**Information Systems & Technology**

Vulnerability fix deployment plan

Application Server Hardening

|  |  |  |  |
| --- | --- | --- | --- |
| **Status** | Draft | **Revision** | 0.1 |
| **Doc No.** | #2 | | |
| **Date** | 04 Aug 2022 | | |
| **Originator** |  | | |
| **Project Location** |  | | |
| **Business Unit / Product Group** |  | **Momentum ID** | XXXXX |
| **RTTMS Demand #** | DMNDXXXXXXX | **Project #** | S2093 |
| **WBS** |  | **CAPS #** |  |

**Key search words**

*Add below key words, separated with a semi-colon, to be used to locate this guidance.*

|  |
| --- |
| Vulnerability fix deployment plan; |

**Revision history**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Date | Revision | Owner | Reviewed | Approved | Comments |
| 04/08/2022 | 1 | Hitender Yadav |  |  | Draft |
| 18/08/2022 | 2 | Achroo Batta (AB) |  |  | Addition of relevant section for I4.3 and A3.1 |

**Document responsibilities**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Role | Business Partner\* | Risk | Cyber | Project Manager | Hub PMO | G&I Finance | Area of Excellence | Service Transition to Support | Enterprise Architecture | Project Sponsor | Operations |
| RAPID | I | I | I | P | R | I | I | I | I | D | I |

\* Service Owner acts as Business Partner for IS&T-funded projects.

**Endorsements**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Position | Signed | Date |
|  | Business Partner \* | Embedded email /  Link to approval /  DocuSign |  |
|  | Project Manager |  |  |
|  | Position, Hub PMO |  |  |

\* Service Owner acts as Business Partner for IS&T-funded projects.

**Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Position | Signed | Date |
|  | Project Sponsor | Embedded email /  Link to approval /  DocuSign |  |
|  | Operations |  |  |
|  | Steering Committee members |  |  |

Contents page

[1. Project Overview 6](#_Toc112138089)

[**1.1.** **Summary of problem to be addressed and proposed solution** 6](#_Toc112138090)

[2. Introduction 7](#_Toc112138091)

[**2.1.** **What this document is** 7](#_Toc112138092)

[**2.2.** **What this document is not** 7](#_Toc112138093)

[**2.3.** **Audience** 7](#_Toc112138094)

[**2.4.** **Document notes** 8](#_Toc112138095)

[3. Identified Vulnerabilities 9](#_Toc112138096)

[**3.1.** **A3.1 - Clear Text** 9](#_Toc112138097)

[**3.2.** **I4.1 - RDP Timeout** 9](#_Toc112138098)

[**3.3.** **I4.3 - NTLM** 9](#_Toc112138099)

[**3.4.** **I4.5 - PowerShell v2** 9](#_Toc112138100)

[4. High-level project deployment approach 12](#_Toc112138101)

[5. Process Flows 13](#_Toc112138102)

[**5.1.** **Discovery and Analysis** 13](#_Toc112138103)

[**A3.1** CTP (Discovery completed. Analysis is under progress by Ansible Team – under progress, List shared to David on 18 Aug) 13](#_Toc112138104)

[**I4.3** NTLM (Discovery completed. Analysed by RT team querying LM Compatibility Level) 14](#_Toc112138105)

[**5.2.** **Build and Test vulnerability fix** 17](#_Toc112138106)

[**5.3.** **Change Management** 17](#_Toc112138107)

[6. Deployment Methods 18](#_Toc112138108)

[**6.1.** **Overview of deployment methods available** 18](#_Toc112138109)

[**6.1.1.** **Deployment method for A3.1 Clear text** 18](#_Toc112138110)

[**6.1.2.** **Deployment method for I4.1 RDP timeout** 18](#_Toc112138111)

[**6.1.3.** **Deployment method for I4.3 NTLM V1 to NTLM V2** 18](#_Toc112138112)

[**6.1.4.** **Deployment method for I4.5 PowerShell version update** 18](#_Toc112138113)

[**6.2.** **Vulnerability fix deployment test** 18](#_Toc112138114)

