Test Specification

For

FreeEDR

Submitted by

FreeEDR

|  |  |
| --- | --- |
| **Instructor: Professor Greg Hislop** |  |
| **Team Members:** Bryan Bolesta, Ryan Fiers, Declan Kelly, Matthew Horger, Layla Phills, Zachary Santoro, Marisa Tranchitella |  |
| **Cycle: 1** |  |
| **Date Submitted: 2/23/2020** |  |

Document template copyright 2005-2019, Gregory W. Hislop. Version 2.2. Use permitted under Creative Commons license CC-BY-NC-SA. See http://creativecommons.org/licenses/by-nc-sa/3.0/.

Grading Rubric – Test Specification

This rubric outlines the grading criteria for this document. Note that the criteria represent a plan for grading. Change is possible, especially given the dynamic nature of this course. Any change will be applied consistently for the entire class.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Achievement** | **Minimal** | **Exemplary** | **Pts** | **Score** |
| **Content** | Section(s) missing, not useful, inconsistent, or wrong. | Provides all relevant information correctly and with appropriate detail |  |  |
| Introduction |  |  | 5 |  |
| Test Specs |  |  |  |  |
| Selection | Aspects tested are trivial | Tests clearly address core system functions | 20 |  |
| Organization | Tests are disorganized, IDs or Objectives are not meaningful | Tests are well-organized with structured IDs and clear objectives | 20 |  |
| Set-up | Steps are unclear or incomplete | Complete, easy to follow conditions and steps | 20 |  |
| Results | Unclear or incomplete | Complete and clear | 20 |  |
| **Grammar and Spelling** | Many serious mistakes in grammar or spelling | Grammar, punctuation, and spelling all correct | 5 |  |
| **Expression** | Hard to follow or poor word choices | Clear and concise. A pleasure to read | 5 |  |
| **Tone** | Tone not appropriate for technical writing | Tone is consistently professional |  |  |
| **Organization** | Information difficult to locate | All information is easy to find and important points stand out | 5 |  |
| **Layout** | Layout is inconsistent, visually distracting, or hinders use | Layout is attractive, consistent, and helps guide the reader |  |  |
| **Late Submission** |  |  |  |  |
| **Total** |  |  | 100 |  |

Table of Contents

[**Introduction**](#_heading=h.tyjcwt)5

[Purpose](#_heading=h.3dy6vkm) 5

[References](#_heading=h.1t3h5sf) 5

[**Testing Specifications**](#_heading=h.5c0fh6ddue97)5

[Server Requirements Testing](#_heading=h.t19xcwck9e5s) 5

[ST.1 - Server Test: Write Access (BB & LP)](#_heading=h.ti9pmm6h8j9r) 5

[ST.2 - Server Test: Read Access (BB & LP)](#_heading=h.h2rzubjlr7gq) 6

[ST.3 - Server Test: Execute Access (BB & LP)](#_heading=h.yuq0to40v773) 6

[ST.4 - Server Test: Least Privilege Access (BB & LP)](#_heading=h.4u1u1plwry5e) 7

[ST.5 - Server Test: Threat Intelligence Sources (BB & LP)](#_heading=h.bo9s85fvdbna) 7

[Client Requirements Testing](#_heading=h.i630d6ka9t4w) 8

[C.1. - Client Test: Client-Server Communication (BB)](#_heading=h.dpf3ewcxun6h) 8

[C.2 - Client Test: End-User Permissions (BB)](#_heading=h.9sb65vbaimu) 8

[C.3. - Client Test: Low-Impact Script Execution (BB & MT)](#_heading=h.yi45503oc5sb) 8

[C.4 - Client Test: Network Security Protocols (All)](#_heading=h.11dz29e57pru) 9

[C.5 - Client Test: Forensic API Communication (BB & MT)](#_heading=h.dl3r0ho3cjov) 10

[C.6 - Client Test: File-System Forensic Storage Access (MT & ZS)](#_heading=h.w5yo7nc115yk) 10

[C.7 - Client Test: File-System Forensic Storage Time (RF & MT)](#_heading=h.xd7z6mmd17nn) 10

[C.8 - Client Test: Incident Response Alerts (BB & MT)](#_heading=h.3lx56ud4oxoc) 11

[C.9 - Client Test: Forensics Identification (BB & MT)](#_heading=h.xu5eeqdk40yo) 11

