

# The STIG and Database Security

John Calandra  
McCallie Associates  
DoD Contractor

# Agenda

- ▶ The Information Assurance Support Environment Web Site
- ▶ Security Technical Implementation Guides (STIGs)
- ▶ Finding A STIG
- ▶ The STIG Viewer
  - ❖ Loading a STIG
  - ❖ Manual Checklist
  - ❖ Checklist Export
- ▶ Security Posture
  - ❖ Reporting
  - ❖ Strategy
  - ❖ Framework
  - ❖ Filtering & Refactoring SQL code from STIG
- ▶ Questions & Answers

# The Information Assurance Support Environment Web Site

The screenshot displays the IASE website interface. At the top, the browser address bar shows the URL <http://iase.disa.mil/stigs/Pages/index.aspx>. The page header features the IASE logo and the text "Information Assurance Support Environment". A navigation menu includes links for Home, Cybersecurity Training, Topic Map, STIGs, Tools, News, Help, and RSS Feeds. A search bar is located on the right side of the header.

The main content area is titled "Security Technical Implementation Guides (STIGs)". A sidebar on the left lists various resources, including "STIGs Home", "SRG/STIG Tools", "STIGs Technologies", "Security Requirement Guides", "DoD Annex for NIAP Protection Profiles", "Vendor Process", "STIG Library Compilation Bulk Download (zip format)", "Control Correlation Identifier (CCI)", "FAQs", "Contact Us", and "STIG Mailing List". A note indicates that a DoD PKI Cert is required for certain resources.

The main content area includes a "STIGs Updates!" section with a list of recent updates:

- Draft Voice Video Session Management Security Requirements Guide (SRG), Version 1
- Draft Voice Video Endpoint SRG, Version 1 Release Memo
- Draft Voice Video Endpoint SRG, Version 1 Comment Matrix
- STIG Viewer, Version 2.1
- Draft Juniper SRX Services Gateway STIG, Version 1 Release Memo
- Draft Juniper SRX Services Gateway V12 X44 STIG Overview, Version 1
- Draft Juniper SRX Services Gateway V12 X44 Application Layer Gateway (ALG) STIG, Version 1
- Draft Juniper SRX Services Gateway V12 X44 Intrusion Detection and Prevention System (IDPS) STIG, Version 1

Below the list, a paragraph explains that STIGs and NSA Guides are configuration standards for DOD IA and IA-enabled devices/systems. It notes that since 1998, DISA has played a critical role in enhancing the security posture of DoD's security systems by providing these guides. The guides contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

A section titled "Questions or comments?" provides contact information for the DISA STIG Customer Support Desk: [disa.stig\\_spt@mail.mil](mailto:disa.stig_spt@mail.mil).

The footer of the page includes links for Home, Privacy Policy, Accessibility, Policy and Guidance, Cybersecurity Related Links, Cybersecurity Acronyms, Help Desk, Webmaster, and Site Map. It also states that IASE is sponsored by the Defense Information Systems Agency (DISA) and provides the page revision date: 5/21/2015 10:45 AM.

# The Information Assurance Support Environment Web Site: Finding Your STIG

The screenshot displays the IASE (Information Assurance Support Environment) website interface. At the top left is the IASE logo, consisting of a lowercase 'i' in a circle followed by the acronym 'IASE' in large purple letters and the full name 'Information Assurance Support Environment' in smaller text. To the right of the logo is a search box containing the text 'All Sites' and a dropdown arrow. Below the logo and search box is a dark navigation bar with the following items: Home, Cybersecurity Training (with a dropdown arrow), Topic Map (with a dropdown arrow), STIGs (with a dropdown arrow), Tools (with a dropdown arrow), News, Help, and RSS Feeds (with an RSS icon). A secondary navigation menu is open below the 'STIGs' menu item, listing: STIGs Home, SRG/STIG Tools, STIGs Technologies (highlighted in green), Security Requirements Guides, DoD Annex for NIAP Protection Profiles, Vendor Process, STIG Library Compilation Bulk Download (.zip format), Control Correlation Identifier (CCI), FAQs, Contact Us, STIG Mailing List, Draft Voice Video Endpoint SRG, Version 1 Cor, and STIG Viewer, Version 2.1, Update 12/16/2015. On the left side of the page, there is a vertical purple sidebar menu with the following items: STIGs Home, SRG/STIG Tools, STIGs Technologies, Security Requirement Guides, DoD Annex for NIAP Protection Profiles, Vendor Process, STIG Library Compilation Bulk Download (.zip format), Control Correlation Identifier (CCI), FAQs, and Contact Us. In the center of the page, the word 'Security' is partially visible, and below it is a blue 'STIGs' button. To the right of the 'STIGs Technologies' menu item, there is a 'STIGs Master List (A to Z)' section with a list of categories: Operating Systems, Application Security, Mobility, Network / Perimeter / Wireless, Cross Domain Solutions, Sunset Products, HBSS, Policy, and SCAP Content/Tools.

