netwrix

Netwrix Auditor

Избранные встроенные отчеты

Содержание

Содержание

Содержание

Содержание

Содержание

Оценка IT рисков

IT Risk Assessment Overview

Отчет обеспечивает детальный обзор имеющихся IT рисков. Контролируйте риски и снижайте их, непрерывно отслеживая и устраняя слабые места в среде, такие как хаотично организованная структура привилегий, теневые учетные записи пользователей и компьютеров, неправильное содержимое общих файловых ресурсов.

Total risk level for Users and Computers: ■ Take action

Risk	Ratio	Level
User accounts with Password never expires	23	■ Take action
User accounts with Password not required	0	■ Acceptable
Disabled computer accounts	3 of 22 (13.6%)	■ Take action
Inactive user accounts	0	■ Acceptable
Inactive computer accounts	9 of 19 (47.4%)	■ Take action

Total risk level for Permissions: ■ Take action

Risk	Ratio	Level
User accounts with administrative permissions	23 of 39 (59%)	■ Take action
Administrative groups	9 of 84 (10.7%)	■ Take action
Empty security groups	51 of 84 (60.7%)	■ Take action

Total risk level for Data: ■ Take action

Risk	Ratio	Level
Shared folders accessible by Everyone	1 of 32 (3.1%)	■ Pay attention
File names containing sensitive data	15	■ Take action
Potentially harmful files on file shares	16	■ Take action
Direct permissions on files and folders	205 of 205 (100%)	■ Take action

Анализ поведения пользователей и "слепых зон"

Data Access Trend

Отчет содержит сводную статистику по использованию данных на файловых серверах и серверах SharePoint. Отслеживайте всплески активности, предотвращайте потенциальные угрозы безопасности данных.

Creation of Files with Sensitive Data

Отчет собирает данные по пользователям, которые создают файлы с ценной информацией, присваивая этим файлам соответствующие названия: например, "МоиПароли.docx". Формируйте этот отчет, чтобы отслеживать появление таких файлов, а также, чтобы обеспечить защиту подобных документов. Некоторые слова запрещены по умолчанию: password, social security number, credit card, cardholder, payment, payroll.

Filter	Value

What	User Name	Actions	When Created
\\fs1\shared\Accounting**PWD**.docx	ENTERPRISE\T.Simpson	9	6/14/2016 2:19:18 PM
\\fs1\shared\IT**PASSWORD**.txt	ENTERPRISE\J.Carter	2	8/9/2016 3:06:11 AM
\\fs1\shared\Office**SSN**.xlsx	ENTERPRISE\J.Brown	2	8/22/2016 4:33:46 PM
\\fs1\shared\Accounting**payment**.xlsx	ENTERPRISE\G.Law	2	8/25/2016 3:04:31 AM

Activity Outside Business Hours

Отчет содержит данные по всем пользователям, которые проявляют активность в сети в нерабочее время. Используйте отчет для выявления подозрительной активности.

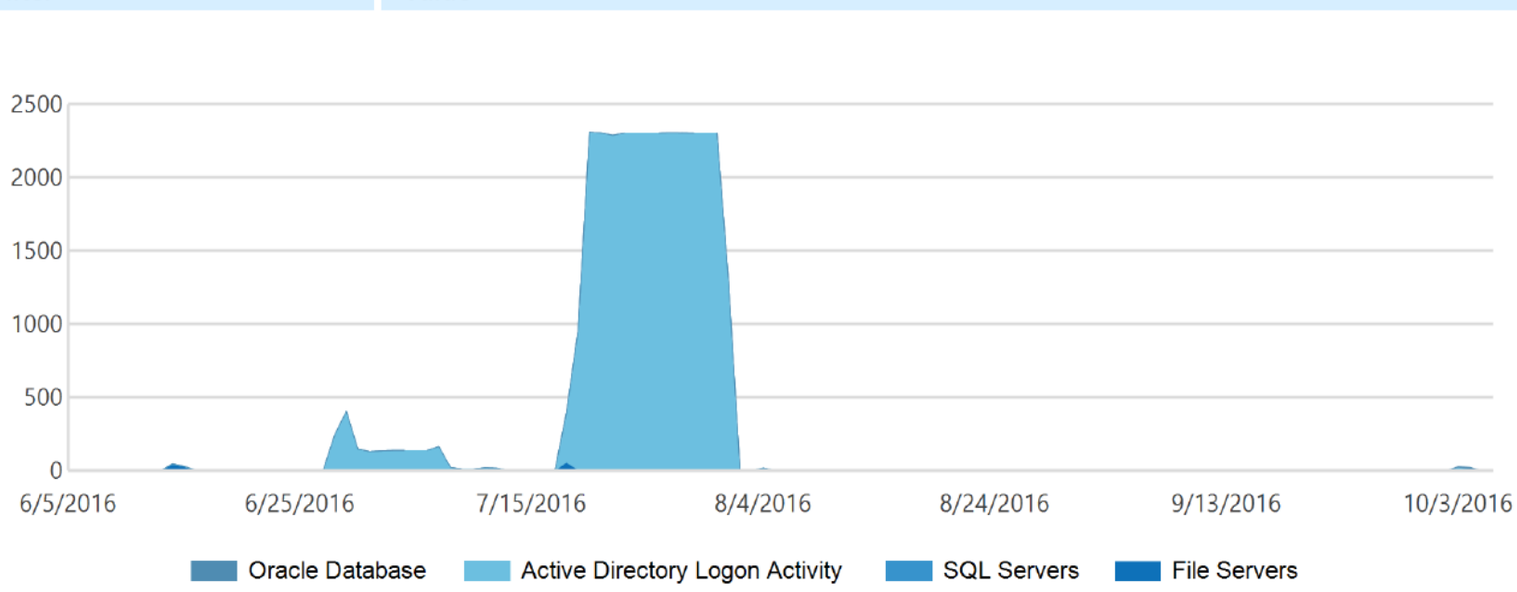
Filter	Value

Who	Actions
ENTERPRISE\P.Smith	171
ENTERPRISE\J.Carter	64
ENTERPRISE\T.Simpson	22
ENTERPRISE\B.Johnson	9

Failed Activity Trend

Отчет показывает сводную статистику по всем неудачным действиям: неудачные попытки чтения или модификации файлов, неудачные попытки входа в систему и т. д. Отчет также содержит список пользователей с наибольшим количеством подобных инцидентов. Определенное количество неудачных попыток неизбежно во время работы, но внезапный резкий (или постепенный) рост такой активности может свидетельствовать о вирусе или атаке.

Filter	Value



Date: 6/14/2016 (Attempts: 40)

Who	Attempts
ENTERPRISE\G.Brown	33
ENTERPRISE\T.Simpson	7

Potentially Harmful Files – Activity

Отчет показывает доступ к потенциально вредоносным файлам (установщики, скрипты и reg-файлы) на ваших файловых ресурсах и сайтах SharePoint, а также изменения, вносимые в эти файлы. Эти файлы могут быть вирусами, поэтому не должны храниться на общих ресурсах. Используйте этот отчет для отслеживания инцидентов и предотвращения угроз безопасности.

Filter	Value

Audited System: File Servers

Action	What	Who	When
Added	\\192.168.10.200\ifs\share\Distrib\Dell Change Auditor Agent 6 (x64).msi	ENTERPRISE \J.Carter	5/4/2016 2:43:32 PM
Read	\\fs1\shared\Dev\isass.inf	ENTERPRISE \J.Carter	5/4/2016 2:43:32 PM
Read	\\fs1\shared\Managers\nvcpl.exe	ENTERPRISE \J.Carter	5/4/2016 2:43:35 PM
Added	\\192.168.10.200\ifs\shared\Managers\nvcpl.exe	ENTERPRISE \J.Carter	5/4/2016 2:43:35 PM
Read	\\fs1\shared\PM\crss.hta	ENTERPRISE \J.Carter	5/4/2016 2:43:37 PM

Logons by Single User from Multiple Endpoints

Отчет содержит данные по пользователям, которые вошли в систему с нескольких рабочих станций в течение короткого периода времени. Подобные инциденты могут свидетельствовать о краже пароля УЗ. Используйте отчет для выявления подозрительных действий пользователей и предотвращения утечки данных.

