



STIG Viewer 2.x Benutzerhandbuch

Version 1, Freigabe 13

August 2022

Entwickelt von DISA für das DoD

UNCLASSIFIED

Inhaltsübersicht

Seite

EINFÜHRUNG 1

Über DoD/DISA STIG Viewer 1

1. INSTALLIEREN UND AUSFÜHREN VON STIG VIEWER 2.X 3

- 1.1 Installation des Java JAR STIG Viewer 3
- 1.2 Installation von Standalone STIG Viewer 4
- 1.3 Installieren des STIG Viewer Windows MSI-Pakets 5
- 1.4 Überprüfen der Integrität von STIG-Viewer-Paketen 6
- 1.5 Freigabe unter Windows 6
- 1.6 Linux File Access Policy 6
- 1.7 Digitale Signaturen 7

2. STIG VIEWER 2.X 8 VERWENDEN

- 2.1 STIG Viewer öffnen 8
- 2.2 STIG-Viewer-Menüleiste 11
- 2.3 STIGS 12 laden
- 2.4 Checkliste aus STIG 14 erstellen
- 2.5 Registerkarte Checkliste - Menüauswahlen 16
 - 2.5.1 Menü Datei 16
 - 2.5.2 Menü "Importieren" 17
 - 2.5.3 Menü "Exportieren" 17
 - 2.5.4 Optionen 18

3. CHECKLISTE ABSCHNITTE 20

- 3.1 Checkliste - Zieldaten Abschnitt 20
- 3.2 Checkliste - Summen Abschnitt 22
- 3.3 Checkliste - STIGs Abschnitt 22
- 3.4 Checkliste - Technologiebereich Abschnitt 23
- 3.5 Checkliste - Filterplatte Abschnitt 23
- 3.6 Checkliste - Allgemeine Informationen Abschnitt 24
- 3.7 Checkliste - Schwachstelleninformationen Abschnitt 25
- 3.8 Checkliste - Abschnitt "Befunddetails" und Abschnitt "Kommentare" 27

EINFÜHRUNG

STIG Viewer Version 2.x ist ein Ersatz für das vorherige DISA-Tool (STIG Viewer 1.2). Der Zweck dieses Benutzerhandbuchs ist es, die Navigation in 2.x zu erleichtern und die Funktionen aus der Sicht der Benutzer zu beschreiben.

Über DoD/DISA STIG Viewer

Das DoD/DISA STIG-Viewer-Tool bietet die Möglichkeit, eine oder mehrere STIGs im XCCDF-Format (Extensible Configuration Checklist Description Format) in einem leicht zu navigierenden, menschenlesbaren Format anzuzeigen. Sie ist mit den von der DISA für das DoD entwickelten und veröffentlichten STIGs kompatibel. Der Zweck des STIG-Viewers ist die Bereitstellung einer intuitiven grafischen Benutzeroberfläche, die einen einfachen Zugriff auf die STIG-Inhalte ermöglicht, zusammen mit zusätzlichen Such- und Sortierfunktionen, die mit der derzeitigen Methode zur Anzeige der STIGs (unter Verwendung eines Style Sheets in einem Webbrowser) nicht verfügbar sind. STIG Viewer unterstützt auch zusätzliche Funktionen mit den folgenden Merkmalen:

- Ermöglicht es, mehrere STIGs zu importieren und bei der Erstellung von Checklisten zu verwenden.
- Lädt einzeln eine oder mehrere XCCDF-STIG-Dateien.
- Extrahiert XCCDF-STIG-Dateien aus gepackten STIG-Paketen.
- Erstellt einen lokalen Daten-Cache auf einem System, um Benutzerkonfigurationsdaten und den aktuellen Satz von importierten STIGs zu speichern. Dies ermöglicht das erneute Laden des letzten Satzes geladener STIGs bei jedem Start des STIG-Viewers.
- Löscht den lokalen Daten-Cache aus dem Optionsmenü des Viewers. STIG Viewer kann jeweils nur einen lokalen Daten-Cache erstellen.
- Mehrere XCCDF-STIG-Dateien können gleichzeitig entpackt und aus einer .zip-Datei geladen werden, die einen oder mehrere Ordner mit gezippten STIG-Paketen enthält. Der STIG-Viewer findet alle XCCDF-Dateien und lädt sie. Anschließend extrahiert er alle XCCDF-Dateien in seinen lokalen Ordner, da für diesen Vorgang ein lokaler Daten-Cache erforderlich ist.
- Sortiert die Liste der STIG-Anforderungen/Schwachstellen nach Schwachstellen-ID, STIG-ID, Regel-ID, CCI oder Gruppen-/Regelname.
- Durchsucht oder filtert alle geladenen STIG-Dateien anhand eines oder mehrerer Schlüsselwörter. Durchsucht alle Felder oder einzelne Felder und gibt dann eine gefilterte Liste von STIG-Anforderungen/Schwachstellen zurück.
 - Die Suche kann auch auf Regeltitel, STIG-ID, Schwachstellen-ID, Regel-ID, Schweregrad oder CCI beschränkt werden.
- Zeigt CCI-Daten an, wenn der CCI-Bezug in den STIG-Anforderungen enthalten ist.
- Druckt oder exportiert (HTML- und RTF-Dateiformate) ausgewählte STIG-Daten zur Verwendung mit anderen Programmen (z. B. Webbrowser und Microsoft Word).
 - Basiert die gedruckten/exportierten Daten auf der Liste der Anforderungen, die im mittleren Bereich des Viewers angezeigt wird, und formatiert die Ausgabe als

Tabelle, die jede Anforderung enthält.

- Importiert automatische SCAP- (Security Content Automation Protocol) oder XCCDF-Prüfergebnisse in die Checkliste und füllt die Checkliste mit den automatischen Ergebnissen. Der manuelle Teil der Überprüfung kann vervollständigt und den automatischen Ergebnissen hinzugefügt werden.
- Exportiert die Checkliste als .CSV-Datei.

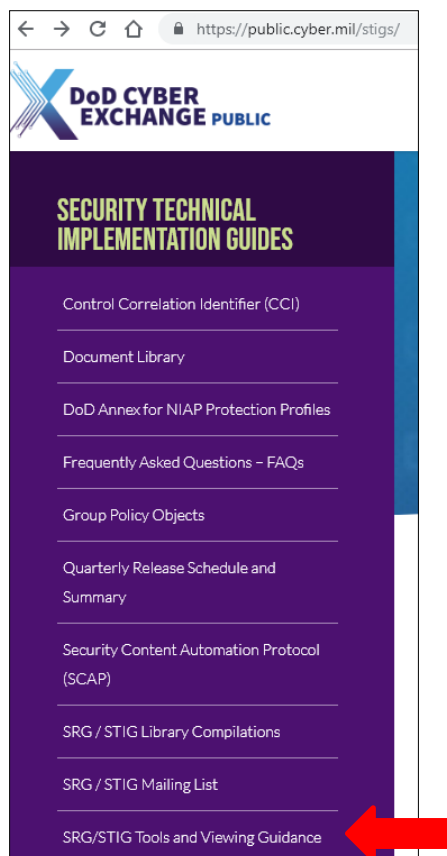
***** NOTE:** DISA entwickelte den STIG Viewer zunächst in Java und lieferte ihn als einzelne JAR-Datei zur Verwendung mit der Oracle Java 8 Java Runtime Environment (JRE). Aufgrund von Änderungen bei der Java-Lizenzierung und -Verteilung, die mit der Veröffentlichung von Java 11 einhergehen, stellt DISA jetzt eine eigenständige STIG-Viewer-Anwendung in einer ZIP-Datei zur Verfügung, die nicht die Oracle JRE benötigt. Dadurch kann die Anwendung auf 64-Bit-X86-Systemen unter Windows und Linux mit minimaler Beeinträchtigung der bestehenden Arbeitsabläufe ausgeführt werden. Dadurch wird das Programm auf die Berechtigungsstufe des aktuell angemeldeten Benutzers beschränkt.

- STIG Viewer öffnet und verwendet keine Netzwerkverbindungen.
- Java erstellt lokale Daten-Caches im lokalen Verzeichnis des angemeldeten Benutzers. Dies ist bei jedem Betriebssystem ein anderer Ort.
 - Unter Windows 10 befindet sich diese im folgenden Verzeichnis:
%USERPROFILE%\AppData\Local\STIGV_AppData
(Wenn Sie den lokalen Daten-Cache löschen, löscht Java den Ordner und den lokalen Daten-Cache gleichzeitig)
- Die Eingabe für den STIG-Viewer ist XCCDF, das in einer XML-Datei enthalten ist. Der STIG-Viewer lehnt andere Dateitypen ab. STIG Viewer ist für XCCDF-formatierte STIGs optimiert, die von der DISA für das DoD erstellt wurden.

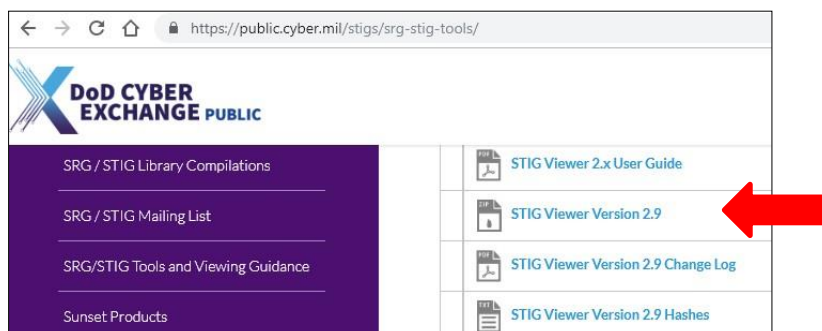
1. INSTALLIEREN UND AUSFÜHREN VON STIG VIEWER 2.X

1.1 Installation des Java JAR STIG Viewer

1. Laden Sie die ZIP-Datei STIG Viewer 2.x von der Cyber Exchange-Website herunter. Gehen Sie zu SRGs/STIGs >> SRG/STIG Tools und Viewing Guidance:



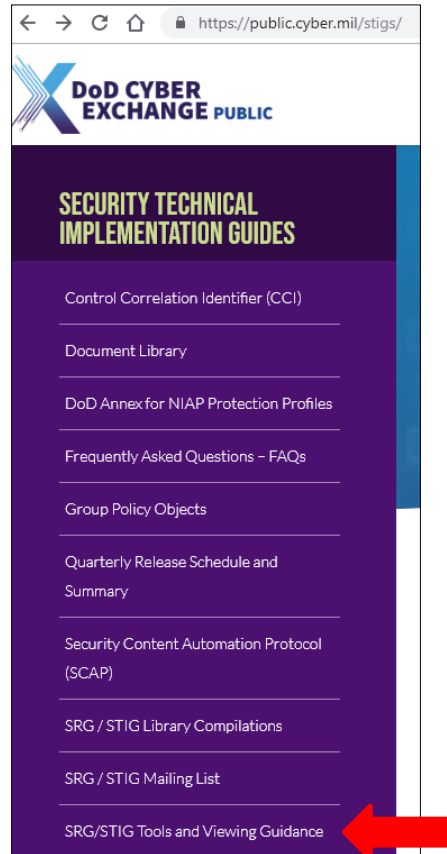
2. Klicken Sie mit der rechten Maustaste auf STIG Viewer Version 2.x.