# The Information Assurance Support Environment Web site: A-Z STIG List

UNCLASSIFIED

http://iase.disa.mil/stigs/Pages/a-z.aspx

A-Z

**IASE** Information Assurance Support Environment

All Sites

Home Cybersecurity Training Topic Map STIGs Tools News Help RSS Feeds

Home > STIGs > A-Z

## STIGs Master List (A to Z)

\*PKI = DoD PKI Certificate Required

Download	Date	Size	Format
General DoD Cloud Computing Policy Questions: <a href="mailto:osd.cloudcomputing@mail.mil">osd.cloudcomputing@mail.mil</a>			
DISA Cloud Services Support home page: <a href="http://iase.disa.mil/cloud_security/Pages/services-support.aspx">http://iase.disa.mil/cloud_security/Pages/services-support.aspx</a>			
DISA Cloud Services Support Contact: <a href="http://disa.mil/Computing/Cloud-Services/Cloud-Support/Contact-Us">http://disa.mil/Computing/Cloud-Services/Cloud-Support/Contact-Us</a>			
DISA milCloud support email: <a href="mailto:disa.milcloud@mail.mil">disa.milcloud@mail.mil</a>			
DISA Cloud Services Support Office email: <a href="mailto:disa.meade.re.mbx.disa-commercial-cloud@mail.mil">disa.meade.re.mbx.disa-commercial-cloud@mail.mil</a>			
Questions, Comments, and Recommendations may be sent via e-mail as follows RE: Cloud Computing SRG: DISA SRG/STIG Support Desk Email: <a href="mailto:disa.stig_spt@mail.mil">disa.stig_spt@mail.mil</a>			
CND CONOPS: DISA SRG/STIG Support Desk Email: <a href="mailto:disa.stig_spt@mail.mil">disa.stig_spt@mail.mil</a>			
All other DISA Cloud Computing related documents: <a href="mailto:disa.meade.re.mbx.disa-commercial-cloud@mail.mil">disa.meade.re.mbx.disa-commercial-cloud@mail.mil</a>			
<b>Red Hat JBoss Enterprise Application Platform (EAP) 6.3 STIG V1R1 Release Memo</b>	12/8/2015	20 KB	PDF
<b>Mobile devices have moved, find them here: <a href="#">Mobility</a></b>			
<b>2015-05-06 DoD Interim Guidance for Implementing Derived PKI Credentials on Unclass CMDs</b>	5/11/2015	686 KB	PDF
<b>Access 2007 STIG - Version 4, Release 12</b>	10/23/2015	353 KB	ZIP
<b>Access 2010 STIG - Version 1, Release 8</b>	1/23/2015	536 KB	ZIP
<b>Access 2010 STIG Benchmark - Version 1, Release 1 (SCC tool use only)</b>	5/18/2015	14 KB	ZIP

<http://iase.disa.mil/Pages/index.aspx>

### STIGs Related Links

- + STIGs Home
- + SRG/STIG Tools
- + STIGs Technologies
- + Security Requirement Guides
- Cloud Computing Security
- DoD Annex for NIAP Protection Profiles
- Vendor Process
- STIG Library Compilation Bulk Download (.zip format)
- Control Correlation Identifier (CCI)
- FAQs
- Contact Us
- STIG Mailing List**

# The Information Assurance Support Environment Web site: Oracle STIGs

<a href="#">Oracle 11g Database STIG - Version 8, Release 15</a>	10/23/2015	705 KB	ZIP
<a href="#">Oracle 12c Database Release Memo</a>	10/18/2015	71 KB	PDF
<a href="#">Oracle 12c Database STIG - Version 1, Release 1</a>	10/18/2015	395 KB	ZIP
<a href="#">Oracle Exadata Integrated Lights Out Manager</a>	3/31/2015	617 KB	PDF
<a href="#">Oracle Exadata Storage Server</a>	3/31/2015	582 KB	PDF
<a href="#">Oracle Exadata Sun Data Center InfiniBand Switch 36</a>	3/31/2015	602 KB	PDF
<a href="#">Oracle Exadata ZFS Storage Appliance</a>	3/31/2015	613 KB	PDF
<a href="#">Oracle Linux 5 IAVM - Version 1, Release 9 *PKI</a>	11/30/2015	191 KB	ZIP
<a href="#">Oracle Linux 5 Manual STIG - Version 1, Release 4</a>	10/23/2015	471 KB	ZIP
<a href="#">Oracle Linux 5 Manual STIG Release Memo</a>	7/16/2014	58 KB	PDF
<a href="#">Oracle Linux 6 IAVM - Version 1, Release 9 *PKI</a>	11/30/2015	191 KB	ZIP
<a href="#">Oracle Linux 6 Manual STIG - Version 1, Release 4</a>	10/23/2015	386 KB	ZIP
<a href="#">Oracle Linux 6 Manual STIG Release Memo</a>	7/13/2014	41 KB	PDF



# The STIG Viewer

The screenshot shows the STIG Viewer website. At the top, there is a browser address bar with the URL `il/stigs/Pages/index.aspx` and a tab titled "STIGs Home". Below the browser is the IASE logo, which stands for Information Assurance Support Environment. To the right of the logo is a search bar with the text "All Sites" and a magnifying glass icon. Below the logo and search bar is a navigation menu with the following items: Home, Cybersecurity Training, Topic Map, STIGs, Tools, News, Help, and RSS Feeds. The main content area is divided into a left sidebar and a main content area. The sidebar is purple and contains the following links: STIGs Home, SRG/STIG Tools, STIGs Technologies, Security Requirement Guides, DoD Annex for NIAP Protection Profiles, Vendor Process, STIG Library Compilation Bulk Download (.zip format), Control Correlation Identifier (CCI), FAQs, Contact Us, and STIG Mailing List. Below the sidebar links is a note: "\*PKI = DoD PKI Cert Required". The main content area has a breadcrumb trail: Home > STIGs. Below the breadcrumb trail is a sub-header: Security Technical Implementation Guides (STIGs). Under this sub-header is a list of STIGs with their respective update dates: Draft Oracle JRE 8 Overview - Version 1 - Update 12/21/2015, Draft Oracle JRE 8 Unix - Version 1 - Update 12/21/2015, Draft Oracle JRE 8 Windows - Version 1 - Update 12/21/2015, Draft Oracle JRE 8 Release Memo - Version 1 - Update 12/21/2015, Draft Oracle JRE 8 - Version 1 Comment Matrix - Update 12/21/2015, Draft Voice Video Session Management Security Requirements Guide (SRG), Version 1 - Update 12/16/2015, Draft Voice Video Endpoint SRG, Version 1 Release Memo - Update 12/16/2015, Draft Voice Video Endpoint SRG, Version 1 Comment Matrix - Update 12/16/2015, and STIG Viewer, Version 2.1 - Update 12/16/2015. Below the list is a paragraph of text: "The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to 'lock down' information systems/software that might otherwise be vulnerable to a malicious computer attack." Below the paragraph is a section titled "Questions or comments?" with the text: "Please contact DISA STIG Customer Support Desk: disa.stig\_spt@mail.mil".

Home > STIGs

## Security Technical Implementation Guides (STIGs)

- Draft Oracle JRE 8 Overview - Version 1 - Update 12/21/2015
- Draft Oracle JRE 8 Unix - Version 1 - Update 12/21/2015
- Draft Oracle JRE 8 Windows - Version 1 - Update 12/21/2015
- Draft Oracle JRE 8 Release Memo - Version 1 - Update 12/21/2015
- Draft Oracle JRE 8 - Version 1 Comment Matrix - Update 12/21/2015
- Draft Voice Video Session Management Security Requirements Guide (SRG), Version 1 - Update 12/16/2015
- Draft Voice Video Endpoint SRG, Version 1 Release Memo - Update 12/16/2015
- Draft Voice Video Endpoint SRG, Version 1 Comment Matrix - Update 12/16/2015
- STIG Viewer, Version 2.1 - Update 12/16/2015

The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

**Questions or comments?**  
Please contact DISA STIG Customer Support Desk:  
[disa.stig\\_spt@mail.mil](mailto:disa.stig_spt@mail.mil)