Filter	Value

Who: ENTERPRISE\J.Carter (First Attempt: 10/6/2016 12:30:09 PM)

Endpoint	Logon Attempts
192.168.10.25	17
ENTWKS0376	15

Who: ENTERPRISE\T.Simpson (First Attempt: 10/6/2016 12:29:07 PM)

Endpoint	Logon Attempts
ENTWKS0376	9
172.17.4.12	7

Идентификация и классификация данных

Sensitive Files Count by Source

Отчет показывает количество файлов, содержащих определенные категории конфиденциальных данных. При нажатии на ссылку " "Categories" или "Source" ваши результаты сужаются до определенного файла в отчете. Используйте отчет для оценки объема конфиденциальных данных в каждой категории и для планирования мер по защите данных.

Content source	Categories	Files count
\\FILESRV07\Accounting	PCI DSS	527
\\FILESRV07\Finance	HIPAA	7
	PCI DSS	310
\\FILESRV07\HR	GDPR	13734
	PCI DSS	1
\\FILESRV07\Marketing	PCI DSS	5
\\FILESRV07\Public	GDPR	2
	HIPAA	2
	PCI DSS	41

Sensitive Files and Folders by Owner

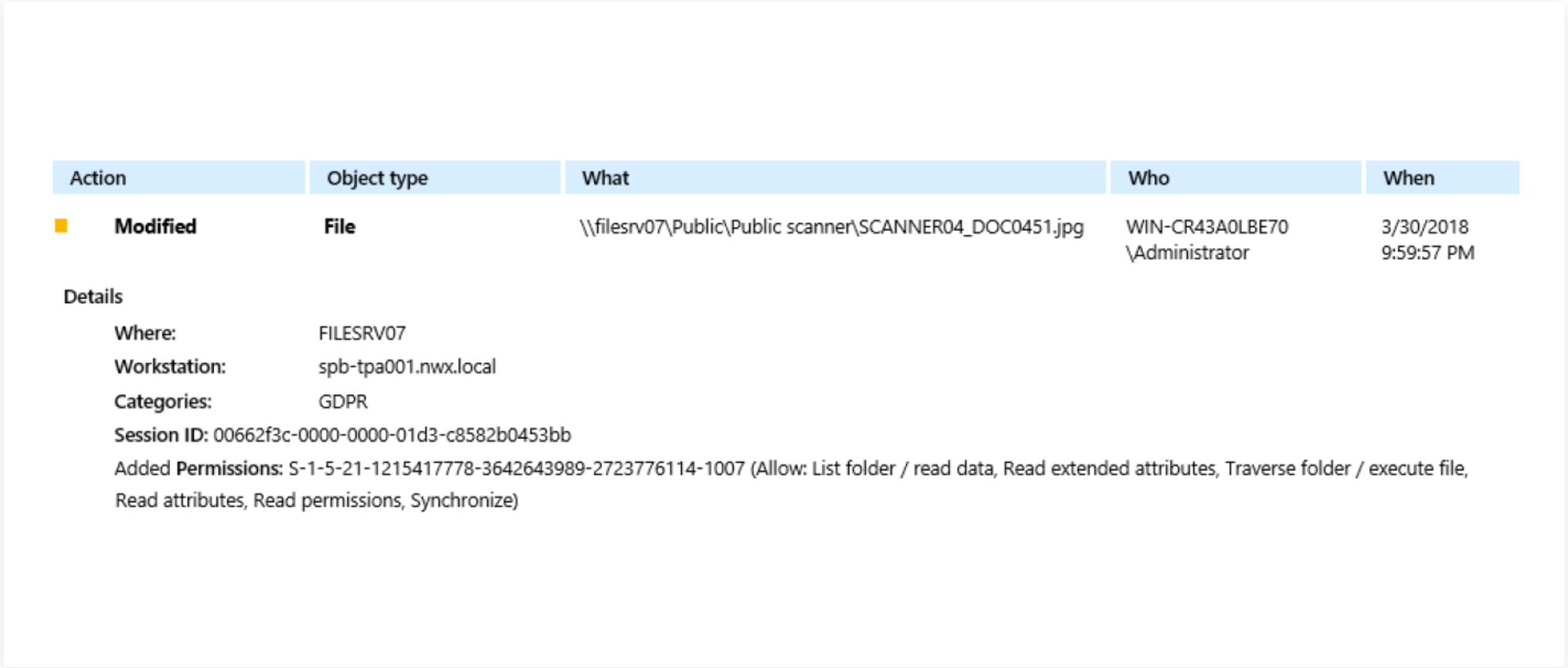
Отчет показывает владельцев файлов и папок, которые хранятся в указанной общей папке и содержат выбранные категории конфиденциальных данных.

Owner: WIN-CR43A0LBE70\Antonio Velazco

UNC path	Categories
\\filesrv07\Public\Incoming	GDPR HIPAA PCI DSS
\\filesrv07\Public\Incoming\licenses registry.xlsx	GDPR
\\filesrv07\Public\Incoming\Personal card.rtf	PCI DSS
\\filesrv07\Public\4Accounting!\urgent_payment.txt	PCI DSS
\\filesrv07\Public\Microsoft Outlook.msg	HIPAA

Activity Related to Sensitive Files and Folders

Показывает все попытки доступа (неудачные и успешные изменения, успешные и неудачные попытки чтения) к файлам и папкам, содержащим определенные категории конфиденциальных данных.



Action	Object type	What	Who	When
Modified	**File**	\\filesrv07\Public\Public scanner\SCANNER04_DOC0451.jpg	WIN-CR43A0LBE70 \Administrator	3/30/2018 9:59:57 PM

Details

Where: FILESRV07

Workstation: spb-tpa001.nwx.local

Categories: GDPR

Session ID: 00662f3c-0000-0000-01d3-c8582b0453bb

Added **Permissions:** S-1-5-21-1215417778-3642643989-2723776114-1007 (Allow: List folder / read data, Read extended attributes, Traverse folder / execute file, Read attributes, Read permissions, Synchronize)

netwrix

Netwrix Auditor

for Active Directory

All Active Directory Changes

Отчет по изменениям всех атрибутов всех объектов AD, добавленных, удаленных и измененных объектах. Самый популярный отчет для оценки состоянии Active Directory. Большой набор фильтров для поиска событий.

Filter	Value

Action	Object Type	What	Who	When
Removed	**user**	\com\enterprise\Managers\Bill Smith	ENTERPRISE\T.Simpson	3/17/2016 7:15:51 AM
Where:	dc1.enterprise.com			
Workstation:	172.17.5.32			
Modified	**group**	\com\enterprise\Users\Managers	ENTERPRISE\T.Simpson	3/17/2016 7:15:52 AM
Where:	dc1.enterprise.com			
Workstation:	172.17.5.32			

Security Local Group Member:

- **Removed:** "enterprise.com/Managers/Glen Johnson"

Administrative Group Membership Changes

Отчет содержит данные по изменению членства в административных группах, таких как: Domain Admins, Enterprise Admins, Schema Admins, Account Operators и т.д. Члены данных групп имеют право на ключевые действия в вашей ИТ-инфраструктуре. Подпишитесь на этот отчет, обеспечьте достаточный уровень безопасности вашей системы, следите за соблюдением политик безопасности вашей компании.