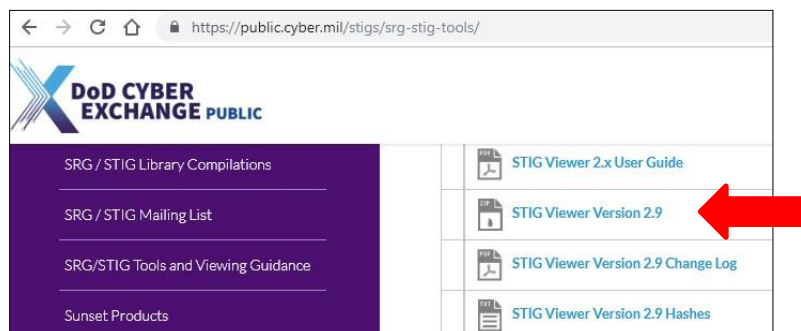
3. Klicken Sie auf **Datei speichern**, um die Datei als STIGViewer2.x.zip auf Ihrem Computer zu speichern. Führen Sie die JAR-Datei direkt aus der ZIP-Datei aus oder extrahieren Sie sie an einen beliebigen Ort, um sie später auszuführen.

1.2 Installation des eigenständigen STIG-Viewers

1. Laden Sie die eigenständige ZIP-Datei von STIG Viewer 2.x von der Cyber Exchange-Website herunter. Gehen Sie zu SRGs/STIGs >> SRG/STIG Tools und Viewing Guidance.



2. Klicken Sie mit der rechten Maustaste auf STIG Viewer 2.x-Win64 oder STIG Viewer 2.x-Linux.

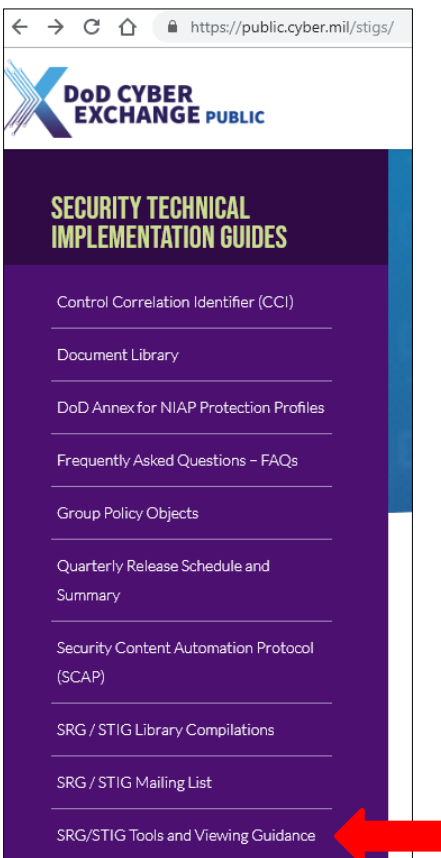


3. Klicken Sie auf **Datei speichern**, um die Datei als STIGViewer2.x-Win64.zip oder STIGViewer2.x-Linux.zip auf Ihrem Computer zu speichern. Extrahieren Sie den gesamten Inhalt der ZIP-Datei auf die lokale Festplatte; die eigenständige Anwendung wird nicht aus der ZIP-Datei heraus ausgeführt.

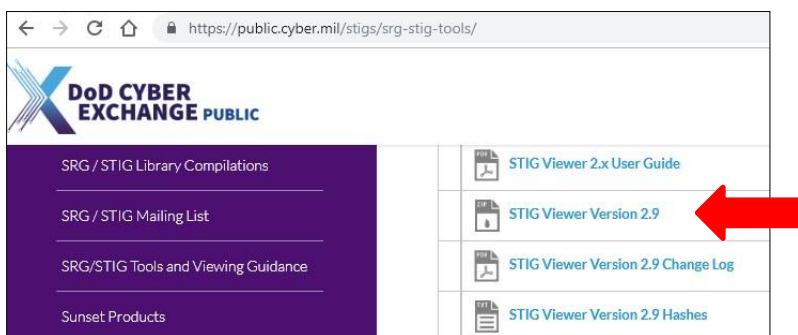
***** **NOTE:** Der eigenständige STIG-Viewer für Linux erfordert GLIBC 2.14 oder höher; dies bedeutet, dass die Anwendung nicht unter RHEL 6 ausgeführt werden kann.

1.3 Installieren des STIG Viewer Windows MSI-Pakets

1. Laden Sie die STIG Viewer 2.x Windows MSI ZIP-Datei von der Cyber Exchange-Website herunter. Gehen Sie zu SRGs/STIGs >> SRG/STIG Tools und Viewing Guidance.



2. Klicken Sie mit der rechten Maustaste auf STIG Viewer Version 2.x-Win64_msi.



3. Klicken Sie auf **Datei speichern**, um die Datei als STIGViewer2.x-Win64_msi.zip auf Ihrem Computer zu speichern.
4. Öffnen Sie die heruntergeladene ZIP-Datei. Öffnen Sie die beigefügte .msi-Datei, um den Installationsvorgang zu starten. Für die Installation sind Administratorrechte erforderlich.

1.4 Überprüfen der Integrität von STIG-Viewer-Paketen

Eine Datei mit sicheren Hash-Werten für die STIG Viewer ZIP-Pakete wird auf cyber.mil veröffentlicht. Diese Hash-Werte können verwendet werden, um die Integrität von STIG Viewer-Paketen zu überprüfen. Es werden Werte für die Algorithmen SHA256, SHA384 und SHA512 angegeben. Um dies zu überprüfen, berechnen Sie den Hash-Wert des zu prüfenden STIG Viewer-Pakets mit Tools wie dem Cmdlet Get-FileHash, das in der Windows PowerShell verfügbar ist, oder den unter Linux verfügbaren Programmen sha256sum, sha384sum und sha512sum. Um die Integrität der Datei zu überprüfen, vergleichen Sie den Hash-Wert der veröffentlichten Datei mit dem berechneten Wert für die zu prüfende Datei mit demselben Algorithmus.

1.5 Aufhebung der Blockierung unter Windows

Wenn STIG Viewer unter Windows heruntergeladen wird, kann die Datei markiert sein, um anzuzeigen, dass sie aus dem Internet heruntergeladen wurde, was die Ausführung der Anwendung verhindern kann. Dies kann auch für den Inhalt einer ZIP-Datei gelten, wenn diese entpackt wird. Wenden Sie sich an Ihren Systemadministrator vor Ort, um Ratschläge zu erhalten. Wird eine überprüfte Datei genehmigt, kann sie entsperrt werden. Wählen Sie im Datei-Explorer die Option Eigenschaften für die Datei. Navigieren Sie im Dialogfeld **Eigenschaften** zur Registerkarte **Allgemein** und zum Abschnitt **Sicherheit**. Heben Sie die Sperrung der Datei auf, indem Sie das Kontrollkästchen **Freigeben** aktivieren und **OK** wählen. Alternativ kann in Windows PowerShell das Cmdlet "Unblock-File" verwendet werden.

1.6 Linux File Access Policy

Linux-Systeme, die den File Access Policy Daemon (fapolicyd) verwenden, können die Ausführung von STIG Viewer blockieren und eine Meldung "Operation Not Permitted" oder "cannot open shared object file" anzeigen, wenn sie versuchen, STIG Viewer zu starten. Das folgende Verfahren kann verwendet werden, um eine gemeinsame Installation von STIG Viewer zu vertrauen:

1. Legen Sie das Verzeichnis für die gemeinsame STIG-Viewer-Installation an.

```
$ sudo mkdir /opt/stigviewer
```

2. Entpacken Sie das STIG Viewer-Paket in das gemeinsame Verzeichnis.

```
$ sudo unzip U_STIGViewer_2-XX_Linux.zip -d /opt/stigviewer
```

3. Fügen Sie die STIG-Viewer-Bibliothek und die Binärdateien zur fapolicyd-Vertrauensdatenbank hinzu.

```
$ sudo fapolicyd-cli --file add /opt/stigviewer/bin  
$ sudo fapolicyd-cli --file add /opt/stigviewer/lib
```

4. Benachrichtigen Sie fapolicyd, dass die Datenbank aktualisiert wurde.

```
$ sudo fapolicyd-cli --update
```

5. Führen Sie STIG Viewer aus dem gemeinsamen Verzeichnis aus.

```
$ /opt/stigviewer/STIGViewer
```

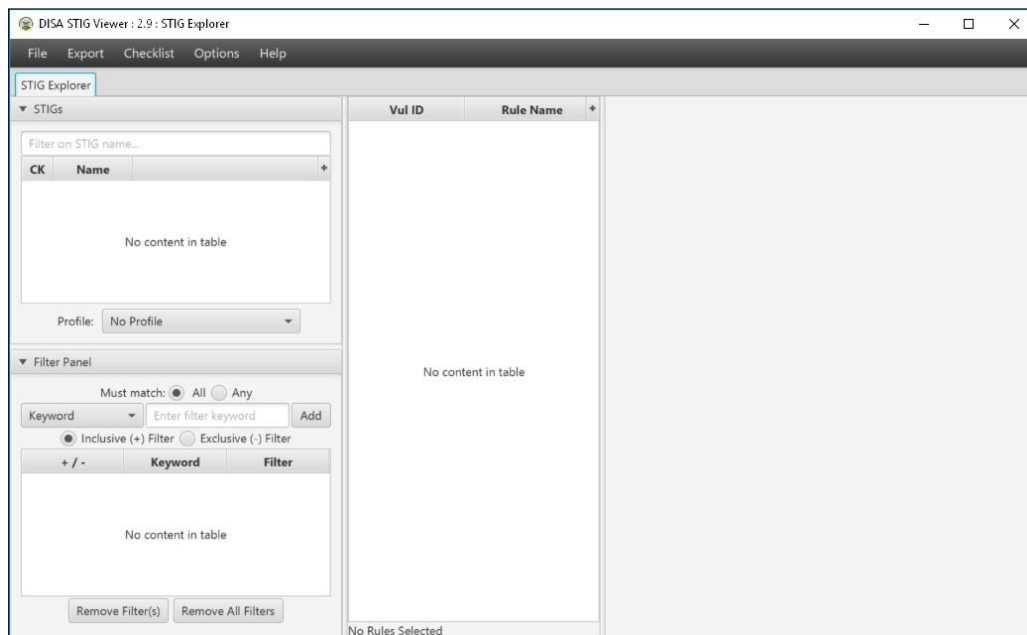
1.7 Digitale Signaturen

Ab Version 2.15 sind die Windows EXE- und MSI-Dateien mit einem DoD-Code Signing-Zertifikat digital signiert. Informationen zur Installation von DoD-Vertrauensankern finden Sie unter <https://public.cyber.mil/pki-pke/>. Um die Signaturen anzuzeigen, öffnen Sie die Eigenschaften der Datei im Windows Explorer und wählen Sie die Registerkarte **Digitale Signaturen**.

