KASPERSKY

Что нового в KES 11.1 и KSC 11. Краткий обзор

Technical Training KL 202.11.1 Kaspersky Endpoint Security and Management. Что нового

Что нового в Kaspersky Security Center 11

Операционные системы

New Web Console

Изменения в интерфейсе ММС-консоли администрирования

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы Новые компоненты KES Компонент AMSI Protection Provider Компонент Adaptive Anomaly Control Проверка зашифрованного трафика Защита от MAC Spoofing Role Based Access Control for KES



Kaspersky Security Center 11: операционные системы и сервера баз данных

• Операционные системы:

- Windows 10 RS5 (October 2018 Update)
- Windows Server 2019

• Сервера баз данных:

- Microsoft SQL Server 2017
- Amazon RDS (MS SQL)
- Microsoft Azure SQL DB



Что нового в Kaspersky Security Center 11

Операционные системы

New Web Console

Изменения в интерфейсе ММС-консоли администрирования

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы Новые компоненты KES Компонент AMSI Protection Provider Компонент Adaptive Anomaly Control Проверка зашифрованного трафика Защита от MAC Spoofing Role Based Access Control for KES



Web Console vs. MMC Console

Protection status	Â	New devices	Throat activity 🔅
 <u>Critical</u> <u>OK</u> <u>OK</u> <u>Warning</u> 1 	5,52 5,52 5,52 5,52 1, 0,92:52:018 10:05:2018 10:05:2018 10:15:2018 10:25:2018 1	New devices (9)	Intreat activity cor 14 10 10 10 8 4 2 0 09/25/2018 10/05/2018 10/25/2018 10/25/2018 Last updated: 10/25/2018 7:29 em
st updated: 10/25/2018 7:32 am			
Most frequent threats { L. Trojan-PSW.Win32.Mimikatz.gen 0 2. HEUR:Trojan- 0 5. HEUR:Trojan- 0 4. HEUR:Trojan PowerShell Generic 0 ast updeted: 10/25/2018 7:29 em	Most heavily infected devices ~ (2) 1. <u>ALEX-DESKTOP</u> 14 Last updated: 10/25/2018 7:29 am	Detection of threats by application components Unknown 0 File Threat Protection 14 Mail Threat Protection 0 Web Threat Protection 0 IM Anti-Virus 0 Lest updated: 10/25/2018 7:29 am	Add widget

- Не требует установки на стороне клиента
- Нет привязки к операционной системе
- Поддерживает работу с сенсорным экраном
- Не требует поддержки
 браузерами Java / ActiveX / Flash
- В текущей версии не поддерживается управление:
 - шифрованием
 - мобильными устройствами
 - уязвимостями и обновлениями

Дистрибутив: KSC 11 Web Console



Kaspersky Endpoint Security for Android

Microsoft Exchange Mobile Devices Server

- Дистрибутив KSC 11 Web Console:
 - является частью дистрибутива КSC
 - Существует в виде отдельного дистрибутива
- Извлечь дистрибутив KSC 11 Web Console в виде отдельного инсталляционного пакета нельзя
- Может быть установлена на отдельный компьютер

×

781 Mb

328 Mb

44 Mb

214 Mb

25 Mb

21 Mb

20 Mb

Web Console: Мастер установки КSC



- При первом запуске Kaspersky Security Center 11 Web Console подключается к локальному Серверу администрирования <u>https://localhost:8080/</u>
- Подключение с удаленной машины <u>https://<IP-address>:8080/</u>

	iter 11 Web Console installation	
This version of Kaspersk console solution for eas Security Center 11 Web	:y Security Center provides an enhanced web-based e of management. Do you want to deploy Kaspersky • Console to the target device?	 C Kaspersky Security Center Web ⊂ X C ▲ Not secure ht
🗹 Install Kaspersky	Security Center 11 Web Console	
© 2018 AO Kaspersky Kaspersky Security Center 1	Lab. All Rights Reserved, < Back Next > Cancel 1 Administration Server — X	Se User name
Kacharolar		Internal or domain u
Security Center	The Kaspersky Security Center 11 Administration Server Setup Wizard has completed.	Password
Security Center	The Kaspersky Security Center 11 Administration Server Setup Wizard has completed. Kaspersky Security Center 11 Administration Server has been successfully installed.	Password *****
Security Center	The Kaspersky Security Center 11 Administration Server Setup Wizard has completed. Kaspersky Security Center 11 Administration Server has been successfully installed. Click Finish to dose the Setup Wizard.	Password *****
Security Center	The Kaspersky Security Center 11 Administration Server Setup Wizard has completed. Kaspersky Security Center 11 Administration Server has been successfully installed. Click Finish to close the Setup Wizard. Start as MMC-based Administration Console Start as Kaspersky Security Center 11 Web Console	Password *****



- 1. Запустите мастер установки
- 2. Примите лицензионное соглашение
- 3. Выберите язык
- 4. Укажите путь установки
- 5. Укажите параметры подключения к Web Console
- 6. Задайте учетные записи
- 7. Выберите сертификат
- 8. Укажите параметры подключения к Kaspersky Security Center
- 9. Запустите установку
- 10. Завершите установку запустите KSC 11 Web Console





Web Console – это отдельный дистрибутив, который можно установить как вместе с Kaspersky Security Center, так и на отдельный компьютер

На первом шаг необходимо выбрать язык мастера установки, доступно 6 языков

KASPERSKY B

- 1. Запустите мастер установки
- 2. Примите лицензионное соглашение
- 3. Выберите язы
- 4. Укажите путь установки
- 5. Укажите параметры подключения к Web Console
- 6. Задайте учетные записи
- 7. Выберите сертификат
- 8. Укажите параметры подключения к Kaspersky Security Center
- 9. Запустите установку
- 10. Завершите установку запустите KSC 11 Web Console



	Kaspersky Security Center 11 Web Console X	Kaspersky Security Center 11 Web Console
нзионное	License Agreement Please carefully read the License Agreement:	Language settings
становки іетры Web Console ые записи ификат іетры Каspersky ановку ановку ановку 11 Web	Please read the End User License Agreement, Privacy Policy, and all the linked documents associated with the EULA. You must accept the terms and conditions of the EULA and Privacy Policy to install the application. Kaspersky Security Center 11 Web Console, Self Service Portal, Microsoft ^ Exchange Mobile Devices Server, Network Agent, Administration Console, Kaspersky Security Center SHV KASPERSKY LAB END USER LICENSE AGREEMENTS (FOR BETA VERSIONS) BY CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR BY USING THE SOFTWARE YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. SUCH ACTION IS A SYMBOL OF > I confirm I have fully read, understood, and accept the terms and conditions of this EULA	This distribution package provides the following languages: Français Englisch Pyccxvi 日本語(日本) 简(仕中) 简(仕中) Tf the required language is not present in the list, you can download the corresponding file by using the link below. After the file is downloaded, specify the path by browsing to the file saved on disk. Additional languages Specify the path to the additional language file. Browse
	< Back Next > Cancel	< Back Next > Cancel

На следующем шаге необходимо принять лицензионное соглашение

Затем смотрим какие языки локализации Web Console доступны в инсталляторе, также можно подготовить и подгрузить любой язык в JSON-формате.

- 1. Запустите мастер установки
- 2. Примите лицензионное соглашение
- 3. Выберите язык
- 4. Укажите путь установки
- 5. Укажите параметры подключения к Web Console
- 6. Задайте учетные записи
- 7. Выберите сертификат
- 8. Укажите параметры подключения к Kaspersky Security Center
- 9. Запустите установку
- 10. Завершите установку запустите KSC 11 Web Console



Установка Web Console

Далее необходимо указать путь установки, рекомендуется оставить по умолчанию

Затем надо указать адрес и порт, которые будут использоваться для подключения к Web Console

Говорят, что к релизу порт 8080 должен будет измениться на 443.

KASPERSKY B

- 1. Запустите мастер установки
- 2. Примите лицензионное соглашение
- 3. Выберите язык
- 4. Укажите путь установки
- 5. Укажите параметры подключения к Web Console
- 6. Задайте учетные записи
- Выберите сертификат 7.
- 8. Укажите параметры подключения к Kaspersky Security Center
- 9. Запустите установку
- 10. Завершите установку запустите KSC 11 Web Console

Account settings Specify the Kaspersky Security Center 11 Web Console account settings.		Client certificate Select how to sp	pecify the certificate:
The Node.js account and update service account are required for starting and update Kaspersky Security Center 11 Web Console. You can use the default accounts or spe ones.	ting ecify custom	Generate new ce Make sure the be	ertificate elow domain is trusted.
Use default accounts	\rightarrow		ABC
○ Specify custom accounts		CRT certificate fi	ile C:\Program Files (x86)\Kaspersky Lab\Kaspersky Se Browse
		PEM certificate fi	ile C:\Program Files (x86)\Kaspersky Lab\Kaspersky Se Browse
		Certificate passw (optional)	vord

По умолчанию, службы Web Console будут запускаться под системными учетными записями, но можно задать свои

Следующий шаг это создание сертификата веб-сервера, на котором будет крутиться Web Console. Сертификат будет генерироваться автоматически или можно подложить свой.

KASPERSKY

Установка Web Console

- 1. Запустите мастер установки
- 2. Примите лицензионное соглашение

Kaspersky Security Center 11 Web Console

- 3. Выберите язык
- Укажите путь установки 4.
- 5. Укажите параметры подключения к Web Conso
- Задайте учетные записи 6.
- Выберите сертификат 7.
- 8. Укажите параметры подключения к Kaspersky Security Center
- 9. Запустите установку
- Завершите установку -10. запустите KSC 11 Web Console

SECURITY-C
13299
13235
C:\Program

На этом шаге администратор указывает с какими Kaspersky Security Center сможет взаимодействовать Web Console

Установка Web Console

Если Web Console ставится на компьютер, на котором уже установлен KSC, то этот KSC автоматически появится в списке

Порт Сервера администрирования, по умолчанию 13299, но его можно изменить в свойствах Сервера

Установка Web Console:

KASPERSKY

Browse

Cancel

- 1. Запустите мастер установки
- 2. Примите лицензионное соглашение
- 3. Выберите язык
- 4. Укажите путь установки
- 5. Укажите параметры подключения к Web Console
- 6. Задайте учетные записи
- 7. Выберите сертификат
- 8. Укажите параметры подключения к Kaspersky Security Center
- 9. Запустите установку
- 10. Завершите установку запустите KSC 11 Web Console





Предпоследний шаг – это запустить процесс установки кнопкой Install.

Ну и последний шаг – запустить Web Console и завершить мастер или просто завершить мастер.

Службы Web Console

Q Services					- 0	×
File Action View	Help					
	à 📑 🗗 🖬 🕨 🔲 II ID					
Services (Local)	Name Name Kaspersky Lab activation proxy server Kaspersky Lab Web Server Kaspersky Security Center 11 Administration Server Kaspersky Security Center 11 automation object	Description Internet Pro Service allo Kaspersky L Administrat Kaspersky S	Status Running Running Running Running	Startup Type Manual (Trig Automatic Automatic Automatic Manual	Log On As Network Service .\KIScSvc .\KIScSvc .\KL-AK-388C4967 Network Service	^
	Kaspersky Security Center Web Console Kaspersky Security Center Web Console Management Service Kaspersky Security Center Web Console Message Queue	Kaspersky S Manageme Kaspersky S	Running Running Running	Automatic Automatic Automatic	Network Service Local System Network Service	
	 KDC Proxy Server service (KPS) KtmRm for Distributed Transaction Coordinator Link-Layer Topology Discovery Mapper Local Session Manager Microsoft (R) Diagnostics Hub Standard Collector Service Microsoft Account Sign-in Assistant Microsoft App-V Client Microsoft Passport Microsoft Passport Microsoft Software Shadow Copy Provider Microsoft Storage Spaces SMP Net.Tcp Port Sharing Service 	KDC Proxy S Coordinates Creates a N Core Windo Diagnostics Enables use Manages A Manages In Provides pr Manages Io Manages so Host service Provides abi	Running	Manual Manual (Trig Manual Automatic Manual Manual (Trig Disabled Manual (Trig Manual (Trig Manual Manual Disabled	Network Service Network Service Local Service Local System Local System Local System Local System Local System Local System Local Service Local System Network Service Local Service	*
	Extended Standard					

В процессе установки Web Console устанавливаются следующие службы:

- Kaspersky Security Center Management
 Service
- Kaspersky Security Center Web Console
- Kaspersky Security Center Web Console
 Message Queue платформа для
 обработки очереди сообщений на
 базе NSQ

Web Console: взаимодействие



Подключение к нескольким KSC

Запустить Update в мастере



Требования к браузерам для работы с Web Console

- Поддерживаемые браузеры:
 - Google Chrome
 - Mozilla Firefox
 - Safari

Где что в Kaspersky Security Center Web Console?

ireat activity ③	Most frequent threats Last updated: 01/16/2019 3:57 pm	0	Most heavily infected devices ~ Last updated: 01/16/2019 3:57 pm	٢
18/2018 12/27/2018 01/07/2019 01/17/2019 t updated: 01/16/2019 3:57 pm				
etection of threats by application ③ mponents				
nknown 0				
le Threat Protection 0 No data				
/eb Threat Protection 0	Add or restore widget			
Anti-Virus				
Tutorial			X	

