

I'm not robot!

Cyberark dna user guide pdf

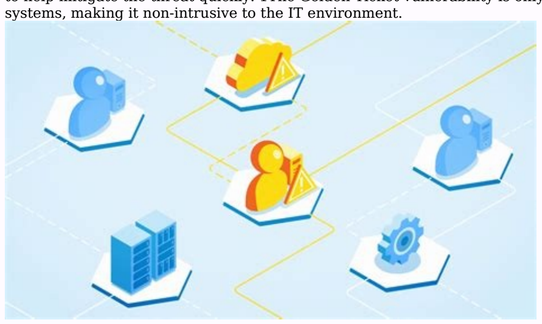
Cyberark user types. Cyberark installation guide. Cyberark setup guide. What is cyberark dna.

No Text Content! CyberArk DNA™ User Guide November 2020 Copyright © 1999-2020 CyberArk Software Ltd. All rights reserved.. This document contains information and ideas, which are proprietary to CyberArk Software Ltd. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, without the prior written permission of CyberArk Software Ltd. DNA 8.3Table of Contents CyberArk DNA™ 5 Considerations 6 Privileged Access Security Status 7 Hard-coded and Embedded Application Credentials 7 Credential Theft 8 Cloud Users and Instance Keys 8 Database Accounts 8 Privilege Escalation 9 Granular, Flexible, Easy to Use 9 Reporting and Visualizing Threats 9 Agentless and Light 11 Install DNA 12 System Requirements 13 General Requirements 13 Windows Requirements 14 Unix/Linux Requirements 18 Installation 22 Use DNA 23 Run DNA 24 Understand the DNA User Interface 26 The DNA user interface 26 The DNA Workflow 27 Perform a Scan 28 Select Sources for Discovery 28 Set up a DNA Scan 29 Run a Scan 36 View the Scan Results 39 Upload Accounts 41 Use DNA Reports 45 Understand DNA Reports 46 Executive Summary Dashboard 46 What are SSH Keys? 55 What is Pass-the-Hash? 56 What is Insecure Privilege Escalation? 57 Windows and Unix Scans 58 Domain Scan 67 SSH Key Trusts 70 Database Scan 77 Hard-Coded Credentials 79 Cloud Users 81 Cloud Instances 82 Scan Errors 82 The Organizational Pass-the-Hash Vulnerability Map 83 2 Table of Contents CyberArk Discovery and Audit (DNA)CyberArk Discovery and Audit (DNA) Table of Contents 3 Display the Map 83 Understand the Map 84 Select the Machines to Display 86 Focus on a Specific Machine 86 The SSH Keys Trusts Map 89 Display the Map 89 Understand the Map 90 Select the Machines to Display 92 Focus on a Specific Machine 93 Use DNA Reports to Expose Security Threats 94 Account Scan 94 Embedded and Hard-Coded Credentials Scan 97 SSH Keys Scan 99 Pass-the-Hash Vulnerabilities Scan 101 Sharing DNA Report Data with CyberArk 105 Share the Automatically Generated Obfuscated Report Data 105 Run the DNA Obfuscation Tool Manually 105 Logging 106 Troubleshooting 107 Scanning Issues 108 General scanning errors and issues are displayed 108 The scan failed on Windows machines 109 The scan failed on Unix/Linux machines 109 The scan runs for a prolonged time 110 The user running the scan doesn’t have required authorization 111 The scan cannot detect the OS version 111 DNA could not finish a scan 112 DNA discovered an SSH key from a machine that was not scanned 113 DNA cannot resolve the IP of a machine listed in the imported file 113 DNA cannot start scanning 114 DNA cannot detect a connection using an SSH key 114 DNA failed to discover MS SQL instances 114 Imported File Issues 115 DNA cannot read a target machine name 115 DNA doesn’t scan all the listed machines 115 DNA cannot retrieve information from the Active Directory 116 Delimiter characters are included in passwords 116 Report Issues and Messages 118 DNA cannot scan the password age 118 DNA cannot scan the DNA machine 118 DNA cannot read the Excel file 118 DNA cannot resolve group members 118 DNA cannot resolve the domain group 119 DNA cannot detect the OS version 119 DNA cannot resolve the IP address of the machine to scan 119 Log Error Messages 120 DNA cannot start scanning 120 DNA cannot authenticate to the machine to scan 120 DNA cannot access the Database 121 Appendices 122Configuration Parameters 123 DNA Configuration 123 Unix/Linux-Specific Configuration 132 Configure Root Permissions Using the Sudoers File 133 Configure AWS Scan Policies 134 Configure Audit Policy 136 Import a File 137 File Format 137 Scan Unix/Linux machines using a Password or an SSH Key 138 Known Behavior and Limitations 141 Known Behaviors 141 Scan Limitations 141 Report Limitations 143 Pass-the-Hash Limitations 143 Hard-Coded Credentials Scanning Limitations 144 File Import Limitations 144 SSH Key Scanning Limitations 144 SSH Key Compliance Criteria 146 Embedded and Hard-Coded Credentials 147 Discover Public SSH Keys 150 Ports used by DNA 151 Configure Logging for ‘Key Last Used’ Data 152 4 Table of Contents CyberArk Discovery and Audit (DNA)5 CyberArk Discovery and Audit (DNA) CyberArk DNA™ The IT security landscape keeps changing and, thus, the tools and techniques that are used to defend organizations must also change to compensate and adapt to these changes. No longer can organizations exclusively rely on preventive security technologies, such as firewalls, anti-virus, and standard configurations of user authentication systems. Now organizations need more agile tools to sufficiently protect them from today’s most sophisticated attacks and operate with modern operation tools (DevOps tools). The reality is that focused, well-funded, and expert attackers can circumvent all of the commonly used preventive security systems. Privileged accounts are built-in vulnerabilities throughout your infrastructure and are what most attackers look for. Unprotected, unmonitored privileged accounts are the weapon of choice for most of attackers. To compensate for this general weakness, organizations must enhance their detection, investigative, and response capabilities. CyberArk Discovery and Audit™ (DNA) is an innovative discovery and audit tool that automatically scans an organization’s network, typically a complex, manual process, for the following: ■ Data related to privileged and non-privileged accounts ■ Hard-coded and embedded application credentials on workstations, servers, MSSQL databases, and DevOps ■ Potential credential theft risks, including Golden Ticket, Pass-the-Hash, Pass-theTicket and Overpass-the-Hash attacks ■ SSH key exposure ■ Privilege escalation risksThe easy-to-use scanner automatically discovers and analyzes any privileged and nonprivileged account within servers and desktops as defined by the