Tenable Cyber Exposure Study - Identity and Access Management

Last Revised: February 28, 2024

Table of Contents

Overview

Compromised identities are a key aspect of most successful cybersecurity data breaches. Identification, authentication, and authorization controls, also known as provision and deprovision processes, must be aligned with business requirements and maintained appropriately, as user roles evolve over time. Very often, organizations have outdated user accounts because of ineffective deprovisioning processes. Two primary challenges organizations face in achieving basic cyber hygiene are limited budgets and a lack of staff with security expertise.

Many exploits require local access to be executed. A common attack path is to trick a user with legitimate local access into executing malware code through phishing attacks or other fraudulent means. Vulnerabilities that an organization may consider to be low risk pose a much higher risk through such attacks.

Microsoft Active Directory servers – a key component of many networks – contain data about users, computers, applications, and shared resources, among other information. These identity management servers are a favorite target for attackers.

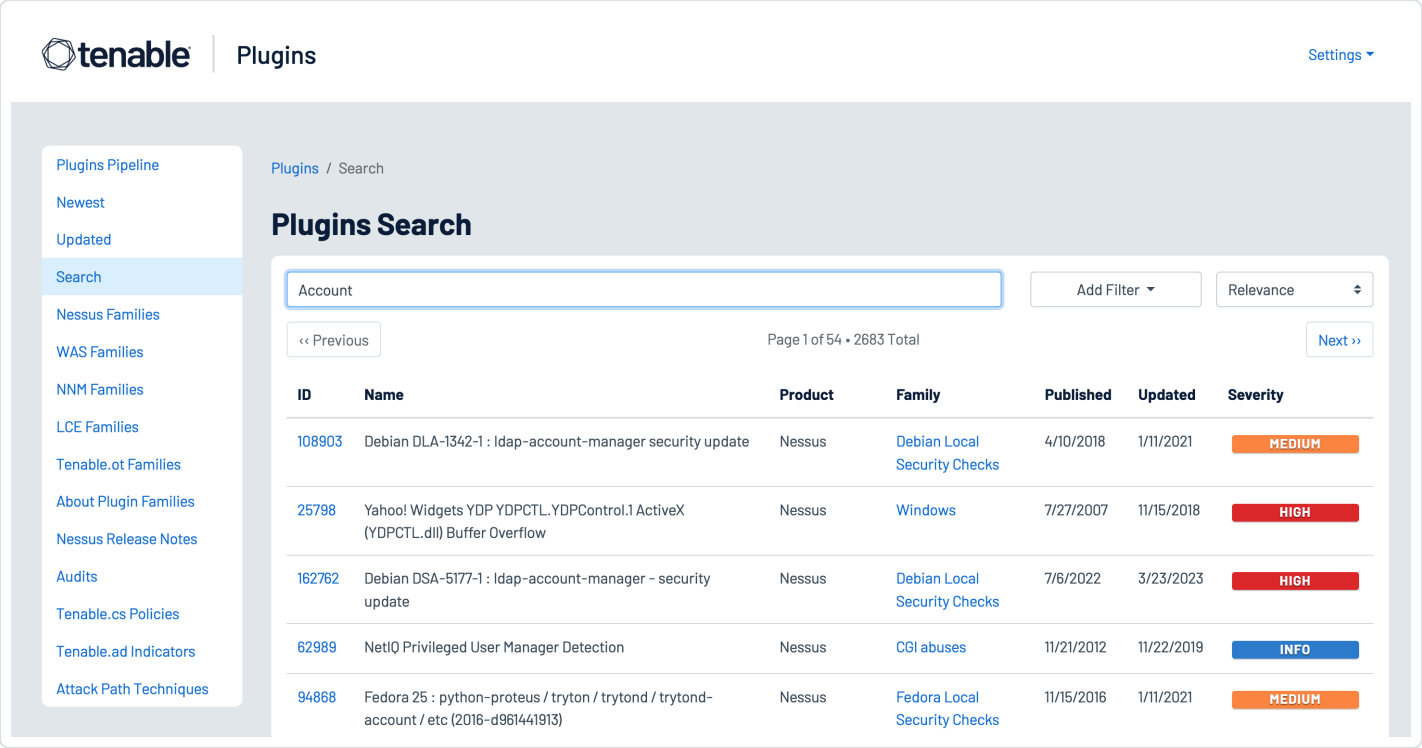
How Tenable Can Help

Leveraging Tenable Security Center (formerly Tenable.sc), Tenable Vulnerability Management (formerly Tenable.io), and Tenable Identity Exposure (formerly Tenable.ad) solutions enables organizations to close attack paths, making the organization a more difficult target to attack. Tenable solutions provide organizations the data needed to identify and evaluate exposures in the environment. Tenable Security Center is an on-premises solution, powered by Nessus, that provides a risk-based view of the organization's IT, security and compliance posture. Tenable Vulnerability Management (formerly Tenable.io) provides similar functions in a cloud-based solution. Tenable Identity Exposure is a fast, agent-less Active Directory security solution that helps organizations analyze their complex Active Directory environment, predict what matters most to reduce risk, and eliminate attack paths before they can be exploited.

Tenable Vulnerability Management

Tenable Security Center and Tenable Vulnerability Management enable security teams to focus on the vulnerabilities and assets that matter most to the organization, while deprioritizing the vulnerabilities that attackers are unlikely to ever exploit.

As information about new vulnerabilities is discovered and released into the public domain, Tenable Research designs plugins to detect and evaluate the risks posed by these vulnerabilities. The plugins contain vulnerability information, a simplified set of remediation actions and the algorithm to test for the presence of security exposures. Tenable Research has published many plugins which detect account issues, as shown below:

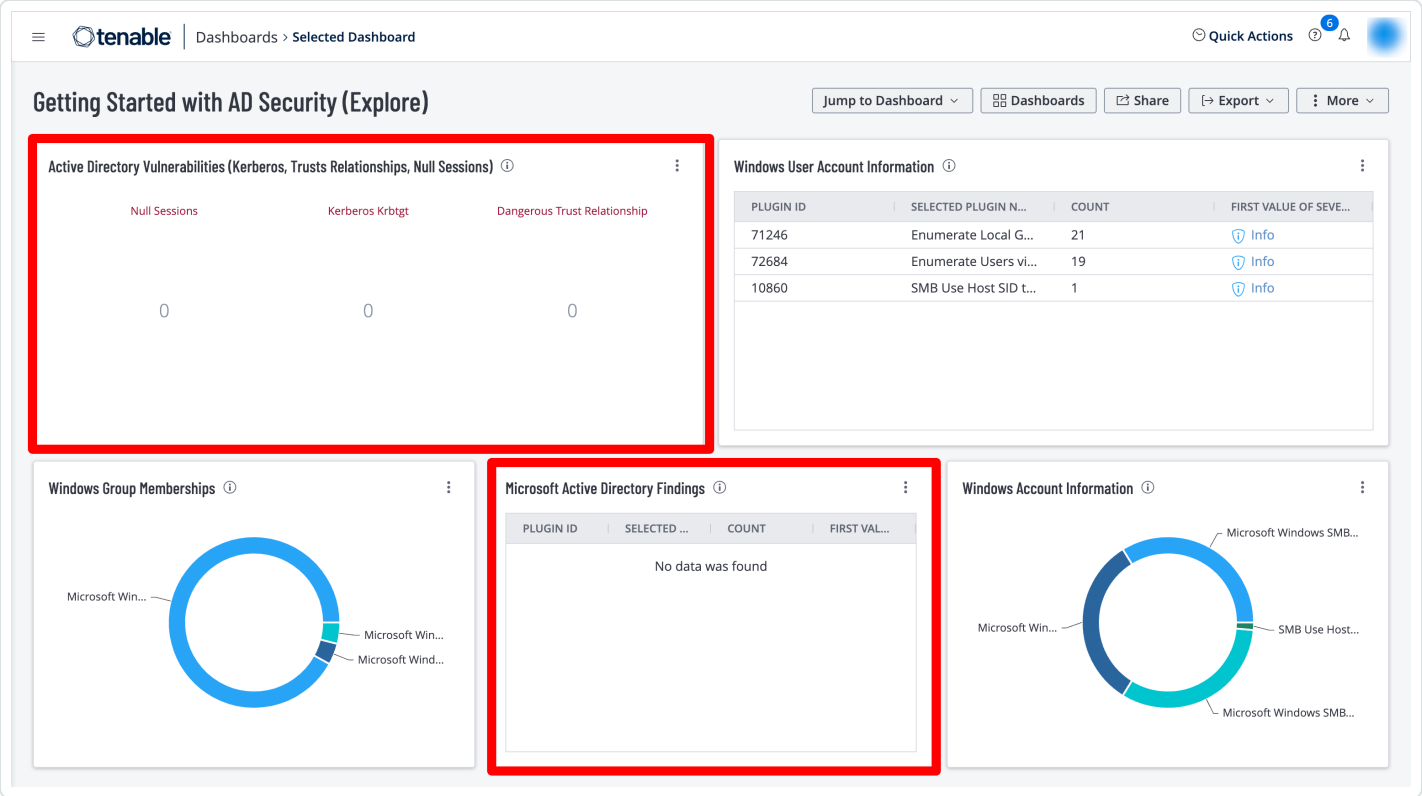


Active Directory Settings

The Getting Started with AD Security Tenable Vulnerability Management dashboard uses output derived from a set of plugins that are part of the Tenable Active Directory Starter Scan Template to help organizations determine the security posture of their Active Directory Servers using the following widgets:

Active Directory Vulnerabilities (Kerberos, Trusts Relationships, Null Sessions) – This widget uses plugins 150488, 150484, and 150486 to list a total count of findings for assets that were identified with the Active Directory vulnerabilities plugins directly related to Kerberos, Trusts Relationships, and Null Sessions.

Microsoft Active Directory Findings – This widget displays a vulnerability summary for assets that contain any vulnerabilities related to Active Directory. The application CPE filter is used to cross reference Tenable plugins that contain "active_directory", including those from the AD Starter Scan.



These widgets leverage the following Tenable Nessus plugins:

- 150480 AD Starter Scan - Kerberoasting

- 150484 AD Starter Scan - Kerberos Krbtgt
- 150486 AD Starter Scan - Dangerous Trust Relationship
- 150481 AD Starter Scan - Weak Kerberos encryption
- 150488 AD Starter Scan - Null sessions
- 150489 AD Starter Scan - Blank passwords
- 150485 AD Starter Scan - Unconstrained delegation
- 150482 AD Starter Scan - Kerberos Pre-authentication Validation
- 150483 AD Starter Scan - Non-Expiring Account Password
- 150487 AD Starter Scan - Primary Group ID integrity

Domain Controllers

Organizations can leverage the following Nessus plugins in Tenable Vulnerability Management to identify security issues in Domain Controllers:

- 10413 - Microsoft Windows SMB Registry: Remote PDC/BDC Detection

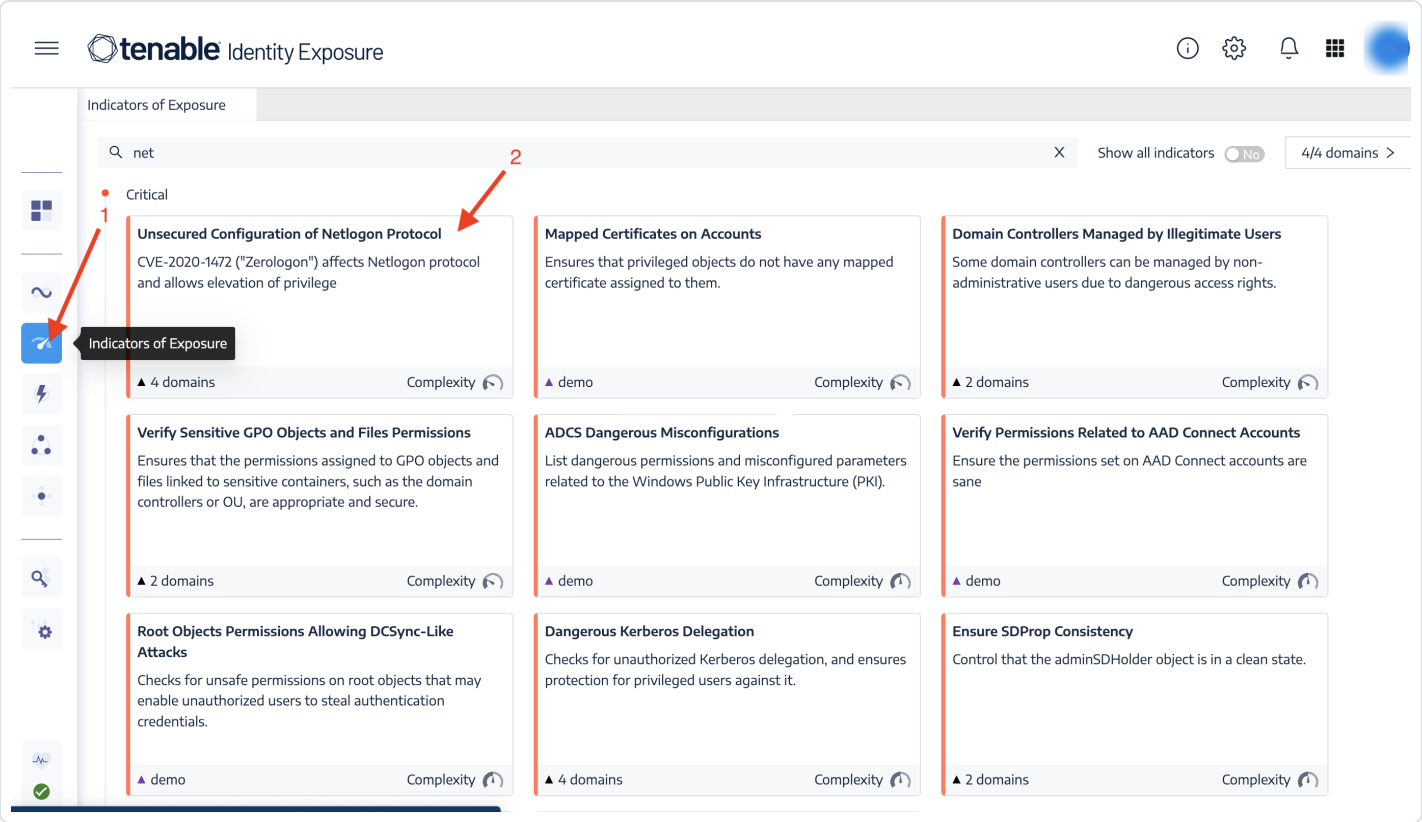
Organizations can leverage the following Nessus plugins in Tenable Security Center to identify security issues in Domain Controllers:

- 44871 - WMI Windows Feature Enumeration With Vuln Text = Active Directory Domain Services
- 10456 - Microsoft Windows SMB Service Enumeration With Vuln Text = Active Directory Domain Services [NTDS]
- 44401 - Microsoft Windows SMB Service Config Enumeration With Vuln Text = Display name : Active Directory Domain Services

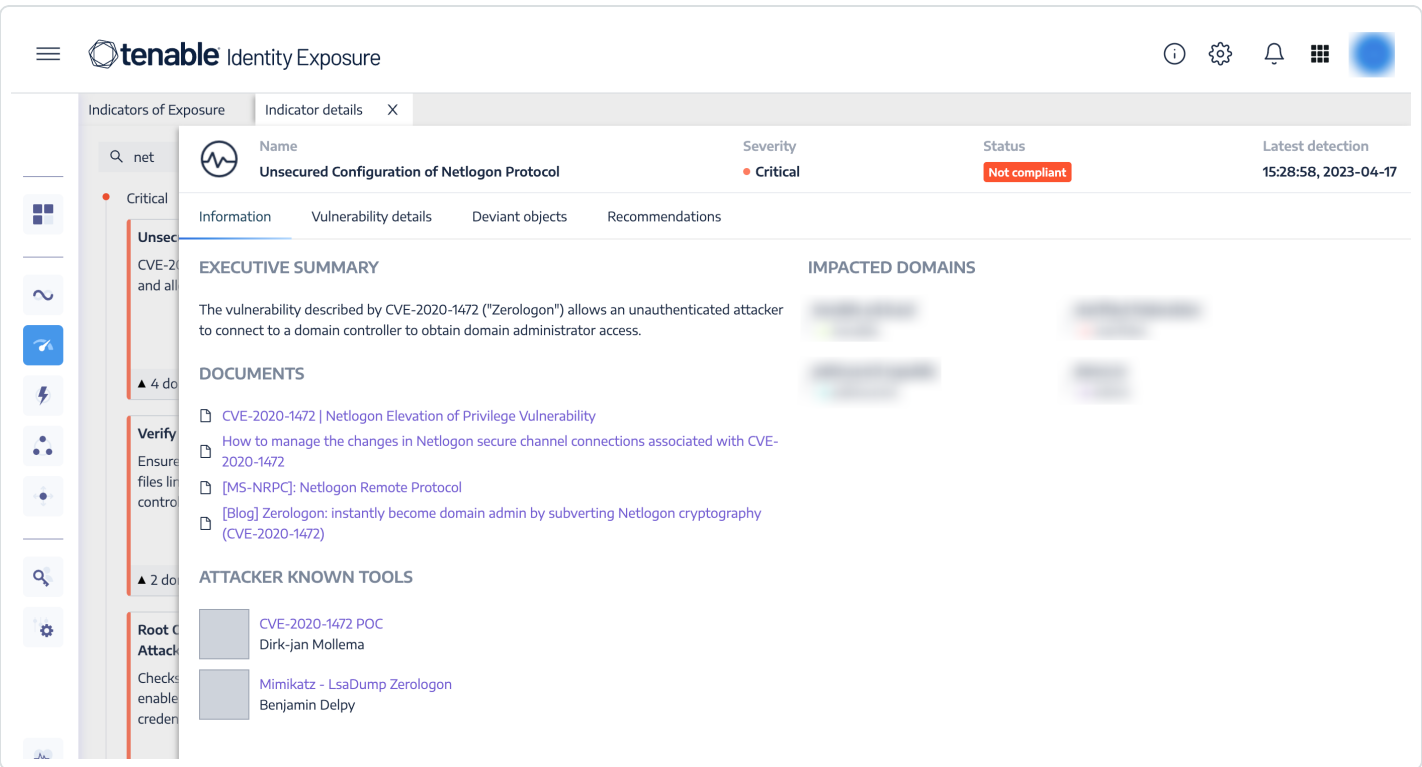
The following Indicators of Exposure (IoE) in Tenable Identity Exposure can be used to identify exposures in Domain Controllers:

- Unsecured Configuration of Netlogon Protocol (Critical)
- Domain Controllers Managed by Illegitimate Users (Critical)
- Insufficient Hardening Against Ransomware (Medium)
- Domain without Computer-Hardening GPOs (Medium)

Step 1: From the Indicators of Exposure tab in Identity Management, search for the above listed IoEs in the search field as shown below:



Step 2: Click on one of the displayed tiles to drill down into more details, as shown below:

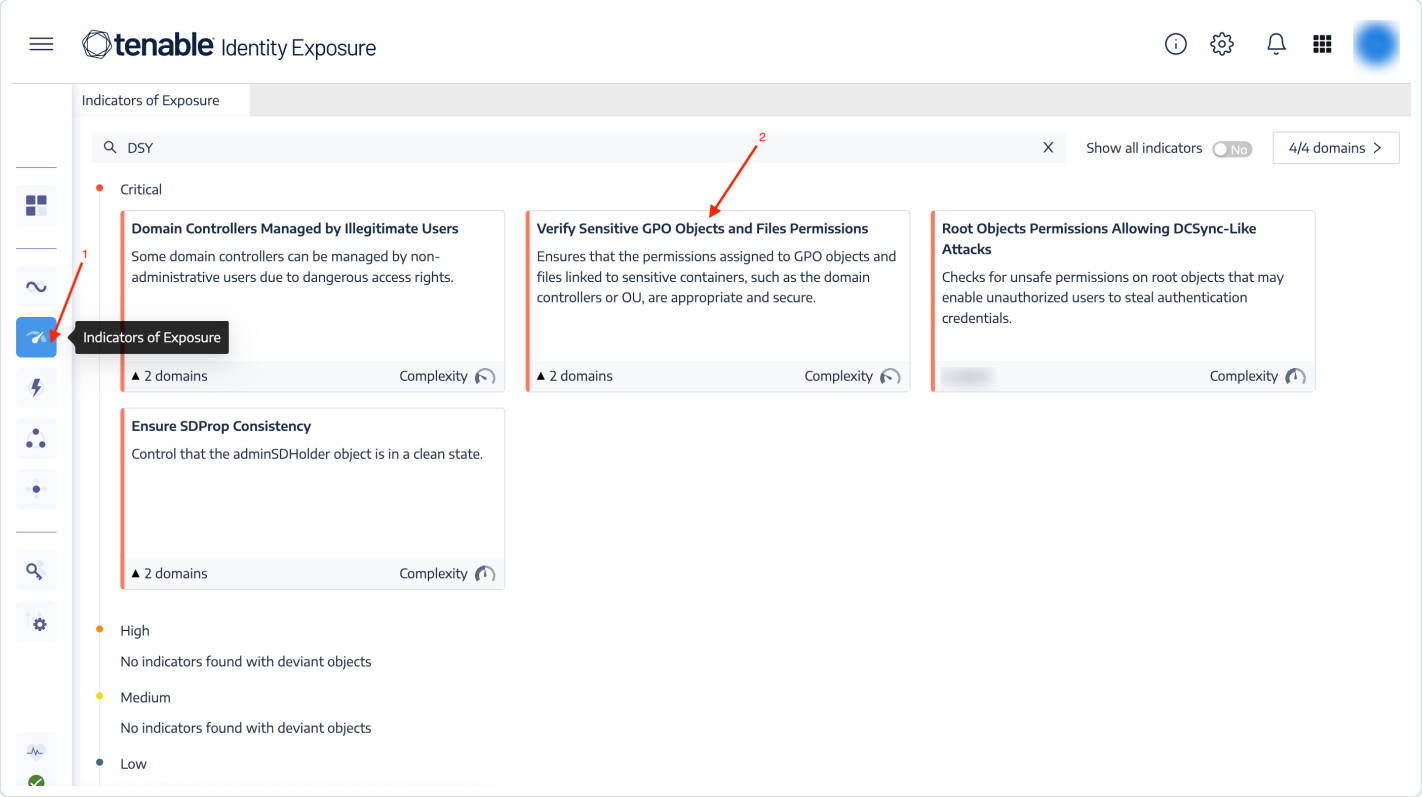


Group and File Permissions

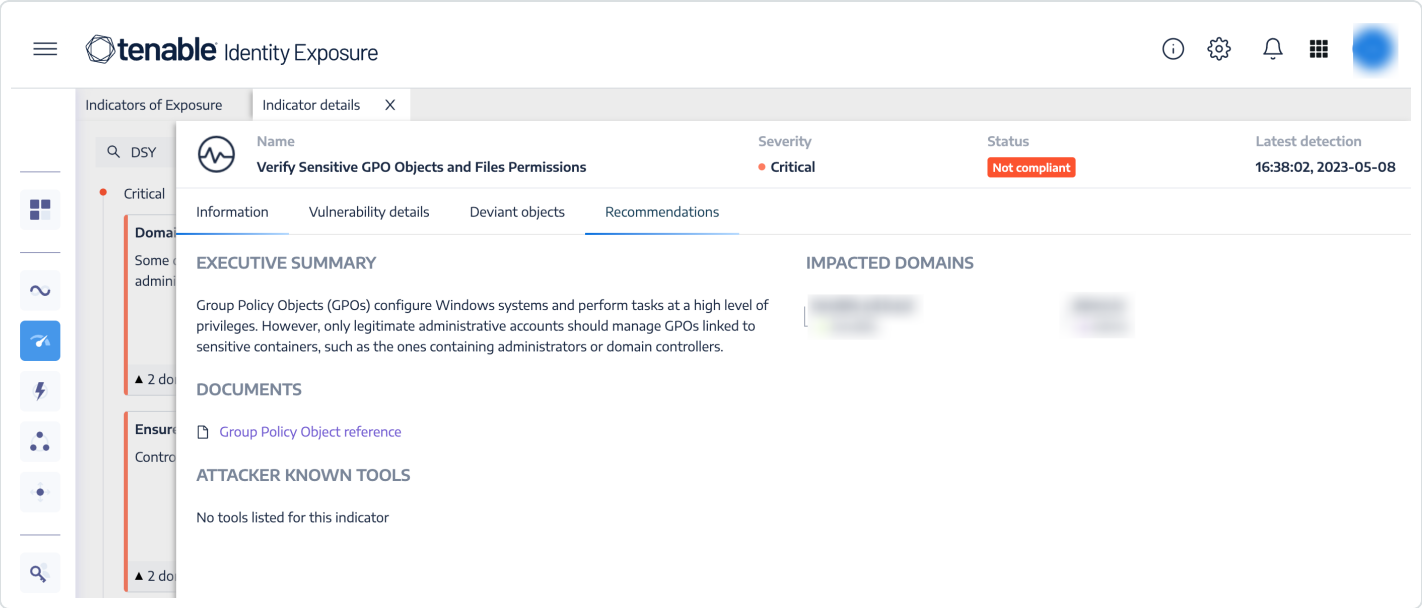
The following Indicators of Exposure (IoE) in Tenable Identity Exposure can be leveraged to determine exposures in group and file permissions:

- Verify Sensitive GPO Objects and File Permissions (Critical)
- User Primary Group (Critical)
- Verify Permissions Related to AAD (Azure Active Directory) Connect Accounts (Critical)
- Root Objects Permissions Allowing DCSync-Like Attacks (Critical)
- Users Allowed to Join Computers to the Domain (Medium)

Step 1: From the Indicators of Exposure tab in Identity Management, search for the above listed IoEs in the search field as shown below:



Step 2: Click on one of the displayed tiles to drill down into more details, as shown below:


tenable Identity Exposure
Indicators of Exposure
Indicator details
DSY
Critical
Name
Verify Sensitive GPO Objects and Files Permissions
Severity
Critical
Status
Not compliant
Latest detection
16:38:02, 2023-05-08
Information
Vulnerability details
Deviant objects
Recommendations
EXECUTIVE SUMMARY
Group Policy Objects (GPOs) configure Windows systems and perform tasks at a high level of privileges. However, only legitimate administrative accounts should manage GPOs linked to sensitive containers, such as the ones containing administrators or domain controllers.
DOCUMENTS
Group Policy Object reference
ATTACKER KNOWN TOOLS
No tools listed for this indicator
IMPACTED DOMAINS

