**EQUIPMENT TEST PLAN**

**Sophos Intercept X - Linux 2 Web Server**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Project Title: | **AWS CyberShift Initiative** |  | Date Prepared: | 23rd of June, 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 a cloud environment.  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** |
| To evaluate the functionality, performance, and compatibility of Sophos Endpoint Security and Control on the specified equipment.  **Test Network :** |

|  |
| --- |
| Test resources required (people, hardware, software, test tools) |
| Test Objectives:  1. Verify the successful deployment of Sophos Endpoint Security and Control on Microsoft Windows Server 2022 and Linux 2. Validate the functionality and performance of Sophos Endpoint Security and Control as a network security solution in conjunction with a Windows 2022 Active Directory (AD) Server environment. 3. Evaluate the effectiveness of Sophos Endpoint Security and Control in detecting, blocking and eradicating virus and malware threats. 4. Assess the scalability of Sophos Endpoint Security and Control in the cloud environment, considering factors such as increased network traffic, the number of users, and resource utilization. 5. Test the failover and high availability capabilities of Sophos Endpoint Security and Control in the cloud, ensuring uninterrupted network security and availability in the event of a failure or maintenance activity. 6. Validate the interoperability of Sophos Endpoint Security and Control with other cloud-based services, such as load balancers, DNS services, or cloud storage, to ensure seamless integration and functionality. 7. Evaluate the logging and reporting capabilities of Sophos Endpoint Security and Control , ensuring that logs are generated accurately, and relevant information is available for monitoring, troubleshooting, and compliance purposes. 8. Test the resilience of Sophos Endpoint Security and Control against common network attacks, such as Denial of Service (DoS) attacks, port scans, and intrusion attempts, to verify its effectiveness in detecting and mitigating threats. 9. Assess the ease of management and configuration of Sophos Endpoint Security and Control in the cloud environment, including features such as remote access, web-based administration, and automation capabilities.  Success Criteria:  1. Successful deployment of Sophos Endpoint Security and Control in a cloud-based virtual machine, without any compatibility issues or errors during the setup process. 2. Verification of essential Sophos Endpoint Security and Control features 3. Adequate performance of Sophos Endpoint Security and Control in terms of throughput, latency, and resource utilization, meeting the requirements of the intended network environment. 4. Effective network security provided by Sophos Endpoint Security and Control , ensuring that virus and malware threats are blocked 5. Scalability of Sophos Endpoint Security and Control in the cloud environment, with the ability to handle increased network traffic, additional users, and resource demands, without compromising performance or stability. 6. Seamless integration of Sophos Endpoint Security and Control with other cloud-based services without any compatibility issues or disruptions to functionality. 7. Reliable failover and high availability capabilities of Sophos Endpoint Security and Control, ensuring uninterrupted network security and availability during failure or maintenance scenarios. 8. Accurate logging and reporting of network activities by Sophos Endpoint Security and Control, providing valuable information for monitoring, troubleshooting, and compliance purposes. 9. Effective detection and mitigation of common virus and malware threats by Sophos Endpoint Security and Control , ensuring the network remains protected and secure. 10. User-friendly management and configuration of Sophos Endpoint Security and Control in the cloud environment, with features such as remote access, web-based administration, and automation capabilities that simplify the management process. |
| **Test resources required (people, hardware, software, test tools)**  **People:**   * **Project Manager** : Responsible for overall test planning, coordination, and management of the test activities. * **Cyber Security Specialist**: Responsible for executing the test cases, documenting results, and troubleshooting issues. * **Network Administrator**: Knowledgeable in network configurations and responsible for setting up the virtual network environment. * **System Administrator**: Familiar with the Azure platform and responsible for provisioning and managing the virtual machine on Azure. * **Security Analyst**: Knowledgeable in network security and responsible for testing the effectiveness of Sophos as a network security solution. * **Test Tools Specialist**: Familiar with various testing tools and responsible for selecting, configuring, and managing the test tools used during the testing process.   **Hardware**:  **Virtual Machine on Azure**: Provision a virtual machine running Linux Web Server as the test environment.  **Sufficient compute resources**: Ensure that the virtual machine has adequate CPU, memory, and storage resources to run Sophos and accommodate the expected network traffic.  **Software**:   * **Sophos Endpoint Security and Control** : Install and configure Sophos Endpoint Security and Control as a virtual machine on the Azure virtual machine. * **Linux Web Server**: Set up and configure the AD Server on the virtual machine to test the integration with Sophos. * **Hyper-V Manager**: Utilize Hyper-V Manager to manage the virtual machine and virtual network settings.   **Testing Tools**:  Select and configure testing tools based on the specific test objectives, such as:   * **Network traffic generator**: To simulate different network traffic scenarios and assess the performance of Sophos Endpoint Security and Control . * **Network monitoring and analysis tool**: To capture and analyze network traffic passing through Sophos Endpoint Security and Control for security and performance evaluation. * **Vulnerability scanner**: To test the effectiveness of Sophos Endpoint Security and Control in detecting and mitigating common network vulnerabilities. * **Logging and reporting tools**: To capture and analyze logs generated by Sophos Endpoint Security and Control for monitoring, troubleshooting, and compliance purposes.  Table - People, Roles, and Time Allocation  |  |  |  | | --- | --- | --- | | **Role** | **Name** | **Resource Allocation** | | **Project Manager** | Giuseppe Raciti | Full-time during test planning and execution | | **Cyber Security Specialist** | Shaun Heywood | As needed, full-time during test execution | | **Cloud Architect / Engineer** | Mark Byrne | As needed, for setting up the virtual network environment. | | **System Administrator** | Mauricio Guerra | As needed, for provisioning and managing the virtual machine on Azure. |  |  | | --- | | **Test schedule** |  |  |  |  | | --- | --- | --- | | **Date** | **Milestones** | **Resource Allocation** | | **19/06/23** | **Test Planning** | Project Manager, Cyber Security Specialist | |  | - Define test objectives | Project Manager, Stakeholders | |  | - Identify test resources | Project Manager, System Administrator | |  | - Define test environment | Project Manager, Server Administrator | |  | - Develop test plan | Project Manager, Cyber Security Specialist | | **25/06/23** | **Test Environment Setup** | System Administrator, Cyber Security Specialist | |  | - Install Windows AD | System Administrator | |  | - Install Sophos | System Administrator, Cyber Security Specialist | | **26/06/23** | **Test Execution** | Cyber Security Specialist | |  | - Test Case Execution | Cyber Security Specialist, Testing Tools Specialist | |  | - Performance Testing | Cyber Security Specialist, Testing Tools Specialist | |  | - Security Testing | Cyber Security Specialist, Server Administrator | | **30/06/23** | **Test Reporting** | Cyber Security Specialist, Project Manager | |  | - Results Compilation | Cyber Security Specialist, Project Manager | |  | - Defect Tracking | Cyber Security Specialist, Project Manager | |  | - Test Summary Report | Cyber Security Specialist, Project Manager | |
| |  | | --- | | **Test Case** | | | **Test ID:** | TC-0005 | | --- | --- | | **Node List:** | Linux Web Server | | **Test Description:** | Perform a simple malware infection to the system, test the effectiveness of the Sophos application | | **Test Phase:** | Baseline - Malware Detection Testing | | **Test Suite:** | | | The Sophos Endpoint Security and Control test suite is a thorough set of test cases created to assess the software's performance, effectiveness, and usability. The security solution is covered from a variety of angles, including malware prevention and detection, data control, and application control. The test suite's goal is to make sure that Sophos Endpoint Security and Control performs as intended, offering reliable security measures with the least possible impact on system performance.  Test cases are created to confirm the anticipated behaviour of Sophos Endpoint Security and Control and compare it to predetermined success criteria throughout the test suite. Any problems or variations from intended behaviour are noted in the test results and observations, which are also documented.  The test suite also includes performance testing to evaluate the effect of Sophos Endpoint Security and Control on system resources in addition to functional testing. This entails keeping track of CPU, memory, disc, and network usage while performing various tasks including real-time scanning and virus detection.  **Test Case Scenario Performed - Malware Detection:**   * Test the ability of Sophos Endpoint Security and Control to detect different types of malware (viruses, worms, Trojans, ransomware, etc.) by executing known malware samples. * Verify that the software promptly detects and responds to malware, taking appropriate actions such as quarantining or removing the infected files. * Ensure that notifications or alerts are displayed for each detected malware. | | | **Test Setup:** | | | The test setup involves a virtual environment hosted on Azure, comprising a Linux Web Server. Sophos Endpoint Security and Control provides virus and malware protection to the Windows AD server.  **Hardware:**  **Virtual Machines:**  Linux Web Server VM: Running on Azure cloud infrastructure.  **Logical Configurations:**  **Linux Web Server VM:**  Configure Linux virtual machine with Apache Web Server  Set up necessary network settings, including IP addresses, subnet masks, and gateway configurations.  Configure appropriate security settings, such as firewall rules and access controls.  **Sophos Endpoint Security and Control:**  Deploy Sophos Endpoint Security and Control on a virtual machine on Azure.  Configure the settings as desired on Sophos, ensuring proper application settings are set.  **Test Tools / Applications /Services:**  **Virtualization Software:**  **Hyper-V Manager:**  Utilized to manage the virtual machine environment, including the creation and management of VMs.  **Cloud Infrastructure:**  **Azure Cloud Infrastructure:**  Provides the underlying platform for hosting the virtual machines and networking infrastructure.  **Malware Samples:**  Collect a diverse set of known malware samples from trusted sources. These samples should encompass various types of malware, such as viruses, worms, Trojans, ransomware, and potentially unwanted applications (PUAs).  **Network Traffic Analyzers:**  Tools like Wireshark or tcpdump can capture and analyze network traffic generated by Sophos Endpoint Security and Control. This helps evaluate the effectiveness of firewall and network protection features, such as inbound and outbound traffic filtering, intrusion prevention, and application control.  **Performance Monitoring Tools:**  Performance monitoring tools can help measure the impact of Sophos Endpoint Security and Control on system resources. Tools like Task Manager (built-in in Windows), Resource Monitor, or third-party utilities like Process Explorer can monitor CPU usage, memory consumption, disk activity, and network utilization during different operations, including real-time scanning and malware detection.  **Reporting and Documentation Tools:**  Test plans and reports can all be created using applications like Microsoft Word, Excel, or Google Docs. These tools aid in the organised collection and presentation of the test results. | | | **Test Steps:** | | | 1. Launch Sophos Endpoint Security and Control on the test machine and ensure that real-time scanning and malware protection features are enabled and up to date. 2. Download a set of known malware samples from a trusted source. Include a variety of malware types, such as viruses, Trojans, worms, and ransomware. 3. Disable any other security software or antivirus programs running on the test machine to avoid interference. 4. Execute each malware sample, one at a time, on the test machine by either running the executable file or opening the infected document 5. Observe the behavior of Sophos Endpoint Security and Control during and after the execution of each malware sample. 6. Monitor the actions taken by Sophos Endpoint Security and Control for each malware sample, such as quarantine, removal, or blocking of malicious activities 7. Record the following details for each malware sample:  * Detection status: Whether the malware was detected by Sophos Endpoint Security and Control or not. * Actions taken: The specific actions performed by Sophos Endpoint Security and Control for each detected malware, such as quarantine, removal, or blocking. * Notifications or alerts: Any notifications or alerts displayed by Sophos Endpoint Security and Control during the detection and response process.  1. Repeat steps 4-7 for all the malware samples in the set. 2. After executing all the malware samples, review the quarantine or removal logs within Sophos Endpoint Security and Control to verify the actions taken for each detected malware. 3. Monitor the network traffic on the Linux Web Server during the simulated malware infection. 4. Observe how Sophos Endpoint Security and Control handles the malware attack by examining its logs, traffic patterns, and any detected anomalies. 5. Assess the impact on the Linux Web Server, such as any disruptions in services or degraded performance. 6. Document the observed results, including any deviations from the expected behavior. 7. Once the test is completed, analyze the test data, including performance metrics, logs, and any identified issues or vulnerabilities. | | | **Expected Results:** | | | * Sophos Endpoint Security and Control should demonstrate a high detection rate for the malware samples, minimising the risk of infection. * Each malware sample should be detected and handled appropriately, whether through quarantine, removal, or other designated actions. * Notifications or alerts should be displayed promptly, providing information on the detection and response to the malware. * The quarantine or removal logs within Sophos Endpoint Security and Control should accurately reflect the actions taken for each detected malware, enabling further analysis if needed. * False positives should be minimised, ensuring that legitimate files or applications are not incorrectly flagged as malware. | | | **Observed Results:** | | | It is usual practice to run an antivirus test using the EICAR test file to confirm the effectiveness of antivirus software. The EICAR test file, created by the European Institute for Computer Antivirus Research, is a safe file that is intended to cause antivirus software to respond in some way. The procedure is outlined as follows:  **Download the EICAR test file:** Obtain the EICAR test file from a reliable source. It is a small text file containing a string of characters that resembles a typical virus signature.  <https://www.eicar.com/download-anti-malware-testfile/>  **Disable real-time protection (optional):** If the antivirus software has real-time protection enabled, you can temporarily disable it to prevent the file from being immediately detected and quarantined.  In our test case, we choose to leave real-time protection on, to identify if Sophos is able to detect the file.  Scan the EICAR test file: If the file is not detected on download, you can Right-click on the downloaded EICAR file and select the option to scan it with the Sophos antivirus software.  **Observe the results**: After initiating the scan, the antivirus software should detect the EICAR file as a threat. The antivirus program should display a warning message or take appropriate actions, such as quarantining the file.  Reactivate real-time protection (optional): Once the test is complete, you can re-enable the real-time protection of your antivirus software if you had disabled it earlier.  It's important to remember that running the EICAR test file is a controlled way to check whether your antivirus program is operating as it should. The software's capacity to detect viruses in the actual world may differ.  **Results of test case:**  Sophos was able to detect the file upon download, and removed the file from our Linux Web Server. Screenshots of the process can be seen below; | | | **Pass/Fail:** | Based on the provided information, we can assess the test result as follows:  **Pass/Fail**: **Pass**  Based on the observed result and the nature of the Sophos log entry, it indicates that Sophos successfully blocked the virus / malware file from being downloaded to the system This aligns with the expected behavior of our antivirus application, Sophos Endpoint Security and Control  Since the observed result matches the expected behavior, we can consider the test result as **Pass**. | | |