

KL 025.6

Kaspersky Anti Targeted Attack. Kaspersky Endpoint Detection and Response.

Kaspersky.TechEdu

Учебный курс

Содержание

1. Введение	1
1.1. Ландшафт угроз	1
1.2. Проблемы при построении системы ИБ	8
1.3. Подходы к построению системы ИБ	11
1.4. Какие задачи заказчика помогает решить KATA Platform	19
2. Подготовка к внедрению	22
2.1. Состав, возможности	22
2.2. Схемы развертывания, масштабирование, совместимость	29
3. Развёртывание платформы KATA	47
3.1. Установка Центрального узла в виде кластера и установка Сенсора	47
3.2. Установка и настройка Sandbox	61
3.3. Активация, обновление, пользователи	75
3.4. Подключение серверов друг к другу	82
4. Эксплуатация KATA	96
4.1. Подключение к источникам трафика	96
4.2. Технологии обнаружения KATA	115
5. Установка Endpoint-агент	134
5.1. Типы Endpoint-агентов	134
5.2. Установка средствами Kaspersky Security Center	136
5.3. Установка без Центрального управления	153
5.4. Результат установки и сбор данных	162
6. Эксплуатация KEDR	168
6.1. Технологии обнаружения KEDR	168
6.2. Расследование инцидента	174
6.3. Реагирование на инцидент	189
7. Результаты анализа Sandbox	212
7.1. Карточка обнаружения Sandbox	212
7.2. Результаты анализа в виртуальной среде	213
7.3. Отладочная информация Sandbox	215
8. Обслуживание платформы KATA	219
8.1. VIP-статус	219
8.2. Проверка архивов с паролем	220
8.3. External API	221
8.4. Отчеты	229
8.5. Почтовые уведомления	231
8.6. Интеграция с SIEM	233
8.7. Мониторинг сервера по SNMP	235
8.8. Сбор информации о системе	236
8.9. Обновление	238
8.10. Обновление с предыдущих версий	240
8.11. Сохранение и восстановление настроек	240
8.12. Изменение системных настроек	241
8.13. Kaspersky Private Security Network (KPSN)	242

Глава 1. Введение

1.1. Ландшафт угроз

Изучаемые продукты и приложения

1



Kaspersky Anti Targeted Attack 6.0

- Центральный узел
- Sandbox
- Sensor



Kaspersky Endpoint Detection and Response Expert 6.0

- Центральный узел
- Sandbox
- Sensor
- Kaspersky Endpoint Agent для Windows (3.12 и 3.13 с ограничениями, 3.15 – 3.16)
- Kaspersky Endpoint Security для Windows (12.1 – 12.3)
- Kaspersky Endpoint Security для Linux (11.4 с ограничениями, 12)
- Kaspersky Endpoint Security для Mac 12

В данном курсе рассмотрим решения Лаборатории Касперского на базе Kaspersky Anti Targeted Attack Platform:

- Kaspersky Anti Targeted Attack (KATA) — средство для глубокого анализа сетевого трафика организации с применением таких технологий как Sandbox, IDS, антивирусная проверка, проверка репутации, YARA.
- Kaspersky Endpoint Detection and Response (KEDR) — средство для сбора и анализа данных об активности на узлах сети, выявления опасной активности, сдерживания и устранения следов атаки инструментами удаленного реагирования.

Серверные компоненты обоих решений совпадают, но выполняют разные функции в зависимости от лицензии. В состав KATA-платформы входят следующие сервера:

- Центральный узел,
- Сенсор,
- Sandbox.

Курс рассматривает версии KATA 6.0 и KEDR 6.0. Версии серверных компонентов основаны на версии KATA, поэтому изучаемые в курсе Центральный узел, Сенсор и Sandbox все имеют версию 6.0. В работе KEDR (но не KATA) критически важную роль играют Endpoint-агенты,

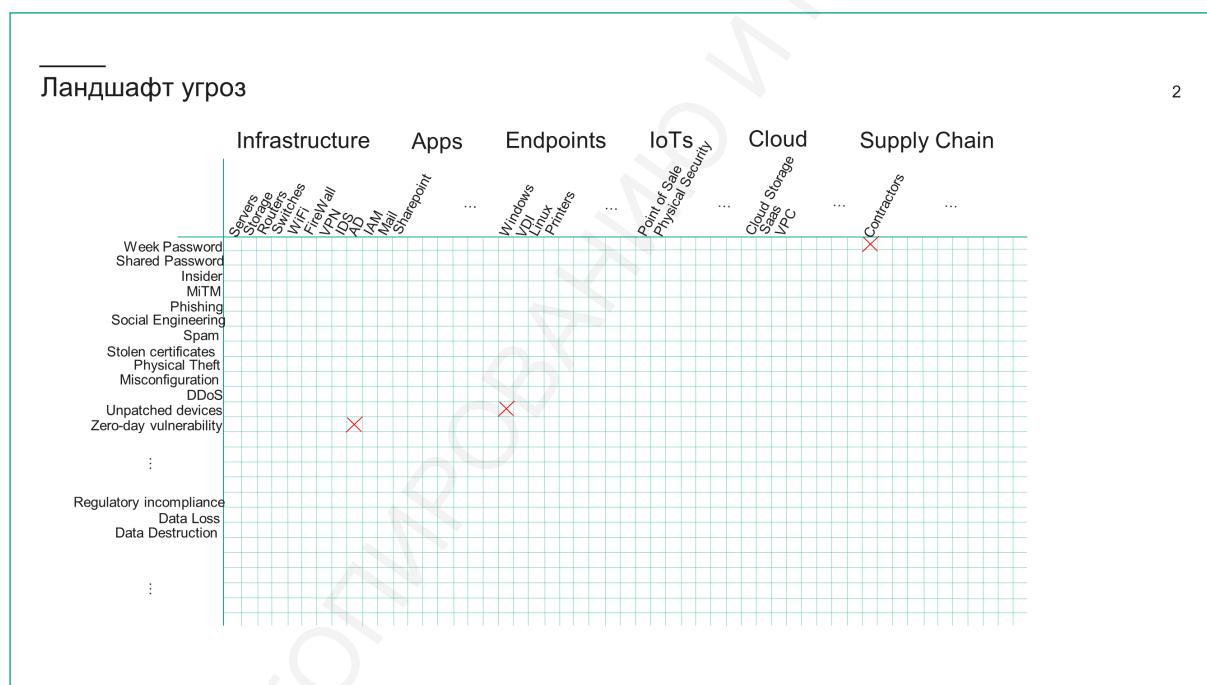
устанавливаемые на узлы сети. В курсе рассматриваются Endpoint-агенты, полностью совместимые с KEDR 6.0.

В курсе также затрагиваются смежные компоненты:

- Kaspersky Security Center (KSC) — в силу того, Kaspersky Endpoint Agent проще всего устанавливать и настраивать через KSC. В курсе рассматривается работа с веб-консолью KSC.
- Kaspersky Endpoint Security (KES) — в силу того, что Kaspersky Endpoint Agent возможно установить в составе KES.

Для всех операций, важных для работы KEDR, представлены подробные инструкции.

Для более глубокого понимания того, как работает KSC, рекомендуется прослушать курс, посвященный основам защиты узлов сети: KL 002 Kaspersky Endpoint Security



Прежде чем мы начнем разбирать особенности работы продуктов KATA Platform, мы поговорим об угрозах, с которыми сталкивается заказчик, почему с ними тяжело справиться базовыми средствами и что необходимо сделать, чтобы противодействовать им.

Начнем с ландшафта угроз. В настоящий момент инфраструктура заказчиков давно уже переросла защищенный периметр, и необходимо учитывать, что часть инфраструктуры или сервисов может располагаться в частном или публичном облаке, часть сотрудников работает в удаленном режиме, существуют подключения партнеров и подрядных организаций, многие сотрудники для работы используют собственные устройства и так далее. Если разделить инфраструктуру заказчика на условные группы объектов/сервисов, то это могут быть

Infrastructure, Apps, Endpoints и другие, представленные на схеме. С другой стороны, можно выделить довольно большой перечень векторов атаки: Weak passwords, Insiders, Spam и прочее. Если сопоставить эти два списка, то получим матрицу ландшафта угроз, где почти на каждом из пересечений может быть угроза. К примеру:

- Уязвимость нулевого дня в Active Directory (AD). От появления новых уязвимостей в используемых сервисах никто не застрахован, и такая ситуация может привести к успешной атаке. Как подтверждение можно посмотреть статистику появления новых уязвимостей — она неуклонно растет
- Отсутствие обновлений на конечных точках Windows. Непропатченные устройства, т.е. устройства, про которых уже известно, что они уязвимы к определенным видам атак на своё ПО, но по которым не приняты меры по устранению данной угрозы. К сожалению, процесс выявления и устранения уязвимостей и патч-менеджмент выстроен далеко не в каждой компании, и вполне обычная ситуация, когда злоумышленнику для проникновения не требуется искать уязвимостей нулевого дня, а достаточно просканировать устройства, найти уязвимые и воспользоваться ими.
- Слабый пароль выданный подрядчикам. В настоящий момент частая ситуация, когда доступ к сети и сервисам заказчика имеют подрядные организации, исполнители или партнеры. В такой парадигме очень важно предоставлять доступ гранулировано по принципу наименьших прав, и контролировать способы подключения.

Примеры

3

The screenshot shows a news aggregator page with several news items highlighted in boxes:

- THE TIMES OF INDIA**: "Government probing 'data breach' of 8 crore ICMR Covid site".
- CYBER SECURITY HUB INCIDENT OF THE WEEK**: "More than 3.8 billion records exposed in DarkBeam data leak".
- we live security by ESET**: "8. T-Mobile".
- 3CX Software Supply Chain Attack**: "The compromise in March of 3CX, a widely used communications software maker, resembled the SolarWinds supply chain attack of 2020 in a number of key ways..."
- water outage in remote Irish region**: "Residents of a remote area on Ireland's west coast were left without water last week due to a cyberattack perpetrated by a pro-Iran hacking group targeting a piece of equipment the hackers complained was made in Israel."

Global cybercrime damage costs are expected to grow by 15% per year over the next two years, reaching \$10.5 trillion USD annually by 2025 (c) Forbes

Общая стоимость ущерба от атак на ИТ инфраструктуру заказчиков постоянно растет из года в год. Можно посмотреть на довольно свежие случаи взлома различных компаний:

- DarkBeam — Более 3,8 миллиардов записей были украдены после того, как фирма по цифровой защите DarkBeam оставила интерфейс, содержащий открытые записи, незащищенным.
- T-Mobile — опять же атака шифровальщика.
- Ferrari — кража данных pfnhjyekf 37 миллионов пользователей.
- Ирландия - отсутствие воды в удаленном регионе из-за кибератаки.
- ЗСХ — атака на цепочки поставок, продукция компании используется в более 600000 заказчиков.

Если посмотреть на данные компании, то можно обнаружить, что, несмотря на различия в индустриях, подходах к выявлению и устраниению инцидентов, используемым техническим средствам и процессам, есть некоторые общие черты:

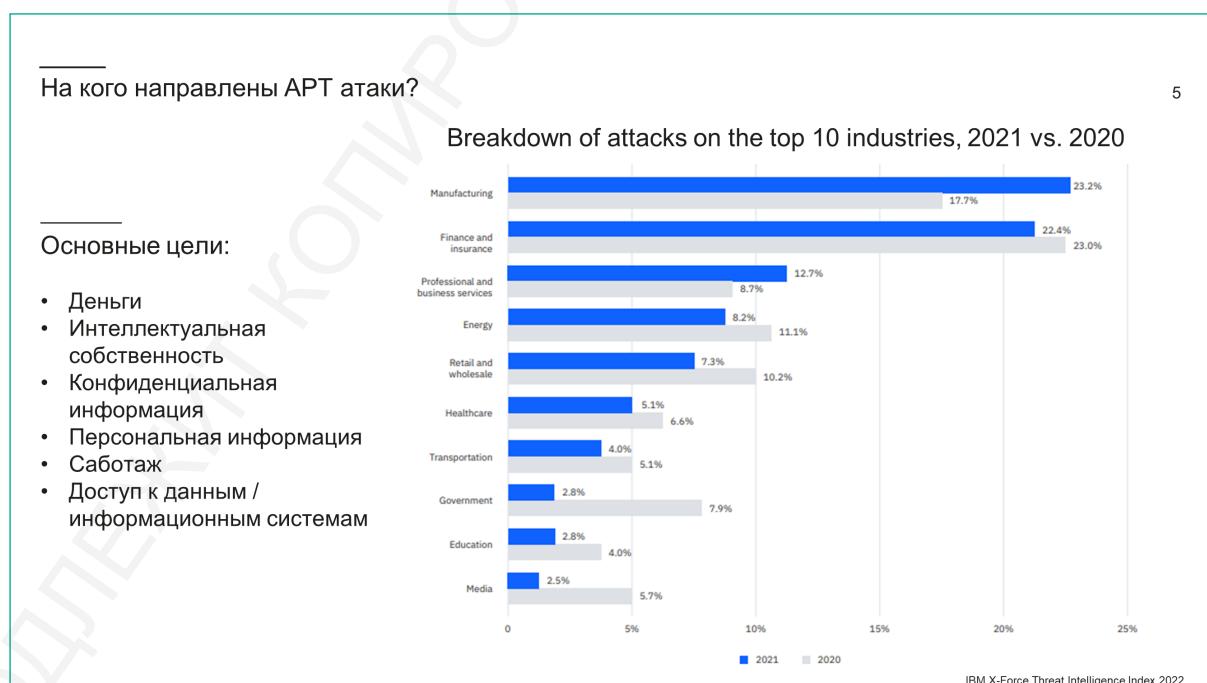
- Компании обладали чем-то, что было нужно атакующим (данные, деньги).
- Компании обладали определенно не нулевым бюджетом на ИБ и штатом сотрудников.

Означает ли это, что данные компании являются какими-то исключениями из правил, и они допустили ошибки и за это поплатились? Скорее нет, чем да. Большое количество успешных взломов, о которых узнаем из новостей, и еще большее количество, о которых мы никогда не узнаем, происходят и из-за каких-либо просчетов в системе ИБ, но в большей степени из-за появления сложных целевых атак, противостоять которым даже крупным компаниям тяжело.



Advanced Persistent Threat или целевые атаки, тяжело детектировать и предотвращать, так как у них есть общие свойства:

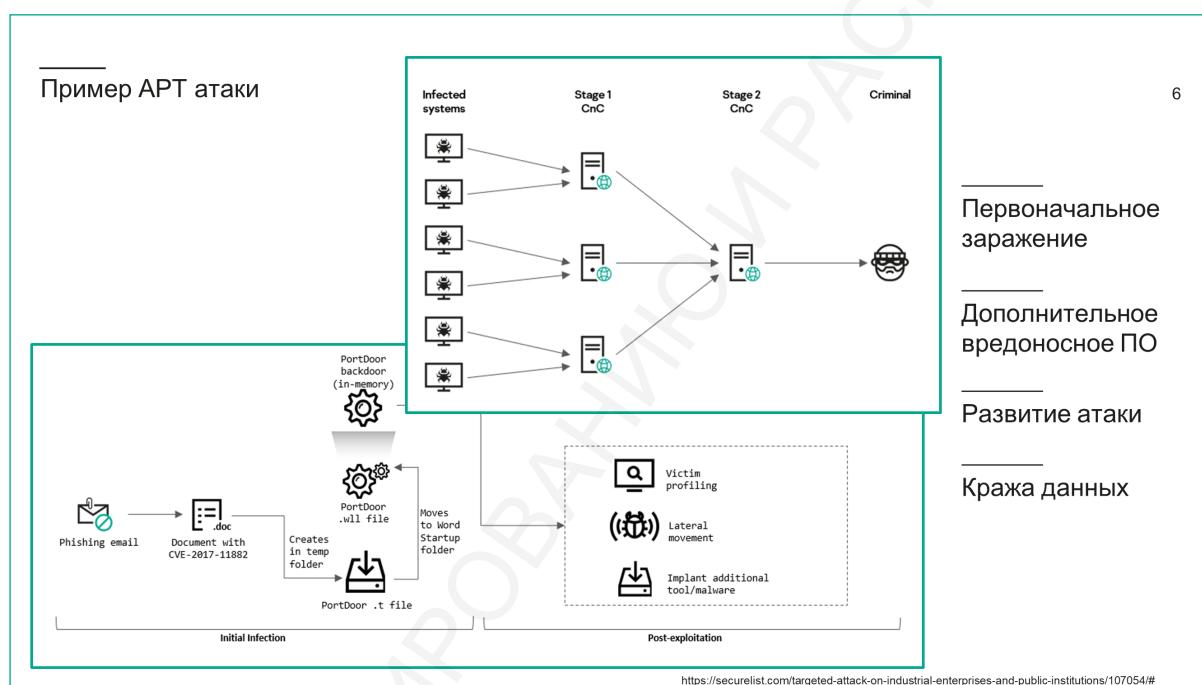
- Скрытные и ускользающие. Атакующие могут использовать как специально подготовленное вредоносное программное обеспечение, так и легитимный софт. При использовании атакующими легитимного софта очень тяжело выявить их вредоносную активность без сбора дополнительной информации о данном действии и контексте, так как одно и тоже действие с одним и тем же программным обеспечением может быть как вредоносным, так и легитимным. К примеру, с помощью командлета Get-ADUser можно получить данные по пользователям домена. Эта операция может быть легитимной, если её выполняет администратор, и вредоносной, если её пытаются выполнить неизвестная учетная запись с пользовательского компьютера, на котором было отключено средство защиты.
- Направленные. Крупные организации представляют собой прибыльную мишень, но возможны ли целевые атаки на небольшую компанию? Есть ли какой-то порог, не переступая который компания может не опасаться таких угроз, так как затраты на атаку будут превышать потенциальную прибыль? Ответ на первый вопрос - "да", на второй - "нет". Атака на цепь поставок (supply chain attack) очень популярный способ проникновения в сеть заказчика, используя менее защищенную компанию партнера / поставщика / исполнителя работ. При данной атаке, злоумышленник в качестве прибыли получает не данные или деньги компании, которую взламывает, и которые не позволят окупиться затраченным ресурсам, а доступ к более привлекательной цели.
- Сложные и настойчивые. Атакующие могут как реализовывать сразу несколько шагов одним вмешательством или, наоборот, повторять одну и ту же фазу атаки несколько раз на протяжении некоторого времени.



На кого направлены АРТ атаки?

Если попытаться перечислить потенциальные цели злоумышленников, то это будет: конфиденциальная информация, деньги, нарушение функционирования компании, и так далее. Также, принимая во внимание возможность атак на цепь поставок, можно предположить, что целевые атаки могут быть направлены практически на любую организацию, независимо от её масштабов, направления деятельности, ценности её ресурсов.

Если посмотреть на различные исследования, например на исследование компании IBM “X-Force Threat Intelligence Index 2022”, то можно увидеть статистику по секторам компаний, которые подверглись атакам. Мы увидим, что целями атакующих становятся не только очевидные сектора экономики, такие как финансы или государственные структуры, но также атакам подвержены менее очевидные цели, к примеру ритейл.



Рассмотрим пример АРТ атаки. В январе 2022, Kaspersky ICS CERT выявили волну целевых атак на ВПК и частные компании в некоторых странах в восточной Европе, целью которых мог быть кибершпионаж.

Первоначальное заражение.

Проникновение в сеть предприятия осуществляется при помощи хорошо подготовленных фишинговых писем, в том числе использующих информацию, специфическую для атакуемой организации и не доступную в публичных источниках. Это может свидетельствовать о проделанной заранее подготовительной работе (например, информация могла быть получена в результате предыдущих атак на ту же организацию или её сотрудников, либо на связанные с ней организации или частных лиц). Документы Microsoft Word, вложенные в фишинговые письма, содержали вредоносный код, эксплуатирующий уязвимость CVE-2017-11882.

Уязвимость позволяет выполнить произвольный код — в исследованных атаках это основной модуль вредоносного ПО PortDoor — без дополнительных действий со стороны пользователя. После запуска PortDoor собирает общие сведения о зараженной системе и отправляет их на сервер управления вредоносным ПО. В случаях, когда зараженная система оказывается интересна злоумышленникам, они используют функциональность PortDoor для удаленного управления системой и установки дополнительного вредоносного ПО.

Дополнительное вредоносное ПО.

Атакующие использовали сразу шесть вредоносных программ класса backdoor — вероятно, для резервирования канала связи с зараженной системой на случай, если одна из вредоносных программ будет обнаружена и удалена защитным решением. Использованные бэкдоры предоставляют обширную функциональность для контроля над зараженной системой и сбора конфиденциальных данных. Из шести бэкдоров, обнаруженных на зараженных системах, пять (PortDoor, nccTrojan, Logtu, Cotx и DNSep) ранее использовались в атаках, которые другие исследователи отнесли к АРТ TA428. Шестой бэкдор оказался новым и в других атаках не встречался.

Развитие атаки.

Закрепившись на первой системе, злоумышленники пытаются распространить вредоносное ПО на другие компьютеры в сети предприятия, для доступа к которым они используют результаты сканирования сети, а также учетные данные пользователей, украденные ранее. В качестве основного инструмента развития атаки используется хакерская утилита Ladon (популярна в Китае), объединяющая в себе инструментарий для сканирования сети, поиска и эксплуатации уязвимостей, атак на пароли и т.д. Также злоумышленники активно используют стандартные утилиты, входящие в состав операционной системы Microsoft Windows. Финальным этапом развития атаки является захват контроллера домена и получение полного контроля над всеми рабочими станциями и серверами организации. В ходе атаки злоумышленники активно использовали техники dll hijacking и process hollowing для противодействия детектированию вредоносных программ защитным ПО.

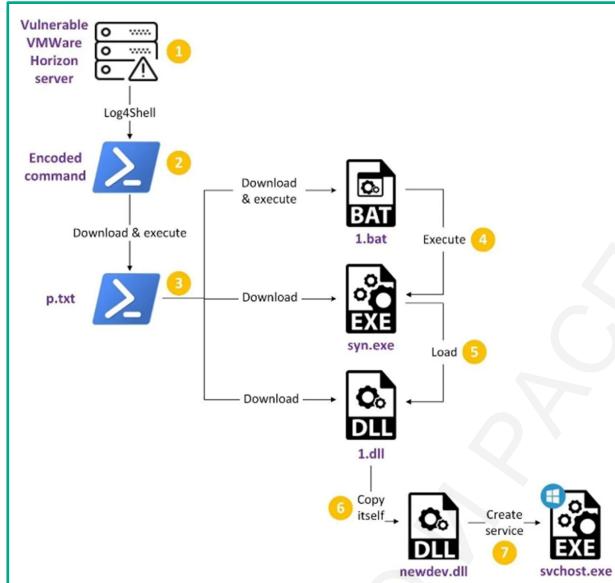
Кража данных.

Получив права доменного администратора, злоумышленники приступали к поиску и загрузке документов и других файлов, содержащих конфиденциальные данные атакованной организации, на свои серверы, развернутые в разных странах. Эти же серверы использовались как серверы управления вредоносным ПО первого уровня. Злоумышленники помещали украденные файлы в зашифрованные ZIP-архивы, защищенные паролем. После получения собранных данных серверы управления вредоносным ПО первого уровня пересыпали полученные архивы на сервер управления второго уровня, расположенный в Китае.

[https://securelist.com/targeted-attack-on-industrial-enterprises-and-public-institutions/
107054/#](https://securelist.com/targeted-attack-on-industrial-enterprises-and-public-institutions/107054/#)

Пример АРТ атаки

7



© https://www.fortinet.com/blog/threat-research/deep-panda-log4shell-fire-chili-rootkits

Рассмотрим ещё один пример АРТ атаки:

- PowerShell команда загружает PowerShell скрипт с удаленного сервера и выполняет его.
- На следующем этапе скрипт скачивает три дополнительных файла с того же удаленного сервера: 1.bat, syn.exe и 1.dll.
- Скрипт запускает 1.bat, который запускает syn.exe и удаляет все три файла с компьютера.
- syn.exe это программа, которая загружает 1.dll. 1.dll модуль и есть финальная полезная нагрузка, бэкдор, который аналитики из Fortinet назвали Milestone, его код основан на Gh0st RAT/Netbot Attacker и упакован с помощью Themida.
- Бэкдор копирует себя в %APPDATA%\newdev.dll и создает сервис msupdate2, создавая запись службы непосредственно в реестре.

1.2. Проблемы при построении системы ИБ

Проблемы при построении системы ИБ

8

Видим только конечные шаги злоумышленника



"43% argue that the attack surface is spiraling out of control" ©

Нет четкого плана действий



"50% of U.S. small businesses have a cybersecurity plan in place for 2022" ©

Нехватка ресурсов



"the median annual salary for information security analysts is \$102,600. This salary is more than double the national median earnings of workers across all industries (\$45,760)" ©

Отсутствие понимания что защищаем



"the majority (54%) of security teams spending too much time investigating low-level security alerts" ©

© Trend Micro survey in partnership with Sapio Research
© UpCity 2022 Study: 50% Of SMBs Have A Cybersecurity Plan In Place
© VmWare The state of incident response 2021: It's time for a confidence boost
© US BLS

Мы разобрались с тем, какие атаки могут быть и на кого они нацелены, разобрали примеры, теперь пора обсудить, с какими проблемами сталкивается заказчик при построении системы ИБ для противодействия современным угрозам.

Видим только конечные шаги злоумышленника.

Если видны только конечные шаги злоумышленника и не проводится расследования всей цепочки атаки, то значит большая часть активности злоумышленника нам не видна, а если мы её не видим, то никак не можем контролировать и остановить. Также, если мы видим конечные шаги, успешно с ними боремся, то это не значит, что так и будет продолжаться. Это будет происходить ровно до того момента, как злоумышленник не подберет вариант действий, который мы не сможем выявить и достигнет своей цели, это может быть как через 1 час, так и через день или месяц. Пример из жизни:

- Заказчик фиксирует наличие вредоносной программы на одном из компьютеров своей сети.
- Удаляет её.
- Заказчик фиксирует наличие вредоносной программы на ещё одном из компьютеров своей сети через сутки после первого обнаружения.
- Удаляет её.
- Еще через сутки ситуация повторяется.
- Так продолжается ровно до того момента, как заказчик не провел процедуру анализа этого инцидента ИБ и не выявил всю цепочки атаки, после чего смог её остановить.

Нет четкого плана действий.

Встречается ситуация, когда у заказчика нет четкого плана действий на случай различных инцидентов ИБ или сотрудники с ним не ознакомлены. Это приводит к тому, что:

- Действия сотрудников могут быть поспешными (удалить файл, удалить виртуальную машину, не успев проанализировать угрозу).
- Действия сотрудников могут быть медленными (сотруднику может потребоваться время, чтобы понять, как лучше действовать в конкретной ситуации).
- Коммуникации между сотрудниками/отделами могут занимать продолжительное время (в рамках инцидента может быть выявлен внутренний нарушитель и потребуется взаимодействие с IT службой и службой физической безопасности, чтобы оперативно ограничить доступы сотрудника к сервисам и помещениям компании, а это в свою очередь может требовать различных согласований).
- Сотрудник «в спешке», если процесс отработки инцидента не описан четко и не отработан, может просто ошибиться, человеческий фактор становится критичным.

Нехватка ресурсов.

Очень часто можно встретить ситуацию, когда у заказчика нет необходимых ресурсов для работы с различными системами ИБ. Это приводит к тому, что хоть системы и генерируют необходимую информацию по инцидентам и могут предоставить необходимый функционал для анализа и предотвращения угрозы, но пользоваться этим у сотрудников просто нет времени из-за большой загрузки. Пример из жизни:

- У заказчика внедрена SIEM система.
- Каждый день она генерирует порядка 400 алертов.
- У заказчика только два специалиста работают с системой помимо своих дополнительных обязанностей.
- Как результат — время на тюнинг и настройку системы нет, алерты создаются и не обрабатываются, инциденты не расследуются.
- Результат от внедрения SIEM — отрицательный, принимая во внимание её стоимость.

Отсутствие понимания, что защищаем.

Даже если есть необходимые ресурсы для расследования инцидента, но нет понимания какие процессы и ресурсы критичны для компании, то результат работы отдела ИБ будет неудовлетворительный. Всегда при принятии каких-либо решений в области ИБ необходимо учитывать, какие последствия это принесет бизнесу компании. Это помогает как при

приоритизации угроз, так и при выполнении защитных мер.

Как пример, будет ли разница, если отключить от сети на 1 день сервер печати? Для компании, бизнес которой связан с разработкой ПО — это будет неприятно, но основные бизнес-процессы будут работать, ущерб минимален. Для банковского офиса — критично, будут затронуты основные бизнес-процессы по заключению договоров, выдаче кредитов (все, для чего необходима бумага). Также и при приоритизации угроз аналитики должны акцентировать внимание на угрозы, которые потенциально могут нанести максимальный ущерб.

1.3. Подходы к построению системы ИБ

Мы обсудили проблемы при построении системы ИБ и сейчас обсудим, какие есть подходы и что мы можем сделать, чтобы противодействовать угрозам.

Подходы к построению системы ИБ

9

Комплексность

Люди

Необходим обученный персонал для выполнения задач комплексной системы ИБ
Необходимо повышать осведомленность пользователей в вопросе ИБ

Процессы

Необходимы процессы по которым сотрудники смогут действовать в различных ситуациях

Технологии

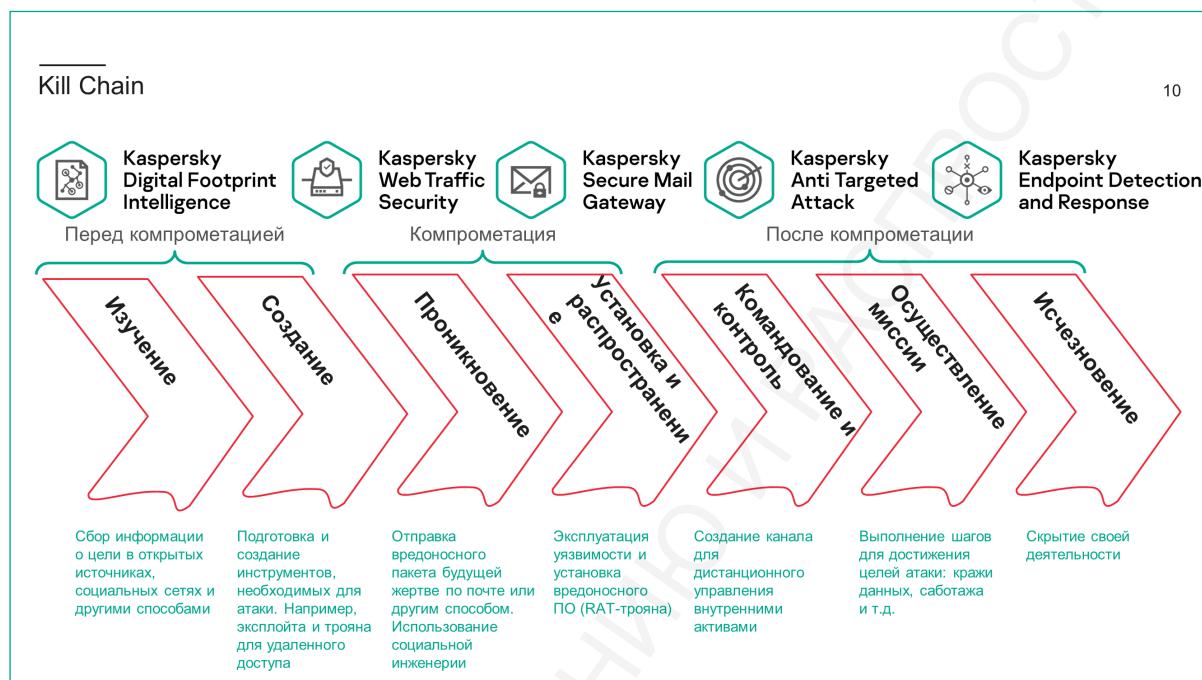
Необходимы технологии, позволяющие следовать соответствующим процессам

Комплексность

Система ИБ должна быть комплексной. Это означает, что одних только технических средств или персонала с нужными навыками недостаточно. Необходимо три составляющих:

- Люди. Необходим обученный персонал для выполнения задач комплексной системы ИБ и это далеко не простая задача, учитывая, что существует постоянная нехватка ресурсов на рынке труда. Также не стоит забывать, что пользователи компании очень часто являются «первым рубежом» обороны и от их осведомленности в вопросах ИБ тоже зависит вероятность появления инцидентов и их критичность, так что, помимо найма сотрудников департамента ИБ, необходимо также вести работу со всем персоналом компании.

- Процессы. Без четкого понимания, какие шаги сотрудник должен предпринять в какой-либо ситуации, он не сможет действовать с максимальной эффективностью.
- Технологии. С этим пунктом обычно не возникает вопросов, для выполнения своих задач специалистам необходимы соответствующие инструменты, которые будут обладать требуемой функциональностью и удобством использования.



Для того, чтобы построить комплексную систему ИБ, очень полезно понимать, как строится атака на организацию, а при детектировании инцидента — на каком этапе находится злоумышленник, какие инструменты он использует и что, возможно, будет делать дальше. Для этого существует множество методов анализа шагов злоумышленника, один из них — это анализ процесса Kill Chain. Рассмотрим пример.

Изучение.

Киберпреступник начинает собирать информацию об организации из открытых источников, социальных сетей и т.д. Его интересует все, что связано с бизнес-процессами, ИТ/ИБ системами и проблемами в компании. На корпоративном сайте или HR-ресурсе он находит информацию об открытых позициях в ИТ- или ИБ-отделе с описанием систем, которые необходимо знать. На LinkedIn — сотрудников этих отделов с описанием их навыков и успешно выполненных проектов. Далее он находит этих людей в Facebook и получает еще больше данных об их работе. Можно пойти еще дальше и найти уволенных и обиженных на работодателя сотрудников — они расскажут много интересного. И наконец, используя бесплатные инструменты (DNS Lookup и т.п.), он получает данные об IP-адресах и внешних ресурсах компании. Теперь киберпреступник знает все об операционных системах, некоторых приложениях, антивирусной защите и защите от спама, межсетевых экранах, СУБД и других

системах организации. То есть знает, что атаковать и какие защитные механизмы обходить.

Создание.

Киберпреступник выбирает способ атаки и готовит инструменты для ее осуществления. Пусть это будет PDF-документ с предложением о сотрудничестве по новому продукту. Он знает об антивирусе, который используется для защиты конечных узлов и почтовых серверов. Поэтому надо подготовить вредоносный объект, который не будет блокироваться только одним или несколькими конкретными защитными продуктами, что упрощает задачу. Киберпреступник находит экспloit-кит и после серии экспериментов создает PDF-файл, который не детектируется антивирусом, установленным у будущей жертвы. Когда сотрудник компании получит и откроет файл, то в результате уязвимости в ПО для просмотра PDF-документов, будет установлен канал связи с C&C-сервером в интернете по заранее зарегистрированному адресу. В результате киберпреступник получит полный доступ к компьютеру.

Проникновение.

На третьем этапе вредоносный объект должен быть доставлен одному из сотрудников компании. Здесь киберпреступник демонстрирует навыки социальной инженерии. Благодаря корпоративному сайту, социальным сетям или звонку в колл-центр, у него уже есть список сотрудников, которые отвечают за взаимодействие с новыми поставщиками. Он звонит одному из них, рассказывает свою «историю» и высыпает коммерческое предложение — тот самый PDF-файл. Если киберпреступнику повезло при создании вредоносного файла, то письмо дойдет до получателя в неизменном виде. Пользователь откроет файл, произойдет заражение машины, и будет установлен канал с C&C-сервером. Если этого не произошло, то придется позвонить сотруднику еще раз и узнать, что случилось. Если файл был заблокирован антивирусом или письмо вообще не дошло, то киберпреступник сошлется на проблемы со своей почтовой системой и предложит переслать файл на личную почту сотрудника, чтобы сотрудник скачал его оттуда или посмотрел дома со своего рабочего ноутбука. В этих сценариях меньше уровней защиты, поэтому вероятность проникновения выше.