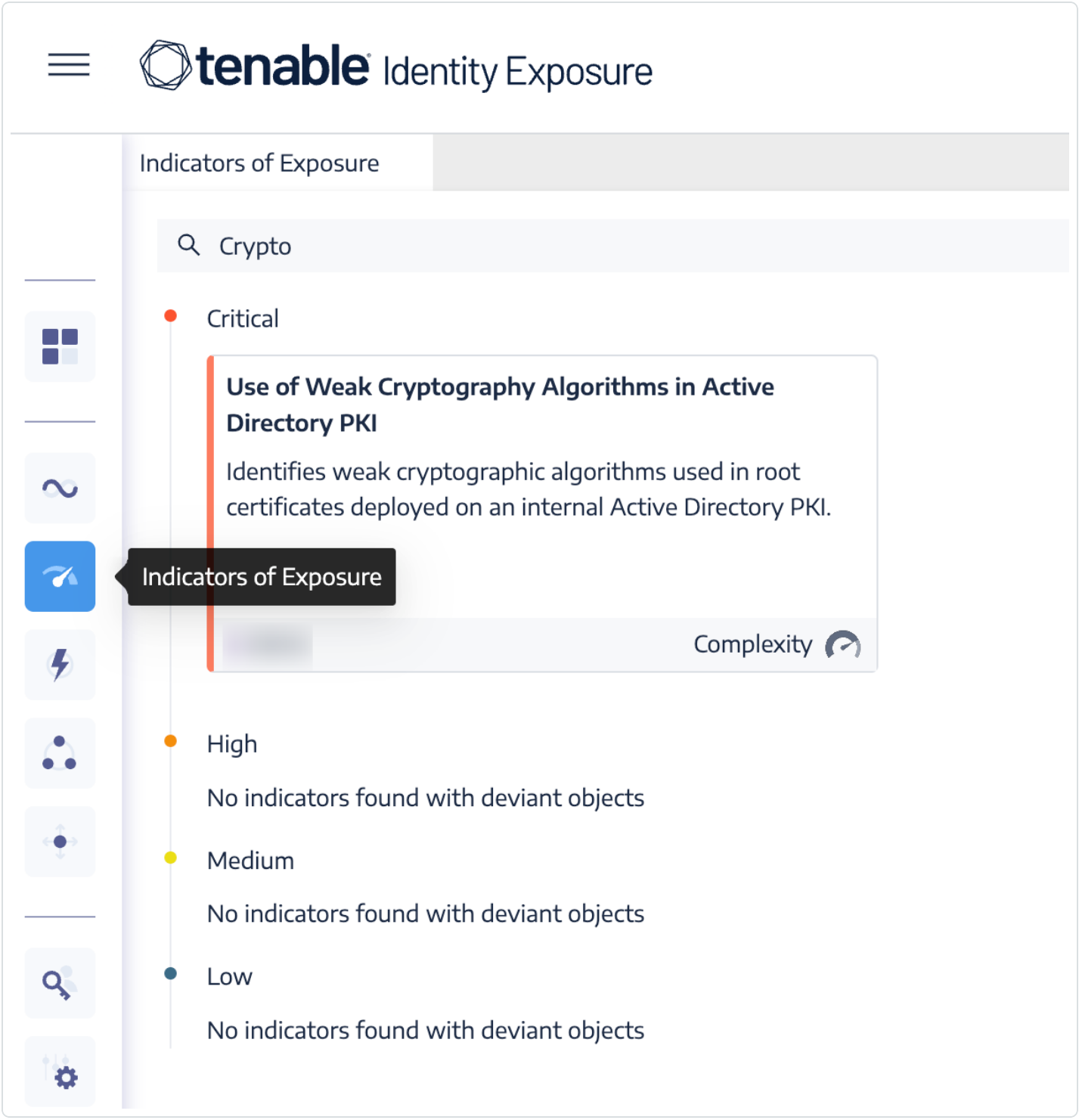
Cryptographic Controls

Applications and servers often support SSL/TLS key exchanges that are cryptographically weaker than recommended. Key exchanges must be recommended by IANA and provide at least 224 bits of security, which translates to a minimum key size of 2048 bits for Diffie Hellman and RSA key exchanges.Nessus has over 1000 plugins that identify vulnerabilities with SSH/OpenSSH, and other cipher suites.

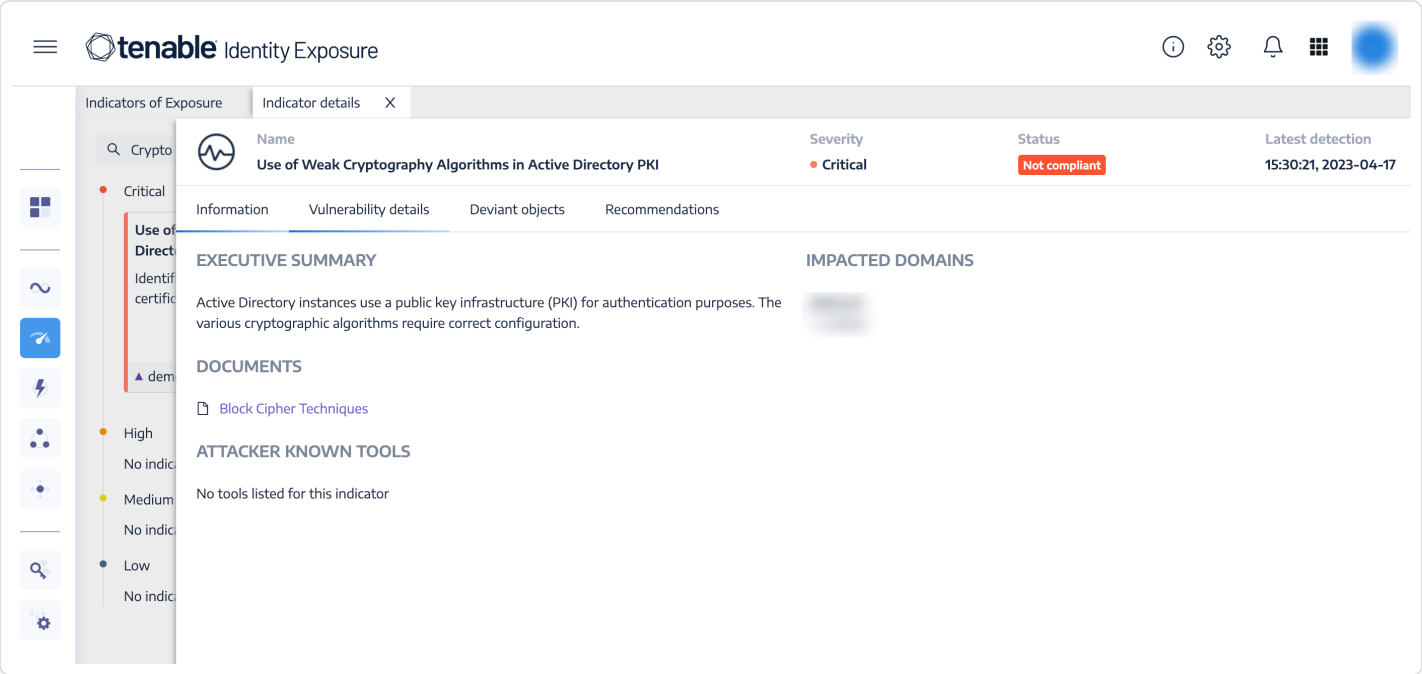
Tenable Identity Exposure has the following Indicators of Exposure to evaluate cryptographic controls:

- ADCS (Active Directory Certificate Services) Dangerous Misconfigurations (Critical)
- Use of Weak Cryptography Algorithms into Active Directory PKI (Critical)
- Reversible Passwords (Medium)
- Vulnerable Credential Roaming Related Attributes (Low)

Step 1: From the Indicators of Exposure tab in Identity Management, search for the above listed IoEs in the search field as shown below:



Step 2: Click on one of the displayed tiles to drill down into more details, as shown below:

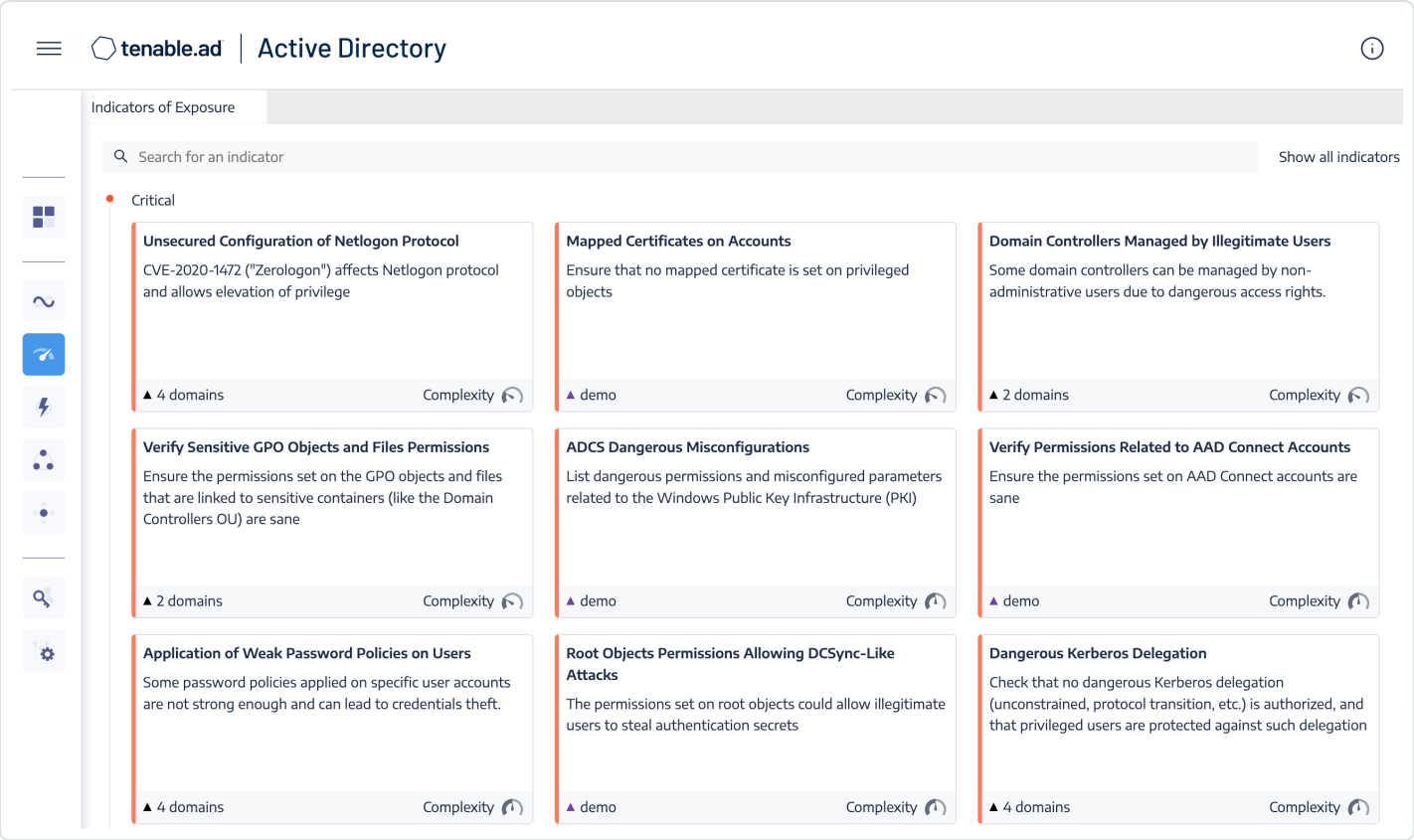

tenable Identity Exposure
Indicators of Exposure
Indicator details
Crypto
Critical
Use of
Direct
Identif
certific
dem
High
No indic
Medium
No indic
Low
No indic
Name
Use of Weak Cryptography Algorithms in Active Directory PKI
Severity
Critical
Status
Not compliant
Latest detection
15:30:21, 2023-04-17
Information
Vulnerability details
Deviant objects
Recommendations
EXECUTIVE SUMMARY
Active Directory instances use a public key infrastructure (PKI) for authentication purposes. The various cryptographic algorithms require correct configuration.
DOCUMENTS
Block Cipher Techniques
ATTACKER KNOWN TOOLS
No tools listed for this indicator
IMPACTED DOMAINS

Tenable Identity Exposure

Tenable Identity Exposure provides information about an organization's Active Directory environment in an intuitive dashboard that monitors Active Directory in real-time, enabling organizations to identify at a glance the most critical vulnerabilities and recommended courses of remediation. Indicators of Exposure and Indicators of Attack discover underlying issues affecting the organization's Active Directory environment. Some of the Identity Management compliance requirements that Tenable solutions address include:

- Identify all accounts in the environment
- Ensure all active accounts are authorized
- Ensure all accounts are configured to use strong authentication controls
- Delete or disable dormant accounts
- Restrict privileged access to only authorized users
- Ensure group access is appropriately assigned
- Understand configuration exposures, such as dangerous permissions

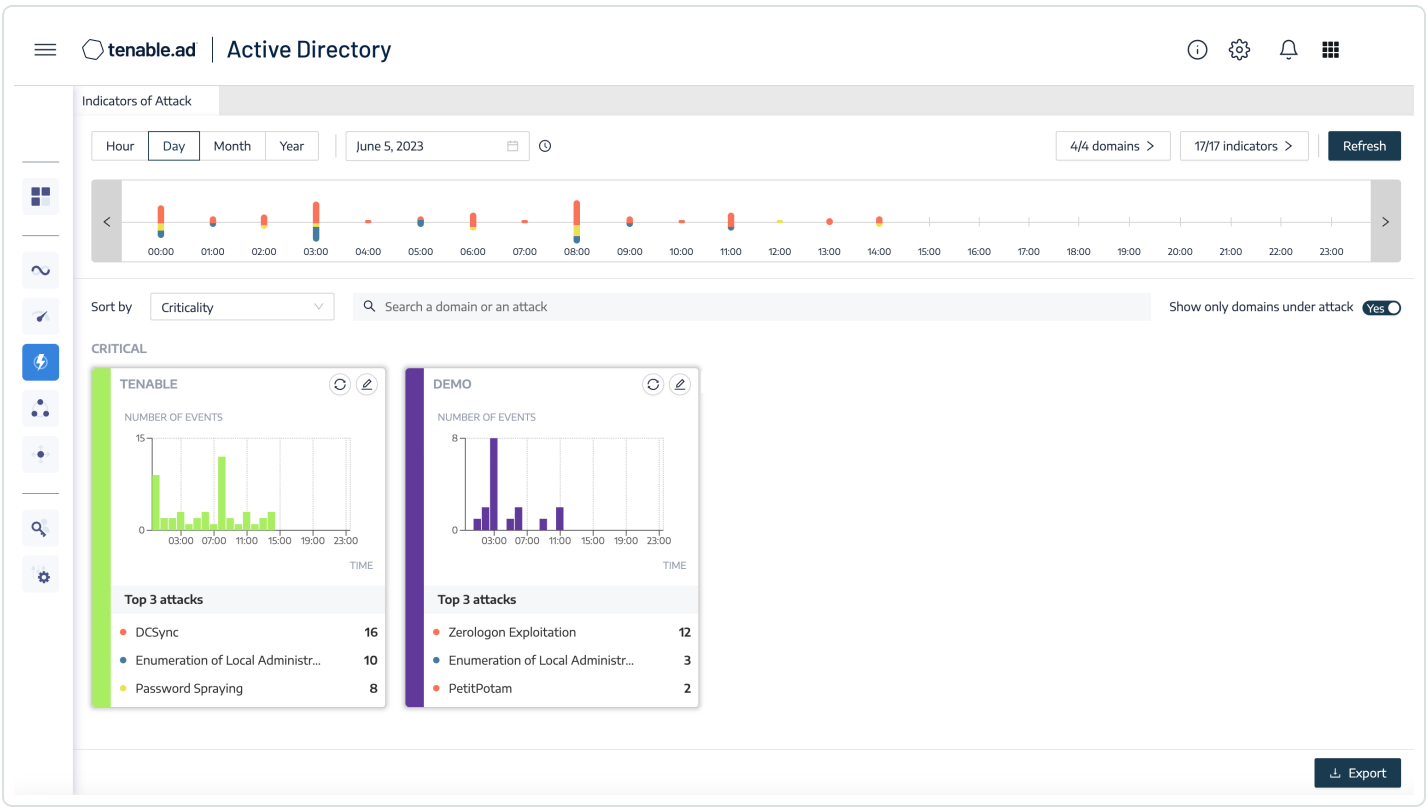
Indicators of Exposure provides an overview of critical, high, medium, and low risk exposures identified across the organization’s domains. From the landing page, security analysts can drill down for more details about which assets are exposed.