user, then generates a report and visual organizational map that evaluates the privileged account security status in the organization. A simple three-step procedure leads to better and more efficient risk management around privileged accounts. In this section: Considerations Privileged Access Security Status Hard-coded and Embedded Application Credentials Credential Theft Cloud Users and Instance Keys Database Accounts Privilege Escalation Granular, Flexible, Easy to Use Reporting and Visualizing Threats Agentless and Light Considerations In order to provide accurate and meaningful results for the security team, the DNA tool uses powerful methods or technologies that mimic those used by attackers. Before running DNA, it is strongly recommended that deploying organizations assess the related legal requirements both under data protection and telecommunication laws as well as any other applicable laws and regulations on their own behalf. We recommend that IT security personnel verify that corporate employment policies or local laws do not prohibit the scanning or analysis of data streams for network security purposes, because the tool involves scanning, locating and analyzing corporate access credentials. CyberArk’s DNA scanner is a certificate-signed tool that does not require agents to be installed on target systems, making it non-intrusive to the IT environment. However, these network activities may trigger alerts in security applications and tools designed to detect anomalous network traffic, so Security Operations Teams may need to be alerted in advance so that the security work is coordinated and does not disrupt or distract from ordinary security monitoring or management of alerts. CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 6Privileged Access Security Status DNA enables an organization to scan its network on local machines, on the cloud (Amazon Web Services, Azure, etc.), and in DevOps tools (Ansible), and retrieve a list of all accounts that have access to its machines and places where privileged accounts are used, such as in accounts embedded in Windows Services, Scheduled Tasks, IIS Application Pools, and more. It scans all local and domain accounts that have permission to logon to endpoints with a password or using SSH Keys, whether on Windows or Unix/Linux devices. Together with basic password-based authenticated users that are detected, DNA identifies private and public SSH keys on Unix and Windows machines in your environment and ascertains the status of each key. DNA distinguishes between the private SSH key and the public SSH key, correlates the potential risk of possible connections and produces a visual organizational map of machines that can be accessed using the detected SSH keys.

In addition to regular service accounts in Windows, there are services that authenticate using Kerberos and are registered in the Active Directory Domain. These accounts have an additional attribute called Service Principal Name (SPN), requesting a SPN domain ticket could allow an attacker to efficiently escalate privileges by creating Silver Tickets or simply impersonate the service account by logging in with the appropriate credentials. CyberArk DNA can discover all defined Domain Service Accounts according to their Service Principal Name (SPN) attribute. In Ansible playbooks, DNA identifies the hard-coded user and password keywords that are saved as task parameters, variables and environment variables, and sends alerts about them as these credentials might have the potential to take down an entire Data Center if they fall into the wrong hands Hard-coded and Embedded Application Credentials DNA enables organizations to find embedded and hard-coded credentials, and assess the extent to which these passwords can be accessed by unauthorized users on the following platforms: ■ WebSphere servers (on Unix/Linux) ■ WebLogic servers (on Unix/Linux) ■ IIS servers ■ Ansible playbooks A clearly organized report lists the discovered embedded credentials and hard-coded credentials to aid in understanding the current risk and threat caused to servers, applications, and target systems to which the applications connect (e.g. databases). CyberArk Discovery and Audit (DNA) Privileged Access Security Status 7Credential Theft DNA assesses the current and potential risk of Golden Ticket, Pass-the-Hash, Pass-theTicket and Overpass-the-Hash attacks, a form of credential theft. DNA identifies stored hashes of privileged domain accounts on machines, producing a visual map of machines that are vulnerable to the above mentioned attacks. Cloud Users and Instance Keys DNA enables organizations to find IAM users, access keys and SSH key pairs, and asses the risk of leaving them unmanaged and unmonitored. DNA currently supports Amazon Web Services (AWS) platform using the AWS API. DNA can also integrate with Amazon AWS Inspector to show the number of high severity findings on EC2 instances. AWS recommend to treat these security issue as an emergency and implement an immediate remediation as these high severity findings describe security issues that can result in a compromise of the information confidentiality, integrity, and availability within your assessment target. Database Accounts DNA scans MSSQL databases to discover all privileged or non-privileged users on SQL or Windows/Active Directory. Note: DNA can scan databases on MSSQL 2012 and 2016, but does not scan SQL databases on clusters. On any target machine, the DNA may discover multiple MSSQL instances, each used in several databases and each with its own users (database-level object). An account may be either an SQL login account or a Windows login account, and each may have one or more users even though each user can only access one database. The results of the database accounts scan are only displayed in the Database Scan sheet, and are not represented in the Executive Summary. CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 8Privilege Escalation DNA