# The STIG Viewer



**IASE**

Information Assurance  
Support Environment



All Sites



[Home](#)

[Cybersecurity Training](#) ▾


[Topic Map](#) ▾

[STIGs](#) ▾

[Tools](#) ▾

[News](#)

[Help](#)

 [RSS Feeds](#)

[Home](#) > [STIGs](#) > [STIG Viewer](#)

## STIG Viewer

\*PKI = DoD PKI Certificate Required

### STIG Viewer

Download	Date	Size	Format
<a href="#">STIG Viewer Quick Reference Guide</a>	2/29/2012	2,261 KB	PDF
<a href="#">STIG Viewer Version 2.1</a>	12/16/2015	617 KB	JAR

### Stylesheets Sorted by STIG ID

Download	Date	Size	Format
<a href="#">STIG Sorted by STIG ID</a>	3/30/2015	105 KB	XSL
<a href="#">STIG Sorted by STIG ID - FOUO *PKI</a>	3/30/2015	105 KB	XSL

### Stylesheets Sorted by Vulnerability ID

Download	Date	Size	Format
<a href="#">STIG Sorted by Vulnerability ID</a>	3/30/2015	102 KB	XSL
<a href="#">STIG Sorted by Vulnerability ID - FOUO *PKI</a>	3/30/2015	105 KB	XSL

### STIGs Related Links

- + [STIGs Home](#)
- + [SRG/STIG Tools](#)
- + [STIGs Technologies](#)
- + [Security Requirements](#)
- [Cloud Computing Security](#)
- [DoD Annex for NIAP Profiles](#)
- [Vendor Process](#)
- [STIG Library Compilation Download \(.zip format\)](#)
- [Control Correlation Identifiers \(CCI\)](#)
- [FAQs](#)
- [Contact Us](#)
- [STIG Mailing List](#)



# The STIG Viewer

The screenshot displays the DISA STIG Viewer interface. The window title is "DISA STIG Viewer : 1.2.0". The menu bar includes "File", "Checklist", "Options", and "Help".

**Left Panel (STIGs):**

- STIGs
  - U\_Oracle11\_DB\_Instance\_V8R1.11\_Manual-xccdf.xml
  - U\_Oracle\_Database\_11-2g\_V1R2\_Manual-xccdf.xml
  - U\_Oracle\_Database\_11-2g\_V1R4\_Manual-xccdf.xml
  - U\_Oracle\_Database\_i2c\_STIG\_V1R1\_Manual-xccdf.xml

**Profile:** Profile (none)

View All STIG Data

Buttons: Add Filter, Remove Filter, Remove All Filters

**STIG ID List:**

- O121-BP-021100 - SRG-APP-000516-DB-999900
- O121-BP-021200 - SRG-APP-000516-DB-999900
- O121-BP-021300 - SRG-APP-000516-DB-999900
- O121-BP-021400 - SRG-APP-000516-DB-999900
- O121-BP-021500 - SRG-APP-000516-DB-999900
- O121-BP-021600 - SRG-APP-000516-DB-999900
- O121-BP-021700 - SRG-APP-000516-DB-999900
- O121-BP-021800 - SRG-APP-000516-DB-999900
- O121-BP-021900 - SRG-APP-000516-DB-999900
- O121-BP-022000 - SRG-APP-000516-DB-999900
- O121-BP-022100 - SRG-APP-000516-DB-999900
- O121-BP-022200 - SRG-APP-000516-DB-999900
- O121-BP-022300 - SRG-APP-000516-DB-999900
- O121-BP-022400 - SRG-APP-000516-DB-999900
- O121-BP-022500 - SRG-APP-000516-DB-999900
- O121-BP-022600 - SRG-APP-000516-DB-999900
- O121-BP-022700 - SRG-APP-000516-DB-999900
- O121-BP-022800 - SRG-APP-000516-DB-999900
- O121-BP-022900 - SRG-APP-000516-DB-999900
- O121-BP-023000 - SRG-APP-000516-DB-999900
- O121-BP-023100 - SRG-APP-000516-DB-999900
- O121-BP-023200 - SRG-APP-000516-DB-999900
- O121-BP-023300 - SRG-APP-000516-DB-999900
- O121-BP-023400 - SRG-APP-000516-DB-999900
- O121-BP-023500 - SRG-APP-000516-DB-999900
- O121-BP-023600 - SRG-APP-000516-DB-999900
- O121-BP-023700 - SRG-APP-000516-DB-999900
- O121-BP-023800 - SRG-APP-000516-DB-999900
- O121-BP-023900 - SRG-APP-000516-DB-999900
- O121-BP-024000 - SRG-APP-000516-DB-999900
- O121-BP-024100 - SRG-APP-000516-DB-999900
- O121-BP-024200 - SRG-APP-000516-DB-999900
- O121-BP-024300 - SRG-APP-000516-DB-999900
- O121-BP-024400 - SRG-APP-000516-DB-999900
- O121-BP-024500 - SRG-APP-000516-DB-999900
- O121-BP-024600 - SRG-APP-000516-DB-999900
- O121-BP-024700 - SRG-APP-000516-DB-999900
- O121-BP-024800 - SRG-APP-000516-DB-999900
- O121-BP-024900 - SRG-APP-000516-DB-999900
- O121-BP-025000 - SRG-APP-000516-DB-999900
- O121-BP-025100 - SRG-APP-000516-DB-999900
- O121-BP-025101 - SRG-APP-000516-DB-999900
- O121-BP-025200 - SRG-APP-000516-DB-999900
- O121-BP-025300 - SRG-APP-000516-DB-999900
- O121-BP-025400 - SRG-APP-000516-DB-999900
- O121-BP-025500 - SRG-APP-000516-DB-999900
- O121-BP-025600 - SRG-APP-000516-DB-999900
- O121-BP-025700 - SRG-APP-000516-DB-999900

**Right Panel (Rule Details):**

**Rule Title:** Audit trail data must be retained for at least one year.  
**STIG ID:** O121-BP-021100 **Rule ID:** SV-75899r1\_rule **Vuln ID:** V-61409  
**Severity:** CAT II **Class:** Unclass

**Discussion:**  
Without preservation, a complete discovery of an attack or suspicious activity may not be determined. DBMS audit data also contributes to the complete investigation of unauthorized activity and needs to be included in audit retention plans and procedures.

**Documentable:** No

**Check Content:**  
Review and verify the implementation of an audit trail retention policy.  
Verify that audit data is maintained for a minimum of one year.  
If audit data is not maintained for a minimum of one year, this is a finding.