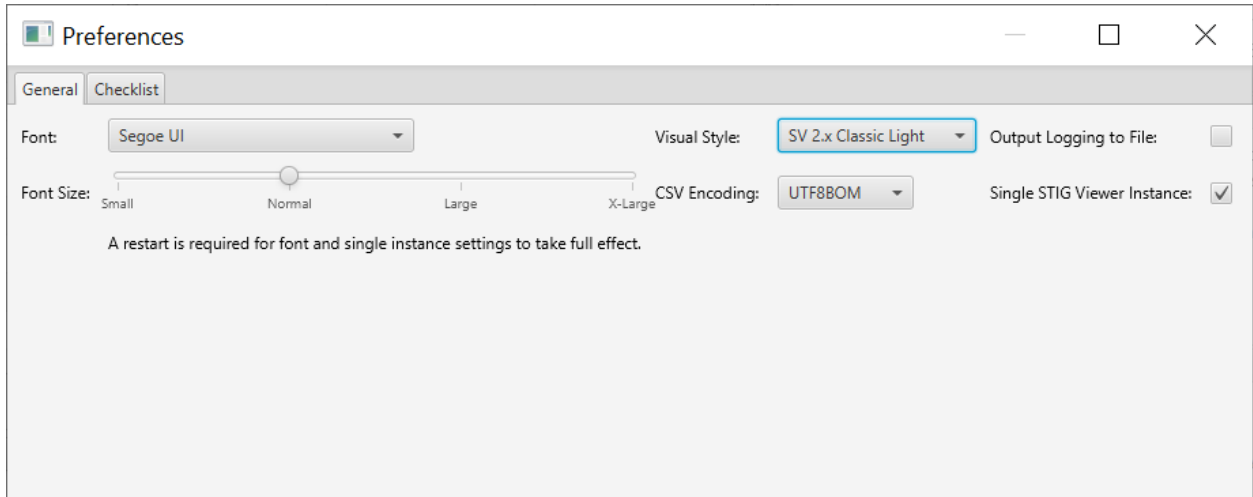
2. STIG VIEWER 2.X VERWENDEN

2.1 STIG Viewer öffnen

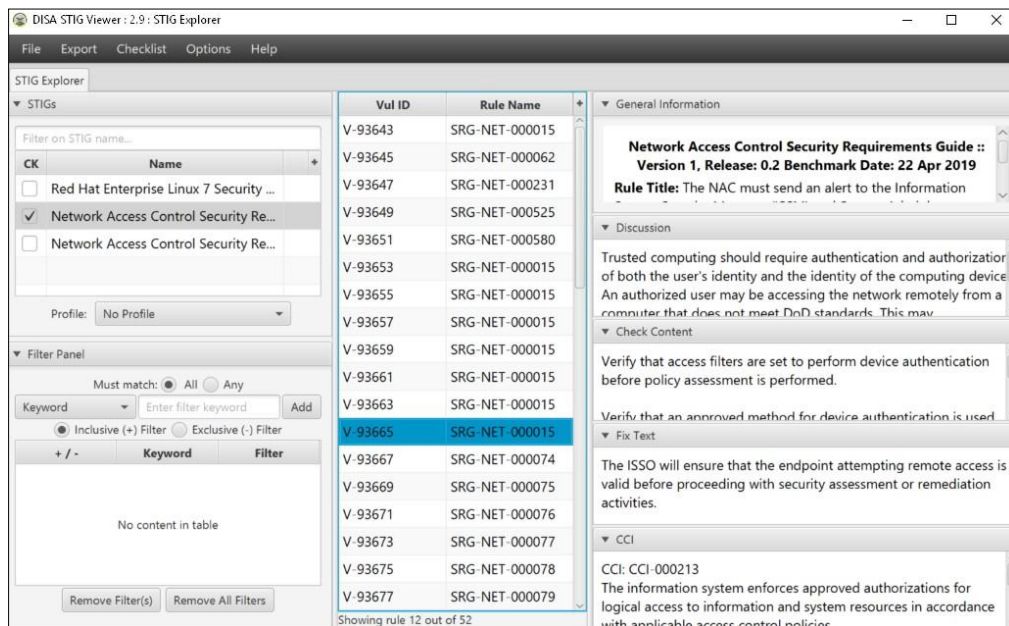
1. Die Vorgehensweise zum Öffnen von STIG Viewer hängt von dem verwendeten Release-Paket ab.
 - a. **STIG Viewer Java Archive (JAR) Paket.**
 - i. Für dieses Paket muss die Version 8 der Oracle Java Runtime Environment installiert sein.
 - ii. Starten Sie STIG Viewer, indem Sie die Datei STIGViewer2.x.jar öffnen.
 - b. **Eigenständiges Windows-Paket.**
 - i. Starten Sie STIG Viewer, indem Sie die Datei "STIG Viewer.exe" öffnen.
 - c. **Windows MSI-Paket.**
 - i. Starten Sie den STIG Viewer, indem Sie den Eintrag "STIG Viewer" im Startmenü öffnen.
 - d. **Eigenständiges Linux-Paket.**
 - i. Starten Sie den eigenständigen STIG-Viewer von der Kommandozeile aus mit der mitgelieferten STIG-Viewer-Shell-Skriptdatei ("STIGViewer").
 - e. **Andere Überlegungen.**
 - i. Wenden Sie sich an die Systemadministratoren vor Ort, um Unterstützung bei der Ausführung von Standalone-Versionen von STIG Viewer mit Anwendungs-Firewalls zu erhalten.
2. Beim Starten sieht ein leerer STIG-Viewer wie folgt aus:



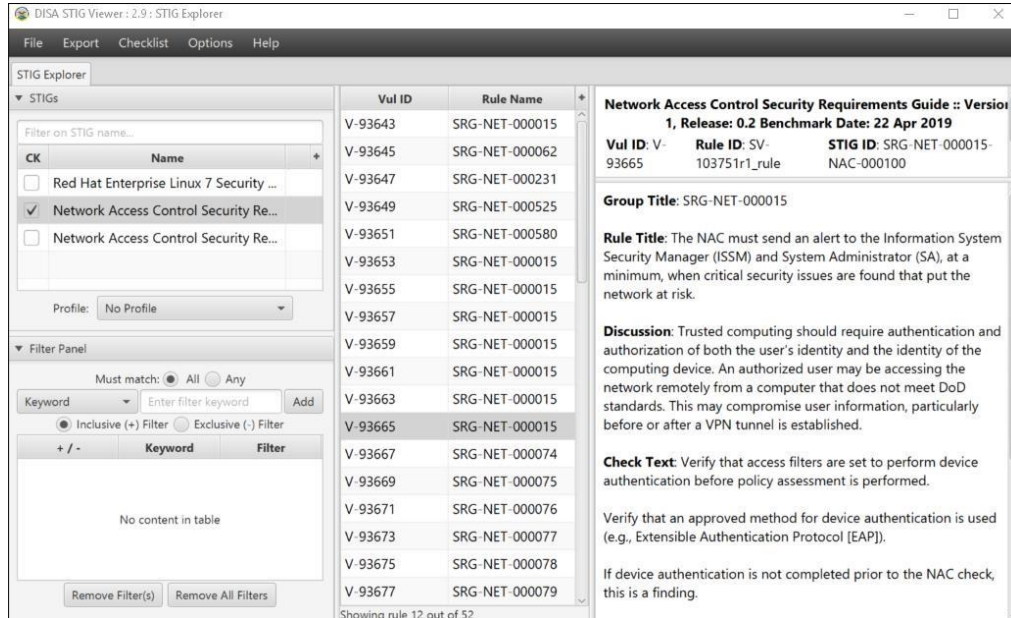
- Wenn STIGs in den STIG Viewer geladen werden, bestimmen die Einstellungen ihr Aussehen. Um das Erscheinungsbild zu ändern, wählen Sie in der oberen Navigationsleiste **Optionen >> Einstellungen** und wählen dann das gewünschte Erscheinungsbild aus dem Dropdown-Feld **Visueller Stil**.



- SV 2.x Klassisches Licht:



b. Thema Licht:



4. Der Viewer besteht aus drei Hauptspalten:

- Linke Spalte: STIGs, die die STIG-Namen und den Filterbereich anzeigt.
- Mittlere Spalte: Informationen zur Schwachstellen-ID.
- Rechte Spalte: Allgemeine Informationen, die die Detailinformationen zur Schwachstelle anzeigen.

5. In den klassischen Themen haben die linke und die rechte Spalte jeweils ausklappbare Abschnitte. Wenn Sie auf die kleinen Pfeilspitzen links neben den einzelnen Abschnittsbezeichnungen klicken, wird der Abschnitt entweder erweitert oder reduziert. Je mehr Abschnitte Sie einklappen, desto höher wird jeder der anderen Abschnitte geöffnet. Die vertikalen Trennlinien zwischen den Spalten lassen sich verschieben, um ihre Größe anzupassen.

