**EQUIPMENT TEST PLAN SUMMARY**

| Project Title: | **AWS CyberShift Initiative** |  | Date Prepared: | | 9th of July, 2023 |
| --- | --- | --- | --- | --- | --- |

| **Program** | **OS** | **Purpose** | **Expected Outcome** | **Test method** | **Actual Outcome** | **Pass / Fail** |
| --- | --- | --- | --- | --- | --- | --- |
| **Splunk** | Windows | Log monitoring | When a failed SSH login attempt occurs, the alert should be triggered and a notification should be sent. | Generate test SSH login events with different failure scenarios | 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. | **Pass** |
| **Splunk** | Linux | Log monitoring | When a failed SSH login attempt occurs, the alert should be triggered and a notification should be sent. | Generate test SSH login events with different failure scenarios | The Sophos firewall logs successfully captured the failed login attempts.  Splunk received the forwarded logs and indexed them accordingly.  The Splunk management console displayed the received logs related to the failed logins | **Pass** |
| **pfsense** | Windows | Firewall | The logs and monitoring systems of pfSense should indicate the detection of the DDoS attack. This can be observed through increased traffic, abnormal patterns, or identified anomalies | Execute nmap command to simulate a DDoS attack | The log entry indicates that pfSense blocked a network traffic flow originating from the WAN (Wide Area Network) interface towards the private network with the IP address range of 192.168/16 (192.168.0.0 to 192.168.255.255). The specific traffic flow was identified as a UDP (User Datagram Protocol) communication. | **Pass** |
| **Sophos** | Linux | Firewall | The logs and monitoring systems of pfSense should indicate the detection of the DDoS attack. This can be observed through increased traffic, abnormal patterns, or identified anomalies | Execute nmap command to simulate a DDoS attack | The log entry indicates that pfSense blocked a network traffic flow originating from the WAN (Wide Area Network) interface towards the private network with the IP address range of 192.168/16 (192.168.0.0 to 192.168.255.255). The specific traffic flow was identified as a UDP (User Datagram Protocol) communication. | **Pass** |
| **Sophos** | Windows | Antivirus | Sophos Endpoint Security and Control should demonstrate a high detection rate for the malware samples, minimising the risk of infection. | 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 | 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 | **Pass** |
| **Sophos** | Linux | Antivirus | Sophos Endpoint Security and Control should demonstrate a high detection rate for the malware samples, minimising the risk of infection. | 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 | 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 | **Pass** |
| **Snort** | Windows | IDS / IPS | The hping3 command generates TCP traffic with the content "hping3," triggering the custom rule and generating an alert in Snort. | Run the following command to generate TCP traffic with the content "hping3":  hping3 -c 10 -p 80 -S 192.168.2.100 | The hping3 command generates TCP traffic with the content "hping3," triggering the custom rule and generating an alert in Snort. | **Pass** |
| **Snort** | Linux | IDS / IPS | The hping3 command generates TCP traffic with the content "hping3," triggering the custom rule and generating an alert in Snort. | Run the following command to generate TCP traffic with the content "hping3":  hping3 -c 10 -p 80 -S 192.168.2.100 | The hping3 command generates TCP traffic with the content "hping3," triggering the custom rule and generating an alert in Snort. | **Pass** |
| **Wireshark** | Windows | Packet analysis | Validate that Wireshark accurately interprets and decodes network protocols | Select a network interface from the available options within Wireshark.  Start a capture and confirm that Wireshark is able to capture network traffic.  Analyze the captured packets by applying filters, sorting, and examining protocol details. | Verify that the exported file is generated successfully and contains the captured data. | **Pass** |
| **Wireshark** | Linux | Packet analysis | Validate that Wireshark accurately interprets and decodes network protocols | Select a network interface from the available options within Wireshark.  Start a capture and confirm that Wireshark is able to capture network traffic.  Analyze the captured packets by applying filters, sorting, and examining protocol details. | Verify that the exported file is generated successfully and contains the captured data. | **Pass** |

| **Overall Summary** | | | | | |
| --- | --- | --- | --- | --- | --- |

The equipment test plan aims to validate the functionality and effectiveness of the chosen applications and tools for the AWS CyberShift Initiative, including Splunk, pfSense, Sophos Firewall, Sophos Antivirus, Snort, and Wireshark. Each of these applications serves different purposes within the system.

To test Splunk's log monitoring capabilities, a search query was executed to identify failed SSH login attempts with specific failure reasons and messages. The expected outcome was for Splunk to accurately detect and filter these events, which indicate potential security threats. Splunk successfully completed this test.

The pfSense and Sophos Firewall’s, were tested by generating network traffic from the WAN interface towards the private network with specific IP address ranges and protocols. The aim was to verify that both firewalls log and block the identified traffic flows as expected. In the observed outcomes, both applications successfully blocked UDP traffic flows originating from the WAN interface.

Sophos Antivirus for both the Windows Server and Linux systems was tested by attempting to download a known virus or malware file. Our expected outcome proved to be true, as Sophos was able to successfully block the download and log the event, indicating its ability to protect the system from malicious files.

Snort, an intrusion detection and prevention system (IDS/IPS), was tested using the hping3 command to generate TCP traffic with specific content that triggers a custom rule in Snort. The expected outcome was met, as Snort was able to generate an alert for the detected traffic flow, highlighting its capability to identify and respond to potential security threats.

Wireshark's packet analysis and data capturing functionalities were tested by capturing network traffic and exporting the captured data to a file. The expected outcome was success, shown by the generation of an exported file that contains the captured data for further analysis.

By performing these tests, the equipment test plan aims to ensure that each application and tool operates effectively and fulfills its intended purpose within the system. In all test cases, our applications performed as expected, and passed all tests successfully.

| **Approvals:** |
| --- |
| |  |  |  | | --- | --- | --- | | Project Manager Signature |  | Sponsor Or Originator Signature | |  |  |  | | Project Manager Name |  | Sponsor Or Originator Name | |  |  |  | | Date |  | Date | |