**Fix Text:**  
Develop, document and implement an audit retention policy and procedures.  
It is recommended that the most recent thirty days of audit logs remain available online.  
After thirty days, the audit logs may be maintained off-line.  
Online maintenance provides for a more timely capability and inclination to investigate suspicious activity.

**References:**  
CCI: CCI-000366  
NIST SP 800-53 :: CM-6 b  
NIST SP 800-53A :: CM-6.1 (iv)  
NIST SP 800-53 Revision 4 :: CM-6 b

215 Rules Shown | Displaying Rule: 1

Clipboard

# The STIG Viewer: Loading a STIG

The screenshot displays the DISA STIG Viewer 1.2.0 application window. The title bar reads "DISA STIG Viewer : 1.2.0". The menu bar includes "File", "Checklist", "Options", and "Help". The "File" menu is open, showing options: "Import STIG" (Ctrl+I), "Import STIG from ZIP", "Export", "Print", and "Exit" (Ctrl+Q). A sub-menu is visible under "Export", listing files: "1\_Manual-xccdf.xml", "Manual\_xccdf.xml", "Manual-xccdf.xml", and "R.1\_Manual-xccdf.xml".

Below the menu, there is a "Profile (none)" dropdown, a "View All STIG Data" checkbox, a "Keyword" search field with a "+" button, and three buttons: "Add Filter", "Remove Filter", and "Remove All Filters".

The main area contains a list of STIG IDs under the heading "STIG ID". The first item is selected and highlighted in blue: "O121-BP-021100 - SRG-APP-000516-DB-999900". The list continues with IDs from "O121-BP-021200" to "O121-BP-023500".

On the right side, a panel displays details for the selected STIG ID:

- Rule Title: Aud
- STIG ID: O121-BP
- Severity: CAT II
- Discussion: Without preserva DBMS audit data included in audi
- Documentable: No
- Check Content: Review and verif
- Verify that audi
- If audit data is
- Fix Text: Develop, documen
- It is recommende

# The STIG Viewer: Manual Checklist

The screenshot displays the DISA STIG Viewer 1.2.0 application window. The title bar reads "DISA STIG Viewer : 1.2.0". The menu bar includes "File", "Checklist", "Options", and "Help".

The "Checklist" menu is open, showing the following options:

- Open Checklist from File
- Create Checklist - Current STIG
- Create Checklist - Current List
- U\_Orade\_Database\_12c\_STIG\_V1R1\_Manual-xccdf.xml

The main window is divided into several sections:

- Left Panel:** A tree view showing the selected file: "U\_Orade\_Database\_12c\_STIG\_V1R1\_Manual-xccdf.xml".
- Profile:** A dropdown menu set to "Profile (none)".
- View All STIG Data:** An unchecked checkbox.
- Keyword:** A search field with a "+" button and a dropdown arrow.
- STIG ID List:** A list of STIG IDs, with "O121-BP-021100 - SRG-APP-000516-DB-999900" selected. The list includes IDs from O121-BP-021100 to O121-BP-022700.
- Right Panel:** A detailed view of the selected STIG ID, showing:
  - Rule Title:** (partially visible)
  - STIG ID:** O121-BP-021100 - SRG-APP-000516-DB-999900
  - Severity:** CA
  - Discussion:** Without pres... DBMS audit de... included in...
  - Documentable:**
  - Check Content:** Review and ve...
  - Verify that:**

# The STIG Viewer: Manual Checklist

The screenshot displays the DISA STIG Viewer interface for the Oracle Database 12c Security Technical Implementation Guide Checklist. The application window title is "DISA STIG Viewer: Oracle Database 12c Security Technical Implementation Guide Checklist".

**STIG ID List:** A list of STIG IDs is shown on the left, with O121-BP-021300 highlighted in red. Other IDs include O121-BP-021100, O121-BP-021200, O121-BP-021400, O121-BP-021500, O121-BP-021600, O121-BP-021700, O121-BP-021800, O121-BP-021900, O121-BP-022000, O121-BP-022100, O121-BP-022200, O121-BP-022300, O121-BP-022400, O121-BP-022500, O121-BP-022600, O121-BP-022700, O121-BP-022800, O121-BP-022900, O121-BP-023000, O121-BP-023100, O121-BP-023200, O121-BP-023300, O121-BP-023400, O121-BP-023500, O121-BP-023600, and O121-BP-023700.

**Findings Summary:** The top right shows "Status: Not a Finding" and "Severity: Not Applicable". A "Severity Override" dropdown is also present.

**Rule Details:** The selected rule is "Oracle SQL92\_SECURITY parameter must be set to TRUE." with STIG ID SV-75919r1\_rule and Vuln ID V-61429.

**Discussion:** The discussion explains that the configuration option SQL92\_SECURITY specifies whether table-level SELECT privileges are required to execute an update or delete that references table column values. If disabled (set to FALSE), the UPDATE privilege can be used to determine values that should require SELECT privileges.

**SQL Examples:** The application shows two SQL scripts. The first script sets SQL92\_SECURITY = FALSE and demonstrates a user with delete privilege being able to derive a salary value greater than 3000. The second script sets SQL92\_SECURITY = TRUE and shows the same user being prevented from deriving the salary value.

**Error Message:** An error message is displayed: "ERROR at line 1: ORA-01031: insufficient privileges".

**Overview:** The bottom left shows an overview of findings: Open: 2, Not a Finding: 8, N/A: 1, Not Reviewed: 204, Total: 215.

**Target Data:** The bottom right section includes fields for Target Data: HOST NAME, IP, MAC, and Role, along with a "Get Host Data" button.