[Dashboard Requirements Testing](#_heading=h.6c1jg0fobfuo) 12

[DB.1 - Dashboard Test: Dashboard Repository Connection Test (MH & MT)](#_heading=h.tel07a7cyv9l) 12

[DB.2 - Dashboard Test: Dashboard Okta Integration (MH & MT)](#_heading=h.a1k9yis2bzo8) 12

[DB.3 - Dashboard Test: Dashboard MUI Datatables Integration (MH & MT)](#_heading=h.z5wffkpdq2j3) 13

[DB.4 - Dashboard Test: Dashboard Permissions Matrix (MH & MT)](#_heading=h.huk45w3l0jc9) 13

[DB.5 - Dashboard Test: Dashboard Report Dates (MH & MT)](#_heading=h.54fx677trgq7) 14

[DB.6 - Dashboard Test: Dashboard Report Formats (MH & MT)](#_heading=h.9gpbj7ldrhv2) 14

[DB.7 - Dashboard Test: Dashboard Report Modal (MH & MT)](#_heading=h.har0dmjwrrfh) 14

[DB.8 - Dashboard Test: Dashboard Active Tracking (MH & MT)](#_heading=h.61f6jp4x5nj6) 15

[DB.9 - Dashboard Test: Dashboard Health Check (MH & MT)](#_heading=h.2anwfn7zdt72) 15

[Data Requirements Testing](#_heading=h.w6sf9t31r2sp) 16

[D.1 - Data Test: Data Manipulation Process (MT & LP & RF)](#_heading=h.vevv3bs63lsf) 16

[D.2 - Data Test: Event & Alert Data (BB & MT)](#_heading=h.a1ithqdbqom5) 16

[D.3 - Data Test: Uptime (BB & MT)](#_heading=h.5ebh43iaf336) 17

[D.4 - Data Test: Data Retention (MH)](#_heading=h.gwx01xmlbhjq) 17

[D.5 - Data Test: API Data Security (MH)](#_heading=h.u0gocsr40lca) 17

[D.6 - Data Test: Dashboard Data Access (BB & MT)](#_heading=h.rbbgk127l4wu) 18

[D.7 - Data Test: Dashboard Data Display (BB & MT)](#_heading=h.f4vnagvevnsa) 18

# Introduction

## Purpose

The purpose of this document is to outline all the test cases to be used during the testing cycle of the system FreeEDR. The test cases will outline the purpose of each test as it relates to a specific requirement, as well as define the success/failure threshold for each test case.

## References

Bolesta, B., Fiers, R., Kelly, D., Horger, M., Phills, L., Santoro, Z., & Tranchitella, M. (2020). *Software Requirements Specification for FreeEDR* (v 4.0.0).

# Testing Specifications

## Server Requirements Testing

### 2.1.1 ST.1 - Server Test: Write Access (BB & LP)

|  |  |
| --- | --- |
| **Objective** | To ensure that Script Managers, Incident Response Managers and Organization’s System Administrators have write access for Sigma rules |
| **Requirement** | R1.1 |
| **Setup** | Create accounts for a Script Manager, an Incident Response Manager, and System Administrator. Provide these accounts with Write permissions for the correlation rules stored on the Rule Storage Server. Attempt to write and save new changes to the rules as these accounts. Attempt to write and save new changes to the rules as an End User, Incident Response Supporter, and Auditor account. Rules should be located at "*\\10.0.20.57\freeedr\Rules*" |
| **Expected Results** | The Script Manager, Incident Response Manager, and System Administrator accounts should write changes to the rules. The other accounts, such as End User, IR Supporter, and Auditor should all be restricted from writing changes to the rules. |
| **Actual Results** |  |

### 

### 2.1.2 ST.2 - Server Test: Read Access (BB & LP)

|  |  |
| --- | --- |
| **Objective** | To ensure that Script Managers, Incident Response Managers, Incident Response Supporters, System Auditors and Organization's System Administrators have read access for Sigma rules |
| **Requirement** | R1.2 |
| **Setup** | Create accounts for a Script Manager, an Incident Response Manager, Incident Response Supporter, Auditor, and System Administrator. Provide these accounts with Read permissions for the correlation rules stored on the Rule Storage Server. Attempt to view and read the rules. Attempt to read the rules as an End User account. Rules should be located at "*\\10.0.20.57\freeedr\Rules*" |
| **Expected Results** | The Script Manager, Incident Response Manager, Incident Response Supporter, Auditor, and System Administrator accounts should successfully be able to view and read the rules. The end user account should be restricted from viewing and reading the rules. |
| **Actual Results** |  |