The Indicators of Attack pane provides a consolidated view of exposures that impact the organization's Active Directory environment. Displayed is an event timeline that shows when attacks occurred and identifies the severity level of the vulnerability targeted: Critical (red-orange), High (light orange), Medium (yellow), and Low (blue). The tiles below the timeline provide details on the top three attacks in the organization's domains.

This view enables security teams to:

- Visualize every Active Directory threat from an accurate attack timeline
- Analyze in-depth details about an Active Directory attack
- Explore MITRE ATT&CK descriptions directly from detected incidents

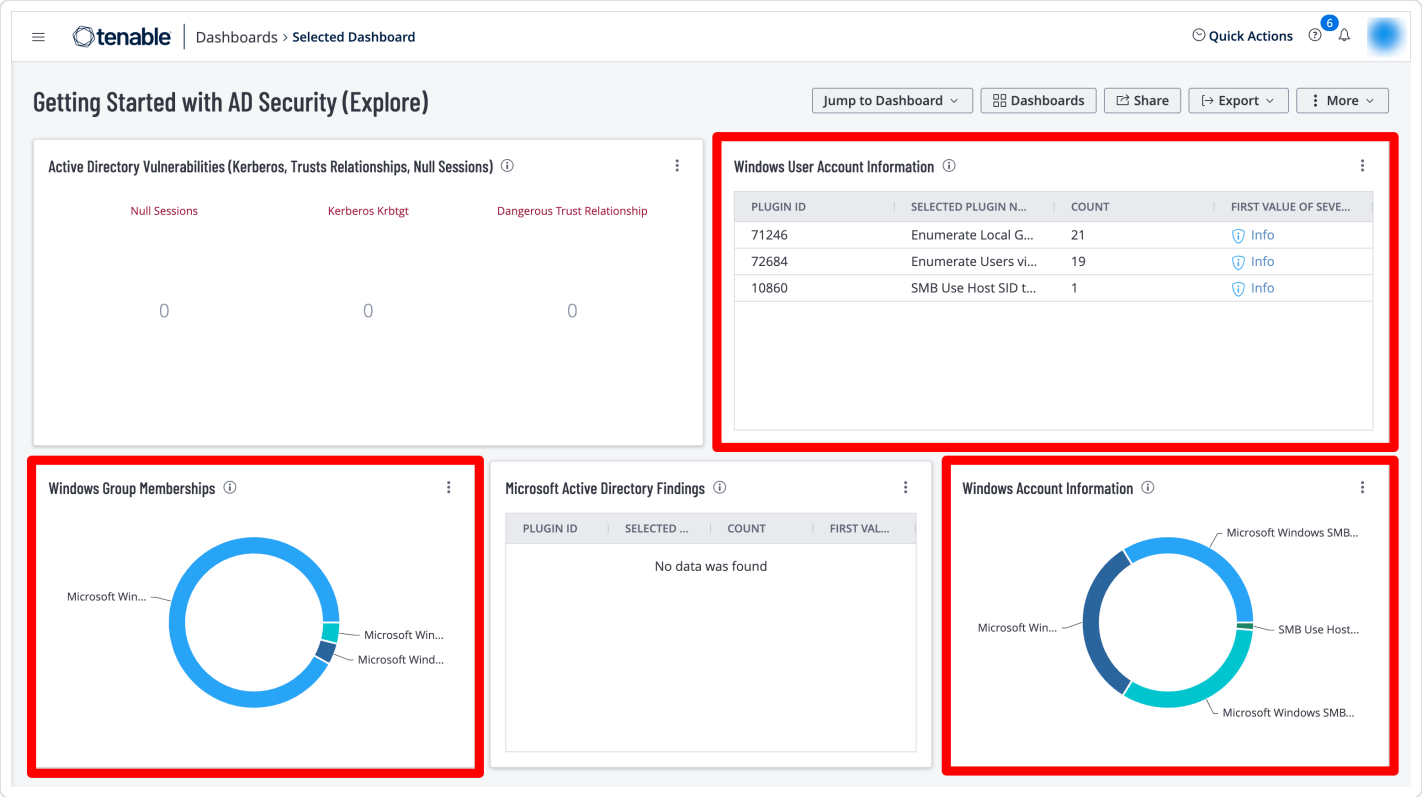

tenable.ad
Active Directory
Indicators of Attack
Hour
Day
Month
Year
June 5, 2023
4/4 domains
17/17 indicators
Refresh
00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00
Sort by
Criticality
Search a domain or an attack
Show only domains under attack
Yes
CRITICAL
TENABLE
NUMBER OF EVENTS
15
0
03:00 07:00 11:00 15:00 19:00 23:00
TIME
Top 3 attacks
DCSync 16
Enumeration of Local Administr... 10
Password Spraying 8
DEMO
NUMBER OF EVENTS
8
0
03:00 07:00 11:00 15:00 19:00 23:00
TIME
Top 3 attacks
Zerologon Exploitation 12
Enumeration of Local Administr... 3
PetitPotam 2
Export

Identifying Exposure

Tenable Identity Exposure provides various methods to access the information collected through the Indicators of Exposure (IoE) and Indicators of Attack (IoA) panes. Tenable Vulnerability Management provides the ability to use the Explore Findings through the use of dashboards and reports.

Identification

The first step in taking control of the organization's Identity Management is to enumerate every user account in the environment and determine the level of access the account is granted. All user accounts must be uniquely identified and assigned to particular entities, such as users and applications.



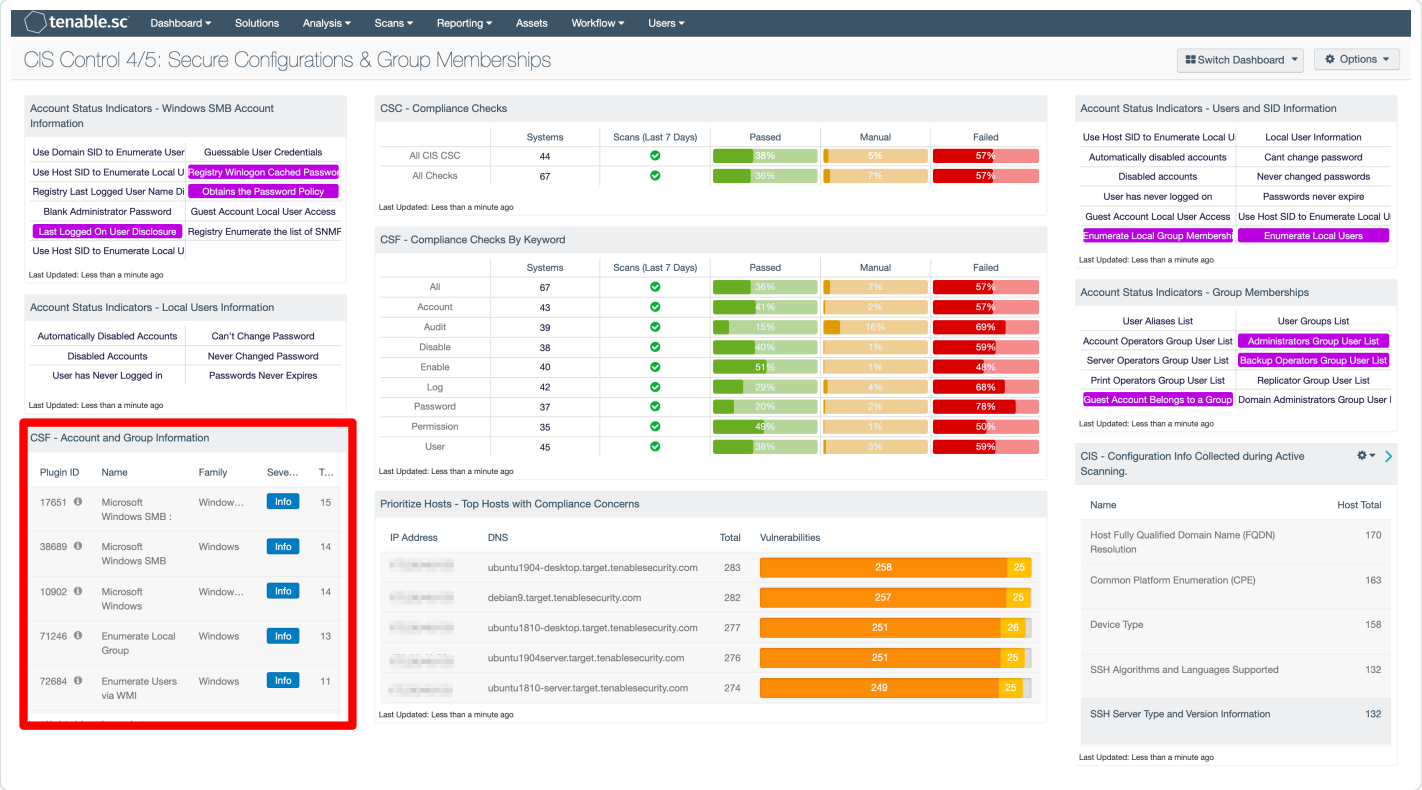
The Getting Started with AD Security dashboard in Tenable Vulnerability Management contains the following widgets to enumerate user accounts:

Windows User Account Information – This widget displays counts for user accounts and security identifiers (SID). Plugins report on potential user account vulnerabilities such as disabled accounts, accounts that have never logged in, accounts with passwords that have never changed, and more.

Windows Group Memberships – This widget displays information for Windows default groups such as administrators, server operators, account operators, backup operators, print operators, and replicator groups.

Windows Account Information – This widget displays counts related to Microsoft Windows SMB plugins that focus on user account information. Plugins focus on vulnerabilities such as SMB blank administrator passwords, SMB password policies, guest accounts, cached passwords, and more.

Organizations can use the **CSF - Account and Group Information** widget located in the **CIS Control 4/5: Secure Configurations & Group Memberships** dashboard in Tenable Security Center, which leverages plugins that enumerate Windows account information.

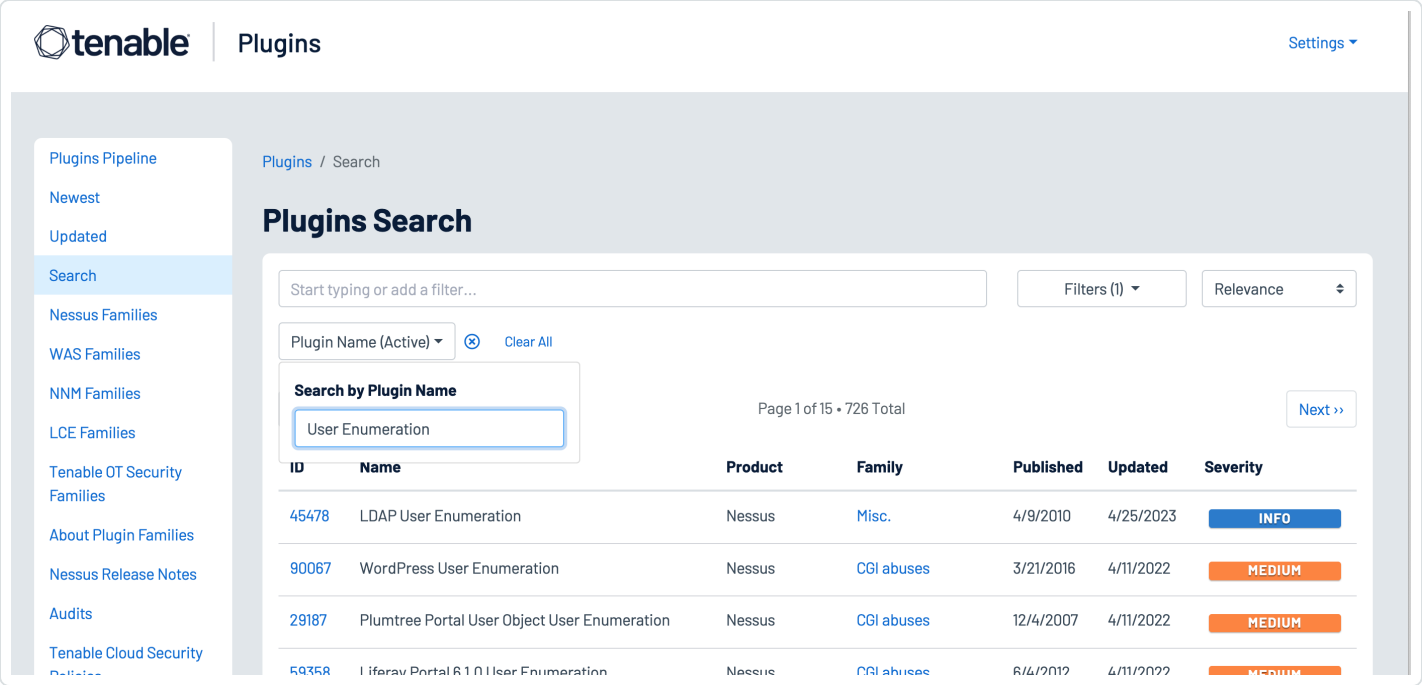


Users and Groups

While Active Directory is typically used by most organizations, there are many other accounts for non-Windows platforms that must be identified. Tenable Nessus contains a number of plugins and plugin families that help organizations enumerate users and groups on the network. The **Windows: User management** plugin family contains nearly 30 plugins that enumerate Microsoft Windows users and groups. Other useful Nessus plugins for user and group enumeration include:

- **10894 Microsoft Windows Users Group List** – This plugin uses the supplied credentials to retrieve the list of groups each user belongs to. Groups are stored for further checks.
- **126527 Microsoft Windows SAM user enumeration** – This plugin enumerates domain users on the remote Windows system using Security Account Manager.
- **95928 Linux User List Enumeration** – This plugin enumerates local users and groups on the remote host.
- **95929 macOS and Mac OS X User List Enumeration –** This plugin extracts the member lists of 'Admin' and 'Wheel' groups on the remote host.