При первом подключении к Web Console выскакивает **Tutorial**

Это 17 шагов, которые рассказывают, где что находится в Web Console

Мы рекомендуем ознакомиться с этим Tutorial

Если вы случайно закрыли Tutorial или хотите еще раз ознакомиться с ним, в главном окне внизу есть ссылка Show Tutorial

При первом подключении после закрытия Tutorial запускается Quick Start Wizard

0	Quick Start Wizard Welcome to the Quick Start Wizard of Administration Server SECURITY-CENTER This Wizard performs initial configuration of Administration Server and downloads updates. It also helps you to do the following:	₽ @ x	Мастер запуска подклк сервер	 первонача ается после учения к сер к работе:
	- Activate Kaspersky Security Center 11		_	Создает зад
	- Configure delivery of notifications by email - Specify the proxy server settings		_	Загружает о хранилище администри
			Мастер	о просит аді
			_	Настроить п Интернет
			_	Добавить ли
			—	Принять сог Security Netw
	NEVT		_	Указать поч [.] который буд уведомлени
	NEXI			

альной настройки е первого рверу и готовит

- ачи и политики
- обновления в на Сервере рования

министратора:

- юдключение к
- ицензию
- глашение Kaspersky vork
- товый адрес, на дут приходить отчеты и 1Я

1.	Настройте Интернет	подключение к
	-	_

- 2. Загрузите обновления
- 3. Добавьте лицензию
- 4. Загрузите новые плагины
- 5. Примите соглашение KSN
- Дайте мастеру создать задачи и политики
- 7. Запустите сканирование сети
- 8. Укажите почтовый ящик для уведомлений и отчетов
- 9. Не запускайте мастер распространения защиты

Internet connection required Use proxy for Internet access Proxy server address Proxy server port Bypass proxy server for local addresses Proxy server authentication User name Password SHOW				
Use proxy for Internet access	Internet connection required			
Proxy server address Proxy server port Bypass proxy server for local addresses Proxy server authentication User name Password SHOW	Use proxy for Internet access			
Proxy server port Bypass proxy server for local addresses Proxy server authentication User name Password SHOW	Proxy server address			
Bypass proxy server for local addresses Proxy server authentication User name Password SHOW	Proxy server port			
Bypass proxy server for local addresses Proxy server authentication User name Password SHOW				
User name Password SHOW SHOW	Bypass proxy server for local addresses Proxy server authentication			
User name Password SHOW		 		
Password SHOW	User name			
	Password	SHOW		
DACK NEXT				

Настройка доступа в Интернет

Укажите параметры прокси-
сервера для доступа в
Интернет, или пропустите этот
шаг, если для доступа в
Интернет прокси-сервер не
используется

Доступ в Интернет нужен:

- Чтобы загружать обновления
- Чтобы перенаправлять запросы в Kaspersky Security Network от клиентских компьютеров, когда Сервер администрирования выступает в роли KSN Proxy

KA\$PER\$KY[®]

- 1. Настройте подключение к Интернет
- 2. Загрузите обновления
- 3. Добавьте лицензию
- 4. Загрузите новые плагины
- 5. Примите соглашение KSN
- Дайте мастеру создать задачи и политики
- 7. Запустите сканирование сети
- 8. Укажите почтовый ящик для уведомлений и отчетов
- 9. Не запускайте мастер распространения защиты



Загрузка обновлений

Сервер администрирования автоматически загружает обновления для продуктов, инсталляционные пакеты которых есть в хранилище

Кнопка **Next** не прерывает обновление

- 1. Настройте подключение к Интернет
- 2. Загрузите обновления
- 3. Добавьте лицензию
- 4. Загрузите новые плагины
- 5. Примите соглашение KSN
- 6. Дайте мастеру создать задачи и политики
- 7. Запустите сканирование сети
- Укажите почтовый ящик для уведомлений и отчетов
- 9. Не запускайте мастер распространения защиты

Выбор лицензии

Quick Start Wizard Application activation Select option Add key later Add key file Add activation code	 Активируйте Сервер администрирования лицензие в виде кода активации или файла-ключа
BACK	Либо пропустите этот шаг и активируйте Kaspersky Security Center позже

KA\$PER\$KY[®]

- 1. Настройте подключение к Интернет
- 2. Загрузите обновления
- 3. Добавьте лицензию
- 4. Загрузите новые плагины
- 5. Примите соглашение KSN
- Дайте мастеру создать задачи и политики
- 7. Запустите сканирование сети
- 8. Укажите почтовый ящик для уведомлений и отчетов
- 9. Не запускайте мастер распространения защиты

Select option			
🔿 Add key later			
🔵 Add key file			
Add activation code			
BAJ74-S9ZWR-9EV52-G1G52			
CENID			
SEND			
SEND 3 keys have been added to the repos	itory.		
SEND 3 keys have been added to the repos	itory.		
SEND 3 keys have been added to the repos	itory.		
SEND 3 keys have been added to the repos	itory.		
SEND 3 keys have been added to the repos	itory.		
SEND 3 keys have been added to the repos	itory.		
SEND 3 keys have been added to the repos	itory.		
SEND 3 keys have been added to the repos	itory.		
SEND 3 keys have been added to the repos	itory.		

Активация кодом

Для активации кодом нужен доступ в Интернет

Кодом можно активировать сразу и Сервер администрирования и Kaspersky Endpoint Security на компьютерах

Опция автоматически распространять лицензию на клиентские устройства отсутствует, но ее можно указать позднее, чтобы не выбирать лицензию в задачах удаленной установки

- 1. Настройте подключение к Интернет
- 2. Загрузите обновления
- 3. Добавьте лицензию
- 4. Загрузите новые плагины
- 5. Примите соглашение KSN
- 6. Дайте мастеру создать задачи и политики
- 7. Запустите сканирование сети
- 8. Укажите почтовый ящик для уведомлений и отчетов
- 9. Не запускайте мастер распространения защиты

Quick Start Wizard		F ¹ (
Application activation		
Select option		
 Add key later 		
 Add key file 		
Add activation code		
SELECT KEY FILE		
Application name	Kaspersky Security for Storage, Server International Edition. 10-14 FileServer 1 year NFR License	
Major version		
Licenses count	10	
License term (days)		
License expiration date	09/02/2019 5:00 pm	
Key type	Commercial	
Automatically deploy key to	o managed devices	
This key is not valid for Kaspers	ky Security Center 11.	

Активация ключом

Если активировать Сервер администрирования ключом, позже нужно будет добавить на Сервер еще один ключ, чтобы активировать Kaspersky Endpoint Security

Используйте активацию ключом, если нет доступа в Интернет

В отличии от кода активации у ключа есть опция автоматического распространения

- 1. Настройте подключение к Интернет
- 2. Загрузите обновления
- 3. Добавьте лицензию
- 4. Загрузите новые плагины
- 5. Примите соглашение KSN
- Дайте мастеру создать задачи и политики
- 7. Запустите сканирование сети
- 8. Укажите почтовый ящик для уведомлений и отчетов
- 9. Не запускайте мастер распространения защиты



Administration Agent 11.0.0.1019 Installed 01/09/2019 1:22 pm KES Windows 0.0.1 Installed 01/09/2019 1:22 pm	11.0.0.1019 Installed 01/09/2019 1:22 pm 0.0.1 Installed 01/09/2019 1:22 pm 11.0.0.1019 Installed 01/09/2019 1:22 pm
KES Windows 0.0.1 Installed 01/09/2019 1:22 pm	0.0.1 Installed 01/09/2019 1:22 pm 11.0.0.1019 Installed 01/09/2019 1:22 pm
	11.0.0.1019 Installed 01/09/2019 1:22 pm
Administration Server 11.0.0.1019 Installed 01/09/2019 1:22 pm	

Мастер первоначальной настройки показывает список предустановленных плагинов

Также можно проверить есть ли другие доступные плагины или обновления для уже установленных

- 1. Настройте подключение к Интернет
- 2. Загрузите обновления
- 3. Добавьте лицензию
- 4. Загрузите новые плагины
- 5. Примите соглашение KSN
- Дайте мастеру создать задачи и политики
- 7. Запустите сканирование сети
- 8. Укажите почтовый ящик для уведомлений и отчетов
- 9. Не запускайте мастер распространения защиты

Загрузка плагинов

- 1. Настройте подключение к Интернет
- 2. Загрузите обновления
- 3. Добавьте лицензию
- 4. Загрузите новые плагины
- 5. Примите соглашение KSN
- Дайте мастеру создать задачи и политики
- 7. Запустите сканирование сети
- 8. Укажите почтовый ящик для уведомлений и отчетов
- Не запускайте мастер распространения защиты





Kaspersky Security Network (KSN) это постоянно обновляемая онлайнбаза (в «облаке») репутаций исполняемых файлов и вебресурсов

Kaspersky Endpoint Security получает из KSN самую свежую информацию об угрозах и о файлах, которым можно доверять

Принимая соглашение KSN, администратор включает KSN для Kaspersky Endpoint Security в политике по умолчанию и для KSC в свойствах сервера администрирования

Администратор всегда может включить или выключить KSN для любого продукта в настройках или политике продукта

KL 002.11.1: Kaspersky Endpoint Security & Management

KASPERSKY B

- 1. Настройте подключение к Интернет
- 2. Загрузите обновления
- 3. Добавьте лицензию
- 4. Загрузите новые плагины
- 5. Примите соглашение KSN
- 6. Дайте мастеру создать задачи и политики
- 7. Запустите сканирование сети
- 8. Укажите почтовый ящик для уведомлений и отчетов
- 9. Не запускайте мастер распространения защиты



Ouick Start Wizard	₽ *	Мастер создает задачи Сервера администрирования:
The Wizard guides you through creation of basic security tasks and policies. Kaspersky Security Center Network Agent Policy for Kaspersky Security Center 11 Network Agent Kaspersky Security Center Administration Server Download updates to the Administration Server repository Database maintenance Backup of Administration Server data Kaspersky Endpoint Security (11.1.0) Policy for Kaspersky Endpoint Security 11 for Windows Updates installation		 Загрузка обновлений в хранилище Обслуживание базы данных
		 Резервное копирование данных Сервера администрирования
BACK CREATE		

KASPERSKY B

- Настройте подключение к Интернет
- 2. Загрузите обновления
- 3. Добавьте лицензию
- 4. Загрузите новые плагины
- 5. Примите соглашение KSN
- Дайте мастеру создать задачи и политики
- 7. Запустите сканирование сети
- 8. Укажите почтовый ящик для уведомлений и отчетов
- 9. Не запускайте мастер распространения защиты



Quick Start Wizard	₽°® X	Мастер создает групповые попитики:
The Wizard guides you through creation of basic security tasks and policies.		
Kaspersky Security Center Network Agent Policy for Kaspersky Security Center 11 Network Agent Kaspersky Security Center Administration Server Download updates to the Administration Server repository Database maintenance Backup of Administration Server data Kaspersky Endpoint Security (11.1.0) Policy for Kaspersky Endpoint Security 11 for Windows		 Агента администрирования кsc
Updates installation		 Kaspersky Endpoint Security for Windows
		Групповые задачи:
		 Установка обновлений
BACK CREATE		

- Настройте подключение к Интернет
- 2. Загрузите обновления
- 3. Добавьте лицензию
- 4. Загрузите новые плагины
- 5. Примите соглашение KSN
- 6. Дайте мастеру создать задачи и политики
- 7. Запустите сканирование сети
- 8. Укажите почтовый ящик для уведомлений и отчетов
- 9. Не запускайте мастер распространения защиты



Сканирование сети

Мастер запускает сканирование сети средствами Microsoft Windows

1.	Настройте подключение к Интернет
2.	Загрузите обновления
3.	Добавьте лицензию
4.	Загрузите новые плагины
5.	Примите соглашение KSN
6.	Дайте мастеру создать
	задачи и политики
7.	Запустите сканирование сети
8.	Укажите почтовый яшик
0.	для уведомлений и отчетов
9.	Не запускайте мастер
	распространения защиты

Настройка доставки почтовых уведомлений

Quick Start Wizard			⊭ '	Параметры используются для доставки уведомлений и
Specify email address for error notif	cations administrator@abc.lab			отчетов Однако мастер не создает
SMTP server address	10.28.0.10			задачу рассылки отчетов, но ее можно создать вручную в любое время
SMTP server port	25			
Password SEND TEST MESSAGE		SHOW		
BACK				

KASPERSKY B

- 1. Настройте подключение к Интернет
- 2. Загрузите обновления
- 3. Добавьте лицензию
- 4. Загрузите новые плагины
- 5. Примите соглашение KSN
- 6. Дайте мастеру создать задачи и политики
- 7. Запустите сканирование сети
- 8. Укажите почтовый ящик для уведомлений и отчетов
- 9. Не запускайте мастер распространения защиты