# The STIG Viewer: Manual Checklist

DISA STIG Viewer : Oracle Database 12c Security Technical Implementation Guide Checklist\*

File Import Export Options

STIG ID	Status
O121-BP-021100 - SRG-APP-000516	Not a Finding
O121-BP-021200 - SRG-APP-000516	Not Reviewed
O121-BP-021300 - SRG-APP-000516	Open
O121-BP-021400 - SRG-APP-000516	Not a Finding
O121-BP-021500 - SRG-APP-000516	Not Applicable
O121-BP-021600 - SRG-APP-000516	
O121-BP-021700 - SRG-APP-000516	
O121-BP-021800 - SRG-APP-000516	
O121-BP-021900 - SRG-APP-000516	
O121-BP-022000 - SRG-APP-000516	
O121-BP-022100 - SRG-APP-000516	
O121-BP-022200 - SRG-APP-000516	
O121-BP-022300 - SRG-APP-000516	
O121-BP-022400 - SRG-APP-000516	
O121-BP-022500 - SRG-APP-000516	
O121-BP-022600 - SRG-APP-000516	
O121-BP-022700 - SRG-APP-000516	
O121-BP-022800 - SRG-APP-000516	
O121-BP-022900 - SRG-APP-000516	
O121-BP-023000 - SRG-APP-000516	
O121-BP-023100 - SRG-APP-000516	
O121-BP-023200 - SRG-APP-000516	
O121-BP-023300 - SRG-APP-000516	
O121-BP-023400 - SRG-APP-000516	

Rule: Oracle SQL92\_SECURITY parameter must be set to TRUE.  
STIG ID: 2100 Rule ID: SV-75919r1\_rule Vuln ID: V-61429  
Severity: Unclass

Discussion:  
The configuration option SQL92\_SECURITY specifies whether table-level column values. If this option is disabled (set to FALSE), the user can derive column values. If this option is enabled (set to TRUE), the user cannot derive column values.

The SQL92\_SECURITY setting of TRUE prevents the exploitation of user column values in that table by performing a series of update/delete operations. For example, with SQL92\_SECURITY set to FALSE, a user with only UPDATE privileges can delete an employee with a salary greater than 3000. With SQL92\_SECURITY set to TRUE, the user cannot delete the employee.

```
SQL92_SECURITY = FALSE
SQL> delete from scott.emp where sal > 3000;
1 row deleted
SQL> rollback;
Rollback complete

SQL92_SECURITY = TRUE
```



# The STIG Viewer: Checklist Export

The screenshot shows the 'DISA STIG Viewer: Oracle Database 12c Security Technical Implementation Guide Checklist' application. The 'Export' menu is open, showing options: 'Generate VMS Import File', 'Generate ARF/ASR Results Files', 'Generate Short-Form Checklist', and 'Generate CSV File (Excel)'. The 'Finding' dropdown is set to 'Finding'. The checklist table has columns for 'STIG ID' and 'Finding'. The selected item is O121-BP-022100 - SRG-APP-000516, with a finding description: 'The Oracle SQL92\_SECURITY parameter must be set to TRUE. CAT II Class: Unclass'. The 'Discussion' section explains that SQL92\_SECURITY specifies whether table column values can be derived. A SQL example shows that with SQL92\_SECURITY set to FALSE, a delete statement on the scott.emp table where salary is greater than 3000 would succeed, but with it set to TRUE, it would fail.

STIG ID	Finding
O121-BP-021500 - SRG-APP-000516	
O121-BP-021600 - SRG-APP-000516	
O121-BP-021700 - SRG-APP-000516	
O121-BP-021800 - SRG-APP-000516	
O121-BP-021900 - SRG-APP-000516	
O121-BP-022000 - SRG-APP-000516	
O121-BP-022100 - SRG-APP-000516	The Oracle SQL92_SECURITY parameter must be set to TRUE. CAT II Class: Unclass
O121-BP-022200 - SRG-APP-000516	
O121-BP-022300 - SRG-APP-000516	
O121-BP-022400 - SRG-APP-000516	
O121-BP-022500 - SRG-APP-000516	
O121-BP-022600 - SRG-APP-000516	
O121-BP-022700 - SRG-APP-000516	
O121-BP-022800 - SRG-APP-000516	
O121-BP-022900 - SRG-APP-000516	
O121-BP-023000 - SRG-APP-000516	
O121-BP-023100 - SRG-APP-000516	
O121-BP-023200 - SRG-APP-000516	

**Discussion:**  
The configuration option SQL92\_SECURITY specifies whether table column values can be derived. If this option is disabled (set to FALSE), the following example, with SQL92\_SECURITY set to FALSE, shows that an employee with a salary greater than 3000 can be deleted. With SQL92\_SECURITY set to TRUE, the delete statement fails.

```
SQL92_SECURITY = FALSE
SQL> delete from scott.emp where sal > 3000;
1 row deleted
SQL> rollback;
Rollback complete
```



# The STIG Viewer: Checklist Export

The screenshot displays the DISA STIG Viewer application window titled "Oracle Database 12c Security Technical Implementation Guide Checklist\*". The window has a green header bar with the text "UNCLASSIFIED". Below the header is a menu bar with "File", "Import", "Export", and "Options".

The main interface shows a list of STIG IDs on the left, with the status "Not a Finding" selected in a dropdown menu. The "Rule Title" field contains the text: "The Oracle SQL92\_SECURITY parameter must be set to TRUE.".

An "Export" dialog box is open in the foreground, featuring a "File..." button and three sections of checkboxes:

- STIG Items:**
  - Vuln\_Num
  - Severity
  - Group\_Title
  - Rule\_ID
  - Rule\_Ver
  - Rule\_Title
  - Vuln\_Discuss
  - IA\_Controls
  - Check\_Content
  - Fix\_Text
  - False\_Positives
  - False\_Negatives
- Checklist Items:**
  - Status
  - Finding\_Details
  - Comments
  - Severity\_Override
  - Severity\_Override\_Justification
- Misc.:**
  - Show\_CCI\_Ref
  - Show\_CCI\_Desc.
  - Show\_CCI\_800-53\_Mapping

An "Export" button is located at the bottom right of the dialog box.