Filter	Value

Group name: \com\enterprise\Users\Domain Admins

Action	Member	Who	When
Removed	enterprise.com/Users/Harry Malicious	ENTERPRISE\T.Simpson	12/7/2015 3:14:35 PM
Where:	dc1.enterprise.com		
Added	enterprise.com/Users/Kenny Smith	ENTERPRISE\J.Carter	12/10/2015 5:49:00 PM
Where:	dc1.enterprise.com		
Added	enterprise.com/Users/Peter Anderson	ENTERPRISE\T.Simpson	1/13/2016 12:43:00 PM
Where:	dc1.enterprise.com		

User Accounts Status Changes

Изменение статуса УЗ пользователей (включена/отключена, заблокирована/разблокирована).

Filter	Value

Total Count: 7

Who: ENTERPRISE\J.Carter

Action	What	When
Enable	\com\enterprise\Users\George Black	4/4/2016 3:37:58 PM
Where:	DC1.enterprise.com	

Who: ENTERPRISE\T.Simpson

Action	What	When
Locked	\com\enterprise\Users\George Black	3/1/2016 3:01:03 PM
Where:	DC1.enterprise.com	
Disable	\com\enterprise\Users\Mary Wells	3/1/2016 5:21:03 PM
Where:	DC1.enterprise.com	
Disable	\com\enterprise\Managers\Dean Galaher	3/7/2016 11:40:14 AM
Where:	DC1.enterprise.com	

All Group Policy Changes

Отчет содержит данные по изменениям всех объектов групповых политик, настроек, ссылок, прав доступа.

Filter	Value

Action	What	Who	When
Modified	Default Domain Controllers Policy	ENTERPRISE\J.Carter	3/15/2016 4:10:55 AM

Where:	dc1.enterprise.com
Workstation:	pl.enterprise.com
Path:	Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Advanced Audit Configuration/Account Logon
Modified	Policy: Audit Credential Validation; Setting: Failure -> Success, Failure;
Modified	Policy: Audit Kerberos Service Ticket Operations; Setting: Failure -> Success, Failure;
Path:	General/Details
Modified	Computer Revisions: 20 (AD), 20 (SYSVOL) -> 21 (AD), 21 (SYSVOL);

Accounts with Most Logon Activity

Отчет содержит данные об учетных записях пользователей с наибольшим количеством попыток входа в систему (включая данные о неудачных попытках входа).

Filter	Value

Who	All Logons	Successful Logons	Failed Logons
ENTERPRISE\J.Carter	280	280	0
ENTERPRISE\J.Smith	234	231	3
ENTERPRISE\T.Simpson	215	215	0
ENTERPRISE\P.Anderson	124	122	2

Failed Logons

Отображает все неудачные попытки аутентификации в Active Directory. Отчет важен для безопасности данных и прохождения аудита на соответствие ИБ стандартам.

Filter	Value

Logon Type	What	Who	When
Non-Interactive	N/A	J.Smith	4/15/2016 3:34:37 PM
Where:	dc1.enterprise.com		
Workstation:	entwks0321.enterprise.com		
Cause: User logon with misspelled or bad user account			
This entry represents 3 matching events occurring within 10 seconds.			
Non-Interactive	N/A	P.Anderson	4/15/2016 6:16:11 PM
Where:	dc1.enterprise.com		
Workstation:	entwks0421.enterprise.com		
Cause: User logon with misspelled or bad password			
This entry represents 2 matching events occurring within 10 seconds.			

Account Permissions in Active Directory (State-in-Time)

Отчет отображает объекты AD, имеющие неоднозначные или унаследованные права доступа, а также способ выдачи этих прав (напрямую или через членство в группе). Разрешения отображаются только для пользователей, принадлежащих к отслеживаемому домену. Можно перейти к отчету "Active Directory Account Permissions Details", щелкнув на имя конкретного объекта.

Account: \com\enterprise\Users\John Carter

Object Name	Object Type	Means Granted
\com\enterprise	domainDNS	Directly, Group, Everyone, Authenticated Users
\com\enterprise\Builtin	builtinDomain	Group
\com\enterprise\Builtin\Access Control Assistance Operators	group	Group, Authenticated Users
\com\enterprise\Builtin\Account Operators	group	Group
\com\enterprise\Builtin\Administrators	group	Group
\com\enterprise\Builtin\Backup Operators	group	Group

Group Members (State-in-Time)

Отчет содержит данные по всем членам выбранной группы, с указанием типа объекта (пользователь, группа, компьютер) и статуса (включен/выключен).

Filter	Value
Security Global Group:	**\com\enterprise\Managers\Managers**

Member Path	Type	Status
\com\enterprise\Managers\Charles Hoffman	user	Enabled
\com\enterprise\Managers\Dean Galaher	user	Enabled
\com\enterprise\Users\Harry Malicious	user	Enabled

Administrative Group Members (State-in-Time)

Списки членов групп Domain Admins и Enterprise Admins, с указанием типа (пользователь, группа и т.д.) и статуса (включен/отключен) для каждого члена группы.

Filter	Value

Group Path: \com\enterprise\Users\Enterprise Admins

Member Path	Type	Status
\com\enterprise\Users\Administrator	user	Disabled
\com\enterprise\Users\John Carter	user	Enabled
\com\enterprise\Users\Tom Simpson	user	Enabled

Group Path: \com\enterprise\Users\Domain Admins

Member Path	Type	Status
\com\enterprise\Inactive Users\Kenny Smith	user	Disabled
\com\enterprise\Users\Administrator	user	Disabled
\com\enterprise\Users\Harry Malicious	user	Disabled
\com\enterprise\Users\John Carter	user	Enabled

User Accounts-Passwords Never Expire (State-in-Time)

Список учетных записей, пароли для которых не имеют срока действия, с указанием расположения и стутуса УЗ (включена/выключена).

Filter	Value

Path	Status
\com\enterprise\Inactive Users\Alex Terry	Disabled
\com\enterprise\Inactive Users\Bill Atkins	Disabled
\com\enterprise\Managers\Eugenia Anderson	Enabled
\com\enterprise\Users\Dian Harris	Enabled
\com\enterprise\Users\Guest	Enabled
\com\enterprise\Users\John Carter	Enabled
\com\enterprise\Users\Kenny Smith	Disabled

Group Policy Objects by Policy Name (State-in-Time)

Отчет представляет собой список всех объектов групповой политики, с указанием настроек для каждого объекта и их значения.

Filter	Value

Policy Name: Account enabled

Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Local Policies/Audit Policy
Policy: Audit account management; Setting: Success, Failure;

General/Delegation
Name: ENTERPRISE\Domain Admins; Allowed Permissions: Edit settings, delete, modify security; Inherited: No;
Name: ENTERPRISE\Enterprise Admins; Allowed Permissions: Edit settings, delete, modify security; Inherited: No;
Name: NT AUTHORITY\Authenticated Users; Allowed Permissions: Read (from Security Filtering); Inherited: No;
Name: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS; Allowed Permissions: Read; Inherited: No;
Name: NT AUTHORITY\SYSTEM; Allowed Permissions: Edit settings, delete, modify security; Inherited: No;

General/Details
Computer Revisions: 4 (AD), 4 (SYSVOL);
Created: 12/9/2015 3:15:32 AM;
Display Name: Account enabled;

netwrix

Netwrix Auditor for Azure AD

Azure AD Logon Activity

Список успешных и неудачных событий входа пользователей в Azure AD.