KASPERSKY

Завершение первоначальной настройки

Автоматическое распространение лицензии

MOI	NITORING & REPORTING 🛱 DEVICES 🤹 USERS &	ROLES 😡 DISCOVERY 8		
LICE	NSING V THIRD-PARTY APPLICATIONS V	Positories ~ 🖻 Kaspei	RSKY LAB APPLICATIONS ~	1
+ Ad	d $ imes$ Delete $ arpi$ Refresh			📰 Filter
	Application name			Key
۲	Kaspersky Endpoint Security for Business - Advanced Inte	ernational Edition. 10-14 Node	1 year NFR License: Kaspersky Security for WS and FS	250A-000
0	Kaspersky Endpoint Security for Business - Advanced Inte	ernational Edition. 10-14 Node	1 year NFR License: Security Center	250A-000
0	Kaspersky Endpoint Security for Business - Advance	250A-000451-571795B2		
		GENERAL DEVICES		
		Кеу	250A-000451-571795B2	
		Application name	Kaspersky Endpoint Security for Business - Advanced Internat 10-14 Node 1 year NFR License: Kaspersky Security for WS an	tional Edition. 1d FS
		Key type	Commercial	
		License term (days)	365	
		License expiration date	02/18/2019 4:00 pm	
		Key expiration date	02/18/2019 4:00 pm	
		Limit	14	

Если в мастере первоначальной настройки добавлялся код активации, то после завершения мастера рекомендуется включить опцию автоматического распространения, чтобы не забыть



Лабораторная работа №1

Установка Веб-консоли Kaspersky Security Center

1. Установите Веб-консоль Kaspersky Security Center

KASPERSKY

2. Пройдите мастер первоначальной настройки Сервера администрирования

Что нового в Kaspersky Security Center 11

Операционные системы

New Web Console

Изменения в интерфейсе ММС-консоли администрирования

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы Новые компоненты KES Компонент AMSI Protection Provider Компонент Adaptive Anomaly Control Проверка зашифрованного трафика Защита от MAC Spoofing Role Based Access Control for KES



Kaspersky Security Center 11: изменения в интерфейсе



- Kaspersky Lab software updates and patches Triggering of rules in Smart Training mode
- Новые узлы в дереве консоли Сервера Администрирования:
 - Multitenant applications
 - Deleted objects
 - Triggering of rules in Smart Training mode
 - Active threats
Kaspersky Security Center 11: узел Deleted objects



В узел Deleted objects попадают все сущности, у которых есть ревизии:

- Policies
- Tasks
- Installation packages
- Virtual Administration Servers
- Users
- Security groups
- Administration groups

Kaspersky Security Center 11: Global list of subnets

New subnet General settings Subnet address: Subnet mask:

Additional settings Name: abc.lab Description:

Sections	Global list of sub	nets			
General Event configuration Keys	Fill the list below with su any section of the appl	ubnets deployed in your orga ication interface by selecting	anization. This will allo them from this list.	w you to specify sub	nets in
KSN Proxy					0
Server connection settings					~
Virus outbreak	Name	IP	Subnet Mask	Description	
Traffic	abc.lab	10.28.0.0	255.255.255.0		
Events storage		192.168.94.0	255.255.255.0		
Neb Server	The Odessa	10.20.3.0	233,233,233,0		
Revision history storage					
Application categories					
Indate agents					
Tanging rules					
Clobal list of subpots					
Notification dolivory sottings					
Rouinication deriver y securitys					
Advanced					
Aavancea					
		Add	Troperaco	Bele	ic.

	информацию о подсетях
_	Список сквозной для KSC
?	×
10 . 28 . 0 . 0 255 . 255 . 255 . 0	0

OK

Cancel

Общий список подсетей, где

можно задавать

KASPERSKY B

Инсталляционный пакет: индикатор уровня

Защиты Kaspersky Security Center 11

Kaspersky Security Center 10

Sections	Properties		Low protection level	Critica
General	Standard installation		Sections	Pro
Properties	Advanced Threat Protection	^	General	
Properties Key Incompatible applications Revision history	Advanced Threat Protection		General Properties Key Incompatible applications Revision history	Protection of the second secon
	Browse	Clear		Con
Help	OK Cancel	Anniv		

otection level	Critical protection components are disabled Learn more	🕨 🕅 Recommended protection components 🛛 🕹 🗙
	Properties	It is recommended to enable the installation of all components to ensure the maximum level of protection.
	Advanced Threat Protection	Enable the installation of all components
ations	Behavior Detection Exploit Prevention Remediation Engine Host Intrusion Prevention (For workstations only)	- Important Host Intrusion Prevention ③ Web Threat Protection
	Essential Threat Protection	OK Cancel
	Main Intel Protection (For Workstations only) Web Threat Protection Firewall BadUSB Attack Prevention AMSI Protection Provider Security Controls	
	Web Control (For workstations only) Application Control Device Control (For workstations only) Adaptive Anomaly Control	
	Data Encryption	
	File Level Encryption (For workstations only) Full Disk Encryption (For workstations only) Bitlocker Management	~
	Path to application installation folder:	
	Path to application installation folder is specified on the application side	
	Configuration file:	Clear

Операционные системы

New Web Console

Изменения в интерфейсе ММС-консоли администрирования

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы Новые компоненты KES Компонент AMSI Protection Provider Компонент Adaptive Anomaly Control Проверка зашифрованного трафика Защита от MAC Spoofing Role Based Access Control for KES



Kaspersky Security Center 11: поддержка DIFF-файлов обновлений

📧 Properties: Download up	lates to the repository	- 🗖	×		
Sections	Settings				
General	Update sources				
otification	List of available sources that will be used to download updates.				
chedule	[10] 101 (10) 1991 (10) R. O'D Ford States and Distance (1995) [Appl 11]	Confid	ure .		
ettings	Updates content	com	di Citti		
pdate verification	Set of components and software modules for which updates must be dow	nloaded.	12		
levision history	Other settings	Confid	ure	V	
	Servers, update settings of software modules, and other settings.	Set of updates to	iff files	is defined automatically for all applications installed	?
<u>Help</u>	OK Car	nce			
2.11.1: Kaspersky Endpoi	nt Security & Management				OK Cancel

- Реализована поддержка DIFFфайлов для обновления баз угроз
- Обновление с помощью DIFFфайлов позволяет уменьшить внутренний сетевой трафик примерно в 20 раз



Агенты администрирования: поддержка DIFFфайлов обновлений

Properties: Kaspersky Security Center	Network Agent	<u>199</u>	∎ ×
Sections	Manage patches and updates		
General Event configuration Settings Repositories Updates and software vulnerabilities	Automatically install applicable updates and patches for co Edit Edit Edit	ing locked omponents with Undefined	 ✓ 1 – status ✓ 1 –
Restart management Windows Desktop Sharing Manage patches and updates	Uownioad updates and anti-virus databases from Adminis	tration Server in advance	(recommended)
Network Update agents Revision history			
Help	ОК	Cancel	Apply

- Параметр загружать обновления заранее (offline-режим обновления) включен в политике Агента по умолчанию
- Ретрансляции DIFF-файлов не работает при включенном offlineрежиме обновления
- DIFF-файлы обновлений не будут передаваться на старые версии Агентов

Операционные системы

New Web Console

Изменения в интерфейсе ММС-консоли администрирования

KASPERSKY

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы Новые компоненты KES Компонент AMSI Protection Provider Компонент Adaptive Anomaly Control Проверка зашифрованного трафика Защита от MAC Spoofing Role Based Access Control for KES

Kaspersky Security Center 11: агенты обновлений

Sections	KSN Proxy		
General Event configuration	Enable KSN Proxy on update agent side		~ (1
Settings Repositories Updates and software vulnerabilities Restart management Windows Desktop Sharing	Forward KSN requests to Administration Se Access KSN Cloud directly over Internet	■ Editing allowed	1
Network Update agents Network polling Internet connection settings KSN Proxy Updates Revision history	Open ports TCP port: Use UDP Port UDP port:	Editing allowed	
Help		OK Cancel A	oply

Properties: Kaspersky Security Center	Network Agent — [)	×
Sections	Updates		
General		_	-
Event configuration	Editing allowed	~	
Settings	Download diff files		
Repositories	This option is not effective if the offline model of update download is enabled in the	setting	js of
Updates and software vulnerabilities	the same Network Agent policy or in the local settings of the managed device.		
Restart management			
Windows Desktop Sharing			
Manage patches and updates			
Network			
Update agents			
Network polling			
Internet connection settings			
KSN Proxy			
Updates			
Revision history			
Help	OK Cancel	Apply	

KASPERSKY B

Update Agent: поддержка 10 000 узлов

Kaspersky Security Center 11



Update Agent





Update Agent: системные требования

- Процессор:
 - частота 3,6 ГГц или выше
- Оперативная память:
 - от 8 ГБ
- Объем свободного места на диске:
 - от 120 ГБ

Папка KLSHARE переехала

🚇 Computer Management					- 🗆 X
<u>File</u> <u>Action</u> <u>View</u> <u>H</u> elp					
🗢 🏟 🗖 📰 🖾 🗟 🔽	1				
 Computer Management (Local) System Tools Task Scheduler Event Viewer Shared Folders Shares Sessions Open Files Local Users and Groups Operformance Device Manager Storage Windows Server Backup Disk Management 	Share Name Share Name ADMINS Sea CS IPCS KLSHARE	Folder Path C:\Windows C:\ C:\ProgramData\KasperskyLab\adminkit\1093\.working\share	Type Windows Windows Windows	# Client Connections 0 0 1	Description Remote Admin Default share Remote IPC

C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\

Операционные системы

New Web Console

Изменения в интерфейсе ММС-консоли администрирования

KASPERSKY

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы Новые компоненты KES Компонент AMSI Protection Provider Компонент Adaptive Anomaly Control Проверка зашифрованного трафика Защита от MAC Spoofing Role Based Access Control for KES

Kaspersky Security Center 11: обратная совместимость плагинов KES

Administration Server SEC Policies Devices Policies Create a policy Import	URITY-CENTER > Managed de Tasks policy from file <u>Add/Remove co</u>	ivices > Worksta	ations		<u>Group properties</u> <u>Refresh</u>	— По ра	олитики спростр	и задачи аняются	KES 1: Ha KE
Inherited policies: hide <u>sho</u> Name Kaspersky Endpoint Security for Kaspersky Endpoint Security f	Windows (11.1.0) for Windows (11.1.0)	Status	Application Kaspersky Endpoint Security for Windows (11.1.0)	Kaspersky (11.1.0)	Endpoint Security for Windows ×		tesults of policy enfo Export to file.	rcement	
				Created:	Windows (11.1.0) 10/29/2018 2:06:38 PM	De	vice	Windows domain	Date
				Changed:	10/29/2018 2:06:59 PM	0	ABC-TEST	ABC	11/2/2018
				► Configure	Affected: 2 devices	→	ALEX-DESKTOP	ABC	11/2/2018 (
Name	Connecting to Server	Agent inst	alled Real-time protection statu	s Created	Application version				
ABC-TEST	2 minutes ago	Ves	Running	1 weeks ago	11.0.0.6499				
ALEX-DESKTOP	6 minutes ago	🗸 Yes	Running	2 weeks ago	11.1.0.15605				

1.1 теперь S 11

	Windows domain	Date	
ST	ABC	11/2/2018 6:10:46 PM	
ESKTOP	ABC	11/2/2018 6:10:47 PM	

Refresh

Kaspersky Security Center 11: удаленная установка

Kaspersky Security Center 10

Force download of the inst	llation package		
Using Network Agent			
Using operating system	resources by means of update	agents	
Using operating system	resources by means of Admini	stration Server	
To use AWS Integration,	the Administrator needs dedic	ated keys.	
Do not install application in	it is already installed		
Assign the package install	ation in the Active Directory gro	oup policies	
	<u>Closing runnir</u>	og applications before installation st	arts

Kaspersky Security Center 11

		×
	New Task Wizard	
2	Settings	
	Force installation package download ✓ Using Network Agent Using operating system resources through distribution points ✓ Using operating system resources through Administration Server To perform installation by using the API of a doud service provider, you need a special license. Learn more	
	Behavior for devices managed through other Administration Servers Install always Install only on devices managed through this Administration Server	
	Do not re-install application if it is already installed Assign package installation in Active Directory group policies	
	Close all running applications before installation starts	
	Next Cance	4

Операционные системы

New Web Console

Изменения в интерфейсе ММС-консоли администрирования

KASPERSKY

Поддержка DIFF-файлов обновлений

Изменения в работе Агентов обновлений

Обратная совместимость плагинов KES

Улучшения в RBAC

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы Новые компоненты KES Компонент AMSI Protection Provider Компонент Adaptive Anomaly Control Проверка зашифрованного трафика Защита от MAC Spoofing Role Based Access Control for KES

Kaspersky Security Center 11: улучшение RBAC

Kaspersky Security Center 10

Properties: Administration Server SECU	RITY-CENTER —		×
Sections	User roles		
General Event configuration Keys KSN proxy server Server connection settings Virus outbreak Traffic Events storage Web server Revision history storage Application categories Security User roles Update agents Tagging rules Notification delivery settings Revision history Advanced	List of user roles: Name Administration Server Administrator Administration Server Operator Installation Administrator Kaspersky Endpoint Security Administrator Kaspersky Endpoint Security Operator Main Administrator Mobile Device Management Administrator Mobile Device Management Operator Self Service Portal User Vulnerability and Patch Management Operator Vulnerability and Patch Management Operator Vulnerability and Patch Management Operator Mobile Device Management Operator		×
<u>Help</u>	OK Cancel	App	bly

