2020

StealthAUDIT®

Stealthbits Credential & Data Security Assessment User Guide

stealthbits

Table of Contents

stealthbits

Credential & Data Security Assessment Overview

Proper data security begins with a strong foundation. The Stealthbits Credential & Data Security Assessment (CDSA) provides a deep-dive into the security of your structured and unstructured data, Active Directory, and Windows infrastructure.

The CDSA Job depends upon several StealthAUDIT solutions for data collection. See the *POC Installation Requirements – Stealthbits Credential & Data Security Assessment* for installation and database requirements.

Supporting Solutions

At a minimum the following solutions need to run prior to the CDSA Job to provide the data used to generate the CDSA presentations:

→ .Active Directory Inventory Solution

☐ See the *StealthAUDIT .Active Directory Inventory Solution Admin Guide* for additional information.

→ Active Directory Solution

☐ See the *StealthAUDIT Active Directory Solution Admin Guide* for additional information.

→ Active Directory Permissions Analyzer Solution

☐ See the *StealthAUDIT Active Directory Permissions Analyzer Solution Admin Guide* for additional information.

→ File System Solution

☐ See the *StealthAUDIT File System Solution Admin Guide* for additional information.

→ Windows Solution

☐ See the *StealthAUDIT Windows Solution Admin Guide* for additional information.

Other solutions will also provide data to the CDSA Job:

→ .Azure Active Directory Inventory Solution
→ AWS Solution
→ Box Solution
→ Dropbox Solution
→ Exchange Solution
→ Oracle Solution
→ SharePoint Solution
→ SQL Solution

Additionally, the Sensitive Data Discovery Add-on also contributes to the CDSA presentations.

CDSA Job

The CDSA Job is available through the Instant Job Library under the CDSA library. See the StealthAUDIT Instant Job Wizard section of the *StealthAUDIT User Guide* for instruction to add this instant job to the Jobs tree. When installing the job, select **Local host** on the Hosts pages of the StealthAUDIT Instant Job Wizard.

Ensure the supporting solutions have successfully collected and analyzed data prior to running this job. See the StealthAUDIT Job Dependencies section for alignment between presentation slides and jobs that supply the data points.

The CDSA Job generates three PowerPoint files.

→ For the Presenter

☐ The *Stealthbits_CDSA_Presentation_Presentation.pptx* file is designed to be presented live to the customer.

→ For the Customer as printable assets

☐ The *Stealthbits_CDSA_8.5x11_Presentation.pptx* file is designed to be given to the customer for self-review as a PDF file.

☐ The *Stealthbits_CDSA_A4_Presentation.pptx* file is designed to be given to the customer for self-review as a PDF file.

CAUTION: Do not send any these presentations to a customer in PowerPoint format.

The printable assets can be converted to PDFs or printed "booklet style" at a professional print shop (suggested) if desired.

These presentations are located within the job's folder in the StealthAUDIT installation directory, which varies according to the location of the job within the Jobs tree. Navigate to this folder by clicking **Open Folder** on the job description.

The presentation files contain slides for both a classic CDSA presentation applicable to most organizations and an ePHI Security Assessment applicable to the healthcare industry.

Delivering a CDSA Presentation Slide Show

The *Stealthbits_CDSA_Presentation_Presentation.pptx* file is designed to be presented live to the customer. There are two presentation options for the live slide show:

→ The CDSA – Classic slide show contains the first 24 slides and is applicable for most organizations

→ The ePHI Security Assessment contains the ending slides with select summary slides from the Classic slide show and is applicable to the healthcare industry

Use the Custom Slide Show drop-down menu on the Slide Show ribbon in PowerPoint to select the appropriate presentation.

NOTE: Slide 17 is hidden by default as same information is available on Slides 18-20.

The Stealthbits University includes a training module with details on the key talking points for a live delivery of the slide shows. Check out the 315 – Getting Started with Credential & Data Security Assessment training course.

