

CYBER AWARENESS REPORTING TOOL



ATHENA CONSULTING GROUP

1083-C East Montague Ave, North Charleston, SC 29405

Cyber Awareness Reporting Tool (CART) User Manual

CONTENTS

Registering CART.....	1
Overview.....	5
Status Overview	5
Controls Overview	7
Importing Vulnerabilities	10
ACAS-Nessus Scan Results	10
STIG Viewer Checklists	13
Import SCAP Results.....	15
Resetting CART.....	17

REGISTERING CART

1. Upon opening the CART application, a Security Warning will most likely appear. This warning is due to the Visual Basic for Applications code in the Access Database file. It is safe to open the file.

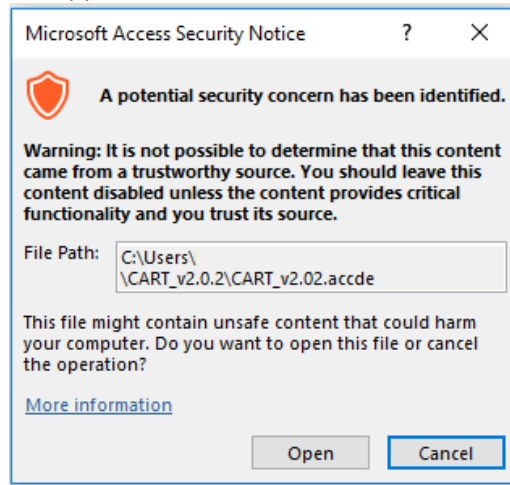


Figure 1

2. After the Security Notice, the End User Licensing Agreement (EULA) will appear. You must read and agree to the terms of the EULA to continue using CART.

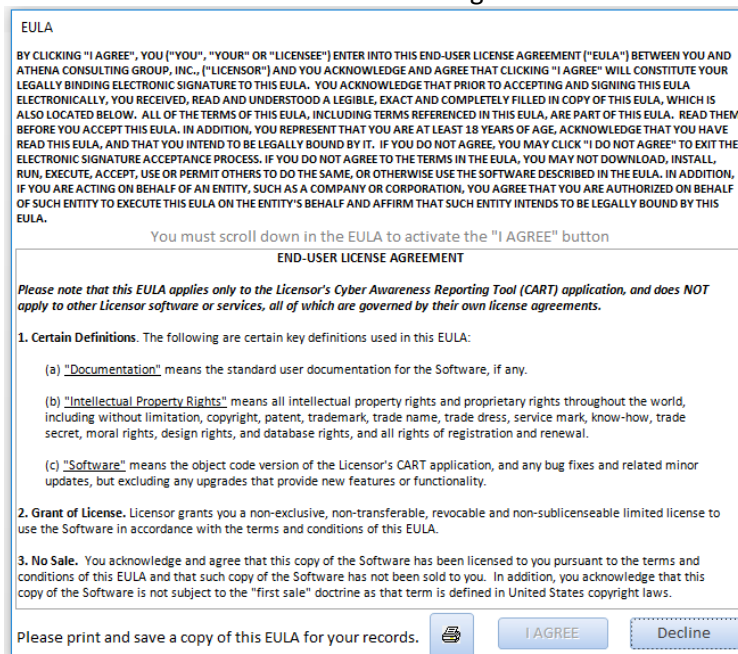


Figure 2

Declining the agreement will immediately close the program. The “I Agree” button will not be enabled until scrolling through the EULA.

3. After reading the EULA and clicking "I Agree", the application will check the license. If the license is invalid/expired or the application has not been registered yet, a prompt to register the program will appear.