Kaspersky Security Center 11

Properties: Administration Serv	er SECURITY-CENTER —		×
Sections	User roles		
General	List of user roles:		
Event configuration Keys KSN Proxy Server connection settings Virus outbreak Traffic Events storage Web Server Revision history storage Application categories Security User roles Update agents	Name Administration Server Administrator Administration Server Operator Auditor Installation Administrator Installation Operator Kaspersky Endpoint Security Administrator Kaspersky Endpoint Security Operator Main Administrator Main Operator Mobile Device Management Administrator Security Officer Self Service Portal User Supervisor Vulnerability and Patch Management Administrator Vulnerability and Patch Management Operator		×
Tagging rules Global list of subnets Notification delivery settings Revision history Advanced	Add Modify Add Relay list of roles to slave Administration Servers	~	0-
Help	OK Cancel	Appl	у

KASPERSKY[®]

Kaspersky Security Center 11: НОВЫЕ ОТЧЕТЫ

Kaspersky Security Center 11					KASPERSKY	— Добав	лены н
Report on the status of application components Friday, November 2, 2018 7:40:53 PM This report provides information about the statuses of con installed, and the number of administration groups to whi	nponents installed / not installed on the networked devices. For each ch those devices belong. This report is generated for all groups.	of the installed components, the report includes the nu	mber of devices on whi	ch this component is	Open report template properties Configure report columns Save to disk Refresh report data	— Ada — Rep rule	ptive Ar ort on A es state
2 2 2 2 2 2 2 2 2 5 5 5 5 5 5 5 5 5 5 5	2 2 2 Components: 1 1 1 1 Application Control 11.1.0.155 1 Behavior Detection 11.1.0.159	546-2 546-2				— Rep con — Rep	ort on t nponent ort on t
Number o	Exploit Prevention 11.1.0.1554 File Threat Protection 11.1.0.1554 File Threat Protection 11.1.0.1554 Network Threat Protection 11.1.0.1554 Network Threat Protection 11.1.0.156 Application Control 11.1.0.156 Behavior Detection 11.1.0.156	66 2 155546: 2 5546: 2 1.0.15546: 2 5546: 2 1.10.15605: 1 505: 1 Construction of application of	components			by o tecl	compone nnology
Summary:		Details 54 of 54	Group A	During O	Ambientice	Composition of the	Composite to the
Component name ^	Component version ^	Virtual Administration Server	Group	CRV2000D2	Application -	Component name 44	component status
Application Control	11.1.0.15005		Servers	<u>3RV2000R2</u>	Naspersky endpoint security for windows [1].	(Adaptive Assessed) Control	Nationate II and
Application Control	11.1.0.15546		Comune	CRV2008R2	Kananala, Endersint Casualt, for Windows (11)	1.0) Adaptive Anomaly Control	Not installed
	11.1.0.15546		Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.	Adaptive Anomaly Control 1.0) AMSI Protection Provider	Not installed
Behavior Detection	<u>11.1.0.15546</u> <u>11.1.0.15605</u> <u>11.1.0.15546</u>		<u>Servers</u>	<u>SRV2008R2</u> <u>SRV2008R2</u>	Kaspersky Endpoint Security for Windows (11. Kaspersky Endpoint Security for Windows (11.	Adaptive Anomaly Control 1.0) AMSI Protection Provider 1.0) Application Control	Not installed Not installed Stopped
Behavior Detection Behavior Detection	11.1.0.15546 11.1.0.15605 11.1.0.15546 11.1.0.15605		<u>Servers</u> <u>Servers</u> <u>Servers</u>	<u>SRV2008R2</u> <u>SRV2008R2</u> <u>SRV2008R2</u>	Kaspersky Endpoint Security for Windows (11. Kaspersky Endpoint Security for Windows (11. Kaspersky Endpoint Security for Windows (11.	Adaptive Anomaly Control 1.0) AMSI Protection Provider 1.0) Application Control 1.0) BadUSB Attack Prevention	Not installed Not installed Stopped Not installed
Behavior Detection Behavior Detection Device Control	11.1.0.15546 11.1.0.15546 11.1.0.15605 11.1.0.15605 11.1.0.15605		<u>Servers</u> <u>Servers</u> <u>Servers</u> <u>Servers</u>	<u>SRV2008R2</u> <u>SRV2008R2</u> <u>SRV2008R2</u> <u>SRV2008R2</u>	Kaspersky Endpoint Security for Windows (11. Kaspersky Endpoint Security for Windows (11. Kaspersky Endpoint Security for Windows (11. Kaspersky Endpoint Security for Windows (11.	Adaptive Anomaly Control 1.0) AMSI Protection Provider 1.0) Application Control 1.0) BadUSB Attack Prevention 1.0) Behavior Detection	Not installed Not installed Stopped Not installed Running
Behavior Detection Behavior Detection Device Control Exploit Prevention	11.1.0.15546 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15546		Servers Servers Servers Servers Servers	<u>SRV2008R2</u> <u>SRV2008R2</u> <u>SRV2008R2</u> <u>SRV2008R2</u> <u>SRV2008R2</u>	Kaspersky Endpoint Security for Windows (11. Kaspersky Endpoint Security for Windows (11.	I.0) Adaptive Anomaly Control I.0) AMSI Protection Provider I.0) Application Control I.0) BadUSB Attack Prevention I.0) Behavior Detection I.0) Device Control	Not installed Not installed Stopped Not installed Running Not installed
Behavior Detection Behavior Detection Device Control Exploit Prevention Exploit Prevention	11.1.0.15546 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15646 11.1.0.15605		Servers Servers Servers Servers Servers Servers	<u>SRV2008R2</u> <u>SRV2008R2</u> <u>SRV2008R2</u> <u>SRV2008R2</u> <u>SRV2008R2</u> <u>SRV2008R2</u>	Kaspersky Endpoint Security for Windows (11. Kaspersky Endpoint Security for Windows (11.	Adaptive Anomaly Control 1.0) AMSI Protection Provider 1.0) Application Control 1.0) BadUSB Attack Prevention 1.0) Behavior Detection 1.0) Device Control 1.0) Endpoint Sensor	Not installed Not installed Stopped Not installed Running Not installed Not installed Not installed
Behavior Detection Behavior Detection Device Control Exploit Prevention Exploit Prevention Elie Threat Protection	11.1.0.15546 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15546 11.1.0.15546 11.1.0.15546		Servers Servers Servers Servers Servers Servers Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11. Kaspersky Endpoint Security for Windows (11.	L0) Adaptive Anomaly Control L0) AMSI Protection Provider L0) Application Control L0) BadUSB Attack Prevention L0) Behavior Detection L0) Device Control L0) Endpoint Sensor L0) Exploit Prevention	Not installed Not installed Stopped Not installed Running Not installed Not installed Not installed Running Running
Behavior Detection Behavior Detection Behavior Detection Device Control Exploit Prevention Exploit Prevention Eile Threat Protection Eile Threat Protection	11.1.0.15546 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15546 11.1.0.15605 11.1.0.15605		Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11. Kaspersky Endpoint Security for Windows (11.)	L.0) Adaptive Anomaly Control L.0) AMSI Protection Provider L.0) Application Control L.0) BadUSB Attack Prevention L.0) Behavior Detection L.0) Device Control L.0) Endpoint Sensor L.0) Exploit Prevention L.0) Exploit Prevention	Not installed Not installed Stopped Not installed Running Not installed Not installed Running Not installed Running Not installed
Behavior Detection Behavior Detection Behavior Detection Device Control Exploit Prevention Exploit Prevention Eile Threat Protection Eile Threat Protection Eile Threat Protection Eile Threat Protection	11.1.0.15546 11.1.0.15805 11.1.0.15605 11.1.0.15605 11.1.0.15546 11.1.0.15546 11.1.0.15546 11.1.0.15546 11.1.0.15546		Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11. Kaspersky Endpoint Security for Windows (11.	1.0) Adaptive Anomaly Control 1.0) AMSI Protection Provider 1.0) Application Control 1.0) BadUSB Attack Prevention 1.0) Behavior Detection 1.0) Device Control 1.0) Endpoint Sensor 1.0) Exploit Prevention 1.0) Exploit Prevention 1.0) File Level Encryption 1.0) File Threat Protection	Not installed Not installed Stopped Not installed Running Not installed Running Not installed Running
Behavior Detection Behavior Detection Behavior Detection Device Control Exploit Prevention Exploit Prevention Eile Threat Protection Eile Threat Protection Eile Threat Protection Eile Threat Protection Eile Avention Eile Avent	11.1.0.15546 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15546 11.1.0.15546 11.1.0.15546 11.1.0.15546 11.1.0.15546 11.1.0.15546		Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11.	1.0) Adaptive Anomaly Control 1.0) AMSI Protection Provider 1.0) Application Control 1.0) BadUSB Attack Prevention 1.0) Behavior Detection 1.0) Device Control 1.0) Endpoint Sensor 1.0) Exploit Prevention 1.0) File Level Encryption 1.0) File Threat Protection	Not installed Not installed Stopped Not installed Running Not installed Not installed Running Not installed Running Not installed Running Running Running Running Running
Behavior Detection Behavior Detection Device Control Exploit Prevention Exploit Prevention File Threat Protection File Threat Protection Eirewall Host Intrusion Prevention Mail Threat Protection	11.1.0.15546 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15546 11.1.0.15546 11.1.0.15546 11.1.0.15546 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605		Servers	SRV2008R2 SRV2008R2	Kaspersky Endpoint Security for Windows (11.	1.0) Adaptive Anomaly Control 1.0) AMSI Protection Provider 1.0) Application Control 1.0) BadUSB Attack Prevention 1.0) Behavior Detection 1.0) Device Control 1.0) Endpoint Sensor 1.0) Exploit Prevention 1.0) File Level Encryption 1.0) File Threat Protection 1.0) Exploit Prevention	Not installed Running Not installed Running Not installed Running Not installed Running Not installed
Behavior Detection Behavior Detection Behavior Detection Device Control Exploit Prevention Exploit Prevention Eile Threat Protection Eirewall Host Intrusion Prevention Mail Threat Protection Network Threat Protection	11.1.0.15546 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605		Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11. Kaspersky Endpoint Security for Windows (11.)	L0 Adaptive Anomaly Control L0 AMSI Protection Provider L0 Application Control L0 BadUSB Attack Prevention L0 Behavior Detection L0 Device Control L0 Endpoint Sensor L0 Exploit Prevention L0 Eile Level Encryption L0 File Threat Protection L0 Firewall L0 Encryption	Not installed Not installed Stopped Not installed Running Running Not installed Not installed Running Runn
Behavior Detection Behavior Detection Behavior Detection Device Control Exploit Prevention Exploit Prevention Eile Threat Protection Eirewall Eirewall Host Intrusion Prevention Mail Threat Protection Network Threat Protection	11.1.0.15546 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15646 11.1.0.15646 11.1.0.15646 11.1.0.15646 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15546		Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11. Kaspersky Endpoint Security for Windows (11.)	L0 Adaptive Anomaly Control L0 AMSI Protection Provider L0 Application Control L0 BadUSB Attack Prevention L0 Behavior Detection L0 Device Control L0 Endpoint Sensor L0 Exploit Prevention L0 Eile Level Encryption L0 File Threat Protection L0 File Threat Protection L0 File Unit Sensor L0 File Threat Protection L0 File Threat Protection L0 File Threat Protection	Not installed Not installed Stopped Not installed Running Not installed Not installed Not installed Not installed
Behavior Detection Behavior Detection Device Control Exploit Prevention Exploit Prevention Elie Threat Protection Eirewall Firewall Host Intrusion Prevention Mail Threat Protection Network Threat Protection 002.11.1: Kaspersky Endpoint Security	11.1.0.15546 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15646 11.1.0.15646 11.1.0.15646 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15605 11.1.0.15546		Servers	SRV2008R2	Kaspersky Endpoint Security for Windows (11. Kaspersky Endpoint Security for Windows (11.) Kaspersky Endpoint Security for Windows (11.)	L.0 Adaptive Anomaly Control L.0 AMSI Protection Provider L.0 Application Control L.0 BadUSB Attack Prevention L.0 Behavior Detection L.0 Device Control L.0 Endpoint Sensor L.0 Exploit Prevention L.0 File Level Encryption L.0 File Threat Protection L.0 File Unsk Encryption L.0 Full Disk Encryption L.0 Host Intrusion Prevention	Not installed Stopped Stopping Not installed Running Not installed Not installed Running Not installed Running Not installed Running Not installed Running Not installed

Re Re

ены новые отчеты

- ive Anomaly Control report
- t on Adaptive Anomaly Control state
- t on the status of application onents
- t on threat detection distributed mponent and detection ology