Choosing a PDF Version

Both of the printable assets have two customized options for converting to a PDF:

→ The CDSA Classic slide show contains the first 24 slides and is applicable for most organizations

→ The ePHI Security Assessment contains the ending slides with select summary slides from the Classic slide show and is applicable to the healthcare industry

Use the **Save As** option to create the appropriate custom PDF.

Step 1 – Set the file name as desired and change the Save As type to **PDF**.

Step 2 – Click the **Options** button and change the Range to **Custom show**.

Step 3 – By default, this is set to the CDSA Classic show. If needed, change it to the ePHI Security Assessment show.

Step 4 – Click **OK** to confirm the option, and then click **Save** to generate the PDF.

The presentation is converted to a PDF with only the applicable slides included.

NOTE: Slide 16 is hidden by default as same information is available on Slides 17-19.

Custom Slide Show Alignment

The table lists each slide as it is listed in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file. It indicates which slides are included in each custom slide show. There are slight variations in page numbering with the files designed to be saved as PDFs.

#	Slide Title	CDSA Classic	ePHI Security Assessment
1	Executive Summary	X	
2	Stealthbits' Credential and Data Security Assessment (CDSA)	X	
3	Data Security	X	
4	Condition: Open Access	X	x
5	Sensitive Data	X	
6	Stale Data	X	
7	Active Directory Security	X	x
8	Password Issues	X	
9	Toxic Active Directory Conditions	X	
10	Non-Administrators that can Perform Sensitive AD Actions	X	
11	Active Directory Sensitive Security Groups	X	
12	Windows: Assessment Summary	X	x
13	Local Administrators	X	
14	Service Accounts	X	
15	Ticket and Credential Management	X	
16	Shadow Access Rights	X	
~~17~~	Additional Findings (FS, AD, Windows OS)		
18	Additional Findings (FS, SharePoint, Box, Dropbox)	X	x
19	Additional Findings (Exchange, Databases)	X	x
20	Additional Findings (AD, Windows OS)	X	X
21	Product Portfolio	X	X
22	Path To Success	X	X
23	Stealthbits	X	X
24	Thank You	X	X
25	Executive Summary: ePHI Security Assessment		X
26	Stealthbits' ePHI Security Assessment		X
27	ePHI Data		x
28	Condition: Stale Data		x
29	AD Security Assessment		x

#	Slide Title	CDSA Classic	ePHI Security Assessment
30	Windows: Security Assessment		x
31	Shadow Access Rights to ePHI Data		x

StealthAUDIT Job Dependencies

In the following subsections, each slide is aligned to the jobs that supply its data. The slide number is specific to the *Stealthbits_CDSA_Presentation_Presentation.pptx* file, as there are slight various in page numbering with the files designed to be saved as PDFs. Many jobs contribute to multiple slides, so jobs are highlighted yellow the first time they are listed after the Data Security list.

Executive Summary Slide

Slide 1 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has no data points.

Stealthbit's Credential and Data Security Assessment (CDSA) Slide

Slide 2 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has no data points.

Data Security Slide

Slide 3 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan

→ FileSystem

☐ 0.Collection > 1-FSAA System Scans
☐ 0.Collection > 2-FSAA Bulk Import

Data is also supplied by the following jobs when they have been executed:

→ AWS

☐ 0.Collection > 1.AWS_OrgScan
☐ 0.Collection > 2.AWS_S3Scan

→ Box

☐ 0.Collection > 1-Box_Access Scans
☐ 0.Collection > 2-Box_Import

→ Dropbox

☐ 0.Collection > 1-Dropbox_Permissions Scan

☐ 0.Collection > 2-Dropbox_Permissions Bulk Import

→ Exchange

☐ 4. Mailboxes > Sizing > 0. Collection > EX_MBSize

☐ 5. Public Folders > Growth and Size > Collection > PF_FolderScans

→ Oracle

☐ 0.Collection > 1.Discovery > Oracle_Servers

☐ 0.Collection > 2.Collection > 1-Oracle_PermissionsScan

→ SharePoint

☐ 0.Collection > 2-SPAA_SystemScans

☐ 0.Collection > 5-SPAA_BulkImport

→ SQL

☐ 0.Collection > 0-SQL_InstanceDiscovery

☐ 0.Collection > 1-SQL_PermissionsScan

Condition: Open Access Slide

Slide 4 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan

→ FileSystem

☐ 0.Collection > 1-FSAA System Scans

☐ 0.Collection > 2-FSAA Bulk Import

☐ 1.Open Access >FS_OpenAccess

Data is also supplied by the following jobs when they have been executed:

→ AWS

☐ 0.Collection > 1.AWS_OrgScan

☐ 0.Collection > 2.AWS_S3Scan

☐ 6.S3 Permissions > AWS_OpenBuckets

→ Box

- ☐ 0.Collection > 1-Box_Access Scans
- ☐ 0.Collection > 2-Box_Import

→ Dropbox

- ☐ 0.Collection > 1-Dropbox_Permissions Scan
- ☐ 0.Collection > 2-Dropbox_Permissions Bulk Import

→ Exchange

- ☐ 4. Mailboxes > Permissions > 0. Collection > EX_Delegates
- ☐ 4. Mailboxes > Permissions > 0. Collection > EX_MBRights
- ☐ 4. Mailboxes > Permissions > 0. Collection > EX_Perms
- ☐ 4. Mailboxes > Permissions > 0. Collection > EX_SendAs
- ☐ 4. Mailboxes > Permissions > EX_MailboxAccess
- ☐ 4. Mailboxes > Sizing > 0. Collection > EX_MBSize
- ☐ 5. Public Folders > Growth and Size > Collection > PF_FolderScans
- ☐ 5. Public Folders > Permissions > Collection > PF_EntitlementScans

→ Oracle

- ☐ 0.Collection > 1.Discovery > Oracle_Servers
- ☐ 0.Collection > 2.Collection > 1-Oracle_PermissionsScan
- ☐ 3.Permissions > Oracle_PublicPermissions

→ SharePoint

- ☐ 0.Collection > 2-SPAA_SystemScans
- ☐ 0.Collection > 5-SPAA_BulkImport
- ☐ 2.High Risk Sites > SP_OpenAccess

→ SQL

- ☐ 0.Collection > 0-SQL_InstanceDiscovery
- ☐ 0.Collection > 1-SQL_PermissionsScan
- ☐ 3.Permissions > SQL_PublicPermissions

Sensitive Data Slide

Slide 5 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan

→ FileSystem

☐ 0.Collection > 1-SEEK System Scans
☐ 0.Collection > 2-SEEK Bulk Import
☐ 7.Sensitive Data > FS_DLPResults

Data is also supplied by the following jobs when they have been executed:

→ AWS

☐ 0.Collection > 1.AWS_OrgScan
☐ 0.Collection > 4.AWS_S3SddScan
☐ 8.S3 Sensitive Data > AWS_SensitiveData

→ Dropbox

☐ 0.Collection > 1-Dropbox_SDD Scan
☐ 0.Collection > 2-Dropbox_SDD Bulk Import
☐ 5.Sensitive Data > Dropbox_SensitiveData

→ Exchange

☐ 7. Sensitive Data > 0.Collection > EX_Mailbox_SDD
☐ 7. Sensitive Data > 0.Collection > EX_PublicFolder_SDD
☐ 7. Sensitive Data > EX_SDDResults

→ Oracle

☐ 0.Collection > 1.Discovery > Oracle_Servers
☐ 0.Collection > 2.Collection > 1-Oracle_PermissionsScan
☐ 0.Collection > 2.Collection > 2-Oracle_SensitiveDataScan
☐ 5.Sensitive Data > Oracle_SensitiveData

→ SharePoint

☐ 0.Collection > 1-SPSEEK_SystemScans
☐ 0.Collection > 4-SPSEEK_BulkImport
☐ 7.Sensitive Data > SP_SensitiveData