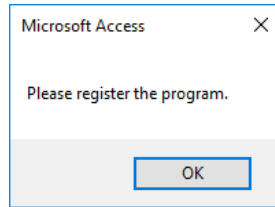


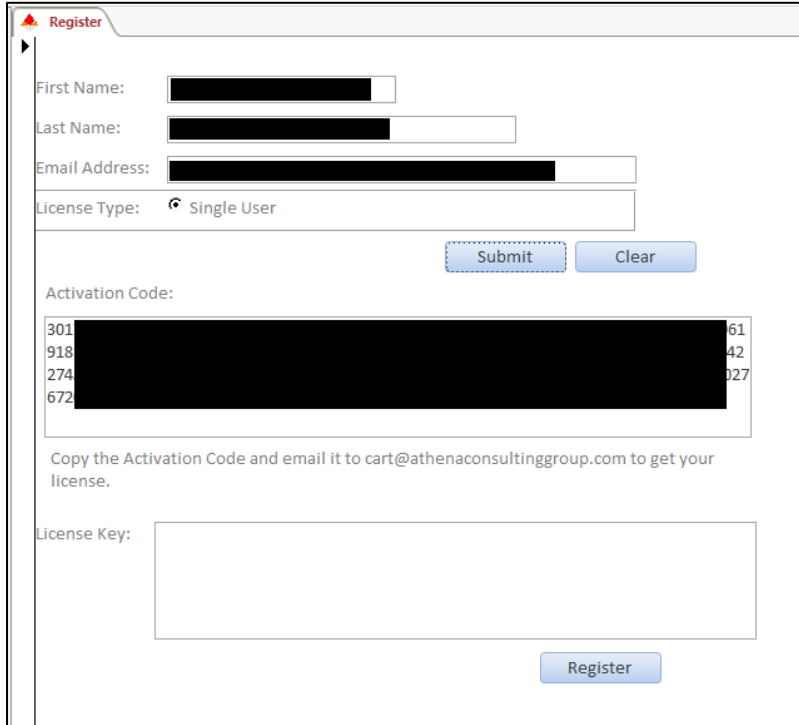
Figure 3

4. Next, the Registration Form will appear.

A registration form window titled "Register" with a red triangle icon. The form contains several input fields and buttons. The fields are: "First Name:" with a text box; "Last Name:" with a text box; "Email Address:" with a text box; "License Type:" with a dropdown menu showing "Single User" and a radio button icon; "License Key:" with a large text box. There are three buttons: "Submit" and "Clear" are positioned to the right of the "License Type" dropdown; "Register" is positioned below the "License Key" text box.

Figure 4

5. Complete the Registration Form and click the Submit button to generate the Activation Code.

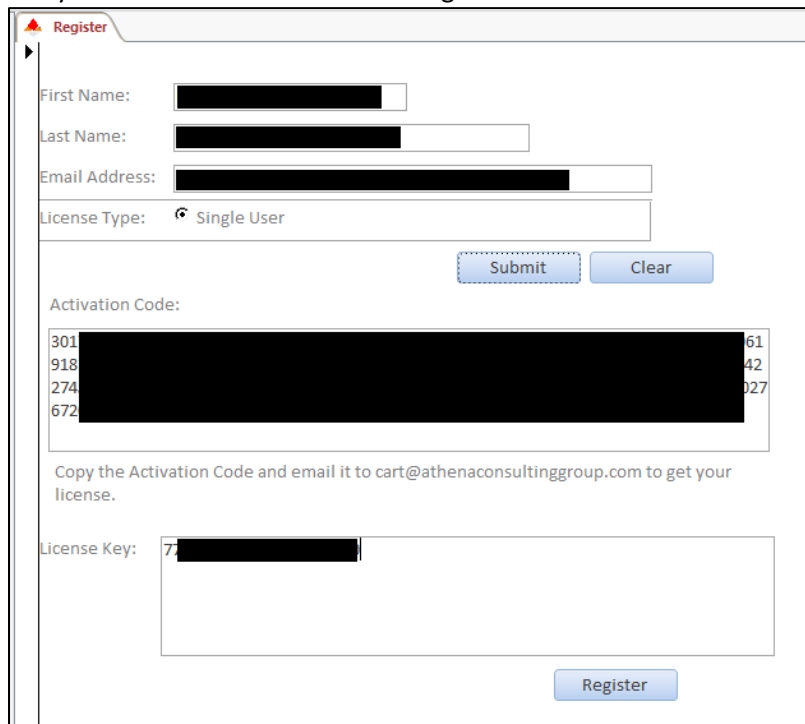


The screenshot shows a web browser window titled "Register". The form contains the following fields and elements:

- First Name: [Redacted]
- Last Name: [Redacted]
- Email Address: [Redacted]
- License Type: Single User
- Buttons: Submit, Clear
- Activation Code: [Redacted]
- Text: Copy the Activation Code and email it to cart@athenaconsultinggroup.com to get your license.
- License Key: [Empty text box]
- Button: Register

Figure 5

6. Copy the Activation Code, in its entirety, and paste it into the body of an email to cart@athenaconsultinggroup.com. A License Key will be generated and sent back within 24 hours. Upon receipt of the email with the License Key, open CART if not already opened and paste the License Key in the text box and click the Register button.



The screenshot shows the same "Register" web browser window. The form is identical to Figure 5, but with the following changes:

- License Key: [7 [Redacted]]
- Button: Register

Figure 6

7. After pasting in the License Key and clicking the Register button, the program will be activated and ready for use.

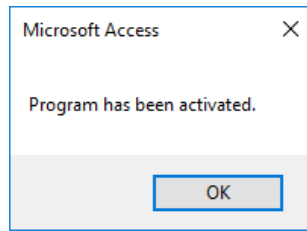


Figure 7

OVERVIEW

The CART Dashboard presents a detailed summary of the vulnerabilities imported into the database. All import and reporting functions are conducted from the “Controls” tab.