Установка и распространение.

Как только сотрудник получает файл, он открывает его, и система заражается. Далее вредоносные модули распространяются по сети под контролем злоумышленника, заражая другие машины.

Командование и контроль.

Зараженные машины устанавливают связь с C&C-сервером. Теперь у киберпреступника есть контроль над машинами, в том числе над системами, которые задействованы в банковских

транзакциях.

Осуществление миссии.

Киберпреступник достигает цели — получает данные банковских карт тысяч покупателей и продает их заказчику киберпреступления.

Исчезновение.

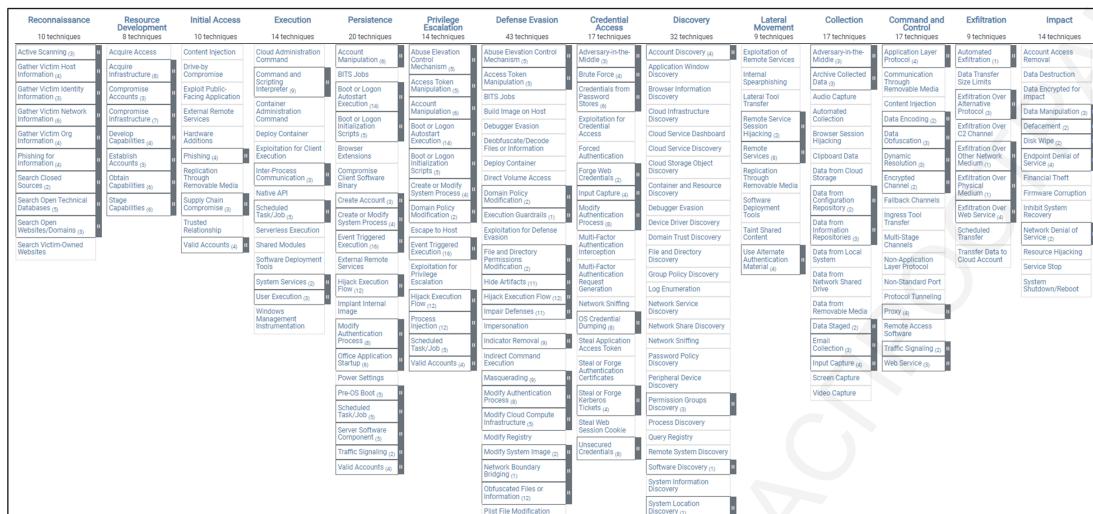
На последнем этапе он стирает следы своего присутствия: файлы, записи в журналах и подобное. Это optionalный шаг, который выполняется не всегда. Одна из особенностей целевых атак в том, что они преследуют не только краткосрочные, но и долгосрочные цели. Краткосрочная цель в данном случае — украсть базу с финансовыми данными пользователей. Долгосрочная цель — продолжать это делать в будущем.

Если посмотреть на ситуацию со стороны жертвы, то складывается безрадостная картина. На первых двух этапах (перед компрометацией) компания не может выявить действия злоумышленника и может только отслеживать доступную в сети Интернет информацию о себе. Понять, что кто-то собирает информацию и готовит атаку, практически невозможно. На следующих шагах (после компрометации) необходимое, но явно недостаточное условие — это применение традиционных средств защиты. Они помогут в случае массовой атаки, но в случае целевой атаки злоумышленник обойдет как минимум часть из них после серии попыток.

Выход здесь только один — задуматься о новом подходе к защите, в котором используются не только средства, направленные на немедленное блокирование отдельных вредоносных объектов или сетевых пакетов, но и средства, позволяющие обнаруживать признаки целевых атак на организацию. И в любом случае следует постоянно повышать осведомленность сотрудников об ИБ-угрозах.

MITRE ATT&CK

11

<https://attack.mitre.org/>

Международное сообщество специалистов информационной безопасности постоянно отслеживает и анализирует деятельность киберпреступных групп. Их тактические и стратегические цели изучаются, описываются и классифицируются. Результатом этой работы является база данных известных тактик и техник MITRE ATT&CK.

Если Kill Chain разделяет действия злоумышленников, начиная с проникновения, на 5 крупных этапов, MITRE ATT&CK выделяет 12 различных тактических целей злоумышленников при атаках на организации:

- Initial access — проникновение.
- Execution — запуск вредоносного кода.
- Persistence — организация повторного запуска.
- Privilege escalation — повышение привилегий.
- Defense evasion — ускользание от обнаружения.
- Credential access — получение доступа к другим учетным записям.
- Discovery — обнаружение устройств, учетных записей и других объектов в сети.
- Lateral movement — компрометация других узлов в сети.
- Collection — сбор данных для выгрузки с целью кражи или анализа.
- Command and control — организация удаленного доступа и управления.
- Exfiltration — выгрузка данных.

- Impact — вмешательство в работу организации.

Эти цели в классификации MITRE ATT&CK называются тактиками. В рамках каждой тактики перечислены и описаны известные способы достижения указанной цели. Эти способы называются техниками.

База данных (так называемая матрица) MITRE ATT&CK является удобным инструментом для понимания сути вредоносной активности и прогнозирования дальнейших шагов злоумышленников.

Подходы к построению системы ИБ 12

Понимание собственных бизнес-процессов Getting the fundamentals right

1 Understand the criticality of your most important assets

2 Adopt a security posture relevant to your risk profile

3 Build a robust monitoring and response plan

© Deloitte Cyber Security Landscape 2022

Понимание собственных бизнес-процессов

Следующий подход к построению системы ИБ, который мы обсудим — Понимание собственных бизнес-процессов.

Для построения системы защиты критически важно понимать, что конкретно мы защищаем, как устроены бизнес-процессы, какие из них критичны, какие информационные системы вовлечены в них.

Эта информация важна и на этапе проектирования системы ИБ, и на этапе операционной деятельности в рамках расследования инцидента, к примеру:

- При проектировании системы ИБ необходимо понимать какая информация или сервисы компании являются наиболее критичными для неё и выстраивать систему исходя из этой информации и учитывая тот уровень риска, который считается приемлемым для данных ресурсов. Допустим, что простой работы сайта организации в течении 4 часов приведет к

потерям репутационным и денежным в размере нескольких сотен тысяч долларов и будут затронуты критичные бизнес-процессы. Принимая во внимание данный факт и учитывая вероятность подобного инцидента, можно проектировать систему ИБ, которая с высокой вероятностью предотвратит исполнение данного риска, при условии, что стоимость внедрения и обслуживания данной системы будет ниже потенциального ущерба. В реальности существуют различные формулы расчета, но в рамках данного курса для наглядности достаточно и этой.

- При расследовании инцидента информация об объектах, которые мы защищаем и их критичности, может быть полезна в различных случаях:
 - дополнительная информация для анализа инцидента;
 - возможность приоритизации инцидентов;
 - возможность предсказать цели злоумышленника.



Адаптивность

Следующий подход к построению системы ИБ, который мы обсудим — Адаптивность.

При любом подходе к безопасности важно понимать, что это не разовые действия, а непрерывный циклический процесс, включающий предотвращение, обнаружение, реагирование и прогнозирование. Для успешной защиты компаниям необходимо использовать решения и услуги, отвечающие всем четырем категориям:

- Предотвращение — набор политик, продуктов и процессов, которые предотвращают атаку. Основная цель категории — уменьшить атакуемую поверхность и заблокировать

опасную активность до того, как будет нанесен ущерб компании.

- Обнаружение — функциональность, которая предназначена для выявления попыток и фактов проникновения, которые не были замечены средствами из предыдущей категории из-за активного использования техник маскировки. Основная цель категории — как можно быстрее обнаружить распространение атаки, чтобы минимизировать ущерб. В идеале компания должна исходить из того, что она находится под атакой, а системы уже скомпрометированы.
- Реагирование — навыки и инструменты, необходимые для проведения расследования и устранения проблем, обнаруженных решением из предыдущей категории. По результатам расследования должны быть предложены меры для избегания таких ситуаций в будущем.
- Прогнозирование — возможности, которые позволяют организации узнать о новых типах атак и тенденциях из внешних источников. Эти данные позволяют проактивно отвечать на новые угрозы и менять приоритеты, внося необходимые изменения в методы предотвращения и обнаружения.



В проекции на адаптивную стратегию безопасности Kaspersky Anti Targeted Attack Platform и Kaspersky Endpoint Detection and Response обеспечивают обнаружение целевых атак, которые могут быть не замечены средствами предотвращения угроз. Ката обнаруживает угрозы в сетевом трафике. KEDR обнаруживает угрозы на узлах сети.

Kaspersky Endpoint Detection and Response также предоставляет инструменты для реагирования: позволяет удаленно изолировать хост от сети, запрашивать файлы для анализа, останавливать и запускать процессы, запрещать запуск определенных файлов и т. д. Ката

инструментов реагирования не содержит.

KATA и KEDR могут использоваться и по отдельности, и как интегрированное решение.

1.4. Какие задачи заказчика помогает решить KATA Platform

Какие задачи заказчика KATA Platform может помочь решить?

15

Кому KATA Platform будет полезна:

Руководству компании

- снижение возможного ущерба для компании
- снижение рисков

Руководителю департамента / отдела

- обеспечение работы департамента / отдела с большей эффективностью и как следствие возможность получения дополнительных ресурсов
- подготовка необходимых материалов для отчета перед руководством по возникающим угрозам

Инженеру

- решение поставленных задач с меньшими трудозатратами благодаря техническим возможностям решения
- повышение собственных навыков и ценности в компании и на рынке труда

После того, как мы обозначили задачи, посмотрим, как KATA Platform их может помочь решить:

- Руководству компании:
 - снижение возможного ущерба для компании;
 - снижение рисков.
- Руководителю департамента / отдела:
 - обеспечение работы департамента / отдела с большей эффективностью и, как следствие, возможность получения дополнительных ресурсов;
 - подготовка необходимых материалов для отчета перед руководством по возникающим угрозам.
- Инженеру:
 - решение поставленных задач с меньшими трудозатратами благодаря техническим возможностям решения;
 - повышение собственных навыков и ценности в компании и на рынке труда.

Классы решений

16

Класс решения	Основные функции	Примеры решений
EPP Endpoint Protection Platform	Защищает узлы сети, обрабатывает инциденты в автоматическом режиме	Kaspersky Endpoint Security for Business, KSWS
EDR Endpoint Detection and Response	Анализирует активность узлов, ищет признаки атак, дает инструменты реагирования	Kaspersky EDR Expert Kaspersky EDR Optimum
NTA Network Traffic Analysis	Анализирует трафик, ищет признаки сложных угроз и подозрительной активности	Kaspersky Anti Targeted Attack
XDR eXtended Detection and Response	Анализирует сетевую активность и активность узлов, ищет признаки атак и необычного поведения	Kaspersky Extended Detection and Response

Разберемся с таксономией средств защиты, чтобы верно позиционировать KATA Platform:

- Традиционные средства защиты узлов относятся к классу решений Endpoint Protection Platform (EPP). Их задача — автоматически заблокировать и обезвредить все угрозы, которые поддаются 100%-ному алгоритмическому детектированию и тем самым:
 - Усложнить злоумышленникам задачу по созданию необнаруживаемых инструментов;
 - Уменьшить число инцидентов, требующих анализа специалистами ИБ.

К решениям этого класса относятся продукты из состава Kaspersky Endpoint Security для бизнеса: Kaspersky Endpoint Security (для Windows, Linux, Mac), Kaspersky Security для серверов Windows и другие

- Endpoint Detection and Response (EDR) — класс решений, которые обнаруживают потенциально опасную, но не на 100% вредоносную активность на узлах сети и предоставляют специалистам ИБ расширенный контекст для принятия решений и инструменты для реагирования на инцидент. Таким решением является Kaspersky Endpoint Detection and Response.
- Network Traffic Analyzer (NTA) — класс решений, анализирующих сетевой трафик, и обнаруживающих следы вредоносной или подозрительной активности. К этой категории относится Kaspersky Anti Targeted Attack Platform.
- Extended Detection and Response (XDR) — интегрированные решения, способные сопоставлять признаки опасной активности на узлах и в сетевом трафике для более

эффективного обнаружения следов атак и их обезвреживания. КАТА и КЕДР совместно составляют решение такого класса.

Каким образом строится работа с KATA Platform

17

Подходы к построению системы ИБ

- Комплексность
- Адаптивность
- Понимание собственных бизнес-процессов

1

Понимание ИТ инфраструктуры и бизнес-процессов компании

2

Встраивание KATA Platform в систему ИБ и процессы компании

3

Выявление угроз в рамках операционной деятельности, устранение их и минимизация ущерба для компании

4

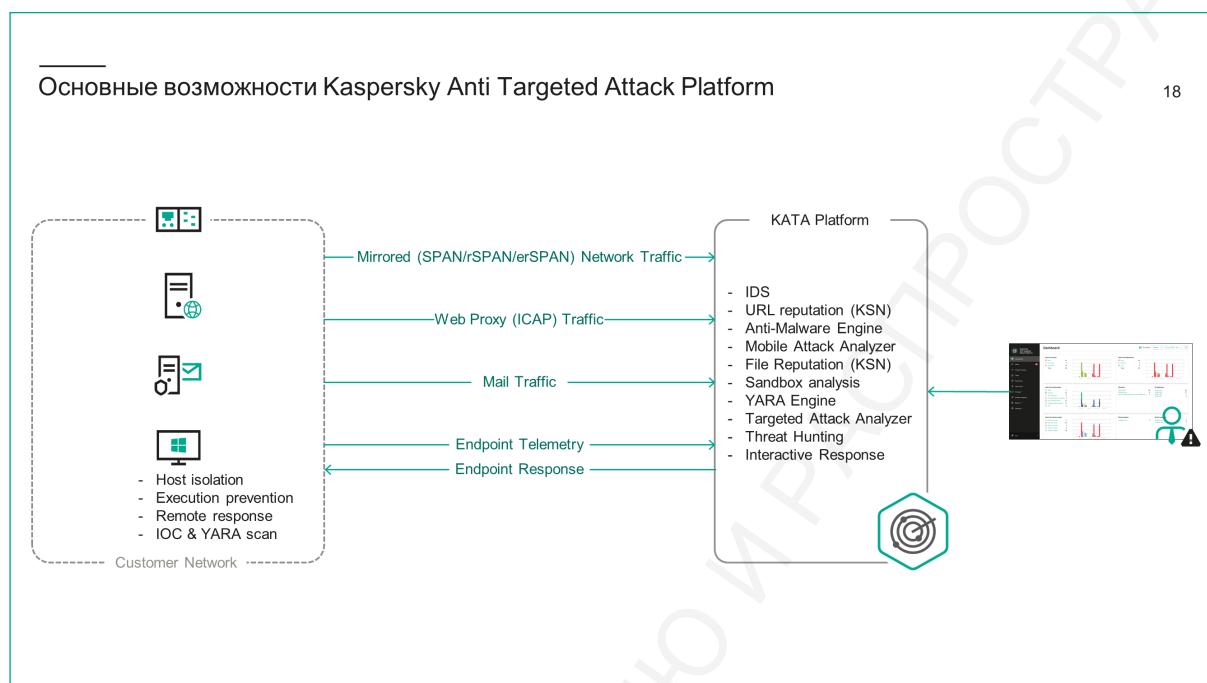
Адаптация процессов, системы ИБ, системы ИТ для предотвращения появления инцидентов в будущем

Работа с KATA Platform строится, принимая во внимание подходы к построению системы ИБ: комплексность, адаптивность, понимание собственных бизнес-процессов.

- Понимание ИТ инфраструктуры и бизнес-процессов компании. Это важный шаг, так как без него нельзя правильно спроектировать систему ИБ и организационные нормы работы.
- Встраиваем KATA Platform в систему ИБ и процессы компании. На этом этапе происходит интеграция KATA Platform в систему ИБ, настраивается техническое взаимодействие между KATA Platform, ИТ-системами, ИБ-системами, а также создаются организационные нормы для работы и обслуживания системы.
- В рамках операционной деятельности выявляем угрозы, устранием их и минимизируем ущерб для компании. Идет оперативная работа по выявлению инцидентов, расследованию и реагированию на атаки.
- Адаптируем процессы, системы ИБ, системы ИТ для предотвращения появления инцидентов в будущем. Последний этап не менее важен, нам необходимо адаптировать наши системы и процессы исходя из полученной информации для того, чтобы инциденты не повторялись.

Глава 2. Подготовка к внедрению

2.1. Состав, возможности

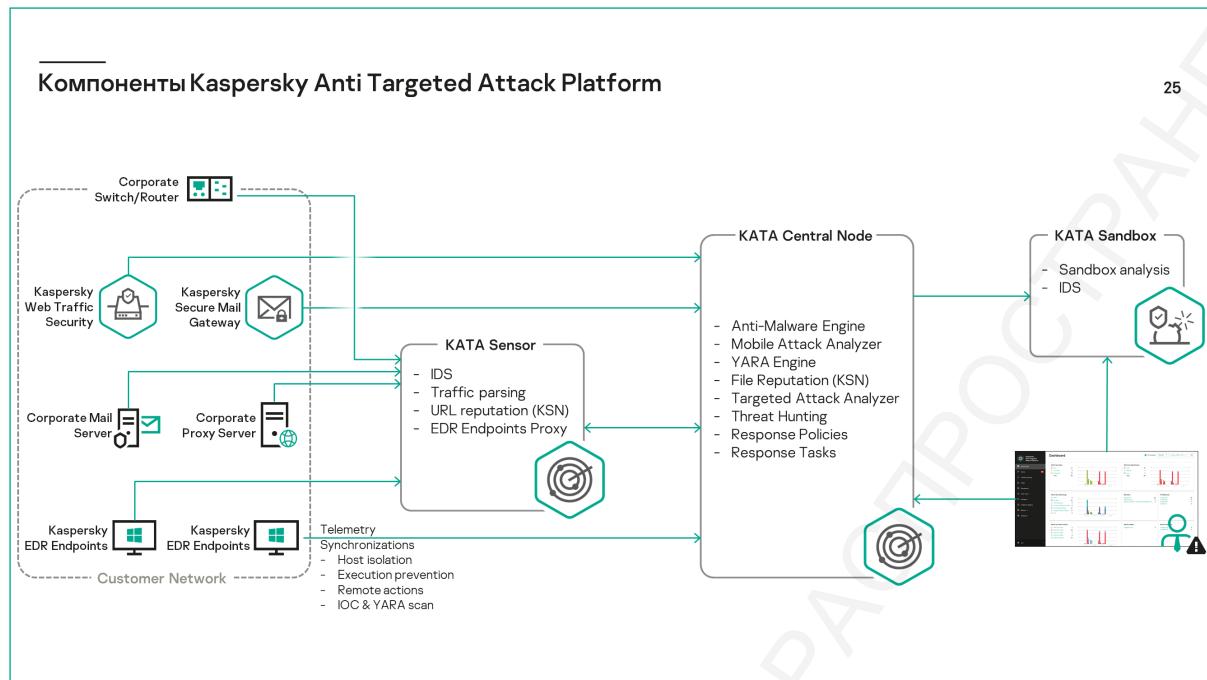


Kaspersky Anti Targeted Attack Platform.

- Анализирует данные в сетевом трафике: в сырой копии сетевого трафика, а также в сообщениях, полученных от почтовой системы, и в объектах, полученных от прокси-сервера.
- Применяет разнообразные технологии обнаружения угроз:
 - Intrusion Detection System к сырому трафику.
 - URL reputation к адресам, извлеченным из трафика и из текста почтовых сообщений.
 - Антивирусную проверку, проверку репутации файлов, проверку цифровой подписи, эмуляцию в виртуальной среде, YARA — к файлам, извлеченным из трафика и почтовых сообщений, а также загруженным по ссылкам в почтовых сообщениях.
- Предоставляет подробную информацию об обнаружениях через веб-консоль.
- Позволяет искать дополнительную информацию об обнаруженных объектах на Kaspersky Threat Intelligence Portal.

Kaspersky Endpoint Detection and Response.

- Собирает данные об активности на узлах сети (телеметрию).
- Автоматически анализирует телеметрию технологией Targeted Attack Analyzer на предмет подозрительной активности.
- Публикует обнаруженную подозрительную активность в веб-консоли.
- Позволяет сотрудникам службы ИБ вручную анализировать базу данных телеметрии (Threat hunting).
- Предоставляет инструменты для удаленного реагирования на инцидент:
 - Изолировать узел от сети.
 - Запретить доступ к файлу.
 - Удалить файл.
 - Поместить файл на карантин.
 - Загрузить файл в централизованное хранилище.
 - Завершить процесс.
 - Запустить программу.
 - Получить данные форензики.
 - Получить дампы памяти процесса или системы.
 - Получить образ диска.
- Применяет к файлам в централизованном хранилище различные технологии обнаружения: антивирусную проверку, проверку репутации файлов, проверку цифровой подписи, эмуляцию в виртуальной среде, YARA.
- Позволяет искать дополнительную информацию об обнаруженных объектах на Kaspersky Threat Intelligence Portal.
- Позволяет искать индикаторы компрометации в базе телеметрии и на узлах сети.



В состав KATA/KEDR входят следующие приложения:

Сенсор.

Сенсоры используются для интеграции с сетевой инфраструктурой организации:

- Он получает данные от сетевых коммутаторов, прокси-серверов, почтовых серверов и почтовых шлюзов. Затем выполняет предварительную проверку: анализирует сетевые пакеты и ссылки, а также извлекает файлы из трафика и передает их вместе с метаданными на Центральный узел для более детального анализа.
- Сенсор может быть встроенным в Центральный узел или отдельным сервером. В сети может быть несколько выделенных Сенсоров.
- В продукте KEDR Сенсор выступает исключительно в роли прокси-сервера для передачи телеметрии от Endpoint-агентов на Центральный узел. Такая функция может быть полезна, например, для оптимизации трафика телеметрии из регионального офиса в штаб-квартиру организации.

Endpoint-агенты.

Endpoint-агенты устанавливаются на рабочие станции и серверы, работающие под управлением ОС Microsoft Windows / Linux / Mac:

- Программа собирает данные об активности процессов, операциях с файлами и реестром, а также об устанавливаемых соединениях. Собранные данные отправляются на Центральный узел для дальнейшего анализа.

- По команде с Центрального узла Endpoint-агенты выполняют действия по сдерживанию опасной активности:
 - Изолировать компьютер от сети (с исключениями);
 - Запретить доступ к заданным файлам;
 - Передать файл на Центральный узел для анализа;
 - Удалить файл или поместить его на карантин;
 - Завершить процесс;
 - Выполнить команду или запустить программу с параметрами

Отличия в функционале Endpoint-агентов под различные ОС мы рассмотрим позднее в курсе.

Центральный узел.

Центральный узел — главный компонент системы:

- получает объекты и данные от Сенсоров и Endpoint-агентов;
- проверяет объекты антивирусным ядром, технологиями Yara и KSN;
- передает объекты для проверки на Sandbox и забирает результаты;
- анализирует данные, выявляя подозрительную активность в трафике и на узлах сети;
- публикует результаты проверки в веб-интерфейсе;

В организациях с большим количеством компьютеров возможна распределенная установка с несколькими Центральными узлами, которые составляют единую иерархию и управляются из единой консоли. Центральный узел может быть совмещен с Сенсором. Также Центральный узел поддерживает кластерную архитектуру, но об этом поговорим позднее.

Sandbox.

Sandbox — это технология анализа поведения объектов в виртуальной среде. В продуктах KATA и KEDR используется Sandbox собственной разработки Лаборатории Касперского. Он основан на технологиях автоматического детектирования вредоносного ПО, которые более 15 лет успешно используются для внутренних нужд компании и постоянно совершенствуются:

- Sandbox-сервер представляет собой специализированный гипервизор с набором виртуальных машин, на которых установлены операционные системы и популярные

приложения разных версий.

- Виртуальные машины запускаются, когда от Центрального узла поступает задача на анализ поведения объекта. Файл или ссылка передаются на виртуальную машину и запускаются. Все действия записываются, а потом анализируются.
- Sandbox запускает исполняемые файлы, офисные документы, скрипты и мультимедиафайлы.

Sandbox — это отдельное устройство, которое «не знает» о существовании других серверов KATA/KEDR. Задача отправки объектов и получения результатов их анализа лежит на стороне Центрального узла. Sandbox-сервер KATA/KEDR работает только с Центральным узлом KATA/KEDR.

Веб-интерфейс.

Веб-интерфейс — это основной инструмент сотрудника службы безопасности для мониторинга и изучения результатов анализа, проведенного продуктами KATA и KEDR. Компонент реализован в виде веб-сервера на центральном узле, к которому можно подключиться, используя любой популярный веб-браузер.

Сенсор, Центральный узел и Sandbox — это отдельные физические или виртуальные серверы. Все соединения между приложениями (компонентами) KATA/KEDR защищены TLS. Соединения между Центральными узлами и Сенсорами дополнительно защищены IPSec.



KATA Platform и KEDR не единственные решения Лаборатории Касперского, которые

предлагают расширенные возможности обнаружения сложных угроз и реагирования на них. КАТА и КЕДР — это мощные инструменты сбора и анализа данных, которые требуют соответствующей высокой квалификации специалистов для эффективного использования.

Не у всех компаний есть такие специалисты. Понимая это, Лаборатория Касперского предлагает таким компаниям решения, которые автоматизируют большую часть анализа, но дают сравнимые возможности обнаружения сложных угроз и ручного реагирования — Kaspersky Endpoint Detection and Response Optimum (KEDR Optimum).

Конечно, квалифицированный аналитик, вооруженный КАТА и КЕДР, сможет обнаружить более скрытные атаки и извлечь больше сведений о проникновении и распространении угрозы по сети. КАТА и КЕДР относятся к так называемой экспертной платформе (expert framework), тогда как КЕДР Optimum относятся к оптимальной платформе (optimum framework). Две платформы предлагают решения для схожих проблем, но для специалистов разной квалификации, с соответствующей разницей в детализации, глубине контекста, а также в требованиях к оборудованию.

В то же время, чтобы клиентам было проще мигрировать с более простого решения на более сложное по мере повышения квалификации, обе платформы частично состоят из общих приложений. Рассмотрим кратко, что объединяет решения в каждой из платформ, и что является ключевым отличием между платформами.

В экспертной платформе главным сервером, который координирует работу всего решения, является Центральный узел КАТА:

- На центральном узле запущена основная консоль управления, которая используется для анализа и обработки обнаружений и в КАТА и в КЕДР.
- В продукте КАТА Центральный узел принимает и анализирует трафик (сам или через выделенный Сенсор).
- Центральный узел посыпает объекты для анализа на сервер КАТА Sandbox и забирает результаты.
- В продукте КЕДР к центральному узлу подключены Endpoint-агенты на компьютерах сети, которые:
 - Шлют телеметрию на Центральный узел.
 - Принимают от Центрального узла команды в рамках реагирования на инциденты.
 - На центральном узле расположены базы данных телеметрии и обнаружений.

В оптимальной платформе главным сервером является Сервер администрирования Kaspersky Security Center:

- Основным инструментом для анализа и обработки обнаружений является веб-консоль Kaspersky Security Center.
- База данных обнаружений подключена к серверу Kaspersky Security Center.
- В продукте KEDR Optimum к серверу Kaspersky Security Center подключены Endpoint-агенты на компьютерах сети:
 - Шлют телеметрию на сервер Kaspersky Security Center.
 - Принимают команды реагирования от сервера Kaspersky Security Center.

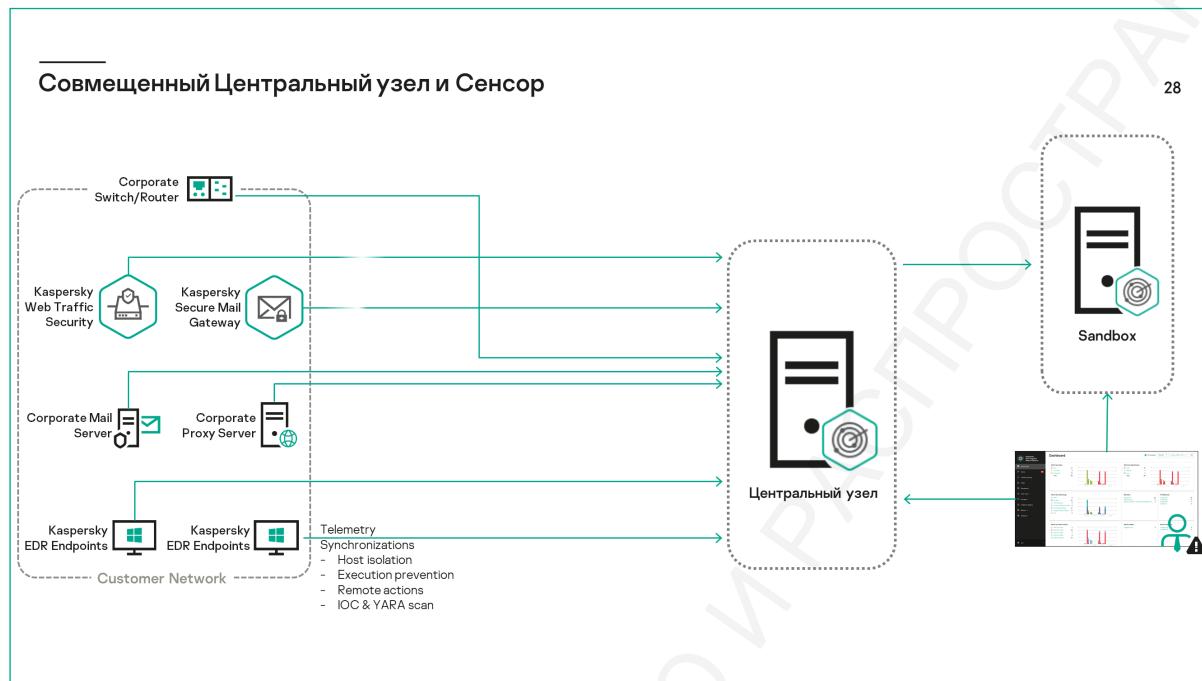
Принимая во внимание, что существует часть заказчиков, которая заинтересована в экспертной платформе, но не имеет возможности и ресурсов развернуть платформу KATA/KEDR локально, создан второй вариант экспертной платформы — Kaspersky EDR Expert. В данном варианте:

- Основным инструментом для анализа и обработки обнаружений является веб-консоль Kaspersky Security Center Cloud Console.
- Телеметрия появляется в хранилище на базе KSN и хранится в облаке.
- Endpoint-агент не предусмотрен в виде отдельного приложения, он является компонентом средств защиты, установленных на узле (например, KES).

Также существует решение Kaspersky XDR, которое может интегрироваться с решением KEDR, и которое позволяет:

- Собирать данные из множества различных источников и хранить их в виде, удобном для анализа
- Вручную и автоматически анализировать собранные данные и выявлять угрозы
- Опираясь на отчеты и панель мониторинга комплексно оценивать уровень корпоративной безопасности
- Анализировать этапы развития киберугроз используя граф расследования
- Управлять конечными устройствами и надежно защищать их с помощью Kaspersky Endpoint Security
- Автоматически и вручную реагировать на угрозы, что в комбинации интеграционными возможностями продукта позволяет реализовывать сложные кросс-продуктовые сценарии защиты. Можно запускать не только какое-то одно определенное действие вручную, но и автоматически выполнять сложные многоходовые сценарии реагирования.
- Эффективно работать с собранными данными.

2.2. Схемы развертывания, масштабирование, совместимость



Рассмотрим схему развертывания Центрального узла совмещенного с Сенсором. При использовании этой схемы развертывания компоненты Центральный узел и Сенсор устанавливаются на одном физическом или виртуальном сервере. Этот сервер принимает трафик, выполняет первичный анализ трафика и более глубокий анализ извлеченных файлов. По результатам проверки компоненты выявляют признаки целевых атак на IT-инфраструктуру организации.

При использовании функциональности KATA и KEDR вы можете установить Endpoint-агент на компьютерах локальной сети организации. При использовании функциональности KATA Endpoint-агент не устанавливается.

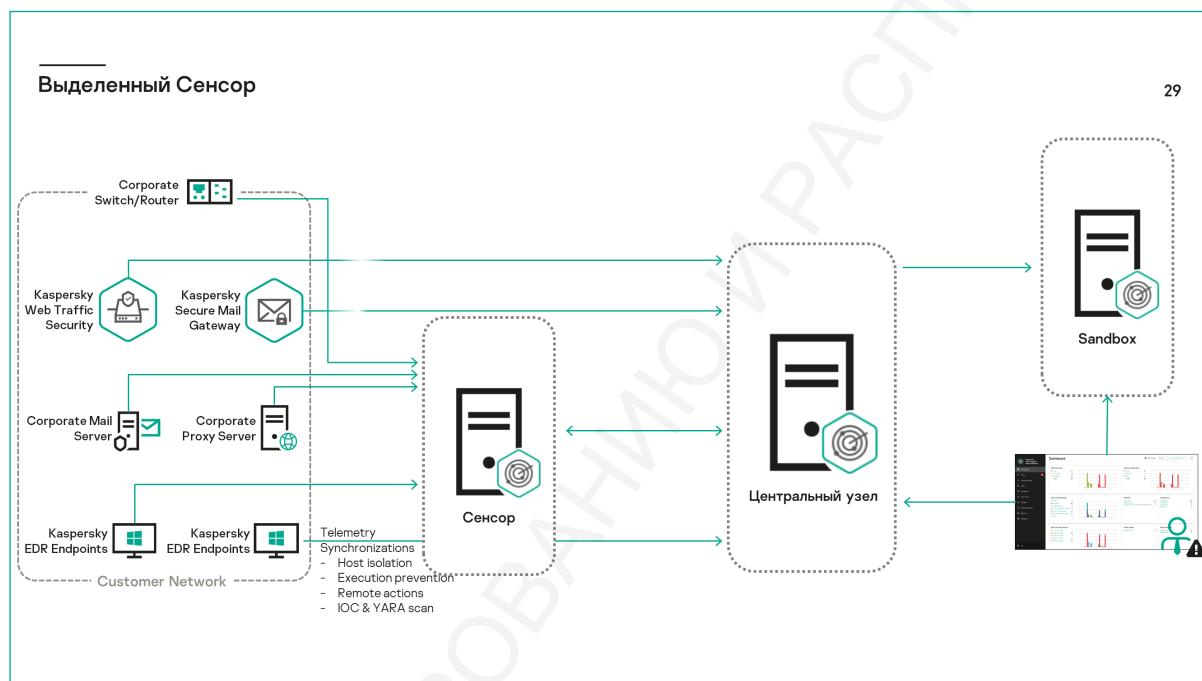
Схема подходит разворачивания на основной площадке, когда:

- Мощности одного сервера для компонентов Центральный узел и Сенсор хватает для захвата трафика, глубокого анализа, а также обработки данных с конечных узлов (пропускная способность канала до 1 Гбит/с, Endpoint-агенты могут использоваться или не использоваться);
- Нет необходимости в анализе трафика на удаленных площадках;
- Выход в интернет с удаленных площадок осуществляется через основной сайт;
- Есть возможность захватывать сетевой, веб и почтовый трафик одним устройством.

К одному центральному узлу можно подключить до 15 000 Endpoint-агентов. Если в организации больше узлов, используйте распределенную установку с несколькими Центральными узлами или кластер Центральных узлов, к которому будет возможность подключить до 30000 Endpoint-агентов.