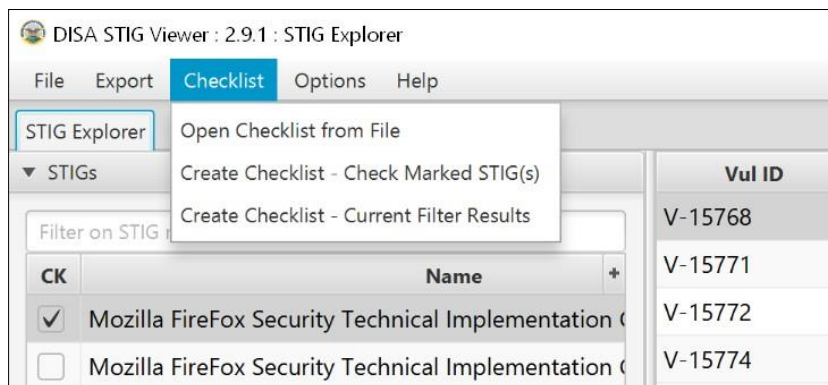
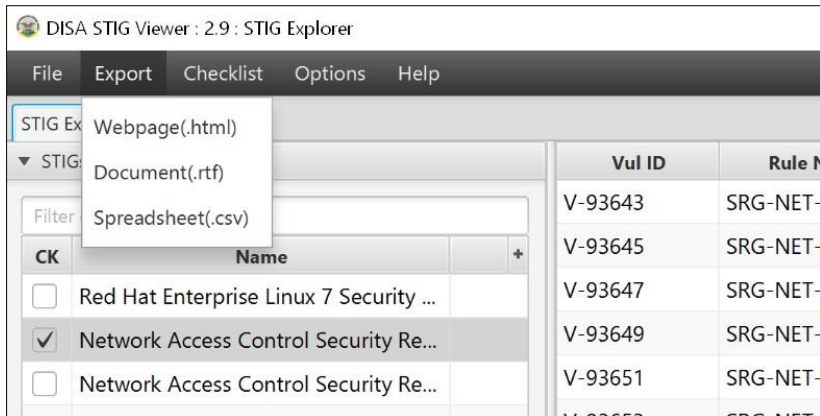
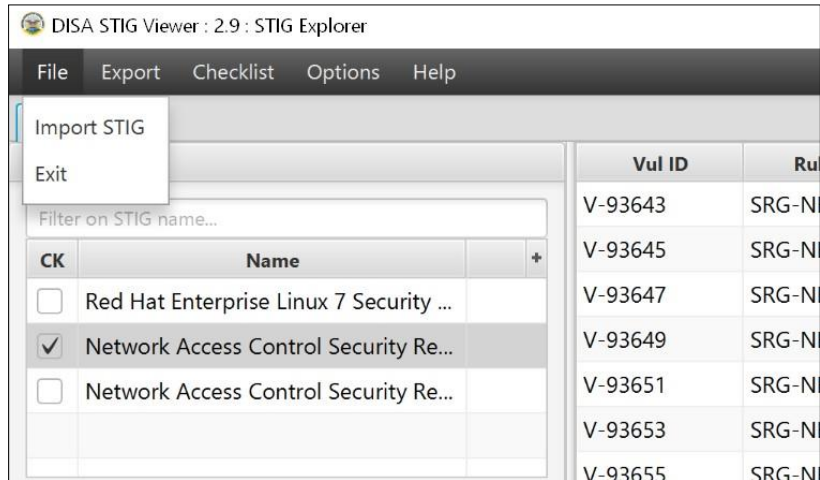
- Beschriftung der linken Spalte: **STIGs, Filterplatte.**
- Bezeichnungen in der rechten Spalte: **Allgemeine Informationen, Diskussion, Inhalt prüfen, Text korrigieren, CCI, Sonstiges** (falls zutreffend).

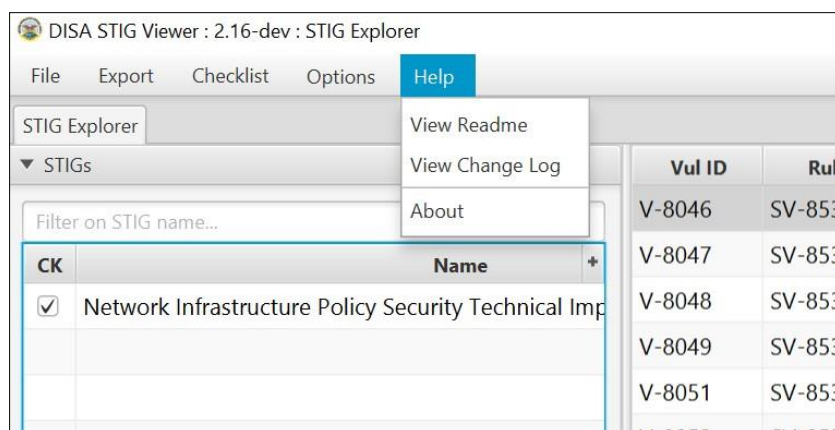
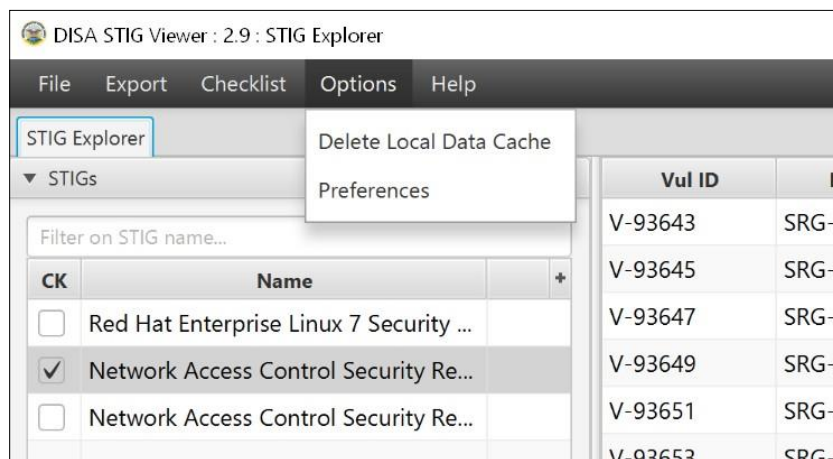
6. Bei den nicht-klassischen Themen gehen die verschiedenen Abschnitte der rechten Spalte in zwei über.

7. Zusätzlich zu den oben vorgestellten **Light-Themen** gibt es auch entsprechende **Dark-Themen**.

2.2 STIG Viewer-Menüleiste

- Die Menüleiste des STIG-Viewers enthält fünf Dropdown-Menüs, die Sie auswählen können: **Datei**, **Export**, **Checkliste**, **Optionen** und **Hilfe**. Die Auswahlmöglichkeiten innerhalb jeder Auswahl sind unten aufgeführt:

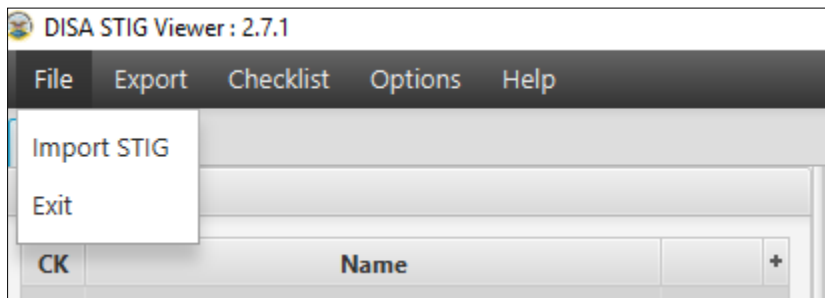




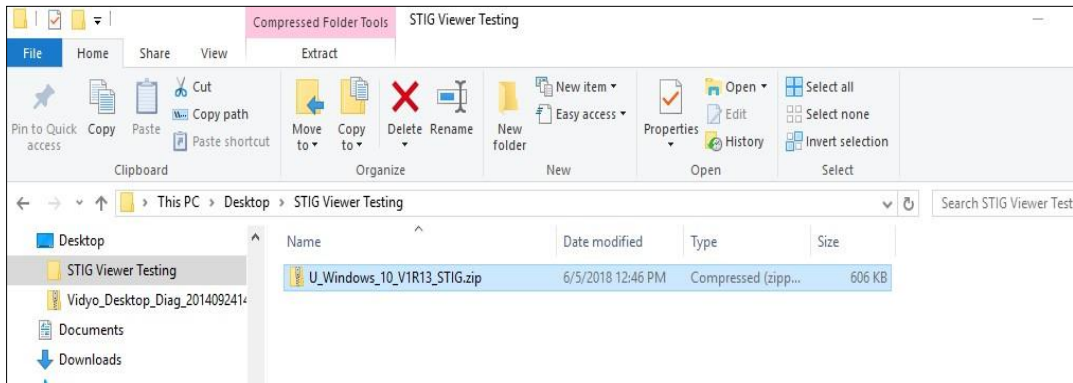
2.3 STIGS laden

STIGs, die von der Cyber Exchange Website heruntergeladen werden, liegen im .zip-Format vor, das in den STIG Viewer geladen wird. STIG Viewer behandelt alle STIGs auf die gleiche Weise; dieser Leitfaden enthält allgemeine Anweisungen, die für alle Technologien geeignet sind.

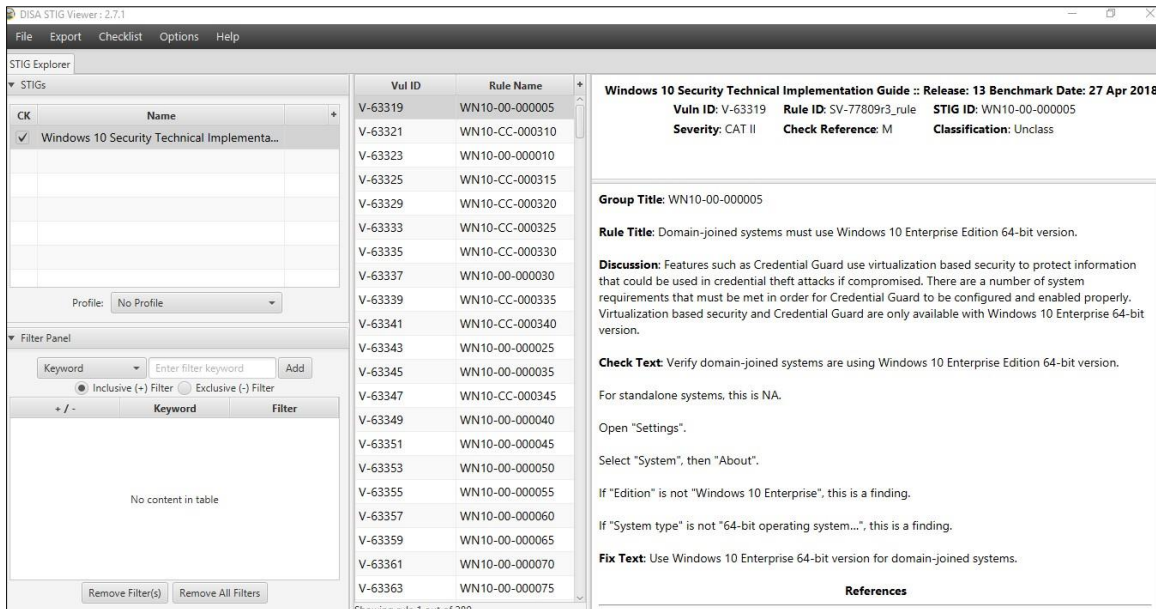
1. Wählen Sie in der Menüleiste des STIG Viewers **Datei >> STIG importieren**.