Status Overview

1. The Status page displays the CART Dashboard.

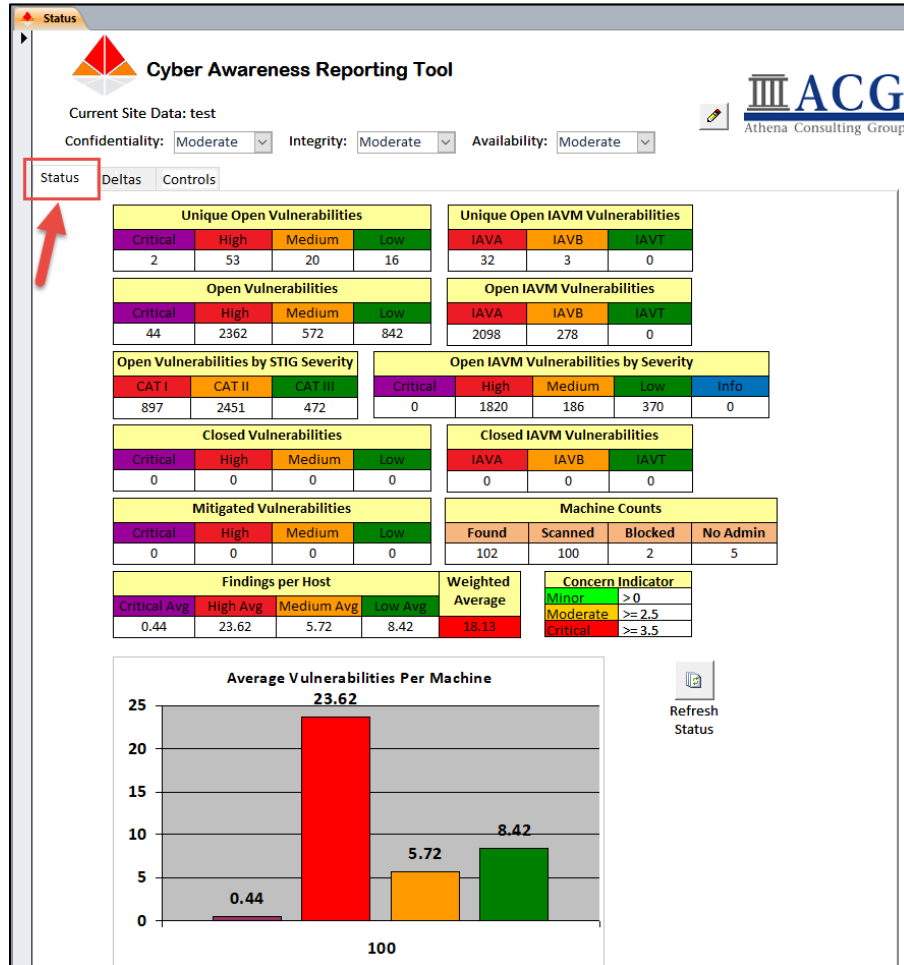


Figure 8

2. The following vulnerability information is displayed on the Dashboard:
 - a. Unique Open Vulnerabilities: Displays the aggregated unique open vulnerabilities by severity.
 - b. Unique Open IAVM Vulnerabilities: Displays the aggregated unique open IAVM related vulnerabilities by severity.
 - c. Open Vulnerabilities: Displays the total number of open vulnerabilities by severity.
 - d. Open IAVM Vulnerabilities: Displays the total number of IAVM related vulnerabilities by IAVM category.
 - e. Open Vulnerabilities by STIG Severity: Displays the total number of vulnerabilities by STIG severity (Category I, Category II, and Category III).
 - f. Open IAVM Vulnerabilities by Severity: Displays the total number of IAVM related vulnerabilities by STIG severity (Category I = High, Category II = Medium, Category III = Low).

- g. Closed Vulnerabilities: Displays the total number of vulnerabilities, by severity, that have been updated in CART as Closed.
- h. Closed IAVM Vulnerabilities: Displays the total number of IAVM related vulnerabilities, by severity, that have been updated in CART as Closed.
- i. Mitigated Vulnerabilities: Displays the total number of vulnerabilities, by mitigated severity, that have been mitigated down to a lower severity but still remain Open. Mitigated severities are subtracted from the Open Vulnerabilities. For example, if there are 45 High severity Open Vulnerabilities and 1 is mitigated to a Low severity, then the Open Vulnerabilities table will show 44 High and the Mitigated Vulnerabilities table will show 1 Low severity.
- j. Machine Counts:
 - i. Found: Total number of machines found in the scan results
 - ii. Scanned: Total number of machines successfully scanned
 - iii. Blocked: Total number of machines with no audit information, indicating the scans were blocked by the Host Intrusion Prevention System (HIPS).
 - iv. No Admin: Total number of machines with scan information, but the scanner was not able to successfully authenticate with administrator privileges.
- k. Findings per Host and Weighted Average: Displays the (Cybersecurity Compliance Readiness Inspection (CCRI) Score for the aggregated results.
- l. Average Vulnerabilities Per Machine Graph