Filter	Value

Action	Who	When
Successful Logon	T.Simpson@enterprise.onmicrosoft.com	10/5/2016 2:45:05 AM

Where: enterprise.onmicrosoft.com
Client IP: 12.95.21.122
Client: Exchange
Login Status: 0
User Domain: enterprise.onmicrosoft.com
Origin: Azure AD

Failed Logon	J.Carter@enterprise.onmicrosoft.com	10/5/2016 6:12:16 AM

Where: enterprise.onmicrosoft.com**Client IP:** 12.95.21.123
Client: Exchange
Login Status: 0
User Domain: enterprise.onmicrosoft.com
Origin: Azure AD

Group Membership Changes in Azure AD

Отчет содержит данные по всем изменениям состава групп в Azure AD. Используйте его для обеспечения безопасности ваших данных.

Filter	Value

What	Who	When
Office Group **Where:** enterprise.onmicrosoft.com **Member:** • **Added**: "Adam Jones"	T.Simpson@enterprise.onmicrosoft.com	10/1/2016 10:42:38 AM
Managers **Where:** enterprise.onmicrosoft.com **Member:** • **Removed**: "Adam Jones"	T.Simpson@enterprise.onmicrosoft.com	10/1/2016 10:42:18 AM
Production **Where:** enterprise.onmicrosoft.com **Member:** • **Added**: "Glen Johnson"	J.Carter@enterprise.onmicrosoft.com	10/1/2016 10:14:58 AM

User Account Management in Azure AD

Отчет по изменениям учетных записей пользователей в Azure AD, включая создание УЗ, модификацию или удаление.

Filter	Value

Action	What	Who	When
Added	Tom Smith	N.Hamphry@enterprise.onmicrosoft.com	10/1/2016 10:41:01 AM

Where: enterprise.onmicrosoft.com

Account Enabled: "False"

Dir Sync Enabled: "True"

Display Name: "T.Smith"

Mail Nickname: "T.Smith"

On Premises Security Identifier: "S-1-5-21-270264179-917534861-3001894179-126647"

User Principal Name: "T.Smith@enterprise.onmicrosoft.com"

User Type: "Member"

Origin: On-premises Active Directory

User Accounts Created and Deleted Directly in Azure AD

Отчет показывает учетные записи пользователей, которые были созданы или удалены напрямую в Azure AD, без использования локальной версии Activer Directory. Изменения, внесенные непосредственно в Azure AD, представляют потенциальную угрозу безопасности. Используйте этот отчет, чтобы вычислить злоумышленников, пытающихся скрыть вредоносную активность.

Filter	Value

Action	What	Who	When
Added	Tom Smith	J.Carter@enterprise.onmicrosoft.com	9/14/2016 3:06:34 AM

Where: enterprise.onmicrosoft.com
Account Enabled: "True"
Display Name: "T.Smith"
Mail Nickname: "T.Smith"
Password Policies: "None"
User Principal Name: "T.Smith@enterprise.onmicrosoft.com"
User Type: "Member"
Origin: Azure AD

netwrix

Netwrix Auditor

for Exchange

All Exchange Server Changes

Все изменения объектов, настроек и прав доступа на сервере Exchange.

Filter	Value

Action	Object Type	What	Who	When
Modified	**user**	\com\enterprise\Managers\Alex Terry	ENTERPRISE\J.Carter	11/5/2015 1:08:39 PM

Where: exchange.enterprise.com

Workstation: 192.168.10.5

Exchange Mailbox Security:

- **Added:** "FullAccess"

User changed to "T.Allen"

Action	Object Type	What	Who	When
Modified	**user**	\com\enterprise\Managers\Alex Terry	ENTERPRISE\T.Simpson	11/5/2015 1:08:40 PM

Where: exchange.enterprise.com

Exchange Mailbox Security:

- **Added:** "Permissions: ENTERPRISE\T.Allen (Allow: Create all child objects)"

msExchDelegateListLink:

- **Added:** "CN=Tom Allen,OU=Production,DC=enterprise,DC=com"

Action	Object Type	What	Who	When
Modified	**user**	\com\enterprise\Users\Help Desk	ENTERPRISE\J.Carter	12/10/2015 5:55:52 PM

Where: exchange.enterprise.com

Workstation: 192.168.10.3

Mailbox Created

Proxy Addresses changed to "SMTP:helpdesk@enterprise.com"

Mailbox Delegation and Permissions Changes

Список изменений прав доступа и делегирования почтового ящика.

Filter	Value

Who: ENTERPRISE\J.Carter

Action	Object Type	What	When
Modified	**user**	\com\enterprise\Managers\Alex Terry	10/26/2015 12:33:45 PM

Where: exchange.enterprise.com

Exchange Mailbox Security:
- **Added**: "FullAccess"

User changed to "J.Carter"

Modified	**user**	\com\enterprise\Managers\Alex Terry	10/26/2015 1:01:59 PM

Where: exchange.enterprise.com

Exchange Mailbox Security:
- **Added**: "FullAccess"

User changed to "T.Simpson"

Modified	**user**	\com\enterprise\Managers\Alex Terry	11/5/2015 1:08:39 PM

Where: exchange.enterprise.com

Exchange Mailbox Security:
- **Added**: "FullAccess"

User changed to "T.Allen"

All Exchange Server Non-Owner Mailbox Access Events

Отчет содержит информацию по доступу к почтовым ящикам сторонними пользователями. Используйте этот отчет для выявления несанкционированных действий и защиты Exchange.

Filter	Value

Action	Object Type	What	Who	When
Read	**Mailbox Folder**	T.Simpson@enterprise.com\Drafts	John Carter	3/18/2016 4:44:31 AM
Where: exchange.enterprise.com **Client:** Outlook Web Access **Client IP:**192.168.10.45				
Added	**Mailbox Item**	T.Simpson@enterpriseoft.com\Contacts \Recipient Cache\Tom Simpson	John Carter	3/18/2016 4:45:12 AM
Where: exchange.enterprise.com **Client:** Outlook Web Access **Client IP:**192.168.10.45				
Added	**Mailbox Item**	T.Simpson@enterprise.com \Contacts\Recipient Cache \Harry Malicious	John Carter	3/18/2016 4:45:33 AM
Where: exchange.enterprise.com **Client:** Outlook Web Access **Client IP:**192.168.10.45				

Netwrix Auditor

for Office 365

All Exchange Online Changes

Все изменения объектов, настроек и прав доступа Exchange Online.

Filter	Value

Action	Object Type	What	Who	When
Modified	**Mailbox**	T.Simpson	J.Carter@enterprise2016.onmicrosoft.com	3/18/2016 4:11:31 AM

Where: DM3PR15MB0603

Access Rights:

- **Added:** "NAMPR15A001\J.Carter (FullAccess)"

Action	Object Type	What	Who	When
Modified	**Mailbox**	T.Anderson	J.Carter@enterprise2016.onmicrosoft.com	3/18/2016 4:29:06 AM

Where: DM3PR15MB0603

Access Rights:

- **Added:** "NAMPR15A001\J.Carter (FullAccess)"

Action	Object Type	What	Who	When
Modified	**Mailbox**	J.Carter	J.Carter@enterprise2016.onmicrosoft.com	3/18/2016 4:29:30 AM

Where: DM3PR15MB0603

First Name changed to "John"

Last Name changed to "Carter"

Exchange Online Mailbox Permission Changes

Список изменений в правах доступа к почтовому ящику.

Filter	Value

Who: J.Carter@enterprise2016.onmicrosoft.com

Action	What	When
Modified	T.Simpson	3/18/2016 4:11:31 AM
	Where: DM3PR15MB0603	
	Access Rights: • **Added:** "NAMPR15A001\B.Atkins (FullAccess)"	
Modified	T.Anderson	3/18/2016 4:29:06 AM
	Where: DM3PR15MB0603	
	Access Rights: • **Added:** "NAMPR15A001\B.Atkins (Read)"	

All Exchange Online Non-Owner Mailbox Access Events

Отчет содержит информацию по доступу к почтовым ящикам сторонними пользователями. Используйте этот отчет для выявления несанкционированных действий и защиты Exchange Online.