Component version

1.1.0.15546

1.1.0.15546

1.1.0.15546

11.1.0.15546

1.1.0.15546

KASP	ERSKY

Новые отчеты: Report on threat detection distributed by component and detection technology

eport on threat dete	ection distrib	uted b	y com	ponent	and o	letecti	on tec	hnolo	gy														0.770	Ø
aspersky Secur	ity Center	11																					KAS	PERSKY
oort on threat detu ay, November 2, 2018 od: from Wednesday, report provides infoi	tection distrit 8 7:35:29 PM October 3, 2011 rmation about 1	outed 8 to Fri threats	by con	ember 2	nt and 2, 2018 ious co	dete	ction t	echno	blogy	chnolo	ogies.	. This re	eport is generate	ed for	all groups.							Open	report templat Configure rep <u>Refresh</u>	te properti port colum Save to di preport da
	Detection	sby	ompor	ents a	nd tee	hnolo	dies:																	⊖ Prin
									2	m	4	5												
Unknown			4		14		0, 1		1	1	1	-												
le Threat Protection			_						_	_	10	-												
I Threat Protection			1	-		-	-	-			15	_												
h Threat Protection			_		_	_	-		_	_														
D Threat Protection		_	_		_	_		_	_	_	_	_												
IN Anti-Virus	_					_		-			-	-												
xploit Prevention					-	-	-				-	-												
Intrusion Prevention	ion						_			_	_	D	etection tech	nolog	ay:									
Firewall						_					-		Unknown											
ehavior Detection										_	_		Machine lear	ning										
xploit Prevention												_	Cloud analys	HS										
	0 - 0	n v	4	9 2	2	00	6 0	=	12	13	14	15	Behavior De	tection	n									
	0 - 0	n n	4	9 2	7	60	6	2 1	12	13	14	15	Behavior De Automatic an	tection alysis	n 5									
mary:	D - C	~ T	+	6 9	- C	eats	6 01	2 E	71	13	14	Se e	Behavior Dei Automatic an	tection alysis	n 5 reats	Threat	rs ^	Uniqu	e threats ^	Devices with	∧ First detect	ed ^	Last detecte	ed ^
nponent ^ Dr	Detection echnology	ν m d	+ hreats etected	و ک	- C Thr disi	eats	6 0	C Db	jects leted	13	- 14	Spanner Stratter	Behavior Del Automatic an s that have	Thi log	n s reats	Threat	ts ^	Uniqu	e threats ^	Devices with detected threats	^ First detect	ed ^	Last detecte	ed ^
Imary: Imponent ^ Driventian Dri	etection echnology	^ T d 1	threats etected	م	- Z Thr disi	eats nfected	o C	C E Ob del	jects eted	13	1	Sp Threats	Behavior Del Automatic an s that have fisinfection	This of the second seco	n 5 reats ^ gged	Threat blocke	ts ^ ed	Uniqu 4	e threats ^	Devices with detected threats 2	 First detect Thursday, 6 2018 12:37 	ed ^ October 25, :04 PM	Last detecte Friday, Nov 2018 7:34:4	ed ^ ember 2, 1 PM
nmary: mponent ^ D. te Infreat tection As tection As	b – c Petection echnology xpert analysis utomatic analys	^ T d 1 sis 1	treats etected	<u>م</u>	- L Thr disi 0 0	eats nfected	0 0	Cob del 14	jects	13		SP Threats failed d 0	Behavior Del Automatic an	This log	n s reats ^ gged	Threat blocke 0 1	ts ^ ed	Uniqu 4 1	e threats ^	Devices with detected threats 2 1	 First detect Thursday, (2018 12:37 Friday, Nov 2018 7:32:2 	ed October 25, 04 PM vember 2, 19 PM	Last detecte Friday, Nove 2018 7:34:4 Friday, Nove 2018 7:32:20	ed o ember 2, 1 PM ember 2, 9 PM
nmary: pmponent ^ D, te e Threat eb Threat tection b Threat tection Ex	b - c Petection echnology xpert analysis utomatic analysis xpert analysis	A T d A A T d A A T d A A T d A A T d A	hreats atected	م م	-L Thr disi 0 0	eats nfected	6	2 E 0b del 14 0 0	jects eted	13	()	Threats failed d 0	Behavior Del Automatic an	tection alysis Thi log 0 0 0	n s	Threat blocke 0 1	ts ^ ed	Uniqu 4 1	e threats ^	Devices with detected threats 2 1 1	 First detect Thursday, (2018 12:37 Friday, Nov 2018 7:32:3 Friday, Nov 2018 7:29:3 	ctober 25, :04 PM rember 2, !9 PM rember 2, :66 PM	Last detects Friday, Nov 2018 7:34:4 Friday, Nov 2018 7:32:2 Friday, Nov 2018 7:29:5	ed ^ ember 2. 1 PM ember 2. 9 PM ember 2. 6 PM
mmary: pmponent ^ Drite le Threat <u>Ea</u> otection <u>Au</u> eb Threat <u>Ex</u> otection <u>Ex</u> otection <u>Ex</u> otection <u>Ex</u>	b – o Petection echnology xpert analysis utomatic analysis xpert analysis Unique t	A T d d 1 1 1 1 1 1 1 1 1	ogies: 2		- C Thr disi 0 0 0 0 Jnique	eats nfected device:	5 C	2 E Obj del 14 0	-72 jects eted	13	()	Threats failed d	s that have sisinfection	tection alysis 0 0 0	n s	Threat blocke 0 1	ts ^	Uniqu 4 1	e threats ^	Devices with detected threats 2 1 1	 First detect Thursday, J. 2018 12:37 Friday, Nov 2018 7:32:1 Friday, Nov 2018 7:29:1 	eed October 25, 04 PM vember 2, 19 PM vember 2, 56 PM	Last detecte Friday. Nov 2018 7:34:4 Friday. Nov 2018 7:32:2 Friday. Nov 2018 7:29:5	ed ^ 1 PM ember 2, 9 PM ember 2, 6 PM
nmary: imponent ^ Dr te <u>e Threat</u> Es <u>threat</u> As <u>thection</u> Ex <u>thection</u> Ex <u>thection</u> Ex <u>que components: 2</u> <u>ails 17 of 17</u>	b – o echnology xpert analysis utomatic analysis xpert analysis Unique t	T T d	hreats etected	<u>له</u> الم	 Thr disi 0 0 0 Jinique 	eats nfected	o	2 E	72 jects eted	13	()	Threats failed d 0	Behavior Del Automatic an	Thillog 0	n s	Threat blocke 0 1	ts A	Uniqu 4 1	e threats ^	Devices with detected threats 2 1 1	 First detect Thursday, I 2018 12:37 Friday, Nov 2018 7:32:1 Friday, Nov 2018 7:29:1 	ed Cotober 25, 04 PM rember 2, 19 PM rember 2, 6 PM	Last detecte Friday, Nov 2018 7:34:4 Friday, Nov 2018 7:32:2 Friday, Nov 2018 7:29:5	ember 2, 1 PM ember 2, 9 PM ember 2, 6 PM
mmary: mponent D: te e Threat eb Threat stection eb Threat stection ique components: 2 cails 17 of 17 Dup Den	b = c Detection echnology xpert analysis utomatic analysis vert analysis Unique t evice ^	T T d T d T d T d T d T d Dete	the state of the s	L L L L L L L L L L L L L L L L L L L	 Thr 0 0 0 Jnique 	eats nfected	o c d s: 2 Detect	2 E del 14 0 0	jects ieted	£ Comp	2 1 1 1 ((((((((((((((((바 Threats failed d 0 0 0	Behavior Del Automatic an sthat have disinfection	 Thillog 0 0 0 	n s	Threat blocke	ts ^ ed Object type	Uniqu 4 1	e threats ^ Action ^	Devices with detected threats 2 1 1	 First detect Thursday, No 2018 12:37 Friday, No 2018 7:29:3 	eed Cotober 25, 304 PM rember 2, 36 PM Accourt	Last detects Friday. Nov 2018 7:34:4 Friday. Nov 2018 7:29:51 Friday. Nov 2018 7:29:51	ember 2, 1 PM ember 2, 9 PM ember 2, 6 PM
mmary: pomponent ^ Dr te ie Threat otection Ai deb Threat Ai otection Es otection Es tails 17 of 17 roup ^ Der forkstations ABS	b = c Petection echnology xpert analysis utomatic analysis vice ^ c-TEST	A T d d d 1 1 1 1 1 1 0 ecchnol	nreats etected 5 cted obj R-Test-F	در م ect م ile	C Thr disi 0 0 0 Unique	eats nfected	on c s: 2 Detect Friday, Novem 2018 7	2 E Object 2, 29:56	2 jjects jeted	Comp Web 1	* 1 ((((()	Threats failed d 0 0	Behavior Del Automatic an sthat have bisinfection Detection technology Expert analy	tection alysis 0 0 0 0 0 0	Path to file Attp:// www.eicar.org download/eici	Threat blocke 0 1 1 1	ts ^ ed Object type	Uniqu 4 1 1	e threats ^ Action ^ Result Blo Administra 275a021bb c2fe2a202	Devices with detected threats 2 1 1 1 1 1 cked: EICAR-Test-File tor (Active user) Obje tor (Active user) Obje rog/downloa/kiear. e: 11/1/2018 2-39-00 fb6489e54d4718997 fb88ab4f511dd7	 First detect Thursday, No 2018 12:37 Friday, No 2018 7:29:3 Friday, No 2018 7:29:3 User ABC, ct. http:// m Database PM Hash; db9416637c69 	eed Detober 25, :04 PM rember 2, :9 PM rember 2, :6 PM Accour <u>Accour</u> <u>Accour</u> <u>Accour</u>	Last detects Friday. Nov 2018 7:34:4 Friday. Nov 2018 7:29:5 Friday. Nov 2018 7:29:5 t t A strator Er fg	ember 2, 1 PM ember 2, 1 PM ember 2, 9 PM ember 2, 6 PM pplication aspersky rddpoint 3

Интеграция с SIEM через Syslog

Properties: Events	- D X	
Sections	Event export	
Notification		
Event export	Automatically export events to SIEM system database	QRadar (LEEF format)
	SIEM system:	ArcSight (CEF format)
	Syslog (RFC 5424) format V	Syslog (RFC 5424) format
	SIEM system server address: 10.28.0.70 SIEM system server port: 514 Protocol: TCP/IP Maximum message size, in bytes: 2048 To export listed events starting from the specified date, click the Export archive button. Export archive	Чтобы отправлять события из Kaspersky Security Center в SIEM-систему по протоколу Syslog больше не нужна лицензия
Help	OK Cancel Apply	

Kaspersky Security Center 11: итого

• Основные изменения

- Появилась полноценная KSC Web Console
- Реализована поддержка DIFF-файлов обновлений
- Реализована поддержка обратной совместимость плагинов KES
- Агенты обновлений могут выступать в роли KSN-прокси и поддерживают до 10000 узлов

- Неосновные изменения
 - Добавление новых ролей в RBAC не требует лицензии KSC
 - Добавлены новые отчеты
 - Интеграция с SIEM системами через Syslog больше не требует лицензии KSC



Лабораторная работа №2

Внедрение Kaspersky Endpoint Security

- 1. Установите Kaspersky Endpoint Security для Windows на компьютеры сети
- 2. Изучите результаты установки

Лабораторная работа №3

Создание структуры управляемых компьютеров

1. Создайте группы рабочих станций, мобильных компьютеров и серверов

KASPERSKY

2. Распределите компьютеры по группам с помощью правил

Операционные системы New Web Console Изменения в интерфейсе ММС-консоли администрирования Поддержка DIFF-файлов обновлений Изменения в работе Агентов обновлений Обратная совместимость плагинов KES Улучшения в RBAC

KASPERSKY

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы

Новые компоненты KES Компонент AMSI Protection Provider Компонент Adaptive Anomaly Control Проверка зашифрованного трафика Защита от MAC Spoofing Role Based Access Control for KES

Kaspersky Endpoint Security 11.1: операционные системы

KASPERSKY

• Операционные системы:

- Windows 10 Redstone 5
- Windows Server 2019

Операционные системы New Web Console Изменения в интерфейсе ММС-консоли администрирования Поддержка DIFF-файлов обновлений Изменения в работе Агентов обновлений Обратная совместимость плагинов KES Улучшения в RBAC

то но	вого в Kaspersky Endpoint Security 11.1
	Операционные системы
	Новые компоненты KES
_	Компонент AMSI Protection Provider
	Компонент Adaptive Anomaly Control
	Проверка зашифрованного трафика
	Защита от MAC Spoofing
	Role Based Access Control for KES

Kaspersky Endpoint Security 11.1: НОВЫЕ КОМПОНЕНТЫ

Kaspersky Endpoint Security 11.0

Properties: Kaspersky Endpoin	t Security for Windows (11.0.0) (11.0.0.6499) — 🛛	×
Sections	Properties	
General	Standard installation \sim	
Properties	Advanced Threat Protection	^
Key Incompatible applications Revision history	Advanced innext Protection Behavior Detection Exploit Prevention Remediation Engine Host Intrusion Prevention (For workstations only) Essential Threat Protection Mail Threat Protection (For workstations only) Web Threat Protection (For workstations only) Web Threat Protection (For workstations only) Web Threat Protection File Threat Protection Web Threat Protection (For workstations only) Web Threat Protection Security Controls Web Control (For workstations only) Application Control Device Control (For workstations only) Data Encryption File Level Encryption (For workstations only) Bitlocker Management Endpoint Sensor Path to application installation folder: Path to application installation folder is specified on product side. Configuration file:	~
Help	OK Cancel Apply	