На другом сервере устанавливается компонент Sandbox.

Стоит учитывать, что одного сервера Sandbox может быть недостаточно, если в организации используется Kaspersky Anti Targeted Attack.



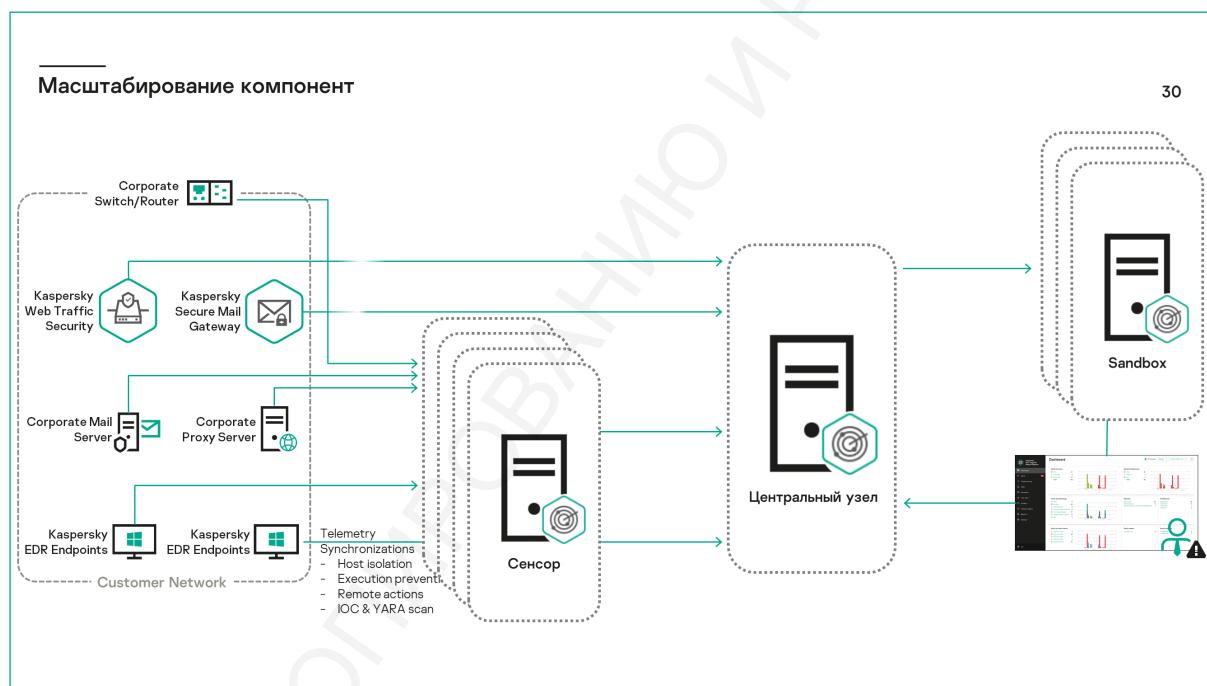
Если в организации есть локальные офисы, их компьютеры не обязательно подключать прямо к центральному узлу. Это может быть неудобно из-за необходимости создавать слишком широкие исключения в сетевых экранах. Вместо этого можно установить в удаленном офисе Сенсор и подключить Endpoint-агенты к нему, а уже Сенсор подключить к центральному узлу в главном офисе. В такой конфигурации Сенсор будет передавать данные от Endpoint-агентов на Центральный узел. К одному Сенсору можно подключить до 15 000 Endpoint-агентов.

Центральный узел с ролью Сенсора тоже может захватывать трафик и проводить первичный анализ. В таком сценарии выделенный Сенсор устанавливают на одной из удаленных площадок, трафик на которой требуется анализировать. На основной площадке захват будет осуществляться Центральным узлом, который должен быть достаточно мощным для совмещения двух ролей, а также иметь возможность получать трафик из всех интересующих источников. Если пропускная способность канала на основном сайте составляет более 1 Гбит/с, то выделенный Сенсор нужен и на основной площадке в дополнение к центральному узлу.

Трафик между Центральным узлом и Сенсором составляет 10% от трафика на SPAN-порте при обычной нагрузке или 20% от трафика на SPAN-порте при пиковой нагрузке + почтовый трафик + трафик по протоколу ICAP, получаемого Сенсором.

Поскольку трафик от почтовых и прокси-серверов не создает заметной дополнительной нагрузки ни на Сенсор, ни на Центральный узел, его можно направить на любой из этих серверов.

То есть, например, можно весь трафик: и SPAN, и от почтовой системы, и от прокси-сервера — направить на Сенсор, а на центральном узле оставить только функции проверки объектов. Или же можно, при тех же аппаратных характеристиках серверов, направить на Сенсор только SPAN-трафик, а почтовые сообщения и трафик от прокси-сервера направить прямо на Центральный узел. Оба варианта могут работать одинаково хорошо и предпочтительный вариант будет зависеть от топологии сети.



Предел в 15 000 Endpoint-агентов на один Центральный узел не зависит от способа подключения Endpoint-агентов: прямо или через Сенсор в роли прокси. Если к Центральному узлу подключено 10 000 Endpoint-агентов через 2 Сенсора в роли прокси, значит к нему можно подключить еще до 5 000 Endpoint-агентов.

Для использования функционала КАТА может потребоваться использовать выделенный Сенсор для захвата трафика, первичного анализа, извлечения файлов и передачи их на Центральный узел для более глубокого исследования. Таких выделенных Сенсоров может быть несколько.

Схема используется для разворачивания на основной площадке, когда:

- Мощности одного сервера не хватает для захвата трафика и глубокого анализа (пропускная способность канала более 1 Гбит/с);
- Нет возможности захватывать трафик одним устройством со всех интересующих почтовых серверов, почтовых шлюзов, прокси-серверов и сетевых коммутаторов.

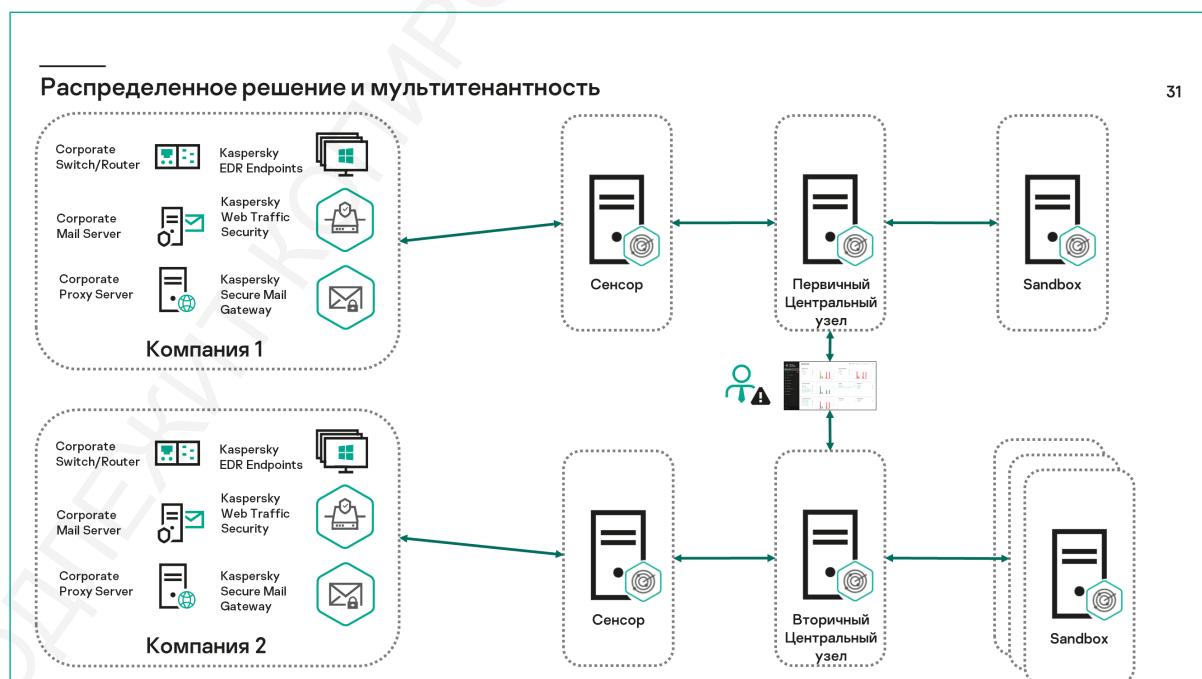
Требуемая мощность Sandbox-серверов в установке КАТА будет зависеть от количества и типов файлов в трафике.

Чтобы обработать большой поток файлов в трафике потребуется параллельно запускать много виртуальных машин на сервере Sandbox. В то же время количество виртуальных машин, которые могут быть запущены одновременно на сервере Sandbox, ограничено аппаратными ресурсами сервера. Если поток файлов требует запускать больше виртуальных машин, потребуется увеличивать ресурсы Sandbox. Это можно делать двумя путями:

- Наращивать аппаратные ресурсы сервера: добавить память, установить больше процессоров или более мощные процессоры; Подойдет для bare-metal установок Sandbox-сервера.
- Увеличить количество Sandbox-серверов.

Этот подход проще, так как не нужно ничего менять в уже имеющихся серверах.

Если объем трафика требует использовать больше одного сервера Sandbox, их все можно и нужно подключить к центральному узлу. Центральный узел отвечает за распределение файлов между серверами Sandbox.



Чтобы получать и обрабатывать информацию о локальной активности на более чем 15 000 компьютеров, потребуется несколько Центральных узлов. Чтобы информация об угрозах и инструменты реагирования по-прежнему были доступны в одной консоли (а не в отдельных консолях разных Центральных узлов), нужно использовать распределенный режим. В этом режиме один из Центральных узлов назначается первичным, а остальные Центральные узлы подключаются как вторичные. Все управление и мониторинг будут сосредоточены в консоли первичного Центрального узла.

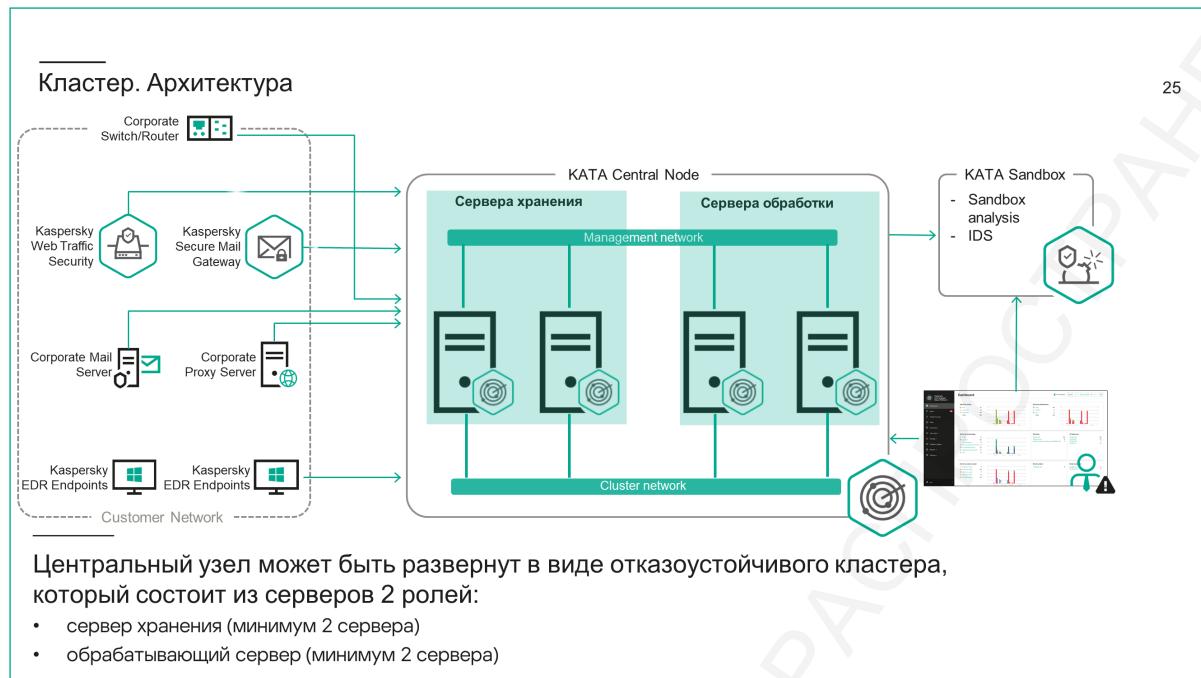
Чтобы обрабатывать больший трафик, также потребуется установка, в которой больше чем один Центральный узел отвечает за обработку объектов из трафика. Например, если нужно проверять 12 Гбит/с трафика, потребуется как минимум 2 Центральных узла. Дополнительно нужно учесть, что Центральный узел не может непосредственно обрабатывать больше 1 Гбит/с трафика, поэтому сырой трафик нужно будет обрабатывать через выделенные Сенсоры. Также нужно учитывать топологию сети: как именно маршрутизируется внешний трафик организации, и как его можно разделить на несколько потоков для проверки разными Сенсорами. Топология может накладывать дополнительные ограничения на количество и расположение Сенсоров.

В таких случаях, Центральные узлы можно объединить в распределенную установку, чтобы обрабатывать все обнаружения из общей консоли первичного Центрального узла.

Если вы используете режим распределенного решения, учитывайте, что аппаратные требования к серверу первичного Центрального узла на 10% выше чем обычно.

Вы можете подключить к одному первичному Центральному узлу до 30 вторичных Центральных узлов.

В распределенной установке KATA/KEDR почти наверняка потребуется больше одного сервера Sandbox. Для оптимальной загрузки Sandbox можно подключить каждый Центральный узел к каждому серверу Sandbox.



Компонент Центральный узел может быть развернут в виде отказоустойчивого кластера, который состоит из серверов 2 ролей — серверов хранения и обрабатывающих серверов. Отказоустойчивость достигается за счет дублирования данных между серверами хранения и избыточности вычислительных ресурсов: при выходе из строя одного сервера его функции выполняет другой сервер с аналогичной ролью. Программа при этом продолжает работать.

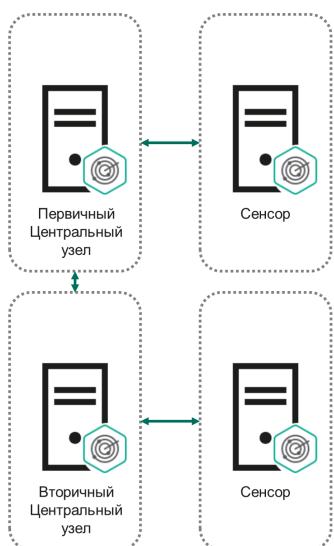
Кластер должен включать минимум 4 сервера: 2 сервера хранения и 2 обрабатывающих сервера. Есть возможность масштабировать кластер для увеличения количества обрабатываемого трафика или количества подключенных хостов, но рекомендуется добавлять в кластер серверы с одинаковой аппаратной конфигурацией. В противном случае пропорциональное увеличение производительности не гарантируется.

Если для обрабатывающего сервера настроено получение зеркальированного трафика со SPAN-портов, то при выходе из строя этого сервера SPAN-трафик не обрабатывается. Кластер использует Ceph — программно-определенную распределенную файловую систему с открытым исходным кодом — и из-за этого накладывается ряд требований на дисковую подсистему для хранения телеметрии и файлов:

- Использовать не менее 3 дисков для Ceph-хранилища.
- Рекомендовано использовать диски одинакового объема.

Требования для Центрального узла

26



Трафик не больше **1 Гбит/с**. При превышении необходимо **развернуть сенсор** для обработки входящего трафика

Максимальное количество **агентов** для одного центрального узла - **15000**

Требования к хранилищу:

- Первая дисковая подсистема – 2ТБ
- Вторая дисковая подсистема – минимум 2.4ТБ и максимум 12ТБ

Формула расчета требуемого пространства для **второй** дисковой подсистемы (в гигабайтах):

- $150 + (\text{количество агентов})/15000 * (400+240*(\text{срок хранения в днях}))$

Перед внедрением важно оценить, сколько и каких ресурсов потребуется серверам КАТА/KEDR, исходя из предполагаемой загрузки.

Аппаратные требования к серверу, на котором установлены компоненты Central Node и Sensor, зависят от следующих условий:

- объем обрабатываемого трафика;
- количество обрабатываемых сообщений электронной почты в секунду;
- количество хостов с Kaspersky Endpoint Agent.

Одна из распространенных ошибок при пилотном или производственном внедрении — это использование недостаточных ресурсов для серверов КАТА/KEDR. Недостаток памяти, процессорных ядер и места на диске может снижать эффективность технологий обнаружений и повышать риск пропустить признаки атаки.

Лучше ошибиться в большую сторону и дать серверам больше ресурсов, чем абсолютно необходимо. В конце концов pragmatically ожидать, что объем обрабатываемой информации со временем будет увеличиваться.

Чтобы не ошибиться в меньшую сторону, полезно понимать, о какого порядка ресурсах идет речь для минимальной, средней и максимальной нагрузки. В первую очередь имеет смысл обращать внимание на память и процессор. Дисковое пространство гораздо проще нарастить без переустановки системы.

Требования к центральному узлу определяются нагрузкой. В продукте КАТА это поток объектов,

поступающих из трафика, а также объем трафика, непосредственно поступающего на Центральный узел в роли Сенсора. В продукте KEDR это число подключенных Endpoint-агентов.

Максимальная конфигурация Центрального узла с лицензией KEDR, способная обрабатывать данные 15 000 узлов, требует:

- 192 ГБ оперативной памяти;
- 32 логических ядра процессора с минимальной частотой в 3 ГГц.

Максимальная конфигурация Центрального узла (с компонентом Sensor на отдельном сервере) с лицензией KATA, способная обрабатывать объем трафика 10000 Мбит/с со SPAN-портов:

- 128 ГБ оперативной памяти;
- 112 логических ядра процессора с минимальной частотой в 3 ГГц.

Конфигурация Центрального узла, для обработки событий с 10000 Endpoint-агентов и 1000 Мбит/с:

- 192 ГБ оперативной памяти;
- 48 логических ядра процессора с минимальной частотой в 3 ГГц.

Расчет места, необходимого для хранения телеметрии с Endpoint-агентов, зависит от нескольких переменных:

- Количество узлов,
- Время хранения телеметрии в днях.

Для работы Центрального узла необходимо выделить две дисковых подсистемы:

- первая подсистема для ОС и самого Центрального узла
- вторая подсистема для хранения событий

Объем первой дисковой подсистемы от 1 до 2 ТБ.

Формула расчета требуемого пространства для второй дисковой подсистемы на которой хранятся события (в гигабайтах):

- $150 + (\text{количество Endpoint-агентов})/15000 * (400+240*(\text{срок хранения в днях}))$

Подробная информация по требуемым ресурсам Центрального узла доступна по

ссылке <https://support.kaspersky.com/KATA/6.0/ru-RU/247136.htm>

Требования для Центрального узла

27



Поддерживается только **Ubuntu**

Не поддерживается отказоустойчивость со стороны приложения

Сенсор должен быть развернут **вместе** с центральным узлом

Sandbox – **вне KVM**

Отдельный сетевой интерфейс для **SPAN-трафика**

Версия 6.0 поддерживает установку решения на гипервизор KVM. Важно отметить, что в таком сценарии существует ряд ограничений:

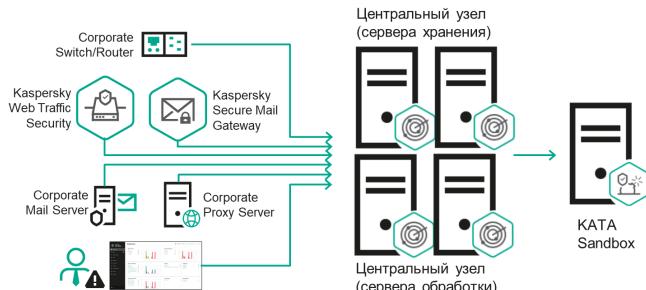
- поддерживается только совместная установка Центрального узла и Сенсора в рамках одной виртуальной машины;
- следует использовать операционную систему Ubuntu и выделить отдельный интерфейс для SPAN-трафика;
- возможна установка только неотказоустойчивой версии приложения;
- возможно подключение только компонента Sandbox, развернутого вне платформы виртуализации KVM;
- невозможно использование API для получения внешними системами информации об обнаружениях приложения и API для получения внешними системами информации о событиях приложения;
- не гарантируется поддержка KVM-виртуализаций, используемых в облачных решениях.

Аппаратные требования к Центральному узлу с развернутым решением KEDR и подключенными 250 Endpoint-агентами:

- 24 ГБ оперативной памяти;
- 6 логических ядра процессора с минимальной частотой в 3 ГГц.

Требования для серверов кластера центрального узла

28



Дополнительные требования для кластера:

- 2 сервера хранения и 2 обрабатывающих сервера
- два сетевых адаптера для настройки кластерной и внешней подсети
- Кластерная подсеть должна функционировать со скоростью 10 Гбит/с
- Серверы кластера должны находиться в одном L1- или L2-сегменте. Для этого вы можете подключить все серверы кластера к одному коммутатору или использовать программное туннелирование. Например, L2TPv3 или Overlay Transport Virtualization (OTV)
- Значение сетевой задержки ("network latency") должно удовлетворять требованию "single digit latency", то есть в миллисекундах значение должно быть менее 10

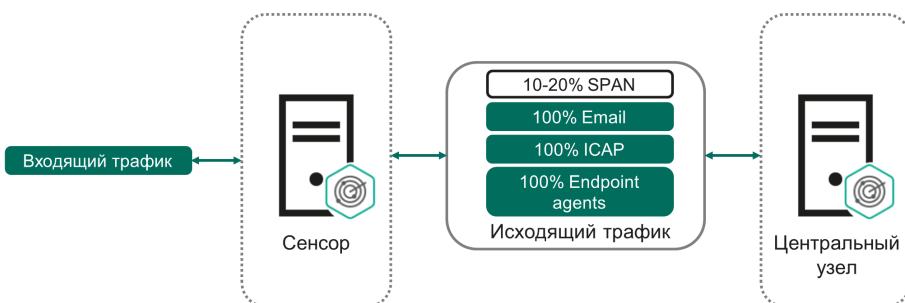
Каждый сервер кластера должен иметь два сетевых адаптера для кластерной и внешней подсети. Кластерная подсеть должна функционировать со скоростью 10 Гбит/с.

Для кластерной подсети также должны выполняться следующие требования:

- В кластерную подсеть должны входить только серверы кластера и сетевые коммутаторы;
- Кластерная подсеть должна быть изолированной;
- Серверы кластера должны находиться в одном L1- или L2-сегменте. Для этого вы можете подключить все серверы кластера к одному коммутатору или использовать программное туннелирование. Например, L2TPv3 или Overlay Transport Virtualization (OTV);
- Значение сетевой задержки ("network latency") должно удовлетворять требованию "single digit latency", то есть в миллисекундах значение должно быть менее 10.

Требования для Сенсора

29



Максимальный объем трафика для одного сенсора – 10 Гбит/с

Сенсор отправляет на Центральный узел **от 10% до 20%** полученного **SPAN-трафика**

Сенсор отправляет на Центральный узел **100% трафика** почтовых сообщений, ICAP-трафика и трафика от Endpoint-агентов

В конфигурациях Kaspersky Endpoint Detection and Response выделенный Сенсор только проксирует соединения между Endpoint-агентами и Центральным узлом, никаких сложных вычислений не выполняет и поэтому большого количества ресурсов не требует.

В сценариях Kaspersky Anti Targeted Attack Сенсоры нужны дополнительные ресурсы для обработки большого количества зеркального сетевого трафика. Почтовые сообщения и объекты по протоколу ICAP Сенсор практически без обработки пересыпает на Центральный узел.

Сенсор может работать как на физическом, так и на виртуальном сервере.

При расчете аппаратных требований к компоненту Сенсор требуется учитывать, что максимальный объем обрабатываемого трафика составляет 10 Гбит/с. Для обработки трафика максимального объема можно использовать как один компонент Сенсор, установленный на отдельном сервере, так и несколько компонентов Сенсор, установленных на отдельных серверах, которые подключены к одному компоненту Central Node. Суммарный объем передаваемого трафика от всех компонентов Sensor, подключенных к одному компоненту Central Node, не должен превышать 10 Гбит/с.

Подробная информация по требуемым ресурсам компонента Сенсор доступна по ссылке <https://support.kaspersky.com/KATA/6.0/ru-RU/211923.htm>

Требования для Sandbox

30

Физический сервер**Только Intel CPU**

Количество запускаемых виртуальных машин-песочниц = $\text{sum}(\text{ядер CPU}) * 1.5$

- но не больше 200

Количество серверов = $\text{sum}(\text{поступающих файлов}) * \text{sum}(\text{образов ОС}) / 1000$

Виртуальная машина**Только Intel CPU**

Количество запускаемых виртуальных машин-песочниц = $\text{sum}(\text{ядер CPU}) * 1.5$

- но не больше 12

Количество серверов = $\text{sum}(\text{поступающих файлов}) * \text{sum}(\text{образов ОС}) / 280$

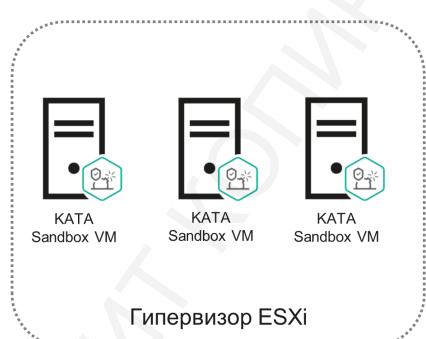
Потребуется в **4 раза больше** экземпляров Sandbox VM по сравнению с физическим Sandbox-сервером

Sandbox будет работать как на физическом сервере, так и в виртуальной среде VMware ESXi.

При установке компонента Sandbox на виртуальную машину VMware ESXi нужно установить ограничение для количества одновременно запускаемых виртуальных машин — 12. Поддерживаются только процессоры Intel, процессоры AMD не поддерживаются.

Требования для Sandbox

31



В настройках CPU виртуальной машины:

- Expose hardware-assisted virtualization to guest OS
- **Зарезервируйте** весь объем производительности **CPU**

В настройках RAM виртуальной машины:

- **Зарезервируйте** весь объем **RAM**

В настройках виртуальной машины:

- Latency Sensitivity = **High**

При установке компонента Sandbox на виртуальную машину VMware ESXi:

- Процессор Intel Xeon 15 Core (HT);
- 32 ГБ оперативной памяти;
- HDD объемом 300 ГБ.

На виртуальной машине:

- Разрешена вложенная виртуализация.
- Установлены параметры High Latency Sensitivity.
- Зарезервирована вся оперативная память.
- Зарезервирована вся частота процессора.

При настройке виртуальной машины вам требуется задать описанную выше конфигурацию. Допускается изменение только частоты процессора: вы можете задать частоту 2.2 ГГц и выше. Если при настройке виртуальной машины вы зададите конфигурацию, отличную от описанной, корректная установка и работа компонента Sandbox не гарантируется.

Если планируется использовать несколько Sandbox-серверов, то для балансировки нагрузки рекомендуется одинаковая спецификация серверов и одинаковый набор виртуальных машин

Сетевые интерфейсы:

- Первый сетевой адаптер используется в качестве управляющего интерфейса и получения задач проверки от Центрального узла.
- Второй сетевой интерфейс необходим для анализа поведения объектов и обновления баз.

Запретите доступ в локальную сеть организации для защиты сети от анализируемых объектов и предоставьте неограниченный доступ в Интернет.

Для второго интерфейса желательно отключить любые ограничения и фильтрацию трафика, чтобы обрабатываемые объекты могли беспрепятственно устанавливать соединения в Интернет. Так будет проще выявить активность вредоносных модулей, пытающихся просканировать сеть или связаться с центром управления.

Sandbox сможет проверять объекты и без второго интерфейса. В этом случае вместо доступа в Интернет виртуальные машины получат доступ в «фальшивый Интернет», организованный специальной виртуальной машиной в составе Sandbox. Вероятность успешного обнаружения вредоносных объектов в такой конфигурации ниже.

Требования для Sandbox

32

Configuration Parameters

Add New Configuration Params

Name: numa.nodeAffinity Value: 0

CANCEL OK

Виртуальная машина должна размещаться в пределах **одного узла NUMA**:

- Убедитесь, что количество ядер VM **не превышает** суммарное количество ядер физического CPU
- Убедитесь, что на физическом сервере виртуализации **достаточно RAM в рамках одного NUMA-узла**
- В настройках виртуальной машины выставлен параметр **numa.nodeAffinity**

Важно отметить, что Sandbox в виде виртуальной машины нельзя масштабировать вертикально, увеличивая или уменьшая количество ресурсов виртуальной машины. Требования к количеству виртуальных машин Sandbox зависят от предполагаемой нагрузки. Для точного расчета рекомендуется провести пилотное тестирование под полноценной нагрузкой.

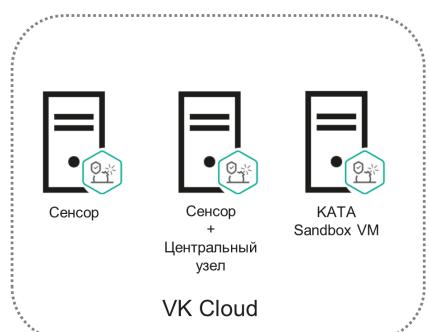
Мы рекомендуем размещать виртуальную машину Sandbox с привязкой к определенному NUMA-узлу. Это снизить задержки и уменьшит вероятность детектирования песочницы вредоносным программным обеспечением.

Убедитесь, что у NUMA-узла физического сервера достаточно ресурсов для размещения виртуальной машины Sandbox.

Обязательно выставьте параметр numa.NodeAffinity в настройках виртуальной машины.

Требования для Центрального узла в VK Cloud

33



Только сертифицированная версия на базе ос
Astra Linux

Не поддерживается отказоустойчивость со
стороны приложения

Отдельный сетевой интерфейс для **SPAN-**
трафика

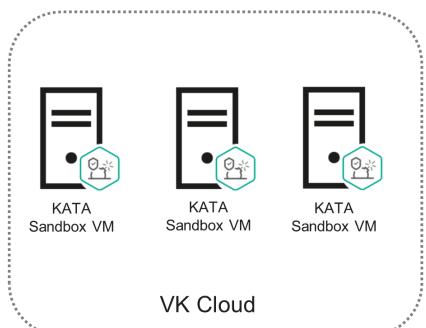
Релиз версии 6.0 поддерживает установку в облаке VK Cloud. Важно отметить, что:

- Поддерживается только сертифицированная версия на базе операционной системы Astra Linux.
- Нельзя сформировать кластер. Используйте технологии высокой доступности облачной среды виртуализации.
- Требуется обязательно указать отдельный сетевой интерфейс для SPAN-трафика.

При этом нет ограничений на установку компонентов решения. Вы можете установить отдельный Сенсор и виртуальную машину Sandbox.

Требования для Sandbox в VK Cloud

34



Включите вложенную виртуализацию

Разделите интерфейсы управления и выхода в интернет на **разные подсети**

Настройте **выход в интернет** для интерфейса, который используют виртуальные машины-песочницы

Изолируйте этот интерфейс **от сети** вашей организации

Не используйте **статический** публичный **IP-адрес** для интерфейса с выходом в интернет

Для работы виртуальной машины Sandbox в облаке VK Cloud требуется соблюсти ряд требований:

- Включите вложенную виртуализацию. Иначе Sandbox не сможет запустить виртуальные машины-песочницы.
- Обязательно разделите интерфейсы управления и выхода в интернет на разные подсети.
- Настройте выход в интернет для интерфейса, который используют виртуальные машины-песочницы и оградите его доступа в сеть организации.
- Не используйте публично-доступный статический IP-адрес для интерфейса с выходом в интернет.

Требования для сбора телеметрии

35

Endpoint agent**Только Windows**

Развертывание с помощью локального дистрибутива или Kaspersky Security Center

Полноценная поддержка начиная с версии **3.15 и выше**

Ограниченнная поддержка версий 3.12 и 3.13

Необходимо рассчитать требуемую **полосу пропускания**

Endpoint Security

Поддержка нескольких типов систем – **Windows, Linux и Mac**

Развертывание с помощью локального дистрибутива или Kaspersky Security Center

Есть ограничения для старых версий (см. справку соответствующего продукта)

Необходимо рассчитать требуемую **полосу пропускания**

Для сбора телеметрии с конечных точек используются Endpoint-агенты. Одним из нововведений стала поддержка Kaspersky Endpoint Security (KES) актуальных версий для сбора телеметрии вместо Kaspersky Endpoint Agent (KEA). Теперь вы можете выбирать тот или иной тип Endpoint-агента, в зависимости от ваших потребностей.

Важно учитывать, что KEA доступен только для Windows-систем. Если вы планируете собирать данные телеметрии с операционных систем Linux и Mac, вам потребуется KES. В любом случае, важно соблюдать поддерживаемую версионность между КАТА-платформой и Endpoint-агентами.

В обоих случаях поддерживается как локальная, так и централизованная установка с помощью Kaspersky Security Center.

В зависимости от общего числа и расположения компьютеров, внедрение может потребовать больше серверов для подключения всех Endpoint-агентов:

- В больших организациях, где число компьютеров от 15 000 до 30 000, для сбора и обработки телеметрии можно развернуть Центральный узел в виде кластера. В случае, если количество компьютеров превышает 30 000 или вы не хотите использовать кластер, то вам потребуется развернуть несколько Центральных узлов и связать их в общую структуру в рамках распределенного режима.
- Для подключения компьютеров, расположенных за пределами сетевого периметра, нужно использовать дополнительный сервер в DMZ. Из соображений безопасности лучше разместить в DMZ KATA Sensor и использовать его в качестве прокси-сервера для соединений с Endpoint-агентов.

- В распределенных организациях с удаленными офисами можно уменьшить трафик между офисами, если разместить в каждом из них отдельный Центральный узел. Обмен данными между Центральными узлами сводится в основном к репликации списков Endpoint-агентов, обнаружений и настроек. Телеметрия компьютеров хранится в локальной базе данных Центрального узла, к которому они подключены, и между Центральными узлами не реплицируется. Но при поиске событий с помощью инструмента Threat hunting, запрос копируется на все Центральные узлы и результаты поиска передаются на первичный Центральный узел для отображения в консоли. В любом случае это значительно меньше данных, чем непрерывный поток телеметрии от компьютеров.
- В небольшом офисе можно использовать Сенсор в роли прокси из соображений безопасности. В этом случае не нужно разрешать всем компьютерам соединяться с Центральным узлом в главном офисе, а достаточно дать такое разрешение только Сенсору. Сенсор не уменьшает трафик от Endpoint-агентов к центральному узлу.

Глава 3. Развёртывание платформы КАТА

3.1. Установка Центрального узла в виде кластера и установка Сенсора

Внедрение Kaspersky Anti Targeted Attack требует изучения сетевой инфраструктуры заказчика:

Сначала необходимо собрать общие данные о сети заказчика:

- Точки выхода в интернет;
- Наличие удаленных офисов;
- Ширине каналов;
- Соединениях между головным офисом и удаленными площадками.

Далее определите способы интеграции с инфраструктурой и расположение интересующих устройств и серверов:

- Получение копии трафика от сетевых устройств;
- Получение копий объектов от прокси-серверов;
- Загрузка копий почтовых сообщений с почтовых серверов или получение сообщений от почтовых шлюзов;
- Получение данных от Kaspersky Secure Mail Gateway, Kaspersky Security for Linux Mail Server или Kaspersky Web Traffic Security.

Не рекомендуется получать один и тот же трафик разными способами.