discovers and flags potential excessive privileges that have been escalated on Unix and Linux. The assignment of account privileges can be error-prone on Unix and Linux machines, where the root account is the only privileged account by default, and escalating account privileges is typically and commonly done using an un-centralized sudoers configuration file. Since the sudoers configuration file was not designed for cyber-security, the process of escalating account privileges may result in excessive privileges for accounts. DNA detects these excessive privileges and exposes the risk. Granular, Flexible, Easy to Use Users can select organizational units (OUs) in the Active Directory or import a list of target machines to scan. For Windows systems, users can determine whether DNA will scan only workstations, only servers, or both workstations and servers contained in the OU. On Unix and Mac devices, DNA will always scan both workstations and servers. Reporting and Visualizing Threats The resulting Discovery and Audit report is a comprehensive Excel file that provides an Executive Summary Dashboard as well as detailed information about the current status of each privileged account in your organization, and extensive machine and account information for potential attack vectors pertaining to various Credential Theft attacks (Golden Ticket, Pass-the-Hash, Pass-the-Ticket and Overpass-the-Hash) and SSH key exposure. The report reveals privileged account security issues, highlights non-compliance of passwords and SSH Keys, vulnerabilities to Credential Theft attacks (Golden Ticket, Pass-the-Hash, Pass-the-Ticket and Overpass-the-Hash) and Insecure Privilege Escalations. The report shows how privileged accounts (those using passwords or SSH Keys) are managed, thus enabling your organization to better manage, secure and automate its privileged account processes. The report displays the following sheets: ■ Windows Sheet – A list of accounts on Windows and Unix machines (when an Active Directory bridge solution is used) throughout your organization, including detailed information about accounts that can be accessed using SSH Keys, as well as information about each SSH Key, and accounts that are vulnerable to Credential Theft attacks (Golden Ticket, Pass-the-Hash, Pass-the-Ticket and Overpass-theHash). The list also includes Service Accounts (embedded Windows credentials) that are being used by certain services to carry out their functions. For example, Windows Services, Scheduled Tasks, IIS Application Pool, IIS Anonymous Authentication, etc. ■ Unix Sheet – A list of accounts on Unix/Linux machines throughout your organization, including detailed information about accounts that can be accessed using SSH Keys, as well as information about each SSH Key. CyberArk Discovery and Audit (DNA) Privilege Escalation 9■ Domain Scan Sheet – A list of domain accounts that have the SPN attribute set, including detailed information about the accounts and their SPN Service name as well as the SPN itself. ■ SSH Key Trusts – The organizational status of all SSH keys, the trusts found between Unix and Windows accounts and machines, their potential exposure, as well as their compliancy status. ■ Hard-Coded Credentials – A list of hard-coded credentials found in applications running on WebSphere, WebLogic, IIS servers, and DevOps tools playbooks (for Ansible) throughout your organization, including detailed information about where the password was discovered and which target system it is used for (e.g. database). ■ Cloud Users - A list of all IAM users and Access Keys found on AWS, including detailed information about their privileged policies and compliance which can indicate highly privileged users. ■ Cloud Instances - A list of all EC2 instances in the selected region (or all regions) and their relevant key pairs.

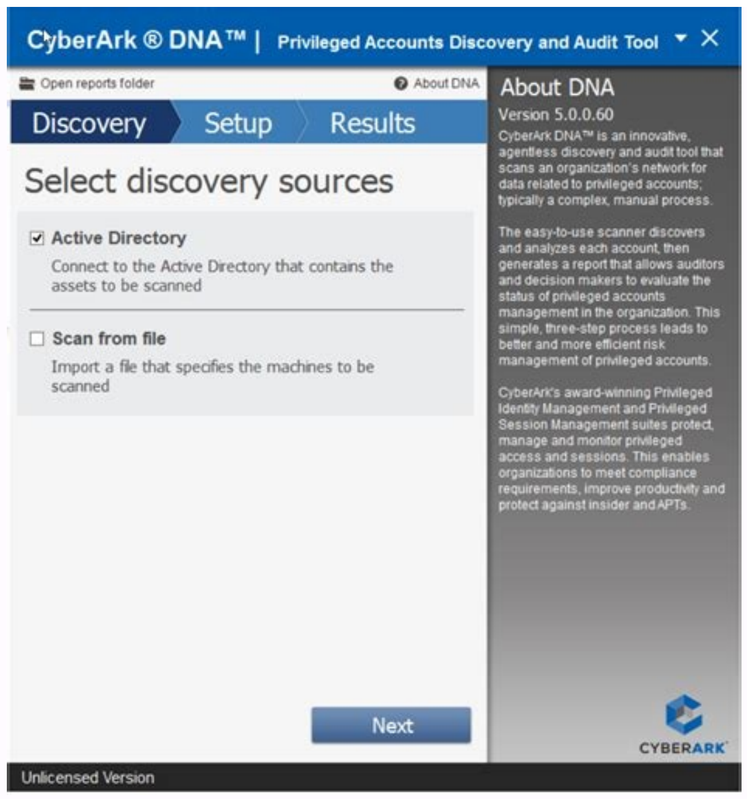


This information can help an organization perform a DNA scan on their cloud assets and enumerate all their EC2 instances information. ■ What is Insecure Priv. Esc. - An explanation about insecure privileged escalation and how it affects the organization. ■ What are SSH Keys – A summary of how SSH Keys are used, what their risks are, and how DNA helps you assess the current and potential risk of SSH key exposure in your organization. ■ What is Pass-the-Hash – An explanation about how Pass-the-Hash attacks work and how DNA helps you to assess the current and potential risk of Pass-the-Hash attacks in your organization. In addition, visual maps of all the machines in your organization display the following: ■ SSH Keys: Organizational SSH Trust Map – This map displays the possible SSH key trusts between Unix and Windows accounts and machines in your organization. It distinguishes between the “client side” (private SSH key) and the target system (public SSH key), resulting in relationships between accounts and machines that are based on potential access. This map makes it easy and quick to understand on which machines SSH keys have been used throughout the years, and exactly which SSH Key trusts can be used to connect from one machine to another. ■ Pass-the-Hash: Organization Vulnerability Map – This map displays the machines in your organization that are vulnerable to Golden Ticket1 and Pass-theHash and attacks, as well as the machines that are at fault and threaten the organization. This map makes it easy and quick to understand how an attacker can leverage these vulnerabilities in your organization. You can use these maps to focus on the machines and accounts that require immediate attention to help mitigate the threat quickly. 1The Golden Ticket vulnerability is only shown in the Pass-the-Hash map if there is indication of a potential attack. CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 10Agentless and Light CyberArk’s DNA scanner is a certificate-signed tool that does not require agents to be installed on target systems, making it non-intrusive to the IT environment.