### 2.1.3 ST.3 - Server Test: Execute Access (BB & LP)

|  |  |
| --- | --- |
| **Objective** | To ensure that Script Managers, Incident Response Managers and Organization's System Administrators have read access for Sigma rules |
| **Requirement** | R1.3 |
| **Setup** | Create accounts for a Script Manager, an Incident Response Manager, and System Administrator. Provide these accounts with Execute permissions for the correlation rules stored on the Rule Storage Server. Attempt to execute and deploy the rules as these accounts. Attempt to execute and deploy the rules as an End User, Incident Response Supporter, and Auditor account. Rules should be located at "*\\10.0.20.57\freeedr\Rules*" |
| **Expected Results** | The Script Manager, Incident Response Manager, and System Administrator accounts should successfully be able to execute and deploy the rules. The other accounts, such as End User, IR Supporter, and Auditor should all be restricted from executing and deploying the rules. |
| **Actual Results** |  |

### 2.1.4 ST.4 - Server Test: Least Privilege Access (BB & LP)

|  |  |
| --- | --- |
| **Objective** | To ensure that End Users do not have permissions to read, write or execute Sigma rules |
| **Requirement** | R1.4 |
| **Setup** | Create an End User account and do not provide this account with any permissions pertaining to the rules stored on the Rule Storage Server. Attempt to read the rules, write changes to the rules, and execute the rules as the End User account. The rules should be located at "*\\10.0.20.57\freeedr\Rules*" |
| **Expected Results** | End User should be unsuccessful at accessing, reading, writing, and executing any of the correlation rules stored in the Rule Storage Server rule repository. |
| **Actual Results** |  |

### 2.1.5 ST.5 - Server Test: Threat Intelligence Sources (BB & LP)

|  |  |
| --- | --- |
| **Objective** | To ensure that FreeEDR is able to communicate and connect with threat intelligence sources, as well as discover and store new sigma rules in the rule repository |
| **Requirement** | R1.5 |
| **Setup** | Ensure there are new sigma correlation rules stored in Security Risk Advisors’ TALR GitHub project. The rules are located at ([https://github.com/SecurityRiskAdvisors/TALR/tree/master/Rules](https://github.com/SecurityRiskAdvisors/TALR/tree/master/Rules/Sigma)). As a Script Manager account, use the main FreeEDR script to communicate with the Threat Intelligence sources (such as TALR) to discover the new sigma correlation rules and store them on the Rule Storage Server’s rule repository |
| **Expected Results** | The new sigma correlation rules from the TALR GitHub page should be copied into Rule Storage Server’s rule repository. The rules should be located at "*\\10.0.20.57\freeedr\Rules*" |
| **Actual Results** |  |

## Client Requirements Testing

### 2.2.1 C.1. - Client Test: Client-Server Communication (BB)

|  |  |
| --- | --- |
| **Objective** | To ensure that clients can use the communication channel to pull down correlation rules from the Rule Storage Server |
| **Requirement** | R2.1 |
| **Setup** | The Rule Storage Server should contain new rules in the rule repository that the client system does not currently possess. As a Script Manager account, attempt to use the main FreeEDR script to communicate and deploy new correlation rules to the client system. |
| **Expected Results** | The client system successfully pulls all new rules from the Rule Storage Server. Rules should be located on the client system under the"*C:\Windows\freeedr\*" folder. The files in this folder should match what is stored in the Rule Storage Server’s rule repository, located under "*\\10.0.20.57\freeedr\Rules*" |
| **Actual Results** |  |

### 2.2.2 C.2 - Client Test: End-User Permissions (BB)

|  |  |
| --- | --- |
| **Objective** | To ensure that End Users cannot read, write, or execute correlation rules stored on the client system |
| **Requirement** | R2.2 |
| **Setup** | Create an End User account and do not provide any permissions pertaining to FreeEDR or the correlation rules. As the End User account, attempt to read, write, and execute the correlation rules stored on the client system. The rules should be located at "*C:\Windows\freeedr\*" |
| **Expected Results** | The End User account should be unsuccessful at reading, writing, or executing any of the rules stored on the client system. |
| **Actual Results** |  |