# The STIG Viewer: Checklist Export

12cSTIG - Microsoft Excel

File Home Insert Page Layout Formulas Data Review View Approval Acrobat

Clipboard Font Alignment Number Styles

G8

	A	B	C	D	E
1	<b>Vuln ID</b>	<b>Severity</b>	<b>STIG ID</b>	<b>Rule Title</b>	<b>Status</b>
2	V-61409	medium	O121-BP-021100	Audit trail data must be retained for at least one year.	NotAFinding
3	V-61411	medium	O121-BP-021200	Access to default accounts used to support replication must be restricted to authorized DBA	NotAFinding
4	V-61413	medium	O121-BP-021300	Oracle instance names must not contain Oracle version numbers.	Open
5	V-61415	medium	O121-BP-021400	Fixed user and public database links must be authorized for use.	NotAFinding
6	V-61417	medium	O121-BP-021500	A minimum of two Oracle control files must be defined and configured to be stored on separate	NotAFinding
7	V-61419	medium	O121-BP-021600	A minimum of two Oracle redo log groups/files must be defined and configured to be stored	Not_Applicable
8	V-61421	medium	O121-BP-021700	The Oracle WITH GRANT OPTION privilege must not be granted to non-DBA or non-Application	NotAFinding
9	V-61423	medium	O121-BP-021800	Execute permission must be revoked from PUBLIC for restricted Oracle packages.	Open
10	V-61425	high	O121-BP-021900	The Oracle REMOTE_OS_AUTHENT parameter must be set to FALSE.	NotAFinding
11	V-61427	high	O121-BP-022000	The Oracle REMOTE_OS_ROLES parameter must be set to FALSE.	NotAFinding
12	V-61429	medium	O121-BP-022100	The Oracle SQL92_SECURITY parameter must be set to TRUE.	NotAFinding
13	V-61431	medium	O121-BP-022200	The Oracle REMOTE_LOGIN_PASSWORDFILE parameter must be set to EXCLUSIVE or NONE.	Not_Reviewed
14	V-61433	medium	O121-BP-022300	System privileges granted using the WITH ADMIN OPTION must not be granted to unauthorized	Not_Reviewed
15	V-61435	medium	O121-BP-022400	System Privileges must not be granted to PUBLIC.	Not_Reviewed
16	V-61437	medium	O121-BP-022500	Oracle roles granted using the WITH ADMIN OPTION must not be granted to unauthorized a	Not_Reviewed
17	V-61439	medium	O121-BP-022600	Object permissions granted to PUBLIC must be restricted.	Not_Reviewed
18	V-61441	high	O121-BP-022700	The Oracle Listener must be configured to require administration authentication.	Not_Reviewed
19	V-61443	medium	O121-BP-022800	Application role permissions must not be assigned to the Oracle PUBLIC role.	Not_Reviewed
20	V-61445	medium	O121-BP-022900	Oracle application administration roles must be disabled if not required and authorized.	Not_Reviewed
21	V-61447	medium	O121-BP-023000	Connections by mid-tier web and application systems to the Oracle DBMS must be protected	Not_Reviewed

# Security Posture

- ▶ John's definition of Security Posture:

A security posture is the means by which all events contrary to planned operation of a system are detected and thwarted.

- ▶ A [database] security posture includes detection of invalid
  - ❖ User events (logins, access)
  - ❖ Account events (creation, locked)
  - ❖ Configuration settings (permissions, settings)
  - ❖ Jobs (failures, long-running)

# Security Posture

A security posture is not only detection/mitigation of threats – it is also ensures your database is set up and running properly!

# Security Posture: Reporting

- ▶ Two types
  - ❖ Full-blown STIG reports
  - ❖ Monitoring reports
- ▶ Full-blown STIG reports
  - ❖ All items on STIG reported
  - ❖ Open items on report (findings) may be required to be placed on a POA&M (Plan of Action & Milestones)
  - ❖ POA&M typically required by Security/IA personnel
- ▶ Monitoring reports
  - ❖ Customized reports intended for internal use
  - ❖ Purpose is for maintenance of the security posture
  - ❖ Monitoring reports
- ▶ To be manageable, both types of reporting should be automated

# Security Posture: Reporting

## ▶ Full-Blown STIG

- ❖ All STIG items reported (coded + policy)
- ❖ Non-STIG related items excluded
- ❖ Item status
  - Coded checks: OPEN (finding) or Not A Finding
  - Policy checks: OPEN or CLOSED with explanation (one-liner)

## ▶ Monitoring

- ❖ Reports contain only invalid items
- ❖ Reports include non-STIG related items
- ❖ Reports exclude policy items
- ❖ Intent of report is to mitigate invalid items



# Security Posture: Strategy

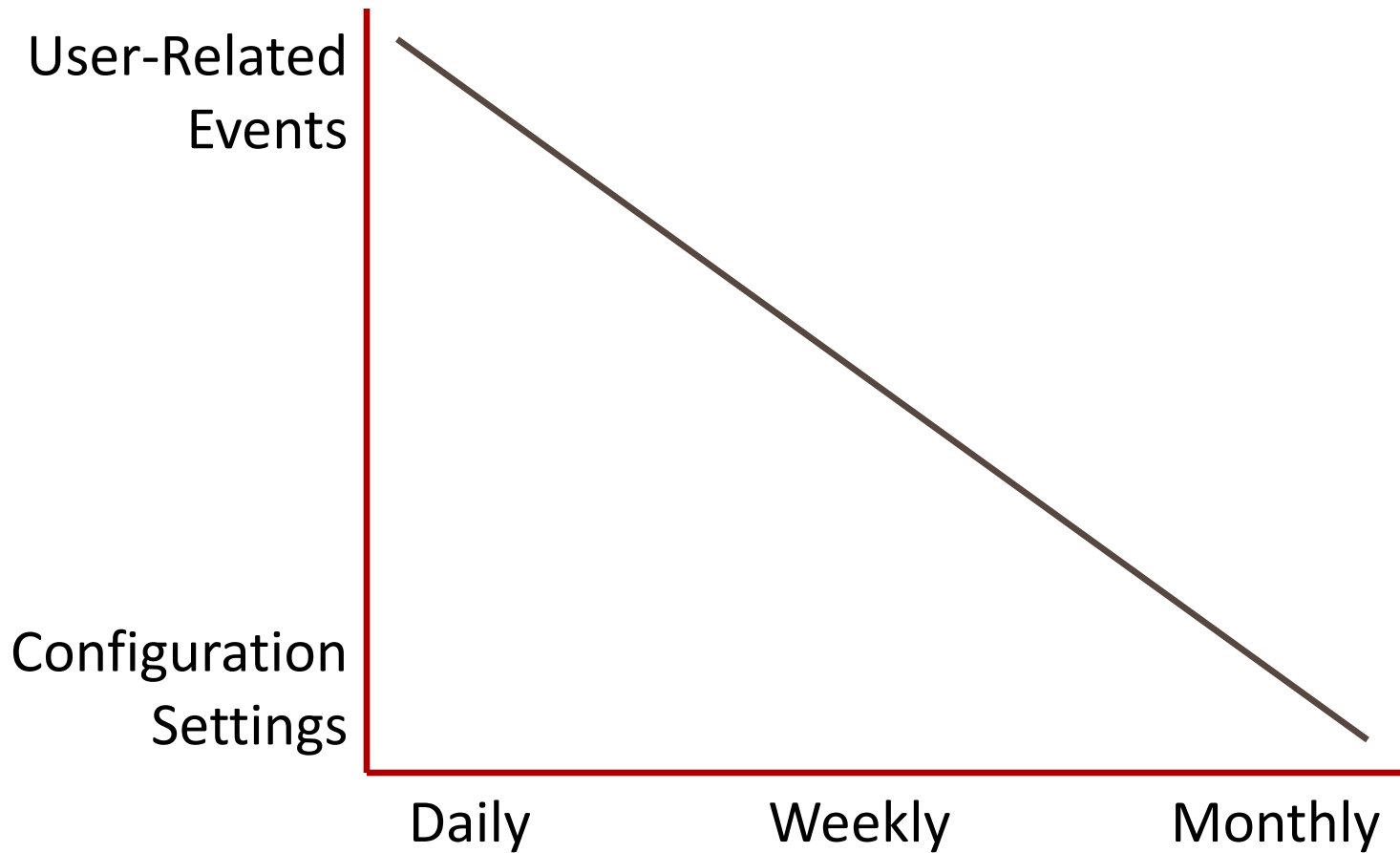
- ▶ **Goal: Programming that automates detection/reporting of invalid events on a scheduled basis**
- ▶ Two general types of invalid events
  - ❖ User-related events
  - ❖ Configuration settings
- ▶ Frequency of checks
  - ❖ Daily
  - ❖ Weekly
  - ❖ Monthly
  - ❖ Quarterly (full STIGs)

