






Fortifying SDLC on Azure with Defender for DevOps

Discover and evaluate the application security risk posture on Azure by conducting a maturity assessment leveraging Defender for DevOps....

Engagement Highlights

-  Discover security risk and maturity score of application hosted on Azure and multi-cloud
-  Scan for vulnerabilities with code, app configuration, OSS component and prioritize remediation effort
-  Reduce the attack surface area for applications
-  Discover benefits and capabilities of Wipro's Application Security Framework & Microsoft Defender for DevOps.
-  Develop defined next steps based on your needs and objectives.

Application layers have been a focal point of entry for adversaries looking to compromise mission-critical organizational assets. They contain critical customer, financial, and product data. A breach of these systems may lead to data loss, major business disruption, reputational loss, legal implications, and direct revenue impact. Wipro's approach is to perform a maturity assessment on the application technology stake from a people, process, and technology standpoint, followed by a recommendation roadmap to secure application code, configuration, and CI/CD infrastructure. The Wipro Application Security Assessment Framework refers to industry standard frameworks like OWASP SAMM and DSOMM while performing maturity scoring.

The assessment seeks to offer an "AS-IS" risk posture as well as to detect security gaps between existing risk and target states. The Wipro application security lifecycle assessment report covers results and recommendations for safeguarding Azure and multi-cloud applications. During the assessment phase, Azure Defender for DevOps will be used to gain code, configuration, and CI/CD infrastructure-level vulnerability insights. The assessment duration varies based on the number of applications in scope.

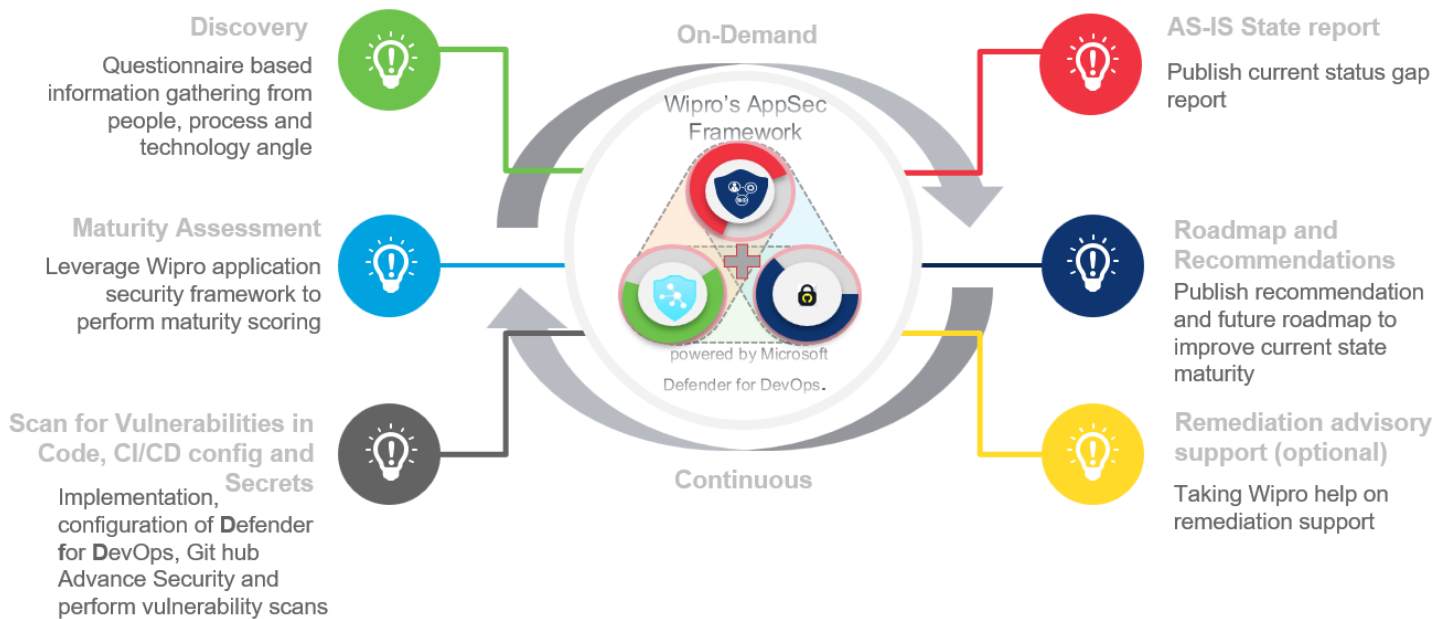
Discover, assess, and remediate applications code security risks through Wipro's SDLC maturity framework powered by Defender for DevOps.

Microsoft provides technologies like Defender for DevOps and GitHub Advanced Security to assist developers and organizations in securing their software development lifecycle on Microsoft and multiple clouds.

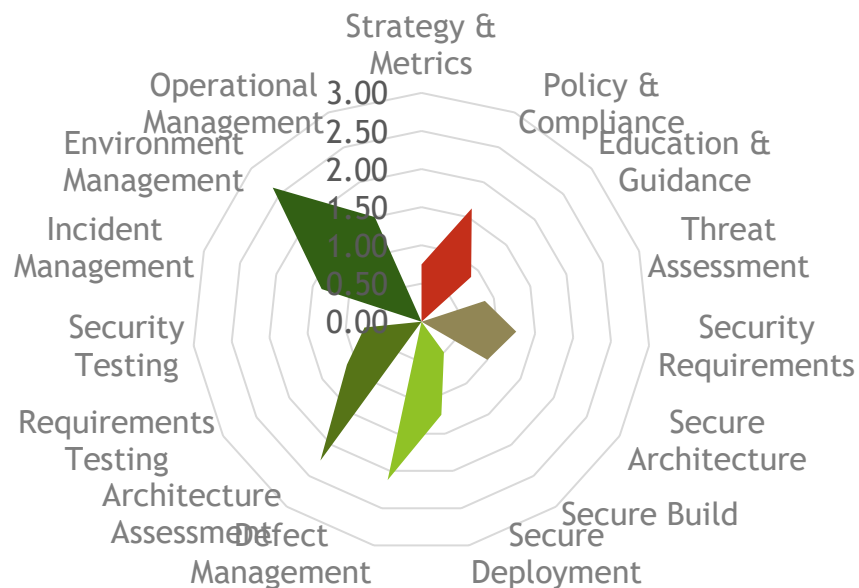
With a risk-based perspective, the Wipro Application Security Framework offers the ability to conduct current state analyses, recommend security controls, and tailor domains and sub-domains to correspond with organizational strategic, operational, and tactical goals.

What to expect:

During this engagement, we'll partner with you to strengthen your organization's approach to fortify application security landscape on Azure and multi-cloud. We'll help you better understand potential application security gaps and how to prioritize and mitigate potential attacks:



A glimpse of sample maturity score



The diagram depicts the application security maturity scoring across various domains and sub-domains within the scale of 0 to 3. This helps prioritize security control implementation, improving security posture and adherence regulatory requirements.