Рассчитайте аппаратную конфигурацию КАТА-серверов на основе данных об инфраструктуре, полученных при выполнении двух предыдущих шагов. При планировании учтите, что:

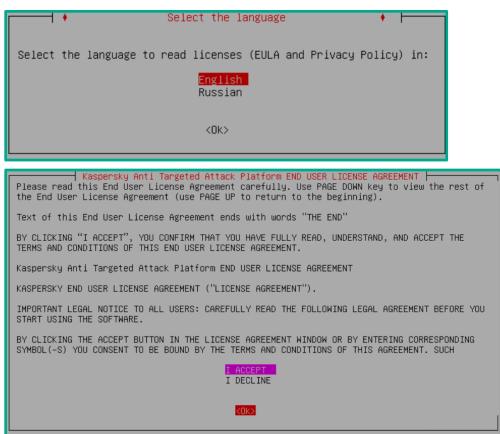
- В сети может быть один или несколько Сенсоров;
- Роль Сенсора и Центрального узла может выполнять один и тот же сервер;
- Рекомендуется проверять сетевой и почтовый трафик, а не какой-то один вид;
- Kaspersky Secure Mail Gateway может играть роль Сенсора для захвата почтового трафика;
- Kaspersky Web Traffic Security может заменять интеграцию с прокси-сервером;
- При необходимости можно использовать несколько Центральных узлов в распределенной установке.

Компоненты Центральный узел, Сенсор, Sandbox можно устанавливать в произвольном порядке. При установке кластерного варианта Центрального узла важно первым сервером установить узел хранения, далее можно добавлять узлы кластера в произвольном порядке.

Кластер. Установка сервера хранения

36

Вставьте инсталляционный диск и загрузите с него сервер



Выберите язык Лицензионного соглашения и Политики конфиденциальности

Прочтите Лицензионное соглашение и нажмите **I accept**

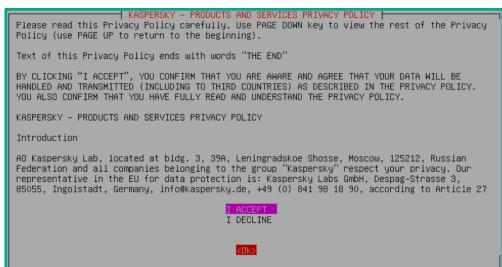
Чтобы начать установку сервера хранения кластера Центрального узла вставьте инсталляционный диск в сервер или подключите ISO-образ. Загрузите сервер с него и дождитесь автоматического начала установки. В ходе установки Центрального узла будет развернута операционная система с необходимыми пакетами.

Выберите язык лицензионного соглашения. Установка выполняется только на английском языке, но лицензионное соглашение можно также прочитать на русском.

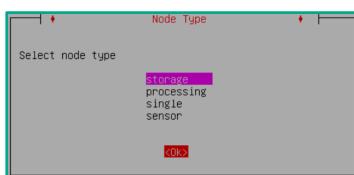
Ознакомьтесь и нажмите **I accept**, если вы согласны с условиями. Администратор не может продолжить установку продукта без согласия с текстом лицензионного соглашения.

Кластер. Установка сервера хранения

37



Прочтите Политику конфиденциальности и нажмите **I accept**



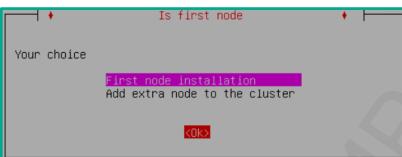
Выберите тип сервера **storage** и нажмите **Ok**

Прочтайте и примите политику конфиденциальности. Система предложит выбрать тип сервера, который планируется установить, первым всегда устанавливается сервер хранения.

Выберите Storage и нажмите Ok.

Кластер. Установка сервера хранения

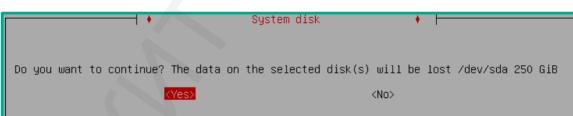
38



Выберите установку первого узла кластера **First node installation** и нажмите **Ok**



Выберите **диск** для установки системы и нажмите **Ok**



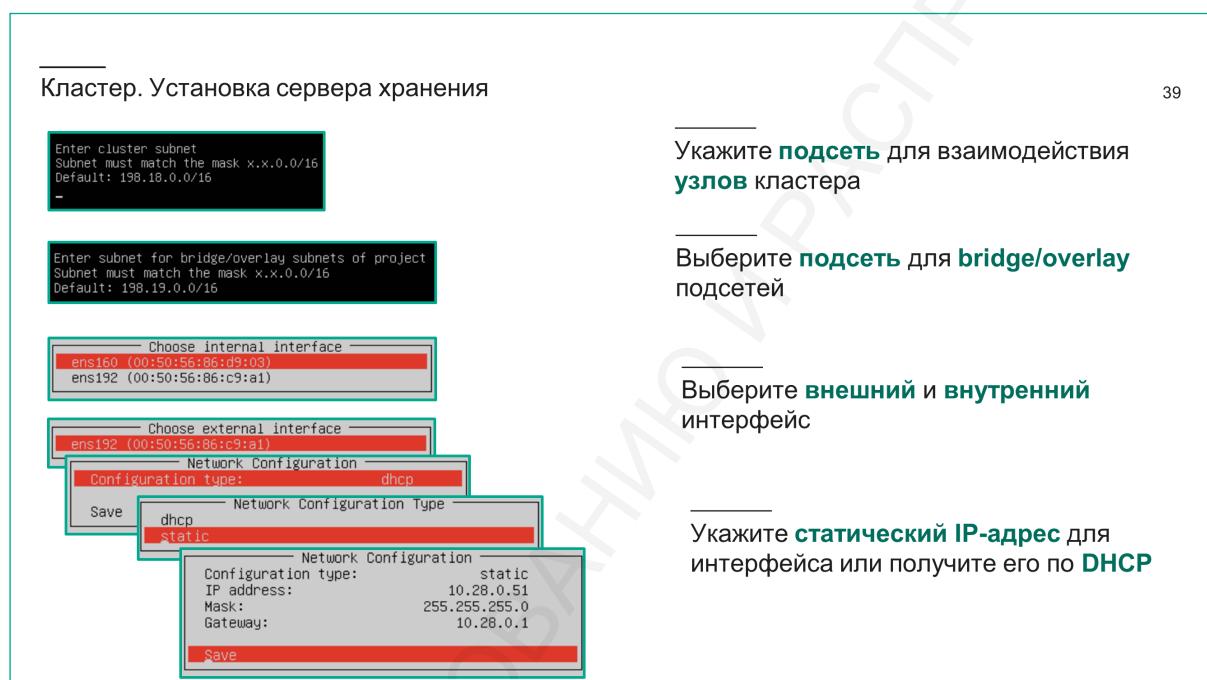
Подтвердите установку нажав **Yes**

После этого система спросит является ли наш узел первым узлом кластера или мы добавляем новый узел к существующему кластеру. Мы выберем первый вариант, так как ставим первый узел нового кластера.

Выберите диск из списка для установки операционной системы Центрального узла. Мастер

установки произведет разметку диска, установит операционную систему и программное обеспечение, необходимые для работы Центрального узла.

Для хранения данных рекомендуется использовать отдельный раздел, размещенный на производительном RAID-массиве. Подробности есть в онлайн-справке. Диски для данных выбираются позже в ходе установки. Также необходимо выбрать подсети для работы кластера и работы самого продукта, при этом будут автоматически выделены IP-адреса для взаимосвязи различных компонентов продукта. В случае, если значения по умолчанию не пересекаются с адресным пространством других решений вашей сети, то менять их не требуется.



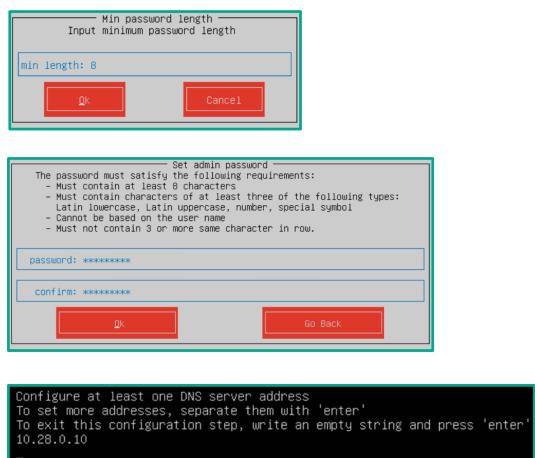
Выберите внутренний интерфейс, который будет использоваться для коммуникаций узлов кластера друг с другом, и внешний интерфейс для коммуникации с внешними системами.

Укажите подсеть для взаимодействия узлов кластера.

Для внешнего интерфейса можно получить сетевые настройки используя DHCP или задать их статически, для чего необходимо будет указать IP-адрес, маску подсети, шлюз.

Кластер. Установка сервера хранения

40



Укажите минимальную длину пароля

Задайте пароль учетной записи **admin**

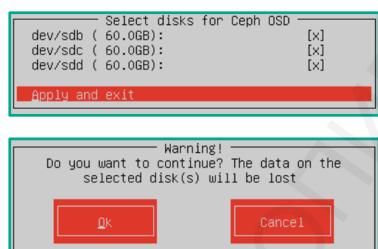
Укажите **DNS** сервер

Задайте пароль учетной записи admin, которая будет использоваться для конфигурации кластера и доступа к нему локально или через ssh. Укажите DNS-сервер.

Кластер. Установка сервера хранения

41

Configure NTP server addresses.
Input one or more NTP server addresses, confirming each with an "Enter" key press.
To finish this configuration step, input an empty string.
10.28.0.10



Укажите **NTP** сервер

Выберите **диски** для **Ceph-хранилища**

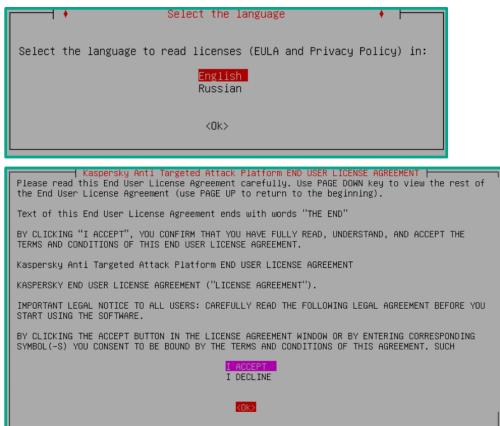
Подтвердите установку нажав **Ok**

Укажите NTP-сервер. Выберите диски для Серф-хранилища, необходимо выбрать как минимум 3 диска.

Кластер. Установка сервера обработки

42

Вставьте инсталляционный диск и загрузите с него сервер



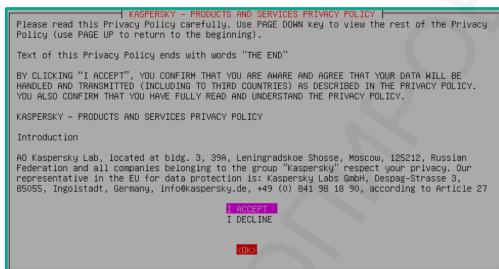
Выберите язык Лицензионного соглашения и Политики конфиденциальности

Прочтите Лицензионное соглашение и нажмите **I accept**

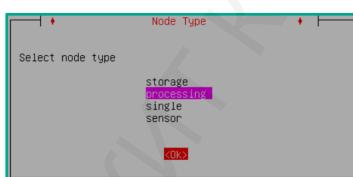
Чтобы начать установку сервера обработки кластера Центрального узла вставьте инсталляционный диск в сервер или подключите ISO-образ. Загрузите сервер с него и дождитесь автоматического начала установки. В ходе установки Центрального узла будет развернута операционная система с необходимыми пакетами.

Кластер. Установка сервера обработки

43



Прочтите Политику конфиденциальности и нажмите **I accept**



Выберите тип сервера **processing** и нажмите **Ok**

Прочтайте и примите политику конфиденциальности. Система предложит выбрать тип сервера, который планируется установить, первым всегда устанавливается сервер хранения.

Выберите Processing и нажмите Ok.

Кластер. Установка сервера обработки

44



Выберите диск для установки и нажмите **Ok**

Подтвердите установку нажав **Yes**

Укажите **подсеть** для взаимодействия **узлов** кластера

Выберите диск из списка для установки операционной системы Центрального узла. Мастер установки произведет разметку диска, установит операционную систему и программное обеспечение, необходимые для работы Центрального узла. Также необходимо выбрать подсети для работы кластера и работы самого продукта.

Кластер. Установка сервера обработки

45



Выберите **подсеть** для **bridge/overlay** подсетей

Выберите **внешний** и **внутренний** интерфейс

Укажите статический **IP-адрес** для интерфейса или получите его по **DHCP**

Выберите внутренний интерфейс, который будет использоваться для коммуникаций узлов кластера друг с другом, и внешний интерфейс для коммуникации с внешними системами.

Для внешнего интерфейса можно получить сетевые настройки используя DHCP или задать их статически, для чего необходимо будет указать IP-адрес, маску подсети, шлюз.

Укажите пароль учетной записи admin, которая будет использоваться для конфигурации кластера и доступа к нему локально или через ssh. Пароль должен совпадать с паролем, который ввели при установке первого узла хранения кластера.

Кластер. Установка сервера обработки

46



Активируйте возможность анализировать копию сетевого трафика, нажмите **Y**

Укажите, необходимо ли добавить возможность захвата трафика для этого узла, если есть необходимость получения трафика со SPAN-интерфейса, то выберите **Y**.

Кластер. Конфигурация

47

Server type	Status	Host name	RAM	CPU	Action
Storage	Connected	1av-node2-node dyn.xata	12.47%	6.15%	
Storage	Connected	1av-node3-node dyn.xata	11.25%	5.45%	
Processing	Connected	1av-node3-node dyn.xata	13.08%	18.83%	

Откройте в браузере страницу <https://<ip-address>:8443>. Учетная запись – **admin** (указав **Local Administrator**)

В разделе **Cluster** можно увидеть подключенные **узлы** и их статус

Откройте страницу <https://<ip-address>:8443>, чтобы настроить кластер:

<ip-address> — это адрес любого узла кластера, для входа используйте учетную

запись admin (указав Local Administrator) и пароль к ней, созданный во время установки первого узла хранения кластера.

В разделе Cluster можно увидеть подключенные узлы и их статус

Кластер. Конфигурация

48

В разделе **Server Configuration** необходимо указать:

- Количество агентов
- Объем почтового трафика
- Объем span трафика

Система укажет **предполагаемый размер** БД событий, хранилища. Эти значения можно **отредактировать**

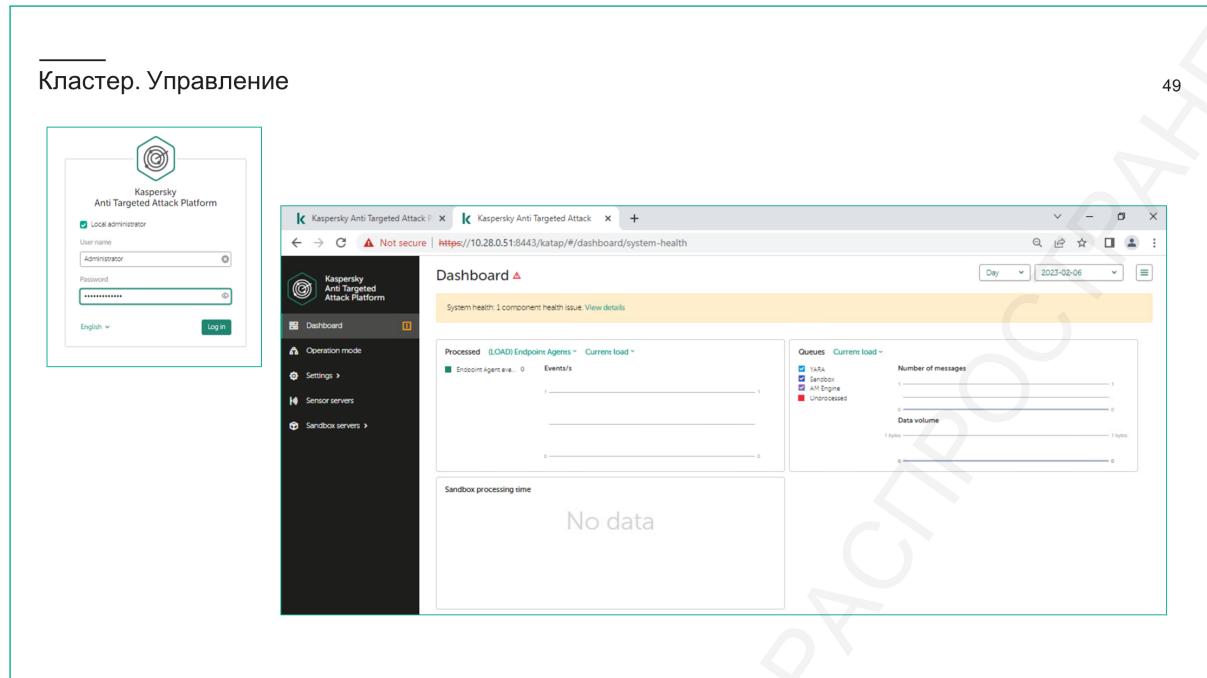
Нажмите Configure

После завершения конфигурации можно будет авторизоваться с учетной записью **Administrator** с паролем **Administrator** (указав **Local Administrator**)

В разделе Server Configuration необходимо указать планируемые значения:

- Количество Endpoint-агентов;
- Объем почтового трафика;
- Объем span трафика.

Система укажет предполагаемый размер БД событий, хранилища. Эти значения можно отредактировать. Нажмите Configure для старта конфигурации кластера. После завершения конфигурации можно будет войти с учетной записью Administrator с паролем Administrator (указав Local Administrator).



Теперь доступен интерфейс работы с Центральным узлом.

Установка Центрального узла на одном сервере.

Установка Центрального узла в виде одного сервера не сильно отличается от установки кластера, за исключением того, что все компоненты устанавливаются на один сервер.

Порядок установки:

- Чтобы начать установку сервера Центрального узла, вставьте инсталляционный диск в сервер или подключите ISO-образ. Загрузите сервер с него и дождитесь автоматического начала установки. В ходе установки Центрального узла будет развернута операционная система с необходимыми пакетами.
- Система предложит выбрать тип сервера, который планируется установить, если необходимо установить Центральный узел не в варианте кластера, то выберем тип 3.
- Выберите язык лицензионного соглашения. Установка выполняется только на английском языке, но лицензионное соглашение можно также прочитать на русском.
- Ознакомьтесь и нажмите `I accept`, если вы согласны с условиями. Администратор не может продолжить установку продукта без согласия с текстом лицензионного соглашения.
- Выберите диск из списка для установки продукта. Мастер установки произведет разметку диска, установит операционную систему и программное обеспечение, необходимые для работы Центрального узла.

- Подтвердите установку
- Необходимо выбрать подсети для работы кластера и работы самого продукта.
- Выберите внешний интерфейс. Сетевые настройки можно получить, используя DHCP или задать их статически, для чего необходимо будет указать IP-адрес, маску подсети, шлюз.
- Укажите пароль учетной записи admin, которая будет использоваться для конфигурации кластера и доступа к нему локально или через ssh.
- Укажите как минимум 1 DNS сервер.
- Укажите, необходимо ли добавить возможность захвата трафика для этого узла, если есть необходимость получения трафика со SPAN-интерфейса, то выберите у.
- Укажите как минимум 1 NTP сервер.
- Необходимо провести конфигурацию Центрального узла, для этого необходимо открыть в браузере страницу <https://<ip-address>:8443>

При этом <ip-address> — это адрес Центрального узла, для входа используйте учетную запись admin (указав Local Administrator) и пароль к ней, созданный во время установки первого узла хранения кластера.

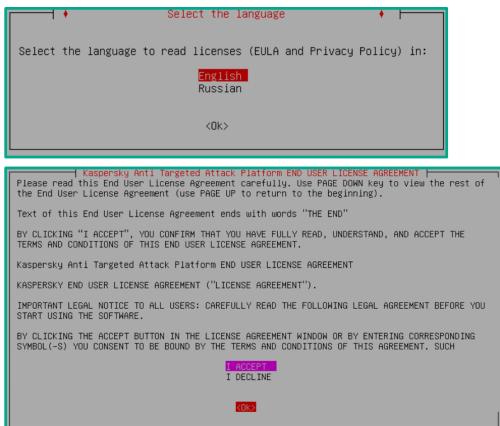
- В разделе Server Configuration необходимо указать планируемые значения:
 - Количество Endpoint-агентов;
 - Объем почтового трафика;
 - Объем span трафика.

Система укажет предполагаемый размер БД событий, хранилища. Эти значения можно отредактировать. Нажмите Configure для старта конфигурации Центрального узла. После завершения конфигурации можно будет войти с учетной записью Administrator с паролем Administrator (указав Local Administrator).

Сенсор. Установка

50

Вставьте инсталляционный диск и загрузите с него сервер



Выберите язык Лицензионного соглашения и Политики конфиденциальности

Прочтите Лицензионное соглашение и нажмите **I accept**

Сенсоры устанавливаются из того же образа, что и Центральные узлы.

Чтобы начать установку Сенсора:

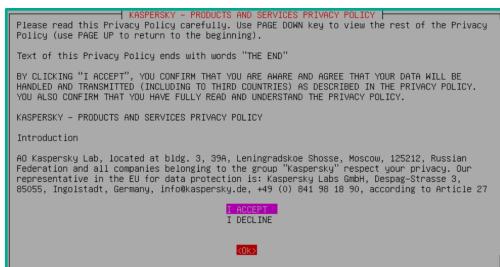
- Вставьте инсталляционный диск в сервер или подключите ISO-образ.
- Загрузите с него сервер.
- Дождитесь автоматического начала установки. В ходе установки Центрального узла будет развернута операционная система с необходимыми пакетами.

После этого необходимо подтвердить, что мы готовы прочитать лицензионное соглашение.

Выберите язык лицензионного соглашения. Установка выполняется только на английском языке, но лицензионное соглашение можно также прочитать на русском. Ознакомьтесь и нажмите **I accept**, если вы согласны с условиями. Администратор не может продолжить установку продукта без согласия с текстом лицензионного соглашения.

Сенсор. Установка

51



Прочтите Политику конфиденциальности и нажмите **I accept**



Выберите тип сервера **sensor** и нажмите **Ok**

Прочтайте и примите политику конфиденциальности. Система предложит выбрать тип сервера, который планируется установить, нам необходимо установить Сенсор, поэтому выберем Sensor.

Сенсор. Установка

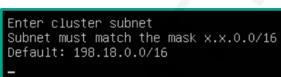
52



Выберите **диск** для установки и нажмите **Ok**



Подтвердите установку нажав **Yes**



Укажите **подсеть** для взаимодействия **узлов** кластера

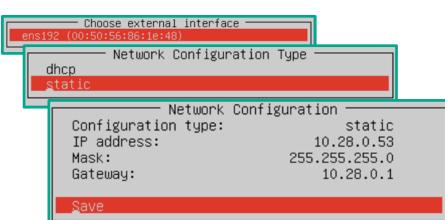
Выберите диск из списка для установки операционной системы Центрального узла. Мастер установки произведет разметку диска, установит операционную систему и программное обеспечение, необходимые для работы Центрального узла. Также необходимо выбрать подсети для работы кластера и работы самого продукта.

Сенсор. Установка

53

```
Enter subnet for bridge/overlay subnets of project
Subnet must match the mask x.x.0.0/16
Default: 198.19.0.0/16
```

Выберите подсеть для **bridge/overlay** подсетей



Выберите **внешний** интерфейс

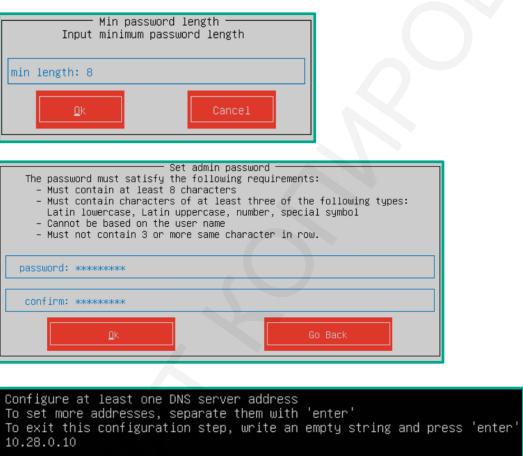
Укажите статический **IP-адрес** для интерфейса или получите его по **DHCP**

Выберите внутренний интерфейс, а так же внешний интерфейс для коммуникации с внешними системами.

Для внешнего интерфейса можно получить сетевые настройки используя DHCP или задать их статически, для чего необходимо будет указать IP-адрес, маску подсети, шлюз.

Сенсор. Установка

54



Укажите **минимальную** длину пароля

Задайте **пароль** учетной записи **admin**

Укажите **DNS** сервер

Укажите пароль учетной записи admin, которая будет использоваться для конфигурации кластера и доступа к нему локально или через ssh. Укажите DNS-сервер.

Сенсор. Установка

55

Configure NTP server addresses.
Input one or more NTP server addresses, confirming each with an "Enter" key press.
To finish this configuration step, input an empty string.
10.20.0.10

Укажите NTP сервер

Укажите NTP-сервер и дождитесь окончания установки.

3.2. Установка и настройка Sandbox

Дополнительные требования при установке Sandbox на гипервизоре

56



Оборудование

- Гипервизор: **VMware ESXi 6.7, 7.0**
- Процессор: **Intel Xeon 15 Core (HT)**
- Оперативная память: **32 ГБ**
- Место на диске: **300 ГБ**

Настройки виртуальной машины

- Разрешить **вложеннную виртуализацию**
- Зарезервировать всю **частоту процессора**
- Зарезервировать всю **оперативную память**
- Включить **High Latency Sensitivity**

Дополнительные требования при установке Sandbox на гипервизоре:

- Оборудование:

- Гипервизор: VMware ESXi 6.7, 7.0;

- Процессор: Intel Xeon 15 Core (HT);
 - Оперативная память: 32 ГБ;
 - Место на диске: 300 ГБ.
- Настройки виртуальной машины:
 - Разрешить вложенную виртуализацию;
 - Зарезервировать всю частоту процессора;
 - Зарезервировать всю оперативную память;
 - Включить High Latency Sensitivity.

Sandbox. Установка

57

Прочтайте и примите лицензионное соглашение и положение о защите данных

В случае отказа инсталлятор прекращает процесс установки

Чтобы начать установку Sandbox, вставьте инсталляционный диск в сервер или подключите ISO-образ. Загрузите с него машину. Выберите Install product to disk или дождитесь автоматического начала установки.

Sandbox Kaspersky Anti Targeted Attack/Kaspersky Endpoint Detection and Response устанавливается с операционной системой CentOS 7.9 и необходимыми программными пакетами. Репозитарии для установки обновлений в системе отключены. Предусмотрена установка только обновлений, выпускаемых Лабораторией Касперского.

Выберите язык лицензионного соглашения и положения о защите данных. Установка выполняется только на английском языке, но лицензионное соглашение и положение о защите данных можно также прочитать на русском. Ознакомьтесь и нажмите I accept, если вы согласны с их условиями.

Если администратор откажется принять любое из двух положений, установка будет прекращена.

Sandbox. Установка

58

The screenshot shows three steps of the CentOS installation:

- Select device:** A window titled "Select device" asks to select a disk drive for system installation. It lists "/dev/sda 171.8 GB Virtual disk" as suitable. Buttons include "Disk: /dev/sda 171.8 GB Virtual disk", "Cancel installation ...", and a red "Install" button.
- Install product on disk /dev/sda?**: A window asking if you want to erase all data on the disk and continue installation. It has "Install ..." and "Cancel" buttons.
- Hostname:** A window titled "Hostname" asking to specify the host name for the machine. The input field contains "sb.abc.lab". Buttons include "OK" and "Cancel".

Инсталлятор произведет **разметку диска** и **установит** операционную систему с необходимыми пакетами

После развертывания системы автоматически запускается консольный мастер настройки

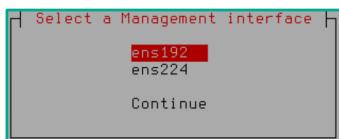
Выберите диск для установки. После выбора диска мастер установки произведет его разметку и установит операционную систему CentOS, в состав которой входят пакеты, необходимые для работы сервера Sandbox.

Если администратор прервёт процесс до того, как операционная система с программными пакетами установлена, то повторный запуск мастера установки начнется с первого шага — выбора языка EULA.

Выберите имя для сервера Sandbox. Это имя ни на что не влияет и нигде потом не используется. Для подключения Центрального узла к Sandbox вы будете использовать IP-адрес. Но сервера без имени быть не может, поэтому имя нужно задать.

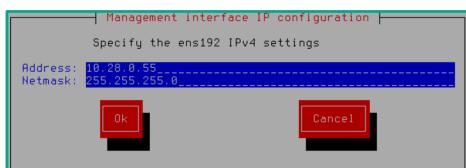
Sandbox. Установка

59



Sandbox использует два интерфейса:

- Management — для **управления сервером**
- Internet — для доступа в Internet **проверяемых объектов**



В ходе установки настройте управляющему интерфейсу статический **IP-адрес (DHCP не поддерживается)**

Internet-интерфейс настраивается позже в **веб-консоли** Sandbox

Выберите сетевой интерфейс, на который Sandbox будет принимать подключения администратора и подключения Центрального узла для передачи объектов на проверку и запроса результатов.

Это так называемый управляющий интерфейс. Укажите IP-адрес и маску подсети управляющего интерфейса.

Настройка параметров IP по протоколу DHCP не поддерживается.

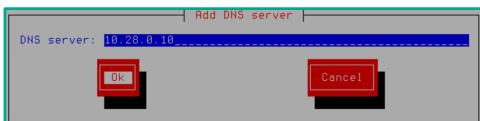
Для оптимальной работы серверу Sandbox нужен еще один интерфейс для выхода в интернет виртуальных машин, на которых анализируется поведение объектов. Этот интерфейс настраивается в веб-консоли Sandbox, а не во время установки.

Sandbox. Установка

60



DNS нужен для **загрузки обновлений** через интернет из инфраструктуры «Лаборатории Касперского»



Sandbox может обойтись **без DNS**, если настроен получать обновления от центрального узла

Виртуальные машины, на которых анализируются объекты, эти настройки **DNS не используют**, у них свои встроенные параметры DNS

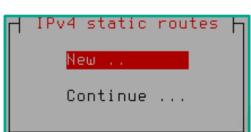
На следующем шаге добавьте DNS-сервер и укажите его IP-адрес. Если нужно, добавьте дополнительные DNS-сервера.

Настройки DNS на сервере Sandbox используются исключительно для загрузки обновлений.

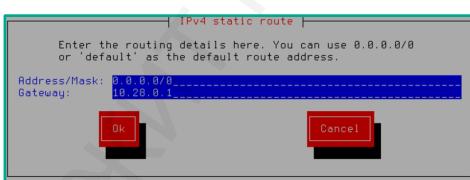
Внутри виртуальных машин, где анализируются потенциально опасные объекты, используются совсем другие настройки для разрешения имен, никак не связанные с инфраструктурой организации.

Sandbox. Установка

61



На этапе установки задайте **маршрут** по умолчанию через **управляющий интерфейс**



От этого маршрута требуется, чтобы сервер **Sandbox** мог обмениваться пакетами с **компьютером администратора**

Другие маршруты вы добавите позже в **веб-интерфейсе** Sandbox

Далее укажите маршрут, который позволит серверу Sandbox связываться с сетью, из которой

администратор будет подключаться к веб-интерфейсу Sandbox после установки.

Если компьютер администратора находится в той же подсети, что и Sandbox, то маршрут не имеет значения. Если же администратор будет подключаться из другой подсети, укажите адрес шлюза, который сможет передать пакеты от Sandbox в эту подсеть.

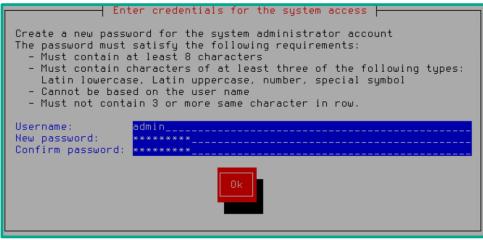
Пока вы настроили только управляющий интерфейс, поэтому укажите шлюз, который доступен с управляющего интерфейса. Позже в веб-консоли можно будет изменить настроенные маршруты.

Sandbox. Установка 62



Выберите **минимальную** длину пароля

- По умолчанию 12
- Не может быть меньше 8



Задайте **имя** и **пароль** администратора

Эта учетная запись является **одновременно**:

- Учетной записью операционной системы с правом локального и удаленного (SSH) входа в систему
- Учетной записью продукта с правом входа в веб-консоль Sandbox

Установите минимальную длину пароля для учетных записей Sandbox. По умолчанию предлагается 12 символов. Выбрать меньше 8 символов нельзя. Затем укажите имя и пароль администратора Sandbox. Пароль должен:

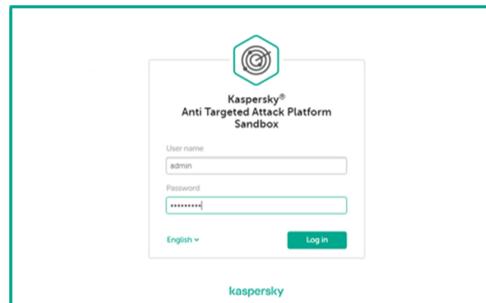
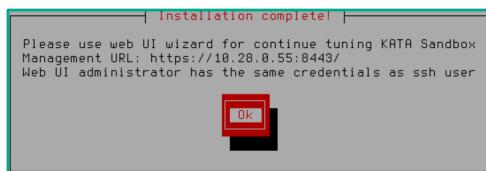
- Быть не короче заданного шагом ранее ограничения на число символов;
- Содержать как минимум 3 из 4 видов знаков: строчные буквы (a-z), заглавные буквы (A-Z), цифры, символы;
- Отличаться от имени пользователя.

Имя учетной записи администратора по умолчанию `admin`. Имя пользователя чувствительно к регистру.

Учетная запись администратора имеет право локального (или через SSH) входа в операционную систему, а также право входа в веб-консоль Sandbox. В сценариях использования Sandbox никакие другие учетные записи не нужны.

Sandbox. Установка

63



Продолжите настройку Sandbox в веб-интерфейсе по адресу:

- <https://<IP-адрес сервера Sandbox>:8443>

На этом установка и предварительная настройка сервера Sandbox закончена.

В мастере установки нет кнопки назад. Поэтому чтобы изменить ошибочно введенные параметры нужно либо начать установку заново, либо завершить установку как есть и перенастроить параметры через текстовую консоль или веб-интерфейс Sandbox.

При входе на Sandbox-сервер локально или через SSH от имени учетной записи администратора после завершения установки появляется консоль управления.

После установки Sandbox еще не полностью готов к работе. Его работа состоит в том, чтобы запускать поступающие для проверки файлы внутри виртуальных машин, протоколировать локальную и сетевую активность виртуальной машины, анализировать журналы активности и делать вывод об опасности файла.

Для этого на сервере Sandbox должны быть готовые для запуска виртуальные машины. Образы этих виртуальных машин поставляются в виде отдельных ISO-файлов, и их еще предстоит загрузить через веб-интерфейс Sandbox.

Также для оптимального обнаружения опасных объектов нужно настроить дополнительный интерфейс для выхода в интернет изнутри виртуальных машин. Это тоже делается в веб-интерфейсе.

Чтобы подключиться к веб-консоли Sandbox, введите в браузере <https://<IP-адрес-Sandbox>:8443>. По умолчанию Sandbox использует для защиты соединений самоподписанный сертификат, поэтому в браузере нужно будет подтвердить исключение безопасности. Сертификат сервера можно заменить в его настройках.