2. Wählen Sie die zu ladende STIG.zip-Datei aus und klicken Sie auf die Schaltfläche Öffnen. Dieses Beispiel zeigt eine Windows 10 STIG.



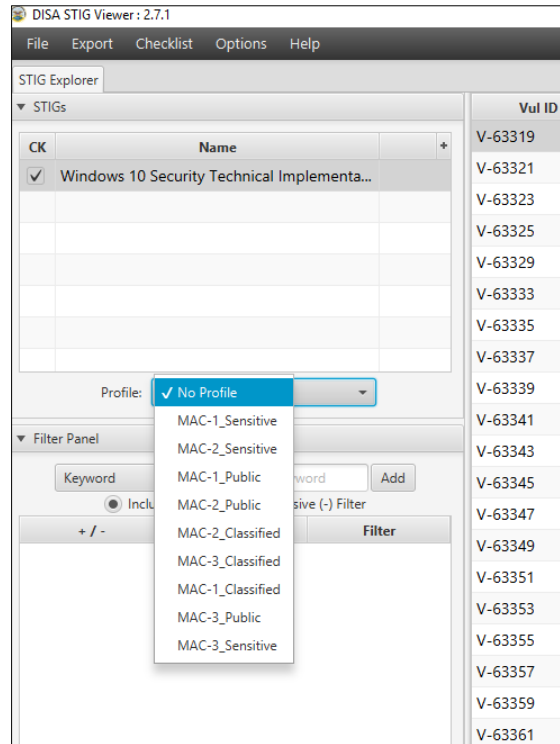
3. Der STIG Viewer zeigt an, dass die STIG geladen wurde.



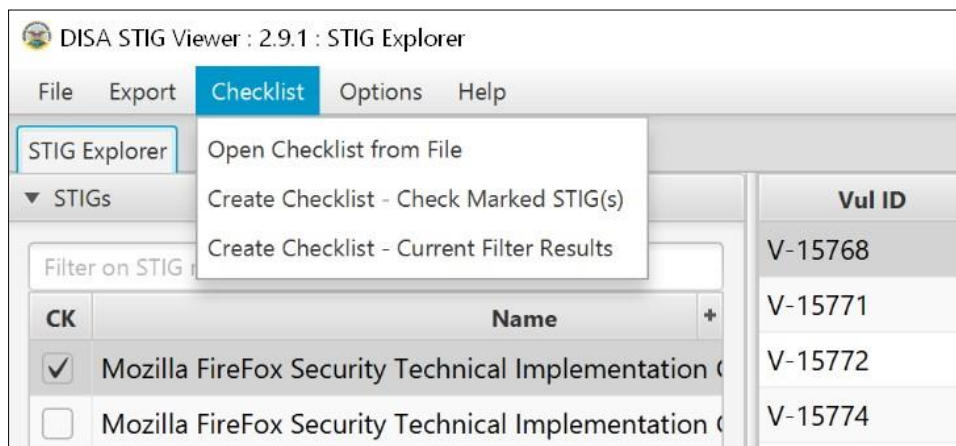
Wenn mehr als eine STIG geladen ist, können Sie mit der rechten Maustaste auf die Liste der STIGs klicken, um die Option **Alle prüfen** aufzurufen. Diese Option ist für die Suche nach Schlüsselwörtern nützlich. Außerdem können Sie mit der Tastenkombination Strg+A alle STIGs in der Liste markieren.

2.4 Checkliste aus STIG erstellen

1. Kreuzen Sie das Kästchen neben der/den gewünschten STIG an.
2. Klicken Sie auf das Dropdown-Menü **Profil** und wählen Sie die MAC-/Klassifizierungsstufe für die Checkliste und das zu überprüfende Gut.

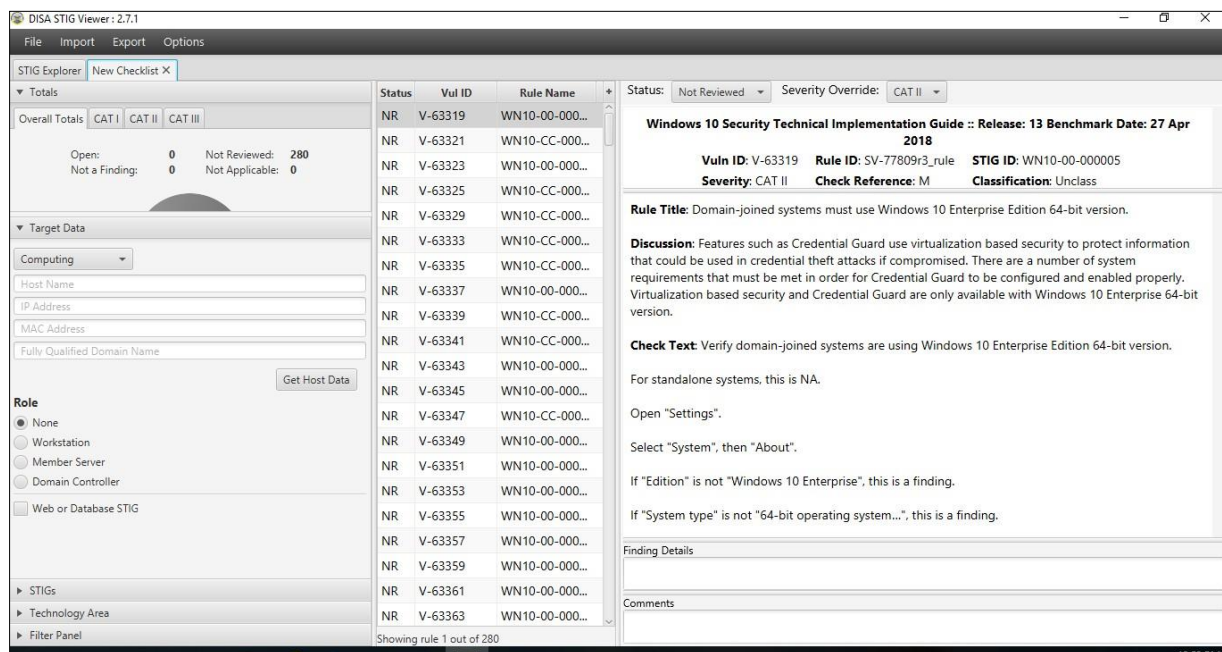


3. Klicken Sie auf den Menüpunkt **Checkliste** >> **Checkliste erstellen - Markierte STIG(s) prüfen**.



4. -ODER- Erstellen Sie eine Checkliste aus den gefilterten Ergebnissen, indem Sie **Checkliste** >> **Checkliste erstellen** wählen
- **Aktuelle Filterergebnisse**.

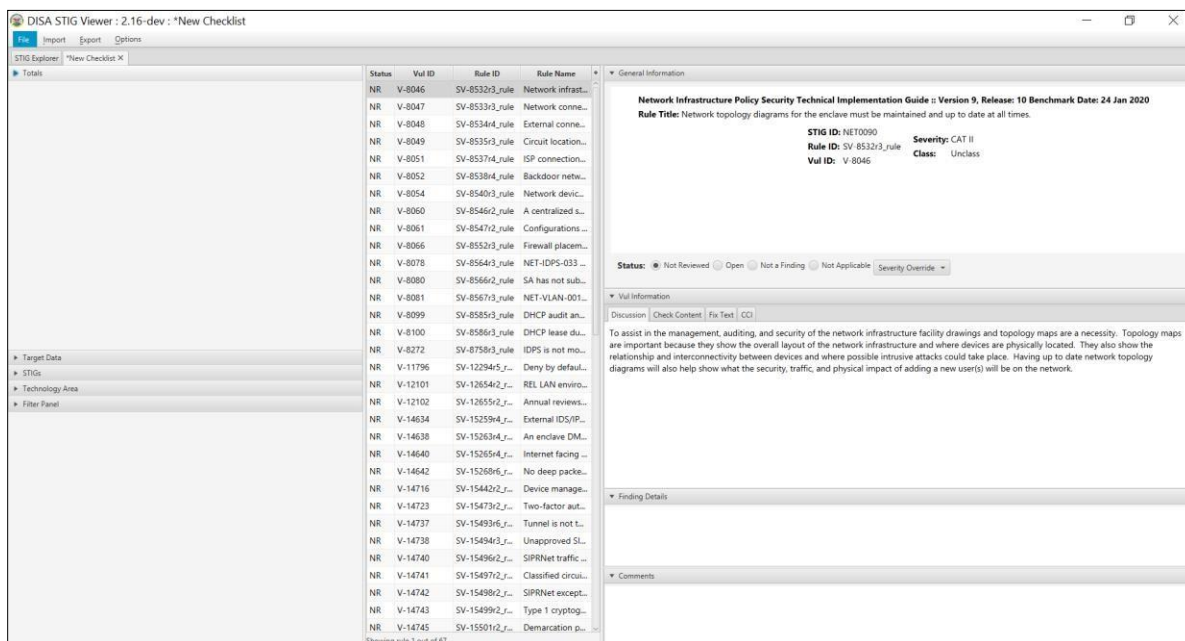
5. Es öffnet sich eine Registerkarte "**Checkliste**" mit den Checklisteninformationen für die ausgewählte STIG.



6. Die Spalten der Registerkarte **Checkliste** unterscheiden sich von den Spalten der Registerkarte **STIG** :

- Linke Spalte: Summen, Zieldaten, STIGs, Technologiebereich und Filterfeld.
- Mittlere Spalte: Schwachstellen in der Checkliste.
- Rechte Spalte: Allgemeine Informationen, Informationen über Schwachstellen, Funddetails und Kommentare.