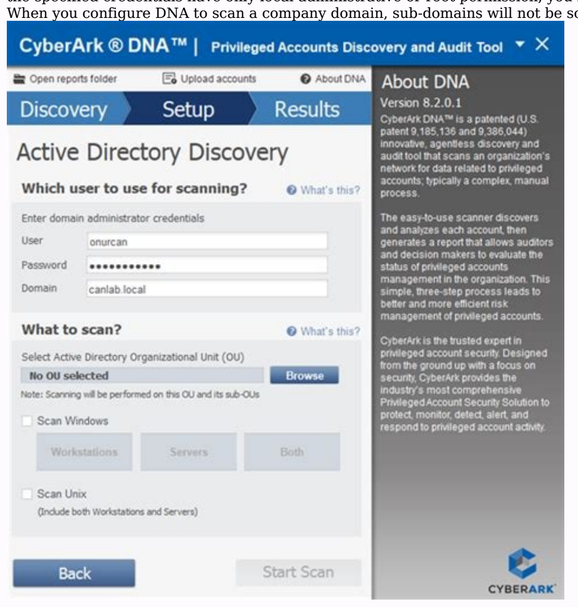


Target device properties are scanned in read-only mode1 . Please see the FAQ for a detailed explanation regarding DNA’s performance and network bandwidth usage. 1Target device properties are scanned in read-only mode, except when scanning for SSH keys on Windows without Cygwin. CyberArk Discovery and Audit (DNA) Agentless and Light 1112 CyberArk Discovery and Audit (DNA) Install DNA This chapter describes how to install DNA. In this section: System Requirements InstallationSystem Requirements General Requirements This section describes the minimum requirements for running CyberArk DNA. Operating System Windows 8/8.1 Windows 10 Windows Server 2012 Windows Server 2016 Windows Server 2019 Disk space At least 1GB of free disk space License DNA requires a license. The DNA license includes an expiration date, and limits the number of Windows machines and the number of Linux/Unix machines that can be scanned per scan, both when scanning from an Active Directory and from an imported file. This version of DNA is backwards compatible to support older license versions. Supported Active Directory DNA can perform scans on the following Active Directories: Microsoft Active Directory 2012, 2016, 2019 Note: DNA does not support scanning Active Directory domain controllers. Supported SSH Keys DNA can discover the following types of SSH keys: OpenSSH private keys up to 20 kilobytes Private PuTTY Supported SSH Servers OpenSSH Server 6.7 and lower On OpenSSH Server 6.2-6.7, DNA cannot discover the time when an SSH key was last used. For information about configuring the server to log this data, refer to Configure Logging for ‘Key Last Used’ Data, page 152. CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 13DNA discovers private and public SSH keys on all OpenSSH servers using SSH2 protocol. SunSSH v2.2 and below Microsoft Office Application Reports generated by DNA can be viewed in the following Microsoft Office applications: Microsoft Excel 2010, 2013, 2016 Note: DNA is not compatible with Microsoft Office 2007. .NET Framework Make sure that .NET Framework is installed. Windows Requirements The section describes the minimum operating system requirements for scanning Windows machines with DNA. Credentials for scanning Domain Administrator Equivalent Domain User: User with read permissions on the Active Directory User with local administrative rights for Windows Note: A user who is not a domain Administrator must be a domain user and must belong to the Administrators group or to a group nested within the Administrators group. Supported target machines Machine Windows Version Workstations Windows 8 Windows 10 Servers Windows Server 2012 Windows Server 2016 Windows Server 2019 Supported protocols The following protocols are supported when accessing the Active Directory: CyberArk Discovery and Audit (DNA) System Requirements 14 2013 runtime library needs to be installed on the target machines Prerequisites To enable DNA to discover all the private SSH keys on the machines to scan, the user who will perform the scan must have access to all these keys. Note: By default, DNA doesn't scan single core machines for private SSH keys. This can be CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 15changed by setting the SSH Keys scan parameters in the DNA.exe.config file. For more information, refer to Configuration Parameters, page 123. Scanning for cloud users and instances Supported Platforms AWS AWS Inspector Prerequisites Make sure that the machine where DNA runs can access the AWS console via API. Supported target windows machines and Cygwin versions Cygwin 1.7.32 and above Supported target Windows machines where Cygwin is installed: Windows Server 2012 P rerequisi tes Make sure that OpenSSH is installed within Cygwin. To discover public SSH Keys on Windows, make sure that Cygwin is installed in your environment. To scan a Windows machine that has Cygwin installed, the following packages and commands must be installed in Cygwin: Packages: openssh-server – This package must be installed. openssh – This package must be installed. sshd daemon – This package must be started and configured. SSH connection – DNA requires an SSH connection to scan machines for SSH Keys. Commands: ssh-keygen – DNA uses the ssh-keygen command. Note: ■ To make sure the SSH Server is running and available, run the "ssh localhost" command. At the prompt, specify your password. If a new command line is now displayed, your SSH server is listening on the standard SSH port. ■ The SSH Server must support password, SSH key, or keyboard interactive authentication, which can be configured in the /etc/ssh/sshd_config file.
For more information, refer to Log Error Messages, page 120, in Troubleshooting. ■ By default, machines with a single core CPU will not be scanned for private SSH keys. This can be changed by configuration parameters in the DNA.exe.config file. For more information, refer to Configuration Parameters, page 123. CyberArk Discovery and Audit (DNA) System Requirements 16Additional requirements on target machines Configure the Audit Policy in the Local Security Policy or Group Policy to audit the following types of events: Audit logon events Audit system events For information about how to configure the Audit Policy, see Configure Audit Policy, page 136.
CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 17Unix/Linux Requirements This section describes the minimum requirements for scanning a Unix/Linux environment with DNA. Credentials for Scanning To scan Unix/Linux/MacOS machines, the following credentials are required: Note: These credentials are not relevant to IBM Virtual I/O Server or IBM Hardware Management Console platforms. For information about credentials that are required to scan these machines, refer to the relevant information at the end of the Unix/Linux Requirements section. Type of user Required Credentials User with root permissions for Unix/Linux/Mac It is possible to configure DNA to scan with users who authenticate with a password, as well as SSH Keys Connected via an Active Directory bridge, using the Active Directory as a source. ■ Domain Administrator with root permissions on Unix/Linux/Mac machines or, ■ Equivalent Domain User: ■ User with read permissions on the Active Directory ■ User with root permissions for Unix/Linux Note: To scan using the Active Directory as a source, your organization must use an Active Directory bridge solution.
