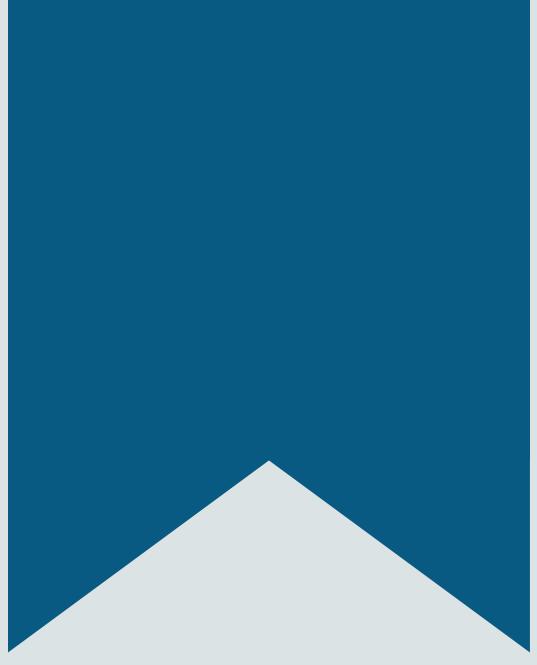
Continuous Assessment

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

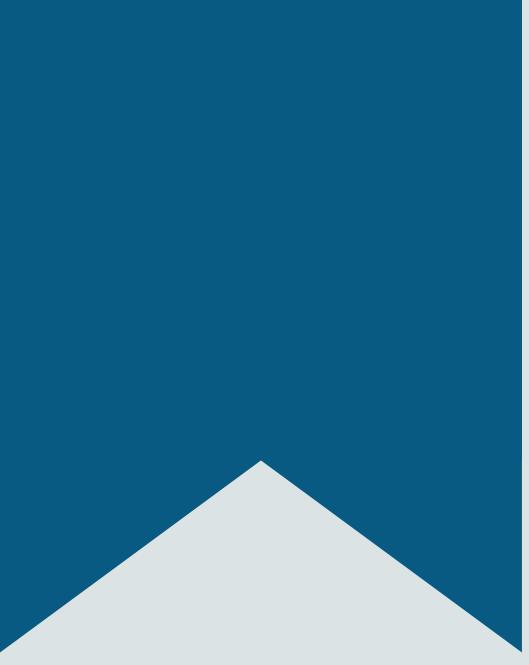




Demo: Manage Technical Debt with Azure DevOps and SonarCloud

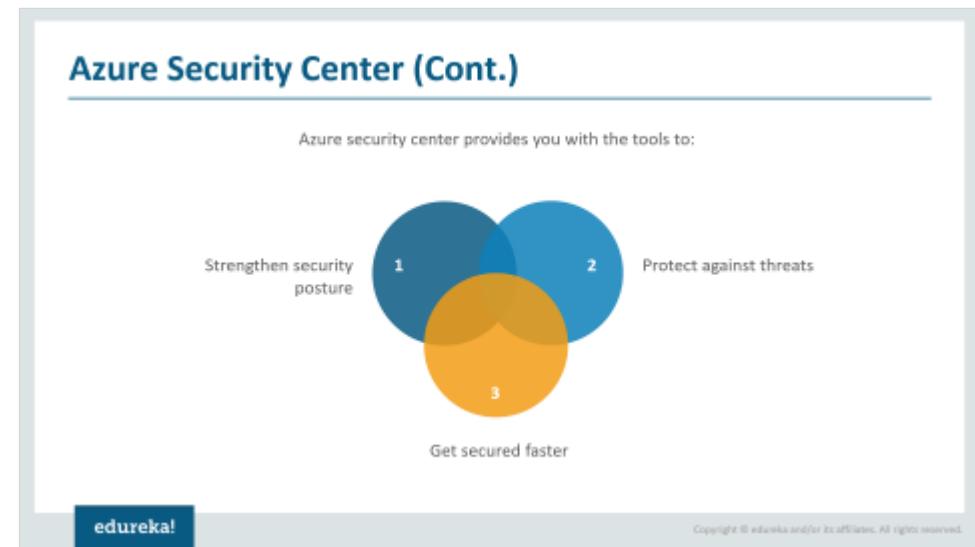
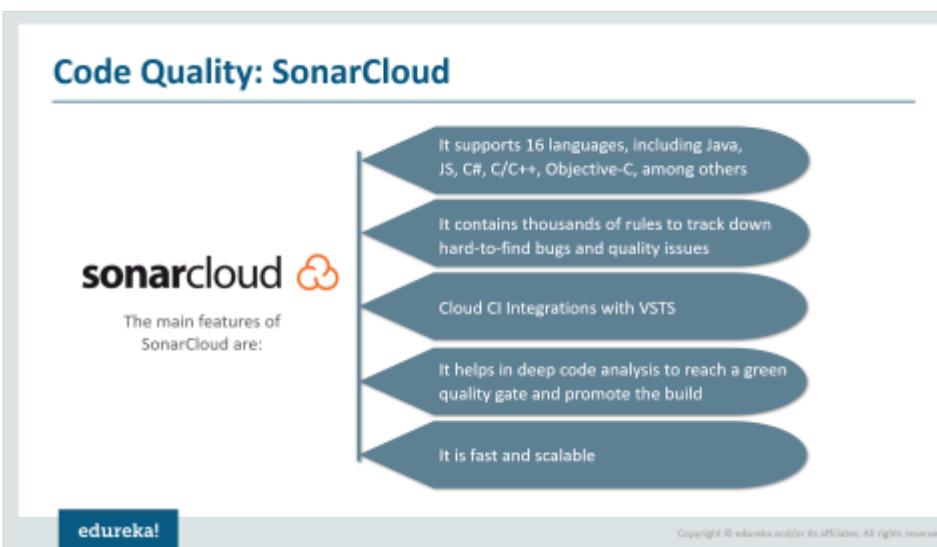
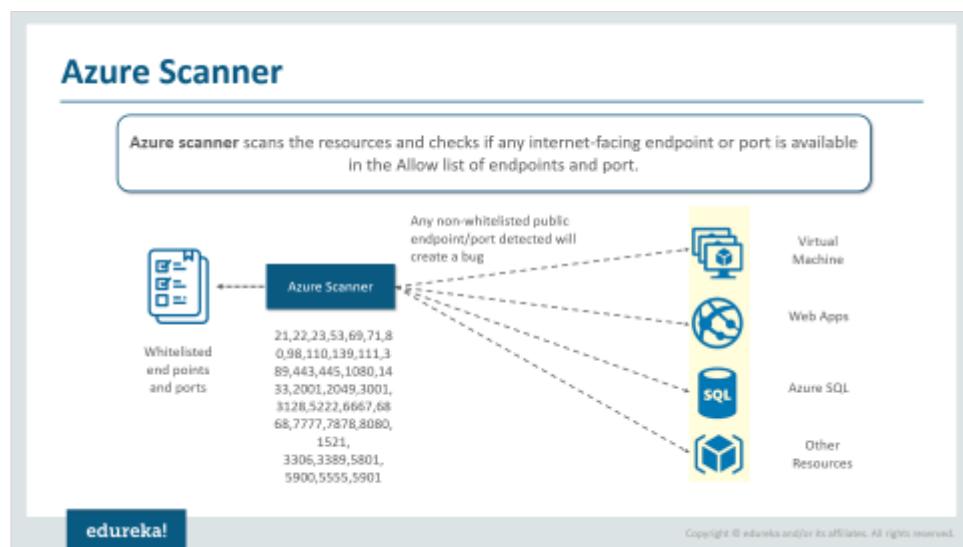