[**6.2.1.** **Deployment test for A3.1 Clear text** 18](#_Toc112138115)

[**6.2.2.** **Deployment test for I4.1 RDP timeout** 18](#_Toc112138116)

[**6.2.3.** **Deployment test for I4.3 NTLM V1 to NTLM V2** 18](#_Toc112138117)

[**6.2.4.** **Deployment test for I4.5 PowerShell version update** 18](#_Toc112138118)

[7. Appendix 19](#_Toc112138119)

1. **Project Overview**
   1. **Summary of problem to be addressed and proposed solution**

This project focuses on the review of Rio Tinto’s servers in light of the assessment conducted by Rio Tinto’s Third- Party Vendor.

The purpose of the project is to:

* Establish a detailed understanding of Rio Tinto’s current exposure to the vulnerabilities in the current environment and as stipulated in the Business Requirements Document Cyber Program – Server Hardening provided by Rio Tinto
* Assess Rio Tinto’s server virtual machines to define a current state baseline of existing vulnerabilities
* Track progression on remediation of those vulnerabilities across the Production environments
* Existing tools should be evaluated to analyse environment coverage and threat detection capabilities
* Identify processes to rectify/remediate each of the identified controls and facilitate the remediation.

1. **Introduction**

This document provides a high-level process flow overview of vulnerability fix and deployment methods. AvanadeThis is in preparation for Rio Tinto’s application server Avanadehardening project. This document will provide the process flows (vulnerability fix, change management, communication etc..), vulnerability fix and deployment model for four (4) identified vulnerabilities A3.1 - Clear Text, I4.1 - RDP Timeout, I4.3 - NTLM, I4.5 - PowerShell in the environment.

* 1. **What this document is**

This document is a vulnerability fix deployment document covering several areas of guidance as they apply to each vulnerability and Avanadeapplication servers differently on application servers. This document also covers recommended practices as well as the requirements discussed during the workshop that are unique to each vulnerability fix deployment.

* 1. **What this document is not**

This document is not a design (low level or high-level) document for vulnerability fix build and deployment infrastructure. It does not discuss how to use or resolve issues discovered within Rio Tinto’s applications.

* 1. **Audience**

This document assumes a 300-level knowledge of Vulnerabilities, associated vulnerable components and deployment methods e.g group policy, ansible, PowerShell script etc...

**Level 300**: Advanced material. In-depth understanding of features in a real-world environment, and strong coding skills. Provides a detailed technical overview of a subset of product/technology features, covering architecture, performance, migration, deployment, and development.

* 1. **Document notes**

Throughout the document Avanade will summarize the outputs of each section. These outputs can be categorized under the following headings:

|  |  |
| --- | --- |
| Icon  Description automatically generated | ***Note***  *This header is to make the reader aware of something specific in the document and will give some additional context to the section.* |

|  |  |
| --- | --- |
| Icon  Description automatically generated | ***Important Note***  *This header is to ensure the reader is fully aware of the point being highlighted. The information provided should be fully considered when understanding the context of the section.* |

|  |  |
| --- | --- |
| Icon  Description automatically generated | ***Recommendation***  *A recommendation being made by Avanade, but not necessarily a design decision.* |

|  |  |
| --- | --- |
| Icon  Description automatically generated | ***Assumption***  *Based on the workshops and knowledge of infrastructure, assumptions on configurations and requirements are listed.* |

|  |  |
| --- | --- |
| Icon  Description automatically generated | ***Design Decision***  *A design decision based on requirements and Avanade/Microsoft recommended best practices.* |

1. **Identified Vulnerabilities**
   1. **A3.1 - Clear Text**

An independent cyber security review identified significant risks and control deficiencies which significantly weaken the security and resilience of Rio Tinto.