Controls Overview

1. Clicking the Controls tab will show the Controls page.

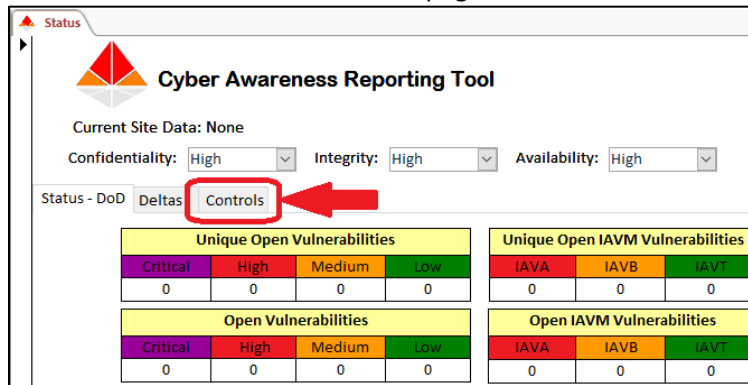


Figure 9

2. From here, all the import and reporting functions of the database are conducted.

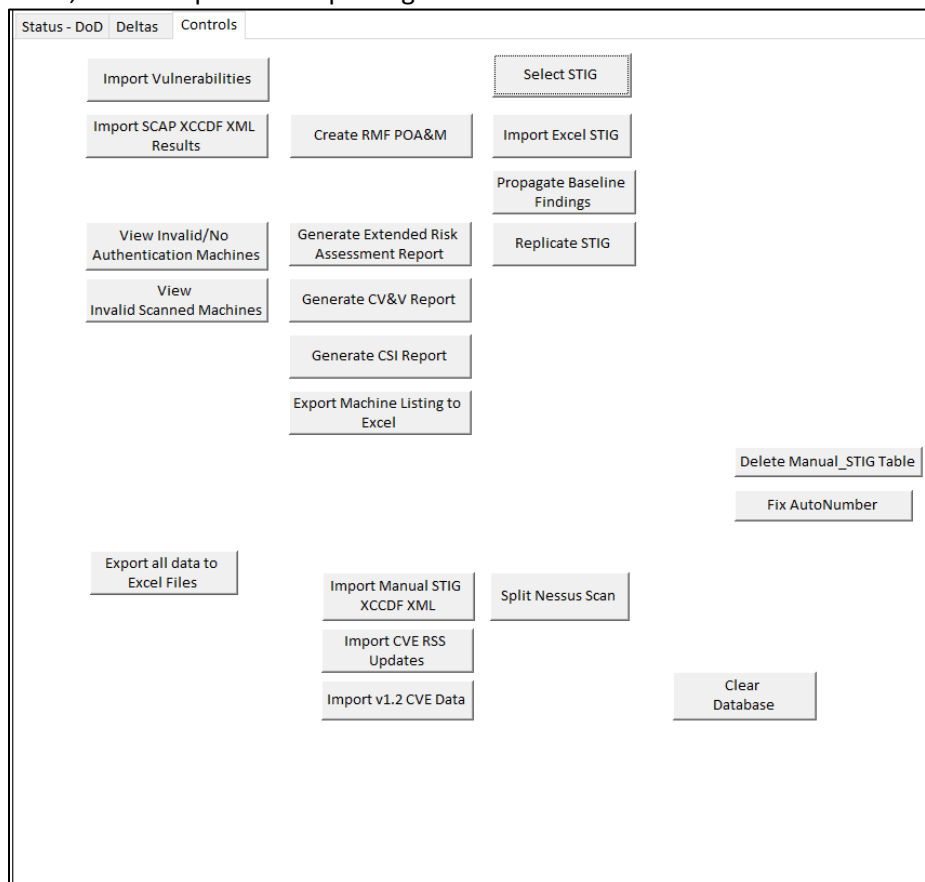


Figure 10

3. The following is a description of each of the buttons on the Controls page:

- **Import Vulnerabilities:**
Using the Import Vulnerabilities button, the CART application can import the following types of files:
 - ACAS Nessus Scan Results (.nessus files)
 - STIG Viewer Checklist Results (.ckl files)
- **Import SCAP XCCDF XML Results**

Using the Import SCAP XCCDF XML Results button, the CART application can import the XCCDF results from the SCAP Compliance Checker (SCC) tool.