### 

### 2.2.3 C.3. - Client Test: Low-Impact Script Execution (BB & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will force clients to check correlation rules against the event log at a rate configured by the Script Manager (should be non-disruptive to normal client activity) |
| **Requirement** | R2.3 |
| **Setup** | As a Script Manager account, configure the script to check rules against event logs at a rate that will not disrupt normal client activity. Deploy the FreeEDR script to a client system and ensure it runs at the configured rate. On the client system, simulate normal client activity as the FreeEDR script executes. Ensure that normal client activity is not disrupted because of the FreeEDR script running and checking rules against the event log. |
| **Expected Results** | The FreeEDR script checks rules against the event log at the rate configured by the Script Manager. The user was able to complete normal client activity on the client system without any disruptions from the FreeEDR script. |
| **Actual Results** |  |

### 

### 2.2.4 C.4 - Client Test: Network Security Protocols (All)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will establish network security protocols to permit clients to communicate with APIs. |
| **Requirement** | R2.4 |
| **Setup** | WCF service properly setup on an IIS instance. Okta roles setup for endpoint security |
| **Expected Results** | Client will navigate to the Dashboard, upon which the service account running the UI will call the endpoints. If a client then copies the endpoint url, the client should not be able to retrieve data back, as the security protocol is in place. |
| **Actual Results** |  |

### 

### 2.2.5 C.5 - Client Test: Forensic API Communication (BB & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will allow clients to receive information from APIs to perform network and process forensics on an event. |
| **Requirement** | R2.5 |
| **Setup** | Generate an event on a client system that will match the requirements of a correlation rule and trigger an alert. As a Script Manager account, deploy the FreeEDR script to the client. Then view the newly generated event and check to see if process and network forensics information from the APIs has been added to the event. |
| **Expected Results** | Generated events should display process and network forensic information retrieved from APIs |
| **Actual Results** |  |

### 

### 2.2.6 C.6 - Client Test: File-System Forensic Storage Access (MT & ZS)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will be able to store clients’ process and network forensic information within the organization’s filesystem. |
| **Requirement** | R2.6 |
| **Setup** | Generate an event on a client system that will match the requirements of a correlation rule and trigger an alert. Open the Windows Event Viewer and confirm that custom Windows event exists. |
| **Expected Results** | A custom Windows Event will exist in the Windows logs section of the Event Viewer. |
| **Actual Results** |  |

### 

### 2.2.7 C.7 - Client Test: File-System Forensic Storage Time (RF & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will store the referenced forensic information for the amount of time set by the organization’s system administrator. |
| **Requirement** | R2.7 |
| **Setup** | Generate an event on a client system that will match the requirements of a correlation rule and trigger an alert. Once the event has been generated, view the associated forensic data. At the point at which the forensic data is supposed to be deleted, ensure it exists up to the deletion point. |
| **Expected Results** | The event forensic data will exist for the amount of time set by the system administrator. After that point in time has been reached, the forensic data will be deleted from the FreeEDR system. |
| **Actual Results** |  |

### 

### 2.2.8 C.8 - Client Test: Incident Response Alerts (BB & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR can forward forensic events from clients to the Incident Response Manager in order for them to properly perform their user roles. |
| **Requirement** | R2.8 |
| **Setup** | Generate an event on a client system that will match the requirements of a correlation rule and trigger an alert. As a Script Manager account, deploy the FreeEDR script to the client system. Once FreeEDR has finished deploying, view FreeEDR alerts as an Incident Response Manager account and check for new alerts generated from the script deployment. |
| **Expected Results** | The Incident Response Manager should receive an alert notification stating that the event performed during the test has occurred and has triggered an alert. |
| **Actual Results** |  |

### 

### 2.2.9 C.9 - Client Test: Forensics Identification (BB & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR can distinguish which forensics must be applied for different client processes and network events. |
| **Requirement** | R2.9 |
| **Setup** | Generate process and network events on a client system that will match the requirements of correlation rules and generate alerts. As a Script Manager account, deploy the FreeEDR script to the client system. Once FreeEDR has finished deploying, view FreeEDR alerts as an Incident Response Manager account and check for new alerts generated from the script deployment. View the alerts for the process and network events generated during the test. Ensure that alerts pertaining to a process event contain process forensic information. Ensure that alerts pertaining to a network event contain network forensic information. |
| **Expected Results** | Generated events and alerts for process events will contain process forensic information. Generated events and alerts for network events will contain network forensic information. |
| **Actual Results** |  |