# Security Posture: Strategy

## ▶ Steps

1. Review STIG – make list of “coded” checks vs. “policy” checks
  - Coded check: STIG supplies SQL – some items may need to be checked by OS commands only or SQL + OS commands
  - Policy check: No code, it is a one-time manual inspection but requires explanation
2. Determine items that need to be checked by automation but not in STIG – write code
3. Categorize coded checks by frequency (daily, weekly, monthly)

# Security Posture: Strategy

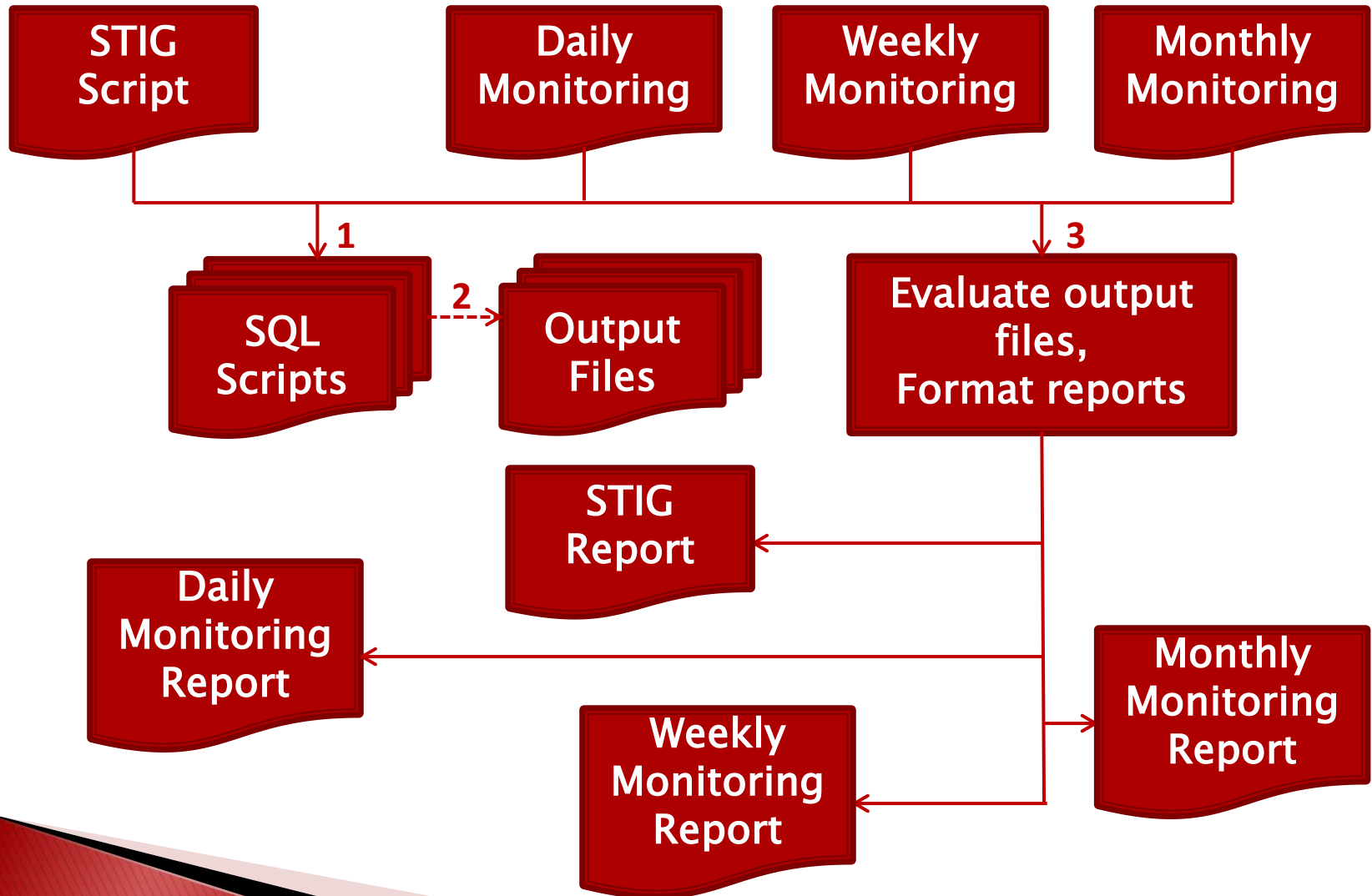


# Security Posture: Strategy

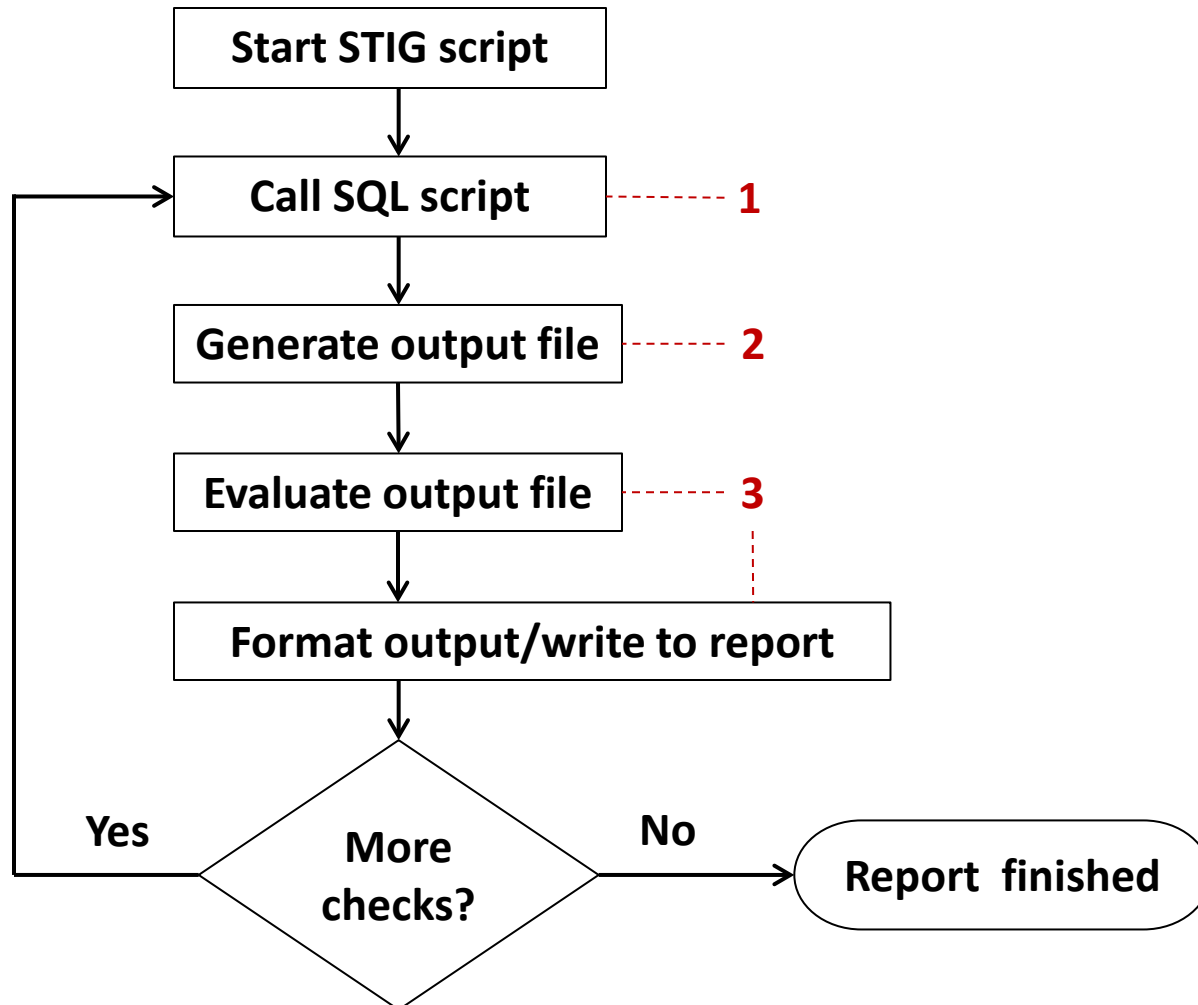
## ▶ Steps

1. Review STIG – make list of “coded” checks vs. “policy” checks
  - Coded check: STIG supplies SQL – some items may need to be checked by OS commands only or SQL + OS commands
  - Policy check: No code, it is a one-time manual inspection but requires explanation
2. Determine items that need to be checked by automation but not in STIG – write code
3. Categorize coded checks by frequency (daily, weekly, monthly)

# Security Posture: Framework



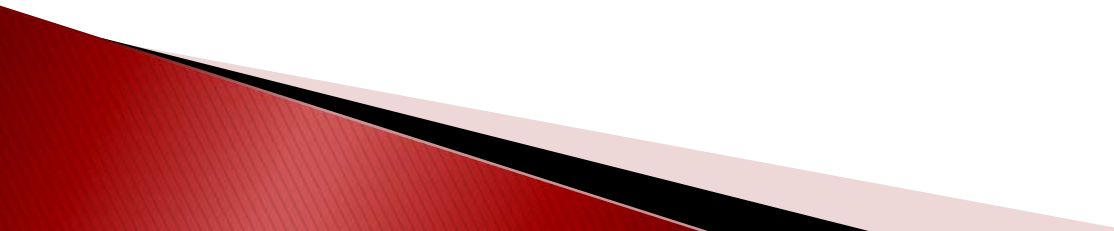
# Security Posture: Framework





# Security Posture:

## Filtering & Refactoring SQL code from STIG

- ▶ Rule Title: System privileges granted using the WITH ADMIN OPTION must not be granted to unauthorized user accounts.
  - ▶ STIG ID: O121-BP-02230
  - ▶ Code (next slide)
- 

# Security Posture:

## Filtering & Refactoring SQL code from STIG

- ▶ STIG ID: O121-BP-02230