A number of other Nessus plugins that contain the key words "User Enumeration" in a plugin name search using the Plugin Name filter identify WordPress, VMware, LDAP, and other software applications that maintain user accounts, as shown in the following image:

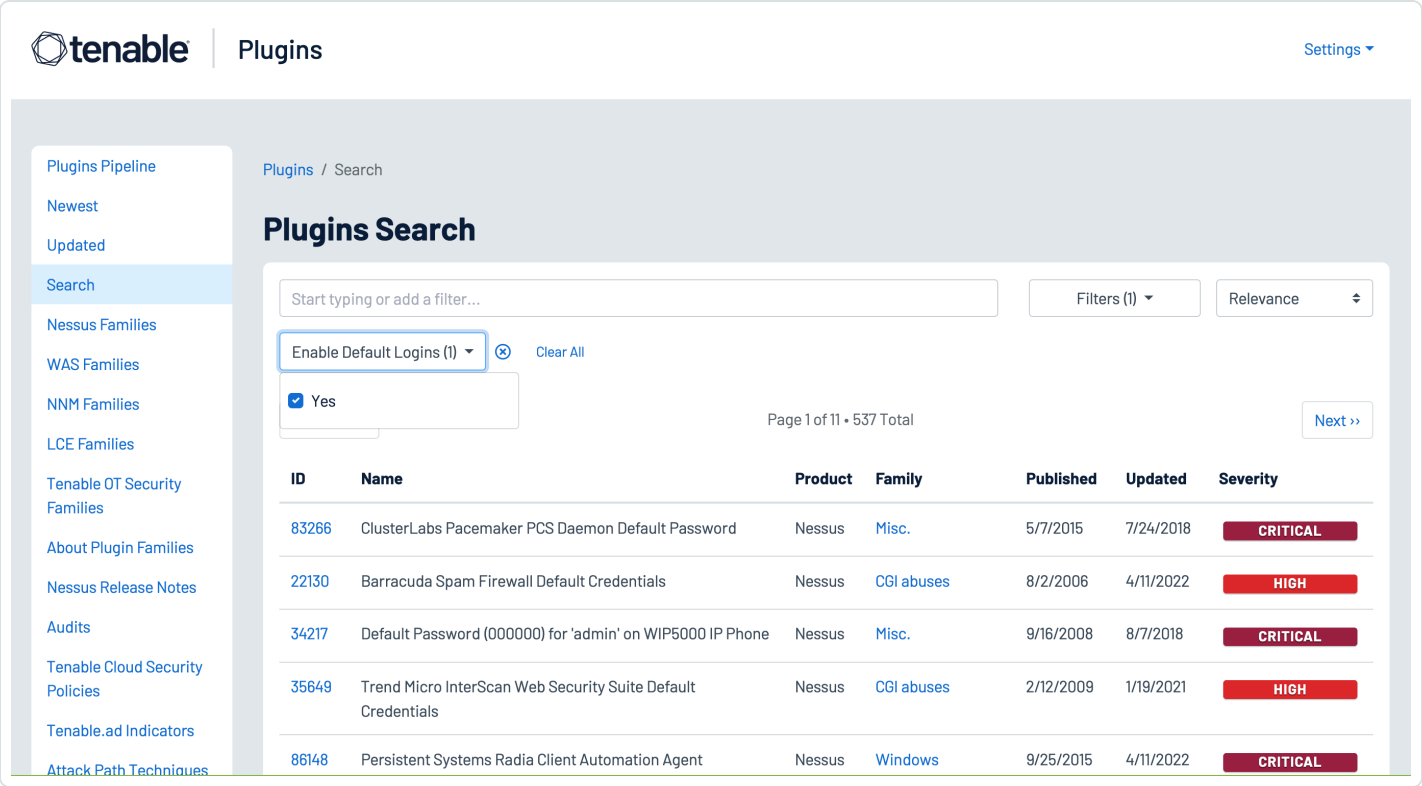


Service and Default Accounts

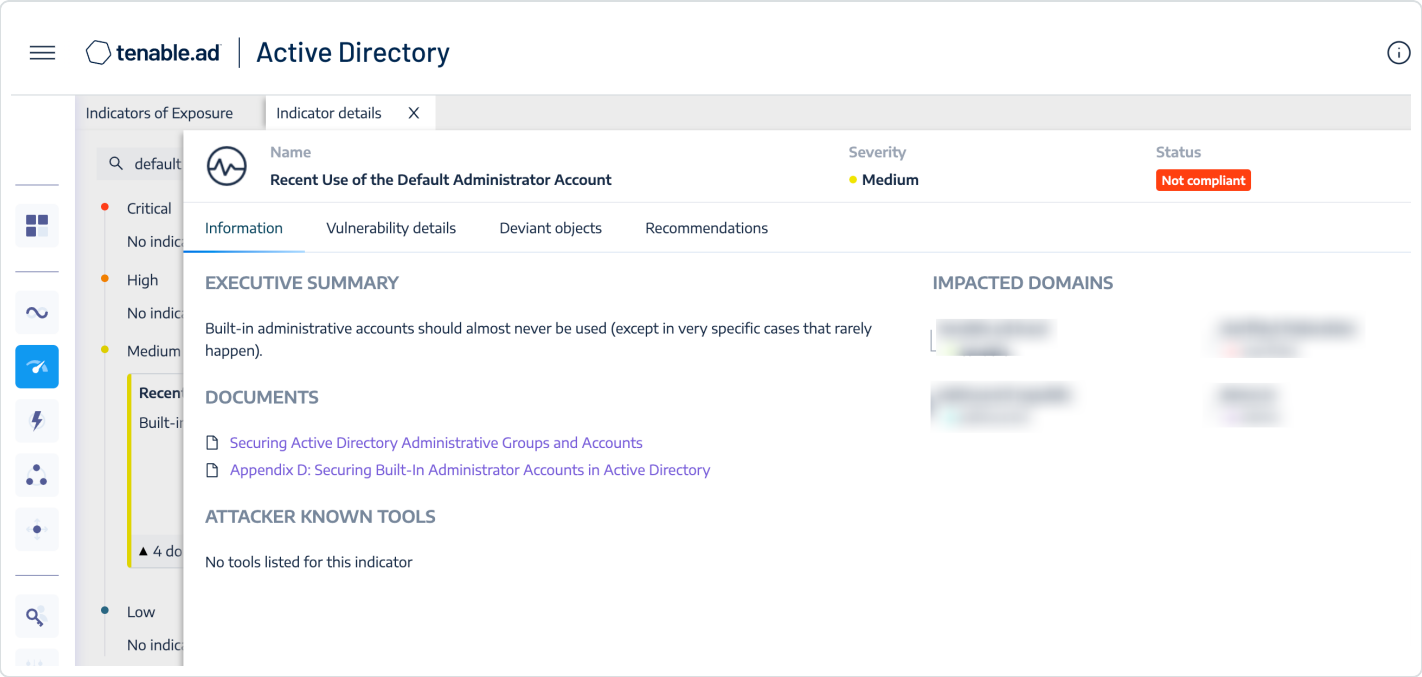
Operating Systems and applications are often distributed with service and default accounts that are either not password-protected or have a default password that is well-known. Tenable Nessus and Tenable Identity Exposure help identify these accounts, enabling organizations to review and disable any unnecessary accounts to reduce the attack surface. Organizations can leverage the following Nessus plugins to enumerate service and default accounts:

- **Plugin Family: Default Unix Accounts –** This plugin family contains over 170 Nessus plugins that check for the existence of default accounts/passwords on a number of devices. In addition, there are many plugins that check for simple passwords such as "0000", "1234", and more commonly identified password combinations for "root" or administrator accounts.
- **171959 Windows Enumerate Accounts –** This plugin enumerates all Windows Accounts

Several hundred plugins can be identified by searching for "Default Account" from the Nessus Plugins Search page using the Enable Default Logins filter. Nessus default account plugins are available for Databases, Web Servers, SCADA devices, Unix/Linux devices, Cisco devices and more. Many of the plugins are associated with the Default Unix Account Nessus family, however, many are in other families as well.



In addition, Tenable Identity Exposure provides the ability to determine if a default administrator account was recently used in the environment, as shown in the image below:

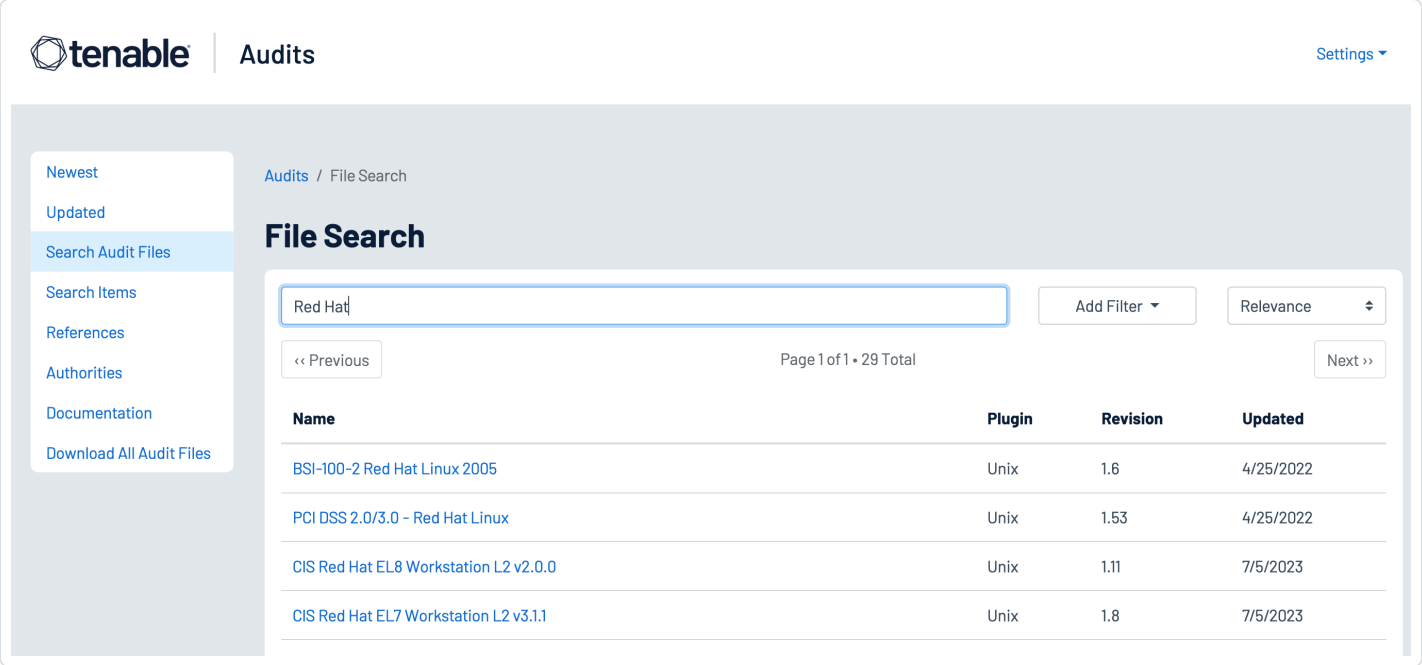


User Access Controls

Strong authentication mechanisms help validate that accounts are being used by the authorized user to read, create, modify, or delete data in accordance with business needs. The Center for Internet Security (CIS) provides benchmarks for a large number Operating System platforms and applications. Tenable Research writes audit files for these benchmarks to help organizations quickly determine their alignment with the CIS recommendations. The benchmarks include guidance on access controls for both non-privileged and privileged accounts.

User Accounts

Non-privileged user accounts require strong access controls to prevent attackers from gaining local access to the network. Attackers often target user accounts to exploit weaknesses in the local network and escalate privileges. Security teams can use the Tenable Audits Search Page to find audit files for their Operating System platforms, which check for common compliance requirements such as "Lock Workstations after Inactivity" and other issues.



Active Directory accounts can be configured to escape global password renewal policies. Accounts set up in this manner can be used indefinitely without ever changing their password. Tenable recommends reviewing user and administrator accounts to ensure they are not configured to have this attribute.

