Service Description

WIZ SPRINTS



TABLE OF CONTENTS

1. ENGAGEMENT OVERVIEW 3

2. SPRINT SCOPE AND CATEGORIES 3

2.1 Rapid Onboarding 3

2.2 Advanced Deployments 3-4

2.3 Cloud Security Posture 4

2.4 Migrations & Integrations 4

2.5 Data & AI Security 4

2.6 Scripting and Custom Reporting 4-5

2.7 Secure Code Development 5

2.8 Cloud Detection & Response (CDR) 5

3. ENGAGEMENT ACTIVITIES 6

3.1 Discovery Workshop 6

3.2 Sprint Planning Workshop 6

3.3 Sprint Execution 6

3.4 Knowledge Transfer 6

3.5 Engagement Close Out 6-7

4. ROLES AND RESPONSIBILITIES 7

4.1 Wiz Roles 7

4.2 Assumptions and Responsibilities 7-8

Capitalized terms not defined in this Service Description will have the meanings provided in the Professional Services Addendum, the Sprints Rider, or the Agreement, as applicable.

1. Engagement Overview

Wiz Sprint services are designed for flexibility to address customer needs during the adoption of the Wiz Platform. Sprints will be planned and categorized by the Project Manager to ensure proper technical resource availability.

Engagement Timeline:

The anticipated duration of this engagement and basis for the number of Sprints purchased will be dependent on the needs of the customer.

2. Sprint Scope & Categories

During the scoping phase of a Sprint engagement, we will review a variety of potential areas of focus for the engagement. Depending on Customer's desired outcomes, Wiz will recommend an appropriate number of Sprint engagements to purchase to align with the objectives of the services engagement. Below is a summary of the various focus areas and common activities associated with each:

2.1 Rapid Onboarding

Insert brief description of this focus area or "type" (e.g. "Rapid Onboarding is the perfect solution for a customer who wants to accelerate their Time-to-Value with Wiz and fast-track their path to giving their organization the visibility they need to begin the journey of adopting Wiz across their organization.")

- Connect Wiz to SSO for authentication and authorization.
- Configure projects and role-based access controls.
- Set up and customize dashboards for visibility.
- Connect Wiz with cloud providers, Kubernetes, and container registries.
- Setup connection to notification and monitoring systems.

2.2 Advanced Deployments

- Architecture and unique Customer requirements review.
- Expert guidance on specific configurations for cloud solutions providers for Wiz

Outposts designs:

- Self-Managed Network
- Private Registry On-Prem
- Self-Managed Network with Private Registry
- Self-Managed Network with Proxy
- Gov Cloud
- Sovereign Cloud

- Fine tuning Wiz Outpost deployment(s) based on Customer's environment.
- Knowledge transfer of implemented design.

2.3 Cloud Security Posture

- Customize Wiz with tailored policies & frameworks.
- Expert guidance and implementation of graph controls.
- Creation of customer specific cloud configuration rules (CCR) and host configuration rules (HCR).
- Integration with ticketing and messaging systems.
- Creation of dashboards, projects, and overall project strategy.

2.4 Migrations & Integrations

- Current CNAPP or CSPM usage and rule evaluation.
- Conduct gap analysis of current rules and align security policies.
- Creation and validation of CCR, HCRs, and Graph Controls.

2.5 Data & AI Security

- DSPM and AISPM configuration and implementation.
- Creation of data, secret, and threat detection rules.
- Integration of DSPM and AISPM with ticketing and messaging systems.
- DSPM and AISPM dashboard creation.

2.6 Scripting and Custom Reporting

- Develop custom scripts to automate repetitive tasks within the Platform.
- Establish tooling for working with (e.g. extracting) data to integrate across existing critical workflows.

- Build data parsing mechanisms to achieve reporting enhancements.
- Create and implement bespoke reports for enhanced visibility.
- Curate customized Terraform modules using the Wiz provider to introduce lifecycle management practices across deployment components.

2.7 Secure Code Development

- Implementation and integration of version control systems (VCS).
- CI/CD pipeline review and integration.
- Implementation of admission controller.
- Creation of dashboards, custom policies, and reporting.
- Wiz CLI and IDE integration and how-to use overview workshop.
- Guidance on SBOM and SSC best practices.
- Integration with ticketing and messaging systems.