Kaspersky Endpoint Security 11.1

Properties: Kaspersky Endpoint Secu	urity for Windows (11.1.0) (11.1.0.15546) —		×
High protection level	All recommended protection components are enabled.		
Sections	Properties		
General Properties	Advanced Threat Protection		^
Key Incompatible applications Revision history	Behavior Detection Exploit Prevention Remediation Engine Host Intrusion Prevention (For workstations only) Essential Threat Protection		
	File Threat Protection Mail Threat Protection (For workstations only) Web Threat Protection (For workstations only) Network Threat Protection Firewall BadUSB Attack Prevention AMSI Protection Provider		
\rightarrow	Security Controls Image: Web Control (For workstations only) Image: Provide Control (For workstations only)		
	Data Encryption File Level Encryption (For workstations only) Full Disk Encryption (For workstations only) Bitlocker Management		~
	Path to application installation folder: Path to application installation folder is specified on the application side. Configuration file:		
Help	Browse	Clear	

Операционные системы New Web Console Изменения в интерфейсе ММС-консоли администрирования Поддержка DIFF-файлов обновлений Изменения в работе Агентов обновлений Обратная совместимость плагинов KES Улучшения в RBAC

KASPERSKY

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы Новые компоненты KES Компонент AMSI Protection Provider Компонент Adaptive Anomaly Control Проверка зашифрованного трафика Защита от MAC Spoofing Role Based Access Control for KES

Как поставщик AMSI-защиты защищает от новых

угроз?

spersky Security Center Web 🗧 🗙 🕂		– 0 ×	Взаимо
C A Not secure https://127.0.0.1	/#/management/policies/10	☆ ⊖ :	VNOBEHI
Kaspersky Endpoint Security for Windo	ws (11.1.0) XXX	₽° @ X	сценарі
High protection level.			примен
GENERAL EVENT CONFIGURATION	APPLICATION SETTINGS REVISION HISTORY POLICY PROFILES		loniusca
Advanced Threat Protection	File Threat Protection		
Essential Threat Protection	This component resides in RAM, scanning all opened, saved, and active files to er protection at all times.	AMSI Protect	ction Provider
Security Controls	Web Threat Protection This component scans inbound traffic on your computer.	AMSI provid	der
Local Tasks	Mail Threat Protection This component scans incoming and outgoing messages for dangerous objects. protocols are supported: POP3, SMTP, IMAP, MAPI, and NNTP.	AMS Enab to pe	I Protection Provider EN les Microsoft Office (and oth rform on-demand virus sca
General Settings	Network Threat Protection If Kaspersky Endpoint Security for Windows detects an attempted attack onto you any network activity of the attacking computer towards your computer will be bl	Componen	t settings
	<u>Firewall</u> This component filters all network activity according to the specified rules.	Scan of c	compound files chives stribution packages
	BadUSB Attack Prevention The component prevents the use of hacker-compromised USB devices that emu behavior.	Scan Of	ffice formats
	AMSI Protection Provider Enables Microsoft Office (and other third-party) applications to use Kaspersky End Windows to perform on-demand virus scan using Windows Antimalware Scan In	☑ Do not This setting dr Maximum fi	unpack large compoun oes not affect the scanning ile size
		8	MB (1 to 9999)

Взаимодействие с AMSI, позволяет KES увеличить уровень обнаружения вредоносных скриптов, сценариев выполняющихся в памяти и применяющих различные технологии маскировки (obfuscation and evasion techniques)

KASPERSKY



间 Kas

AMSI Protection Provider: как это работает

😕 Administrator: Windows PowerShell	- 144	×
Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved.		^
PS C:\Windows\system32> cd C:\test_files\bsstest_amsi\ PS C:\test_files\bsstest_amsi> . <mark>\bsstest_amsi.ps1</mark> @{Version=5.1.17134.228} At line:1 char:1 + #KLBssBlockMeBasesKdbAmsi#		
This script contains malicious content and has been blocked by your antivirus software. At line:1 char:1 + #KLBssBlockMeBasesKdbAmsi# AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
This script contains malicious content and has been blocked by your antivirus software. Test succeded PS C:\test_files\bsstest_amsi>		

Программа, прежде чем выполнить скрипт, отсылает его AMSI (Windows Antimalware Scan interface), и ждет вердикта

AMSI получает скрипты от программ, обрабатывает их и передает на проверку Protection Provider (KES)



KES – получает PowerShell, VBSript, Jscript от AMSI, проверяет их и отсылает назад вердикты

Выполнит или нет программа скрипт, зависит от полученного вердикта и настроек программы

AMSI Protection Provider: события

object scan result has been sent to a third-party application

The object scan result has been sent to a third-party application

Hash: 5f853d3b102811bbca1b9912c44d8aa627d0e91ed2900602ce96c73e085bfa8a

Reason: Logged

Kaspersky Endpoint Security for Windows (11.1.0)

Event properties

		Sections	General	
3 Reports	⊙ – □ ×	General	Malicious objec	t detected
 System Audit Advanced Threat Protection Behavior Detection Exploit Prevention Host Intrusion Prevention Essential Threat Protection File Threat Protection Web Threat Protection Mail Threat Protection Firewall Network Threat Protection Advanced Threat Protection Mail Threat Protection Firewall Network Threat Protection 	AMSI Protection Provider Save report Show period: Day Today, 12-Nov-18 Show importance Today, 12-Nov-18 Today, 12-Nov-18 Show importance The object scan result has been sent to a third-party application Show Show T2-Nov-18 Show importance The object scan result has been sent to a third-party application Show Show T2-Nov-18 Show importance The object scan result has been sent to a third-party application Show Show T2-Nov-18 Show importance The object scan result has been sent to a third-party application Show Show T2-Nov-18 Show importance The object scan result has been sent to a third-party application Show Show T2-Nov-18 Show importance The object scan result has been sent to a third-party application Show Show T2-Nov-18 Show importance The object scan result has been sent to a third-party application Show Show T2-Nov-18 Show importance The object scan result has been sent to a third-party application Show Show T2-Nov-18 Show importance The object scan result has been sent to a third-party application Show Show T2-Nov-18 Show Show T2-Nov-18		Severity: Application: Version number: Task name: Device: Group: Time: Virtual Administration Serv Description: Result: Detected: HEU User: DESKTOP-M38QE Object: unnamed_ams Reason: Expert analys Database release date	Critical event Kaspersky Endpoint Security for Windows (11.1.0) 11.1.0.15626 AMSI Protection Provider DESKTOP-MJ8QETO WORKGROUP 11/12/2018 11:53:29 AM ver name: IR:Trojan.Multi.AmsiKdbDetect.gen ETO[VB (Active user) is_stream_17 sis
Security Controls Application Control Device Control Control Adaptive Anomaly Control Tasks Control Control Tasks Control Control Tasks Control Control Tasks Control C	12-Nov-18 11:53:26 : The object scan result has been sent to a third-party application Application: Windows PowerShell Use: DESKTOP-MU8QETO/VB (Active user) Component: AMSI Protection Provider Result: Untreated: HEURTrojan.Multi.AmsiKdbDetect.gen Object: unnamed_amsiztream_16 Reason: Logged Hash: S7b998003317995fe77ba724267e555aeeb6be33930c5febbacbf54351c514e5	Ceneral	berties General Severity Applicati Version Task nai Device: Group: Time:	al The object scan result has been sent to a third-party applica The object scan result has been sent to a third-party appli
	Close		Virtual A Descripti Event 1 Applica Applica User: Compo Result ¹ Result ¹ Result ¹ Result ¹ Result ¹ Object Object Object	Idministration Server name: ion: type: The object scan result has been sent to a third-party ap ition\Vame: Windows\System32\VindowsPowerShell ition\Parti: C:\Vindows\System32\VindowsPowerShell\v1.0\ tion\ProcessID: 6900 DESKTOP+M3QETO\V8 (Active user) nent: AMSI Protection Provider \Description: Untreated (Type: Trojan Wame: HEUR:Trojan.Multi.AmsiKdbDetect.gen (Threat level: High \Precision: Exactly t: unnamed_amsi_stream_17//amsi_script_utf8 \Vame: amsi script_utf8

KASPERSKY

K Reports



Лабораторная работа №4

Как проверить Защиту от бесфайловых угроз



Операционные системы New Web Console Изменения в интерфейсе ММС-консоли администрирования Поддержка DIFF-файлов обновлений Изменения в работе Агентов обновлений Обратная совместимость плагинов KES Улучшения в RBAC

KASPERSKY

Что нового в Kaspersky Endpoint Security 11.1

- Операционные системы Новые компоненты KES Компонент AMSI Protection Provider Компонент Adaptive Anomaly Control Проверка зашифрованного трафика Защита от MAC Spoofing
- Role Based Access Control for KES

Что такое Adaptive Anomaly Control

- Новый компонент, который предназначен для детектирования и блокирования нетипичного поведения приложений
- Для детектирования аномального поведения Adaptive Anomaly Control использует набор правил, которые поставляются вместе с базами
- Нетипичное поведение необязательно вредоносное, поэтому по умолчанию компонент Adaptive Anomaly Control работает в Smart Mode
- В течение нескольких недель компонент отслеживает активность на компьютерах и передает информацию о срабатываниях на Сервер администрирования
- Администратор должен обработать событие, подтвердить, что это аномальная активность или добавить в исключения, если активность легитимная
- На каждом компьютере, для каждого правила обучение происходит независимо, т.е. где-то обучение завершится раньше, где-то позже

Где настраивается Adaptive Anomaly Control

Kaspersky Endpoint Security 11 for Windows	≓	В политике Kaspersky Endpoint Security			
High protection level.		По умолчанию ААС вклю	анию ААС включен и работает в режиме		
GENERAL EVENT CONFIGURATION APPLICATION SETTINGS REVISION HISTORY POLICY PROFILE	S	Smart			
Advanced Threat Protection Application Control Essential Threat Protection This component monitors users' attempts to start applications and control startup of applications by using rules.	ontrols the				
Security Controls Device Control	Adaptive Anomal	r Control	г ^а © х		
Endpoint Sensor					
Local Tasks Web Control General Settings This component allows you to control access to web resources their content and location. Adaptive Anomaly Control This component detects and blocks abnormal behavior of apple	Adaptive Anomal Adaptive A This compo Reports Rule status report Rule triggering re	r Control nomaly Control ENABLED ⑦ hent detects and blocks abnormal behavior of applications.	A Enforce		
	Rules		🔒 Enforce 📧		
	Rules				
	Templates				
	Blockage	Message to administrator			
			ок		

Правила Adaptive Anomaly Control

0 0	O Rules				۳° ۵	0 0 0	⑦ Rule				F 0
0	Rules It is required to approve updates for the Adaptive Anomaly Control rul		×			Non-standard file for the folder The program and/or script is run from a stand Status On Action Smart			a standard or system directory that does not contain such executable files in the default cor		
	✓ Edit ✓ Approve updates SE Import SE Export						Block Notify				
	Rule	Status	Action	Exclusion	Changes		Exclusion				
	□ > Activity of office applications						+ Add ∥ Edit ×	Delete			≝≣ Filter
	Use of Windows Management Instrumentation (WMI)						User or group	Source process	Source object	Target process	Target object
	Activity of script engines and frameworks								No data		
	□ ∨ Abnormal program activity										
_	Non-standard file for the folder	On On	Smart v	No	New	Из наст	гроек у прав	ил есть со	стояние Е	Зкл/Вык <mark>л</mark>	1 , режим
	System file in a non-system folder	On On	Smart 🗸	No	New	работы	Smart/Block	/Notify и и	сключени	Я	
	Untrusted application with a system-like name	On On	Smart 🗸	No	New						
				ОК	CANCEL						

Adaptive Anomaly Control имеет предустановленный набор правил, которые могут обновляться вместе с базами

Сообщение Approve Updates носит уведомительный характер

Что происходит в режиме Smart Training

BACKUP

Kaspe	rsky Security Center ORING & REPORTIN	ADMINISTRA IG 🗖 DEVICE PARTY APPLICATI	TION SERVER SECURITY-CENTER ~ 🕸 S 🖧 USERS & ROLES 🕼 DISCON	Console Settings ~ ABC\A	dministrator ~ 🏳		 QUARANTINE active threats INSTALLATION PACKAGES HARDWARE
✓ Confi	rm + Exclude	Properties	≞≞ Filter				 DELETED OBJECTS TRIGGERING OF RULES IN SMART TRAINING MODE
	dministration group	Device name	User name	Name	Detections count		
	anaged devices		ABC\Tom	Non-standard file for the folder	1	0 Sm	умолчанию ААС работает в режиме
	anaged devices		ABC/IOM	System rite in a non-system rolder	1	5111	
Ma Ma	anaged devices	TOM-LAPTOP	NT AUTHORITY/NETWORK SERVICE	Start of Microsoft Powershell From WMI	2	Ba	том режиме ничего не блокируется,
□ Ma	anaged devices	TOM-LAPTOP	NT AUTHORITY\NETWORK SERVICE	Start of Microsoft HTML Application Host from WMI	1	оді	нако информация обо всех
🗌 Ma	anaged devices	TOM-LAPTOP	NT AUTHORITY\NETWORK SERVICE	Start of Microsoft Powershell From WMI	1	CDa	абатываниях попадает в KSC в
						КОН	нтейнер Triggering of Rules in Smart
						Tra	ining Mode
							5

Что делать с событиями в режиме Smart

0		F.	0	×	
✓ Confirm + Exclude					
Name	Non-standard file for the folder				
Processed					
Status					
Virtual Administration Server					
Administration group	Managed devices				
Device name	TOM-LAPTOP				
Detections count	1				
User name	ABC\Tom				
Source process path	c:\kes11.1_aac_trigger\abnormal_program_activity\non_standard_file_for_the_folder.bat				
Source process hash	68091E112629715D54B535DD8F267BCCBFE07B5C6A72B1ED925D8078845B5252				
Source object path					
Source object hash					
Target process path	C:\Users\tom.ABC\poWeRSHell.exe				
Target process hash	34507738F84B9D4F231DC0C187FEE4A03B4DDB84CF63FF56A4A1761A9BD56EA6				
Target object path	object://cmdline:C:\Users\tom.ABC\poWeRSHell.exe				
Target object hash					

Режим Smart предполагает участие администратора

Администратору желательно обработать событие:

- Confirm
- Exclude
Что увидит пользователь, если ААС перешел в режим Block?