The following Indicators of Exposure (IoE) in Tenable Identity Exposure can be used to identify issues with user accounts in an organization's Active Directory environment:

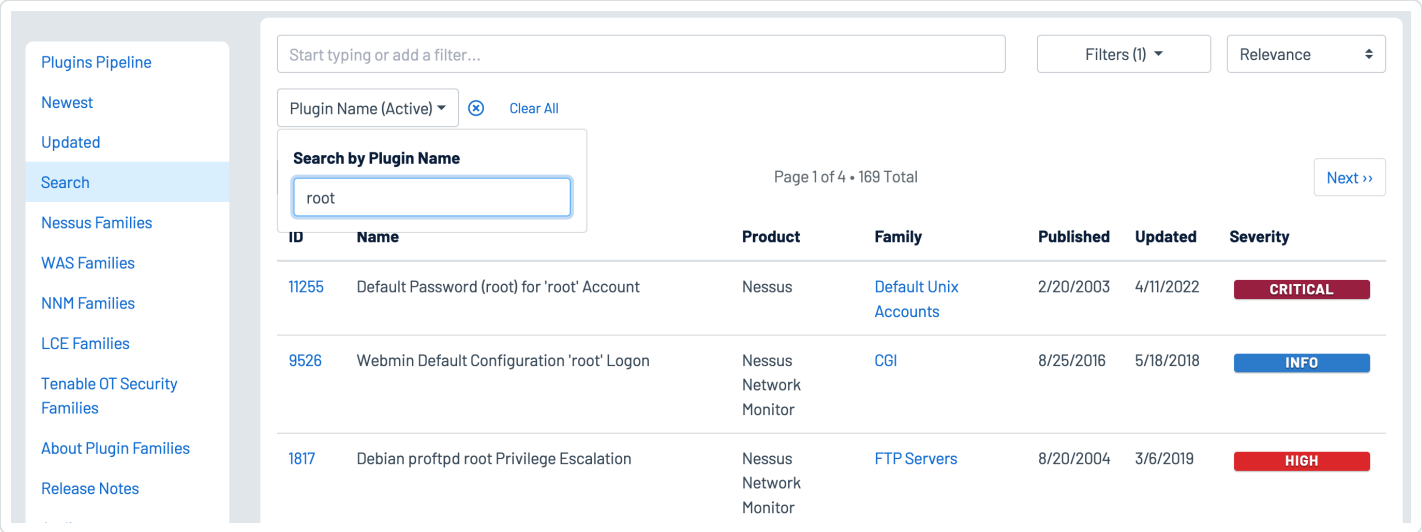
- Accounts with Never Expiring Passwords
- Application of Weak Password Policies on Users
- Dangerous Kerberos Delegation
- Account that Might Have an Empty Password

- AdminCount Attribute Set on Standard Users
- User Account Using Old Password
- Kerberos Configuration on User Account

Privileged Accounts

Most compliance standards and frameworks require privileged users to have a non-privileged account for standard user activities, such as web browsing or reading emails. Tenable Nessus and Tenable Identity Exposure provide the tools to identify settings for root and admin accounts.

Using the Plugin Name filter on the Plugins Search page enables analysts to search for plugins with terms that identify privileged accounts such as “root,” “admin,” or “privileged,” as shown below:



The following Indicators of Exposure (IoE) in Tenable Identity Exposure can be used to identify Active Directory settings for privileged accounts:

- Mapped Certificates on Accounts
- Ensure SDProp Consistency
- Native Administrative Group Members
- Privileged Accounts Running Kerberos Services
- Potential Clear-Text Password
- Protected Users Group not Used
- Logon Restrictions for Privileged Users
- Local Administrative Account Overview Management

Dormant Accounts

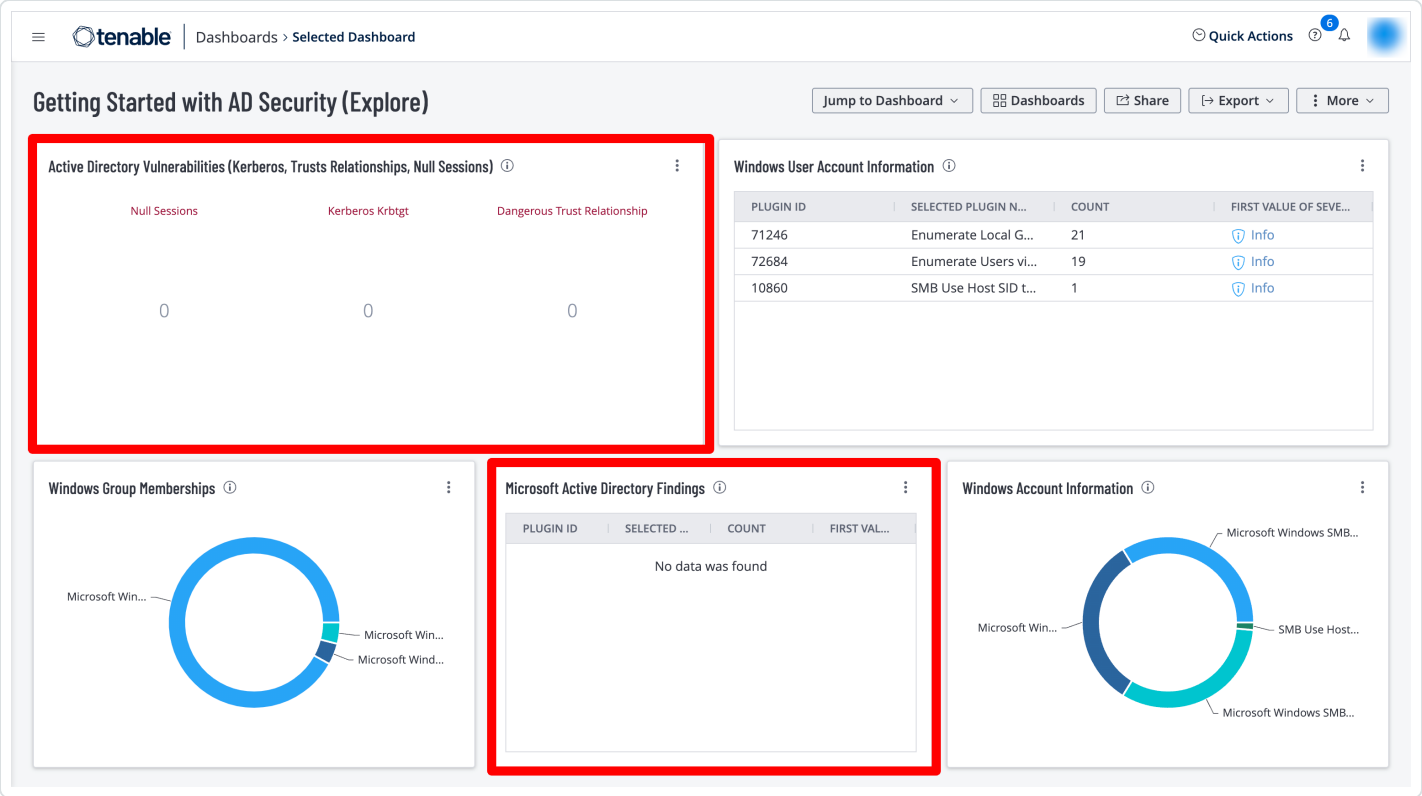
User accounts that have not been accessed in more than a year provide an opportunity for attackers to leverage compromised credentials and perform brute-force attacks. Nessus plugins 10915 or 10899 Microsoft Windows - Local Users Information: User Has Never Logged In displays a list of Windows accounts where the user has never logged in. The Sleeping Accounts Indicator of Exposure in Tenable Identity Exposure detects accounts that have not been accessed in over a year.

Active Directory Settings

The Getting Started with AD Security Tenable Vulnerability Management dashboard uses output derived from a set of plugins that are part of the Tenable Active Directory Starter Scan Template to help organizations determine the security posture of their Active Directory Servers using the following widgets:

Active Directory Vulnerabilities (Kerberos, Trusts Relationships, Null Sessions) – This widget uses plugins 150488, 150484, and 150486 to list a total count of findings for assets that were identified with the Active Directory vulnerabilities plugins directly related to Kerberos, Trusts Relationships, and Null Sessions.

Microsoft Active Directory Findings – This widget displays a vulnerability summary for assets that contain any vulnerabilities related to Active Directory. The application CPE filter is used to cross reference Tenable plugins that contain "active_directory", including those from the AD Starter Scan.



These widgets leverage the following Tenable Nessus plugins:

- 150480 AD Starter Scan - Kerberoasting

- 150484 AD Starter Scan - Kerberos Krbtgt
- 150486 AD Starter Scan - Dangerous Trust Relationship
- 150481 AD Starter Scan - Weak Kerberos encryption
- 150488 AD Starter Scan - Null sessions
- 150489 AD Starter Scan - Blank passwords
- 150485 AD Starter Scan - Unconstrained delegation
- 150482 AD Starter Scan - Kerberos Pre-authentication Validation
- 150483 AD Starter Scan - Non-Expiring Account Password
- 150487 AD Starter Scan - Primary Group ID integrity

Domain Controllers

Organizations can leverage the following Nessus plugins in Tenable Vulnerability Management to identify security issues in Domain Controllers:

- 10413 - Microsoft Windows SMB Registry: Remote PDC/BDC Detection

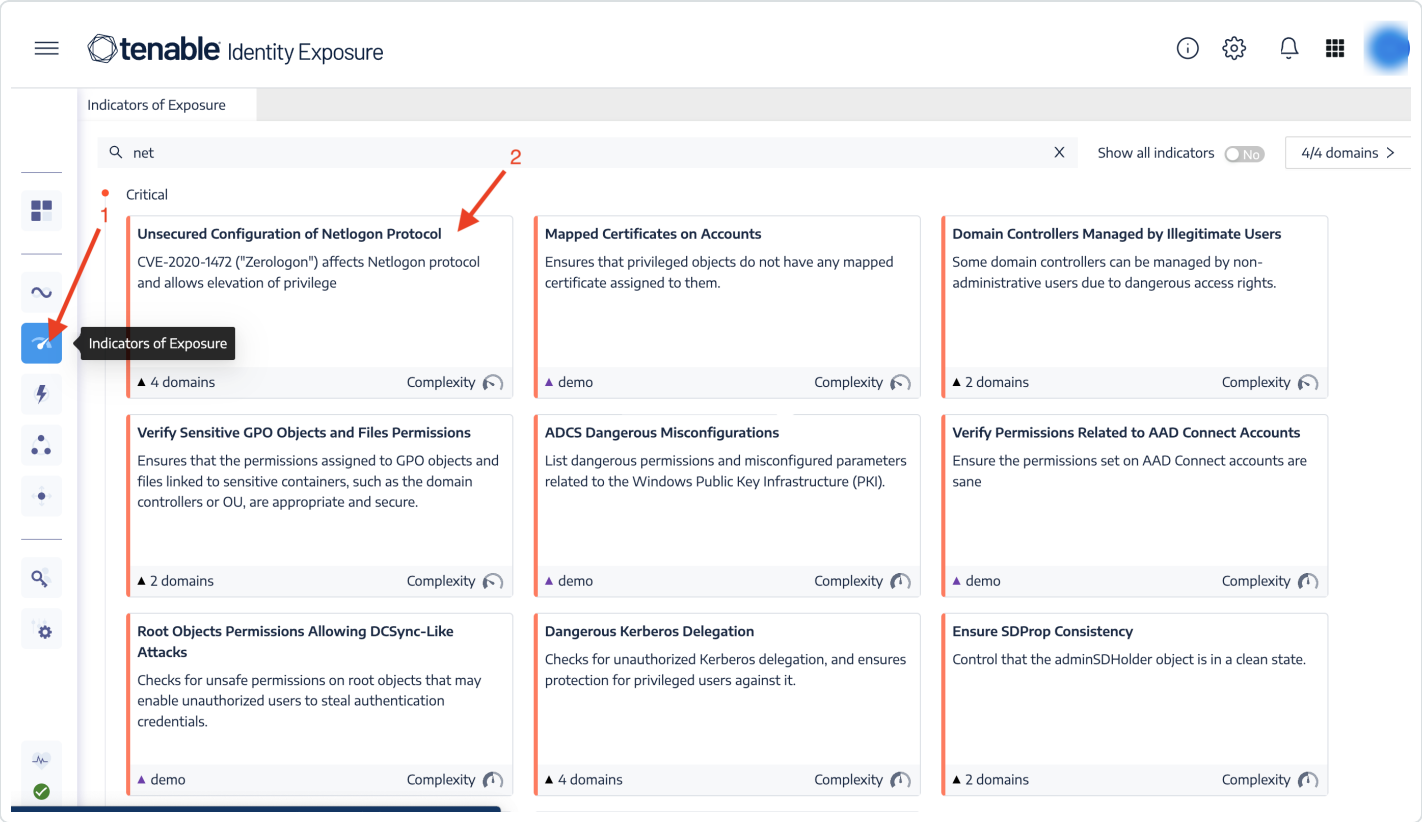
Organizations can leverage the following Nessus plugins in Tenable Security Center to identify security issues in Domain Controllers:

- 44871 - WMI Windows Feature Enumeration With Vuln Text = Active Directory Domain Services
- 10456 - Microsoft Windows SMB Service Enumeration With Vuln Text = Active Directory Domain Services [NTDS]
- 44401 - Microsoft Windows SMB Service Config Enumeration With Vuln Text = Display name : Active Directory Domain Services