2.8 Cloud Detection and Response (CDR)

- Enable ingestion of CSP, IdP, VCS, and other SaaS Cloud Logs/Events to accelerate investigation and troubleshooting activities.
- Install Runtime Sensors across CSP and On-prem environments.
    - Consider leveraging Sensor Workload Scanner features for On-Prem.
- Configure and customize Wiz's Cloud Detection & Response (CDR) features (AI Remediation, Forensics Package Collections, Forensics Accounts).
- Implement custom Threat Detection Rules for real-time monitoring.
- Analyze Current Threat Detections and implement any necessary Threat Detection Ignore Rules.
- Associate Threat Detections with Controls to produce additional correlations. Create tailored automated workflows for incident response.
- Create Automation Rules to integrate with native SOC tools and workflows.
    - Assessment of current CDR workflows.
- Tune and configure capabilities for risk and behavior analysis.
- Consolidate cloud signals into a single, actionable timeline.
- Overview and best practices for remediation and response functionality within Wiz.
- Creation of custom dashboards, Ignore Rules for Threat Detection Findings, and reporting.
- Integration with ticketing and messaging systems.

3. Engagement Activities

3.1 *Discovery Workshop* (estimated duration is no more than one [1] Business Day)

The Discovery Workshop takes place in advance of the first Sprint. The Discovery Workshop will familiarize Wiz Personnel with the environment, set goals for the Sprint Planning Workshop, identify the Customer systems and people that Wiz Personnel will be provided access to during the Sprint engagement, and cover key topics such as ticketing processes, security tools, access control, regulatory requirements, external integrations, product goals, risks, and the Deployment Workbook review.

3.2 *Sprint Planning Workshop* (estimated duration is one [1] Business Day per Sprint)

The Sprint Planning Workshop will provide insights into the Customer's environment and help populate the Deployment Workbook to create user stories for the Sprint Backlog. Key stakeholders from Wiz and the Customer will outline tasks to prepare for upcoming Sprints. The Sprint Planning Workshop will identify user stories, tasks, and sub-tasks to achieve the goals, determine required testing for the Engagement Close Out, and outline additional configuration.

3.3 *Sprint Execution (duration varies)*

During Sprint Execution, Wiz and the Customer will work through the Sprint Backlog.

3.4 Knowledge Transfer (estimated duration is eight [8] Business Hours over a total of one [1] Business Day)

Knowledge transfer activities can be added to the Sprint Backlog and prioritized by Customer's designated Product Owner. At the end of the Sprint engagement, if additional knowledge transfer is needed, Wiz Personnel can provide a knowledge transfer and hand-off session on the design, integrations, and Platform for up to ten (10) Customer team members. This will occur at the conclusion of the final Sprint in the Sprint engagement but prior to the Professional Services End Date as set forth in the applicable Order..

3.5 *Engagement Close Out* (estimated duration is two [2] Business Hours over a total of one [1] Business Day)

During Engagement Close Out, Wiz will provide a final set of Deliverables (as applicable) and demonstrate to Customer through testing which portions of the Sprint Backlog have been completed by Wiz during the Sprint Execution phase and conduct a Sprint engagement retrospective.

The schedule and logistics of the Sprint engagement will be agreed upon during the Discovery Workshop and will be adhered to throughout the engagement. The parties will define:

1. Working Hours
2. Systems Access
3. Identification of Customer's Product Owner

4. Roles and Responsibilities

4.1 Wiz Roles

The following roles will be involved in this effort from Wiz:

Advanced Delivery Architect

- Leads requirements gathering, use case discovery, and design initiatives.
- Deploy and configure the Wiz platform and components that are a part of the solution.
- Runs acceptance testing validation activities.
- Creates and delivers engagement documentation for the customer.

Project Manager

- Resource scheduling.
- Responsible for engagement structure.
- Creation and adoption of communication plan.
- Creation of project plan and related activities.
- Escalation triage and risk register.
- Final deliverables handoff.
- Handles planning and pre-engagement preparation.

4.2 Assumptions and Responsibilities

This section describes the responsibilities of Customers to Wiz regarding this engagement.

- Customer will actively participate in engagement and sprint review meetings.
- Customer will provide access to stakeholders that are required for this engagement as outlined below:
    - Security team
    - Platform team.
    - DevOps team.

    - Networking team.
    - Cloud Team.
- Customer has already purchased Wiz.
- Customer will provide the necessary information to complete the Deployment Workbook working with the Project Manager.
- Customer will provide Subject Matter Experts for the target platforms identified for Wiz integration.
- Customer will provide written confirmation upon completion of the engagement.
- Customer will provide access to the Wiz platform for the delivery team.
- Customer will coordinate communications with, and provide contacts for, all necessary third parties for engagement completion.
- Customer will deliver timely responses to requests for information, technical questions, and requested decisions pertaining to the engagement.
- Customer is responsible for designing and implementing all supporting infrastructure necessary for the deployment and integration of Wiz.
- Wiz delivery personnel will not configure, install, change, or mutate any systems outside of the Wiz platform to include features that can be performed from the Wiz platform that would configure, change, or mutate systems other than Wiz.