# Table of Contents

- Introduction and Purpose .......................................................................................... 2
- Vulnerability Management Solution & Remediation Service Levels ....................... 3
- Vulnerability Scan Targets .......................................................................................... 4
- Vulnerability Scan Frequency/Schedule ...................................................................... 4
- Vulnerability Reporting ............................................................................................... 5
- Remediation Management ............................................................................................ 6
- Exceptions Management ............................................................................................... 7
- Next Steps ...................................................................................................................... 8

Introduction and Purpose

This document details the vulnerability management policies and controls required to maintain high levels of system and application security in a diverse IT environment. It outlines the technology and procedures necessary for implementing a comprehensive, integrated program to detect and remediate vulnerabilities in operating systems, applications, mobile devices, cloud resources, and network devices to maintain maximum levels of security.

Vulnerability Management Solution & Remediation Service Levels

The primary vulnerability assessment solution is Retina CS Enterprise Vulnerability Management from BeyondTrust®. Retina scans the network infrastructure for devices on a scheduled periodic basis and generates a report on the vulnerabilities identified across all assets.

Retina CS is capable of reporting and logically grouping results for a consistent workflow within the organization. This automated technology can adhere to other established processes for change control, ticketing, and asset security.

Upon receipt of the reports, the Operations Team is responsible for:

- Reviewing the results
- Providing a remediation via configuration changes or deploying security patches
- Implementing other mitigating measures
- Properly documenting any exceptions

Vulnerability remediation is to be completed as soon as possible following these guidelines:

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
<th>Service Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Critical vulnerabilities have a CVSS score of 8.0 or higher. They can be readily compromised with publicly available malware or exploits.</td>
<td>2 Days</td>
</tr>
<tr>
<td>High</td>
<td>High-severity vulnerabilities have a CVSS score of 8.0 or higher, or are given a High severity rating by PCI DSS v3. There is no known public malware or exploit available.</td>
<td>30 Days</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium-severity vulnerabilities have a CVSS score of 6.0 to 8.0 and can be mitigated within an extended time frame.</td>
<td>90 Days</td>
</tr>
<tr>
<td>Low</td>
<td>Low-severity vulnerabilities are defined with a CVSS score of 4.0 to 6.0. Not all low vulnerabilities can be mitigated easily due to applications and normal operating system operations. These should be documented and properly excluded if they can’t be remediated.</td>
<td>180 Days</td>
</tr>
<tr>
<td>Severity</td>
<td>Description</td>
<td>Service Level</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Information</td>
<td>Information vulnerabilities have a CVSS score lower than 4.0. These are considered risks but are generally reference information for the state and configuration of an asset.</td>
<td>Not Required</td>
</tr>
</tbody>
</table>

Any findings that need to be mitigated later than the service level must be approved by the management and documented as exceptions. These are to be reviewed and approved by the operations manager and director of security.

Team members may also use specialized scanners to identify specific vulnerabilities or gain a deeper level of analysis, such as the Retina Web Security Scanner, FireEye, SourceFire, etc.

**Vulnerability Scan Targets**

All devices connected to both public and private segments of the network are scanned. Device scans are organized by the individually defined address spaces, active directory queries, cloud resources, and locally installed agents. These are referred to as “Smart Groups” in this document and in Retina CS Enterprise Vulnerability Management.

A Smart Group specifies a collation of hosts to be scanned and is named for the “commonality” that it holds for assets. A Smart Group name also identifies its classification or a general description of the hosts/devices on the network, and is used for role-based access for team members to restrict unauthorized access.

A new Smart Group can be established, or an existing one changed, by submitting a request through a help desk ticket directed to the Security Team and assigned to the Assessment Team.

**Vulnerability Scan Frequency/Schedule**

All devices are scanned on a consistent scan schedule and also on a by-request or as-needed basis. The defined scan frequency makes provisions for an assessment at least once per week for servers and sensitive hosts, and once per month using a rolling scan for all other devices on the network.