A key finding of this review was the presence of cleartext credentials in application configuration and code files. These credentials can allow an intruder to easily move laterally into databases and other systems.

|  |  |
| --- | --- |
| Server Backlog | 1818 |
| Servers Already completed in previous Pilot | 101 |
| Decommissioned Servers | 213 |
| Pilot Servers – Non-critical | 50 |
| Pilot Servers – Critical | 20 |

* 1. **I4.1 - RDP Timeout**

Currently there is no time limit for idle or disconnected RDP sessions for most the most servers. This can increase risk of RDP Session Hijacking.

|  |  |
| --- | --- |
| Server Backlog | 5798(To be updated) |
| Pilot Servers – Non-critical | 50 |

* 1. **I4.3 - NTLM**

New Technology LAN Manager (NTLM) v1 lacks crucial security protocols like including a timestamp in response and generating a variable-length challenge, which has been built into NTLMv2

|  |  |
| --- | --- |
| Server Backlog | 5798 |
| Pilot Servers – Non-critical | 50 |
| Pilot Servers – Critical | 20 |

* 1. **I4.5 - PowerShell v2**

3.4.1 Overview

The number of servers were identified in Rio Tinto environment that has deprecated version of PowerShell installed. PowerShell v2 lacks security protections that have been built into later versions.

PowerShell v2 needs to be removed and updated to Version 5.1 if possible. This will allow to reduce the cyber risk and improve security posture of Rio Tinto’s IT infrastructure.

PowerShell version 2 (PSv2) comes pre-installed on Windows Server 2008. It is also installed on other versions of Windows Server OS in Rio Tinto fleet.

|  |  |
| --- | --- |
| Server Backlog | 189+XX |
| Pilot Servers – Non-critical | 50 |

3.4.2 Scan reports (move to 5.1 Discover and analysis section)

Rio Tinto provided Scan Reports on PowerShell v2 vulnerability. Based on report analysis we identified the number of servers with PSv2 installed.

|  |  |
| --- | --- |
| Not Scanned | 168 |
| PSv2 only installed | 189 |
| PSv2 and PSvX installed | XXX not provided yet |

Out of scanned Servers the distribution of OS is the following:

|  |  |  |
| --- | --- | --- |
| Windows Server 2003 | 14 | Out of scope |
| Windows Server 2008 | 15 | Out of scope |
| Windows Server 2008 R2 | 160 | In Scope |
| Windows Server 2012 | Not provided yet | In Scope |
| Windows Server 2012 | Not provided yet | In Scope |
| Windows Server 2019 | Not provided yet | In Scope |
|  |  |  |

Discovery Analysis

|  |  |  |
| --- | --- | --- |
| Windows Server 2003 | 14 | Windows 2003 Server cannot be updated to PowerShell version higher than 2.0. Out of Scope for PS version upgrade. |
| Windows Server 2008 | 15 | Windows 2003 Server cannot be updated to PowerShell version higher than 2.0. Out of Scope for PS version upgrade. |
| Windows Server 2008 R2 | 273 | In Scope for PowerShell V 5.1 upgrade. |
| Windows Server 2012 | Not provided yet | Windows 2012 Server that have PS 2.0 version installed as well as higher version of PS. PowerShell version 2 will be disabled and removed. |
| Windows Server 2016 | Not provided yet | Windows 2016 Server that have PS 2.0 version installed as well as higher version of PS. PowerShell version 2 will be disabled and removed. |
| Windows Server 2019 | Not provided yet | Windows 2019 Server that have PS 2.0 version installed as well as higher version of PS. PowerShell version 2 will be disabled and removed. |
|  |  |  |

1. **High-level project deployment approach**

Below is the details of high-level project plan

Timeline

Description automatically generated

1. **Process Flows**
   1. **Discovery and Analysis**

**A3.1** CTP (Discovery completed. Analysis is under progress by Ansible Team – under progress, List shared to David on 18 Aug)

List of CTP

|  |  |
| --- | --- |
| **Server-Criticality** | **Pilot Servers** |
| **Level 3** | **16** |
| Windows Server 2012 R2 Standard | 3 |
| Windows Server 2016 Datacenter | 1 |
| Windows Server 2016 Standard | 1 |
| Windows Server 2019 Datacenter | 11 |
| **Level 4** | **4** |
| Windows Server 2012 R2 Standard | 2 |
| Windows Server 2019 Datacenter | 1 |
| Windows Server 2019 Standard | 1 |
| **Level 5** | **12** |
| Windows Server 2012 R2 Standard | 6 |
| Windows Server 2019 Datacenter | 1 |
| Windows Server 2019 Standard | 5 |
| **Level 6** | **38** |
| Windows Server 2012 R2 Standard | 6 |
| Windows Server 2016 Standard | 5 |
| Windows Server 2019 Datacenter | 10 |
| Windows Server 2019 Standard | 17 |
| **Grand Total** | **70** |