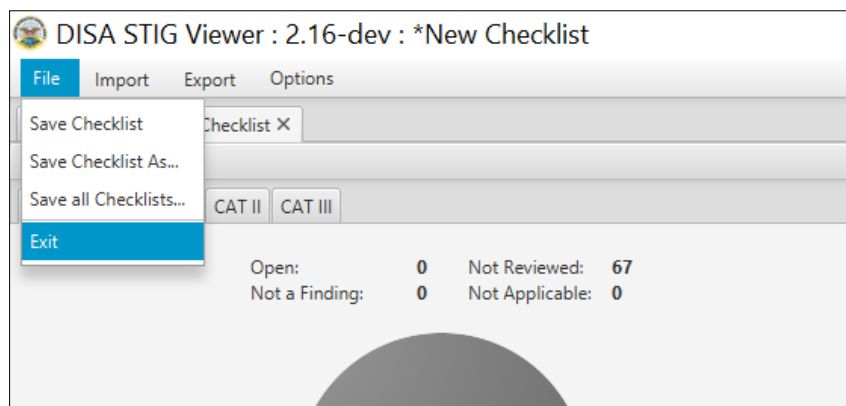
***** NOTE:** Diese Registerkarten befinden sich in der Option SV 2.x Classic Light visueller Stil unter **Optionen** >> **Einstellungen** . Um die Abschnitte der rechten Spalte auszublenden, wechseln Sie vor der Erstellung der Checkliste zum **Thema Light** . Um alle Abschnitte anzuzeigen, klappen Sie einige davon aus. Die folgende Abbildung zeigt eine Ansicht mit eingeklappten Abschnitten:



2.5 Registerkarte Checkliste - Menüauswahlen

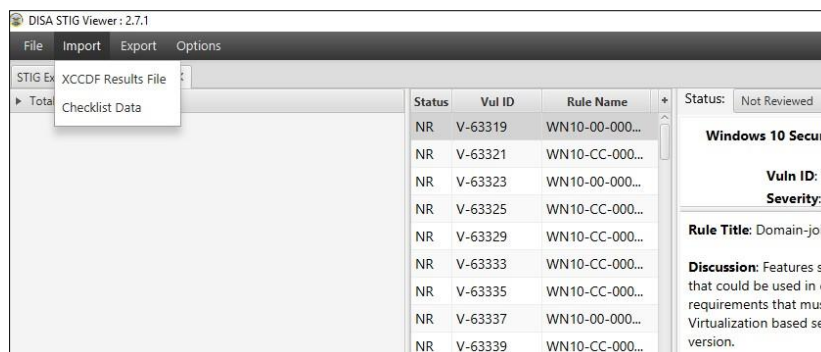
2.5.1 Menü "Datei"

Über das Menü **Datei** können Sie die Checkliste speichern, die Checkliste unter einem neuen Dateinamen/Speicherort speichern oder alle geöffneten Checklisten speichern.



2.5.2 Menü "Importieren"

Im Menü **Import** können Sie eine **XCCDF-Ergebnisdatei** oder **Checklistendaten** importieren. Die XCCDF-Ergebnisdatei ist eine Datei mit der Erweiterung .xml, die die Ergebnisse eines Scans mit einem SCAP-kompatiblen Tool, wie dem SCC-Tool(<https://cyber.mil/stigs/scap/>), enthält.



Das Menü **Importieren** bietet die Möglichkeit, zuvor gespeicherte STIG Viewer Checklist-Dateien (.ckl) zu importieren. Ergebnisse für kürzlich aktualisierte Regeln werden nicht importiert, da sich ihre Regel-IDs geändert haben. **Voreinstellungen** ermöglichen ein unterschiedliches Verhalten bei der Regelanpassung.

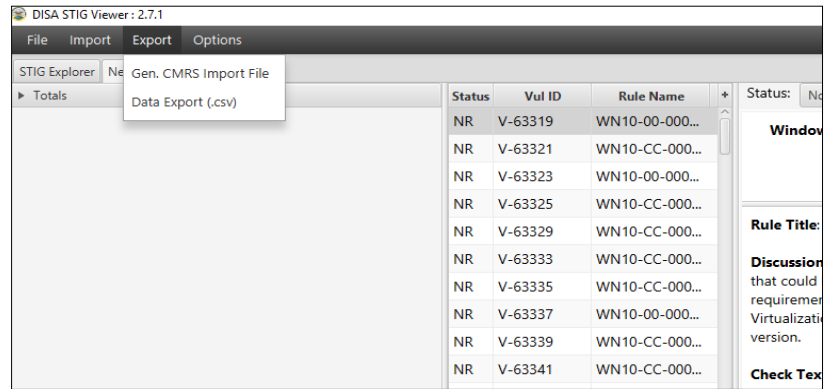
Sobald der Import abgeschlossen ist, kümmern Sie sich um die verbleibenden nicht überprüften (NR) Regeln, bei denen es sich um manuelle Prüfungen handelt. Vergewissern Sie sich, dass Sie alle Punkte mit dem Status **NR** auf den entsprechenden Status setzen, um die Checkliste abzuschließen.

2.5.2.1 Beschränkungen

- Die Auswahl der Technologiebereiche wird **nicht** importiert.
- Schweregradüberschreibungen aus STIG Viewer Version 1.2 Checklistendateien werden **nicht** importiert.

2.5.3 Menü "Exportieren"

Das Menü "**Export**" bietet die Möglichkeit, die Daten der Checkliste in eine allgemeine CMRS-Importdatei für die Berichterstattung zu exportieren. Sie können die Daten der Checkliste auch in ein Excel-Tabellenblatt (.csv) exportieren.



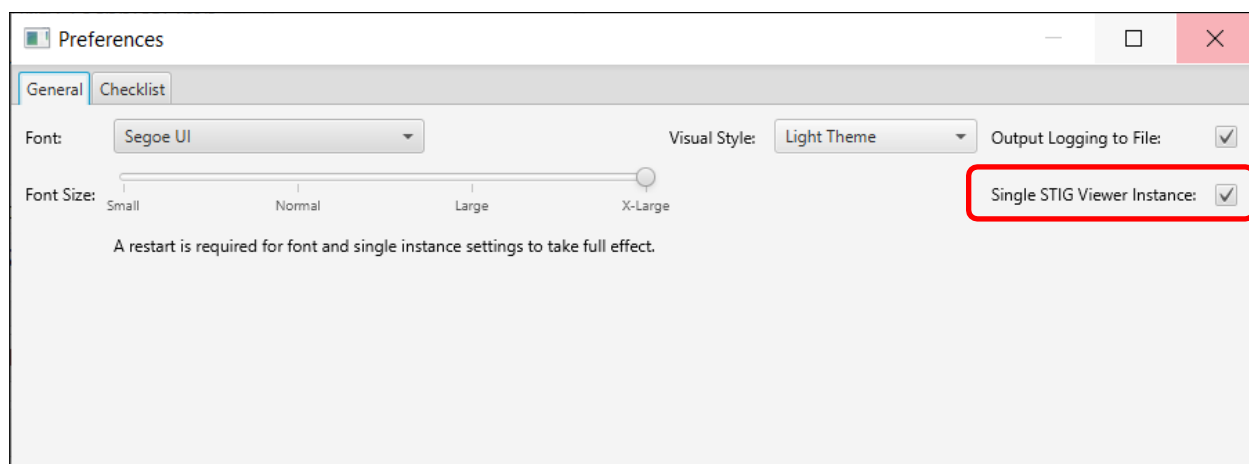
2.5.4 Optionen

Im Menü **Optionen** können Sie die Schriftgröße, den visuellen Stil und die Textfarben der Checkliste ändern. Die Optionen für den visuellen Stil umfassen die Themen "Hell" und "Dunkel" sowie das Erscheinungsbild einiger Abschnitte sowohl für die STIG als auch für die Checkliste.

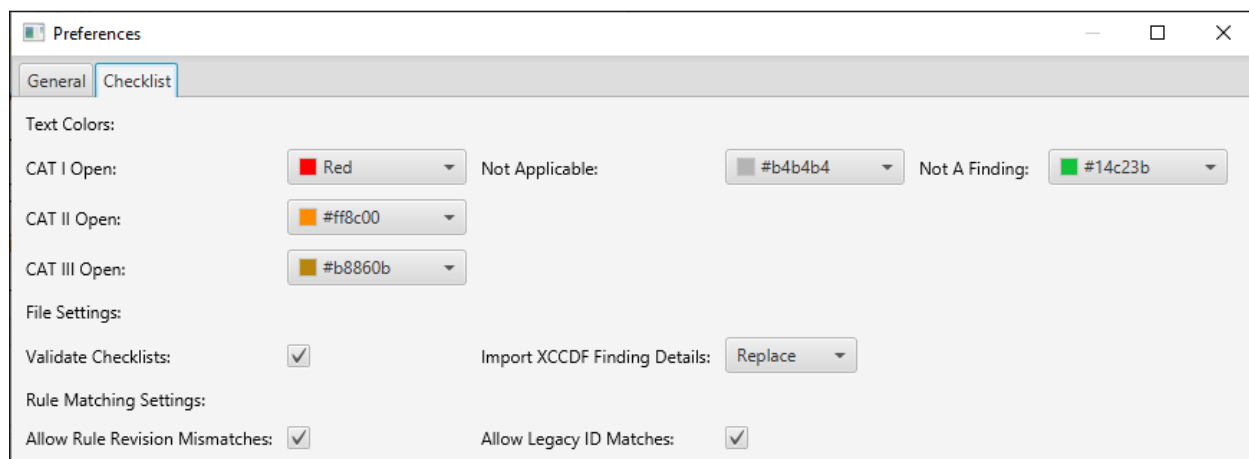
2.5.4.1 Allgemeine Präferenzen

2.5.4.1.1 Einzelne STIG-Viewer-Instanz

Wenn diese Option aktiviert ist, wird von STIG Viewer nur eine einzige Instanz pro Benutzer ausgeführt. Um mehrere Instanzen von STIG Viewer auszuführen, deaktivieren Sie diese Einstellung.



2.5.4.2 Checkliste Präferenzen



2.5.4.2.1 Einstellungen für den Regelabgleich

Die Einstellungen für den Regelabgleich ändern das Verhalten des Regelabgleichs, der beim Import von XCCDF-Ergebnisdateien und Checklistendaten durchgeführt wird.