→ SQL

☐ 0.Collection > 0-SQL_InstanceDiscovery

☐ 0.Collection > 1-SQL_PermissionsScan

☐ 0.Collection > 2-SQL_SensitiveDataScan

☐ 5.Sensitive Data > SQL_SensitiveData

Stale Data Slide

Slide 6 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan

→ FileSystem

☐ 0.Collection > 1-FSAA System Scans

☐ 0.Collection > 2-FSAA Bulk Import

☐ 4.Content > Stale > FS_StaleContent

Data is also supplied by the following jobs when they have been executed:

→ Box

☐ 0.Collection > 1-Box_Access Scans

☐ 0.Collection > 2-Box_Import

→ Dropbox

☐ 0.Collection > 1-Dropbox_Permissions Scan

☐ 0.Collection > 2-Dropbox_Permissions Bulk Import

→ Exchange

☐ 5. Public Folders > Content > Collection > PF_ContentScans

→ Oracle

☐ 0.Collection > 1.Discovery > Oracle_Servers

☐ 0.Collection > 2.Collection > 1-Oracle_PermissionsScan

→ SharePoint

☐ 0.Collection > 2-SPAA_SystemScans

☐ 0.Collection > 5-SPAA_BulkImport

☐ 4.Content > SP_StaleFiles

→ SQL

☐ 0.Collection > 0-SQL_InstanceDiscovery

☐ 0.Collection > 1-SQL_PermissionsScan

Active Directory Security Slide

Slide 7 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan

→ Active Directory Permissions Analyzer

☐ 0.Collection > AD_ComputerRights
☐ 0.Collection > AD_ContainerRights
☐ 0.Collection > AD_DomainRights
☐ 0.Collection > AD_GroupRights
☐ 0.Collection > AD_OURights
☐ 0.Collection > AD_SiteRights
☐ 0.Collection > AD_UserRights

Data is also supplied by the following jobs when they have been executed:

→ .Azure Active Directory Inventory

☐ 1-AAD_Scan

Password Issues Slide

Slide 8 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan

→ Active Directory

☐ 2.Users > AD_WeakPasswords
☐ 2.Users > AD_PasswordStatus
☐ 4.Group Policy > AD_CPassword

Toxic Active Directory Conditions Slide

Slide 9 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan
☐ 3-AD_Exceptions

→ Active Directory

☐ 1.Groups > AD_CircularNesting
☐ 1.Groups > AD_EmptyGroups
☐ 1.Groups > AD_SensitiveSecurityGroups
☐ 1.Groups > AD_StaleGroups
☐ 2.Users > AD_SIDHistory
☐ 2.Users > AD_StaleUsers

Non-Administrators that can Perform Sensitive AD Actions Slide

Slide 10 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan

→ Active Directory Permissions Analyzer

☐ 0.Collection > AD_ComputerRights
☐ 0.Collection > AD_ContainerRights
☐ 0.Collection > AD_DomainRights
☐ 0.Collection > AD_GroupRights
☐ 0.Collection > AD_OURights
☐ 0.Collection > AD_SiteRights
☐ 0.Collection > AD_UserRights
☐ 1.Users > AD_ResetPasswordPermissions
☐ 2.Groups > AD_GroupMembershipPermissions
☐ 8.Domains > AD_DomainReplication

Active Directory Sensitive Security Groups Slide

Slide 11 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan

Windows: Assessment Summary Slide

Slide 12 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan

→ Windows

☐ Application > SG_LSASettings
☐ Application > SG_SecuritySupportProviders
☐ Application > SG_WDigestSettings
☐ Open Access > SG_OpenFolders
☐ Privileged Accounts > Local Administrators > SG_LocalAdmins
☐ Privileged Accounts > Local Administrators > SG_MicrosoftLAPS
☐ Privileged Accounts > Logon Rights > SG_LocalPolicies
☐ Privileged Accounts > Service Accounts > SG_ServiceAccounts
☐ Security Utilities > SG_PowerShellCommands