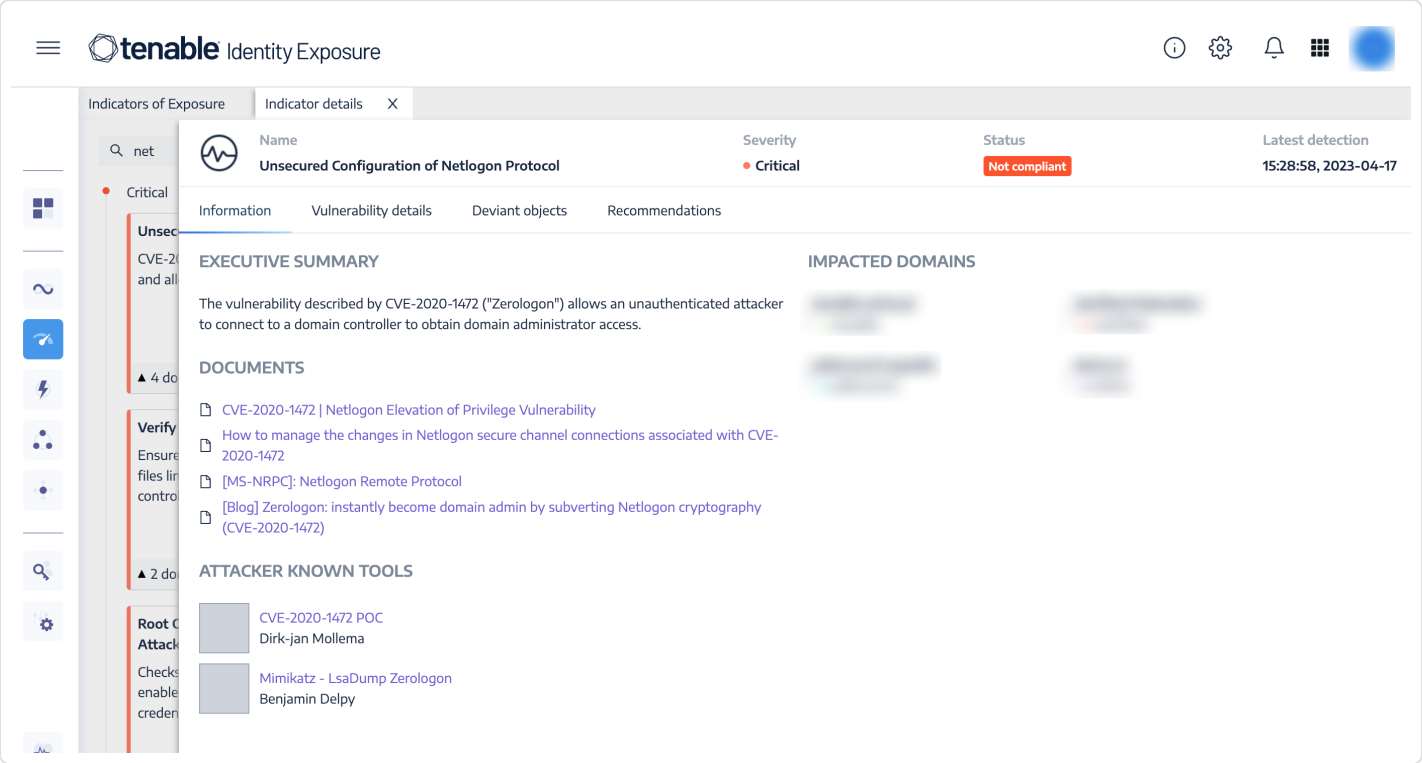
The following Indicators of Exposure (IoE) in Tenable Identity Exposure can be used to identify exposures in Domain Controllers:

- Unsecured Configuration of Netlogon Protocol (Critical)
- Domain Controllers Managed by Illegitimate Users (Critical)
- Insufficient Hardening Against Ransomware (Medium)
- Domain without Computer-Hardening GPOs (Medium)

Step 1: From the Indicators of Exposure tab in Identity Management, search for the above listed IoEs in the search field as shown below:



Step 2: Click on one of the displayed tiles to drill down into more details, as shown below:

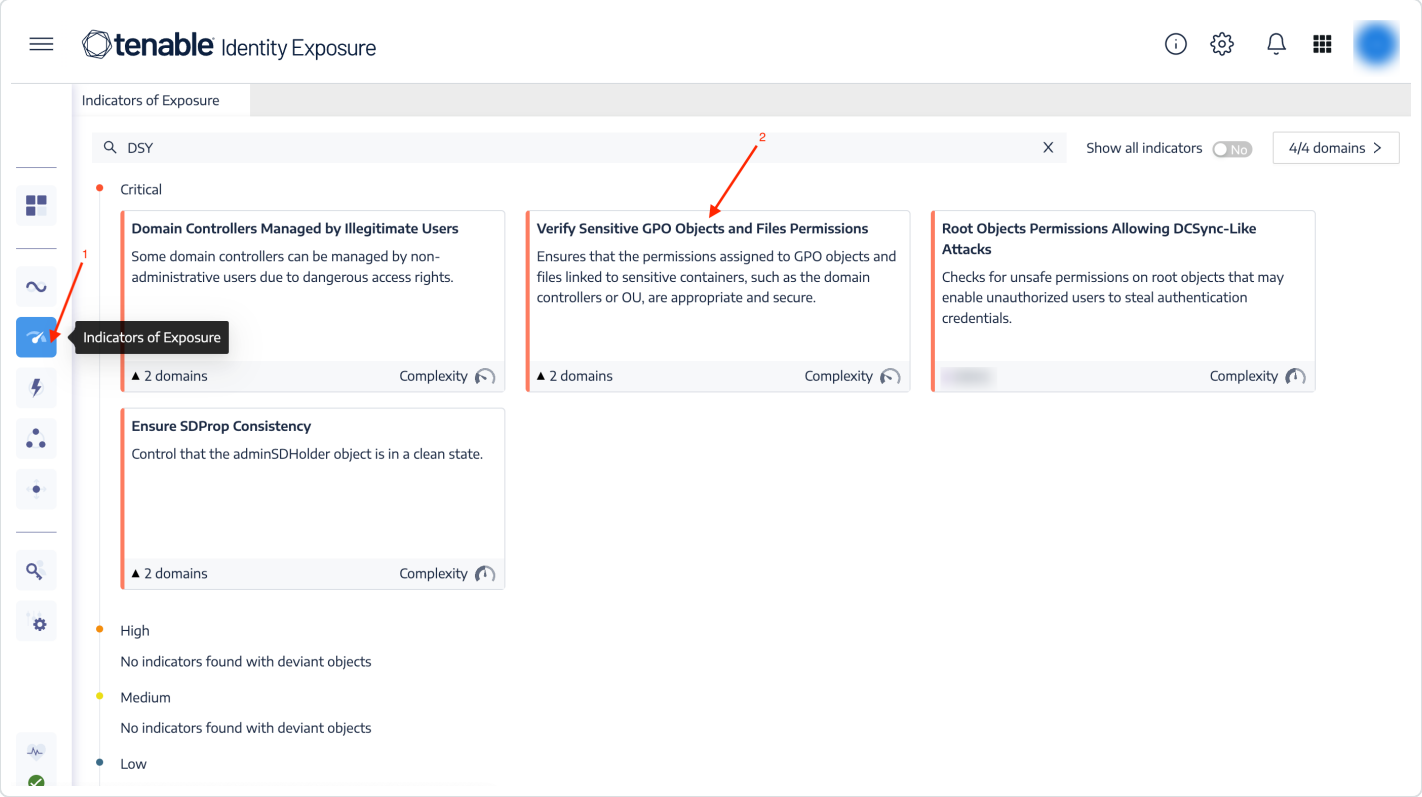


Group and File Permissions

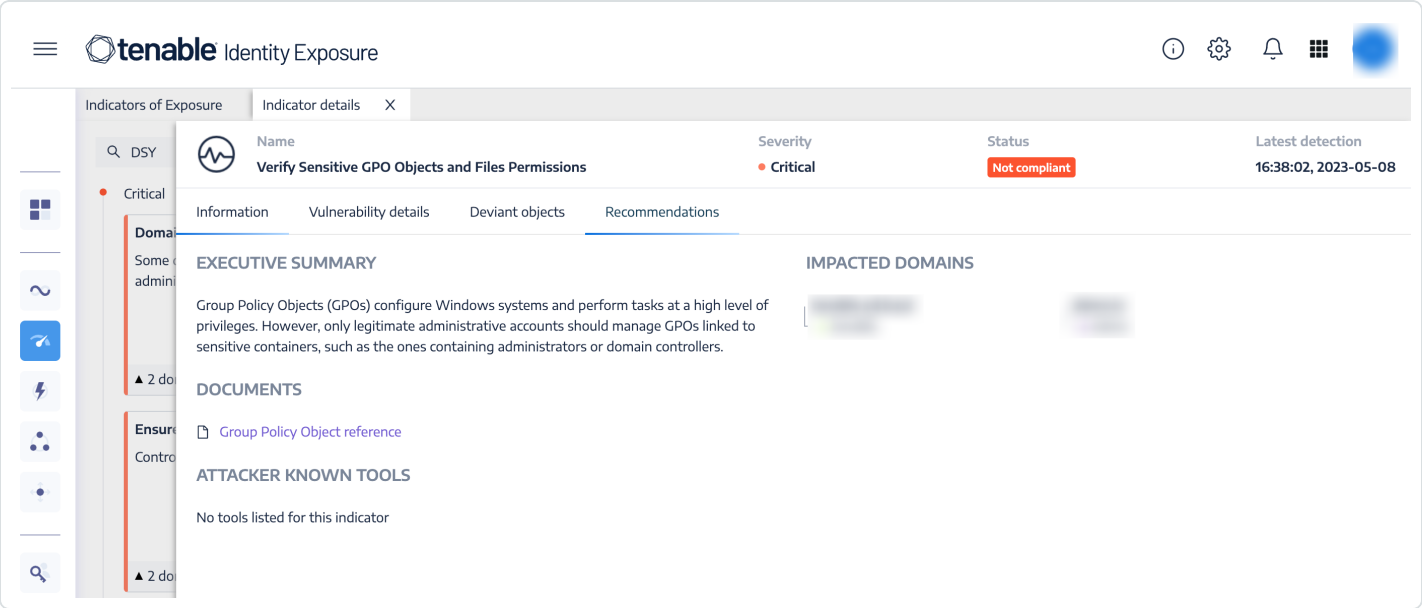
The following Indicators of Exposure (IoE) in Tenable Identity Exposure can be leveraged to determine exposures in group and file permissions:

- Verify Sensitive GPO Objects and File Permissions (Critical)
- User Primary Group (Critical)
- Verify Permissions Related to AAD (Azure Active Directory) Connect Accounts (Critical)
- Root Objects Permissions Allowing DCSync-Like Attacks (Critical)
- Users Allowed to Join Computers to the Domain (Medium)

Step 1: From the Indicators of Exposure tab in Identity Management, search for the above listed IoEs in the search field as shown below:



Step 2: Click on one of the displayed tiles to drill down into more details, as shown below:


tenable Identity Exposure
Indicators of Exposure
Indicator details
DSY
Critical
Name
Verify Sensitive GPO Objects and Files Permissions
Severity
Critical
Status
Not compliant
Latest detection
16:38:02, 2023-05-08
Information
Vulnerability details
Deviant objects
Recommendations
EXECUTIVE SUMMARY
Group Policy Objects (GPOs) configure Windows systems and perform tasks at a high level of privileges. However, only legitimate administrative accounts should manage GPOs linked to sensitive containers, such as the ones containing administrators or domain controllers.
DOCUMENTS
Group Policy Object reference
ATTACKER KNOWN TOOLS
No tools listed for this indicator
IMPACTED DOMAINS

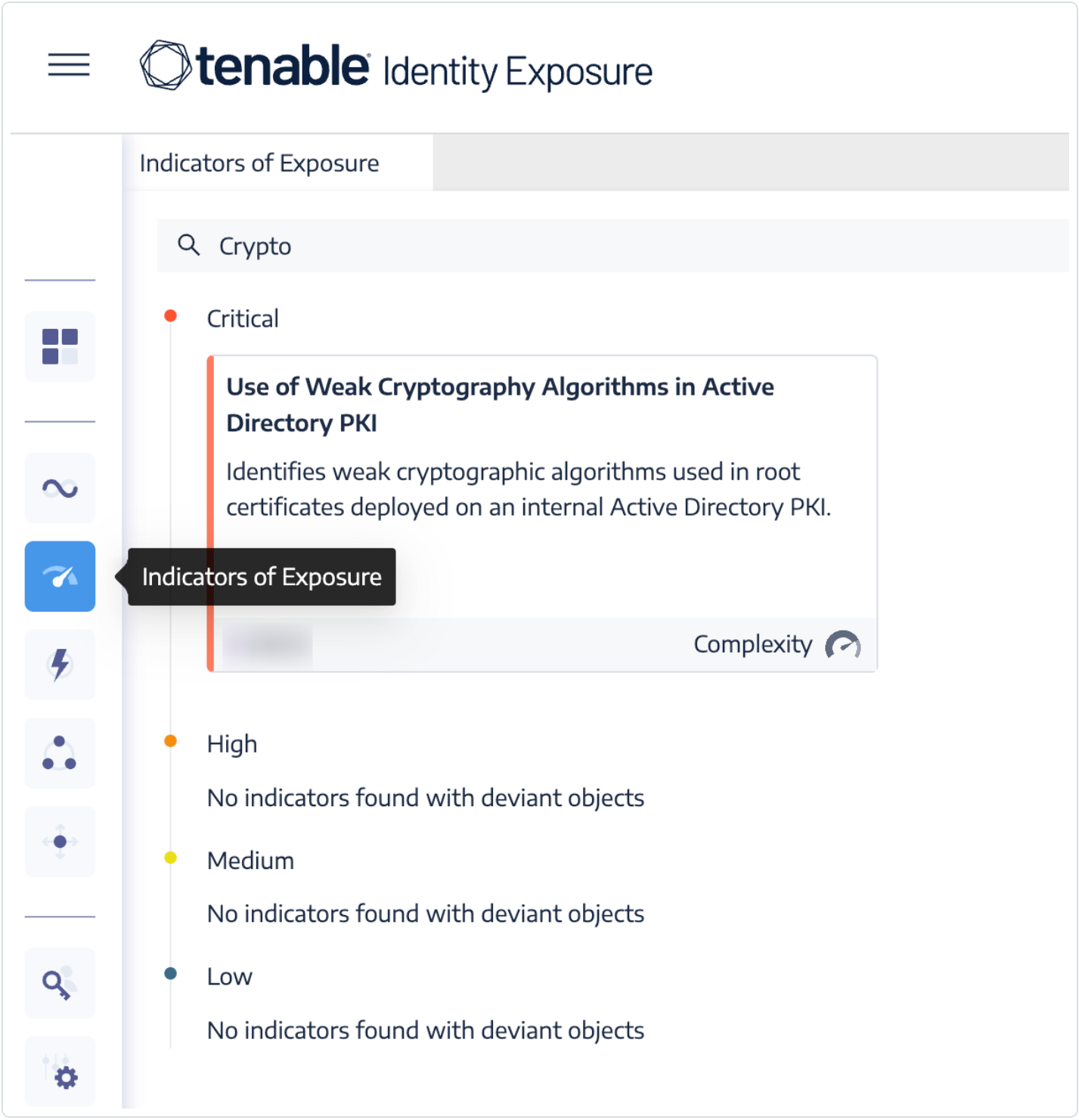
Cryptographic Controls

Applications and servers often support SSL/TLS key exchanges that are cryptographically weaker than recommended. Key exchanges must be recommended by IANA and provide at least 224 bits of security, which translates to a minimum key size of 2048 bits for Diffie Hellman and RSA key exchanges.Nessus has over 1000 plugins that identify vulnerabilities with SSH/OpenSSH, and other cipher suites.