- **View Invalid/No Authentication Machines:**
Executes a query to display all of the machines that Nessus scanned without proper credentials or was not able to authenticate. Scanning without authentication is considered an invalid scan because the registry and local files are not able to be checked.
- **View Invalid Scanned Machines:**
Executes a query to display all of the machines that Nessus was not able to successfully scan. Essentially creates a machine with no audits/vulnerabilities. This can be due to HBSS blocking the Nessus scanner.
- **Export all data to Excel Files:**
Exports the data for each machine and each data source to Excel. For example, if there is a Windows 7 workstation with Nessus scan results and Windows 7 STIG results, two Excel files will be generated with the Machine Name and Source for the name of each file.
- **Create RMF POA&M:**
Generates an eMASS importable RMF POA&M.
- **Generate Extended Risk Assessment Report:**
Generates a customized Risk Assessment Report that combined elements of the RMF POA&M and the Navy Risk Assessment Report.
- **Generate CV&V Report:**
Generates a HTML report of the top offenders and top vulnerabilities.
- **Generate CSI Report:**
Generates a HTML report customized for Cyber Security Inspection reporting.
- **Export Machine Listing to Excel:**
Generates an Excel file listing all Workstations on one sheet, Servers on another sheet, and Other on a third sheet.
- **Import Manual STIG XCCDF XML:**
Imports the Manual Security Technical Implementation Guide XCCDF XML files into the database. Manual STIG checklists are not preloaded into CART, allowing the user to update the database with the most current releases from DISA.
- **Split Nessus Scan:**
Splits a large .nessus file into smaller chunks. Due to limitations within Access, Nessus files near or larger than 2 gigabytes cannot be imported. By splitting the large files into multiple smaller files, the scan results can be imported into and processed by CART.
- **Select STIG:**
Once a STIG has been imported, through "Import Manual STIG XCCDF XML", it can be selected and linked to a machine/site.
- **Import Excel STIG:**
Imports a completed Excel formatted STIG Checklist. CART will create a table link to the Excel spreadsheet and merge the results to the appropriate tables. If using Microsoft Access Runtime and not the full version of Microsoft Access, then the "Delete Manual_STIG Table" button must be used prior to importing each additional Excel STIG checklist.
- **Propagate Baseline Findings:**
Applies the findings from a baseline machine to all "like-kind" machines in the sample group.
- **Replicate STIG:**
Links a STIG checklist to several machines.
- **Delete Manual_STIG Table:**

When using CART with the Microsoft Access Runtime, there is a bug with the importing of Excel STIG Checklists and requires the table link to the Excel file to be deleted through this button. This bug does not occur when using CART with the full Microsoft Access application.

- Clear Database:
Removes all imported machines and data, resetting CART for next test event.

IMPORTING VULNERABILITIES

ACAS-Nessus Scan Results

1. From the main Status page, click the “Controls” tab.

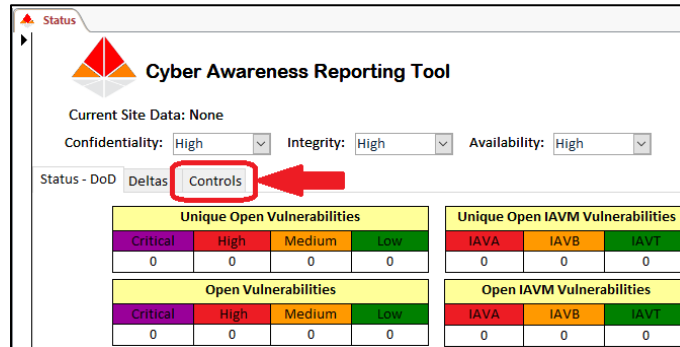


Figure 11

2. On the “Controls” page, click the “Import Vulnerabilities” button.

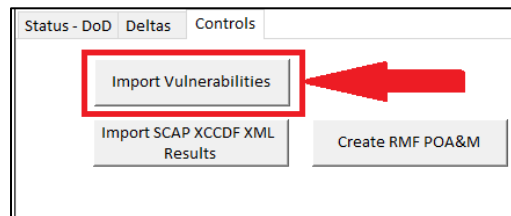


Figure 12

3. The tool can import the following formats through the Import Vulnerabilities button:
 - a. Nessus Vulnerability Scan Results file (.nessus file extension)
 - b. STIG Viewer Checklist (.ckl file extension)
4. Select the file to import. For the purpose of this section, a Nessus Scan Result file is being used.

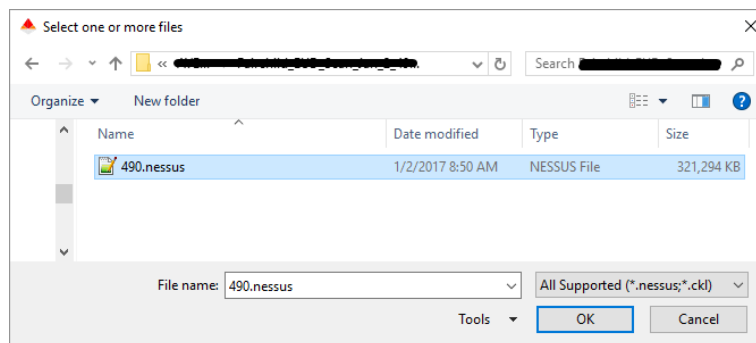


Figure 13

5. Enter the site/program name the scan data is for.

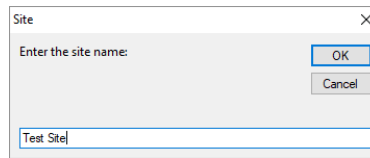


Figure 14

6. CART will display the progress of the import.

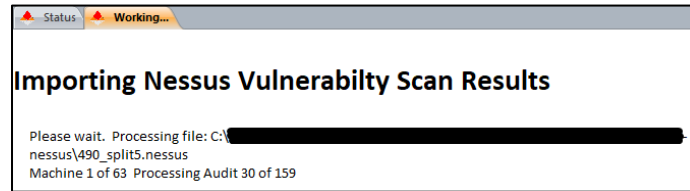


Figure 15

7. If the Nessus scan has STIG Benchmarks included, CART will prompt for the import of the applicable STIG Template if it has not already been imported into the tool. NOTE: There is a known problem with a couple of the STIG XCCDF Templates where the name of the STIG does not match the name of the file. CART uses the XCCDF file name for matching. One in particular is the Microsoft .NET Framework STIG. See Appendix A for detailed instructions on resolving these issues until a fix in CART is implemented.