Process Flow

Diagram

Description automatically generated

|  |  |
| --- | --- |
| **1** | Received list of **1504** servers from RT (Backlog from Rahul’ project) |
| **2** | List of servers will be considered in enterprise rollout plan |
| **3** | Only APAC servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| **4** | Only Non-Prod servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| **5** | Only Non PCN servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| **6** | Criticality 3, 4, 5 or 6 will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| **7** | Pilot list Approved by RT (Craig Young) |
| **8** | Based on Criticality list is segregated in Non-Critical and Critical |
| **9** | 50 Non-Critical Pilot List shortlisted |
| **10** | 20 Critical Pilot List shortlisted |
| **11** | Group servers based on server owners (use Pivot Table through Excel) |
| **12** | Send email communication to owners along with questionnaire |
| **13** | Check if you receive response from owners |
| **14** | If answer to 13 is yes, Workshop/Discussion required with owners |
| **15** | Is there any Action Item comes out from Workshop/Discussion? |
| **16** | Implement on Action Item, if there is any outcome from 15 |
| **17** | Send reminder email to owners |
| **18** | Check if you receive response from owners |
| **19** | Raise Change Requests based on Non-critical/Critical/feedbacks of owners |
| **20** | Send email communication to Owners along with change request and deployment date |
| **21** | Check if you receive response from owners |
| **22** | Take backup of config files and name it as. bk and place it on server |
| **23** | Run PowerShell commands to encrypt config files |
| **24** | Run PowerShell commands to query config files |
| **25** | Did remediation work? |
| **26** | If remediation did not work, mark it as exception. |
| **27** | Update Tracker with comments |
| **28** | App/Server Got Impacted. Did you receive any communication on the same? |
| **29** | Rollback by reverting to original config files |
| **30** | Notify stakeholders appropriately |

**I4.3** NTLM (Discovery completed. Analysed by RT team querying LM Compatibility Level)

|  |  |
| --- | --- |
| **Server-Criticality** | **Pilot-Servers** |
| **Level 3** | **6** |
| Windows Server 2012 R2 Datacenter | 3 |
| Windows Server 2016 Standard | 1 |
| Windows Server 2019 Standard | 2 |
| **Level 4** | **14** |
| Windows Server 2012 R2 Datacenter | 1 |
| Windows Server 2012 R2 Standard | 3 |
| Windows Server 2016 Standard | 4 |
| Windows Server 2019 Standard | 6 |
| **Level 5** | **11** |
| Windows Server 2008 R2 Standard | 2 |
| Windows Server 2012 R2 Standard | 3 |
| Windows Server 2016 Standard | 2 |
| Windows Server 2019 Datacenter | 2 |
| Windows Server 2019 Standard | 2 |
| **Level 6** | **39** |
| Windows Server 2008 R2 Enterprise | 4 |
| Windows Server 2008 R2 Standard | 1 |
| Windows Server 2012 R2 Datacenter | 4 |
| Windows Server 2012 R2 Standard | 2 |
| Windows Server 2016 Datacenter | 1 |
| Windows Server 2016 Standard | 9 |
| Windows Server 2019 Datacenter | 1 |
| Windows Server 2019 Standard | 17 |
| **Grand Total** | **70** |