## Dashboard Requirements Testing

### DB.1 - Dashboard Test: Dashboard Repository Connection Test (MH & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will allow for communication between the dashboard and the secure repository used for rule storage. |
| **Requirement** | R3.1 |
| **Setup** | Ensure that the internal data service (WCF) is running in an application pool and the UI Dashboard is hosted. |
| **Expected Results** | Visit the Dashboard’s Admin page. When the page loads, an endpoint will be called which will try to communicate with the repository. If no connection can be made, a warning message is shown to the user. |
| **Actual Results** |  |

### 

### DB.2 - Dashboard Test: Dashboard Okta Integration (MH & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will grant permission all users read access to the deployed dashboard and to block all external traffic to the dashboard. |
| **Requirement** | R3.2 |
| **Setup** | Setup user roles within developer Okta instance. Add the redirect URL from the React application to the Native app instance. |
| **Expected Results** | A user who has not received an authorization token will be prompted with the Okta SSO login screen. Those who enter valid credentials are allowed access. Those who do not have access will be prompted by Okta that they do not have permissions to the application. |
| **Actual Results** |  |

### 

### DB.3 - Dashboard Test: Dashboard MUI Datatables Integration (MH & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR must provide the ability for clients to view previously generated reports as well as produce fresh reports. |
| **Requirement** | R3.3 |
| **Setup** | Constructor for MUI Datatables in React JSX |
| **Expected Results** | Clients should be presented with the list of recent reports on the home page. Client then switches to the report tab to generate a report. After generation, a new row should be inserted in the table on the home page. |
| **Actual Results** |  |

### 

### DB.4 - Dashboard Test: Dashboard Permissions Matrix (MH & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will allow for the Dashboard Infrastructure Manager to permission certain clients to view specific reports and actions. |
| **Requirement** | R3.4 |
| **Setup** | Setup a user role in Okta as a Dashboard Infrastructure Manager |
| **Expected Results** | Specific user with access visits the permissions matrix via the admin tab. This user then can modify the active directory groups to grant permissions to other users linked in Okta to the specific reports. |
| **Actual Results** |  |

### DB.5 - Dashboard Test: Dashboard Report Dates (MH & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will allow clients to select a range of dates for report generation within the dashboard. |
| **Requirement** | R3.5 |
| **Setup** | Client selects a report to generate from the Dashboard. |
| **Expected Results** | Client should first generate a report in PDF format for the current date. Then, client should then generate the same report in PDF format for an effective date to make sure the content of the document has changed. |
| **Actual Results** |  |

### 

### DB.6 - Dashboard Test: Dashboard Report Formats (MH & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will allow clients to select a specific format to download their generated reports from the dashboard. |
| **Requirement** | R3.6 |
| **Setup** | Client selects a report to generate |
| **Expected Results** | Client should first generate a report in the default PDF format. Then, client should generate the same report in the DOCX format to ensure content is the same. |
| **Actual Results** |  |

### 

### DB.7 - Dashboard Test: Dashboard Report Modal (MH & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will have an option to export a dashboard report to send via interdepartmental communication (email, IM, etc). |
| **Requirement** | R3.7 |
| **Setup** | Client must select a report to export |
| **Expected Results** | Once a report is generated, client selects the option to export the report via email. Client enters in the intended email address. Client then verifies in-person that this email in fact was sent. Client then sends another report, this time in a different format, via the same export function via the reporting modal. |
| **Actual Results** |  |

### DB.8 - Dashboard Test: Dashboard Active Tracking (MH & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will allow the dashboard to have a responsive algorithm that allows for regeneration of reports once fresh data is produced. |
| **Requirement** | R3.8 |
| **Setup** | Client must be connected to the dashboard. |
| **Expected Results** | One client connects to the Dashboard and halts. Another client performs two unique report generations using the Dashboard. The hanging client then resumes operations and tries to generate a report. Before the report is generated, the page is refreshed with the latest data and datetimes from the reporting folder. |
| **Actual Results** |  |

### 

### DB.9 - Dashboard Test: Dashboard Health Check (MH & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will maintain dashboard accessibility 90% of normal business hours, with the exception of disaster recovery downtime or failover procedures. |
| **Requirement** | R3.9 |
| **Setup** | N/A |
| **Expected Results** | Test client will be used with an automated test script, running every hour in Postman, to test our WCF endpoint which returns the status of the IIS service. If a successful result is obtained, the test client continues operations in the next iteration. If a failure is obtained, an email message is sent out to [freeedr@outlook.com](mailto:freeedr@outlook.com). This test will require the dashboard to be brought down in order to test the email alert. |
| **Actual Results** |  |