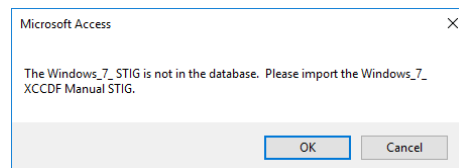


Figure 16

8. Upon completion of the import, the updated "Status" page will be presented.

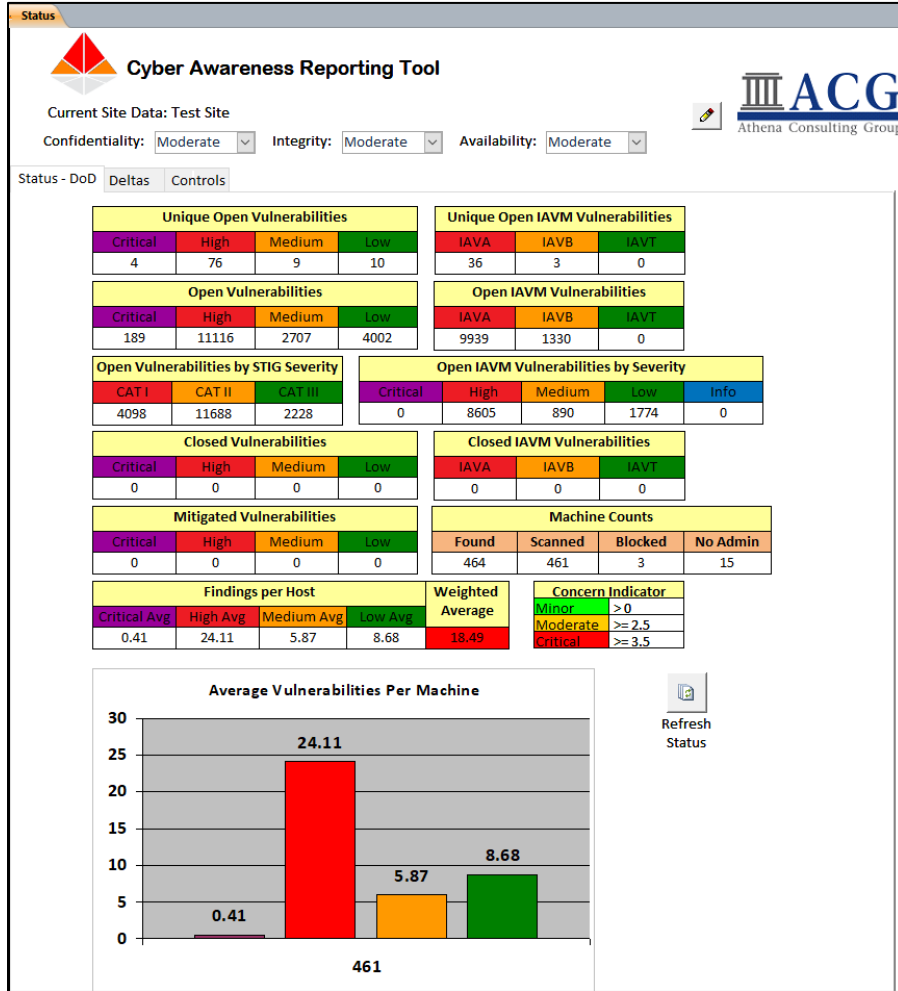


Figure 17

STIG Viewer Checklists

1. From the main Status page, click the “Controls” tab.

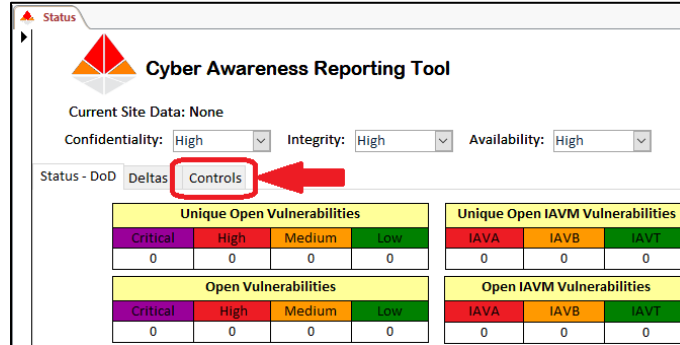


Figure 18

2. On the “Controls” page, click the “Import Vulnerabilities” button.

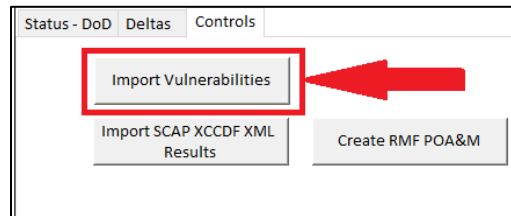


Figure 19

3. Select the STIG Viewer Checklist(s) to import. More than one file can be selected.

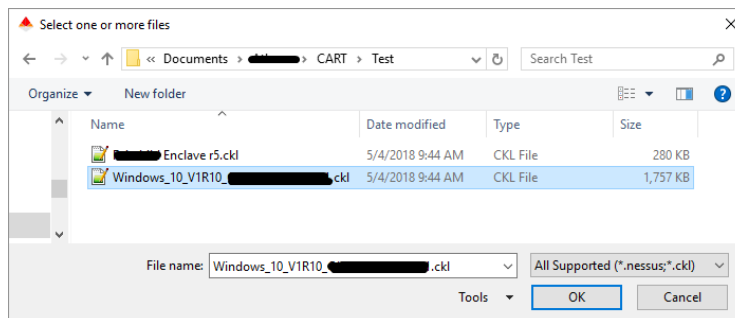


Figure 20

- If the Manual STIG XCCDF Template has not been imported, CART will prompt for the import of the applicable STIG. The name of the STIG should be the file name of the .kcl, as shown below. NOTE: There is a known problem with a couple of the STIG XCCDF Templates where the name of the STIG does not match the name of the file. CART uses the XCCDF file name for matching. One in particular is the Microsoft .NET Framework STIG.