Для входа на сервер используйте учетную запись, которую вы создали во время установки. По умолчанию имя этой учетной записи admin. Все настройки Sandbox доступны в его веб-консоли. В ней администратор может:

- Изменить источник обновлений и загрузить обновления;
- Авторизовать подключения со стороны Центральных узлов;
- Изменить настройки сети;
- Установить пакеты исправлений;
- Настроить время;
- Загрузить образы виртуальных машин;
- Экспортировать настройки и журналы;
- Изменить пароль администратора;
- Перезагрузить или выключить сервер;
- Выбрать язык интерфейса.

Текстовая (ssh) консоль нужна преимущественно для устранения неполадок. Например, если вы неправильно задали параметры сети и не можете открыть веб-консоль, зайдите на сервер Sandbox локально и перенастройте сеть.

В веб-консоли Sandbox можно изменить настройки сети, заданные при установке:

- Имя сервера;
- Адреса DNS-серверов;
- IP-адрес управляющего интерфейса;
- Маршруты.

Настройка времени на Sandbox

64

Для корректной работы **время** между серверами КАТА должно быть **синхронизировано!**

Используйте NTP-серверы для автоматической синхронизации времени

Все соединения между серверами КАТА защищены TLS. Чтобы сервера КАТА доверяли сертификатам, которыми защищены TLS-соединения, важно, чтобы на всех серверах было согласованное время.

Настройка сети для выхода в интернет из виртуальных машин

65

При изменении параметров сети **Sandbox** автоматически **перезагружается**, чтобы применить настройки

Трафик виртуальных машин **полностью отделен** от трафика управления Sandbox и взаимодействия Sandbox с центральным узлом:

- отдельный шлюз
- отдельные вшитые настройки DNS (корневые серверы DNS интернета)

Рекомендуется иметь на Sandbox-сервере два интерфейса:

- Один для управления и получения данных от Центрального узла (интерфейс управления);
- Второй для выхода анализируемых образцов в интернет (Интернет-интерфейс).

Если интерфейс один, он будет использоваться для взаимодействия с Центральным узлом и управления, выхода в интернет у образцов не будет.

Рекомендуется предоставить доступ в интернет анализируемым образцам. Вредоносный объект сможет связаться с С&С-сервером или загрузить модуль для атаки. Дополнительные данные о функциональности объекта повысят уровень обнаружения и помогут во время расследования инцидента.

Запретите доступ в сеть организации с этого интерфейса для защиты сети и других КАТА-серверов от анализируемых объектов. Не сканируйте трафик этого интерфейса средствами защиты, включая КАТА.

Чтобы подключить виртуальные машины Sandbox к интернет-сети, в разделе Internet interface в веб-консоли выберите имя интернет-интерфейса и настройте для него:

- IP-адрес;
- Маску подсети;
- Адрес шлюза.

Заданный для Интернет-интерфейса адрес шлюза используется только внутри виртуальных машин. Операционная система сервера Sandbox использует маршруты (в том числе и маршрут по умолчанию), заданные в разделе Static routes.

Сначала в списке статических маршрутов есть только маршрут по умолчанию, заданный во время установки для управляющего интерфейса. Всего серверу Sandbox для работы нужны маршруты для следующих направлений:

- От Центрального узла;
- К источнику обновлений;
- К заданным DNS-серверам для разрешения имен серверов обновлений Лаборатории Касперского;
- В подсеть, откуда администратор подключается к веб-интерфейсу или к текстовому интерфейсу по SSH.

В зависимости от топологии сети все эти направления может охватывать один маршрут по умолчанию, или может потребоваться настроить несколько статических маршрутов.

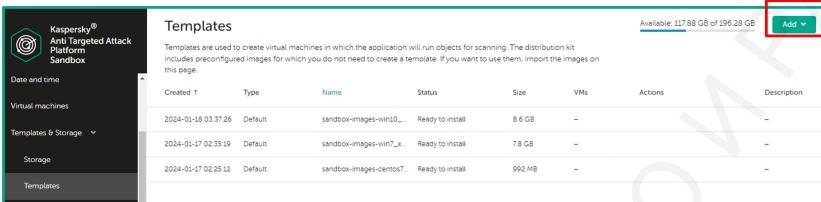
Маршруты из этого списка использует только операционная система Sandbox. Виртуальные машины, внутри которых запускаются потенциально вредоносные файлы, используют настройки Интернет-интерфейса, речь о котором шла выше.

Если у Sandbox есть Интернет-интерфейс, подключенный к изолированному каналу в Интернет, рекомендуется настраивать статические маршруты следующим образом:

- В настройках маршрута по умолчанию 0.0.0.0/0 указать имя Интернет-интерфейса и адрес шлюза Интернет-интерфейса;
- Маршруты до подсети, откуда подключаются администраторы, и до Центрального узла задать отдельно через управляющий интерфейс.

При такой конфигурации Sandbox будет устанавливать исходящие соединения только через изолированный Интернет-интерфейс.

Загрузка готовых образов гостевых виртуальных машин



Created	Type	Name	Status	Size	VMs	Actions	Description
2024-01-18 03:37:26	Default	sandbox-images-win10...	Ready to install	8.6 GB	-	-	
2024-01-17 02:35:19	Default	sandbox-images-win7_x...	Ready to install	7.8 GB	-	-	
2024-01-17 02:25:12	Default	sandbox-images-centos7...	Ready to install	992 MB	-	-	

66

Специальные образы
виртуальных машин
поставляются отдельно

Для работы технологии **Sandbox** необходимо **загрузить** только необходимые образы виртуальных машин из списка:

- Windows 7 64-bit
- Windows 10 64-bit
- Astra Linux 1.7
- CentOS 7.8

Список виртуальных машин должен соответствовать **одному из** наборов:

- Windows 7, Windows 10
- CentOS 7.8, Windows 7, Windows 10
- Astra Linux 1.7, Windows 7, Windows 10
- Пользовательские

Сервер Sandbox устанавливается без виртуальных машин. Для проверки объектов вы можете использовать свои (пользовательские) образы операционных систем и преднастроенные образы из комплекта поставки. Если вы используете пользовательские образы, вы можете установить в этих операционных системах любые приложения. Набор приложений для образов из комплекта поставки невозможно изменить. Преднастроенные образы виртуальных машин доступны в виде отдельных ISO-файлов. Их нужно:

- Загрузить на сервер Sandbox.
- Распаковать
- Активировать лицензии на программное обеспечение (опционально)
- Подготовить для работы и установить.

От администратора нужно только несколько раз нажать на кнопки в веб-консоли, и указать путь

к ISO-файлам. Все остальные действия выполняет сервер Sandbox автоматически.

Для загрузки на Sandbox-сервер доступны следующие образы гостевых виртуальных машин:

- Windows 7 64-bit SP1;
- Windows 10 64-bit;
- Astra Linux 1.7;
- CentOS 7.8.

На каждой из виртуальных машин установлены разнообразные версии офисных приложений, веб-браузеров и некоторые другие популярные приложения. Версии приложений в образах с разными операционными системами отличаются. Активация образов операционных систем Windows 7 (64-разрядная), Windows 10 (64-разрядная) и пакета приложений Microsoft Office выполняется с помощью файла `kata_images.py`. Файл входит в комплект поставки.

Чтобы загрузить на сервер образ виртуальной машины, используйте кнопку Add в разделе Templates & Storage | Templates в веб-интерфейсе Sandbox. Чтобы извлечь из образа файлы виртуальной машины и подготовить ее для работы, используйте кнопку Create VM. Прочитайте лицензионное соглашение для ПО Microsoft и Adobe для образов операционной системы Windows и нажмите I accept the terms, если вы согласны с его условиями. Лицензионное соглашение будет появляться при добавлении в систему каждого из образов. Для Astra Linux необходимо прочитать лицензионное соглашение по Astra Linux и нажать I accept the terms, если вы согласны с его условиями. При установке виртуальной машины с операционной системой CentOS 7.8 окно Лицензионное соглашение не открывается, так как для использования этой операционной системы не требуется принимать условия лицензионного соглашения.

Когда все образы добавлены, нажмите Install ready VMs в разделе Virtual machines | Preconfigured и дождитесь завершения подготовки среды. Это последний шаг в процессе установки Sandbox-сервера, после завершения которого сервер будет готов к работе.

В общей сложности загрузка образов на сервер и подготовка виртуальных машин к работе занимает несколько часов.

В ходе подготовки виртуальных машин к работе Sandbox создает в них пользовательские файлы и имитирует следы пользовательской активности, чтобы у документов были свежие метки создания и доступа к файлам. После этого Sandbox создает снэпшоты, из которых в последствии будут запускаться виртуальные машины для анализа.

Sandbox обновляет снэпшоты каждый день, чтобы внутри виртуальной машины всегда были

свежие следы работы пользователя, и чтобы вредоносный объект не мог легко отличить среду виртуальной машины от нормального компьютера в сети организации.

Виртуальные машины Sandbox настроены специальным образом, чтобы у вредоносных объектов не было простого способа понять, что они выполняются в специализированной для анализа песочнице, а не на реальной системе.

Для завершения установки нужно указать максимальное количество виртуальных машин, которое Sandbox сможет запускать одновременно для анализа файлов.

Значение по умолчанию для количества одновременно работающих ВМ равно 48.

Максимальное значение равно 200.

Каждый файл обычно проверяется на нескольких типах виртуальных машин. Кроме этого, Sandbox может собирать данные о поведении файла в двух режимах:

- Режиме полного журналирования, при котором Sandbox может получить более детальную картину для анализа, но не может следить за действиями объекта слишком долго по ресурсным соображениям;
- Режим быстрой проверки, при котором уровень детализации ниже, но эффективное время наблюдения за объектом больше.

На каких виртуальных машинах и в каком режиме проверять тот или иной объект зависит от типа объекта (документ, скрипт, исполняемый файл, URL) и того, откуда он поступил на проверку (трафик, почта, загружен аналитиком вручную). Логика принятия решений обновляется вместе с базами для обнаружения угроз.

Загрузка пользовательских образов гостевых виртуальных машин

67

Пользовательские образы могут быть **только из** определенного перечня:

- Windows XP SP3 or later
- Windows 7
- Windows 8.1 64-bit
- Windows 10 64-bit (version 1909 or earlier)

Created	Type	Name	Status	Size	VMs	Actions	Description
2023-05-10 13:39...	Custom	10_custom	Powered off	9.4 GB	10_custom_2	10	
2023-05-10 14:51...	Preconfigured	sandbox-images-win7_x64-1.0.28832	Ready to install	7.1 GB	-	-	
2023-05-10 14:17...	Preconfigured	sandbox-images-win10_x64-1.1.28833	Ready to install	8.1 GB	-	-	

Образы после установки
требуется настроить

Для загрузки пользовательских образов гостевых виртуальных машин для Sandbox-сервера поддерживается только строго определенные версии операционных систем:

- Windows XP SP3 or later
- Windows 7
- Windows 8.1 64-bit
- Windows 10 64-bit (version 1909 or earlier)

Загрузить пользовательские образы можно в виде iso файлов в разделе Templates & Storage | Storage. После загрузки образа создайте шаблон в разделе Templates & Storage | Templates, установите и активируйте операционную систему, потом настройте образ.

Чтобы установить пользовательское программное обеспечение (ПО), загрузите данное ПО в виде iso-файла в раздел Templates & Storage | Storage, далее подключите загруженный iso к шаблону виртуальной машины и установите ПО.

Создание гостевых виртуальных машин

Created	Type	Name	Status	Size	VMs	Actions	Description
2023-05-10 15:39	Custom	10_custom	Powered off	9.4 GB	10_custom_2	Create VM	10

Created	Name	Status	Actions	Description
2023-05-10 17:39:48	10_custom_2	Enabled		10

В разделе **Templates** нажмите **Create VM**

В разделе **Virtual machines | Custom** нажмите **Enable**

В разделе **Administration** необходимо указать **максимальное количество** одновременно **запущенных** гостевых виртуальных машин

Чтобы создать гостевые пользовательские виртуальные машины, перейдите в раздел **Templates & Storage | Templates** и нажмите **Create VM**.

В разделе **Virtual machines | Custom** нажмите **Enable**.

3.3. Активация, обновление, пользователи

Веб-интерфейс Центрального узла — это основной инструмент сотрудника службы безопасности для работы с Kaspersky Anti Targeted Attack/Kaspersky Endpoint Detection and Response. Для работы с решением через веб-интерфейс на компьютерах должен быть установлен один из следующих браузеров:

- Mozilla Firefox (Linux or Windows),
- Google Chrome (Linux or Windows),
- Edge (Windows),
- Safari (Mac).

Веб-интерфейс Kaspersky Anti Targeted Attack/Kaspersky Endpoint Detection and Response защищен от атак Cross-Site Request Forgery (CSRF) и работает, если только веб-браузер пользователя предоставляет Referer HTTP-запроса POST. Поэтому убедитесь, что ваш браузер не модифицирует заголовок Referer HTTP-запроса POST. Если соединение осуществляется через прокси-сервер, он тоже не должен модифицировать этот заголовок.

Чтобы открыть веб-консоль Центрального узла, введите в адресной строке браузера <https://<IP-адрес-Центрального-узла>:8443>

Чтобы войти на сервер используйте учетную запись Administrator. Учетная запись admin, под которой можно войти локально или через ssh имеет доступ только к странице конфигурации Центрального узла.

Когда вы входите в веб-консоль под учетной записью Administrator или admin, отмечайте флаг Local administrator над полем ввода имени.

Позже вы сможете создать дополнительные учетные записи администраторов и сотрудников службы безопасности. Для них флаг Local administrator отмечать не нужно.

Если веб-консоль открыта на любом разделе, кроме Dashboard, и пользователь не активен более 1 часа, то сессия завершается.

Доступные функции в зависимости от лицензии			
Функция	Без лицензии	Только KATA	Только KEDR
Обновление	Нет	Да	Да
KSN	Нет	Да	Да
Прием и обработка данных из трафика	Нет	Да	Нет
Прием и обработка телеметрии	Нет	Нет	Да
Поиск угроз, Задачи реагирования, Блокирование запуска, Хранилище	Нет	Нет	Да

Без лицензии Центральный узел не скачивает обновления баз, не отправляет запросы в Kaspersky Security Network и не применяет никакие технологии обнаружения. Многие разделы веб-интерфейса скрыты.

Лицензия устанавливается на Центральный узел через веб-интерфейс. К нему периодически подключаются Сенсоры, чтобы проверить наличие лицензии. Sandbox в Kaspersky Anti Targeted Attack/Kaspersky Endpoint Detection and Response принимает задачи проверки только от Центрального узла, поэтому если Центральный узел не активирован, то и Sandbox ничего не получает и не проверяет. Отдельно активировать лицензией Sandbox не нужно.

70

Активируйте центральный узел

Сенсоры используют информацию о лицензионном ключе **центрального узла**

Sandbox не требует активации, но принимает объекты для проверки **только от** центрального узла, который **должен быть активирован**

- Центральный узел поддерживает **только** активацию **ключом**
- Ключи **KATA** и **KEDR** устанавливаются **отдельно** и **независимо**
- Резервные ключи **не предусмотрены**

Чтобы добавить лицензию, войдите в веб-интерфейс от имени администратора и перейдите в раздел **Settings | License**. Нажмите **Import** в секции **KATA** или **KEDR** и укажите файл с лицензионным ключом. После загрузки файла в консоли отобразятся:

- Серийный номер,
- Дата активации,
- Дата окончания срока действия,
- Осталось дней.

Центральный узел Kaspersky Anti Targeted Attack/Kaspersky Endpoint Detection and Response не поддерживает коды активации.

Впоследствии вы сможете заменить или удалить файл ключа. Когда лицензия истекает, то перестают обновляться базы, и прекращается доступ в KSN.

Настройте обновление центрального узла

Обновление запускается автоматически раз в 30 мин

Доступные источники

- Kaspersky Lab secure update server
- Kaspersky Lab update server
- Custom server (только http) — для обновления в изолированных сетях используйте диод данных

Есть возможность выбрать один из трех источников получения обновлений:

- Kaspersky Lab secure update server;
- Kaspersky Lab update server;
- Custom server (только http) — для обновления в изолированных сетях используйте диод данных.

Роли пользователей		72
Роль	Функции	
Администратор	<ul style="list-style-type: none"> • Дашборды состояния и загрузки компонентов • Настройки сети, времени, обновления, подключения узлов, пользователей • Настройки подключения к источникам трафика локального сенсора 	
Администратор локальный (Administrator)	<ul style="list-style-type: none"> • Дашборды состояния и загрузки компонентов • Настройки сети, времени, обновления, подключения узлов, пользователей • Настройки подключения к источнику трафика локального сенсора • Управление распределенным режимом 	
Администратор локальный (admin)	<ul style="list-style-type: none"> • Необходим для первичной конфигурации 	
Старший сотрудник службы безопасности	<ul style="list-style-type: none"> • Нет доступа к виджетам и настройкам администратора • Доступ ко всем настройкам технологий обнаружения • Доступ ко всем инструментам реагирования • Обработка обнаружений, в том числе VIP 	
Сотрудник службы безопасности	<ul style="list-style-type: none"> • Настройки технологий обнаружения в режиме чтения • Нет доступа к инструментам реагирования • Доступ к обнаружениям и телеметрии, обработка обнаружений • Нет доступа к VIP-обнаружениям, и телеметрии VIP-узлов 	
Аудитор	<ul style="list-style-type: none"> • Все разделы интерфейса в режиме чтения 	

В Kaspersky Anti Targeted Attack/Kaspersky Endpoint Detection and Response предусмотрены учетные записи для локального входа на сервер для Центрального узла, Сенсора и Sandbox.

Эти учетные записи создаются во время установки серверов; на центральном узле их пароли можно изменить после установки в веб интерфейсе, нажав на имя учетной записи и выбрав Change Password. Пароль учетной записи сервера sandbox можно изменить в текстовой консоли в разделе Change the system administrative account password.

Роль администратора веб-интерфейса предназначена для настройки параметров работы серверов и поиска неисправностей. Она не предназначена для настройки параметров обнаружения атак и обработки обнаружений.

За настройку и мониторинг обнаружения атак отвечают сотрудники службы безопасности. Учетные записи для них можно создать в веб-консоли администратора Центрального узла в разделе Settings | Users.

Kaspersky Anti Targeted Attack/Kaspersky Endpoint Detection and Response поддерживает шесть ролей пользователей, которые обладают разными правами при работе в веб-интерфейсе:

- Администратор отвечает за настройку и сопровождение продукта, но не работает с событиями безопасности;
- Администратор локальный (Administrator) отвечает за настройку и сопровождение продукта, но не работает с событиями безопасности и обладает возможностью управления распределенным режимом;
- Администратор локальный (admin) - необходим для первичной конфигурации;
- Старший сотрудник службы безопасности имеет права настройки технологий обнаружения и обработки обнаружений, но не имеет доступа к настройкам, которые касаются взаимодействия серверов друг с другом или с инфраструктурой заказчика;
- (Обычный) Сотрудник службы безопасности не имеет права менять настройки технологий обнаружения и имеет доступ только к части обнаружений в веб-интерфейсе. Он не видит подробную информацию об обнаружениях, отмеченных VIP-статусом;
- Аудитор имеет доступ ко всем разделам интерфейса в режиме чтения

Создайте администраторов, аудиторов и сотрудников службы безопасности 73

Действия с учетными записями

- Создать
- Изменить пароль
- Отключить или включить

Нет действий

- Удалить
- Изменить роль

При создании учетной записи введите пароль, который должен:

- Отличаться от имени пользователя.
- Быть не короче указанного при установке количества знаков.
- Содержать как минимум 3 из 4 видов знаков: строчные буквы (a-z), заглавные буквы (A-Z), цифры, символы.

Один пользователь может обладать только одной ролью. Учетную запись нельзя удалить, нельзя изменить ее роль, но можно поменять пароль или заблокировать.

Администратор веб-интерфейса, созданный при установке Центрального узла, обладает такими же правами, что и администраторы, созданные через веб-консоль. Но в отличии от них, учетную запись изначального администратора не видно в списке пользователей веб-консоли, ее нельзя отключить, и при входе в веб-консоль от ее имени нужно отмечать параметр Local administrator.

Право менять параметры распределенного режима установки (повышать статус Центрального узла до первичного, подключать вторичные Центральные узлы к первичному) есть только у локального администратора веб-интерфейса (Administrator).

Аутентификация через Active Directory

74

The screenshot shows the 'Active Directory integration' configuration page. Under 'Integration', the 'Enabled' checkbox is checked. The 'Keytab file' field contains 'kata.keytab', which is being browsed from a local file system. The 'File name' field in the browser window also shows 'kata.keytab'. The 'File type' dropdown in the browser window is set to 'KEYTAB File'.

Что нужно для включения интеграции

- А-запись для имени центрального узла в зоне DNS домена Active Directory со ссылкой в зоне обратного разрешения имен
`Add-DnsServerResourceRecord -A -Name kata-cn -ZoneName abc.lab -IPv4Address 10.28.0.51 -CreatePtr`
- пользователь Active Directory, от имени которого центральный узел будет взаимодействовать с Active Directory
`New-ADUser -Name kata-ad -Enabled $true -AccountPassword $password`
- keytab-файл для взаимодействия со службой Kerberos
`ktpass -princ HTTP/kata-cn.abc.lab@ABC.LAB -mapuser kata-ad@ABC.LAB +rndpass -out kata.keytab`

Для того, чтобы не создавать дополнительные локальные учетные записи для сотрудников компании, работающих с KATA/KEDR, возможно подключить интеграцию с Active Directory.

Для интеграции необходимо:

- Создать DNS-запись.
- Создать keytab-файл.
- Настроить интеграцию в интерфейсе Центрального узла.

Добавьте доменные учетные записи и выберите им роли

75

The screenshot shows the 'Users' section with a list of existing users. A new user dialog box is open, titled 'New user'. It shows the 'Status' as 'Enabled', 'Authentication type' as 'Domain user account', 'Role' as 'Senior security officer', and 'User name' as 'administrator@abc.lab'. The note at the bottom of the dialog box states: 'The user name must be the same as the domain name. The domain name must follow the user-name@domain-format.'

Действия с учетными записями

- Создать
- Изменить пароль
- Отключить или включить

Нет действий

- Удалить
- Изменить роль

После интеграции с Active Directory будет возможно выбрать Domain user account при создании нового пользователя системы. И в данном случае будет работать SSO для входа доменного пользователя, авторизованного на рабочей станции в интерфейс KATA. Аутентификация по паролю для доменных учетных записей не поддерживается.

Аутентификация от имени доменной учетной записи 76

Условия

- открывать веб-консоль центрального узла по DNS-имени
- DNS-имя центрального узла (или имя домена целиком) должно быть в зоне **Local Intranet**

Чтобы воспользоваться SSO необходимо:

- Авторизоваться на рабочей станции под доменной учетной записью, которая добавлена в KATA.
- Открывать веб-консоль Центрального узла по DNS-имени.
- DNS-имя Центрального узла должно быть в зоне Local Intranet.

3.4. Подключение серверов друг к другу

Чтобы проверять объекты на сервере Sandbox, нужно подключить к нему Центральный узел. При подключении сервера обмениваются сертификатами, и администратор подтверждает аутентичность этих сертификатов. Впоследствии Центральный узел будет устанавливать с Sandbox защищенные соединения и оба сервера будут аутентифицировать друг друга с помощью сохраненных сертификатов.

Центральный узел можно подключить к нескольким серверам Sandbox. И к одному серверу Sandbox можно подключить несколько Центральных узлов. Подключить Центральный узел к серверу Sandbox можно прямо во время установки. Но можно сделать это и позже, например, в следующих ситуациях:

- Чтобы подключить Центральный узел к новому серверу Sandbox;
- Чтобы восстановить подключение после обновления версии или замены сертификата.

По умолчанию серверы KATA используют самоподписанные сертификаты, созданные во время установки. Их можно заменить на сертификаты заказчика, но все соединения между серверами придется авторизовать заново.

Если время на серверах Kaspersky Anti Targeted Attack/Kaspersky Endpoint Detection and Response отличается, это может помешать проверить достоверность сертификата, и вы не сможете подключить Центральный узел к Sandbox. Перед подключением серверов друг к другу обязательно проверьте, что на них настроено эквивалентное время в пересчете на UTC. Чтобы избежать проблем из-за расхождений в настройках времени, проще всего настроить на всех серверах один и тот же сервер NTP.

Отправьте запрос на подключение к Sandbox со стороны центрального узла 77

The screenshot shows two main windows from the Kaspersky Anti Targeted Attack Platform:

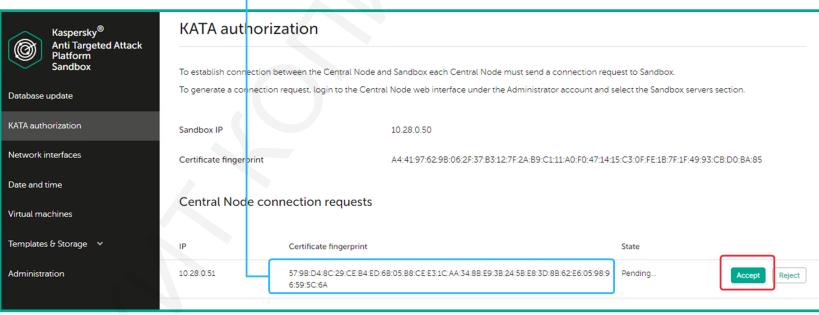
- Sandbox servers** window: Shows a table of servers with columns: IP and name, Authorization, Status, Certificate fingerprint, and Virtual machines. One row for '10.28.0.50' is selected, showing 'Request sent' and 'Enabled'. The 'Certificate fingerprint' column contains several entries, including 'A4:41:97:62:9B:06:2F:37:B3:12:7F:2...' and 'A8:7F:1F:49:93:C8:D0:8A:85'. A callout box points to this column with the text: 'Отпечатки сертификатов должны совпадать' (Certificate fingerprints must match).
- KATA authorization** window: Shows a 'Sandbox server connection' dialog. It has fields for 'IP' (10.28.0.50), 'Certificate fingerprint' (A4:41:97:62:9B:06:2F:37:B3:12:7F:2...), 'Name' (se), and a checked 'Enable' checkbox. A callout box points to the 'Certificate fingerprint' field with the same text: 'Отпечатки сертификатов должны совпадать'.

Запрос на подключение между Центральным узлом и Sandbox отправляется со стороны Центрального узла и подтверждается на стороне Sandbox. Чтобы отправить запрос:

- Войдите в веб-консоль Центрального узла от имени администратора. Учетные записи сотрудников службы безопасности не могут подключать Центральный узел к Sandbox.
- Выберите раздел **Sandbox servers** и нажмите кнопку **Add**.
- Введите IP-адрес сервера Sandbox и нажмите кнопку **Get certificate fingerprint**. Центральный узел выполнит TLS-соединение по указанному адресу и в случае успеха отобразит отпечаток сертификата сервера Sandbox.

- Сравните полученный отпечаток сертификата с действительным отпечатком сертификата на сервере Sandbox. Если вы не ошиблись в IP-адресе Sandbox, то отпечаток, который вы видите в консоли Центрального узла, должен совпадать с отпечатком сервера Sandbox в веб-консоли Sandbox в разделе KATA Authorization. Если отпечатки не совпадают, это может означать, что:
 - Вы ввели не тот IP-адрес, проверьте еще раз, что введенный IP-адрес на центральном узле совпадает с IP-адресом сервера Sandbox (его видно в веб-консоли Sandbox в разделе KATA Authorization).
 - Кто-то или что-то инспектирует защищенные соединения методом подмены сертификата (*man-in-the-middle*). Узнайте в службе ИТ, не используют ли они средства анализа защищенных соединений, и, если нет, поздравляем! Вы обнаружили следы атаки в сети.
- Если отпечатки сертификата Sandbox совпадают, отправьте запрос на подключение. Для этого в консоли Центрального узла задайте имя для сервера Sandbox и нажмите кнопку Add.

Центральный узел отправит запрос подключения на Sandbox, и вы должны увидеть этот запрос в веб-консоли Sandbox в разделе KATA Authorization. В запросе на стороне Sandbox будет отпечаток сертификата Центрального узла.

78

Отпечатки сертификатов в запросе и на центральном узле должны **совпадать**

Разные отпечатки могут указывать на **прослушивание трафика** или **проблемы в сети**

- Сравните отпечаток сертификата в запросе на стороне Sandbox с отпечатком сертификата Центрального узла в его собственной веб-консоли. Отпечаток сертификата Центрального узла в его веб-консоли можно найти в разделе Settings | General settings. Если отпечатки не совпадают, приступайте к расследованию инцидента: кто-то в сети

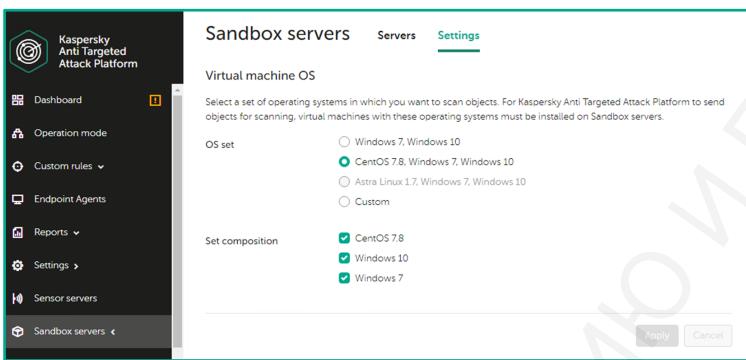
прослушивает защищенные соединения за счет подмены сертификата.

- Если отпечатки сертификата Центрального узла совпадают, примите запрос на стороне Sandbox. Для этого в строке запроса нажмите Accept и после этого еще нажмите кнопку Apply внизу страницы.

Статус подключения на стороне Центрального узла изменится на Approved. В будущем, если потребуется, авторизацию подключения можно отозвать как со стороны Sandbox, так и со стороны Центрального узла.

Выберите набор виртуальных машин для Sandbox

79



Необходимо выбрать **один из** наборов виртуальных машин

Вы можете выбрать набор операционных систем, на основе которого будут формироваться задачи на проверку объектов для компонента Sandbox:

- Windows 7 64-bit, Windows 10 64-bit;
- Windows 7 64-bit, Windows 10 64-bit, Astra Linux 1.7;
- Windows 7 64-bit, Windows 10 64-bit, CentOS 7.8.
- Пользовательские

Если вы выбрали набор "Пользовательские", в блоке параметров Состав набора установите флагки напротив операционных систем, которые вы хотите использовать в наборе.

Пользовательские операционные системы отображаются в списке, если виртуальные машины с этими операционными системами были установлены на сервере Sandbox. Преднастроенные операционные системы всегда отображаются в списке, но если виртуальные машины с этими операционными системами не развернуты, рядом с названием операционной системы отображается статус Неизвестно.

Пользовательские правила для sandbox

Если в разделе **Sandbox servers | Settings** выбран набор **Custom с пользовательским образом** ОС, то для использования этого образа в дополнение к стандартным необходимо создать **Пользовательские правила** sandbox

Если в разделе **Sandbox servers | Settings** выбран набор "Пользовательские", то для использования этого набора необходимо создать Пользовательские правила Sandbox-сервера.

Пользователи с ролями Старший сотрудник службы безопасности и Администратор могут создать правила для проверки файлов и URL-адресов. Если правила не добавлены, объекты не отправляются на проверку.

Чтобы добавить пользовательское правило Sandbox для проверки файлов перейдите в раздел **Пользовательские правила | Sandbox**.

Задайте значения следующих параметров:

- Состояние – состояние правила запрета. Установите флажок, если вы хотите включить правило
- Виртуальная машина – виртуальная машина, на которой будут проверяться файлы по этому правилу. Для выбора доступны только виртуальные машины с пользовательскими образами операционных систем.
- Хотя бы одно из значений: маску или категорию файла
- Размер файла – размер проверяемых файлов.

Загрузка обновлений на Sandbox

81

The screenshot shows the 'Database update' section of the Kaspersky Anti Targeted Attack Platform Sandbox interface. On the left, there is a sidebar with the following menu items: Database update, KATA authorization, Network interfaces, Date and time, and Virtual machines. The main area displays the 'Database update' configuration. It includes a table with 'Last update' (2024-01-31 02:01) and 'Failed'. A large red 'Update' button is prominently displayed. Below this, there is a dropdown menu labeled 'Update source' set to 'Custom server', and a text input field containing 'Central Node: 10.28.0.51'.

Доступные источники

- Kaspersky Lab secure update server
- Kaspersky Lab update server
- Custom server (только http)

Подключенные центральные узлы являются custom-источниками обновлений

Обновление запускается раз в 30 минут

Для загрузки обновлений, после подключения sandbox к центральному узлу, доступны следующие варианты:

- Kaspersky Lab secure update server;
- Kaspersky Lab update server;
- Custom server (только http).

Подключение Сенсора к центральному узлу.

Если в установке есть Сенсор, его нужно подключить к центральному узлу. Принцип подключения такой же, как и между центральном узлом и Sandbox.

Сенсор можно подключить только к одному центральному узлу, но к одному центральному узлу можно подключить несколько Сенсоров. Если в установке несколько Центральных узлов и несколько Сенсоров, разные Сенсоры могут быть подключены к разным Центральным узлам.

Поскольку подключение включает проверку подлинности сертификатов, проверьте на что Сенсоре и центральном узле настроено одинаковое время (в пересчете на UTC).

Чтобы подключить Сенсор к центральному узлу:

- Войдите на Сенсор (локально или через SSH) от имени учетной записи администратора admin.
- В текстовой консоли перейдите в раздел Program settings | Configure Central Node.

- Нажмите Change и укажите адрес Центрального узла.

Примите запрос подключения к центральному узлу со стороны сенсора 83

Проверьте совпадение отпечатков и **примите запрос** на подключение сенсора

Сенсор попытается установить защищенное соединение с указанным адресом. В случае успеха Сенсор отобразит отпечаток сертификата Центрального узла:

- Подтвердите подлинность сертификата Центрального узла. Проверьте, что отпечаток, который показывает Сенсор, совпадает с действительным отпечатком сертификата Центрального узла. Отпечаток сертификата Центрального узла смотрите в разделе Settings | General settings.
- Если отпечатки совпадают, в текстовой консоли Сенсора нажмите Ok. Это отправит на Центральный узел запрос подключения. Отправив запрос, Сенсор покажет окно с отпечатком своего сертификата.
- Сравните отпечаток сертификата Сенсора с отпечатком в запросе на стороне Центрального узла. Найдите запрос от Сенсора в веб-консоли администратора Центрального узла в разделе Sensor servers. Чтобы увидеть сертификат в запросе, кликните мышью по ссылке Certificate fingerprint в строке запроса.
- Если отпечатки совпадают, примите запрос на стороне Центрального узла. Для этого нажмите Accept в строке запроса.

Переведите центральный узел в статус первичного

84

Роль первичного или вторичного Центрального узла выбирается уже после установки. Сначала все Центральные узлы нужно установить, как обособленные.

Чтобы объединить несколько серверов в общую структуру в распределенном режиме:

- Сначала сделайте один Центральный узел первичным.
- Затем подключите к нему другие Центральные узлы, и они станут вторичными.

Чтобы сделать Центральный узел первичным:

- Войдите в веб-консоль от имени пользователя с ролью локального администратора.
- Перейдите в раздел Operation mode и измените режим на Distributed solution.
- Выберите для сервера роль Primary Central Node и введите имя компании.
- Примените выбранную роль и подтвердите выбор.

Преобразование занимает некоторое время. При этом сессия пользователя автоматически завершается и нужно будет заново войти в веб-консоль, когда преобразование закончится.