Action	Object Type	What	Who	When
Added	**Mailbox Item**	T.Simpson@enterprise2016.onmicrosoft.com\Drafts\security stuff **Where:** CY1PR15MB0217 **Client:** Outlook Web Access **Client IP:** 81.95.21.122	John Carter	3/18/2016 4:45:51 AM
Read	**Mailbox Folder**	A.Terry@enterprise2016.onmicrosoft.com\Inbox **Where:** BLUPR15MB0195 **Client:** Outlook Web Access **Client IP:** 81.95.21.122	Harry Malicious	3/18/2016 5:11:25 AM
Read	**Mailbox Folder**	A.Terry@enterprise2016.onmicrosoft.com\Inbox\Production **Where:** BLUPR15MB0195 **Client:** Outlook Web Access **Client IP:** 81.95.21.122	Harry Malicious	3/18/2016 5:11:32 AM

All SharePoint Online Activity by User

Отчет по изменениям и попыткам доступа к фермам Sharepoint Online.

Filter	Value

Who: T.Simpson@enterprise.onmicrosoft.com

Action	Object Type	What	When
Removed	**Document**	https://enterprise.sharepoint.com/Office/TempTT.docx	9/14/2016 10:23:18 AM
Where:	https://enterprise.sharepoint.com		
Workstation:	82.25.21.122		
Added	**Document**	https://enterprise.sharepoint.com/HR/Holidays.docx	9/14/2016 10:30:23 AM
Where:	https://enterprise.sharepoint.com		
Workstation:	82.25.21.122		
Modified	**Document**	https://enterprise.sharepoint.com/IT/VXManual.pdf	9/14/2016 10:30:28 AM
Where:	https://enterprise.sharepoint.com		
Workstation:	82.25.21.122		

Content Management

Отчет по изменениям контента (добавление, загрузка, модификации и т. д.) сайтов, списков, элементов списков и документов. Используйте отчет для выявления подозрительной активности и предотвращения потери важных данных.

Filter	Value			
Action	**Object Type**	**What**	**Who**	**When**
Added	**Document**	https://enterprise.sharepoint.com/IT/Virtual.xlsx	t.simpson@enterprise.onmicrosoft.com	9/12/2016 7:36:48 AM
Where:	https://enterprise.sharepoint.com/IT/			
Workstation:	82.25.21.122			
Added	**Document**	https://enterprise.sharepoint.com/IT/ALC.xlsx	t.simpson@enterprise.onmicrosoft.com	9/12/2016 7:37:09 AM
Where:	https://enterprise.sharepoint.com/IT/			
Workstation:	82.25.21.122			
Moved	**Document**	https://enterprise.sharepoint.com/IT/1471696404149.jpg	t.simpson@enterprise.onmicrosoft.com	9/12/2016 7:37:41 AM
Where:	https://enterprise.sharepoint.com/IT/			
Workstation:	82.25.21.122			
Url changed to "Shared/1471696404149.jpg"				

Data Access

Отчет показывает, какие пользователи просматривали списки SharePoint Online, пытались получить доступ к документам или загружали документы.

Filter	Value

What	Who	When
https://enterprise.sharepoint.com/sites/IT/VXManual.docx	T.Simpson@enterprise.onmicrosoft.com	10/6/2016 3:04:20 PM
Where: https://enterprise.sharepoint.com/sites/IT		
Workstation: 84.45.21.122		
https://enterprise.sharepoint.com/sites/IT/ACL.xlsx	T.Simpson@enterprise.onmicrosoft.com	10/6/2016 3:05:02 PM
Where: https://enterprise.sharepoint.com/sites/IT		
Workstation: 84.45.21.122		
https://enterprise.sharepoint.com/sites/Sales/Prices.docx	J.Carter@enterprise.onmicrosoft.com	10/6/2016 4:05:14 PM
Where: https://enterprise.sharepoint.com/sites/Sales		
Workstation: 41.68.113.81		

netwrix

Netwrix Auditor

for Windows File Server, for EMC, and for NetApp

File Server Changes

Данные по событиям на файловых серверах: изменение файлов, чтение, неудачные попытки прочтения и т.д.

Filter	Value

Action	Object Type	What	Who	When
Added	**File**	\\fs1\Shared\IT\New Text Document.txt	ENTERPRISE\ J.Carter	3/22/2016 10:45:40 AM

Where: fs1.enterprise.com

Modified	**Folder**	\\fs1\Shared\Managers	ENTERPRISE\ J.Carter	3/23/2016 4:44:22 AM

Where: fs1.enterprise.com

Permissions:

- **Added:** "ENTERPRISE\E.Anderson (Allow: List folder / read data, Read extended attributes, Traverse folder / execute file, Read attributes, Read permissions, Synchronize) Apply onto: This folder, subfolders and files"

Modified	**File**	\\fs1\Shared\Managers\KPI Q4 2015.rtf	ENTERPRISE\ J.Carter	3/23/2016 4:44:22 AM

Where: fs1.enterprise.com

Permissions:

- **Added:** "ENTERPRISE\E.Anderson (Allow: List folder / read data, Read extended attributes, Traverse folder / execute file, Read attributes, Read permissions, Synchronize)"

Permission Changes

Отчет по изменениям прав доступа к файлам, папкам и общим ресурсам. Отчет необходим для выявления несанкционированного доступа.

Filter	Value

Action	Object Type	What	Who	When
Modified	**Folder**	\\fs1\shared\IT	ENTERPRISE\ J.Carter	11/16/2015 4:08:49 PM

Where: fs1.enterprise.com

Permissions:

- **Added:** "ENTERPRISE\T.Simpson (Allow: List folder / read data, Create files / write data, Create folders / append data, Read extended attributes, Write extended attributes, Traverse folder / execute file, Delete subfolders and files, Read attributes, Write attributes, Delete, Read permissions, Change permissions, Take ownership, Synchronize) Apply onto: This folder, subfolders and files"

Action	Object Type	What	Who	When
Modified	**File**	\\fs1\shared\IT\manual.rtf	ENTERPRISE\ J.Carter	11/16/2015 4:08:49 PM

Where: fs1.enterprise.com

Permissions:

- **Added:** "ENTERPRISE\T.Simpson (Allow: List folder / read data, Create files / write data, Create folders / append data, Read extended attributes, Write extended attributes, Traverse folder / execute file, Delete subfolders and files, Read attributes, Write attributes, Delete, Read permissions, Change permissions, Take ownership, Synchronize)"

Successful File Reads

Отчет содержит данные по всем удачным попыткам прочтения файлов.

Action	Object Type	What	Who	When
Read	**File**	\\fs1\Shared\Managers\KPI Q4 2015.rtf	ENTERPRISE\ J.Carter	3/15/2016 4:15:05 AM
Where:	fs1.enterprise.com			
Read	**File**	\\fs1\Shared\Managers\log.txt	ENTERPRISE\ J.Carter	3/15/2016 4:15:35 AM
Where:	fs1.enterprise.com			
Read	**File**	\\fs1\Shared\QA Production\Alliance Plan.rtf	ENTERPRISE\ J.Carter	3/15/2016 4:17:11 AM
Where:	fs1.enterprise.com			
Read	**File**	\\fs1\Shared\QA Production\gpreport.html	ENTERPRISE\ J.Carter	3/15/2016 4:18:07 AM
Where:	fs1.enterprise.com			

Folder and File Permissions Details (State-in-Time)

Отчет показывает разрешения для папок и файлов (выданные напрямую или через членство в группе). Используйте отчет, чтобы увидеть, кто имеет доступ к определенной папке и ее содержимому, и показать объекты, имеющие разрешения, отличные от прав родительской папки. Локальные пользователи и группы файлового сервера не включены.