Local Administrators Slide

Slide 13 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan

→ Windows

☐ Privileged Accounts > Local Administrators > SG_LocalAdmins
☐ Privileged Accounts > Logon Rights > SG_LocalPolicies

16

stealthbits

Service Accounts Slide

Slide 14 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

- → .Active Directory Inventory

  - ☐ 1-AD_Scan

- → Windows

  - ☐ Application > SG_LSASettings
  - ☐ Application > SG_WDigestSettings
  - ☐ Privileged Accounts > Service Accounts > SG_ServiceAccounts
  - ☐ Security Utilities > SG_PowerShellCommands

Ticket and Credential Management Slide

Slide 15 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

- → .Active Directory Inventory

  - ☐ 1-AD_Scan

- → Windows

  - ☐ Application > SG_LSASettings
  - ☐ Application > SG_WDigestSettings
  - ☐ Security Utilities > SG_PowerShellCommands

Shadow Access Rights Slide

Slide 16 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

- → .Active Directory Inventory

  - ☐ 1-AD_Scan

- → Active Directory

  - ☐ 1.Groups > AD_SensitiveSecurityGroups
  - ☐ 2.Users > AD_WeakPasswords

→ Active Directory Permissions Analyzer

☐ 0.Collection > AD_ComputerRights
☐ 0.Collection > AD_ContainerRights
☐ 0.Collection > AD_DomainRights
☐ 0.Collection > AD_GroupRights
☐ 0.Collection > AD_OURights
☐ 0.Collection > AD_SiteRights
☐ 0.Collection > AD_UserRights
☐ 1.Users > AD_ResetPasswordPermissions
☐ 2.Groups > AD_GroupMembershipPermissions
☐ 7.Containers > AD_AdminSDHolder
☐ 8.Domains > AD_DomainReplication

→ FileSystem

☐ 0.Collection > 1-SEEK System Scans
☐ 0.Collection > 2-SEEK Bulk Import
☐ 7.Sensitive Data > FS_DLPResults

→ Windows

☐ Privileged Accounts > Local Administrators > SG_LocalAdmins
☐ Privileged Accounts > Local Administrators > SG_Sessions

Data is also supplied by the following jobs when they have been executed:

→ SQL

☐ 0.Collection > 0-SQL_InstanceDiscovery
☐ 0.Collection > 1-SQL_PermissionsScan
☐ 0.Collection > 2-SQL_SensitiveDataScan
☐ 5.Sensitive Data > SQL_SensitiveData

Additional Findings (FS, AD, Windows OS) Slide

Slide 17 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file is "hidden" by default. It is recommended to use Slides 18-20 instead, even when the primary jobs are the only ones supplying data. Slide 17 is an alternative to slides 18-20. It has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan

→ Active Directory

- ☐ 1.Groups > AD_StaleGroups
- ☐ 2.Users > AD_ServiceAccounts
- ☐ 2.Users > AD_StaleUsers
- ☐ 2.Users > AD_UserToken
- ☐ 3.Computers > AD_StaleComputers
- ☐ 4.Group Policy > AD_CPassword
- ☐ 8.Domains > AD_DomainReplication

→ FileSystem

- ☐ 0.Collection > 1-FSAA System Scans
- ☐ 0.Collection > 1-SEEK System Scans
- ☐ 0.Collection > 2-FSAA Bulk Import
- ☐ 0.Collection > 2-SEEK Bulk Import
- ☐ 2.Direct Permissions > FS_DomainUserACLs
- ☐ 3.Broken Inheritance > FS_BrokenInheritance
- ☐ 4.Content > Stale > FS_StaleContent
- ☐ 7.Sensitive Data > FS_DLPResults

→ Windows

- ☐ Application > SG_LSASettings
- ☐ Application > SG_WDigestSettings
- ☐ Privileged Accounts > Local Administrators > SG_LocalAdmins
- ☐ Privileged Accounts > Service Accounts > SG_ServiceAccounts