Новая роль Центрального узла отображается на экране входа в веб-консоль и в самой веб-консоли под боковым меню.

Назначение серверу роли PCN необратимо. После изменения роли сервера на PCN вы не сможете изменить роль этого сервера на SCN или отдельный сервер. Если вы захотите изменить роль этого сервера снова, вам потребуется переустановить программу.

Добавьте компании

Важно:

- Каждый центральный узел **должен относиться** к какой-то компании
- Компании предназначены для организации клиентов MSP
- Не-MSP клиенты могут назначить все центральные узлы **одной компании** или создать **псевдо компании** для территориальных или организационных подразделений

The screenshot shows the 'Operation mode' section of the Kaspersky Anti Targeted Attack Platform. On the left is a sidebar with various navigation options. The main area displays a table of tenants. One row for 'All Corp' is highlighted with a red border. A green arrow points from this row to a modal dialog titled 'Add tenant'. The 'Add tenant' dialog has a single input field 'Name' containing 'All Corp' and two buttons: 'Add' and 'Cancel'. Another green arrow points from the 'Add' button back to the main tenant list, indicating the addition of the new company.

Распределенная установка используется и в MSP-сценариях, когда поставщик услуг помогает нескольким заказчикам анализировать и обрабатывать угрозы. В этом случае первичный Центральный узел полностью контролируется поставщиком услуг, у каждого заказчика должен быть как минимум один Центральный узел, и Центральные узлы заказчиков подключены вторичными к центральному узлу поставщика услуг.

Для разграничения доступа в этом случае используются компании. Администратор первичного Центрального узла создает в веб-консоли объекты для всех подключенных компаний (включая саму компанию поставщика услуг). При подключении вторичного Центрального узла администратор на первичном узле указывает, к какой компании он относится. Подключить вторичный узел, не выбрав для него компанию, нельзя.

Если распределенный режим использует обычная компания просто потому, что у нее очень много компьютеров или большой объем трафика или из-за особенностей топологии сети, ей все равно нужно будет создать хотя бы одну компанию. Но при этом вполне можно будет указать, что все Центральные узлы относятся к этой единственной компании. Или даже и в этом случае можно создать фиктивные компании для подразделений внутри организации и использовать их для разграничения доступа.

The screenshot shows two main windows from the Kaspersky Anti Targeted Attack Platform:

- Top Window (Operation mode):** Shows the current mode as "Standalone solution". The server role is set to "Secondary Central Node". The PCN IP is listed as "10.28.0.51". A "Get certificate fingerprint" button is present. The PCN certificate fingerprint is displayed as: 93:25:AA:51:D3:E4:89:48:C8:44:39:43:05:E7:F4:1F:A5:04:F4:27:B2:F3:A2:A7:96:11:61:C9:F0:D2:87:01. A note says: "Attention! Changing the server role to SCN will reset:
List of user accounts
Assigning alerts to users". Buttons for "Send connection request" and "Cancel" are shown.
- Bottom Window (Operation mode):** Shows the current mode as "Distributed solution". The server role is listed as "Primary Central Node". The PCN certificate fingerprint is: 93:25:AA:51:D3:E4:89:48:C8:44:39:43:05:E7:F4:1F:A5:04:F4:27:B2:F3:A2:A7:96:11:61:C9:F0:D2:87:01. A "Add" button is visible. Below it is a table for "Tenants" with rows for "ABC corp" and "All corp". A "Servers pending authorization" table shows one entry for "IP 10.28.0.31 Server Kata Certificate fingerprint E4:36:61:31:2E:3B:DA:9E:94:P0:3B:DA:47:70:A0:7C:C8:6F:4B:02:7F:F0:12:44:0A:B0:C4:BE:19:2C:86:77 Status Authorization pending". Buttons for "Reject" and "Accept" are shown.
- Right Panel (Certificates):** A modal window titled "Сертификаты должны совпадать" (Certificates must match) asks: "Change the role of this server to SCN and connect to PCN 10.28.0.51?". It has "Yes" and "No" buttons.
- Bottom Right (Certificates):** A "Users" section shows a "Server certificate" with a copy icon, "Generate", "Import", and "Export" buttons. A "Certificates" section shows a certificate with the ID: E4:36:61:31:2E:3B:DA:9E:94:P0:3B:DA:47:70:A0:7C:C8:6F:4B:02:7F:F0:12:44:0A:B0:C4:BE:19:2C:86:77 and an expiration date of "2028-02-09".

Чтобы сделать обособленный Центральный узел вторичным, первичный Центральный узел уже должен быть готов.

Порядок действий следующий:

- Войдите в веб-консоль Центрального узла, который должен стать вторичным, от имени пользователя с ролью локального администратора.
- Перейдите в раздел Operation mode и измените режим на Distributed solution.
- Выберите для сервера роль Secondary Central Node.
- В поле PCN IP введите IP-адрес первичного Центрального узла и нажмите Get certificate fingerprint. На экране Operation mode появится отпечаток сертификата первичного Центрального узла.
- Сравните его с отпечатком сертификата первичного Центрального узла в консоли самого первичного Центрального узла (в разделе Operation mode).
- Если отпечатки совпадают, в консоли Центрального узла, который должен стать вторичным, нажмите кнопку Send connection request.

Примите запрос от вторичного центрального узла и назначьте ему компанию

87

The screenshot shows two separate instances of the 'Operation mode' section from the Kaspersky Anti Targeted Attack Platform. Both instances display a table of tenants and servers. In the first instance, there is a 'Servers pending authorization' section with one entry: IP 10.28.0.31, Server kata, Certificate fingerprint 6d:36:61:51:2E:2B:DA:9E:94:F0:35:D4:47:70:A0:7C:CB:6F:48:02:7F:FF:12:44:04:80:C4:BE:19:2C:86:77. Below this, there is a 'Accept' button. In the second instance, there is also a 'Servers pending authorization' section with the same entry and a 'Accept' button. To the right of these instances, a modal dialog box titled 'Accept connection request' is displayed. It contains the question 'Accept connection request from SCN 10.28.0.31?' and a dropdown menu labeled 'Tenant' with the option 'Alf corp'. At the bottom of the dialog are 'Accept' and 'Cancel' buttons.

- Перейдите в консоль первичного Центрального узла в раздел Operation mode и проверьте, что появился запрос подключения.
- Сравните отпечаток сертификата Центрального узла в запросе с отпечатком сертификата в консоли самого этого Центрального узла.
- Если отпечатки совпадают, в консоли первичного Центрального узла в строке запроса нажмите кнопку Accept.
- Выберите для вторичного Центрального узла компанию, к которой он относится, и еще раз нажмите Accept.

В сценарии, когда распределенная установка нужна внутри сети одного заказчика, всем вторичным Центральным узлам следует выбирать ту же компанию, которая была задана для первичного Центрального узла.

В сценариях MSP, когда одна компания управляет защитой нескольких других компаний, нужно создать компанию, к которой относится вторичный Центральный узел, перед тем как принимать запрос подключения от этого узла. Для этого служит кнопка Add в разделе Operation mode в консоли локального администратора первичного Центрального узла.

Все подключенные вторичные Центральные узлы отображаются в разделе Operation mode на первичном центральном узле, сгруппированные по компаниям. В аналогичном разделе на вторичном центральном узле отображается адрес первичного Центрального узла, к которому он подключен.

Преобразование Центрального узла во вторичный Центральный узел обратимо. Если

вторичный Центральный узел отключить от первичного кнопкой **Disconnect** в разделе **Operation mode**, такой вторичный Центральный узел снова станет обособленным.

Штатные ситуации, когда нужно отключать вторичный Центральный узел:

- Для обновления версии Центрального узла нужно отключить все вторичные Центральные узлы от первичного, выполнить обновление версии и подключить все назад.
- Чтобы изменить имя компании вторичного Центрального узла, нужно отключить вторичный Центральный узел и добавить заново, выбрав другое имя компании

Пользователи вторичного центрального узла поступают от первичного
88

New user
Edit account

New user
Edit account

В распределенном режиме активировать лицензией нужно только первичный Центральный узел. Вторичные узлы автоматически получают лицензии от первичного Центрального узла и показывают их в разделе **Settings | License**, удалить или заменить лицензию на вторичном Центральном узле можно.

Управление пользователями доступно только на первичном Центральном узле. Вторичные Центральные узлы получают список пользователей от первичного Центрального узла. Любые пользователи веб-консоли, которые были на Центральном узле до того, как он стал вторичным, удаляются, за исключением учетной записи локального администратора.

В настройках учетных записей на первичном Центральном узле, по сравнению с обособленным режимом у учетных записей сотрудников службы безопасности появляются настройки доступа к компаниям и вторичным Центральным узлам. Учетные записи администраторов имеют право доступа ко всем Центральным узлам в распределенной установке.

В распределенной установке основной консолью управления является консоль первичного Центрального узла. Все пользователи, заданные в настройках первичного Центрального узла, имеют право входа в веб-консоль первичного Центрального узла.

В сценарии MSP предполагается, что сотрудники заказчика обрабатывают обнаружения своей компании (или наблюдают за прогрессом обработки) тоже из веб-консоли первичного Центрального узла. Чтобы они видели обнаружения только своей компании, в свойствах учетной записи можно выбрать, к каким компаниям она имеет доступ.

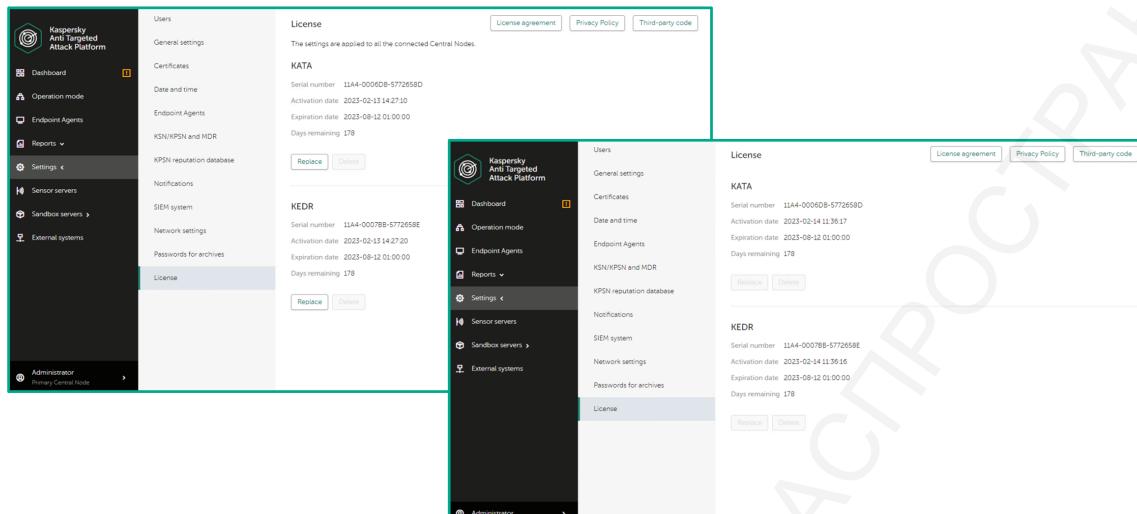
Разграничение доступа по компаниям есть только для учетных записей сотрудников службы безопасности. Администратор, созданный в веб-консоли первичного Центрального узла, имеет право доступа в локальную веб-консоль любого вторичного сервера любой компании. Сделать общего администратора только для вторичных узлов одной компании нельзя, но у этих вторичных узлов всегда есть учетная запись локального администратора, через которую сотрудники заказчика могут менять любые системные настройки.

По умолчанию учетные записи сотрудников службы безопасности имеют право входа только в веб-консоль первичного Центрального узла, где они видят сводную информацию от всех вторичных серверов своей компании. В настройках учетной записи есть флаг SCN web interface, которым можно разрешить вход в веб-консоль вторичного Центрального узла. Это может быть нужно для изменения индивидуальных настроек сервера, таких как, например, список YARA-правил или список пользовательских IDS-правил, которые нужно загружать на каждый сервер отдельно.

Если распределенный режим используется в рамках одной компании, распределение доступа по компаниям не востребовано и все учетные записи сотрудников службы безопасности имеют доступ ко всем обнаружениям через консоль первичного Центрального узла.

Лицензионные ключи вторичного центрального узла поступают от первичного

89



Глава 4. Эксплуатация КАТА

4.1. Подключение к источникам трафика

Чтобы передавать данные для анализа в Kaspersky Anti Targeted Attack Platform, на стороне инфраструктуры необходимо настроить сетевые устройства, прокси-серверы, почтовые серверы, почтовые шлюзы.

Один Сенсор из состава КАТА можно использовать для одного, нескольких или всех видов интеграции. Если требуется обрабатывать несколько видов трафика, но из-за особенностей инфраструктуры это нельзя сделать одним Сенсором, тогда используются два и более Сенсоров. В роли одного из Сенсоров может выступать сам Центральный узел.

Источником почтового трафика для Центрального узла может также быть Kaspersky Secure Mail Gateway/Kaspersky Security for Linux Mail Server. А источником веб-трафика может быть Kaspersky Web Traffic Security.



Направить копию сетевого трафика возможно, используя технологию SPAN или ERSPAN в зависимости от архитектурных особенностей сети заказчика.

Инициализируйте интерфейс для захвата трафика на центральном узле 91

Адрес для этого интерфейса настраивать не обязательно

Если не включили возможность анализа сетевого трафика во время установки, то выполните команду **kata-enable-span**

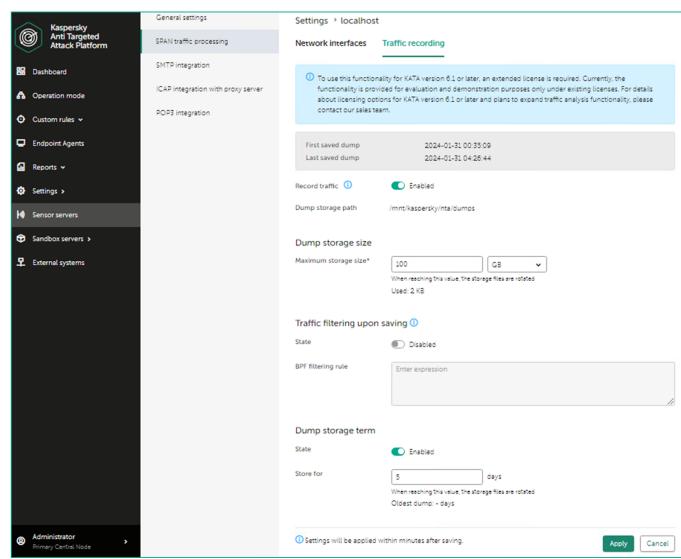
Для приема зеркальированного трафика рекомендуется использовать выделенный интерфейс или несколько: для приема трафика от разных источников.

Зеркалирование — это дублирование пакетов одного или нескольких портов сетевого коммутатора на отдельный интерфейс, к которому подключен анализатор. Применяется для мониторинга трафика в целях безопасности или оценки производительности сетевого оборудования. Для получения зеркальированного трафика один из сетевых интерфейсов Сенсора переводится в «неразборчивый» режим и подключается к зеркальному порту коммутатора. В обычном режиме Ethernet-интерфейс фильтрует пакеты канального уровня. Если MAC-адрес назначения в заголовке принятого пакета не совпадает с MAC-адресом сетевого интерфейса и не является широковещательным, то пакет отбрасывается. При подключении к зеркальному порту сетевая карта будет получать огромное количество пакетов, предназначенных другим узлам сети. Чтобы пакеты не были отброшены, интерфейс переводят в неразборчивый режим, в результате чего он начинает принимать все пакеты.

Чтобы активировать прием трафика на центральном узле, необходимо перейти в раздел Sensor servers, открыть свойства внутреннего Сенсора Центрального узла — localhost и открыть раздел SPAN traffic processing. Для нужного интерфейса включить SPAN traffic scanning и выбрать Capture thread.

Запись трафика на центральном узле

92

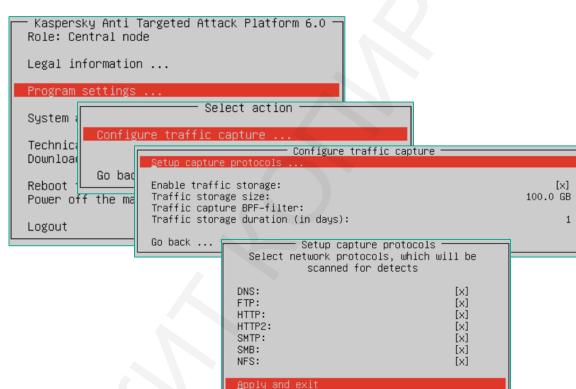


Вы можете управлять тем, как хранится полученный трафик и ограничивать хранения PCAP-файлов:

- По объему
- По правилам фильтрации
- По времени хранения

Запись трафика на центральном узле

93



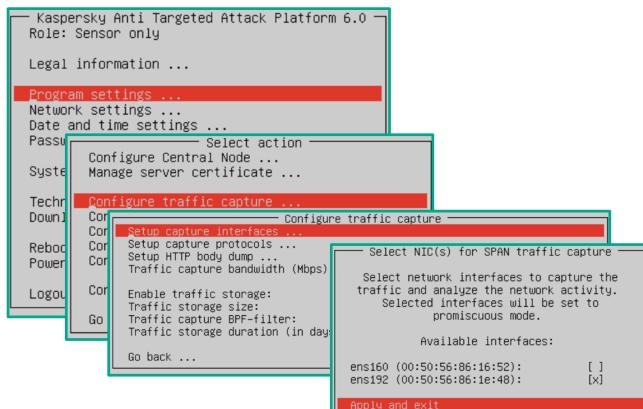
Существует возможность **включить** или **отключить** разбор следующих протоколов в копии сетевого трафика:

- DNS
- FTP
- HTTP
- HTTP2
- SMTP
- SMB
- NFS

Дополнительно можно включить или выключить разбор нескольких популярных протоколов в копии сетевого трафика.

Инициализируйте интерфейс для захвата трафика на сенсоре

94



Адрес для этого интерфейса настраивать **не обязательно**

Чтобы активировать прием трафика на Сенсоре, необходимо в текстовой консоли Сенсора выбрать раздел **Program settings | Configure traffic capture | Setup capture interfaces**. Затем выберите интерфейсы для захвата трафика клавишей ENTER.

Если Сенсор (или Центральный узел) является виртуальной машиной, неразборчивый режим нужно разрешить в настройках виртуального коммутатора, к которому подключен интерфейс для приема зеркалированного трафика.

После того, как вы настроили Сенсор или Центральный узел принимать трафик для анализа, направьте необходимый трафик на соответствующие интерфейсы серверов Kaspersky Anti Targeted Attack настройками сетевого оборудования.

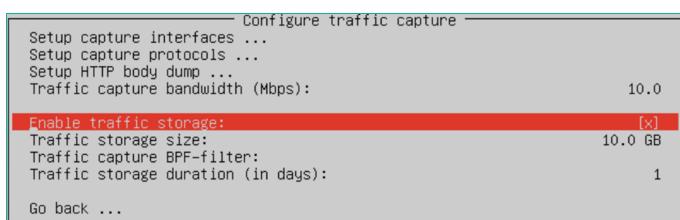
Включите зеркалирование трафика на сетевом коммутаторе, через который трафик идет в организацию и из организации. Платформа КАТА не предназначена для проверки внутрисетевого трафика, поэтому Сенсоры не подключают к коммутаторам уровня доступа к сети.

Подключите интерфейс Сенсора, переведенный в неразборчивый режим, к зеркальному порту коммутатора. На Сенсоре можно активировать несколько таких интерфейсов, чтобы получать трафик с нескольких портов одного или нескольких коммутаторов.

Поддерживается получение зеркалированного трафика по технологиям SPAN, RSPAN и ERSPAN, а также необработанной копии трафика через TAP-устройство.

Запись трафика на сенсоре

95



Возможность запись трафика в **PCAP-файлы** можно ограничить:

- по максимальному объему
- по фильтру
- по времени хранения

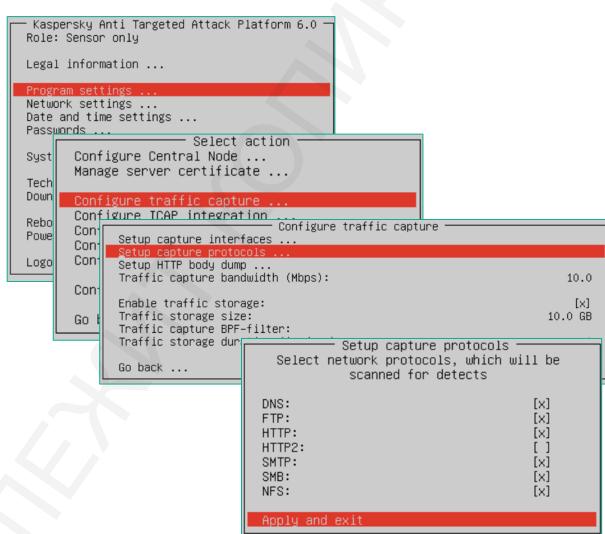
На Сенсоре так же можно управлять тем, как хранится полученный трафик:

- По объему
- По правилам фильтрации
- По времени хранения

В случае Сенсора настройку требуется провести в локальной консоли управления.

Запись трафика на сенсоре

96

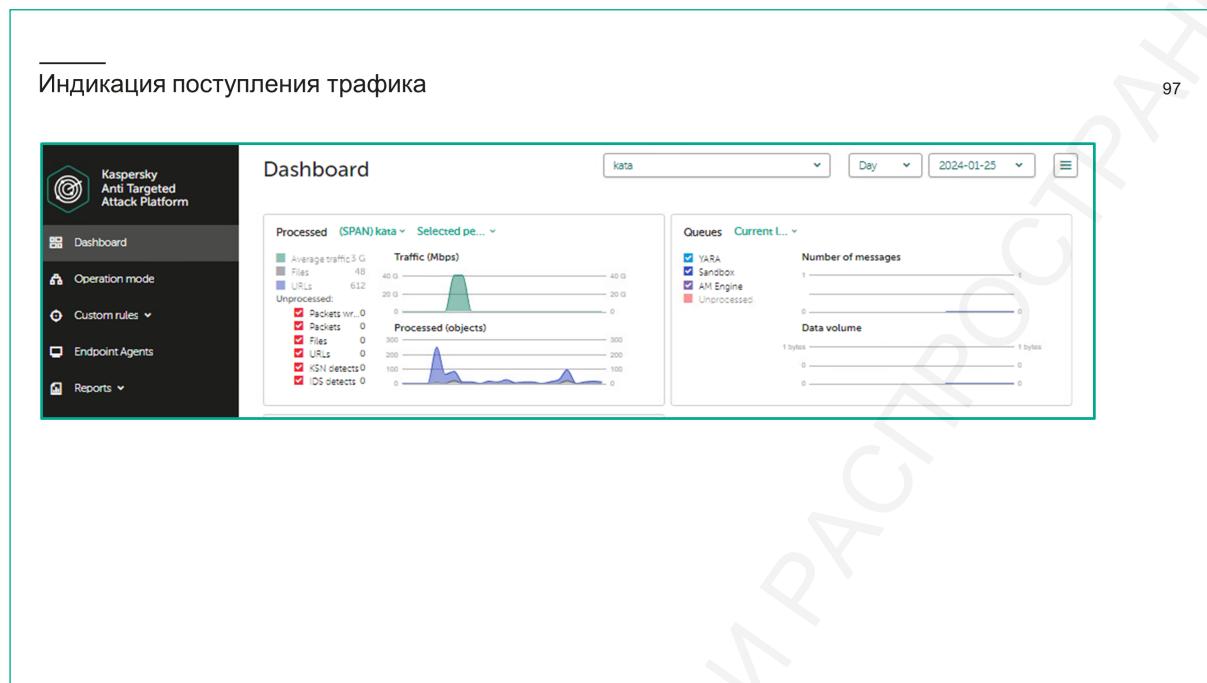


Существует возможность **включить** или **отключить** разбор следующих протоколов в копии сетевого трафика:

- DNS
- FTP
- HTTP
- HTTP2
- SMTP
- SMB
- NFS

Также можно включить или выключить разбор нескольких популярных протоколов в копии

сетевого трафика.



Понять, что Kaspersky Anti Targeted Attack получает зеркалированный трафик, можно из веб-консоли администратора.

В первую очередь стоит проверить, что захват трафика включен. Это можно увидеть в разделе Sensor servers, где отображаются как выделенные Сенсоры, так и Сенсор, встроенный в Центральный узел. Отметка в графе SPAN означает, что на Сенсоре выбран интерфейс для захвата трафика.

Чтобы проверить, что не просто включен захват трафика, а трафик действительно поступает на проверку, нужно смотреть на панели Dashboard. Если в панели Processed выбрать источником SPAN-интерфейс, она будет показывать объем трафика, поступающего через SPAN-интерфейс. Каждый SPAN-интерфейс является отдельным источником.

Чтобы дополнительно удостовериться, что Kaspersky Anti Targeted Attack анализирует трафик и извлекает объекты для проверки, нужно смотреть на показатели URLs и Files на панели Processed.

Альтернативно можно загрузить по протоколу HTTP или отправить по почте тестовый файл EICAR и проверить, что в консоли сотрудника службы безопасности появилось обнаружение от источника SPAN.

Обращайте внимание на сообщения об ошибках в верхней части экрана Dashboard. Среди них могут быть ошибки, связанные с обработкой зеркалированного трафика: например, сообщения о потере пакетов. В этом случае проверьте загрузку ресурсов Сенсора (или Центрального узла),

и перепроверьте, что аппаратная конфигурация Сенсора (Центрального узла) соответствует объему поступающего трафика.

Настройка pcap-фильтра для сырого трафика
98

Kaspersky Anti Targeted Attack Platform 6.0
Role: Central node

- Legal information ...
- Program settings ...
- System administration ...
- Technical Support Mode ...
- Download system logs ...
- Reboot the machine
- Power off the machine
- Logout

```

        },
        "ftp_data_expired_timeout": "PT60S",
        "ftp_data_supposed_max_size_bytes": 10485760,
        "iface_groups": [
            {
                "core_id": null,
                "ifaces": [
                    "ens192"
                ]
            }
        ],
        "memcap": {
            "flow": "256mb",
            "reassembly": "8192mb",
            "stream": "1024mb"
        },
        "pcap_filter": "not host 10.28.2.111",
        "pcap_snaplen": 1600,
        "pcap_timeout": 10,
        "storage_settings": {
            "bpf_filter": null,
            "directory": "/mnt/kaspersky/nta/dumps",
            "size": 1024
        }
    }
-- INSERT --
        342,46      96%

```

Вызвести настройки

```
sudo console-settings-updater get /kata/configuration/product/preprocessor_span | python3 -m json.tool > /tmp/1
```

Загрузить измененные настройки

```
sudo console-settings-updater set /kata/configuration/product/preprocessor_span @/tmp/1
```

Иногда есть ситуации, когда необходимо исключить проверку некоторого трафика и для этого можно воспользоваться pcap-фильтром. Сохраните настройки в файл для дальнейшего редактирования:

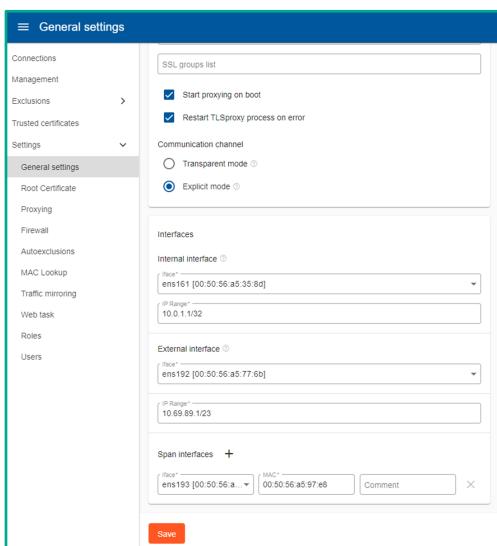
```
sudo console-settings-updater get /kata/configuration/product/preprocessor_span | python3 -m json.tool > /tmp/1
```

Отредактируйте полученный файл в разделе **pcap_filter** текстовым редактором и загрузите его обратно командой:

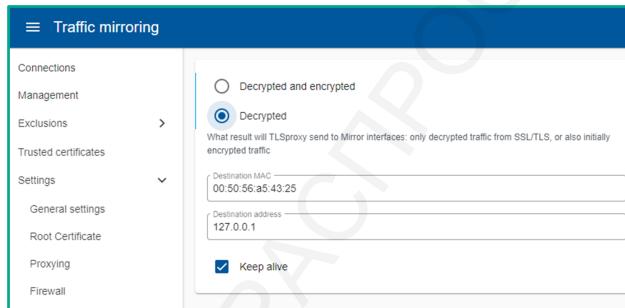
```
sudo console-settings-updater set /kata/configuration/product/preprocessor_span @/tmp/1
```

Разбор копии шифрованного трафика

99



Копия шифрованного трафика может быть проанализирована при интеграции с **ArtX TLSproxy 1.9.1**

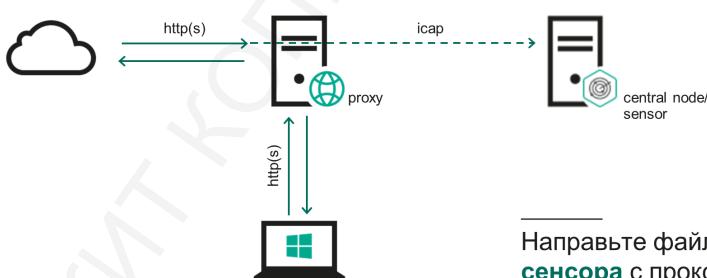


В релизе версии 6.0 появилась возможность интегрироваться с внешними приложениями для раскрытия зашифрованного SSL/TLS-трафика. На текущий момент поддерживается **ArtX TLSproxy 1.9.1**.

Интеграция осуществляется на стороне прокси-сервера. Требуется настроить зеркалирование трафика с указанием отправлять на SPAN-интерфейс решения дешифрованную копию сетевого трафика.

Проверка веб-трафика за счет интеграции по протоколу ICAP

100



Направьте файлы на проверку на **интерфейс сенсора** с прокси-сервера

Internet Content Adaptation Protocol (ICAP) разрабатывался для обеспечения антивирусной защиты и контентной фильтрации при выходе в интернет через прокси-сервер, но со временем

получил более широкое распространение. Сейчас он применяется для обнаружения вредоносного содержимого в системах хранения данных, перехвата трафика при интеграции с системами защиты от утечки данных и т.д.

Киберпреступники используют защищенный канал, чтобы обойти межсетевые экраны и прокси-серверы с антивирусной защитой. После установки соединения с конечным узлом внутри сети отдается команда на загрузку вредоносного объекта или копирование конфиденциальной информации. Проверка таких соединений реализуется на стороне прокси-сервера тоже по методу «человек посередине».

Проверка защищенных соединений работает следующим образом. Когда пользователь набирает в веб-браузере имя сайта, начинающееся с HTTPS, то корпоративный прокси-сервер принимает соединение от клиента и устанавливает соединение с веб-сервером, начиная TLS-сессию. Прокси-сервер получает от веб-сервера сертификат для создания зашифрованного канала. Но вместо того, чтобы передать этот сертификат клиенту, прокси-сервер генерирует свой сертификат, который передается клиенту для создания канала. Таким образом, после установки безопасного соединения все данные между веб-сервером и конечным пользователем расшифровываются на прокси-сервере для инспекции содержимого, после чего снова зашифровываются с использованием уже другого ключа и передаются клиенту. Главное, чтобы такой механизм поддерживался на стороне прокси-сервера, а клиенты доверяли его сертификату. Если механизм поддерживается, то извлеченные объекты будут передаваться Сенсору для анализа.

Также доступна интеграция с прокси-сервером по протоколу ICAP с возможностью блокировки вредоносного контента.

Этот способ интеграции позволяет вам предотвратить попадание вредоносных объектов в локальную сеть организации и ограничить переход на вредоносные или фишинговые веб-сайты пользователям хоста. Kaspersky Anti Targeted Attack Platform выступает в роли ICAP-сервера, а ваш прокси-сервер – в роли ICAP-клиента. В процессе работы прокси-сервер передает запросы по протоколу ICAP на ICAP-сервер. ICAP-сервер выполняет проверку и возвращает результат на прокси-сервер. В случае обнаружения угроз пользователю хоста отобразится HTML-страница оповещения.

Включите ICAP-сервер на центральном узле

101

Sensor servers

IP/Name	Type	Certificate fingerprint	SPAN	SMTP	ICAP	POPS
localhost	Central Node	-	✓	✗	✗	✗

Настройки ICAP-клиента

```
# ICAP settings
icap_enable on
icap_send_client_ip on
icap_service kata_sensor respmod_pcrecache 0 icap://10.28.0.51:1344/av/respmod
icap_service kata_sensor regmod_pcrecache 0 icap://10.28.0.51:1344/av/regmod
adaptation_access kata_sensor allow all
```

General settings

ICAP integration with proxy server

Real-time scanning

If this feature is enabled, Kaspersky Anti Targeted Attack Platform sends information about scanned objects to the ICAP client in real time. This prevents downloading malicious objects and clicking untrusted links. For details about ICAP integration with proxy server, see [Online Help](#).

State:

- Disabled
- Enabled, standard ICAP traffic scanning
- Enabled, advanced ICAP traffic scanning

Apply Cancel

При проверке **ICAP-трафика** есть возможность активировать **проверку** в режиме реального времени:

- Включено, стандартная проверка трафика ICAP
- Включено, усиленная проверка трафика ICAP

Все интерфейсы, не задействованные для приема зеркалированного трафика, смогут принимать объекты от прокси-сервера по протоколу ICAP.

Интеграция с прокси-сервером по протоколу ICAP уместна, например, чтобы проверять файлы и ссылки в защищенном трафике HTTPS. Сенсоры Kaspersky Anti Targeted Attack сами по себе не могут анализировать защищенный протокол HTTPS в зеркалированном трафике. Но организация может настроить свой прокси-сервер расшифровывать HTTPS и передавать файлы из трафика на проверку в Kaspersky Anti Targeted Attack по протоколу ICAP.

В общем случае Сенсор может принимать файлы для проверки по протоколу ICAP не только от прокси-сервера, а от любой системы, которая поддерживает ICAP. Например, многие системы хранения данных могут передавать файлы, к которым происходит обращение, на проверку по протоколу ICAP. Но нужно учитывать дополнительную нагрузку, которую это создаст на серверы Kaspersky Anti Targeted Attack. Рекомендации по лицензированию и аппаратным требованиям для такого сценария могут дать специалисты Лаборатории Касперского.

Чтобы Kaspersky Anti Targeted Attack проверяла объекты, проходящие через прокси-сервер, на прокси-сервере активируйте ICAP и укажите адрес ICAP-сервера, на который будут отправляться объекты.

Если проверка ICAP-трафика в режиме реального времени включена, Kaspersky Anti Targeted Attack Platform передает информацию о проверенных объектах ICAP-клиенту в режиме реального времени. Это позволяет предотвратить скачивание вредоносных объектов и переход по недоверенным ссылкам. Проверка в режиме реального времени может работать в двух режимах:

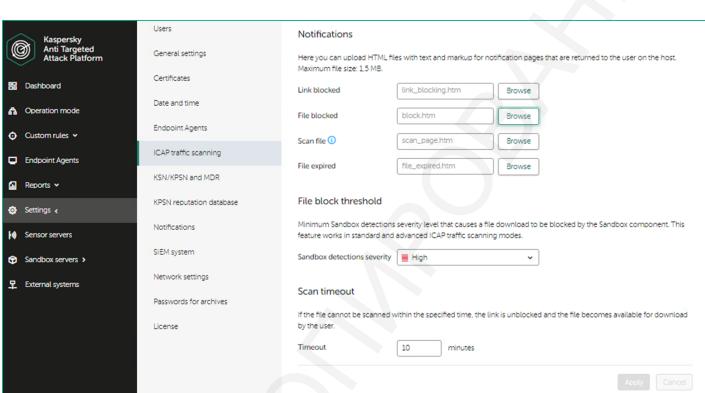
- Стандартная проверка трафика ICAP. При включении этого типа проверки репутация файлов и URL-адресов проверяется в базе знаний Kaspersky Security Network, файлы проверяются модулями Anti-Malware Engine и YARA.
- Усиленная проверка трафика ICAP. При включении этого типа проверки репутация файлов и URL-адресов проверяется в базе знаний Kaspersky Security Network, файлы проверяются компонентом Sandbox и модулями Anti-Malware Engine и YARA.