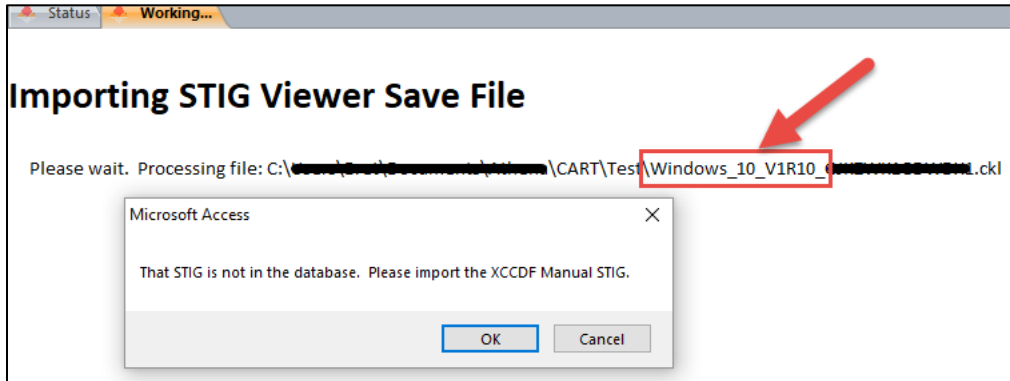


Figure 21

- Select the applicable manual STIG XCCDF XML file. NOTE: The STIG XCCDF must be the Manual STIG and not the Benchmark STIG.

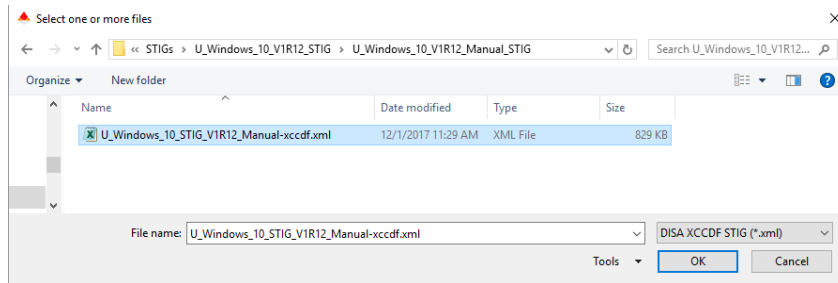


Figure 22

- CART will import the STIG template and then continue with the checklist import; merging the checklist results with the applicable STIG template.



Figure 23

- Upon completion of the import, the updated "Status" page will be presented.

Import SCAP Results

1. Import SCAP Compliance Checker (SCC) results by click the button.
2. Select the file(s) to import. More than one file can be selected.

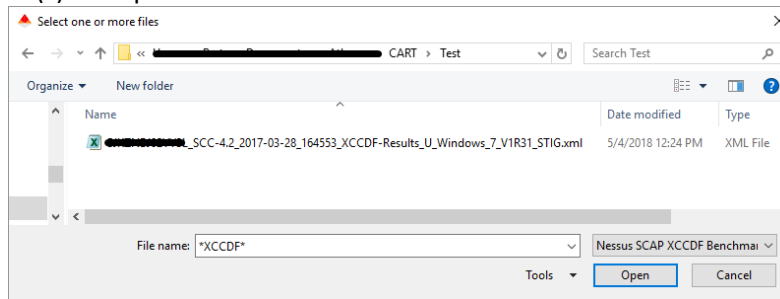


Figure 24

3. If the Manual STIG Checklist Template has no been imported into CART, a prompt will appear to import the XCCDF Manual STIG XML.