- All server and sensitive host scans should be scheduled between the 1st and the 15th of each month. This accommodates critical patches released by vendors such as Microsoft.
- All desktop and other scans should be completed between the 16th and the 29th of each month.
- New asset discovery scans should be run daily to identify any new assets and classified automatically via Smart Groups.
- All new assets to be included as production for desktops or servers must be assessed and documented with no critical or high vulnerabilities.
- All scans should be allocated at 36 hours to complete with no other scans running.
• The scan cycle should be established when the Smart Group is defined and should be part of the assessment request.

• Ad hoc/individual system scans may be requested via a work request and performed at anytime.

• All software images (operating systems) on the network devices (routers, switches, VPN, firewalls, wireless, and DNS/DHCP) are to be reviewed monthly.

Vulnerability Reporting

A flexible reporting schedule that works in tandem with system administration patching cycles has been implemented to manage resources and potential outages. A report will always be generated as proof that an assessment occurred. Automated delivery of the reports will depend on the scan date within the cycle.

Systems are organized into Smart Groups consisting of a collection of systems that pertain to a specific application, managed by a specific set of administrators, etc. A device may belong to one or more groups. Reporting is done by group so that the devices and vulnerabilities can more easily be distributed to staff. Groups may be added or changed via the corporate ticketing system. Below is a listing of key reports that are automatically generated and delivered to implement this process:

<table>
<thead>
<tr>
<th>Status Reports</th>
<th>Frequency</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Analyzer</td>
<td>Weekly</td>
<td>Provides recommended remediations to maximize resources by mitigation type.</td>
</tr>
<tr>
<td>Executive Dashboard</td>
<td>Weekly</td>
<td>Provides executive team members a status of risk mitigation processes established within the organization.</td>
</tr>
<tr>
<td>Service Level Agreement</td>
<td>Monthly</td>
<td>Provides a definitive report to ensure remediations are being implemented in adherence to the SLAs defined in this document.</td>
</tr>
<tr>
<td>Regulatory</td>
<td>Quarterly</td>
<td>Executives and auditors are presented with quarterly reports to ensure that compliance initiatives are being adhered to.</td>
</tr>
<tr>
<td>Exceptions</td>
<td>Monthly</td>
<td>Provides all team members a listing of exceptions and expiration dates for findings throughout the environment.</td>
</tr>
</tbody>
</table>
These reports are generated in sequence, per Smart Group, with an allowance for change control windows and system change control freezes (e.g., holiday season). However, actionable device reports are readily available upon completion of a successive scan. Report information is also available through the BeyondInsight analytics and reporting console (included with Retina CS) at any given time.

**Remediation Management**

Vulnerability reports provide system owners and administrators the opportunity to understand the potential risk to which their systems may be exposed, and to take proactive steps to address the identified vulnerabilities.

Between each official reporting period, the Security Team, system administrators, vendors, or other sources may identify vulnerabilities. The initiation of this process begins with the dissemination of actionable system reports as generated by the weekly scan cycle or by custom reporting based on requests or new asset deployments. Unplanned reports and alerts are made for issues regarding industry-wide or zero-day vulnerabilities and are treated by risk. For example, out-of-cycle critical vulnerabilities should be reported immediately with a custom assessment and remediated within the guidelines of this document. The table below outlines the general responsibilities by role:

<table>
<thead>
<tr>
<th>Actionable Reports</th>
<th>Frequency</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability</td>
<td>Weekly</td>
<td>These reports are sorted by asset, vulnerability, or risk and detail findings by Smart Group.</td>
</tr>
<tr>
<td>Patch Report</td>
<td>Weekly</td>
<td>This report identifies OS specific patches that can be applied per asset</td>
</tr>
<tr>
<td>Delta Reports</td>
<td>Monthly</td>
<td>Delta reports provide “proof” to technical team members that mitigation strategies are affecting the outcome of assessments.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Team</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| The Security Team maintains the vulnerability management solution, generates reports, and monitors the vulnerability posture of the company. The team ensures that systems are scanned for vulnerabilities on a regularly scheduled basis and that identified vulnerabilities are brought to the attention of the appropriate personnel. | - Disseminate vulnerability reports  
- Manage reports and vulnerability database  
- Issue resolution recommendations and guidance  
- Track the vulnerability resolution progress  
- Report unmitigated vulnerabilities of significance to executives  
- Respond to requests for vulnerability reviews |
## System Owner