For example: ■ Centrify DirectControl (DNA does not scan for SSH keys when using AD Bridge on Centrify) Users other than root DNA requires the use of sudo to run commands. Hence, the administrative user account(s) configured to scan with DNA must have permissions to run sudo on the scanned Unix/Linux/Mac machines. For more information, see Configure Root Permissions Using the Sudoers File, page 133. To scan other Unix/Linux machines: Platform Required Credentials ESX machine root user IBM VIOS machines A user with vios.oemsetupenv authorization is required. This authorization allows the user to elevate the shell to CyberArk Discovery and Audit (DNA) System Requirements 18Platform Required Credentials unrestricted shell mode by executing the "oem_setup_env" command. IBM HMC machines An hscroot user or any user with the hmcsuperadmin task role. Supported Unix/Linux Platforms ■ Workstations and servers: ■ RHEL 4-7.1 ■ Solaris Intel and Solaris SPARC 9, 10, 11 – For known limitations, refer to Known Behavior and Limitations, page 141. ■ SUSE 10 ■ Fedora 18, 19, 20 ■ Oracle Linux 5 ■ CentOS 6 ■ AIX 5.3, 6.1, 7.1 ■ ESXi 5.0 and 5.1 ■ IBM Virtual I/O Server 2.2.x ■ IBM Hardware Management Console 7Rx.x and 8Rx.x ■ MacOS Mavericks, Sierra, High Sierra Note: By default, machines with a single core CPU that run Unix/Linux versions will not be scanned for private SSH keys. This can be changed by configuration parameters in the DNA.exe.config file. For more information, refer to Configuration Parameters, page 123. Supported Java Application Servers Note: On Java application servers, DNA only discovers JDBC datasources ■ WebSphere 6.1 and higher (Linux, Solaris, AIX) ■ WebLogic 9.x and higher (Linux, Solaris, AIX) Note: On WebLogic, DNA only discovers WAR applications CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 19Supported DevOps Platforms Ansible version 2.3 and higher on RHEL 4-7.1 Supported Key Exchange Algorithms diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Package Prerequisites To be able to scan a Unix/Linux environment with DNA, the following packages or commands must be installed: Package or Command Details SSH The openssh-server and openssh packages must be installed, and the sshd daemon must be started and configured. DNA will not be able to scan the machine without an SSH connection. DNA uses the following commands: ssh-keygen sudo The sudo package must be installed and configured to enable DNA to perform scan and retrieve account details. Note: ■ This is only a prerequisite when scanning as a user other than “root”.
■ DNA supports the following sudoreplacement solutions: ■ CA Privileged Identity Manager/ControlMinder ■ Centrify Access Manager/DirectAudit For more information, refer to Unix/Linux Requirements, page 18 lastlog command This command retrieves the last login date of an account. Note: The command is not required on AIX systems and Solaris Note: ■ To find out if a specific command is installed, run the "which" command. For example, if sudo is installed, the "which sudo" command will return the full path of the sudo command. If sudo is not installed, the “which” command will CyberArk Discovery and Audit (DNA) System Requirements 20return: no sudo in /usr/bin /etc /usr/sbin /usr/ucb /usr/bin/. ■ To make sure the SSH Server is running and available, run the "ssh localhost" command. At the prompt, specify your password. If a new command line is now displayed, your SSH server is listening on the standard SSH port. ■ The SSH Server must support password, SSH Key, or keyboard interactive authentication, which can be configured in the /etc/ssh/sshd_config file. For more information, refer to Log Error Messages, page 120, in Troubleshooting. CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 21Sudo Replacements DNA supports the following sudo-replacement solutions: ■ CA Privileged Identity Manager/ControlMinder – This solution contains the sesudo command. ■ Centrify Access Manager/DirectAudit - This solution contains the dzdo command.
AD-Bridge support DNA supports the following AD-Bridge solutions: ■ Centrify Access Manager/AD Bridge ■ Quest (OneIdentity) vastool Installation DNA installation 1. From the DNA installation package that you will receive from your CyberArk representative, copy the CyberArk DNA zip file to the machine you want to scan from.

2. Extract the contents of the zip file to any directory on your local hard drive. Note: Make sure you have full read and write permission for the chosen directory 3. Optionally configure the DNA.exe.config configuration file. This file includes the configuration that DNA will use during scanning. For example, you can configure whether or not DNA will scan for Golden Ticket and Pass-the-Hash vulnerabilities, scheduled tasks, and Windows services, and how it will treat non-compliance with the password policy in your organization.
For more information about the configuration parameters, refer to Configuration Parameters, page 123. CyberArk Discovery and Audit (DNA) Installation 2223 CyberArk Discovery and Audit (DNA) Use DNA DNA automatically scans your organization’s network, discovers and analyzes privileged and non-privileged accounts, accounts that use passwords and accounts that use SSH Keys, and also discovers potential Credential Theft attacks (Golden Ticket, Pass-theHash, Pass-the-Ticket and Overpass-the-Hash). This chapter explains how to run DNA, work with its interface, setup and perform a scan, and view the scan results.
In this section: Run DNA Understand the DNA User Interface Perform a Scan View the Scan Results Upload AccountsRun DNA Note: Running DNA might trigger SIEM system alerts due to the way it scans your network. Run DNA for the first time 1. In the CyberArk DNA executable folder, double-click DNA.exe. 2. The first time that DNA is run, the CyberArk DNA Software License Agreement window appears. 3. Read the license agreement and select the checkbox to accept its terms, then click OK; the CyberArk DNA window appears with the License Required pop-up on top. At the bottom left of the CyberArk DNA window, Unlicensed Version is displayed. CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 24To be able to use DNA, you need a license. The DNA license includes an expiration date and limits the number of Windows machines and the number of Unix/Linux machines that can be scanned per scan, both when scanning from an Active Directory and from an imported file. 4.



In the License Required pop-up, click Browse and find the DNALicense.xml file, then choose the file. Note that at the bottom left of the CyberArk DNA window, Unlicensed Version has been replaced by information about the license, the licensee and the remaining number of days until the license expires. CyberArk Discovery and Audit (DNA) Run DNA 25Understand the DNA User Interface The DNA user interface The CyberArk DNA enables you to specify the sources that DNA will use to perform discovery, setup a scan, run it, and view the results. Each CyberArk DNA window contains the following: Workflow steps (e.g., select the discovery source, setup, etc.) Options bar – Includes the following options: Open reports folder – Enables you to access all reports.