Process Flow – NTLM

Diagram

Description automatically generated

|  |  |
| --- | --- |
| **1** | Received list of 5798 servers from RT |
| **2** | List of servers will be considered in enterprise rollout plan |
| **3** | Only APAC servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| **4** | Only Non-Prod servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| **5** | Only Non PCN servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| **6** | Criticality 3, 4, 5 or 6 will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| **7** | Pilot list Approved by RT (Craig Young) |
| **8** | Based on Criticality list is segregated in Non-Critical and Critical |
| **9** | 50 Non-Critical Pilot List shortlisted |
| **10** | 20 Critical Pilot List shortlisted |
| **11** | Group servers based on server owners (use Pivot Table through Excel) |
| **12** | Send email communication to owners along with questionnaire |
| **13** | Check if you receive response from owners |
| **14** | If answer to 13 is yes, Workshop/Discussion required with owners |
| **15** | Is there any Action Item comes out from Workshop/Discussion? |
| **16** | Implement on Action Item, if there is any outcome from 15 |
| **17** | Send reminder email to owners |
| **18** | Check if you receive response from owners |
| **19** | Raise Change Requests based on Non-critical/Critical/feedbacks of owners |
| **20** | Send email communication to Owners along with change request and deployment date |
| **21** | Check if you receive response from owners |
| **22** | Check LM Compatibility and result set of policy by logging on to server |
| **23** | Request Itergy to link GPO through security filtering with servers |
| **24** | Check LM Compatibility and result set of policy by logging on to server |
| **25** | Did remediation work? |
| **26** | If remediation did not work, reboot the servers |
| **27** | Check LM Compatibility and result set of policy by logging on to server |
| **28** | Did remediation work? |
| **29** | Mark server as exception if remediation did not work |
| **30** | Update trackers with appropriate comments |
| **31** | App/Server Got Impacted. Did you receive any communication on the same? |
| **32** | Rollback by unlinking GPO |
| **33** | Notify stakeholders appropriately |