На многих прокси-серверах и устройствах достаточно будет активировать функциональность ICAP-клиента и указать адрес сервера.

В Squid, например, протокол ICAP (без режима блокировки) настраивается через конфигурационный файл squid.conf следующим образом:

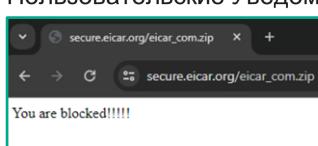
```
icap_enable on
icap_send_client_ip on
icap_service service_resp respmod_precache bypass=1 icap://<IP-
адрес Сенсора>:1344/av/respmod
adaptation_access service_resp allow all
```

Дополнительные настройки ICAP-сервера



102

Пользовательские Уведомления



Порог блокировки файлов (для Sandbox)

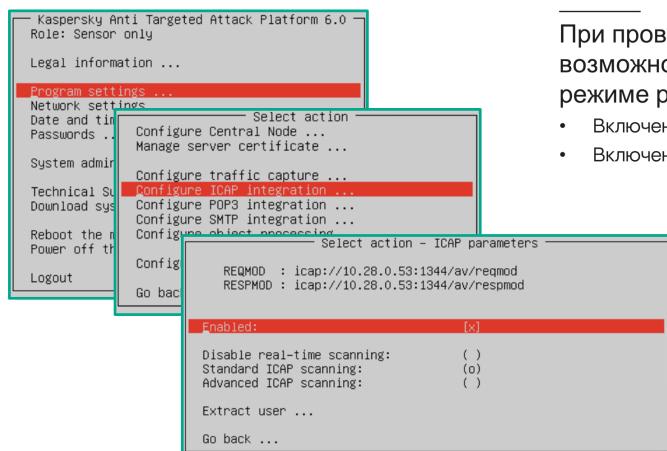
Время ожидания проверки

Вы можете уведомлять пользователя о блокировке файла или ресурса, в случае обнаружения вредоносной активности Sandbox-сервером.

Вы так же можете указать порог блокировки и максимальное время ожидания проверки.

Включите ICAP-сервер на сенсоре

103



При проверке **ICAP-трафика** есть возможность активировать **проверку** в режиме реального времени:

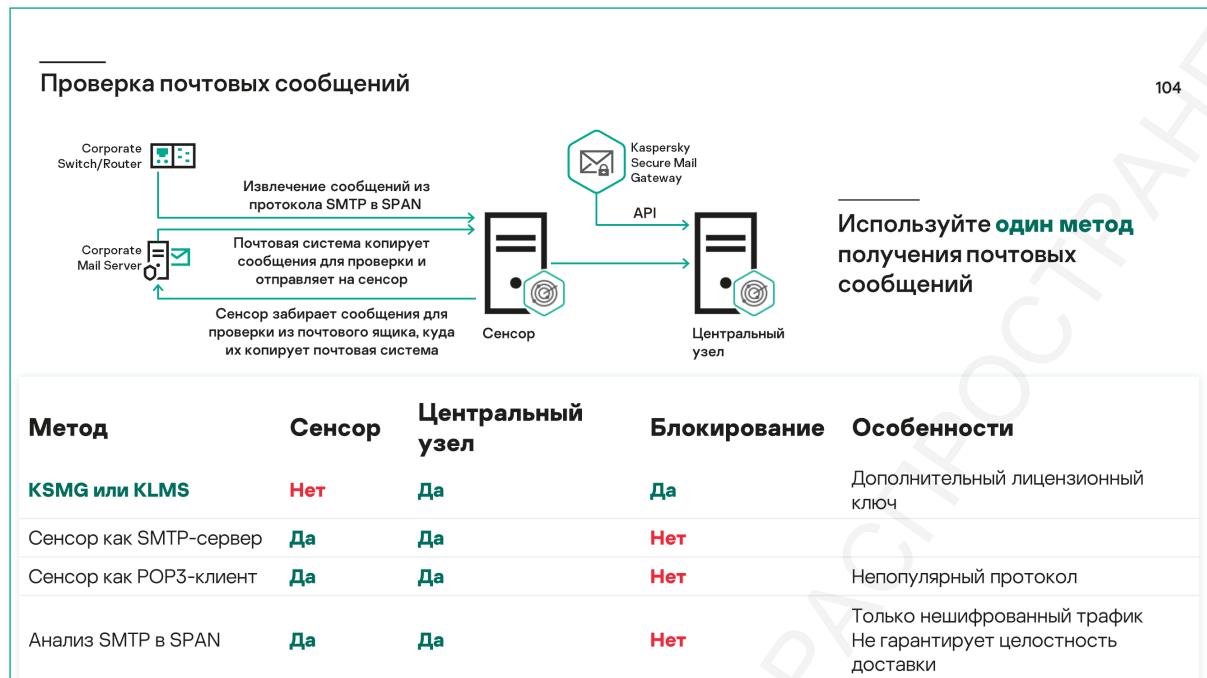
- Включено, стандартная проверка трафика ICAP
- Включено, усиленная проверка трафика ICAP

Так же возможно включить ICAP интеграцию и через консоль самого Сенсора, для этого перейдите в раздел **Program settings | Configure ICAP integration** и выберите Enabled.

Проверить, что что ICAP-трафик попадает на Сенсор и обработка ICAP-трафика работает, можно так же, как и для других источников сетевых данных:

- В разделе Sensor server веб-консоли администратора проверьте, что хотя бы для одного Сенсора в графе ICAP установлена отметка.
- В разделе Dashboard выберите источник ICAP и проверьте, что на графике отображаются поступающие данные, и что показатели URLs и Files растут.

Можно также загрузить тестовый файл EICAR по протоколу HTTP (или HTTPS, если на прокси-сервере настроена инспекция зашифрованного трафика) и проверить, что в веб-консоли сотрудника безопасности появилось обнаружение с источником ICAP.



Во внедрении Kaspersky Anti Targeted Attack важно выбрать оптимальный способ интеграции с почтовой системой. Kaspersky Anti Targeted Attack может получать почтовые сообщения для проверки несколькими способами:

SPAN (разбор нешифрованного SMTP).

Препроцессор KATA (на Сенсоре или на центральном узле в роли Сенсора) распознает в зеркальной копии трафика протокол SMTP и может извлекать из него почтовые сообщения.

Этот способ интеграции подходит только если есть возможность получить зеркальную копию трафика с незашифрованным SMTP-протоколом. Такие ситуации встречаются. Несмотря на то, что рекомендуется всегда использовать защищенный вариант SMTP (с помощью TLS), на практике нередко шифрование применяется только на уровне почтового шлюза для общения с внешними SMTP-серверами, а внутри сети используется нешифрованный SMTP-трафик, который проще анализировать.

Тем не менее, такую интеграцию стоит использовать, только если все остальные способы интеграции по каким-то причинам недоступны. SPAN-трафик ненадежный. На современном сетевом оборудовании, как правило, применяются политики Quality of Service (QoS). Согласно такой политике, разные пакеты имеют разный приоритет обработки на маршрутизаторе или коммутаторе. Пакеты зеркалированного трафика некритичны для работы сети, и, как правило, имеют самый низкий приоритет. Под нагрузкой сетевое оборудование будет сбрасывать зеркальные пакеты в первую очередь, и это не позволит KATA корректно извлечь сообщения.

POP3.

Администратор настраивает почтовую систему посыпать скрытую копию всех сообщений в специальный почтовый ящик в домене организации, и параллельно настраивает Сенсор или Центральный узел забирать сообщения для проверки из этого почтового ящика по протоколу POP3S.

Подходит для любых почтовых систем, где можно создать правило пересылки скрытой копии в отдельный почтовый ящик. В частности, подходит для получения сообщений от Microsoft Office 365.

С другой стороны, ИТ- и ИБ-департаменты заказчика не всегда охотно соглашаются использовать протокол POP3. Это старый протокол, у которого есть проблемы с безопасностью. Часто он полностью отключен в почтовой системе заказчика.

SMTP.

Администратор настраивает почтовую систему посыпать скрытую копию всех сообщений на почтовый ящик в некоем фиктивном домене и указывает Сенсор (или Центральный узел) в качестве почтового сервера для этого фиктивного домена. Параллельно администратор настраивает Сенсор (или Центральный узел) принимать почтовые сообщения по протоколу SMTP.

Подходит для почтовых систем, развернутых на территории заказчика, и полностью управляемых ИТ. Может не подходить для облачных почтовых служб, где нет возможности настроить фиктивный (виртуальный) домен для пересылки копий сообщений.

Интеграция через SMTP не имеет недостатков интеграции через POP3. Протокол SMTP хотя и старый, по-прежнему является основным протоколом для пересылки почтовых сообщений. И при таком способе интеграции KATA получает сообщения не как почтовый клиент, а как почтовый сервер, и не генерирует ненужных уведомлений о доставке или прочтении.

Kaspersky Secure Mail Gateway (KSMG) или Kaspersky Security for Linux Mail Server (KLMS).

Подходит только, если у заказчика уже развернуто решение Kaspersky Secure Mail Gateway/Kaspersky Security for Linux Mail Gateway или он планирует его приобрести вместе с KATA.

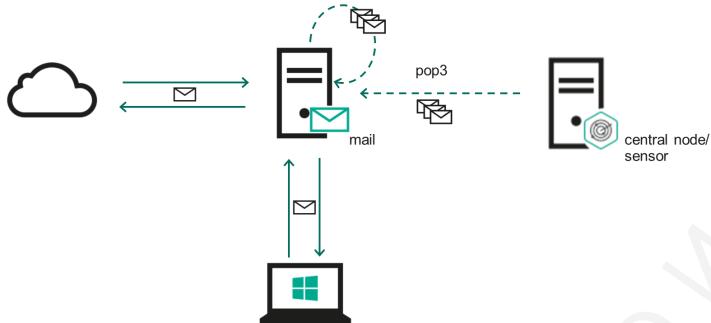
Интеграция с KSMG/KLMS имеет одно большое преимущество по сравнению с другими методами. KSMG/KLMS может блокировать опасные сообщения по результатам проверки KATA.

При всех остальных способах интеграции KATA только сообщает об угрозе постфактум, но не предотвращает доставку опасного сообщения адресату.

Важно настроить получение почтовых сообщений ровно одним способом, чтобы не создавать лишнюю нагрузку на серверы Kaspersky Anti Targeted Attack. Все остальные потенциальные способы получения почтовых сообщений лучше отключить

Проверка почтового трафика за счет интеграции по протоколу POP3

105



Сенсор выступает в роли **почтового клиента**

Настройте **почтовую систему**:

- Копировать сообщения для проверки на ящик в почтовом домене организации
- Не посылать уведомления о доставке для этого почтового ящика

Задайте на сенсоре **параметры подключения** к почтовому ящику

На почтовом сервере создайте почтовый ящик (эта учетная запись указывается во время настройки Сенсора), активируйте доступ к нему по POP3(S) и добавьте правило скрытого копирования всех или части писем. Например, на сервере Microsoft Exchange это называется BCC правилом.

Отключите для почтового ящика отправку дублирующих сообщений о прочтении писем. В противном случае отправитель будет получать уведомление о прочтении, когда Сенсор загрузит копию письма, а не когда его получит адресат.

В случае Microsoft Exchange, чтобы проверить настройку, запустите Exchange Management Shell и выполните команду:

```
Get-MailboxMessageConfiguration -Identity <email address for receiving messages by Kaspersky Anti Targeted Attack Platform> | fl
```

Проверьте значение параметра ReadReceiptResponse. Если стоит значение AlwaysSend, то его надо изменить на NeverSend. Для этого выполните команду:

```
Set-MailboxMessageConfiguration -Identity <email address for receiving messages by Kaspersky Anti Targeted Attack Platform>
```

-ReadReceiptResponse NeverSend

Во многих организациях протокол POP3 отключен за ненадобностью, и ИТ/ИБ могут негативно смотреть на необходимость включать его специально для КАТА. Поэтому при прочих равных лучше использовать интеграцию с помощью протокола SMTP.

Интеграция с помощью протокола POP3 рекомендуется, если другие способы интеграции недоступны, например, в некоторых версиях Office 365.

The screenshot shows the 'Sensor servers' configuration page. On the left, there's a sidebar with navigation options like Dashboard, Operation mode, Custom rules, Endpoint Agents, Reports, Settings, and Sensor servers. The 'Sensor servers' option is selected. The main area displays a table for 'localhost' with columns for IP/name, Type, Certificate fingerprint, SPAN, SMTP, ICAP, POP3, and State. The 'POP3' column for localhost shows 'Enabled'. Below the table, a detailed configuration window for 'localhost' is open, specifically the 'POP3 integration' tab under 'General settings'. It contains fields for Mail server (10.28.0.10), Port (110), Receive every (2), and various security and certificate settings. Buttons for 'Apply' and 'Cancel' are at the bottom right of the config window.

Чтобы настроить интеграцию по POP3 в интерфейсе Центрального узла, перейдите в раздел Sensor servers | localhost (или другой подключенный Сенсор) | POP3 Integration, измените статус на Enabled и укажите параметры доступа к ящику:

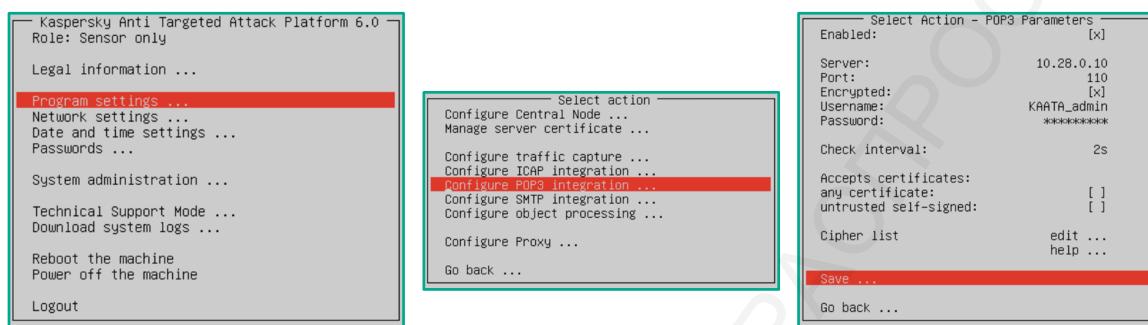
- IP-адрес почтового сервера;
- Хотите ли вы использовать защищенное соединение (рекомендуется);
- Учетную запись для подключения к серверу;
- Пароль;
- Интервал проверки почтового ящика;
- Параметры использования сертификатов для установки защищенного соединения.

Со значениями по умолчанию Сенсор Центрального узла или отдельный Сенсор подключается к почтовому ящику каждые 2 секунды и скачивает все имеющиеся письма. В почтовом ящике они не остаются. За одну сессию скачивается до 3 000 писем. Если писем было больше, то оставшиеся письма плюс новые накопившиеся загружаются во время следующей сессии через 2

секунды. После загрузки Сенсор разбирает каждое письмо, извлекая из него служебный заголовок, тело сообщения и вложения. Здесь наибольший интерес представляют вложенные файлы и ссылки.

Настройте почтовый клиент на сенсоре

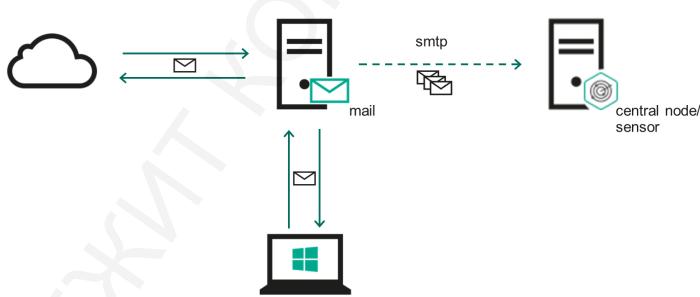
107



Возможно включить ICAP интеграцию и через консоль самого Сенсора, для этого перейдите в раздел **Program settings | Configure POP3 Integration** и выберите Enabled, после чего введите необходимые для подключения данные.

Проверка почтового трафика за счет интеграции по протоколу SMTP

108



Сенсор выступает в роли **почтового сервера**

Настройте **почтовую систему**:

- Копировать сообщения для проверки на ящик в фиктивном домене
- Маршрутизировать сообщения в этот домен через адрес сенсора

В описанном выше способе интеграции Сенсор выступает почтовым клиентом, который получает сообщения для проверки по протоколу POP3. Kaspersky Anti Targeted Attack

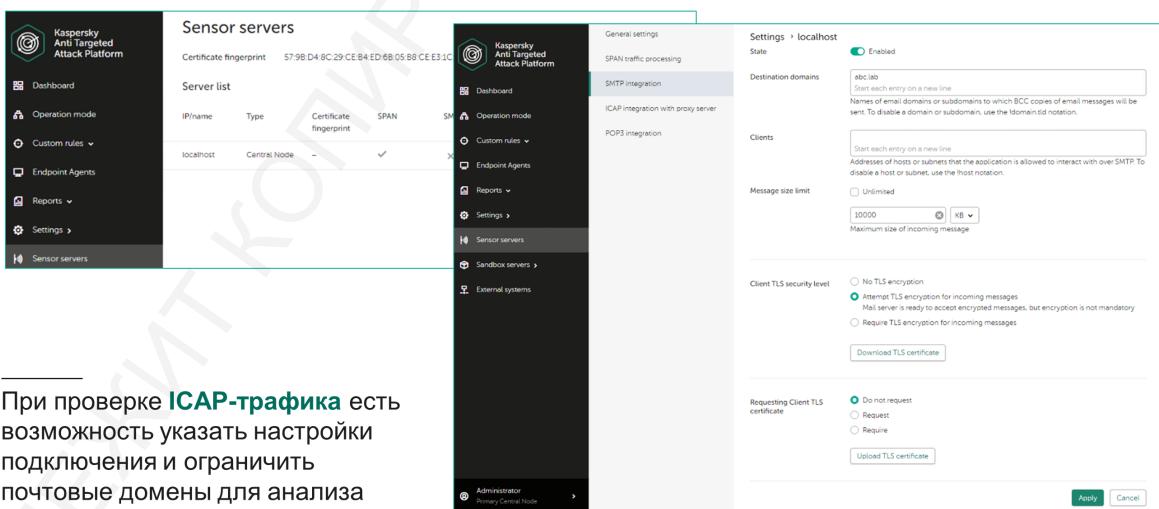
поддерживает альтернативный (и часто предпочтительный) способ интеграции, в котором Сенсор выступает почтовым сервером и получает копии почтовых сообщений по протоколу SMTP.

В контексте интеграции с почтовой системой по протоколу POP3 или SMTP, Сенсор не перехватывает соответствующие протоколы, а получает копии почтовых сообщений для проверки по одному из этих двух протоколов. Почтовая система должна быть настроена отправлять копии на Сенсор. Сенсор может извлекать почтовые сообщения, отправленные по незащищенному протоколу SMTP, из сырого трафика, поступающего на SPAN-интерфейс, но это не рекомендуемый способ проверки почтового трафика организации, и он не имеет отношения к POP3- или SMTP-интеграции с почтовой системой.

Чтобы использовать интеграцию с почтовой системой по протоколу SMTP, на почтовом шлюзе укажите адрес для отправки копий всех почтовых сообщений, например, BCC-адрес sensor@abc.local, где abc.local — это специальный домен для проверки почтовых сообщений, а не основной домен организации. Далее на почтовом шлюзе укажите Сенсор (или Центральный узел) в качестве почтового сервера (MX) для этого домена.

Как только на почтовый шлюз придет письмо, оригинальное письмо будет отправлено на почтовый сервер (например, mail.abc.lab), после чего его получит адресат. Копия письма будет отправлена на адрес sensor@abc.local и ее получит Сенсор.

Включите SMTP-сервер в свойствах центрального узла
109



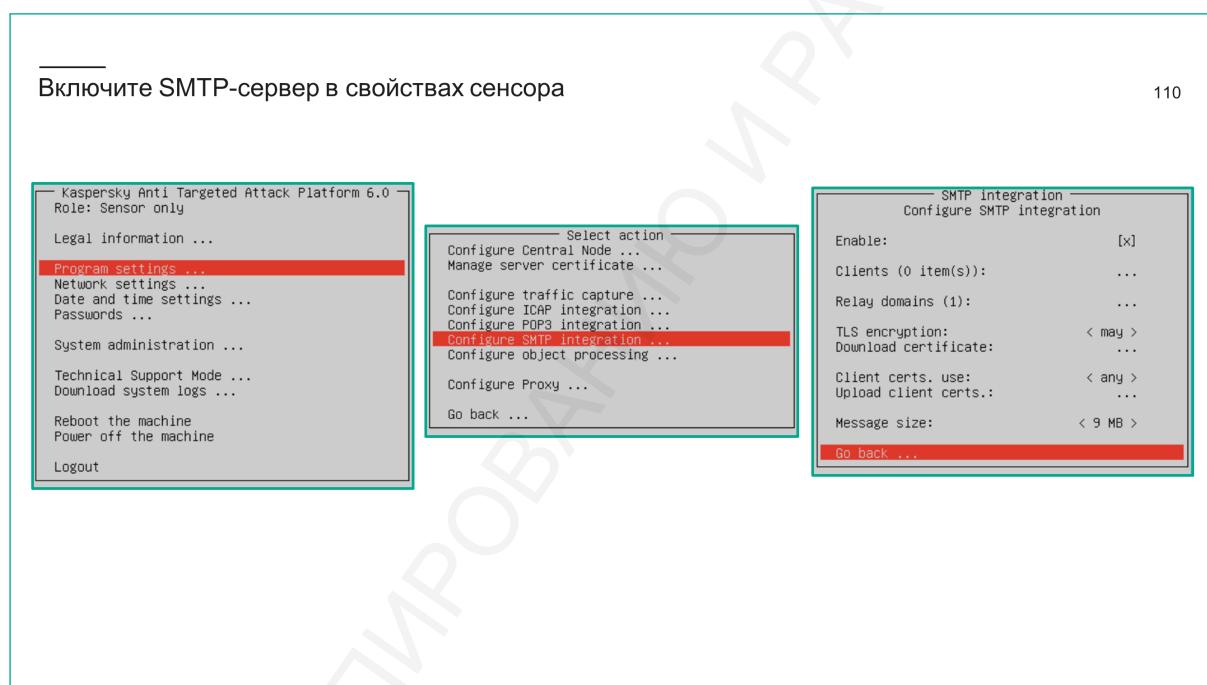
Настройка SMTP-сервера в свойствах центрального узла

При проверке **ICAP-трафика** есть возможность указать настройки подключения и ограничить почтовые домены для анализа

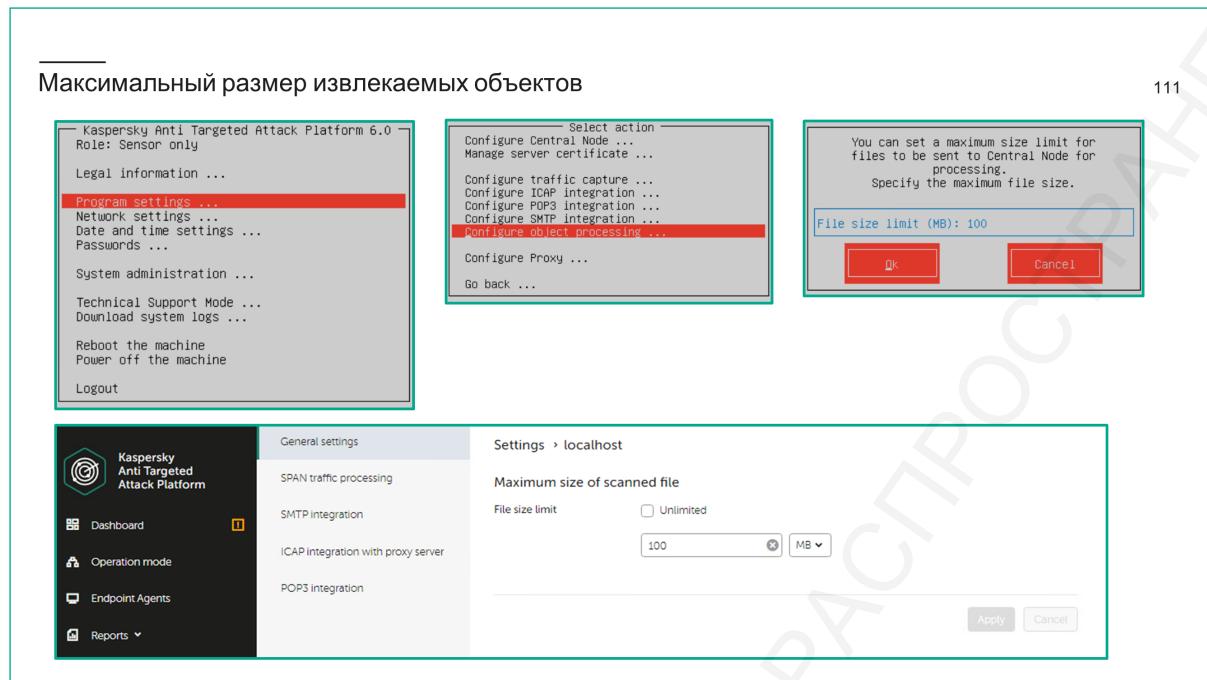
На стороне Kaspersky Anti Targeted Attack настройте Сенсор (или Центральный узел) принимать почтовые сообщения по протоколу SMTP в качестве почтового сервера. Чтобы сделать это, в

интерфейсе Центрального узла перейдите в раздел Sensor servers | localhost (или другой подключенный Сенсор) | SMTP Integration, измените статус на Enabled и укажите параметры подключения:

- Destination Domains (домены назначения, для которых Сенсор будет принимать сообщения);
- Clients (хосты или подсети, из которых Сенсор будет принимать сообщения. Если ничего не указано, Сенсор будет принимать только сообщения из всех локальных подсетей);
- Message size limit;
- Client TLS security level;
- Requesting Client TLS certificate.



Возможно включить SMTP интеграцию и через консоль самого Сенсора, для этого перейдите в раздел Program settings | Configure SMTP Integration и выберите Enabled, после чего введите необходимые для подключения данные.



Максимальный размер сообщения, которое примет Сенсор, по умолчанию 100 МБ.

Проверка работоспособности

Чтобы проверить, что проверка почты работает, используйте веб-консоль администратора:

- Проверьте, что в разделе Sensor servers хотя бы у одного Сенсора стоит отметка в графе POP3 или SMTP. Это значит, что интеграция с почтовой системой по протоколу POP3 или SMTP действительно включена.
- Затем проверьте, что Сенсор получает и обрабатывает почтовые сообщения. Для этого в разделе Dashboard на панели Processed выберите источник POP3 или SMTP и убедитесь, что график показывает поступление сообщений.

Альтернативно, отправьте по почте тестовый файл EICAR и проверьте, что в веб-консоли сотрудника службы безопасности появилось обнаружение с источником POP3 или SMTP. Обращайте внимание на сообщения об ошибках в верхней части экрана Dashboard, среди них могут быть ошибки, относящиеся к POP3 или SMTP интеграции.

4.2. Технологии обнаружения KATA

Технологии Kaspersky Anti Targeted Attack

112

Технология	Описание
IDS	Обнаруживает сетевые атаки в сетевом трафике (SPAN) по обновляемым и пользовательским правилам. Основана на Suricata
URL reputation	Обнаруживает опасные, фишинговые и связанные с АРТ ссылки
Anti-malware Engine	Обнаруживает опасные файлы, извлеченные из сетевого, почтового или веб-трафика по обновляемым сигнатурам
Mobile attack analyzer	Обнаруживает опасные файлы для мобильных платформ, используя методы машинного обучения
Sandbox	Обнаруживает опасные файлы, в том числе расположенные по ссылкам, за счет исполнения файлов в виртуальных машинах и анализа их активности
YARA	Классифицирует извлеченные из трафика файлы по пользовательским правилам YARA

Технологии обнаружения, используемые КАТА.

IDS.

Для обнаружения признаков опасной активности в сетевом трафике Kaspersky Anti Targeted Attack использует систему обнаружения вторжений Suricata.

Suricata — это мультиплатформенная сетевая система обнаружения и предотвращения вторжений с открытым исходным кодом. Она используется в продуктах из области информационной безопасности: межсетевых экранах, IDS/IPS устройствах, DLP и SIEM решениях.

Принцип работы Suricata основан на регистрации и анализе сетевых пакетов в реальном времени. Анализ заключается в проверке трафика с помощью правил, по результатам которой выполняется действие, заранее заданное аналитиком. Система позволяет обнаружить целый ряд атак, сканирований и зондирований, таких как попытки внедрить вредоносный код, атаки на переполнение буфера, атаки на веб-приложения и т.д.

Suricata в составе Kaspersky Anti Targeted Attack Platform работает в пассивном режиме: регистрирует, но не блокирует подозрительные пакеты. Это обусловлено тем, что Сенсор подключается к сети не в разрыв соединения.

База данных с правилами поставляется вместе с решением и впоследствии периодически обновляется через интернет. Она включает в себя правила, созданные экспертами Лаборатории Касперского. Старший сотрудник службы безопасности может добавить свои правила через веб-интерфейс Центрального узла.

Правила Suricata применяются ко всему «сырому» трафику, полученному через зеркальный порт. Получив пакет, Suricata извлекает данные сетевого и транспортного уровней из протоколов канального уровня, нормализует их и анализирует на предмет подозрительной активности.

URL reputation.

Технология URL reputation применяется к ссылкам, извлеченным из трафика. Она применяется в рамках работы так называемого препроцессора — специального модуля, который отвечает за обработку трафика на Сенсоре (или центральном узле).

Препроцессор (APT-Preprocessor) отвечает за извлечение объектов и метаданных из сетевого, веб- и почтового трафика, и передачу этих данных локальному модулю KSN URL Reputation на Сенсоре (центральном узле) для более детального анализа. Препроцессор выполняет следующие функции:

- Получает зеркальный трафик от сетевых устройств. Анализирует протоколы HTTP, FTP, DNS и SMTP. Извлекает из них объекты и метаданные. Таким образом Сенсор получает трафик, после чего препроцессор анализирует одну из копий трафика, разбирая HTTP, FTP, DNS и SMTP протоколы и извлекая из них объекты и метаданные.
- Взаимодействует с прокси-серверами и получает объекты из HTTP- и FTP-трафика по протоколу ICAP. Также возможна проверка HTTPS-трафика, если прокси-сервер поддерживает подмену TLS- сертификата.
- Взаимодействует с почтовыми серверами по POP3(S) и загружает копии почтовых сообщений.
- Взаимодействует с почтовым шлюзом по SMTP(S) и получает копии почтовых сообщений.

Кроме файлов препроцессор извлекает URL-адреса из сетевого, почтового и веб-трафика организации и проверяет их технологией URL reputation. Проверка URL reputation реализована как запрос в Kaspersky Security Network, где переданный хеш URL проверяется по спискам: * адресов, задействованных в целевых атаках (APT-related); * вредоносных URL (включая URL командных серверов ботнетов); * фишинговых URL.

Результаты проверки по адресам, которые уже были проверены в облаке, хранятся в локальном KSN-кеше на Сенсоре согласно значению TTL, которое приходит вместе с ответом из Kaspersky Security Network. Если срок хранения не истек, а из трафика снова извлекается проверенная ранее ссылка, то для повышения производительности используется кешированный результат. Новый запрос в Kaspersky Security Network не отправляется. Если ссылка новая, то запрос отправляется.

Kaspersky Anti Targeted Attack также проверяет активные ссылки в офисных документах, но проверка выполняется антивирусным ядром на центральном узле, а не модулем URL Reputation на Сенсоре.

Исходя из описанного принципа работы URL Reputation, чтобы проверить корректное функционирование модуля, нужно выполнить обращение к URL, который относится к одной из детектируемых категорий и проверить, что в веб-консоли появилось обнаружение от технологии URL reputation.

В качестве проверочного URL можно использовать <http://www.kaspersky.com/test/wmuf>. Это специальный тестовый URL, который распознается продуктами Лаборатории Касперского как вредоносный.

Чтобы инициировать перехват этого URL в трафике, можно воспользоваться одним из следующих способов: * открыть URL в браузере; * отправить по почте сообщение с URL в теле письма.

Модуль URL reputation работает исключительно за счет запросов в Kaspersky Security Network, которые выполняются специальным KSN-клиентом (еще одним модулем в составе Kaspersky Anti Targeted Attack/Kaspersky Endpoint Detection and Response).

Функциональность KSN-клиента разделена на две части: модуль KSN File Reputation входит в состав Центрального узла, а модуль KSN URL Reputation в состав Сенсора. Проверка файлов относительно облачной базы данных осуществляется на центральном узле, чтобы не перегружать Сенсор проверкой извлеченных файлов, т.к. они в любом случае будут отправлены на Центральный узел для дополнительного анализа.

Если доступа к Kaspersky Security Network нет, то и технология URL reputation работать не будет. Информация о статусе обновлений и KSN отображается в веб-интерфейсе любой учетной записи. Перейдите в раздел Dashboard и посмотрите, нет ли в верхней части экрана сообщений об ошибках. Эти статусы обновляются каждые 10 минут. Детали об ошибках подключения к KSN ищите в журнале /var/log/kaspersky/apt-swarm/ksn_proxy/ksn_proxy.log

Anti-malware Engine.

Файлы и ссылки, извлеченные из трафика модулями Kaspersky Anti Targeted Attack, а также файлы, запрошенные аналитиком с узлов сети инструментами Kaspersky Endpoint Detection and Response, попадают в очередь обработки на Центральный узел, где их обрабатывает модуль apt-collector.

Коллектор (APT-Collector) получает объекты для проверки и сортирует их. Результаты

обнаружения технологиями Сенсоров он добавляет в базу обнаружений. Файлы проверяет по «белому списку» и после фильтрации ставит в очередь для проверки антивирусным ядром. Антивирусное ядро получает объекты от коллектора, при необходимости распаковывает, проверяет их и решает, какие еще технологии будут использованы для проверки.

В антивирусном ядре реализованы:

- Сигнатурный анализ,
- Статистический анализ,
- Эвристический анализ,
- Эмуляция,
- и многое другое.

При необходимости антивирусный компонент отправляет запросы в Kaspersky Security Network для дополнительной проверки. Ответ, полученный из KSN, имеет приоритет над результатом, выданным антивирусным ядром. Если антивирусное ядро считает файл вредоносным, а из Kaspersky Security Network приходит ответ, что файл чистый, то файл будет признан чистым и событие об обнаружении вредоносного объекта в веб-интерфейсе не появится. Если антивирусное ядро признает файл чистым, а из KSN возвращается ответ, что файл зараженный, то файл будет считаться зараженным и в веб-интерфейсе появится соответствующее обнаружение.

Результаты по файлам, которые уже были проверены в Kaspersky Security Network, хранятся в локальном KSN-кеше согласно «времени жизни» записи (значению time-to-live). Значение TTL приходит вместе с ответом из Kaspersky Security Network. Если срок хранения не истек, а Центральный узел снова получает проверенный ранее файл, то для повышения производительности используются данные из кеша. Новый запрос в Kaspersky Security Network не отправляется.