Upload accounts – Enables you to upload discovered accounts from a DNA DB file to the CyberArk PAS Pending Accounts. About DNA – Displays information about CyberArk DNA in the Help area. Context-sensitive Help Area – Click "What's this?" to display help about each section. CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 26The DNA Workflow The DNA workflow includes the following steps: Step Description Discovery Determine the sources that DNA will use to perform discovery. DNA can be configured to scan the assets contained in a specified Active Directory, or the machines listed in a specific file, or both. Setup Configure the basic setup of the scan, depending on the sources you selected in the Discovery step. Once you have provided this information, you can start scanning. Scan View live data about the scan in progress. When scanning is complete, you can view statistical information about the scan and access the scan report. CyberArk Discovery and Audit (DNA) Understand the DNA User Interface 27Perform a Scan You can perform a privileged account scan using the following three-step procedure, explained in the sections below: Select Sources for Discovery In the Discovery window, select the sources that DNA will use to perform discovery. Select sources 1.
Select one or all of the following options: Source Description Active Directory DNA will scan the assets contained in the Active Directory that you specify in the Setup window. AWS Discovery Connect to Amazon Web Services to discover cloud assets, such as IAM users, Access keys and EC2 instances and EC2 key pairs (in the selected region). IP Import a file of machines or define a range of IP addresses to scan. CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 28Source Description Address DNA will scan all detected machines listed in the file or that are active in the IP network range from the Setup window. 2. Click Next; the Setup window appears.
Set up a DNA Scan The option you choose in the Discovery page determines what is displayed in the Setup page.
If you selected multiple options in the Discovery window, the setup pages are displayed according to the list order. Set up DNA to Scan from an Active Directory The Active Directory Discovery page enables you to set up DNA to scan from an Active Directory. Scan from an Active Directory 1. In the Which user to use for scanning? section, specify the credentials the scanner will use to access the Active Directory and to perform the scan. CyberArk Discovery and Audit (DNA) Perform a Scan 29Type the user credentials in the relevant fields. Note: ■ DNA uses these credentials to connect to the Active Directory's Organizational Unit (OU) and the target machines. ■ To connect to the OU, read permission is required. ■ To scan both Windows and Unix/Linux/Mac machines via an Active Directory Bridge solution, the credentials must have both of the following permissions: ■ Local administrative permission for Windows ■ Root permission for Unix/Linux machines. This permission is typically configured in the sudoers configuration file. ■ If the specified credentials have only local administrative or root permission, you must scan Windows and Unix/Linux/Mac devices in two separate scans, using the relevant credentials for each operating system. For more information, see Run a Scan, page 36. ■ You must specify the domain name in the fully-qualified domain name (FQDN) format. ■ When you configure DNA to scan a company domain, sub-domains will not be scanned. For example, when you scan the mycompany.com domain, the sub.mycompany.com domain will not be scanned. 2. In the What to scan? Section, specify the target machines to scan for privileged accounts. a.



Select the Active Directory's Organizational Unit (OU) to scan. Use Browse to find the relevant OU and select it, then click OK; the scanner will scan the CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 30selected OU and all of its sub-OUs. b. Check the following options: Scan Windows – Check this option to scan Windows machines, then select the items to scan by clicking the relevant button: Workstations, Servers (default), or Both. By default, DNA automatically scans the selected Windows machines for risks of Golden Ticket and Pass-the-Hash attacks. This can be configured in the DNA configuration file.
By default, any MSSQL server found during the Windows scan is scanned for Database users. This can be configured in the DNA configuration file. For more information, refer to DNA Configuration, page 123.
Scan Unix – Check this option to scan Unix/Linux machines. Note: On Unix/Linux devices, DNA will always scan both workstations and servers MacOS scan is included in the Unix scan. By default, DNA automatically scans the selected Unix/Linux machines for SSH keys exposure. This can be configured in the DNA configuration file. For more information, refer to DNA Configuration, page 123. 3. If you configured DNA to scan from a file/IP range or AWS, as well as from the Active Directory, click Next to proceed to the Setup scanning from a file/IP range CyberArk Discovery and Audit (DNA) Perform a Scan 31or AWS window. Otherwise, click Start Scan. CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 32Set up DNA to Scan from AWS The AWS Discovery page enables you to set up DNA to scan from an AWS platform. Scan from AWS 1. In the Access Key to use for scanning section, specify the access ID and access secret that the scanner will use to access AWS and perform the scan. Type the access ID and secret in the relevant fields. Note: DNA uses these credentials to connect to the AWS console using the AWS API. To run an AWS scan, the user related to the access key provided needs the open read policy. For more specific permissions please refer to the technicalFAQguide. 2. In the What to scan? section, check the following options: IAM users and access keys - Check this option to detail AWS IAM users and their access keys E2 instances and key pairs: CyberArk Discovery and Audit (DNA) Perform a Scan 33Select the required region to scan.
By default, all regions are scanned.
AWS has a limitation when scanning certain regions, such as AWS GovCloud (US) or China (Beijing). Check this option to enumerate the EC2 instances and EC2 key pairs in the selected region.
AWS Inspector security findings: Check this option to list AWS Inspector information on the selected region for all EC2 instances that have the Inspector agent installed. Selecting this option will sum all high severity security finding in the scanned EC2 instances. 3. If you configured DNA to scan from a file as well as from AWS, click Next to proceed to the Setup scanning from a file window.
Otherwise, click Start Scan. Set up DNA to Scan IP addresses Note: ■ When scanning from a file, make sure that none of the passwords in the imported file contain the file delimiter character, since this might cause the account to be locked out. By default, the delimiter character is a comma ",". For more information, refer to Imported File Issues, page 115, in Troubleshooting. ■ To accurately identify machines as "Workstation" or "Server", make sure that the user who will perform the scan is a Domain user. For more information, refer to Scan Limitations, page 141. The Setup scan from IP page enables you to setup DNA to: ■ Scan machines that are not connected to an Active Directory ■ Scan an entire network range ■ Scan a specific list of machines ■ Scan machines by authenticating to them using an SSH Key. For more information, refer to Import a File, page 137. Note: DNA cannot authenticate to Windows machines with Cygwin using SSH Keys CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 34If you specify that DNA will scan from an Active Directory as well as from a file, some machines may be duplicated.