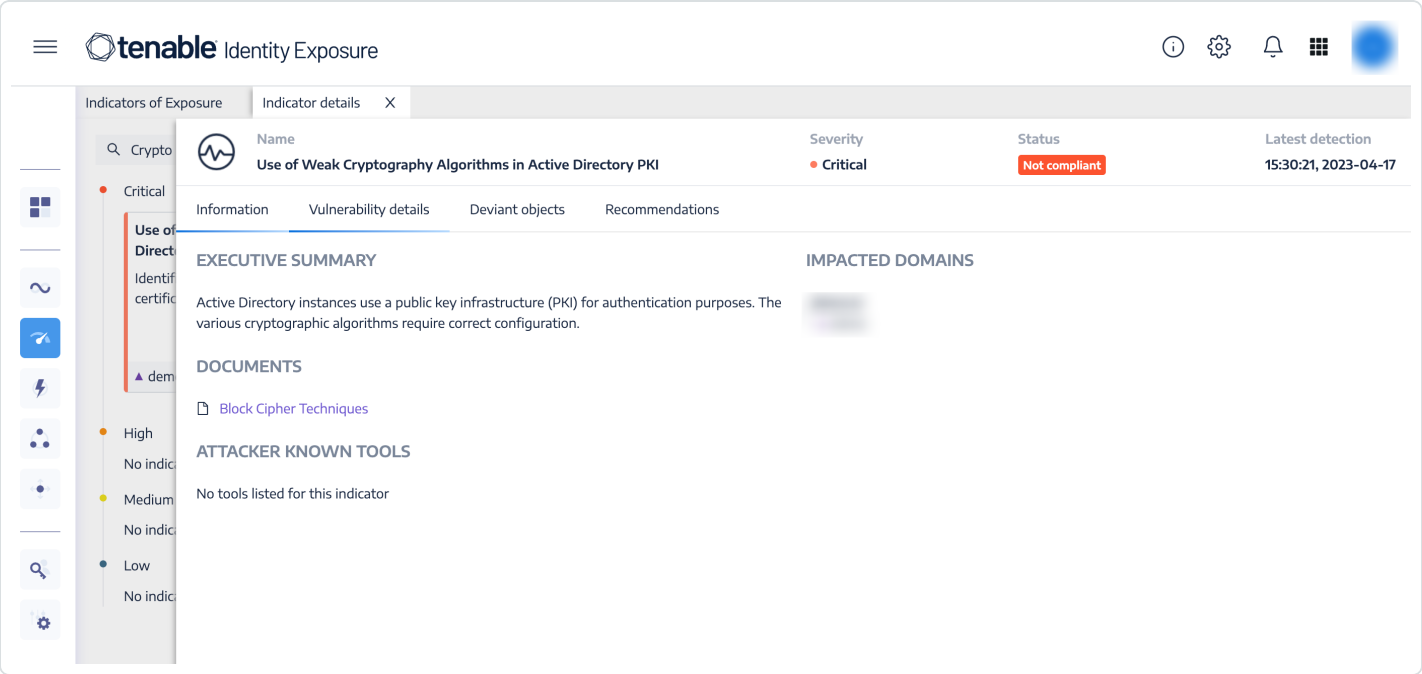
Tenable Identity Exposure has the following Indicators of Exposure to evaluate cryptographic controls:

- ADCS (Active Directory Certificate Services) Dangerous Misconfigurations (Critical)
- Use of Weak Cryptography Algorithms into Active Directory PKI (Critical)
- Reversible Passwords (Medium)
- Vulnerable Credential Roaming Related Attributes (Low)

Step 1: From the Indicators of Exposure tab in Identity Management, search for the above listed IoEs in the search field as shown below:



Step 2: Click on one of the displayed tiles to drill down into more details, as shown below:


tenable Identity Exposure
Indicators of Exposure
Indicator details
Crypto
Critical
Use of
Direct
Identif
certific
dem
High
No indic
Medium
No indic
Low
No indic
Name
Use of Weak Cryptography Algorithms in Active Directory PKI
Severity
Critical
Status
Not compliant
Latest detection
15:30:21, 2023-04-17
Information
Vulnerability details
Deviant objects
Recommendations
EXECUTIVE SUMMARY
Active Directory instances use a public key infrastructure (PKI) for authentication purposes. The various cryptographic algorithms require correct configuration.
DOCUMENTS
Block Cipher Techniques
ATTACKER KNOWN TOOLS
No tools listed for this indicator
IMPACTED DOMAINS

Maintenance

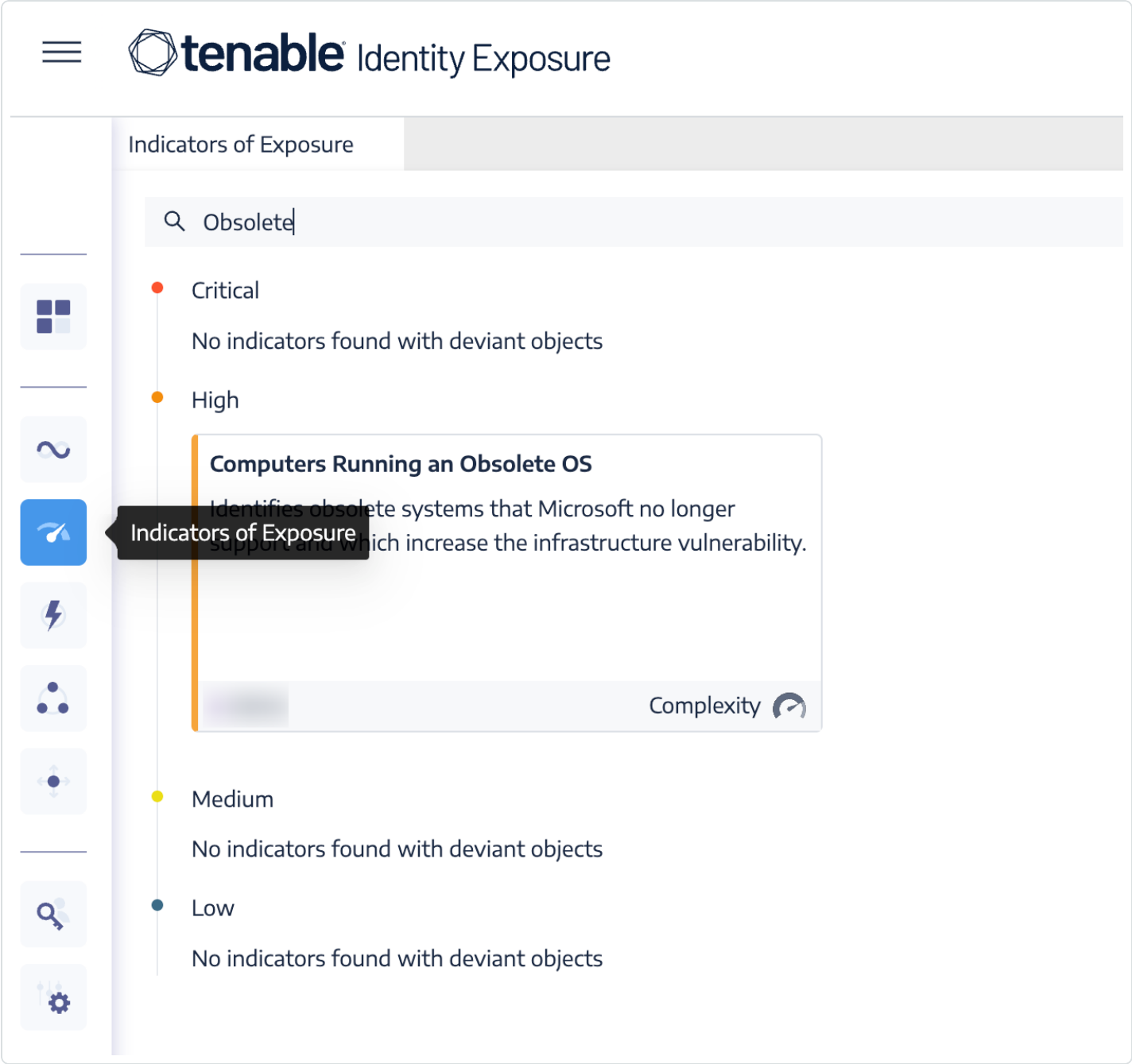
Every structure – physical or virtual – requires maintenance to maintain structural integrity over time. Even the most hardened infrastructure is subject to degradation with regular use. Tenable Security Center, Tenable Vulnerability Management and Tenable Identity Exposure provide comprehensive monitoring to detect drift from the desired state.

Administrator and user activity over time degrades security controls, if the system is not maintained properly. Regular scanning of the environment using the Nessus audit files identifies drift in security controls.

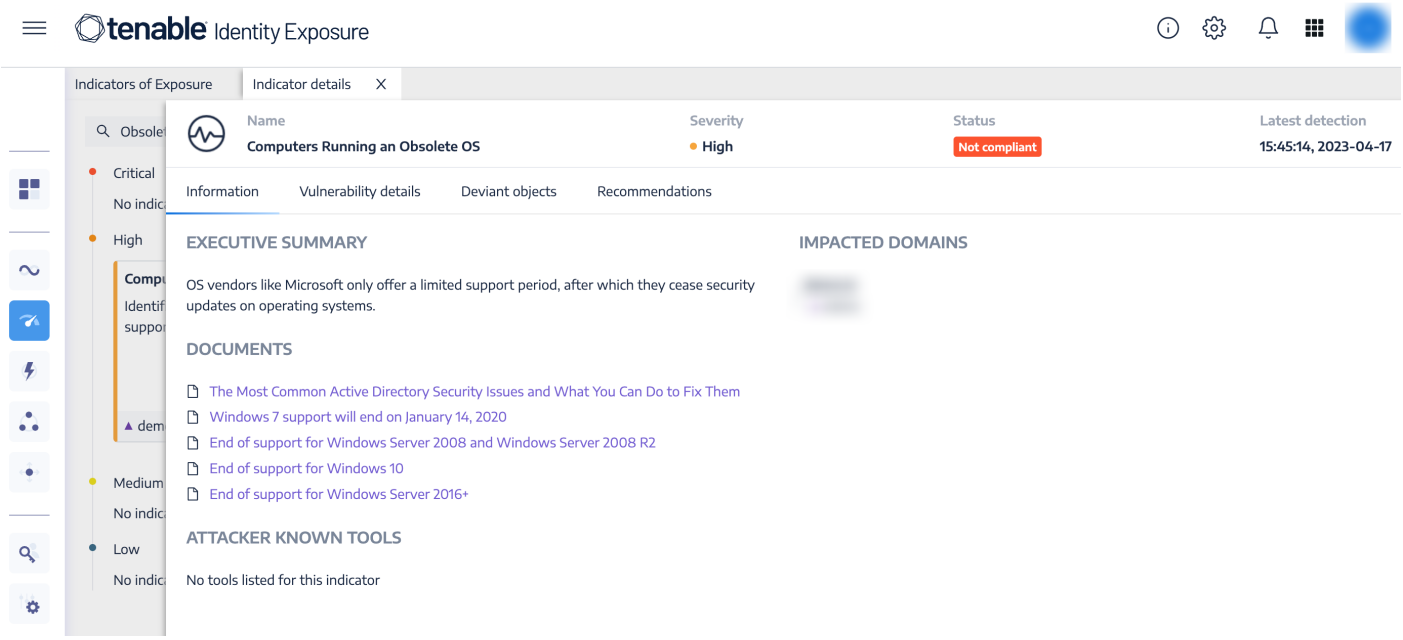
The following Indicators of Exposure (IoE) in Tenable Identity Exposure can be used to identify maintenance issues in Active Directory:

- Computers Running an Obsolete OS (High)
- Disabled Accounts in Privileged Groups (Low)
- Unlinked, Disabled or Orphan GPO (Low)

Step 1: From the Indicators of Exposure tab in Identity Management, search for the above listed IoEs in the search field as shown below:



Step 2: Click on one of the displayed tiles to drill down into more details, as shown below:



Security leaders need to **SEE** everything, **PREDICT** what matters most, and **ACT** to address cyber risk and effectively align cyber security initiatives with business objectives. Tenable Security Center, Tenable Vulnerability Management and Tenable Identity Exposure discover and analyze assets continuously to provide an accurate and unified view of an organization's identity and access management controls.

Learn More

Tenable Resources

- Getting Started with Tenable Identity Exposure
- Getting Started with Active Directory
- Tenable Plugins Page
- Tenable Indicators of Attack
- Tenable Indicators of Exposure

External Resources

- Center for Internet Security (CIS)
- Microsoft: Monitoring Active Directory for Signs of Compromise
- Microsoft: Securing Active Directory Administrative Groups and Accounts
- Microsoft: Azure AD Connect: Accounts and Permissions
- Microsoft: Privileged Accounts and Groups in Active Directory
- Microsoft: Reducing the Active Directory Attack Surface (Privileged Accounts and Groups in Active Directory)
- Microsoft: Securing Privileged Access
- Microsoft: Who Can Add Workstation to the Domain
- MITRE ATT&CK: Steal or Forge Kerberos Tickets: Kerberoasting