<table>
<thead>
<tr>
<th>System Owner</th>
<th>System Administrator</th>
</tr>
</thead>
</table>
| System owners work with the system administrators to authorize, prioritize, and schedule changes to their systems, or implement acceptable mitigating controls to reduce the risk to an acceptable level. Corrective actions such as patches are considered normal business maintenance. However, if other mitigating controls are used, teams should review and approve the controls as appropriate to address the vulnerability. It is ultimately the system owner’s responsibility to accept any unmitigated risk that remains. | Review vulnerability reports  
Assess the degree of risk that the vulnerabilities represent  
Review and approve proposed corrective actions or mitigating controls  
Schedule changes with the users and the system, administrators  
Formally accept unmitigated risk  
Review vulnerability reports  
Assess the risk of vulnerabilities to the system  
Propose corrective actions or mitigating controls to the system owner(s)  
Request vulnerability exceptions where appropriate  
Implement changes authorized by the system owner(s) |

## Exceptions Management

Vulnerabilities may exist in operating systems, applications, web applications, or in the way different components interoperate together. While every effort must be made to correct issues, some vulnerabilities cannot be remediated. Vendors may have appliances that are not patched, services may be exposed for proper application operations, and systems may still be commissioned that are considered end-of-life by the developer and manufacturer.

In these cases, additional protections may be required to mitigate the vulnerability. Exceptions may also be made so that the vulnerabilities are not identified as items of risk to the system and organization. In rare cases, the vulnerability scanner may falsely identify a vulnerability that can’t be correct by the scan vendor. These types of shortcomings don’t accurately reflect the risk of the system and require an exception process. This elaborates itself in the form of multiple exception types:

- **False Positives** arise when the scanner has identified a host as being vulnerable when, in fact, it is not. This can occur because some vulnerabilities can only be identified by software version numbers and some applications will “back patch” or patch the issue without updating version numbers.
numbers. These findings have subsequently been reported back to the scan vendor and no improvements can be performed to the automated check.

- **Acceptable Risk** vulnerabilities are those where the vulnerability is real, but compensating controls are in place to mitigate the risk or the service has been deemed too critical for intervention.

- **Delayed Action** are real vulnerabilities that cannot mitigated in the time frame specified by the SLA due to business impact (downtime to apply remediation) or because of testing that is required to ensure operations are not affected by the recommended remediation.

All exception requests must present justification for the request and an expiration date. No exception can be permanent and each must be reviewed and extended using an expiration date to ensure no exceptions are permanently ignored. The request should clearly state the exception type and be recorded using the exception features in the vulnerability management solution.

- **False Positives** identification may be documented through emails or the corporate ticketing system with the security staff. These will be escalated to BeyondTrust for solution improvement and then re-assessed. If no correction can be made, the exception is logged within the solution.

- **Acceptable Risk** exceptions must be requested through the Information Security Team with an explanation containing:
  - Mitigating controls – what changes, tools, or procedures have been implemented to minimize the risk
  - Risk acceptance explanation – details as to why this risk is not relevant to the company and systems
  - Risk analysis – if the vulnerability is indeed compromised, what risk and systems will be affected

- **Delayed Action** exceptions require a plan to test the recommended remediation and a date that corrections can be implemented by without impacting the business.

Once an exception has been approved, the BeyondInsight console in Retina CS will be updated by security personnel to reflect the exception, along with a brief summary for why it was approved and what controls are now in place, including the exception type. A new Retina scan will be performed on the device to document the impact of the exception being posted. Confirmation of the posting will be reported back to the requester via monthly exception reports.

The Security Team reviews all posted exceptions at least quarterly to validate that the exceptions are still appropriate. The staff will remove any exception that is no longer required and alert the appropriate system administrators.

**Next Steps**