In this case, DNA will omit the duplicates. Click Back to return to the Setup scanning from the Active Directory window. Import machines from file 1. Select Import machines from file, then click Browse, and select the file that specifies the machines to scan; the number of imported machines is displayed below the field. 2. To download a CSV template that you can use to create your CSV file, click Click to download CSV template. CyberArk Discovery and Audit (DNA) Perform a Scan 35For more information about importing a file, refer to Import a File, page 137. 3. Click Start Scan. Import machines from IP range 1. Select Import machines from IP range. 2.
Specify the IP range from which DNA will scan and the IP range to which DNA will scan. Make sure that each number is between 0 and 255. The number of machines to scan is displayed. 3. Specify the name and credentials of the user who will run the DNA scan.
4. To specify additional user credentials to access and scan Unix machines, select Specify different user credentials for Unix machines and type the user's name and credentials. 5. Click Start Scan Run a Scan Once you have provided the information required in the Discovery and Setup windows, you can start scanning. If the credentials you specified above have both local administrative and root permissions, you can scan both Windows and Unix/Linux devices in a single scan.
If the specified credentials have only local administrative or root permission, you must scan Windows and Unix/Linux devices in two separate scans, using the relevant credentials for each operating system.
AWS results are only relevant if you selected the AWS scan and entered the AWS access key credentials. Database scanning results will be available if the supplied credentials have the appropriate permissions on the MS SQL servers. Start the scan To run the DNA scan, click Start Scanning; the Scan window appears. CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 36Stop the Scan To stop the scan before it is complete, click Stop. During scanning, the following live data is displayed: Total Machines Scanned - The current number of Windows and Unix/Linux machines scanned. The Progress bar displays the current percentage of scans completed. When the application is minimized, the scanning progress is indicated in the taskbar. Windows and Unix/Linux Scan Results Machines Found – The total number of Windows and Unix/Linux machines found in the organization. Scanned successfully - The total number of Windows or Unix/Linux machines scanned successfully, along with the current percentage of Windows or Unix/Linux machines scanned.Scanned successfully - The total number of Windows or Unix/Linux machines scanned successfully, along with the current percentage of Windows or Unix/Linux machines scanned. Statistics - Below this information, the following statistics display: Failed partially – The current percentage of Windows or Unix/Linux machines for which at least one but not all types of scans failed due to errors. Failed – The current percentage of Windows or Unix/Linux machines for CyberArk Discovery and Audit (DNA) Perform a Scan 37which all scans failed due to errors. Errors can occur for a variety of reasons, for example because a machine is offline and not available for scanning, or because of insufficient permissions. For information about specific errors, see the Details section in the report. See also the Troubleshooting section. Accounts Found – The total unique number of Windows and Unix/Linux accounts found in the organization. Non-Compliant - The total unique number and percentage of non-compliant Windows or Unix/Linux accounts identified in the scan. An account is considered non-compliant if its password was not changed for a period greater than the threshold value defined in the DNA configuration file. Note: Only enabled accounts (as opposed to disabled or "locked-out" accounts) can have a non-compliant status. When running an AWS scan, the following AWS Scan Results information is added: AWS EC2 instances - The total number of EC2 instances found in the selected region. AWS EC2 Key pairs - The total number of EC2 Key Pairs found on the discovered EC2 instances. AWS IAM Users - The total number of IAM users found in the AWS console. AWS IAM Access Keys - The total number of access keys found on each discovered IAM user. If only the AWS scan is selected, this information will appear on its own. However, if the AWS scan is selected together with other scans, this information will appear alongside all the information from the other scans. CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 38View the Scan Results When the scan is complete (or if you pressed the Stop button), the Results window appears.
This window displays the final scanning data. For more information about the displayed scanning data, see Run a Scan, page 36. You can now open the Discovery and Audit Report, or start a new scan. ■ To access the reports and maps, click Open Report. ■ To start a new scan, click New Scan; the Setup window appears; the same user credentials and OU or region that were used in the previous scan will be used and will appear in the relevant fields. CyberArk DNA will generate a new report name with the current date and time in the Report name field.
To start the scan, click Start Scanning. ■ To upload discovered accounts, click Upload Accounts at the top of the DNA window. For further information, refer to Upload Accounts, page 41. ■ After running a scan using an import file, a warning message recommends that you delete the imported file as it contains credentials in it. CyberArk Discovery and Audit (DNA) View the Scan Results 39CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 40Upload Accounts After DNA discovers accounts in your enterprise, you can initiate an onboarding process to upload accounts listed in the DNA DB file to the Pending Accounts page in the PVWA. Upload accounts 1. In the DNA window, click Upload accounts. The Upload accounts window appears. 2. When you initiate this at the end of a scan, the Import DNA data file will be filled with the relevant data file of the scan that just ended. If this is initiated at a different time (not immediately after a scan), under Import DNA data file, click Browse to select the DNA DB file reports that include the accounts to onboard to the Pending Accounts. 3. Under PVWA connection details, specify the Vault user who will run this process, their Vault password, and the URL of the PVWA to which the accounts will be uploaded (for example: . CyberArk Discovery and Audit (DNA) Upload Accounts 41Note: This process only uploads accounts that do not have dependencies. 4. Under Select the accounts to upload, select the type of accounts in the DNA report that will be uploaded. 5. Click Upload; the DNA uploads the relevant accounts to the Pending Accounts page in the PVWA. CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 426. If any errors occurred during the upload, after the upload is finished, a link to an error log is displayed so that you can view all the errors that happened during the process. 7.
To provision these accounts in the Vault, log onto the PVWA. For more information, refer to Pending Accounts in the Privileged Access Security Implementation Guide. Note: If Automatic Onboarding Rules have been created, they will be CyberArk Discovery and Audit (DNA) Upload Accounts 43applied to the uploaded accounts. This is relevant to version v10.2 and above. CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 4445 CyberArk Discovery and Audit (DNA) Use DNA Reports DNA scans your organization's network, then generates a report and visual organizational maps that evaluate the privileged account security status in your organization. This chapter describes the DNA report, the organizational Pass-the-Hash Vulnerability map, the organizational SSH Keys Trusts map, and explains how to use these tools to expose security threats in your organization.