Object: \\FS1\Shared (Permissions: Different from parent)

Account	Permissions	Means Granted
ENTERPRISE\A.Kowalski	Read (Execute, List folder content)	Group
ENTERPRISE\A.Watson	Read (Execute, List folder content)	Group
ENTERPRISE\Admin1	Read (Execute, List folder content)	Group
ENTERPRISE\Administrator	Full Control	Group
ENTERPRISE\D.Harris	Full Control	Group
ENTERPRISE\D.Johnson	Full Control	Group

Account Permissions (State-in-Time)

Отчет содержит информацию по учетным записям и их правам доступа к файлам и папкам, с указанием способа получения прав: выданы напрямую или за счет членства в группе. Перейдя по ссылке в документе - вы сразу перейдете к отчету "Group Membership by User", в котором есть информация по всем группам в Active Directory, в которых пользователь состоит. Локальные учетные записи не включены в отчет.

Filter	Value

User Account: ENTERPRISE\J.Carter

Object Path	Permissions	Means Granted
\\192.168.10.200\ifs	Full Control	Directly
\\192.168.10.200\ifs\Distrib	Full Control	Directly
\\192.168.10.200\ifs\Finance	Full Control	Directly
\\192.168.10.200\ifs\Human Resources	Full Control	Directly
\\192.168.10.200\ifs\IT	Full Control	Directly
\\192.168.10.200\ifs\IT\New folder	Full Control	Directly
\\192.168.10.200\ifs\Managers	Full Control	Directly

Excessive Access Permissions (State-in-Time)

Показывает учетные записи с разрешениями к документам, которые редко используются. Используйте этот отчет, чтобы определить ненужные чрезмерные разрешения и снизить риски утечки данных.

Filter	Value

Object: \\fs1\shared (Permissions: Different from parent)

Account	Permissions	Means Granted	Times Accessed
ENTERPRISE\Administrator	Full Control	Group	0
ENTERPRISE\B.Atkins	Full Control	Group	0
ENTERPRISE\N.Key	Full Control	Group	0
ENTERPRISE\T.Simpson	Full Control	Group	0
NT AUTHORITY\SYSTEM	Full Control	Directly	0

Object: \\fs1\shared\Finance (Permissions: Different from parent)

Account	Permissions	Means Granted	Times Accessed
ENTERPRISE\A.Wiggin	Write and List folder content	Directly	0
ENTERPRISE\Administrator	Full Control	Group	0
ENTERPRISE\B.Atkins	Full Control	Group	0

Stale Data by Folder (State-in-Time)

Отчет содержит информацию о папках и файлах, с которыми не происходило никаких действий в течении определенного времени (по умолчанию: 180 дней).

Filter	Value

Folder	Owner	Unchanged Files	Unchanged Files Size (MB)
\\fs1\shared	ENTERPRISE \Administrators	7	48.3024
\\fs1\shared\Production	ENTERPRISE\J.Carter	2	48.2537
\\fs1\shared\Managers	ENTERPRISE\N.Key	1	0.0275
\\fs1\shared\Human Resources	ENTERPRISE\B.Atkins	2	0.0207
\\fs1\shared\Finance	ENTERPRISE\A.Terry	2	0.0005

Potential Data Owners by Folder (State-in-Time)

Отчет содержит данные о пользователях, которые часто обращаются к файлам в заданной папке.

Filter	Value

Folder: \\fs1\shared

Owner: BUILTIN\Administrators

Who	Changes	Reads
ENTERPRISE\J.Carter	97	431992
ENTERPRISE\A.Terry	68	0
ENTERPRISE\T.Simpson	18	75
ENTERPRISE\E.Anderson	0	5
ENTERPRISE\P.Morris	0	1
ENTERPRISE\H.Malls	0	13

Netwrix Auditor

for SharePoint

All SharePoint Changes

Отчет по изменениям и попыткам доступа к фермам Sharepoint, коллекции сайтов, приложениям, политикам, правам доступа, спискам, документам и т.д.

Filter	Value

Action	Object Type	What	Who	When
Modified	**Group**	Farm Administrators	ENTERPRISE\J.Carter	4/20/2016 6:36:55 PM

Where: http://sp01:4755

Members:

- **Added:** "ENTERPRISE\T.Simpson"

Added	**List Item**	http://sp01/Shared Documents "Human Resources"	ENTERPRISE\J.Carter	4/20/2016 6:50:48 PM

Where: http://sp01

Workstation: 192.168.10.25

Added	**Document**	http://sp01/Shared Documents/Human Resources/manual.rtf	ENTERPRISE\J.Carter	4/20/2016 6:51:20 PM

Where: http://sp01

Workstation: 192.168.10.25

SharePoint Content Changes by User

Отчет по изменениям контента сайтов, списков, элементов списков и документов, сгруппированным по пользователю, который внес изменения.

Filter	Value

Who: ENTERPRISE\J.Carter

Action	Object Type	What	When
Added	**List Item**	http://sp01/Shared Documents "Human Resources"	4/20/2016 6:50:48 PM
Workstation:	192.168.10.25		
Added	**Document**	http://sp01/Shared Documents/Human Resources/manual.rtf	4/20/2016 6:51:20 PM
Workstation:	192.168.10.25		
Added	**Document**	http://sp01/Shared Documents/Human Resources/project.docx	4/20/2016 6:51:42 PM
Workstation:	192.168.10.25		

SharePoint Read Access

Отчет содержит информацию по пользователям, которые просматривали документы на SharePoint.

Filter	Value

Object Type	What	Who	When
List	http://sp01/Lists/PublishedFeed	ENTERPRISE\J.Carter	4/20/2016 6:36:05 PM
Where:	http://sp01		
List	http://sp01/Lists/PublishedFeed	ENTERPRISE\A.Terry	4/20/2016 6:37:07 PM
Where:	http://sp01		
List	http://sp01/Lists/PublishedFeed	ENTERPRISE\N.Key	4/20/2016 6:40:07 PM
Where:	http://sp01		
List	http://sp01/Shared Documents/IT	ENTERPRISE\J.Carter	4/20/2016 7:04:23 PM
Where:	http://sp01		

netwrix

Netwrix Auditor

for Windows Server

All Windows Server Changes

Отчет по изменениям всех объектов и настроек Windows сервера, включая аппаратные устройства, драйверы ПО, службы, сетевые устройства, запланированные задачи, права доступа и т.д.

Filter	Value

Action	Object Type	What	Who	When
Modified	**Scheduled Task**	Scheduled Tasks\Microsoft\Windows\Customer Experience Improvement Program\Server \ServerCeipAssistant	ENTERPRISE\J.Carter	4/17/2016 1:30:34 AM

Where: ws1.enterprise.com

Triggers:

- **Added**: "At 4/18/2016 1:30:34 AM on 4/18/2016 1:30:34 AM - After triggered, repeat every 1.00:00:00 indefinitely."
- **Removed**: "At 4/17/2016 1:29:06 AM on 4/17/2016 1:29:06 AM - After triggered, repeat every 2.00:00:00 indefinitely."

Action	Object Type	What	Who	When
Modified	**Scheduled Task**	Scheduled Tasks\logon activity task	ENTERPRISE\T.Simpson	4/17/2016 2:12:55 AM

Where: dc1.enterprise.com

Triggers:

- **Added**: "At 4/18/2016 1:12:55 AM on 4/18/2016 1:12:55 AM - After triggered, repeat every 2.00:00:00 indefinitely."
- **Removed**: "At 4/17/2016 1:05:03 AM on 4/17/2016 1:05:03 AM - After triggered, repeat every 1.00:00:00 indefinitely."