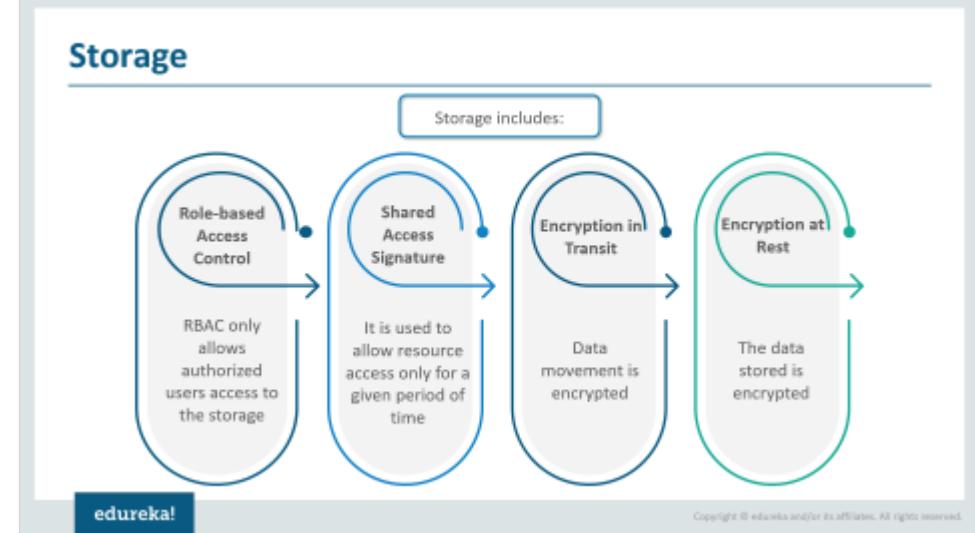
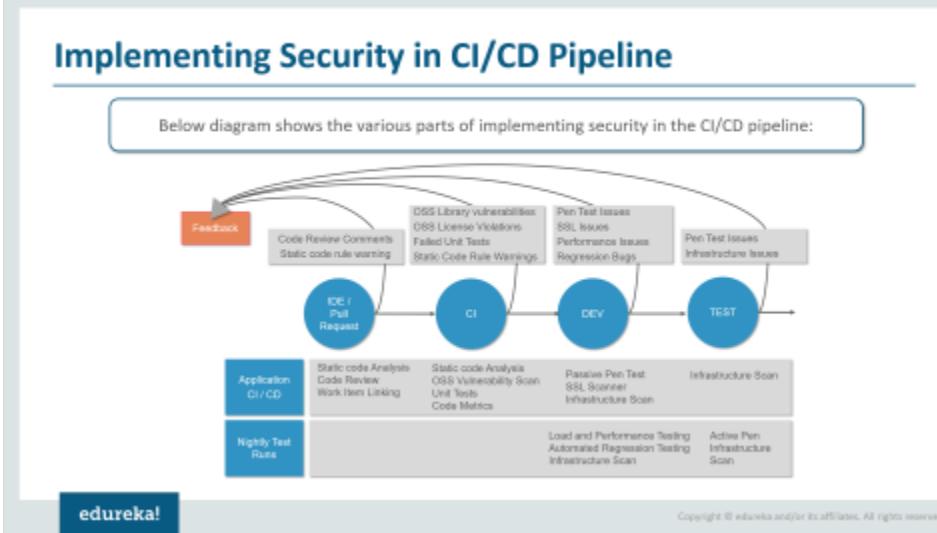


Demo: Integrate Azure Key Vault with Azure DevOps



Demo: Implement Security and Compliance in an Azure DevOps Pipeline

Summary



Questions

FEEDBACK



Survey



Ideas



Ratings



Comments



Suggestions



Likes

Thank You



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