In this section: Understand DNA Reports The Organizational Pass-the-Hash Vulnerability Map The SSH Keys Trusts Map Use DNA Reports to Expose Security Threats Sharing DNA Report Data with CyberArk LoggingUnderstand DNA Reports The Discovery and Audit Report is a comprehensive Excel file that provides detailed information about the current status of each privileged account that is identified. Note: You cannot view the report file using Microsoft Excel Viewer The report includes the following Excel sheets: ■ Executive Summary Dashboard ■ Windows Scan ■ Unix Scan ■ Domain Scan ■ SSH Keys Trust ■ Database scan ■ Hard-Coded Credentials ■ Cloud Users ■ Cloud Instances ■ What is Insecure Priv. Esc. ■ What are SSH Keys? ■ What is Pass-the-Hash? ■ Scan Errors Executive Summary Dashboard The first sheet in the Discovery and Audit Report is the Executive Summary Dashboard, which contains summarized information about the scan using charts and graphs, for a quick and simple overview. Note: The results of the database accounts scan are only displayed in the Database Scan sheet, and are not represented in the Executive Summary. This summary comprises the following main areas: Area Summarizes Machine/Account Data The scan, the accounts that were discovered and their compliance status. For more information, refer to Machine/Account Data. Embedded/HardCoded Credentials Discovery the scan for embedded and hard-coded credentials. For more information, refer to Embedded/Hard-Coded Credentials Discovery, page 50. CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 46Area Summarizes SSH Keys Discovery the SSH keys discovery scan, their usage, and their compliance status. For more information, refer to SSH Keys Discovery, page 51. Credential Theft Vulnerability The threat and vulnerability status of Pass-the-Hash related attacks. For more information, refer to Credential Theft Vulnerability, page 52. Cloud Asset Discovery The cloud discovery scan, their type and their compliance status.
For more information, refer to Cloud Asset Discovery, page 54 Machine/Account Data This area displays a summary of the scan, the machines that were scanned, and the accounts that were discovered. CyberArk Discovery and Audit (DNA) Understand DNA Reports 47It includes the following information: ■ About the Scan – A summary of the scan details: Data Description Scan date The date and time the scan was performed. Licensee name The person or organization DNA is licensed to. Created by The display name of the user logged on to the machine where CyberArk DNA is run. LDAP path The LDAP path used to identify the accounts to scan. Note: If the scan was performed on accounts listed in an imported file, the displayed LDAP path will be N/A.
Windows machine types The type of machines selected for scanning. On Windows machines, this can be Servers, Workstations, or Servers and Workstations. Windows object type The type of objects selected for scanning.
For Windows, this can be Accounts (privileged accounts and non-privileged accounts) or Service Accounts (embedded Windows credentials) or both. Unix machine types The type of machines selected for scanning. On Unix/Linux machines, this is always Servers and Workstations. Unix object type The type of objects selected for scanning. For Unix/Linux, this is Accounts (privileged and non-privileged accounts). Password policy The current password policy that identifies non-compliant accounts. For more information about how policies work, refer to DNA Configuration, page 123, in Configuration Parameters. Machines Scanned – A bar chart that shows the number and percentage of Windows and Unix/Linux devices scanned, displayed by operating system. The number of machines scanned per operating system is displayed below the chart. Note: This number includes both machines that were completed successfully and those where the scan completed with issues Accounts Discovered – A bar chart that shows the number of accounts detected on Windows and Unix/Linux devices, displayed by operating system. Privileged and non-privileged accounts are displayed in different colors. The number of privileged and non-privileged accounts detected per operating system is displayed below the chart. Note: This number does not include non-privileged account members of the Domain Users group Domain Service Accounts Discovered – A bar chart that shows the number of domain accounts that have the SPN attribute set and the machines that are affected CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 48by these SPN. The number of Privileged SPN accounts includes the unique number of users in the domain for each registered Service. A user can appear on several machines and with several registered Services. Risk Status – A set of pie charts that reflect the following: Compliant/non-compliant accounts The percentage of compliant/non-compliant accounts discovered on Windows and Unix machines during the scan. The exact number of compliant/noncompliant accounts is displayed below each chart. DNA identifies compliant/non-compliant accounts according to the following criteria: Compliancy Indicates ... Compliant Accounts that meet organizational and standards compliancy, including a predefined maximum password age, key length, key type, etc. Noncompliant Accounts that do not meet organizational and standards compliancy. Privileged/non-privileged accounts The percentage of privileged/non- privileged accounts discovered on Windows and Unix machines during the scan. The exact number of privileged/nonprivileged accounts is displayed below the chart. DNA identifies privileged/non-privileged accounts according to the following criteria: Privilege Indicates ... Privileged Accounts that are accessed by users in the following groups: On Windows, this includes groups such as Power Users, Administrators, etc. On Unix, this also includes the root group and users listed in the sudoers file. Nonprivileged Accounts that are accessed by users in any group not defined as privileged.
For more information, refer to Account Category in "windows and unix scans' Least Privilege Risk – Windows business users The percentage of privileged/non-privileged Windows business users. The exact number of each type of user discovered on Workstations and Servers is displayed below each chart.
DNA identifies Windows business users according to the following criteria: Privileged Windows business users CyberArk Discovery and Audit (DNA) Understand DNA Reports 49Users included: Privileged domain users Privileged local users Users excluded: Built-in administrator account of the local machine Built-in administrator account of the domain Non-privileged Windows business users Users included: Any non-privileged accounts on Windows privileged domain users Embedded/Hard-Coded Credentials Discovery This area displays a summary of the risk that discovered embedded and hard-coded credentials pose, the machines that were scanned, and the accounts that were discovered.
For more information about how embedded or hard-coded credentials are defined, and how and where they are discovered, refer to Embedded and Hard-Coded Credentials, page 147.
It includes the following information: Summary (left side) – The number of embedded and hard-coded credentials found on WebSphere, WebLogic, IIS, and Ansible servers, the number of WebSphere, WebLogic and IIS servers or Ansible playbooks with these credentials, and the number of target systems (e.g. databases) or playbooks at risk as a result. This list enables you to see the level of risk that your environment is exposed to at a glance. CyberArk Discovery and Audit (DNA) CyberArk DNA™ User Guide 50 Download PDF Expand Fullscreen Scan your network with CyberArk DNA™ to: Discover where privileged accounts exist Clearly assess privileged account security risks Identify machines vulnerable to Pass-the-Hash attacks Collect reliable and comprehensive audit information