Local Users and Groups Changes

Изменения, которые внесены через консоль Local Users или Groups. Этот отчет является основным, поскольку изменения в учетных записях пользователей Windows оказывает решающее влияние на безопасность сервера.

Filter	Value

Where: ws1.enterprise.com

Action	ObjectType	What	Who	When
Modified	**Local Group**	System Information\Local Groups\Users	ENTERPRISE\T.Simpson	4/18/2016 2:10:53 PM
Members: • **Added:** "WS1\Malicious"				
Added	**Local User**	System Information\Local Users\Malicious	ENTERPRISE\T.Simpson	4/18/2016 2:11:24 PM
Account is : "enabled" **Description** changed **Full Name:** "Malicious" **Name:** "Malicious" **Password Never Expires:** "No" **User cannot change password:** "No" **User must change password at next logon:** "Yes"				
Modified	**Local User**	System Information\Local Users\Malicious	ENTERPRISE\T.Simpson	4/18/2016 2:12:33 PM
Password changed				

Windows Server Configuration Details (State-in-Time)

Отчет содержит обзор конфигурации Windows server и содержит следующие сведения: ОС, антивирус, локальные пользователи и группы, общие файловые ресурсы, установленные программы и службы. Можно применить базовые фильтры для выделения проблем безопасности, таких как устаревшая Операционная система или антивирус.

Category: General

Server	OS Name	OS Version	Antivirus Status
dc1	Microsoft Windows Server 2012 R2 Standard Evaluation	6.3.9600	Issues Detected

Category: File Shares

Object Type	Object Name	Object Path	Properties
Default Share	ADMIN$	C:\Windows	Remote Admin
Default Share	C$	C:\	Default share
Shared Folder	NETLOGON	C:\Windows\SYSVOL\sysvol\enterprise.com\SCRIPTS	Logon server share
Shared Folder	SYSVOL	C:\Windows\SYSVOL\sysvol	Logon server share

Local Users and Groups (State-in-Time)

В отчете перечислены локальные пользователи и группы на серверах Windows, сгруппированные по имени сервера. Для каждого объекта сообщается следующее: Тип (пользователь или группа), состояние (если применимо) и свойства, такие как тэги "Срок действия пароля никогда не истекает" или члены группы.

Server: fs1.enterprise.com

Name	Type	Status	Properties
Access Control Assistance Operators	Group	N/A	
Administrators	Group	N/A	Members: J.Carter, ENTERPRISE\Domain Admins, Administrator
Backup Operators	Group	N/A	
Guest	User	Disabled	Password never expires
J.Carter	User	Enabled	

All User Activity by User

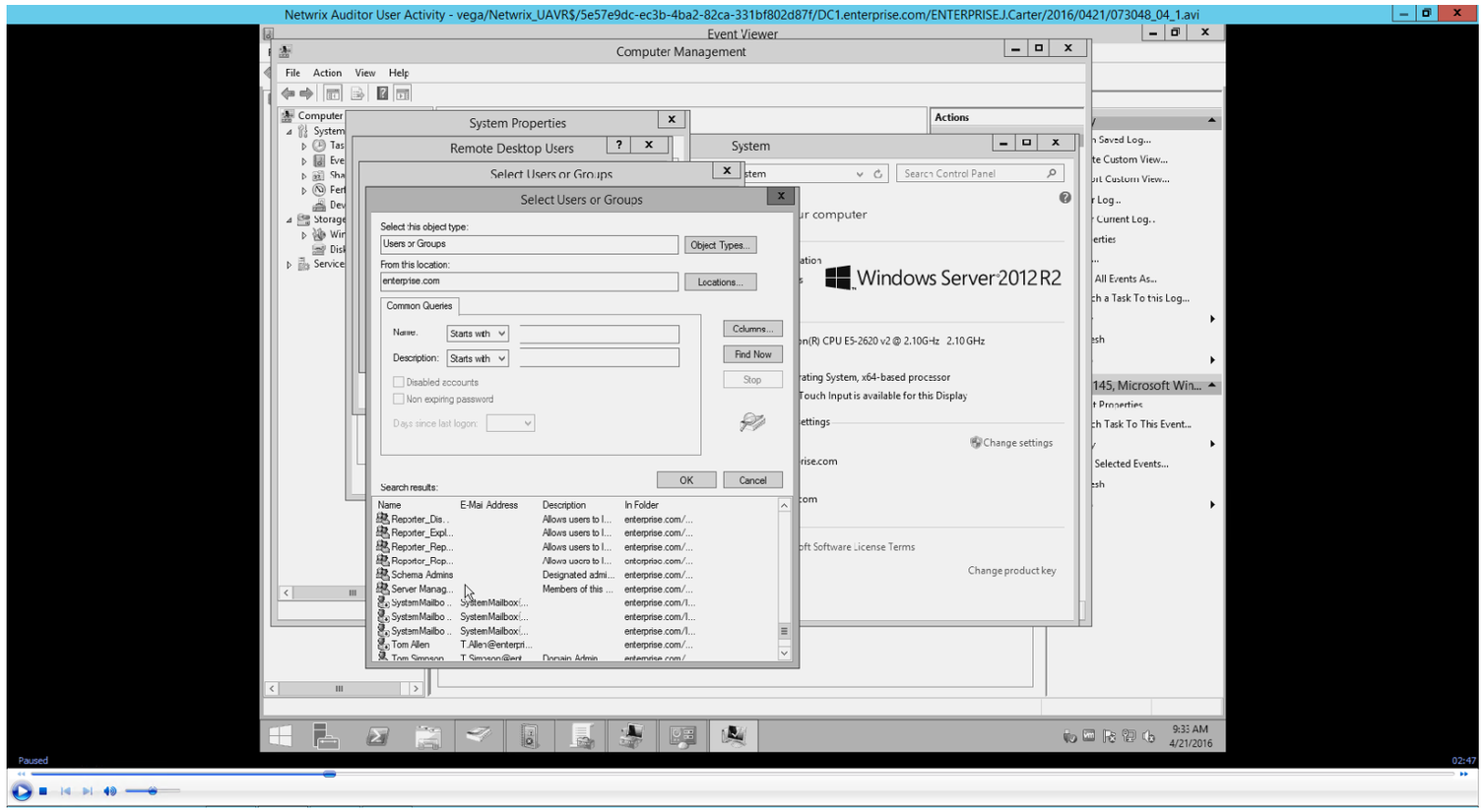
Видеозапись активности пользователей.

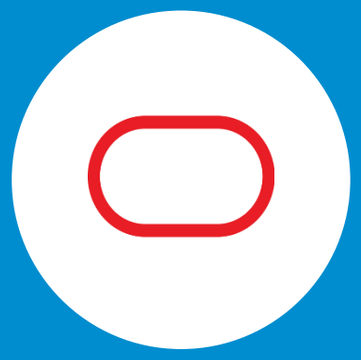
Filter	Value

Who: ENTERPRISE\T.Simpson

Where: dc1.enterprise.com

When	What
4/18/2016 10:31:29 AM	Windows PowerShell
4/18/2016 12:14:12 PM	Console Window Host | Windows PowerShell
4/18/2016 12:15:16 PM	Windows PowerShell
4/18/2016 12:16:45 PM	Console Window Host | Windows PowerShell
4/18/2016 12:18:37 PM	Windows PowerShell





Netwrix Auditor

for Oracle Database

All Oracle Database Activity by Object

Все изменения, внесенные в базы данных Oracle, включая изменение конфигурации и привилегий, успешные и неудачные попытки входа в систему, сгруппированные по имени объекта.

