**EQUIPMENT TEST PLAN**

**Splunk - Windows 2022 AD Server**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Project Title: | **AWS CyberShift Initiative** |  | Date Prepared: | 1st of July, 2023 |

|  |
| --- |
| **Overall project scope and objectives** |
| The AWS CyberShift Initiative project will secure OzCazual's cloud infrastructure and enable a safe and secure migration from their existing local server to Amazon AWS.  The primary goal is to address the sudden 200% increase in online sales and staff, create a scalable infrastructure that can meet future business demands, and ensure the confidentiality, integrity, and availability of the systems and customer data.  The project will Implementing various security controls, and upgrade the systems and tools currently used at OzCazual |
| **Test objectives and success criteria** |
| **Test Objectives:**   * **Verify Splunk Configuration:** Ensure that Splunk is properly configured on the Windows 2022 AD server, with the necessary inputs and filters in place to collect and index the relevant logs related to SSH login attempts. * **Test Search Query:** Validate the effectiveness of the search query designed to detect failed login attempts of remote connections using SSH. * **Real-Time Alerting:** Confirm that the alert triggered by the search query works as expected and provides real-time notifications for failed SSH login attempts. * **Test Scalability:** Evaluate the performance of Splunk in handling a large volume of logs generated by multiple remote connections attempting SSH login. * **Test False Positive/Negative Rates:** Assess the accuracy of the search query in distinguishing between actual failed login attempts and other events that may trigger false positives or negatives. * **Test Data Retention:** Ensure that Splunk retains the necessary logs for an appropriate duration to facilitate investigation and analysis of failed login attempts.   **Success Criteria:**   * **Splunk Configuration:** Splunk should be properly installed and configured on the Windows 2022 AD server, with the necessary log inputs configured to collect SSH-related events. * **Test Search Query:** The search query designed to detect failed login attempts should accurately identify events that match the criteria of "Unknown user name or bad password" for SSH login failures. * **Real-Time Alerting:** The alert should trigger promptly in real-time when a failed SSH login attempt occurs, providing immediate notifications to the designated recipients. * **Test Scalability:** Splunk should be able to handle a significant volume of logs generated by multiple remote connections attempting SSH login without significant degradation in performance. * **Test False Positive/Negative Rates:** The search query should have a low rate of false positives, meaning it should accurately identify genuine failed login attempts. It should also minimize false negatives by ensuring that actual failed login attempts are not missed. * **Test Data Retention:** Splunk should retain the necessary logs for a reasonable duration to allow for investigation and analysis of failed login attempts. The duration should be defined based on compliance requirements or organizational needs.   By achieving these objectives and success criteria, the test plan aims to validate the effectiveness and reliability of Splunk in detecting failed login attempts for remote SSH connections on the Windows 2022 AD server. |
| **Test resources required (people, hardware, software, test tools)** |
| To ensure resource estimation, test build guidance, and historical recording, it is essential to document the people, hardware, software, and test tools required to complete the test. Accurate documentation of hardware and software versions is crucial for consistent and reliable test results. Here is a summary of the necessary components: Software Versions to Be Tested  |  |  | | --- | --- | | **Software Version** |  | | Splunk | Latest | | Splunk Universal Forwarder | Latest | | Azure Management Portal | N/A | | SSH client software | Latest |  People, Roles, and Time Allocation  |  |  |  | | --- | --- | --- | | **Role** | **Name** | **Resource Allocation** | | Project Manager | Giuseppe Raciti | 10% | | Cyber Security Specialist | Shaun Heywood | 20% | | Test LeCloud Architect/Engineer | Mark Byrne | 15% | | Server Administrator | Mauricio Guerra | 15% | |
| **Test schedule** |
| |  |  |  | | --- | --- | --- | | **Date** | **Milestones** | **Resource Allocation** | | **01/07/2023** | Test Kick-off Meeting | Project Manager (Giuseppe Raciti), 5% | | Configure Azure Hyper-V Environment | Cloud Architect/Engineer (Mark Byrne), 30% Server Administrator (Mauricio Guerra), 30% | | Install and Configure Splunk Components | Cloud Architect/Engineer (Mark Byrne), 20% Server Administrator (Mauricio Guerra), 20% | | Define and Test SSH Search Query | Cyber Security Specialist (Shaun Heywood), 40% Server Administrator (Mauricio Guerra), 30% | | Configure Real-Time Alerting | Cyber Security Specialist (Shaun Heywood), 40% | | **02/07/2023** | Scalability and Load Testing | Cyber Security Specialist (Shaun Heywood), 30%  Server Administrator (Mauricio Guerra), 30% | | Bug Identification and Reporting | Cyber Security Specialist (Shaun Heywood), 20%  Server Administrator (Mauricio Guerra), 10% | | Review Test Results with the Team | Project Manager (Giuseppe Raciti), 5% | |
| **Format for Written Test Case** |
| |  |  | | --- | --- | | **Test ID:** | **TC005** | | **Node List:** | Windows 2022 AD server | | **Test Description:** | Test failed SSH login detection using Splunk | | **Test Phase:** | Baseline | | **Test Suite:** | SSH Login Monitoring | | **Test Setup:** | **Deploy a Windows 2022 AD server.**   1. Install and configure Splunk on the Windows 2022 AD server. 2. Set up Splunk Universal Forwarder to forward logs from the Windows 2022 AD server to the Splunk indexer. 3. Configure Splunk Search Head and Alert Manager. 4. Generate test SSH login events with different failure scenarios. 5. Save the search query as an alert that triggers when failed SSH login attempts are detected | | **Test Steps:** | 1. Open the Splunk Web Interface. 2. Navigate to the Search & Reporting section. 3. Enter the search query to filter failed SSH login attempts:   **host="OZCAZUAL-WINDADS" ssh OR sshd EventCode=4625 FailureReason="Unknown user name or bad password." Message="An account failed to log on\*"**   1. Click on the "**Search**" button to execute the search query. 2. Verify that the search results display the failed SSH login events with the specified failure reason and message 3. Confirm that the search query has been saved as an alert. 4. Trigger a test event by simulating a failed SSH login attempt. 5. Verify that the alert is triggered and a notification is sent. | | **Expected Results:** | * The search results should accurately filter and display the failed SSH login events matching the specified criteria. * The search query should be saved as an alert. * When a failed SSH login attempt occurs, the alert should be triggered and a notification should be sent. | | **Observed Results:** | * Upon executing the search query, the search results displayed multiple events of failed SSH login attempts with the "Unknown user name or bad password." failure reason and "An account failed to log on\*" message. The events were correctly detected and filtered by Splunk.      * search query was successfully saved as an alert in Splunk's Alert Manager.      * When a test event simulating a failed SSH login attempt was triggered, the alert was successfully triggered, and a notification was sent as expected. | | **Pass/Fail:** | Pass/Fail: **Pass**  The observed results align with the expected results, indicating that the test case for failed SSH login detection using Splunk has passed.  Splunk successfully identified and displayed the relevant failed SSH login events based on the defined criteria.  Additionally, the search query was saved as an alert, and when a failed SSH login attempt occurred, the alert was triggered, and a notification was sent.  This confirms that Splunk's alerting mechanism for failed SSH login attempts is functioning correctly. | |