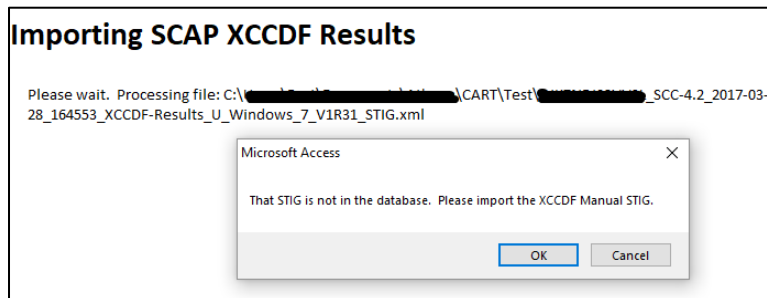


Figure 25

4. Select the applicable XCCDF Manual STIG XML and click OK.

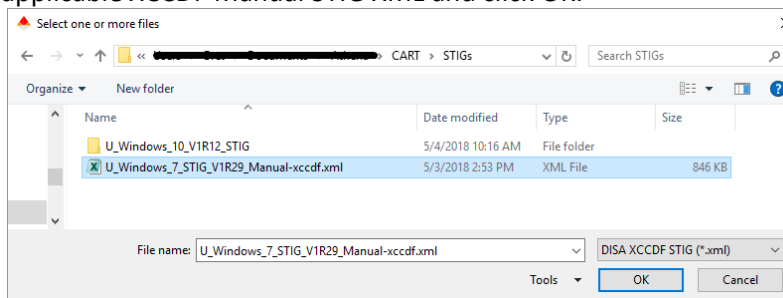


Figure 26

5. CART will merge the SCAP XCCDF Results with the Manual STIG Checklist.

6. After completing the SCAP XCCDF Results import, the Status page will need to be manually refreshed/updated by clicking the Refresh Button to the right of the graph.

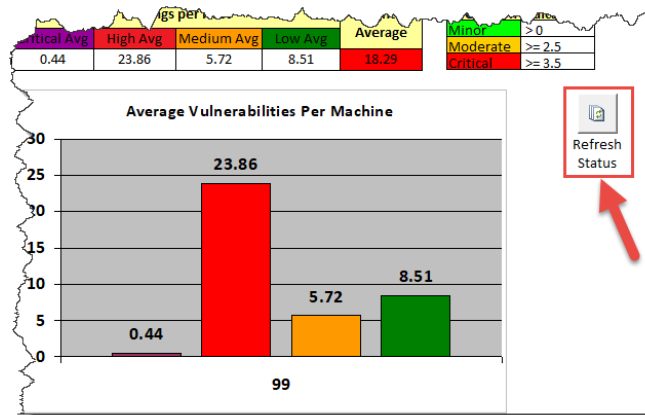


Figure 27

Resetting CART

1. To reset CART and clear all data imported, click the “Clear Database” button at the bottom right of the Controls page.

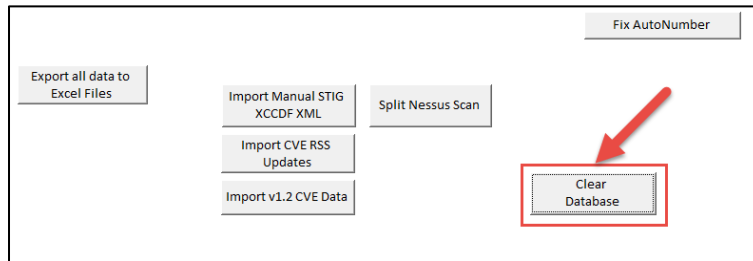


Figure 28

2. A confirmation will appear to ensure the button wasn't clicked by accident.



Figure 29

3. NOTE: Imported STIG Templates are not removed. This could present a problem with future STIG checklist imports because CART will not prompt for an updated STIG. To work around this issue, import new/updated Manual STIG XCCDF XML Templates using the “Import Manual STIG XCCDF XML” button.

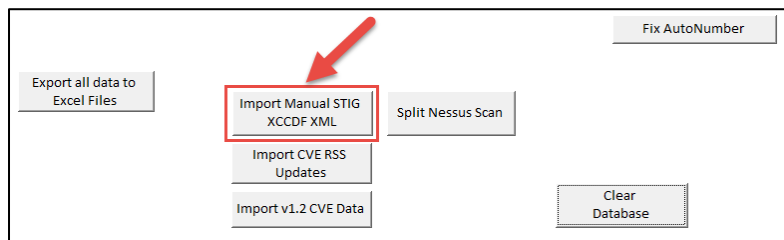


Figure 30