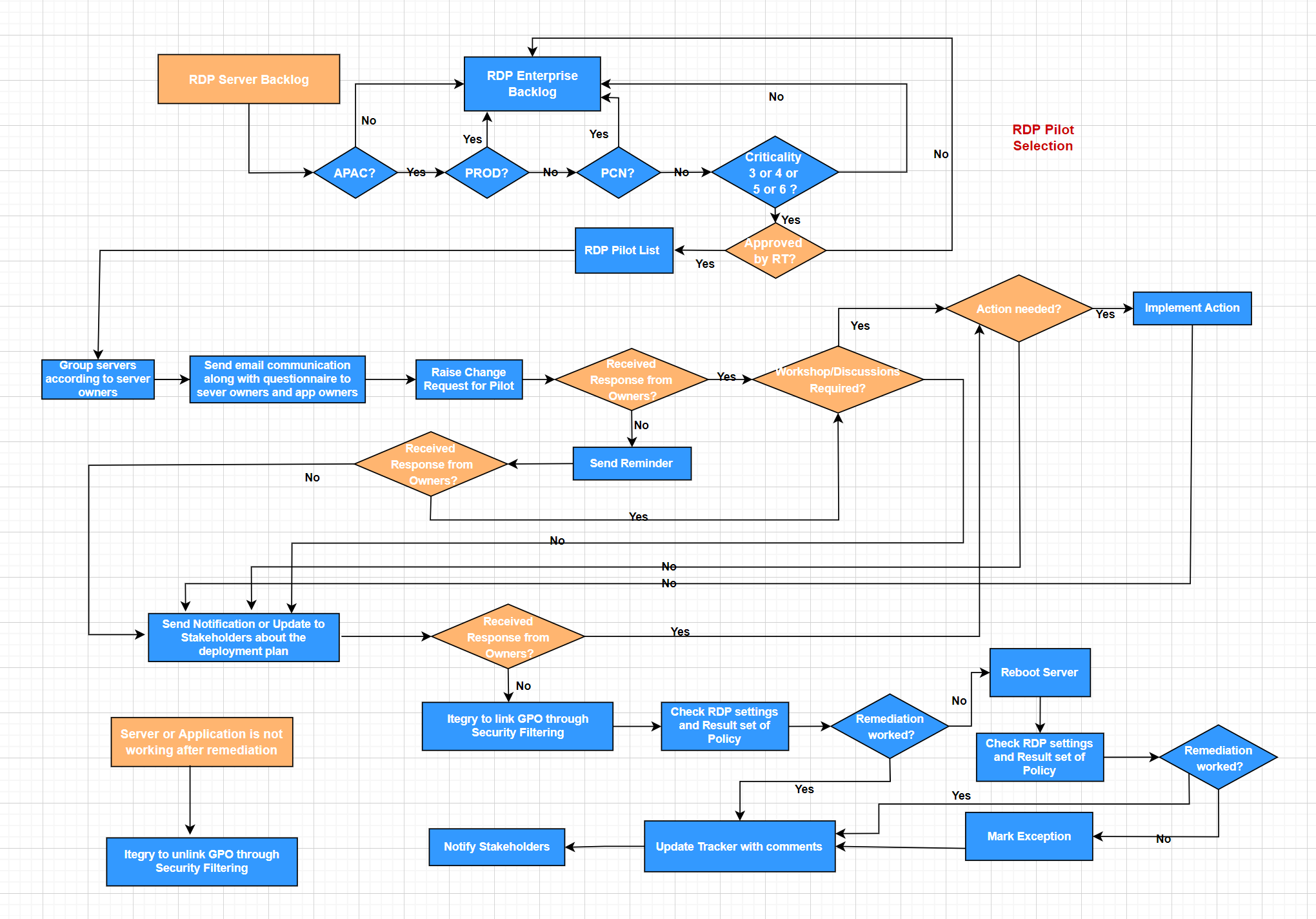
Process Flow – PowerShell

Diagram

Description automatically generated

Pilot Selection Criteria

Process Flow – RDP



1. **Vulnerability fix deployment**
   1. **Overview of vulnerability fix deployment**
      1. **Deployment method for A3.1 Clear text**

Running below set of PowerShell commands by login on to the server or remotely or through Ansible, will encrypt the content in web config files. No server or IIS restart required.

**Instructions**

1. Open the CMD window on the server
2. Go to Server Drive Letter that ClearText File is located
3. Enter below command  
   **reg query “HKLM\SOFTWARE\Microsoft\Net Framework Setup\NDP” /s**
4. Check most recent .Net Framework Version
5. Traverse to that specific directory found in step 4
6. Enter below command

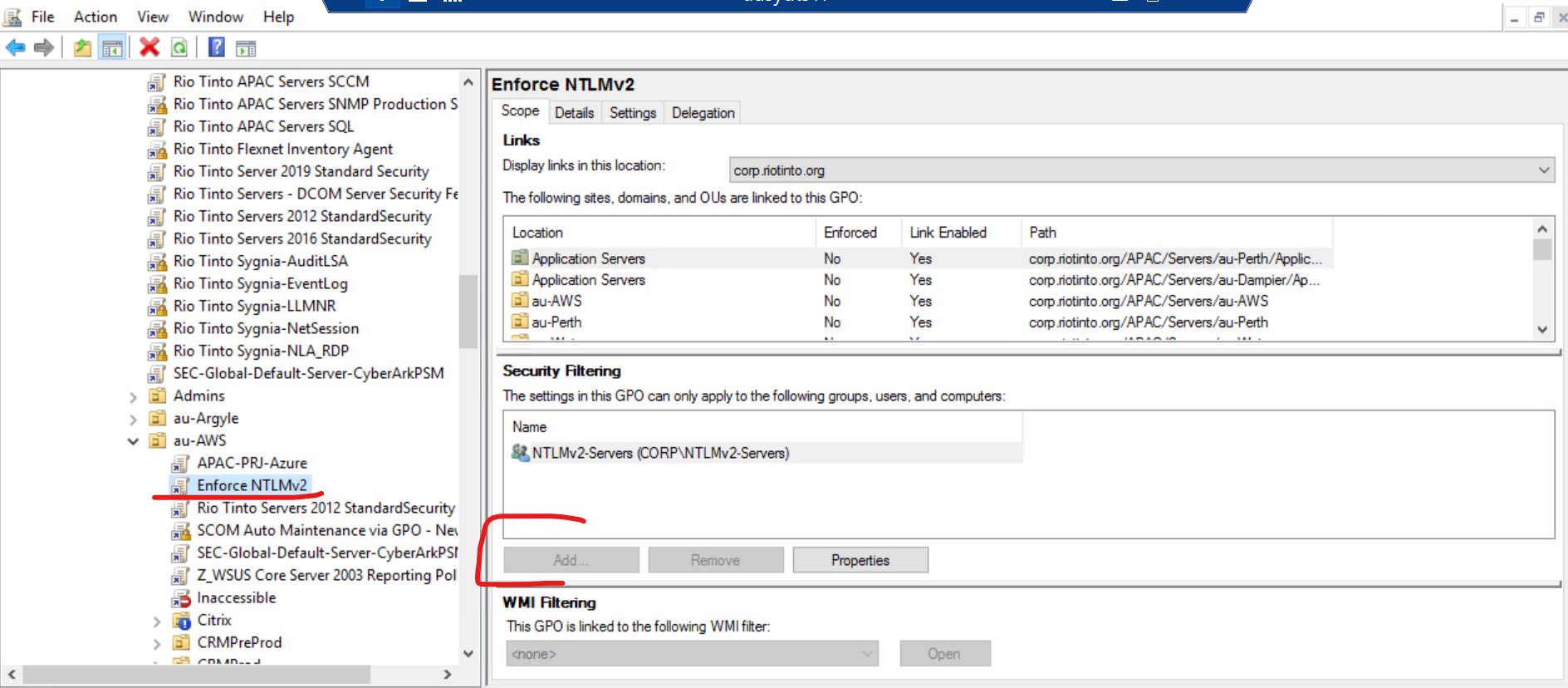
ASPNET\_REGIIS -pef “connectionStrings” “application folder path”