## Data Requirements Testing

### D.1 - Data Test: Data Manipulation Process (MT & LP & RF)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will have an established process in order to track requests, actions, etc in regards to manipulation of data in the system. |
| **Requirement** | R4.1 |
| **Setup** | Create sample forensic data from an endpoint. This can be done by using a sample malicious document and executing it on the endpoint. Ensure a minimum of 3 events have been created.  Generate three sample API requests as well as two sample reports. Ensure each request is manipulating data within the FreeEDR system and producing a resulting file / response. |
| **Expected Results** | Each action will be tracked within the internal FreeEDR system audit log. |
| **Actual Results** |  |

### 

### D.2 - Data Test: Event & Alert Data (BB & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will present Incident Response teams with data on endpoint events (i.e. registry modifications, cross-process events, file executions, network connections). |
| **Requirement** | R4.2 |
| **Setup** | Perform simulated attacks on a test endpoint system to generate sample events. Some sample attacks include attempting to modify the registry, creating scheduled tasks, enumerating system and network information, and more. As a Script Manager account, deploy the FreeEDR script to the client system. Once FreeEDR has finished generating alerts based on the simulated attacks, view the alerts as an Incident Response Manager account. Ensure that the alerts provide data on the events generated by the simulated attacks, as well as process and network forensic information. |
| **Expected Results** | Incident Response Managers are able to view alerts generated by FreeEDR that provide data and forensic information on endpoint events |
| **Actual Results** |  |

### D.3 - Data Test: Uptime (BB & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will maintain 100% uptime access to relevant data sources needed for operations. |
| **Requirement** | R4.3 |
| **Setup** | From the Windows Server that stores the FreeEDR project, launch command-prompt and run the command “*net statistics server*” to display server statistics. Locate the “Statistics since…” line, which indicates the date and time that the uptime started. |
| **Expected Results** | The server that stores FreeEDR has maintained 100% uptime. |
| **Actual Results** |  |

### D.4 - Data Test: Data Retention (MH)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will keep data for up to 5 years in order to comply with SOC1 reporting/audit procedures. Data beyond 5 years retention may be disposed of. |
| **Requirement** | R4.4 |
| **Setup** | Numerous reports and audits must be present in a folder structure within the FreeEDR system. |
| **Expected Results** | Using an automated test script which can be run ad-hoc, an example file with a DateTimeStamp of Effective Run Date - 5 years will be produced and dropped in the file. Then, before the next audit is generated via the dashboard, the stale file will be removed and the audit will be placed in the folder stating which data was removed from the system. |
| **Actual Results** |  |

### 

### D.5 - Data Test: API Data Security (MH)

|  |  |
| --- | --- |
| **Objective** | To ensure data transmitted via every API in FreeEDR is under the proper protocols for security (POST) and sensitive information is encrypted in transit. |
| **Requirement** | R4.5 |
| **Setup** | Postman JSON Endpoint Suite Required |
| **Expected Results** | In Postman, each endpoint will be tested to make sure data is only returned via HTTPS, not HTTP. Any HTTP error will be thrown as 401: Not Found or a Web.config exception from IIS. All POST endpoints will be called with the GET request to make sure data is not returned. |
| **Actual Results** |  |

### D.6 - Data Test: Dashboard Data Access (BB & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR allows dashboard access to all necessary data in order to produce reports, including forensic event information, user machine configuration, and standard log outputs. |
| **Requirement** | R4.6 |
| **Setup** | The FreeEDR script should be used prior to this test so that the dashboard is populated with sample events and alerts. As an Incident Response Manager account, access the dashboard and view the data provided by events. Ensure that the data present includes forensic event information, user machine configuration information, and standard output logs. |
| **Expected Results** | The dashboard should provide access to event data. This data should include forensic event information, user machine configuration, and standard output logs. |
| **Actual Results** |  |

### 

### D.7 - Data Test: Dashboard Data Display (BB & MT)

|  |  |
| --- | --- |
| **Objective** | To ensure FreeEDR will display data in the dashboard in a concise, readable format with an option for details to be viewed separately. |
| **Requirement** | R4.7 |
| **Setup** | The FreeEDR script should be used prior to this test so that the dashboard is populated with sample events and alerts. As an Incident Response Manager account, access the dashboard and view the data provided by events. Ensure the data is in a viewable and readable format with an option to view event details separately. |
| **Expected Results** | The data displayed by the dashboard is in a concise, readable format with an option to view details separately. |
| **Actual Results** |  |