Additional Findings (FS, SharePoint, Box, Dropbox) Slide

Slide 18 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

- ☐ 1-AD_Scan

→ FileSystem

- ☐ 0.Collection > 1-FSAA System Scans
- ☐ 0.Collection > 1-SEEK System Scans
- ☐ 0.Collection > 2-FSAA Bulk Import
- ☐ 0.Collection > 2-SEEK Bulk Import
- ☐ 2.Direct Permissions > FS_DomainUserACLs
- ☐ 3.Broken Inheritance > FS_BrokenInheritance

☐ 4.Content > Stale > FS_StaleContent

☐ 7.Sensitive Data > FS_DLPResults

Data is also supplied by the following jobs when they have been executed:

→ Box

☐ 0.Collection > 1-Box_Access Scans

☐ 0.Collection > 2-Box_Import

→ Dropbox

☐ 0.Collection > 1-Dropbox_SDD Scan

☐ 0.Collection > 2-Dropbox_SDD Bulk Import

☐ 1.Access > Dropbox_Access

→ SharePoint

☐ 0.Collection > 2-SPAA_SystemScans

☐ 0.Collection > 5-SPAA_BulkImport

☐ 2.High Risk Sites > SP_AnonymousSharing

☐ 2.High Risk Sites > SP_OpenAccess

☐ 3.Broken Inheritance > SP_BrokenInheritance

☐ 4.Content > SP_StaleFiles

☐ 7.Sensitive Data > SP_SensitiveData

Additional Findings (Exchange, Databases) Slide

Slide 19 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan

Data is also supplied by the following jobs when they have been executed:

→ Exchange

☐ 4. Mailboxes > Permissions > 0. Collection > EX_Delegates

☐ 4. Mailboxes > Permissions > 0. Collection > EX_MBRights

☐ 4. Mailboxes > Permissions > 0. Collection > EX_Perms

☐ 4. Mailboxes > Permissions > 0. Collection > EX_SendAs

☐ 4. Mailboxes > Permissions > EX_AdminGroups

☐ 4. Mailboxes > Permissions > EX_MailboxAccess

☐ 4. Mailboxes > Sizing > EX_StaleMailboxes

- ☐ 5. Public Folders > Content > Collection > PF_ContentScans
- ☐ 5. Public Folders > Permissions > Collection > PF_EntitlementScans
- ☐ 7. Sensitive Data > 0.Collection > EX_Mailbox_SDD
- ☐ 7. Sensitive Data > 0.Collection > EX_PublicFolder_SDD
- ☐ 7. Sensitive Data > EX_SDDResults

→ Oracle

- ☐ 0.Collection > 1.Discovery > Oracle_Servers
- ☐ 0.Collection > 2.Collection > 1-Oracle_PermissionsScan
- ☐ 0.Collection > 2.Collection > 2-Oracle_SensitiveDataScan
- ☐ 1. Users and Roles > Oracle_PasswordIssues
- ☐ 3.Permissions > Oracle_PublicPermissions
- ☐ 4. Configuration > Oracle_DataDictionaryProtection
- ☐ 4. Configuration > Oracle_InstanceNameIssues
- ☐ 4. Configuration > Oracle_RemoteOSAuthentication
- ☐ 5.Sensitive Data > Oracle_SensitiveData

→ SQL

- ☐ 0.Collection > 0-SQL_InstanceDiscovery
- ☐ 0.Collection > 1-SQL_PermissionsScan
- ☐ 0.Collection > 2-SQL_SensitiveDataScan
- ☐ 1. Users and Roles > SQL_PasswordIssues
- ☐ 3.Permissions > SQL_PublicPermissions
- ☐ 4.Configuration > SQL_Authentication
- ☐ 4. Configuration > SQL_BestPractices
- ☐ 4.Configuration > SQL_CMDShell
- ☐ 5.Sensitive Data > SQL_SensitiveData