* + 1. **Deployment method for I4.1 RDP timeout**

Deployment will be performed by Itergy --completed by Linking GPO policies through security filtering with respective OU members.

* + 1. **Deployment method for I4.3 NTLM V1 to NTLM V2**

Deployment will be Itergy by Linking GPO policies through security filtering with respective OU members.



Enforce NTLMv2 GPO policy is present, we can add members in Security Filtering with the help of Itergy Team.

* + 1. **Deployment method for I4.5 PowerShell version update**

Insert details about the deployment method

* 1. **Vulnerability fix deployment test**

Insert details about the deployment test and status

* + 1. **Deployment test for A3.1 Clear text**

Running PowerShell commands against the servers will help to determine that all config file, no longer contains clear text information.

|  |  |  |
| --- | --- | --- |
| **ServerName** | **Before Deployment** | **After Deployment** |
| Server1 | config file1 | No Result should be returned |
|  | config file2 | No Result should be returned |
|  | config file3 | No Result should be returned |
| Server2 | config file1 | No Result should be returned |
|  | config file2 | No Result should be returned |
| . | config file3 | No Result should be returned |
| . | config file 4 | No Result should be returned |
| Server3 | config file 1 | No Result should be returned |
| Server 4 | config file 1 | No Result should be returned |
|  | config file 2 | No Result should be returned |
| . | config file 3 | No Result should be returned |

* + 1. **Deployment test for I4.1 RDP timeout**

Insert details about the deployment method

* + 1. **Deployment test for I4.3 NTLM V1 to NTLM V2**

Querying LM Compatibility level and result set of policies will confirm if NTLM authentication changed from v1 to v2. The following table will help to determine testing of fix.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Server Name** | **Before Deployment** | | | **After Deployment** | | |
| **REGEDIT** | **GPEDIT** | **GPO** | **REGEDIT** | **GPEDIT** | **GPO** |
| Server1 |  |  |  |  |  |  |
| Server2 |  |  |  |  |  |  |
| Server3 |  |  |  |  |  |  |
| . |  |  |  |  |  |  |
| . |  |  |  |  |  |  |
| . |  |  |  |  |  |  |
| . |  |  |  |  |  |  |
| . |  |  |  |  |  |  |
| . |  |  |  |  |  |  |
| . |  |  |  |  |  |  |
| . |  |  |  |  |  |  |

* + 1. **Deployment test for I4.5 PowerShell version update**

Insert details about the deployment method

1. **Appendix**

|  |  |
| --- | --- |
| Term / Acronym | Definition |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |