Network and Application Vulnerability Management Procedure

Beyond

August 2023

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC4.1, CC4.2, CC5.1, CC6.6, CC7.1, CC7.2, CC9.1

Table 2: Document history

Date	Comment
Aug 14 2023	Initial document
Aug 18 2023	Initial review

1 Purpose and Scope

a. The purpose of this procedure is to outline the steps in IT vulnerability management adhering to the Risk Assessment and Management Policy, to ensure that appropriate tools and methodologies are used to assess vulnerabilities in systems or applications, and to provide remediation.

b. This IT document, and all policies referenced herein, shall apply to all employees and contractors of Beyond (the "User(s)" or "you") who use, access, or otherwise employ, locally or remotely, Beyond IT Resources, whether individually controlled, shared, stand-alone, or networked.

2 Procedure Steps

a. *Discovery Phase* - Vulnerabilities are identified in IT Resources

b. *Prioritization Phase* - Discovered vulnerabilities and assets are reviewed, prioritized, and assessed using results from technical and risk reports

c. *Planning Phase* - Mitigation efforts are devised

d. *Remediation Phase* - Vulnerabilities are addressed

e. *Validation Phase* - Successful remediation measures are determined by subsequent analysis

3 Discovery Phase

a. The following tools may be used to assess systems or applications for vulnerabilities

   i. *Sonarqube* - For static code vulnerability detection, OWASP Top 10, SANS Top 25, security hotspots, taint analysis, quality gates, integrated and run within the CI/CD pipeline

   ii. *GCP Web Security Scanner* - For application vulnerability detection

   iii. *GCP Security Command Center* - For VPC/Network level and cloud services configuration vulnerability detection

   iv. *GCP Cloud IDS* - For real-time intrusion detection

4 Prioritization and planning Phases

a. Application and system owners should prioritize system or application vulnerabilities by the following methods:

   i. Address confirmed Sonarqube severity levels Blocker and Critical within 7 days of discovery, High within 30 days

ii. Address all findings in Web Security Scanner within 7 days

iii. Address all findings in GCP Security Command Center within 30 days

iv. Application and system owners must address content security policy configurations, application header configurations, or certificate configurations (e.g., self-signed, weak encryption) findings

v. If there are conflicting severity levels among the tools, consult the Information Security and Assurance for guidance on prioritization

5 Remediation Phase

a. System and application owners must do one or more of the following:

i. Deploy mitigating control with Information Security and Assurance approval

ii. Deploy patches

iii. Upgrade

iv. Remove or discontinue the use of the IT Resource

v. Deploy configuration changes

6 Validation Phase

a. System and applications owners must confirm the vulnerability no longer appears in the discovery tool

b. If remediation has taken place, and the change is not reflected in a validation scan or deemed not applicable (e.g., if mitigating controls were implemented, vulnerability is a false positive), the application or system owner is responsible for letting the Information Security and Assurance know via email at infosec@beyondpricing.com.