Пользователь может:

- Смириться
- Пожаловаться (ссылка Запросить доступ)

Шаблон запроса настраивается в политике KES

Куда уйдет просьба пользователя?

Kas	spersky Security Center	ADMINISTRATION SERV	ER SECURITY-C	enter - 🗇	<u>Console Settings</u> ~	ABC\Administrator ~ 🏳
В МОК	NITORING & REPORTING	G 🖬 DEVICES 🦓 US	SERS & ROLES		Event details	×
		A EVENT SELECTIONS		IONS	Task name	Protection
Selection		All selections			Application activity bloc 01/23/2019 5:12 am <u>Managed devices</u> <u>TOM-LAPTOP</u>	ckage message to administrator
+ Add	d 🕞 Start 🕞 Rec	onfigure sorting and start	imes Delete		Application	Kaspersky Endpoint Security 11 for Windows
	Selection name			Selection	Version	11.1.0.17068
	User requests		-	Predefine		Hello!
	Recent events			Predefine		Please allow me to perform a susp
	Critical events			Predefine		with the Adaptive Anomaly Contro Parameters of suspicious activity:
	Functional failures			Predefine		Source process: c:\windows\syster Source process hash:
	<u>Warnings</u>			Predefine		ec436aeee41857eee5875efdb7166 Source object: <not defined=""></not>
	Informational message	25		Predefine	Description	Source object hash: <not defined=""> Target process:</not>
	Audit events			Predefine		C:\KES11.1_AAC_trigger\Abnormal Target process hash:
	AppControl			Liter seler		d6de672b339b6782db843578ead Target object:
	<u>Appeontrot</u>			User selec		object://c:\KES11.1_AAC_trigger\Al Target object hash: <not defined=""></not>
	Device Control			User selec		Information about suspicious activ Computer: TOM-LAPTOP
	New event selection			User selec		

На Сервер КSC в виде события, в котором будет:

- Текст, который пользователь может редактировать
- Описание подозрительной _ активности, которая была заблокирована, с указанием процессов и контрольных сумм
- Имя пользователя _
- Компьютер

Дата и время

Администратор может:

- Ознакомиться с сообщением
- Просмотреть свойства компьютера
- Подумать
 - Добавить в исключения ААС **КАЗРЕВЗКУ**

Как еще можно добавить исключения в ААС?

0	Result of	Recent events on 01/23	/2019 7:41 am			≓්
	€ Ref	resh list $ imes$ Delete	④ Export to file	C Assign to category	Revision history	E Exclude from Adaptive Anomaly Control
		Time	Device	Event		Description
		01/23/2019 5:52 am	SECURITY-CENTER	Runtime error.		Runtime error: Database error occured: #19. Error details: 1950/8152 (Generic db error: "&
	M	<u>01/23/2019 5:49 am</u>	TOM-LAPTOP	Process action skipped		Event type: Process action blocked User: ABC\Tom (Active user) Component: Adaptive Anomaly Control Rule name: Start of Microsoft Windows Com Path to source process file: c:\program files Source process file hash: 270fe63cca815691 Path to source object: c:\kes11.1_aac_trigge Source object hash: f5eee1b8c1d0e12b8ea3 Path to target process file: C:\Windows\SysV Target process file hash: 4c3ea4c44aab7435 Path to target object: object://cmd.exe
		01/23/2019 5:46 am	SECURITY-CENTER	Audit: Object has been mo	odified.	Policy "Kaspersky Endpoint Security 11 for W
		01/23/2019 5:45 am	SECURITY-CENTER	Audit: Object has been mo	odified.	Policy "Kaspersky Endpoint Security 11 for W
		711 51		_		Event type: Process action blocked User: ABC\Tom (Active user) Component: Adaptive Anomaly Control Rule name: Start of Microsoft Windows Com Path to source process file: c:\program files

В ААС можно добавлять в исключения прямо из событий

Process action skipped 01/23/2019 5:49 am <u>Managed devices</u> TOM-LAPTOP Application Version	Kaspersky Endpoint Security
Application Version	Kaspersky Endpoint Security
Version	11101 111100103
	11.1.0.17068
Description	Event type: Process action blocked User: ABC\Tom (Active user) Component: Adaptive Anomaly Ci Rule name: Start of Microsoft Wind application Path to source process file: c:\prog office\office15\winword exe Source process file hash: 270fe63cca8156911303ebdf94811 Path to source object: c:\kes111_a prompt.doc Source object hash: f5eee1b8c1d0e12b8ea3ab0266e8 Path to target process file: C:\Wind Target process file hash: 4.3ea4c44aab74350355c4198261 Path to target object: object://cmo
Event registered	01/23/2019 5:49 am

Какие события есть у Adaptive Anomaly Control?

AAC AAC				₽ °
General	Applicati	on name	~	
Events	Version			
Devices Time	Task nan	ne		
Security	Severity	level	Critical	
	Inclu	ide general events		
		Severity level	Event name	
		Critical	The object cannot be deleted	
		Critical	Processing error	
		Critical	Dangerous link blocked	
		Critical	Dangerous link opened	
		Critical	Previously opened dangerous link detected	
		Critical	Process terminated	
		Critical	Unable to terminate process	
		Critical	Process action skipped	
			Pending changes SAVE 0	CANCEL

У Adaptive Anomaly Control есть два типа событий:

- Process action skipped
- Process action blocked

Можно создать отдельную выборку на эти два события

Отчеты есть? Обязательно!

Report on Ada	ptive Anomaly Control (rules state		₽ *
🖉 Edit 💡	⊖ Refresh 🕞 Expo	rt		
Summary	Details			
Report on <i>i</i> Thursday, Febi This report pro	Adaptive Anomaly uary 7, 2019 6:24:58 PM vides information abour	Control rules sta	te Anomaly Control rules. This report is generated for a	all groups.
7.0 6.5 6.0 5.5 5.0 4.5 4.5 4.0 3.5 3.0 -	6	3	Rules in Off state, total: 2 Rules in Smart Training state, total: 6 Rules in Smart Block state, total: 0 Rules in Notify state, total: 3 Rules in Block state, total: 7	

Report on Adaptive Anomaly Control rules state – показывает в каком режиме находится то или иное правило

Это единственное место, где можно посмотреть закончилось ли обучение, т.е. перешло ли правило из Smart Training режима в Smart Block

1.5 1.0 0.5 0.0

Search

Отчеты есть? Обязательно!

0	Adaptive Anomaly Control report	۴	?	×
_	Summary Details			
	Adaptive Anomaly Control report Thursday, February 7, 2019 6:25:20 PM This report provides information about triggered rules of Adaptive Anomaly Control. This report is generated for all groups.			
	Non-standard file for the folder - 3 1 Block			
	System file in a non-system folder – 2			
	Start of Microsoft Register Server from office application - 1			
	Start of Microsoft PowerShell from office application - 1			
	Start of Microsoft HTML Application Host from office application - 1			
	0.0 0.5 1.0 1.5 2.0 2.5 3.0 3.5 4.0			
	Search			

Adaptive Anomaly Control report – показывает как часто какие правила срабатывают



Лабораторная работа №5

Как настроить Adaptive Anomaly Control

- 1. Настройте блокировку запуска макросов и скриптов в офисных документах
- 2. Проверьте, что Adaptive Anomaly Control блокирует запуск вредоносного макроса
- Заблокируйте запуск вредоносного макроса
 Защитой от эксплоитов

Лабораторная работа №6

Как проверить Защиту от эксплоитов

1. Имитируйте хакерскую атаку, используя уязвимость в PowerShell и получите доступ к удаленному компьютеру

KASPERSKY

2. Включите защиту от эксплоитов

Что нового в Kaspersky Security Center 11

Операционные системы New Web Console Изменения в интерфейсе ММС-консоли администрирования Поддержка DIFF-файлов обновлений Изменения в работе Агентов обновлений Обратная совместимость плагинов KES Улучшения в RBAC

KASPERSKY

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы Новые компоненты KES Компонент AMSI Protection Provider Компонент Adaptive Anomaly Control Проверка зашифрованного трафика Защита от MAC Spoofing Role Based Access Control for KES

Как работает защита от сетевых угроз?



Kaspersky Endpoint Security 11.1: проверка шифрованного трафика



🕿 📰 🔏 📭 🗶 🖻 🗟	
 Interprise fusion Trusted Root Certification Auth Certificates Enterprise fusion Trusted Root Certification Auth Trusted Publishers Untrusted Certificates Third-Party Root Certification Trusted People Client Authentication Issuers Preview Build Roots SIM Certification Authorities 	Author GlobalSign Cot CA 3 C C High Root CA GlobalSign Root CA
Homegroup Machine Certifica Smart Card Trusted Roots	ttes DigiCert Global Root
	Certificate Information
	Ensures the identity of a remote computer All issuance policies
	Ensures the identity of a remote computer All issuance policies Issued to: Kaspersky Endpoint Security Personal Root Certificate Issued by: Kaspersky Endpoint Security Personal Root Certificate
	Ensures the identity of a remote computer All issuance policies Issued to: Kaspersky Endpoint Security Personal Root Certificate Issued by: Kaspersky Endpoint Security Personal Root Certificate Valid from 12/9/2008 to 12/4/2028

- Добавлена проверка зашифрованного трафика, основанная на подмене сертификатов
- KES создает сертификат при установке и помещает его в локальное хранилище Trusted Root Certification Authorities
- При каждом запуске KES проверяет наличие сертификата в хранилище и если его там нет восстанавливает

KASPERSKY

KL 202.11.1: Kaspersky Endpoint Security and Management.

Web Threat Protection: подмена сертификата

Kaspersky Endpoint Security for \ × +	- u
Kaspersky Endpoint Security for Windows	
ACCESS DENIED	
The requested web address cannot be provided	
Object web address:	
https://secure.eicar.org/eicar.com	
Reason:	
object is infected by <u>EICAR-Test-File</u>	
-	Kaspersky Endpoint Security for X Image: style in type://secure.eicar.org/eicar.com Image: style in type: style i

- Kaspersky Endpoint Security Personal Root Certificate:
 - срок действия 10 лет
 - алгоритм шифрования SHA 256
 - длинна ключа 2048 bits
- Проверка зашифрованного трафика влияет на работу следующих компонентов:
 - Web Threat Protection
 - Web Control
 - Mail Threat Protection

Что если при проверке защищенных соединений возникает ошибка?

\odot	Network settings 🕫 🔿 🗙	
Ø	Encrypted connections scan	
	Scan encrypted connections When visiting a domain with an untrusted certificate	
	Allow Block	
	When secure connection scan errors occur O Break connection O Add domain to exclusions	
	 Block SSL 2.0 connections (recommended) The SSL 2.0 protocol has flaws that affect the security of data transfer. Decrypt secure connection with EV certificate. If you open a website with an EV certificate for the first time, a secure connection will be decrypted regardless of 	1
	whether the check box is selected or not. <u>Trusted domains</u> <u>Trusted applications</u>	
	ок	



Если при попытке проверки зашифрованного трафика возникает ошибка, домен автоматически добавляется в исключения и весь его трафик шифрованный трафик пропускается без проверки

Список исключения хранится локально на каждом компьютере и не передается на Сервер администрирования

KASPERSKY

OK

connect.facebook.net

sh.scorecardresearch.com

top-fwz1.mail.ru counter.yadro.ru www.tns-counter.ru

Что если проверка зашифрованного трафика мешает работе программы?