2.5.4.2.2 Abweichende Regeländerungen zulassen

Bei dieser Einstellung wird die Revisionskomponente von Regel-IDs ignoriert. Zum Beispiel:

	Regel-ID
STIG-Dokument V2R1	SV-923456r100007_rule
STIG-Dokument V2R2	SV-923456r113112_rule

Wenn diese Einstellung aktiviert ist, stimmen diese beiden Regel-IDs beim Import überein.

Für Dokumente, die aus DPMS 3.x generiert wurden, das im Oktober 2020 veröffentlicht wurde, ändert sich die Revisionsnummer für jede Dokumentenversion. Diese Option ermöglicht den Import von Ergebnissen aus früheren Revisionen gegen neue Revisionen desselben Dokuments.

Vorsicht! Mit dieser Option werden Regeln *auch dann* abgeglichen, wenn sich der Inhalt dieser Regeln geändert hat. Konsultieren Sie die Revisionshistorie des Dokuments, um festzustellen, welche Regeln sich geändert haben und möglicherweise neu bewertet werden müssen.

2.5.4.2.3 Legacy-ID-Abgleiche zulassen

Mit dieser Einstellung wird die importierte Regel-ID mit der ID der alten Regel in der Checkliste abgeglichen.

Dokumente, die mit DPMS 3.x, das im Oktober 2020 veröffentlicht wurde, erstellt wurden, haben andere Regel-IDs als frühere Versionen desselben Dokuments. Um ein Mapping zwischen alten und neuen Versionen zu ermöglichen, werden die Legacy-IDs in den neueren Versionen veröffentlicht. Diese Einstellung ermöglicht einen Abgleich mit der Legacy-Regel-ID.

Vorsicht! Legacy-IDs sind nicht mit bestimmten Revisionen verknüpft. Mit dieser Option werden Regeln *auch dann* abgeglichen, wenn sich der Inhalt dieser Regeln geändert hat. Konsultieren Sie die Revisionshistorie des Dokuments, um festzustellen, welche Regeln sich geändert haben und möglicherweise neu bewertet werden müssen.

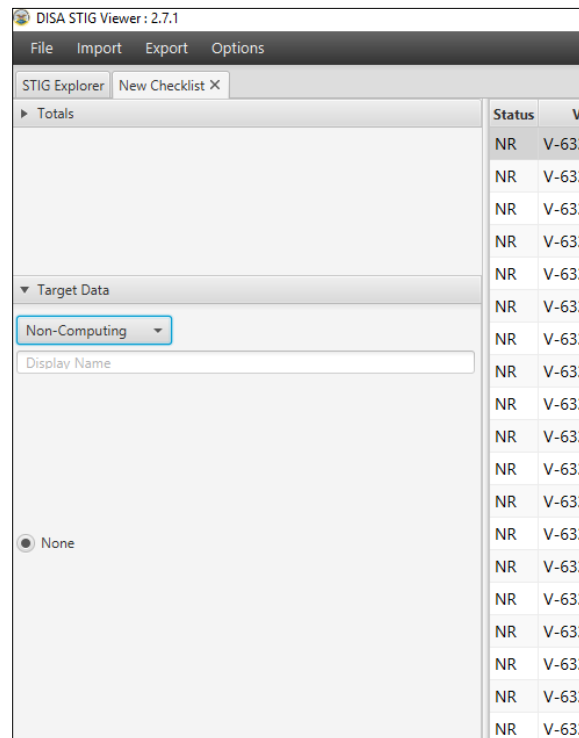
3. ABSCHNITTE DER CHECKLISTE

3.1 Checkliste - Abschnitt Zieldaten

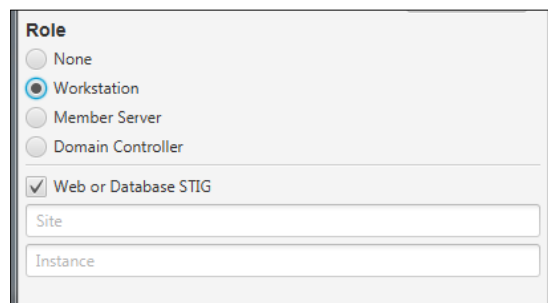
1. Der Abschnitt **Zieldaten** der Checkliste identifiziert das STIG-Vermögen. Mit der Dropdown-Schaltfläche am oberen Rand können Sie zwischen rechnenden und nicht rechnenden Anwendungen umschalten. Geben Sie für die Datenverarbeitung den Hostnamen, die IP-Adresse und die MAC-Adresse des zu überprüfenden Assets ein. Kommentare können auch für alle Assets unter **Zielkommentare** hinzugefügt werden. Bei nicht rechnergestützten Anlagen geben Sie nur den Namen der Anlage ein.

***** NOTE:** Klicken Sie NICHT auf die Schaltfläche Hostdaten abrufen. Dadurch werden die Felder für die Datenverarbeitung nur mit den Daten des von Ihnen verwendeten Computers ausgefüllt.

Status	V-7
NR	V-7
NR	V-7
NR	V-7
NR	V-7
NR	V-7
NR	V-7
NR	V-7
NR	V-7
NR	V-7
NR	V-7
NR	V-7
NR	V-7

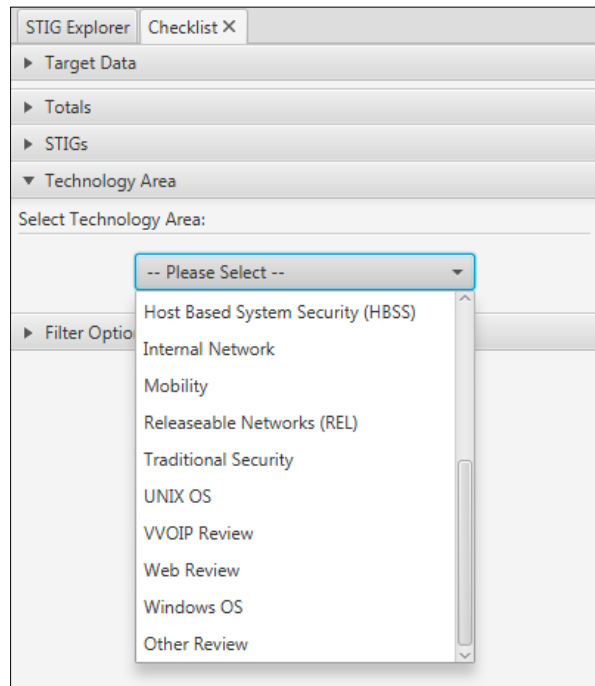


- Wählen Sie das Optionsfeld **Rolle** für den Servertyp. Wenn Sie auf das Feld Web oder Datenbank STIG klicken, werden Felder für **Site-** und **Instanznamen** angezeigt.



3.4 Checkliste - Abschnitt Technologiebereich

Der Abschnitt **Technologiebereich** enthält eine Dropdown-Liste mit Technologien zur Auswahl einer bestimmten Technologie für die zu prüfende Anlage.



3.5 Checkliste - Abschnitt Filterebene

Im Bereich **Filterfeld** können Sie die Sicherheitsrisiken nach Schlüsselwort, Regeltitel, STIG-ID, Sicherheitsrisiko-ID, Regel-ID, Schweregrad, CCI, Legacy oder Status filtern. Wählen Sie das Optionsfeld **Einschließender (+) Filter** oder **Ausschließender (-) Filter**, um Schwachstellen zu finden, die entweder das Kriterium erfüllen oder nicht erfüllen. Kombinieren Sie mehrere Filter, indem Sie den **Must-Match** verwenden : **Alle** oder **Beliebige** Auswahl, so dass entweder alle Filter übereinstimmen müssen oder beliebige Filter übereinstimmen können. Um den Filter zu löschen, wählen Sie entweder die Schaltfläche **Filter entfernen** oder **Alle Filter entfernen**.

▼ Filter Panel

Must match: ☒ All ☐ Any

Keyword Enter filter keyword

☒ Inclusive (+) Filter ☐ Exclusive (-) Filter

+ / -	Keyword	Filter
No content in table		

NR	V-12102
NR	V-14634
NR	V-14638
NR	V-14640
NR	V-14642
NR	V-14716
NR	V-14723
NR	V-14737
NR	V-14738
NR	V-14740
NR	V-14741
NR	V-14742
NR	V-14743
NR	V-14745

Showing rule 1 out of 1

3.6 Checkliste - Abschnitt Allgemeine Informationen

1. Der Abschnitt **Allgemeine Informationen** wird in der rechten Spalte für die in der mittleren Spalte ausgewählte Schwachstelle angezeigt.
2. Wählen Sie das Optionsfeld **Status** aus, um die Schwachstelle als **offen (O)**, **kein Befund (NF)** oder **nicht anwendbar (NA)** zu kennzeichnen. Die Textfarbe der Schwachstelle ändert sich ebenfalls, um den Status wiederzugeben.
3. Klicken Sie bei Bedarf auf das Dropdown-Menü **Schweregradüberschreibung**, um den Status herab- oder heraufzustufen. Es wird ein Popup-Fenster angezeigt, in das Sie den erforderlichen Rechtfertigungstext für die Überschreibung eingeben können.

Status	Vul ID	Rule Name
NF	V-63319	WN10-00-000...
O	V-63321	WN10-CC-000...
NF	V-63323	WN10-00-000...
O	V-63325	WN10-CC-000...
O	V-63329	WN10-CC-000...
NF	V-63333	WN10-CC-000...
NF	V-63335	WN10-CC-000...

General Information

Windows 10 Security Technical Implementation Guide :: Release: 13 Benchmark Date: 27 Apr 2018

Rule Title: Mobile systems must encrypt all disks to protect the confidentiality and integrity of all information at rest.

STIG ID: WN10-00-000030

Status: ☐ Not Reviewed ☐ Open ☒ Not a Finding ☐ Not Applicable Severity Override

4. Um mehrere Schwachstellenprüfungen auszuwählen, klicken Sie auf die erste Auswahl und dann bei gedrückter Umschalttaste auf die folgenden Auswahlen. Markieren Sie alle Schwachstellen mit Strg+A oder klicken Sie mit der rechten Maustaste und wählen Sie dann **Alle auswählen**.

Status	Vul ID	Rule Name
NF	V-63319	WN10-00-000...
NF	V-63321	WN10-CC-000...
NF	V-63323	WN10-00-000...
NF	V-63325	WN10-CC-000...
NF	V-63329	WN10-CC-000...
NF	V-63333	WN10-CC-000...
NF	V-63335	WN10-CC-000...

