|  |  |  |  |
| --- | --- | --- | --- |
| RCA Information & Status | | | |
| Incident Impact Details | | Vendor Review & Submission | |
| Application / Service | CyberArk | Prepared By | Devbrat Yadav |
| Incident Number | PRB0042110 | Preparation Date | June 26, 2023 |
| Submit Date | June 28, 2023 | Submitted By *(vendor manager)* |  |
| Submit Time *(EST)* | 2:48 PM IST | Submitted Date | Click or tap to enter a date. |
| Resolution Date | June 8, 2023 | Axalta Manager Review & Approval | |
| Resolution Time *(EST)* |  | Reviewed By | Gobind Kumar |
| Priority | High (P2) | Review Date | June 28, 2023 |
| Outage Duration *(Hrs / Mins)* | 2hrs 3min | Acceptance Status | Choose an item. |

| Incident Description |
| --- |
| Summarize Incident  *Describe the services that were affected by the outage, such as applications, server names, network circuits and locations.* |
| CyberArk were not opening. |
| Resolution Summary  *Describe the actions that were performed to identify the issue and the steps taken to restore normal operation, including work arounds.*  *(Do not provide a detailed chronology of the incident.)* |
| On June 8th, 2023, at 08:19 EST, users reported that they were not able to open the CyberArk application, causing an outage of 2 hours 3 minutes. The issue occurred because the primary vault server was rebooted without consent or approval from the security team. The server was switched off and maintained down for two hours. When the server was initiated again, the application services were not able to initiate automatically. The support team, along with vendor CyberArk, resolved the issue by making some changes that were misconfigured in the CyberArk application. The support team validated and confirmed with users that the CyberArk application was up and users were able to access it as normal.  The server was switched off and maintained down for 2 hours and when the server was initiated again the application services were not able to automatically initiate again.  The application had migrated to the DR Vault, but this failover is not fully automated, so none of the environments were working.  There was some misconfiguration that needed CyberArk support to bring the application back to the primary environment. Once done the PVWA and the PSM CyberArk components were able to be launched again and functionality was recovered |

| Root Cause Analysis |
| --- |
| Problem Definition  *Describe the problem that must be solved to prevent future outages.* |
| We are preparing the SOP for the critical servers, earlier we don't have any document to check the servers criticality and also we are planning to add Tagging against the production server.  we are ensuring not to commit any human mistake; Change should be implemented only after Application Owner and change must be reviewed by technical leads of the team.  As Currently no Automation done at CSIRT application so before and post any server reboot team must inform to Application team , so that the services should be brought up in a proper way and verification if failover occurs needs to be done |
| Problem Analysis  *Describe the actions performed to analyze the problem and identify underlying issues that led to the outage. Include the questions or theories discussed. Include any references to supporting documentation such as server logs, error messages, support references, external knowledge articles or vendor support tickets. These references can be inserted as embedded documents, or included as attachments.* |
| On June 8th, 2023, at 08:19 EST, users reported that they were not able to open the CyberArk application, causing an outage of 2 hours 3 minutes. |
| Findings & Root Cause  *Summarize the findings and describe the cause (or causes) of the outage.* |
| 1. Why was the Change process not followed?  Ans: Initially server were not reachable for us, VM agent was not ready and even not added into domain .This server was not part of monitoring so in order to bring the server up team rebooted and missed to get approval due to internal communication.  Why was a production server rebooted without a change recorded?  Ans: Team Raise standard change-CHG0052305 to make the server up.  What is going to be done to ensure we don't make changes to production infrastructure without verifying a documented change and approval?  Ans: We are preparing the SOP for the critical servers, earlier we don't have any document check the servers criticality and also we are planning to add Tagging against the production server.  we are ensuring not to commit any human mistake, Change should be implemented only after Application Owner and change must be reviewed by Technical leads of the team.  Before and post any server reboot team must inform to Application team, so that the services should be brought up in a proper way and verification if failover occurs needs to be done.  Why were configuration changes required?  Ans: Configuration changes was done by CSIRT team as no automation were there to route the traffic to secondary vault.  Why was the server down for multiple hours?  Ans: It was Human error, We will ensure not to repeat in future by making strong checker process among the team.  Can failover be automated to avoid down time in the event we lose the production vault again in the future for any reason?  Ans: CSIRT team needs to Automate the manual process and CSIRT Team's add below comments.  It is technically not possible since it requires a manual change in the PVWA component configuration.  the Vault automatically change to the secondary, but taken into consideration that the Vaults are completely hardened, the front end does not migrate... |

| Remediation Plan |
| --- |
| Resolution Actions  *Describe the actions necessary to prevent future failures. This should include references to actions such as planned changes (and associated change requests), monitoring activity, job schedule modifications or operational process changes.* |
| As a Remediation:  • Wintel and Virtualization to prepare a list of all critical servers and application owner names and get them reviewed.  • As a process enhancement all SOPS need to revise and get approved once in a year. All SOPs should be added in one SharePoint to have access to all stakeholders. |