0	Network settings	 ⑦ Trusted domains P¹ 	◎ × Add domain ×
Ø	Encrypted connections scan	Trusted domains	Domain *.secure.eicar.org
	 Scan encrypted connections When visiting a domain with an untrusted certificate Allow Block When secure connection scan errors occur Break connection 	+ Add → Delete □ Domain Status □ *secure.eicar.org ● Enabled □ *eicar.org ● Enabled	For example: example.com Status Enabled Disabled
	 Add domain to exclusions Block SSL 2.0 connections (recommended) The SSL 2.0 protocol has flaws that ffect the security of data transfer. Decrypt secure connection with EV certificate If you open a website with an EV certificate for the first time, a secure connection will be decrypted regardless whether the check box is selected c not. Trusted domains 	Image: Application Path or path mask to the application C:\Program Files (x86)\ABC Do not scan opened files Do not monitor application activity Do not inherit restrictions of the parent process (application) Do not monitor child application activity	Не отключаете проверку зашифрованного трафика полностью Настройте исключения
	⑦ Trusted applications + Add ⇒ Educe	OK □ Do not block interaction with the application interface □ Do not block interaction with AMSI Protection Provider □ Do not scan network traffic • Encrypted traffic only • All traffic Specified remote IP addresses + Add × Delete	приложений
	Application Status No data	IP address No data	

Проверка https-трафика: проблемы сертификата Веб-сайта

		Re expired.badssi.com	Re expired.badssi.com
C https://expired.badssl.com x + ← → C A https://expired.badssl.com x	• × •	General Details Certification Path	General Details Certification Path Certification path
I Visiting a domain with an untrusted certificate Your connection is not secure. Criminals may attempt to intercept your private data. It is recommended to stop working with the website. Web address:		Issued to: *.badssl.com Issued by: COMODO RSA Domain Validation Secure Server CA Valid from 4/9/2015 to 4/12/2015 Issuer Statement	View Certificate Certificate status: This certificate has expired or is not yet valid.
expired.badssl.com Reason: This certificate or one of the certificates in the chain is out of date. <u>View certificate</u> <u>I understand the risk, but want to proceed</u>		tention! × You are about to visit an unsafe web resource. Continue? Application name: Kaspersky Endpoint Security for Windows Action: AO Kaspersky Lab Action: Visiting an unsafe web resource member my action for 5 minutes. Yes No	

Web Control: проверка https-трафика

+ + C Anttps://www.facebook.com	☆ 0
Kaspersky Endpoint Security for Windows	
ACCESS DENIED	
The requested web page cannot be provided.	
Address: <u>https://www.facebook.com</u> .	
The web page has been blocked by the SM rule.	
Reason: the web resource belongs to the Social networks content category(-ies) and the Undetermined data type category(-ies).	
This web resource is prohibited at the company. If you consider the blocking to be mistaken or if you need to access this web resource, contact the administrator of the local corporate network (<u>Request access</u>).	
Message generated on: 11/13/2018 5:42:12 PM	
	Kaspersky Endpoint Security for Windows ACCESS DENIED The requested web page cannot be provided. Address: https://www.facebook.com. The web page has been blocked by the SM rule. Reason: the web resource belongs to the Social networks content category(-ies) and the Undetermined data type category(-ies). This web resource is prohibited at the company. If you coacted the the docking to be mistaken or if you need to access this web resource, contact the administrator of the local corporate network (Request access). Message generated on: 11/13/2018 5:42:12 PM

KASPERSKY[®]

Web Control: новая категория



KASPERSKY B



Лабораторная работа №7

Как проверить защиту от веб-угроз

- 1. Проверьте, что Защита от веб-угроз проверяет https трафик
- 2. Выключите проверку шифрованного трафика для программы PowerShell

Kaspersky Endpoint Security 11.1: поддержка Windows Subsystem for Linux (WSL)

Ø vb@ABC-Test: /tmp − □ ×	Kaspersky Endpoint Security for Windows
vb@ABC-Test:~\$ cd /tmp/	File Threat Protection
vb@ABC-Test:/tmp\$ ls	
eicar drop kl edu.cpp eicar dropper	Malicious object detected
vb@ABC-Test:/tmp\$ eicar_dropper	
eicar_dropper: command not found	Event type: Malicious object detected
vb@ABC-Test:/tmp\$ g++ eicar_drop_kl_edu.cpp -o eicar_drop	Application/Name: eicar drop
vb@ABC-Test:/tmp\$ eicar_drop	Application\Path: C:\Users\administrator\AppData\Local
eicar_drop: command not found	\Packages
vb@ABC-Test:/tmp\$ ls	\CanonicalGroupLimited.Ubuntu18.04onWindows_
eicar_drop eicar_drop_kl_edu.cpp eicar_dropper	Application/Process ID: 7832
vb@ABC-Test:/tmp\$./eicar_drop	User: ABC\Administrator (Active user)
`+hdNNd+ :hNNmhs-	Component: File Threat Protection
oNMMMM/ -mMMMMy`	Result/Description: Detected
/MMsdMN:/osyss+:dMN/MMy DEMO eicar dropper 0.1	Result/Name: EICAR-Test-File
oMM-/MMMMmdhhmMMMMs`NMd	Result\Threat level: High
`mMNMMh/` DEMO :sNMNMM:	Result/Precision: Exactly
. /MMM+ EICAR -mMMy .	Canonical Groupt imited Ubuntu 18 04on Windows
/MNhoMMNMMMmdyyssyhmMMMNMMyymMy	79rhkp1fndgsc\LocalState\rootfs\tmp\eicar.com
/smMMm`-/oyyNMMyys+:.yMMmy/.	Object\Type: File
:MM+ yMM .MMs	Object\Path: C:\Users\administrator\AppData\Local
OMM- YMM MMY	\Packages \CanonicalGroupLimited Ubuntu18 04onWindows
:sssdm: ymm mmmssso	79rhkp1fndgsc\LocalState\rootfs\tmp\eicar.com
/nnnmmy ymm /mmannny	Object\Name: eicar.com
SPM: YPM NMM	Reason: Expert analysis
muuri yrun .muuri-	Hash:
. SNPPPPPIT- yPP SPPPPNY:	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c453
: NPG+ - TIPUMIS/ CPU/ OTPUM/ : YPUO	8aabf651fd0f
··· ···	
vb@ABC-Test:/tmp\$	Details

KASPERSKY B



Лабораторная работа №8

Как проверить защиту от файловых угроз

- 1. Проверить, что Kaspersky Endpoint Security умеет обнаружить вредоносные файлы, которые запускаются в Windows Subsystem for Linux
- 2. Изучите события защиты от файловых угроз

Что нового в Kaspersky Security Center 11

Операционные системы New Web Console Изменения в интерфейсе ММС-консоли администрирования Поддержка DIFF-файлов обновлений Изменения в работе Агентов обновлений Обратная совместимость плагинов KES Улучшения в RBAC

KASPERSKY

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы Новые компоненты KES Компонент AMSI Protection Provider Компонент Adaptive Anomaly Control Проверка зашифрованного трафика Защита от MAC Spoofing Role Based Access Control for KES

Kaspersky Endpoint Security 11.1: защита от MAC Spoofing



Предотвращает подмену адресов в ARP-таблице, принимая только те ответы, для которых был отправлен запрос

После выполнения ARP-запроса все ответы кроме первого игнорируются

Что нового в Kaspersky Security Center 11

Операционные системы New Web Console Изменения в интерфейсе ММС-консоли администрирования Поддержка DIFF-файлов обновлений Изменения в работе Агентов обновлений Обратная совместимость плагинов KES Улучшения в RBAC

KASPERSKY

Что нового в Kaspersky Endpoint Security 11.1

Операционные системы Новые компоненты KES Компонент AMSI Protection Provider Компонент Adaptive Anomaly Control Проверка зашифрованного трафика Защита от MAC Spoofing Role Based Access Control for KES

Как пользователь может помешать защите?

Q

	rograms and Features 🔹 😽	Search Programs and Features
Control Panel Home View installed updates Turn Windows features on or off Install a program from the	Uninstall or change a program To uninstall a program, select it from the list an Repair. Organize Change	d then click Uninstall, Change, or ₿☷ 🔻
network	Name	Publisher
	Kaspersky Endpoint Security for Windows	AO Kaspersky Lab
Kaspersky Endpoint Security for Win Modify, Repair, or Remove applic Select the operation that you want to	Kaspersky Security Center 11 Network Agent Microsoft Office Professional Plus 2013 Microsoft Visual C++ 2017 Redistributable (x64) Microsoft Visual C++ 2017 Redistributable (x66) Adows	AO Kaspersky Lab Microsoft Corporation 14.1 Microsoft Corporation Mozilla Mozilla Mozilla
Hodify Action prohibited by a gro	oup administration policy	Skype Technologies S.A. VMware, Inc.
Modify Action prohibited by a greater Repair Action prohibited by a greater	oup administration policy oup administration policy	Skype Technologies S.A. VMware, Inc. 11.1.0.15669 https://click.kaspersky.com/?hl=en&link=
Modify Action prohibited by a gri Repair Action prohibited by a gri Remove Removes Kaspersky End;	oup administration policy oup administration policy point Security for Windows from your computer.	Skype Technologies S.A. VMware, Inc. 11.1.0.15669 https://click.kaspersky.com/?hl=en&links



- лить Kaspersky Endpoint Security или Агент инистрирования. Без Агента не применяется политика и ьзователь сможет менять настройки
- 2. Удалить лицензию: компоненты остановятся
- 3. Выйти из Kaspersky Endpoint Security: защита остановится

Kaspersky Endpoint Security 11.0: доступ по паролю к локальному интерфейсу KES

	ecunty for Windows (11.0.0) — 🗆 X		
High protection level	All recommended protection components are enabled.		
Sections	Interface		
General Event configuration Advanced Threat Protection Essential Threat Protection Endpoint Sensor Local tasks General Settings Application Settings Exclusions Reports and Storage Interface Policy profiles Revision history	 Interaction with user Display application interface Simplified application interface Settings Settings Settings Settings Settings Warnings on the Kaspersky Endpoint Security for Windows icon in the notification area Settings Warnings on the Kaspersky Endpoint Security for Windows icon in the notification area Settings Variation area Settings Settings Warnings on the Kaspersky Endpoint Security for Windows icon in the notification area Settings Variation area Send the 'Databases out of date' notification if databases were not updated Send the 'Databases extremely out of date' notification if databases Time of day(s) Settings Password protection Settings Password protection disabled Settings Support information 	Password protection Password protection allows you to set restrictions on the management of some of features and settings of Kaspersky Endpoint Security for Windows. This reduces to of unauthorized or unintended changes in the functioning of the application. Recommended default value for the user name is KLAdmin. Password User name: Admin New password: Confirm password: Confirm password: Password scope Score Configure application settings Exit the application Disable protection components Disable control components Remove key Remove key Remove modify / restore the application Restore access to data on encrypted drives View reports Select all Deselect all	

KL 202.11.1: Kaspersky Endpoint Security and Management

KASPERSKY B

Kaspersky Endpoint Security 11.1: доступ по паролю к локальному интерфейсу KES

		51 @ V		
 Kaspersky Endpoint Security 11 for Windows. 	⊙ Interface	0 q	Set the administrator password	×
GENERAL EVENT NOTIFICATION APPLICATION SETTINGS REVISIO	Password protection	🔒 Enforce 💽	Password	
Advanced Threat Protection Essential Threat Protection Security Controls Endpoint Sensor Local tasks General Settings General Setting General Setting General Setings General Setting General Set	Password protection ENAB Password protection allows you settings of Kaspersky Endpoint 3 changes in the functioning of the hards and believe Name + Add Everyone KLAdmin O Password protection Add permissions for Select user No users and/or groups of Permissions Configure application s Remove / modify / rest Disable Kaspersky Secu Exit the application View reports Restore access to data Restore from Backup Disable protection corr Disable control compo	Select user or group Search Q Access Control Assistance Operators Account Operators Administrator Administrator Alex ALEX-DESKTOP\Administrator ALEX-DESKTOP\KINagSvc	Edit permissions for KLAdmin Default administrator account on user computers User name KLAdmin Password •••• Permissions • Configure application settings • Remove / modify / restore the application • Disable Kaspersky Security Center policy • Exit the application • View reports • Restore access to data on encrypted drives • Restore from Backup • Disable protection components • Disable control components	Image: Second
KL 202.11.1: Kaspersky Endpoint Security and Management.		Allowed KODC Password Replication Group Backup Operators	Remove key	KASPERSKY
		DI III TINI Administrators		

Kaspersky Endpoint Security 11.1: поддержка миграции

• При обновлении версии KES больше не нужно расшифровывать зашифрованные диски, если он зашифрован с помощью Kaspersky Full Disk Encryption

KASPERSKY

• Улучшена поддержка миграции с Windows 7 / 8 / 8.1 на Windows 10

Kaspersky Endpoint Security 11.1: итого

- Появились новые компоненты:
 - AMSI Protection Provider
 - Adaptive Anomaly Control
- Реализована проверка HTTPs-трафика
- Реализована поддержка Windows Subsystem for Linux (WSL)
- Реализована защита от MAC Spoofing
- Изменена модель доступа по паролю к локальному интерфейсу KES
- Реализована поддержка Kaspersky Full Disk Encryption при обновлении версий
- Улучшена поддержка миграции с Windows 7 / 8 / 8.1 на Windows 10
- Появилась новая категория Web Control, связанная с криптовалютами и майнигом



Лабораторная работа №9

Как проверить защиту сетевых папок от программ-вымогателей

- Имитируйте заражение вредоносной программой
 вымогателем
- 2. Проверьте результаты работы компонента защиты Behavior Detection
- Разрешите шифрование в сетевых папках общего доступа и настройте исключения для сетевых устройств
- 4. Проверьте, что исключения для сетевых устройств работают корректно



Лабораторная работа №10

Как проверить защиту от сетевых атак

- 1. Имитируйте атаку по сети с компьютера Kali на компьютер Alex-Desktop
- 2. Изучите отчет о сетевых атаках
- 3. Разблокируйте компьютер Kali
- 4. Настройте защиту от сетевых атак не блокировать Kali
- 5. Имитируйте атаку с компьютера Kali на компьютер Alex-Desktop и изучите результаты