General Information

Windows 10 Security Technical Implementation Guide :: Release: 13 Benchmark Date: 27 Apr 2018

Rule Title: Users must be notified if a web-based program attempts to install software.

STIG ID: WN10-CC-000320

Severity: CAT II

Status: ☐ Not Reviewed ☐ Open ☒ Not a Finding ☐ Not Applicable Severity Override

5. Wählen Sie das Optionsfeld " **Status**" oder die Option aus dem Dropdown-Menü, die Sie für alle ausgewählten Prüfungen festlegen möchten.

Status	Vul ID	Rule Name
NF	V-63319	WN10-00-000...
NF	V-63321	WN10-CC-000...
NF	V-63323	WN10-00-000...
NF	V-63325	WN10-CC-000...
NF	V-63329	WN10-CC-000...
NF	V-63333	WN10-CC-000...
NF	V-63335	WN10-CC-000...

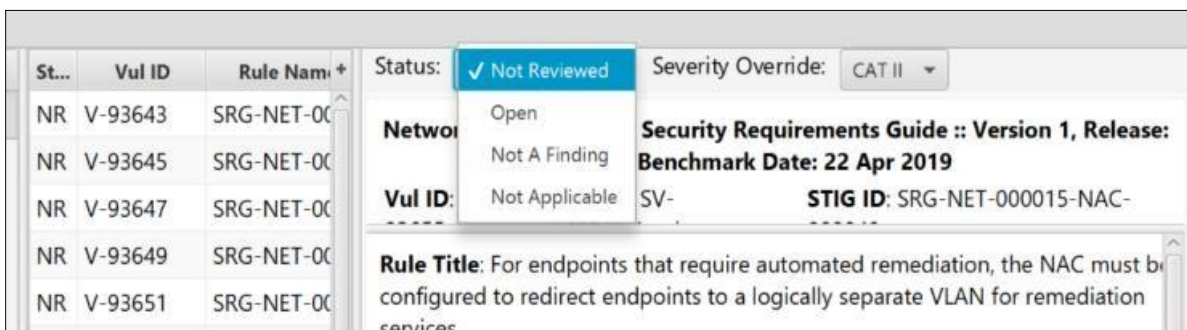
General Information

Windows 10 Security Technical Implementation Guide :: Release: 13 Benchmark Date: 27 Apr 2018

Rule Title: Automatically signing in the last interactive user after a system-initiated restart must be disabled.

STIG ID: WN10-CC-000325

Status: ☐ Not Reviewed ☐ Open ☒ Not a Finding ☐ Not Applicable Severity Override



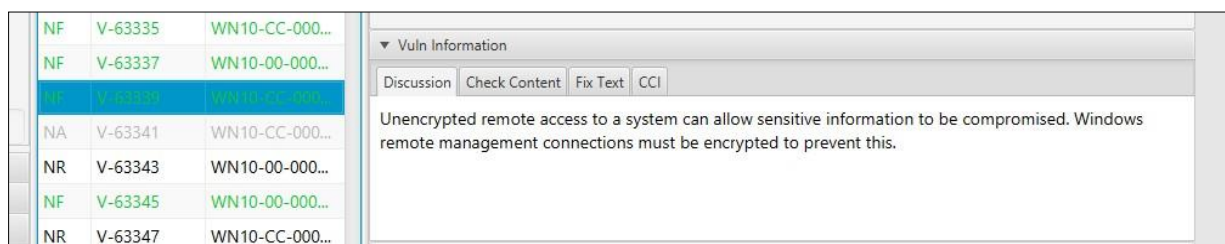
6. Zusätzlich zu den Optionsfeldern "**Status**" (in SV 2.x Classic Light) oder den Optionen des Dropdown-Menüs "**Status:**" (in Light Theme) für die Auswahl des Status für eine oder mehrere Prüfungen gibt es Tastenkombinationen für jeden der vier Status:
- "R" oder "r" kennzeichnet die ausgewählte(n) Prüfung(en) als "Nicht geprüft".
 - "O" oder "o" markiert die ausgewählte(n) Prüfung(en) als "offen".
 - "N" oder "n" kennzeichnet die ausgewählte(n) Prüfung(en) als "Kein Befund".
 - "X" oder "x" markiert das/die ausgewählte(n) Kästchen als "Nicht zutreffend".

3.7 Checkliste - Abschnitt "Informationen zu Schwachstellen"

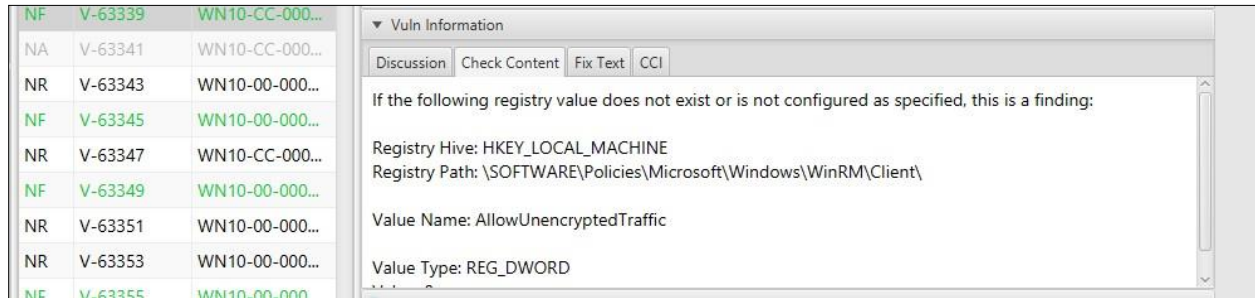
Der Abschnitt "**Schwachstelleninformationen**" der Stile SV 2.x Classic enthält fünf Registerkarten, die sich auf die in der mittleren Spalte ausgewählte Schwachstelle beziehen (die Themenstile Light und Dark enthalten diese Registerkarten nicht). Der Stil kann unter **Optionen** >> **Voreinstellungen** ausgewählt werden (siehe Abschnitt [2.5.4 Optionen](#)).

Die Registerkarten von SV 2.x Classic sind:

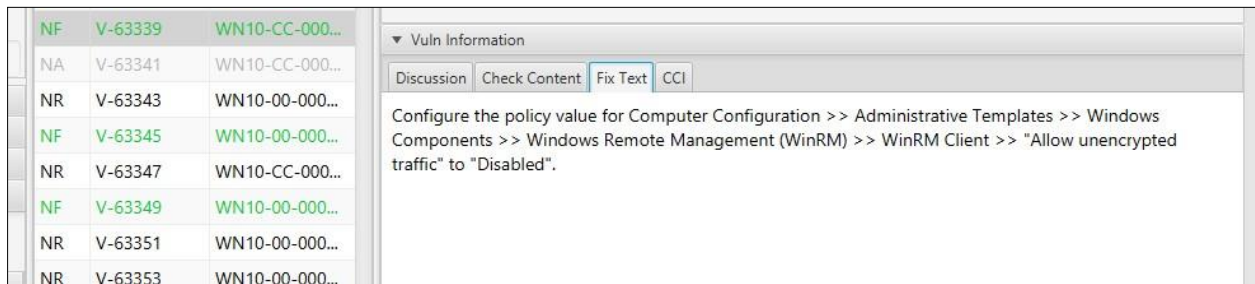
- Registerkarte "**Diskussion**" - Eine kurze Beschreibung der Prüfung.



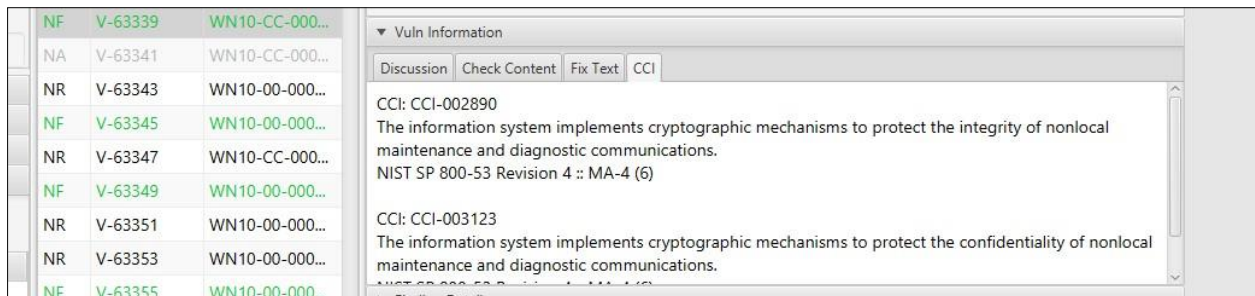
- Registerkarte "**Prüfungsinhalt**" - Beschreibt, wie die Prüfung zur Überprüfung durchzuführen ist (automatisierte Benchmarks enthalten weder diese Registerkarte noch manuelle Prüfungsanweisungen).



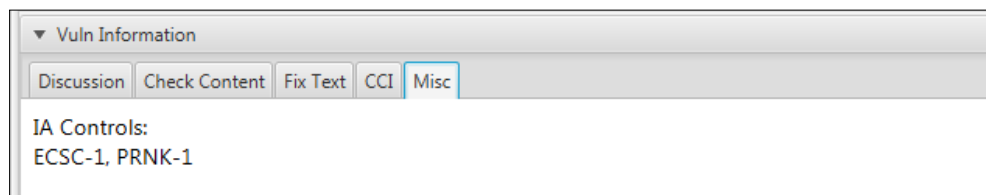
- Registerkarte **"Text reparieren"** - Beschreibt, wie ein offener Befund für die Prüfung repariert werden kann.



- Registerkarte **CCI** - Bietet CCI-Informationen über die Prüfung und die NIST SP 800-53-Referenz.



- Registerkarte **Verschiedenes** - Bietet IA-Kontrollen für die Prüfung (erscheint nur, wenn zutreffend).



3.8 Checkliste - Abschnitt "Funddetails" und Abschnitt "Kommentare"

Verwenden Sie die Abschnitte " **Finding Details**" und " **Comments**" , um Details und Kommentare des Gutachters zu erfassen.

Fügen Sie **Suchdetails** oder **Kommentare** in großen Mengen ein, indem Sie mit der rechten Maustaste in den mittleren Bereich klicken und

Text einfügen wählen Sie dann aus, wo Sie Details oder Kommentare einfügen möchten.