Filter	Value

What: Data_Cardholder

Action	Object Type	Who	When
Read	**Data**	ENTERPRISE\J.Carter	10/3/2016 6:07:13 PM

Where: orcl/orcl.enterprise.com

Workstation: 192.168.1.47

Action name: SELECT

Container name: CDB$ROOT

Database user: SYS

Privilege for action: SYSDBA

Program name: SQL Developer

Session ID: 2729059355

Unified policy name: NWX_ACTIONS_OBJ_POL_EMP

Account Management

Полный список удачных и неудачных попыток создания, изменения, удаления, включения и отключения учетных записей базы данных Oracle.

Filter	Value

Action	Object Type	What	Who	When
Modify (Failed Attempt)	**User**	C##J.Carter	ENTERPRISE\T.Simpson	10/4/2016 4:01:10 PM

Where: orcl/orcl.enterprise.com

Workstation: 192.168.1.49

Action name: ALTER USER

Captured SQL statement: ALTER USER "SYSBACKUP" DEFAULT TABLESPACE "USERS" TEMPORARY TABLESPACE "TEMP" PASSWORD EXPIRE ACCOUNT LOCK ENABLE EDITIONS

Cause: ORA-65074: editions not supported for common users

Container name: CDB$ROOT

Database user: C##J.Carter

Privilege for action: SYSDBA

Program name: SQL Developer

Session ID: 1608348078

Unified policy name: ORA_SECURECONFIG, NWX_ACTIONS_POL

All Oracle Database Logons

Отчет по удачным и неудачным попыткам подключения к базе данных Oracle. По каждой попытке доступа показывается информация об учетных записях, использованных для входа в ОС хоста и подключения непосредственно к БД Oracle.

Filter	Value

Action	Object Type	What	Who	When
Failed Logon	**Logon**	orcl/orcl.enterprise.com	ENTERPRISE\J.Carter	10/3/2016 12:05:39 PM

Where: orcl/orcl.enterprise.com

Workstation: 192.168.1.47

Action name: LOGON

Cause: ORA-01017: invalid username/password; logon denied

Client IP: 172.17.6.7

Container name: CDB$ROOT

Program name: SQL Developer

Session ID: 4025540185

Unified policy name: ORA_LOGON_FAILURES

Data Access

Отчет по всем пользователям, которые получили доступ к базе данных Oracle.

Filter	Value			
Action	**Object Type**	**What**	**Who**	**When**
Read	**Data**	ENT.Customer	ENTERPRISE\J.Carter	10/3/2016 6:07:13 PM

Where: orcl/orcl.enterprise.com

Workstation: ENTERPRISE\ORACLE

Action name: SELECT

Container name: CDB$ROOT

Database user: C##J.Carter

Privilege for action: SYSDBA

Program name: SQL Developer

Session ID: 2729059355

Unified policy name: NWX_ACTIONS_OBJ_POL_EMP

Privilege Management

Изменения ролей и привилегий. Используйте отчет для выявления необоснованных назначений ролей и обеспечения безопасности баз данных Oracle.

Filter	Value

Action	Object Type	What	Who	When
Modified	**Role**	CDB_DBA	ENTERPRISE\J.Carter	10/4/2016 4:00:44 PM

Where: orcl/orcl.enterprise.com

Workstation: 192.168.1.47

Action name: GRANT

Container name: CDB$ROOT

Database user: C##J.Carter

Privilege for action: SYSDBA

Privilege user or role: ANONYMOUS

Program name: SQL Developer

Role name: ADM_PARALLEL_EXECUTE_TASK

Session ID: 1608348078

Statement ID: 79

Unified policy name: ORA_SECURECONFIG

netwrix

Netwrix Auditor
for SQL Server

All SQL Server Changes by Object Type

Все изменения объектов и прав доступа на SQL серверах, сгруппированные по типу измененного объекта.

Filter	Value

Object Type: Database

Action	What	Who	When
Added **Where:** **Workstation:**	Databases\Prod1 sql1\db1 172.17.6.12	ENTERPRISE\J.Carter	2/3/2016 7:04:28 PM

Object Type: Table

Action	What	Who	When
Added **Where:** **Workstation:**	Databases\Test1\Tables\dbo.BUYPOTENCY sql1\db1 172.17.6.12	ENTERPRISE\J.Carter	4/6/2016 2:20:14 PM

Object Type: Column

Action	What	Who	When
Added **Where:** **Workstation:**	Databases\Videorecording\Tables \dbo.VideoSessions\Columns\RelativePath sql1\db1 172.17.5.142	ENTERPRISE\J.Carter	4/6/2016 2:20:14 PM
Added **Where:** **Workstation:**	Databases\Videorecording\Tables \dbo.VideoSessions\Columns\VariablePath sql1\db1 172.17.5.142	ENTERPRISE\J.Carter	4/6/2016 2:20:14 PM

All SQL Server Logons

Данные по успешным и неудачным попыткам подключения к SQL серверу, через систему аутентификации Windows или SQL Server.

Filter	Value

Action	Object Type	Who	When
Failed Logon	**SQL logon**	ENTERPRISE\T.Simpson	10/4/2016 3:35:11 PM
Where:	SQL\MSSQLSERVER		
Workstation:	172.17.6.25		
Cause: An attempt to login using SQL authentication failed. Server is configured for Windows authentication only.			
Failed Logon	**SQL logon**	ENTERPRISE\J.Carter	10/4/2016 3:46:31 PM
Where:	SQL\MSSQLSERVER		
Workstation:	172.17.6.25		
Cause: An attempt to login using SQL authentication failed. Server is configured for Windows authentication only.			
Successful Logon	**Windows logon**	ENTERPRISE\J.Carter	10/4/2016 2:54:09 PM
Where:	SQL\MSSQLSERVER		
Workstation:	172.17.6.25		

Netwrix Auditor for VMware

All VMware Changes by Object Type

Все изменения в инфраструктуре VMware, сгруппированные по типу измененного объекта.

Filter	Value

Object Type: ResourcePool

Action	What	Who	When
Removed	\ha-folder-root\ha-datacenter\host \ENTMKTVMS01.enterprise.com\Resources\John Carter\Enterprise\QA	ENTERPRISE\J.Smith	2/27/2016 3:35:14 AM
Where:	https://entmktvm01.enterprise.com:443		

Object Type: VirtualMachine

Action	What	Who	When
Removed	\ha-folder-root\ha-datacenter\vm\Enterprise	ENTERPRISE\J.Carter	2/8/2016 3:22:20 PM
Where:	https://entmktvm01.enterprise.com:443		
Removed	\ha-folder-root\ha-datacenter\vm\CA Enterprise	ENTERPRISE\J.Carter	2/8/2016 3:22:39 PM
Where:	https://entmktvm01.enterprise.com:443		
Added	\ha-folder-root\ha-datacenter\vm\CA	ENTERPRISE\J.Carter	2/8/2016 3:24:30 PM
Where:	https://entmktvm01.enterprise.com:443		

VMware Virtual Machine Changes

Отчет содержит данные по изменению конфигурации виртуальных машин: настройки, права доступа и т.д.

Filter	Value		
Action	**What**	**Who**	**When**
Removed	\ha-folder-root\ha-datacenter\vm\Enterprise	ENTERPRISE\J.Carter	2/8/2016 3:22:20 PM
Where:	https://entmktvm01.enterprise.com:443		
Removed	\ha-folder-root\ha-datacenter\vm\CA Enterprise	ENTERPRISE\J.Carter	2/8/2016 3:22:39 PM
Where:	https://entmktvm01.enterprise.com:443		
Added	\ha-folder-root\ha-datacenter\vm\CA	ENTERPRISE\J.Carter	2/8/2016 3:24:30 PM
Where:	https://entmktvm01.enterprise.com:443		