Additional Findings (AD, Windows OS) Slide

Slide 20 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

- ☐ 1-AD_Scan

→ Active Directory

- ☐ 1.Groups > AD_StaleGroups
- ☐ 2.Users > AD_ServiceAccounts
- ☐ 2.Users > AD_StaleUsers

    ☐   2.Users > AD_UserToken

    ☐   3.Computers > AD_StaleComputers

    ☐   4.Group Policy > AD_CPassword

    ☐   8.Domains > AD_DomainReplication

→   Windows

    ☐   Application > SG_LSASettings

    ☐   Application > SG_WDigestSettings

    ☐   Privileged Accounts > Local Administrators > SG_LocalAdmins

Product Portfolio Slide

Slide 21 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has no data points.

Path To Success Slide

Slide 22 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has no data points.

Stealthbits Slide

Slide 23 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has no data points.

Thank You Slide

Slide 24 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has no data points.

Executive Summary: ePHI Security Assessment Slide

Slide 25 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has no data points.

Stealthbits' ePHI Security Assessment Slide

Slide 26 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has no data points.

ePHI Data Slide

Slide 27 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan

→ FileSystem

☐ 0.Collection > 1-SEEK System Scans
☐ 0.Collection > 2-SEEK Bulk Import
☐ 0.Collection > 3-FSAA-Exceptions
☐ 7.Sensitive Data > FS_DLPResults

Data is also supplied by the following jobs when they have been executed:

→ AWS

☐ 0.Collection > 1.AWS_OrgScan
☐ 0.Collection > 4.AWS_S3SddScan
☐ 8.S3 Sensitive Data > AWS_SensitiveData

→ Box

☐ 0.Collection > 1-Box_Access Scans
☐ 0.Collection > 2-Box_Import

→ Dropbox

☐ 0.Collection > 1-Dropbox_SDD Scan
☐ 0.Collection > 2-Dropbox_SDD Bulk Import
☐ 5.Sensitive Data > Dropbox_SensitiveData

→ Exchange

☐ 7. Sensitive Data > 0.Collection > EX_Mailbox_SDD
☐ 7. Sensitive Data > 0.Collection > EX_PublicFolder_SDD
☐ 7. Sensitive Data > SDDResults
☐ 4. Mailboxes > Permissions > 0. Collection > EX_Delegates
☐ 4. Mailboxes > Permissions > 0. Collection > EX_MBRights

☐ 4. Mailboxes > Permissions > 0. Collection > EX_Perms

☐ 4. Mailboxes > Permissions > 0. Collection > EX_SendAs

☐ 4. Mailboxes > Permissions > EX_MailboxAccess

→ Oracle

☐ 0.Collection > 1.Discovery > Oracle_Servers

☐ 0.Collection > 2.Collection > 1-Oracle_PermissionsScan

☐ 0.Collection > 2.Collection > 2-Oracle_SensitiveDataScan

☐ 3.Permissions > Oracle_PublicPermissions

☐ 5.Sensitive Data > Oracle_SensitiveData

→ SharePoint

☐ 0.Collection > 1-SPSEEK_SystemScans

☐ 0.Collection > 4-SPSEEK_BulkImport

☐ ==0.Collection > 7-SPAA_Exceptions==

☐ 7.Sensitive Data > SP_SensitiveData

→ SQL

☐ 0.Collection > 0-SQL_InstanceDiscovery

☐ 0.Collection > 1-SQL_PermissionsScan

☐ 0.Collection > 2-SQL_SensitiveDataScan

☐ 3.Permissions > SQL_PublicPermissions

☐ 5.Sensitive Data > SQL_SensitiveData

Condition: Stale Data Slide

Slide 28 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan

→ FileSystem

☐ 0.Collection > 1-SEEK System Scans

☐ 0.Collection > 2-SEEK Bulk Import

☐ 7.Sensitive Data > FS_DLPResults

Data is also supplied by the following jobs when they have been executed:

→ Dropbox

☐ 0.Collection > 1-Dropbox_SDD Scan

- ☐ 0.Collection > 2-Dropbox_SDD Bulk Import
- ☐ 5.Sensitive Data > Dropbox_SensitiveData

→ SharePoint

- ☐ 0.Collection > 1-SPSEEK_SystemScans
- ☐ 0.Collection > 4-SPSEEK_BulkImport
- ☐ 7.Sensitive Data > SP_SensitiveData

AD Security Assessment Slide

Slide 29 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

- ☐ 1-AD_Scan
- ☐ 3-AD_Exceptions

→ Active Directory

- ☐ 1.Groups > AD_SensitiveSecurityGroups
- ☐ 2.Users > AD_WeakPasswords
- ☐ 2.Users > AD_PasswordStatus
- ☐   4.Group Policy > AD_CPassword

→ Active Directory Permissions Analyzer

- ☐ 1.Users > AD_ResetPasswordPermissions
- ☐ 2.Groups > AD_GroupMembershipPermissions
- ☐ 8.Domains > AD_DomainReplication

Windows: Security Assessment Slide

Slide 30 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

- ☐ 1-AD_Scan

→ Windows

- ☐ Application > SG_LSASettings
- ☐ Application > SG_WDigestSettings

☐ Privileged Accounts > Local Administrators > SG_LocalAdmins

☐ Privileged Accounts > Service Accounts > SG_ServiceAccounts

Shadow Access Rights to ePHI Data Slide

Slide 31 in the *Stealthbits_CDSA_Presentation_Presentation.pptx* file has the following primary job dependencies:

→ .Active Directory Inventory

☐ 1-AD_Scan

→ Active Directory

☐ 1.Groups > AD_SensitiveSecurityGroups

☐ 2.Users > AD_WeakPasswords

→ Active Directory Permissions Analyzer

☐ 0.Collection > AD_ComputerRights

☐ 0.Collection > AD_ContainerRights

☐ 0.Collection > AD_DomainRights

☐ 0.Collection > AD_GroupRights

☐ 0.Collection > AD_OURights

☐ 0.Collection > AD_SiteRights

☐ 0.Collection > AD_UserRights

☐ 1.Users > AD_ResetPasswordPermissions

☐ 2.Groups > AD_GroupMembershipPermissions

☐ 7.Containers > AD_AdminSDHolder

☐ 8.Domains > AD_DomainReplication

→ FileSystem

☐ 0.Collection > 1-SEEK System Scans

☐ 0.Collection > 2-SEEK Bulk Import

☐ 7.Sensitive Data > FS_DLPResults

→ Windows

☐ Privileged Accounts > Local Administrators > SG_LocalAdmins

☐ Privileged Accounts > Local Administrators > SG_Sessions

Data is also supplied by the following jobs when they have been executed:

→ SQL

☐ 0.Collection > 0-SQL_InstanceDiscovery

- ☐ 0.Collection > 1-SQL_PermissionsScan
- ☐ 0.Collection > 2-SQL_SensitiveDataScan
- ☐ 5.Sensitive Data > SQL_SensitiveData

More Information

Identify threats. Secure data. Reduce risk.

Stealthbits Technologies is a data security software company focused on protecting an organization's credentials and data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, we reduce security risk, fulfill compliance requirements, and decrease operations expense.

For information on our products and solution lines, check out our website at www.stealthbits.com or send an email to our information center at info@stealthbits.com.

If you would like to speak with a Stealthbits Sales Representative, please contact us at +1.201.447.9300 or via email at sales@stealthbits.com.

Have questions? Check out our online Documentation or our Training Videos (requires login): https://www.stealthbits.com/documentation. To speak to a Stealthbits Representative: please contact Stealthbits Support at +1.201.447.9359 or via email at support@stealthbits.com.

Need formal training on how to use a product more effectively in your organization? Stealthbits is proud to offer FREE online training to all customers and prospects! For schedule information, visit: https://www.stealthbits.com/on-demand-training.