- ▶ Check content code from STIG (code in dark grey is filter list):

```
select grantee, privilege from dba_sys_privs
where grantee not in ('SYS', 'SYSTEM',
'AQ_ADMINISTRATOR_ROLE', 'DBA', 'MDSYS',
'LBACSYS', 'SCHEDULER_ADMIN', 'WMSYS')
and admin_option = 'YES'
and grantee not in
(select grantee from dba_role_privs where
granted_role = 'DBA');
```

# Security Posture:

## Filtering & Refactoring SQL code from STIG

- ▶ Issues with using SQL code from STIG as-is:
  - Code should be refactored for readability and maintainability
  - Something in SQL output is needed so that the output can be recognized as a finding
  - Privileged accounts not in the filter list may show up in output
  - Make SQL code from STIG into a reusable file

# Security Posture: Filtering & Refactoring SQL code from STIG

- ▶ STIG ID: O121-BP-02230
- ▶ There is a privileged account for DBA admins called ORA\_ADMIN
- ▶ Refactored check content code from STIG:

```
SELECT
  'ALERT:' as ALERT,
  grantee,
  privilege
FROM dba_sys_privs where grantee not in (
  'AQ_ADMINISTRATOR_ROLE',
  'DBA',
  'LBACSYS',
  'MDSYS',
  'ORA_ADMIN',
  'SCHEDULER_ADMIN',
  'SYS',
  'SYSTEM',
  'WMSYS')
AND admin_option = 'YES'
AND grantee not in (
  SELECT grantee from dba_role_privs
  WHERE granted_role = 'DBA');
```

ALERT added to  
SELECT as search item

Select, filter list refactored for  
readability/maintainability

ORA\_ADMIN  
added to filter list

with\_admin\_option.sql

# The STIG and Database Security

- ▶ Questions & Answers