Файлы с еще неустоявшейся репутацией в KSN (непопулярные или неизвестные файлы) попадают в очередь на перепроверку. Всегда есть риск того, что злоумышленники смогут уклониться от обнаружения, создав файл, специально заточенный под конкретного клиента и конкретные средства защиты. Если исходная проверка ничего не обнаружила, при повторной проверке шансы обнаружения выше, за счет новых данных, поступающих с обновлениями и доступных в KSN.

Файлы в очереди на перепроверку проверяются повторно через 1, 2, 4, 8 и 16 недель (7, 14, 28, 56 и 112 дней). Размер очереди по умолчанию ограничен 300 Гб. В большой организации этого может оказаться мало и новые файлы будут вытеснять из очереди старые файлы еще до того,

как те пройдут повторную проверку.

Если одна из технологий проверки файлов (антивирусное ядро, YARA или Sandbox-сервер) признает файл вредоносным, и этот файл имеет цифровую подпись, то модуль APT-Certcheck запускает проверку подписи. Проверка выполняется с помощью базы сертификатов, поставляемой вместе с решением. В базе содержится информация о доверенных и недоверенных сертификатах, а также сертификатах с истекшим сроком действия. Результаты проверки добавляются в общее обнаружение и могут быть использованы во время расследования инцидента.

Исходя из вышесказанного, чтобы проверить работоспособность антивирусного ядра, нужно передать в очередь проверки файл, который антивирусное ядро посчитает вредоносным. Традиционно для таких целей используется специальный тестовый файл EICAR (www.eicar.org). Это специальный файл, который не выполняет никаких опасных действий, но по договоренности определяется как вредоносный антивирусными средствами.

Чтобы проверить работоспособность антивирусного ядра в Kaspersky Anti Targeted Attack, загрузите eicar.com с официального сайта (по умолчанию используется протокол HTTPS). Если Kaspersky Anti Targeted Attack не получает от прокси-сервера файлы, загружаемые по HTTPS, переотправьте загруженный eicar.com по почте. В веб-консоли Центрального узла должно появиться обнаружение.

Чтобы проверить работоспособность антивирусного ядра в Kaspersky Endpoint Detection and Response, просто загрузите тестовый файл eicar.com в хранилище кнопкой Upload в разделе Storage в веб-консоли сотрудника службы безопасности.

Mobile attack analyzer

Обнаруживает опасные файлы для мобильных платформ, используя методы машинного обучения.

Sandbox.

Решение о том, что файл нужно проверять на сервере Sandbox, принимает антивирусное ядро. Логика принятия решения содержится в антивирусных базах и регулярно улучшается для достижения оптимальных результатов. Если антивирусное ядро считает, что файл нужно проверить технологией Sandbox, ядро создает задачу проверки файла для Sandbox и ставит его в отдельную очередь. Этую очередь обрабатывает специальный Sandbox-агент.

Sandbox-агент взаимодействует с Sandbox-сервером. Агент получает задачи на проверку файлов и ссылок от антивирусного ядра и отправляет их на сервер для анализа поведения в Windows-среде. При отправке объекта он получает номер задачи, а при следующем

подключении забирает результаты анализа по этому номеру. Соединения со стороны Sandbox-сервера к центральному узлу не предусмотрены.

На Sandbox-устройстве запускаются виртуальные машины с операционными системами Windows 7 64-bit, Windows 10 64-bit, Astra Linux 1.7, CentOS 7.8. Каждая из машин включает в себя набор популярных бизнес-приложений разных версий, таких как Microsoft Office, Adobe Reader и Flash Player, веб-браузеры и т.д. Файл проверяется параллельно на нескольких видах виртуальных машин. Чтобы передать файл на очередной образ, системе не надо дожидаться окончания его проверки на предыдущем образе. Решение о том, на каких типах виртуальных машин будет проверяться файл, принимается антивирусным ядром на центральном узле.

Объекты могут проверяться в двух режимах:

- Full logging mode собирает как можно больше деталей об активности внутри виртуальной машины, но жертвует временем наблюдения за образцом.
- Quick scan mode собирает меньше деталей, но наблюдает за образцом примерно в 10 раз дольше, чем в режиме Full logging mode. При этом проверка в Quick Scan Mode не требует больше времени за счет применения специальных технологий.

После запуска файла на виртуальной машине, все его действия фиксируются. Когда данные собраны, они сохраняются за пределами виртуальной машины, а сама машина удаляется. Для проверки следующего файла будут использоваться новые виртуальные машины, созданные из ежедневно обновляемых снэпшотов.

Собранные данные анализируются на предмет вредоносной или подозрительной активности, включая эксплуатацию уязвимостей, использование техник обхода и попытки связи с командными серверами. За анализ журналов выполнения и артефактов отвечает специальный компонент Scanner. Перехваченный трафик виртуальной машины проверяет модуль IDS Suricata (такой же, как и в сетевом Сенсоре).

Оба компонента, Scanner и IDS (Suricata) используют регулярно обновляемые базы для анализа. Kaspersky Security Network для анализа не используется. Результаты анализа забирает Sandbox-агент. Он соединяется с Sandbox примерно раз в секунду и запрашивает результаты отправленных ранее задач. Соединения со стороны Sandbox-сервера к центральному узлу и другим узлам сети не предусмотрены, чтобы в случае его компрометации, не были скомпрометированы другие машины.

Sandbox реализует многочисленные технологии сокрытия работы в виртуальной среде.

Проверить работоспособность анализа файлов технологией Sandbox проще в продукте

Kaspersky Endpoint Detection and Response. Достаточно загрузить любой исполняемый файл в хранилище кнопкой. Даже если файл чистый, в консоли будут отображаться результаты проверки файла и можно будет скачать архив со всеми артефактами анализа (журналами выполнения, дампами памяти процессов и пр.).

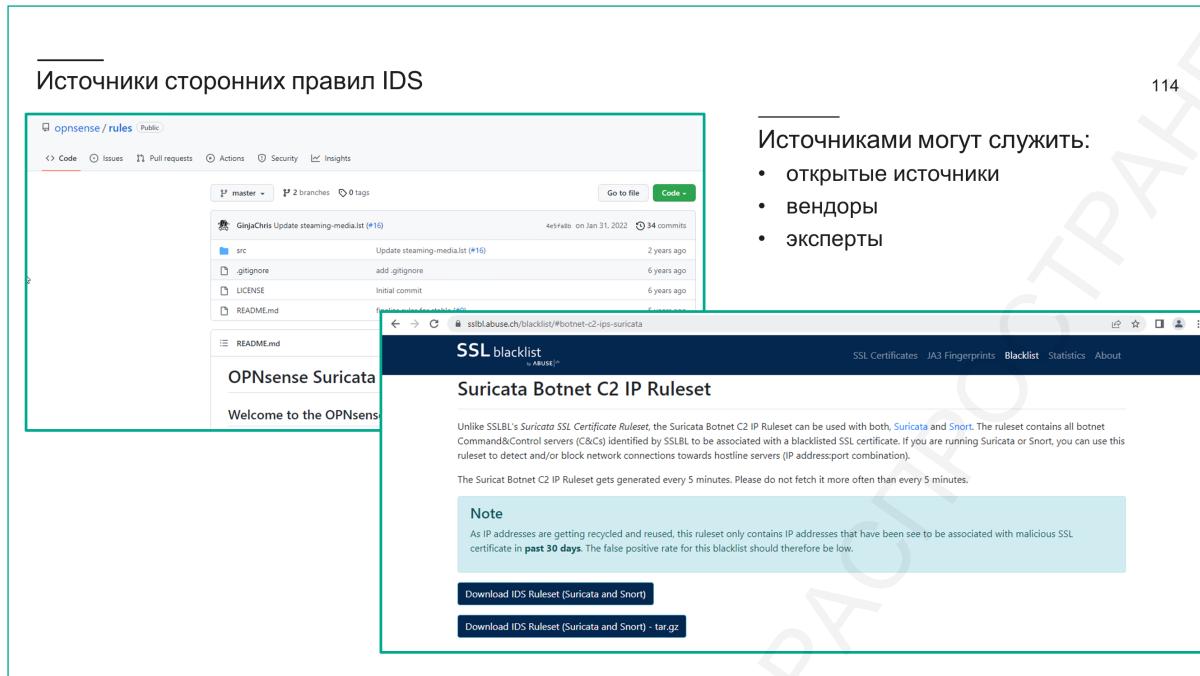
В продукте Kaspersky Anti Targeted Attack проверить работоспособность Sandbox не так просто. Администратор может отправить по почте архив с исполняемым файлом, но, если файл чистый, результаты его анализа не будут опубликованы в веб-консоли.

YARA.

Классифицирует извлеченные из трафика файлы по пользовательским правилам YARA.

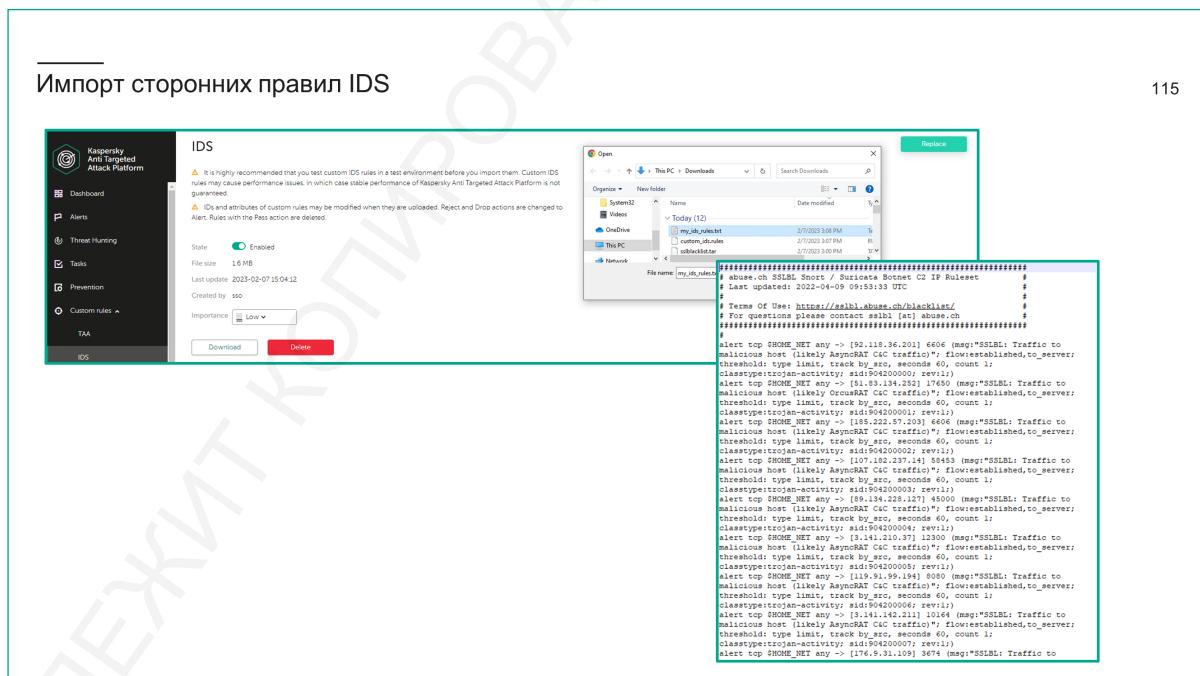
Технологии Kaspersky Anti Targeted Attack				113
Технология	Обновляемая логика	Пользовательские правила	Использует KSN	
IDS	Да	Да	Нет	
URL reputation	Нет	Нет	Да, обязательно!	
Anti-malware Engine	Да	Нет	Да	
Mobile attack analyzer	Да	Нет	Да, обязательно!	
Sandbox	Да	Нет	Нет	
YARA	Нет	Да	Нет	

Для части технологий детектирования возможно написание пользовательских правил, для части нет. Так же часть технологий без подключения к KSN не функционирует.



Списки сторонних правил IDS часто входят в публичные отчеты об обнаруженных атаках или вредоносных программах, их можно найти в открытых источниках или аналитических отчетах.

Важно не добавлять все сторонние правила, что получится найти, а анализировать какие из них действительно будут полезны, каким источникам можно доверять и где есть достоверная информация о том, что же детектируют данные правила.



Правило Suricata состоит из двух частей: заголовка и опций. В заголовке указывается действие, протокол, источник, направление, целевой адрес и порты. Опции позволяют указать дополнительные параметры проверки, а также ввести информацию о правиле. Параметров

может быть довольно много, включая размер IP-пакетов, флаги в TCP заголовках, последовательность байт, глубину проверки содержимого и т.п. Общий вид правила:

```
action protocol source_ip source_port direction destination_ip  
destination_port (options)
```

Пример правила, которое предупреждает обо всех фрагментах, идущих с HTTP портов из внешней сети во внутреннюю сеть, в которых есть слово “violence” (жестокость). Параметр “nocase” позволяет не учитывать регистр при анализе. Предупреждение появится с указанием причины “Violence word matched” (совпадение слова). Здесь используются переменные \$EXTERNAL_NET, \$HOME_NET и \$HTTP_PORTS, описывающие внешнюю сеть (из которой предположительно исходят атаки), внутреннюю сеть (которую предполагается защищать) и HTTP порты. Переменные задаются в конфигурационном файле, в нем же указывается путь к файлам с правилами.

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any  
(msg:"Violence word matched"; content:"violence"; nocase;  
sid:1234567;)
```

Если говорить об обнаружении сложных угроз, то одним правилом здесь не обойтись.

Понадобится от нескольких единиц до нескольких десятков правил.

Исходя из описанного выше принципа работы технологии IDS в Kaspersky Anti Targeted Attack, чтобы проверить ее работоспособность, нужно сгенерировать трафик, на который в продукте есть детектирующее правило IDS. Можно пойти несколькими путями:

Написать свое тестовое правило и загрузить его в продукт. Тестовое правило может быть предельно простым, оно может, например, реагировать на любые соединения с неким IP-адресом:

```
alert tcp any any -> any any (msg:"access to 192.0.2.233";  
content: "192.0.2.233"; sid:1001001;)
```

После загрузки правила достаточно будет обратиться к указанному адресу по сети и проверить, что в списке обнаружений есть обнаружение от технологии IDS с соответствующими деталями обнаружения. На момент написания курса работает, например, запрос:

```
nslookup bandtester.com
```

Использовать тот факт, что среди правил IDS от Лаборатории Касперского есть правило на загрузку строки тестового вируса EICAR. Нужно загрузить страницу, на которой есть строка

тестового вируса EICAR, по протоколу HTTP и проверить, что в веб-консоли сотрудника службы безопасности появляется обнаружение.

Здесь важно, чтобы это был именно протокол HTTP, т. к. Kaspersky Anti Targeted Attack не обладает функцией анализа защищенного трафика. И даже если Kaspersky Anti Targeted Attack получает объекты из трафика HTTPS от прокси-сервера по протоколу ICAP, это именно уже извлеченные файлы и ссылки, а не сырой трафик, и они не проходят проверку технологией IDS.

Чтобы импортировать сторонние правила IDS необходимо перейти в раздел **Custom rules | IDS** и нажать Import чтобы загрузить файл со сторонними правилами IDS.

Файл может быть загружен только один, поэтому если необходимо внести изменения в него, то сначала необходимо скачать существующий, нажав кнопку Download, отредактировать его, а потом загрузить в KATA, используя кнопку Replace.

Источники YARA-правил

116

- **tip.kaspersky.com** (платная подписка)
- другие вендоры
- открытые источники
- YARA-генераторы
- эксперты

YARA Rule	Last Update	Frequency
Mobile Malicious Hash Feed	27/09/2023	Every 20 minutes
Mobile Malicious URL Feed	27/09/2023	Every 20 minutes
Mobile Benign C&C URL Data Feed	13/09/2023	Every 1 hour(s)
IP Reputation Feed	27/09/2023	Every 20 minutes
Resonware URL Feed	27/09/2023	Every 20 minutes
APT URL Feed	27/09/2023	Every 20 minutes
APT IP Feed	27/09/2023	Every 20 minutes
APT Hash Feed	27/09/2023	Every 1 hour(s) (only if there is no new data in Master IOC / YARA feed)
APT YARA Feed	27/09/2023	Every 1 hour(s) (only if there is no new data in Master IOC / YARA feed)
Malicious URL Exact Feed	27/09/2023	Every 10 minutes

Продукты Kaspersky Anti Targeted Attack и Kaspersky Endpoint Detection and Response поставляются без YARA-правил и применяют только правила, загруженные старшим сотрудником службы безопасности.

Yara — это мультиплатформенный инструмент, который позволяет обнаруживать и классифицировать семейства вредоносного ПО. Виктор Альварес, создатель Yara, описывает свою систему, как «швейцарский нож для исследователей вредоносного ПО, работающий по шаблонам», и добавляет, что «Yara для файлов — это то же самое, что Snort/Suricata для сетевых пакетов». Этот инструмент действительно стал довольно популярным в сфере ИБ.

Yara может обнаруживать не только вредоносное ПО, но и утилиты, которые не блокируются антивирусом в силу отсутствия вредоносной составляющей. Такие утилиты могут иметь незадекларированный или побочный функционал и использоваться на одном из этапов атаки. Это индикаторы компрометации. Системный администратор должен быть осведомлен об их присутствии в трафике компании. В качестве примера приведем инструменты для удаленного управления или сбора паролей.

Yara правила не обязательно создавать вручную. Существуют онлайн-генераторы, которые анализируют загру

Условия в Yara-правилах — это строки с описанием вредоносного кода или другого объекта в виде текстовых и/или шестнадцатеричных шаблонов. За каждым описанием следует логическое выражение, определяющее условия, которым должен удовлетворять объект. В общем виде правило выглядит так: сначала указываете название с описанием правила, далее идет раздел с переменными, после чего определяете условия срабатывания.

```
rule RuleNameHere
{
    meta:
        strings:
            $a =
            $b =
        condition:
            $a logical operator $b
}
```

Правила могут быть связаны друг с другом. Одним из условий удовлетворения объекта правилу является удовлетворение этого объекта другому правилу, которое должно стоять раньше по списку. В простейшем случае вы даете правилу название ("TestRule"). Вводите текстовые и шестнадцатеричные переменные: \$my_text_string и \$my_hex_string. Указываете условие срабатывания — обнаружение одной из переменных (\$my_text_string or \$my_hex_string).

```
rule TestRule
{
    strings:
        $my_text_string = "malware"
        $my_hex_string = { 6e 65 77 20 76 69 72 75 73 }
    condition:
        $my_text_string or $my_hex_string
}
```

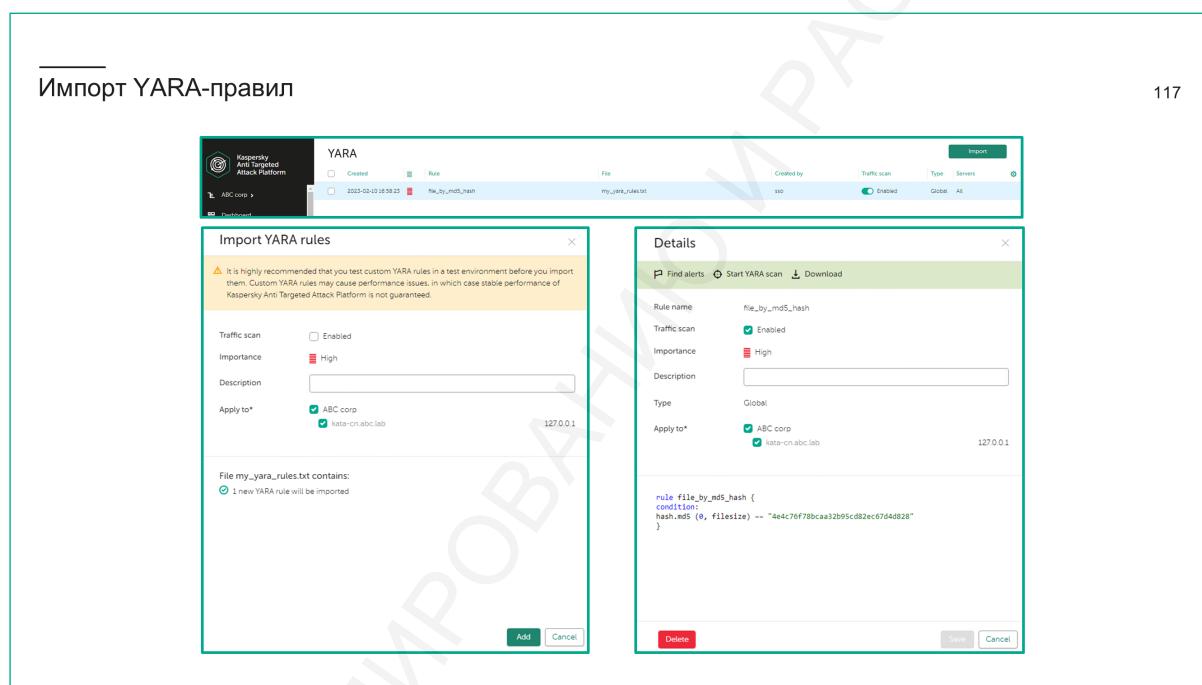
Если при анализе объекта обнаружится текст "malware" или шестнадцатеричная последовательность "6e 65 77 20 76 69 72 75 73", то такой объект вызовет детект.

Обнаружение тестового вируса Eicar выглядит следующим образом. Здесь добавляется

информационный раздел “meta”, содержащий сведения о правиле, но не влияющий на само правило.

```
rule Eicar_test
{
    meta:
        description = "Just Eicar test"
        in_the_wild = true
    strings:
        $a = "EICAR-STANDARD-ANTIVIRUS-TEST-FILE"
    condition:
        $a
}
```

Для описания сложных угроз обычно создают несколько правил.



Чтобы импортировать сторонние правила YARA необходимо перейти в раздел **Custom rules | YARA** и нажать Import для загрузки файла со сторонними правилами YARA.

YARA можно загружать разными файлами, а не только одним, как для IDS. KATA разберет каждое правило из каждого файла по отдельности и позволит по каждому отдельному правилу включить сканирование, посмотреть события, скачать его.

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. In the top left, there's a sidebar with 'ABC Corp >', 'Dashboard', 'Alerts', 'Threat Hunting', 'Tasks', and 'Prevention'. The main area has tabs for 'All alerts', 'Event details #1', 'Assigned to @Me', 'Recommendations', 'Qualifying', and 'Add to exclusions'. Below these are sections for 'State' (Closed), 'Importance' (High), 'Data source' (SPAN Sensor 127.0.0.1 (2024-01-25 05:05:02)), 'Time created' (2024-01-25 05:05:02), 'Time updated' (2024-01-25 05:05:05), 'Scan results' (IDS: HackTool.BruteForce.SSH.C/C; Generic suspicious network activity), 'IDS rule' (Rule details), and 'Investigating' (Find addr, Dow, Dow). A modal window titled 'Add IDS rule to exclusions' is open, showing a table with one row: Rule name: HackTool.BruteForce.SSH.C/C, Generic suspicious network activity; Header: alert tcp any any -> any 22; Flow: established,to_server; Rulelets: isSSH,bruteForce,hydra_1_4; Flags: FA; stream_size: client,>1300; client,<2050; threshold: type both; count 10; seconds 120; track by dst; sid: 60216478; Description: (empty); and Apply to servers: ABC Corp, Italia. The number 127.0.0.1 is also visible.

Если правило IDS создает много малополезных обнаружений, его можно отключить, создав исключение.

Исключения создаются из карточки обнаружения IDS ссылкой Add to exclusions справа в панели рекомендаций. Исключение называется по имени правила и содержит все атрибуты правила. Сотрудник службы безопасности может добавить к исключению описание, в котором указать причину, по которой это правило пришлось отключить.

Позже все исключения можно найти в разделе Settings | Exclusions на вкладке IDS.

Исключение отключает применение правила ко всему трафику. Отключить применение правила для отдельного адреса или диапазона адресов нельзя

Исключения объектов из проверки АМ

The screenshot shows three windows from the Kaspersky Anti Targeted Attack Platform:

- Top Window:** Event details #1785. It displays basic information about an alert (State: Closed, Importance: High, Data source: SPN Sensor 127.0.1 (2024-01-29 03:32:00), Time created: 2024-01-29 03:32:00, Time updated: 2024-01-29 03:32:00). The "Object information" section shows a file named "2 MB MDS SHA256". A context menu is open over this file, listing options like "Find on TIP", "Find events", and "Create prevention rule".
- Middle Window:** Endpoint Agents - Exclusions. It lists "KPSN reputation database" and "Notifications" under "Exclusions". A modal window titled "New rule" is open, showing the "Criteria" dropdown set to "MDS" and a "Value" input field containing "MDS".
- Bottom Window:** Endpoint Agents - Scan tab. It shows the same "Exclusions" list and includes tabs for "IDS", "TAA", and "ICAP". The "IDS" tab has a table with one row: "Exclusions apply only to this Centre Node server" with criteria "MDS" and value "32e92d0160be1c23715ee10ca4f73121".

119

Исключения можно сделать по критериям:

- MD5
- Формат
- Маска URL
- Адрес получателя
- Адрес отправителя
- IP или подсеть источника
- IP или подсеть назначения
- Агент пользователя

При появлении ложных срабатываний на определенные файлы, можно создать правило исключений из проверки. В данном правиле могут использоваться критерии:

- MD5,
- Формат,
- Маска URL,
- Email получателя,
- Email отправителя,
- IP или подсеть источника,
- IP или подсеть назначения,
- Агент пользователя.

Исключения объектов из проверки ICAP

The screenshot shows the 'Alerts' section of the Kaspersky Anti Targeted Attack Platform. A modal window titled 'New rule' is open, prompting the user to select criteria for creating an exclusion from ICAP traffic scanning. The 'Criteria' dropdown is set to 'MD5' and the 'Value' field contains the hash value '52e92d0160be123715ee10ec4f75121'. To the right of the modal, a context menu for the selected MD5 value (52e92d0160be123715ee10ec4f75121) is displayed, with the option 'Create prevention rule' highlighted.

120

Исключения можно сделать по критериям:

- Формат
- MD5
- Маска URL
- IP или подсеть источника
- IP или подсеть назначения
- Агент пользователя

Исключения для ICAP-объектов можно сделать по критериям:

- Формат,
- MD5,
- Маска URL,
- IP или подсеть источника,
- IP или подсеть назначения,
- Агент пользователя.

Скачать трафика с центрального узла

121

The screenshot shows the 'Sensor servers' section of the Kaspersky Anti Targeted Attack Platform. On the left, there's a sidebar with navigation links like Dashboard, Alerts, Threat Hunting, Tasks, Prevention, Custom rules, Storage, Endpoint Agents, Reports, Settings, and Sensor servers. The main area shows a table of sensor servers, with one entry for 'localhost' labeled 'Central Node'. To the right, a modal window titled 'Traffic downloading' is open, showing configuration options for traffic capture. It includes fields for 'Period*', 'Maximum dump size*', 'BPF traffic filter', and 'Filtering rule'. At the bottom right of the modal are 'Download' and 'Cancel' buttons.

При скачивании трафика **можно указать:**

- Временной промежуток
- Максимальный размер файла
- Фильтры

Вы можете скачать копию хранимого трафика в виде PCAP-файлов используя веб-интерфейс решения. При скачивании следует указать:

- Временной промежуток,
- Максимальный размер файла,
- Правила фильтрации.

Скачать трафика с центрального узла

122

The screenshot shows a terminal session on a KATA host. The user runs several Docker commands to inspect volumes and copy a PCAP file from a container. The commands shown are:

```

root@l.srv.node1.node.dyn.kata:~# docker ps | grep span
8f403a0723be    registry.kata.app.ru:5000/kaspersky/network_agent/preprocessor:5le64a0
bin/sh -c "/entryp_"
  9 days ago   Up 9 days
    kata_product_main_1_preprocessor_span.l.ydob591sttp4xclhvv94nx5qr
root@l.srv.node1.node.dyn.kata:~# docker exec -it 8f403a0723be sh
# cd /mnt/kaspersky/nta/dumps
# ls
2023_2a6b-342f-20c9-14ac.pcap

```



```

root@l.srv.node1.node.dyn.kata:/data/volumes/dumps# docker inspect -f '{.Mounts}' 8f403a0723be
[{"volume": "kata_product_preprocessor_span_storage_pcaps_1", "/mnt/kaspersky/nta/dumps": {"local-persist": true}}
root@l.srv.node1.node.dyn.kata:/data/volumes/dumps# docker volume inspect kata_product_preprocessor_span_storage_pcaps_1
[
  {
    "CreatedAt": "2023-01-01T00:00:00Z",
    "Driver": "local-persist",
    "Labels": {
      "com.docker.stack.namespace": "kata_product_main_1"
    },
    "Mountpoint": "/data/volumes/dumps",
    "Name": "kata_product_preprocessor_span_storage_pcaps_1",
    "Options": {
      "mountpoint": "/data/volumes/dumps"
    },
    "Scope": "local"
  }
]
root@l.srv.node1.node.dyn.kata:/data/volumes/dumps# cd /data/volumes/dumps
root@l.srv.node1.node.dyn.kata:/data/volumes/dumps# ls
2023_2a6b-342f-20c9-14ac.pcap
root@l.srv.node1.node.dyn.kata:/data/volumes/dumps#

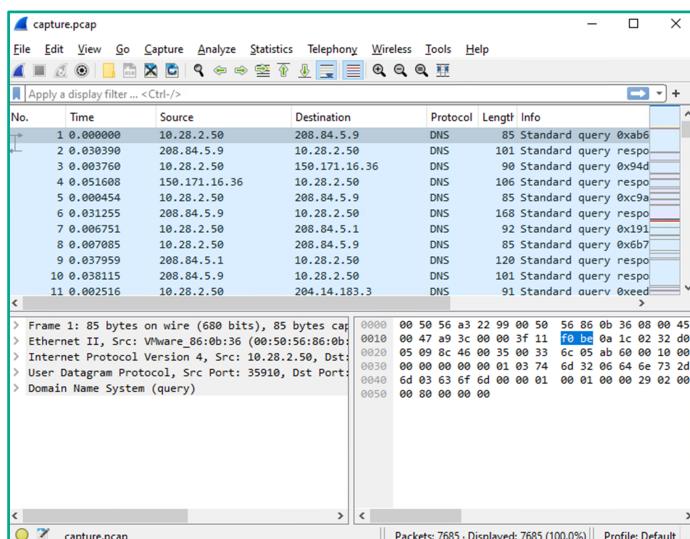
```

Так же **PCAP-файлы** можно скачать напрямую из контейнера **preprocessor** или с самого **Центрального узла**

Вы так же можете скачать копию трафика из контейнера preprocessor или директории этого контейнера на файловой системе узла.

Анализ трафика

123



Трафик можно анализировать в стороннем ПО

Скачанные PCAP-файлы можно анализировать в стороннем программном обеспечении. Это удобно, если вы хотите вручную найти определенные данные и использовать их для написания собственных правил фильтрации или индикаторов компрометации.

Дополнительная информация об артефактах в обнаружении

124

Если обнаружение относится к файлу или URL, сотрудник службы безопасности может легко найти дополнительную информацию об этом объекте на портале Threat Intelligence Лаборатории Касперского.

Перейти на портал Threat Intelligence можно через контекстное меню хеша MD5 или SHA256. Для доступа к порталу нужна специальная аутентификация по имени пользователя и

сертификату, поскольку доступ предоставляется только по платной подписке.

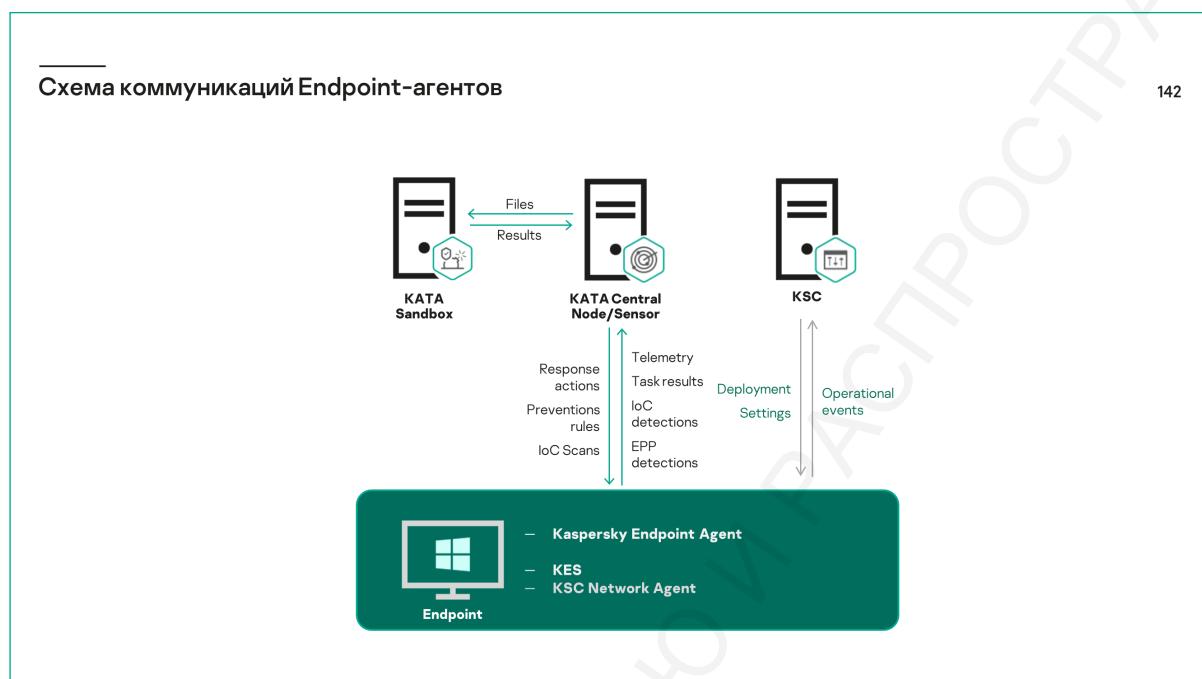
На портале можно найти разнообразную информацию о файле с заданной контрольной суммой. В каких регионах он был замечен, когда, под какими именами и в каких папках. Если это исполняемый файл, то какие процессы его чаще всего запускали, и какие процессы запускал он. Все это может помочь понять, опасный это файл или нет. Информацию на портале можно использовать для поиска признаков компрометации, связанных с обнаруженным файлом.

The screenshot shows two main windows. On the left is the 'All alerts' interface with a sidebar containing navigation links like ABC core, Dashboard, Alerts (with 3 notifications), Threat Hunting, Tasks, Prevention, Custom rules, Storage, Endpoint Agents, Reports, and Settings. The main area displays an alert titled 'Event details #25' with status 'Closed', importance 'High', and a data source 'SMTP Sensor 127.0.0.1, received from'. It includes sections for 'Object information' (sender email, recipient email, original recipient email, server IP, subject, headers) and 'Scan results' (Test smtp processing, Officekit, Download). On the right is a separate window titled 'kaspersky THREATS' showing a threat analysis for 'DANGEROUSOBJECT.ACAD.EICAR-TEST-FILE'. It lists 'Solutions for' categories: Home Products, Small Business 1-50 employees, Medium Business 51-999 employees, and Enterprise 1000+ employees. The threat details include 'Class: DangerousObject', 'Platform: Acad', and a 'Description' section explaining EICAR is a benign file detected as a virus. The description notes it's a short 68-byte COM file that displays a message and returns control to the host program, and it was created to demonstrate how anti-virus programs handle real viruses.

Так же информация о проверяемых файлах доступна на портале Kaspersky Threats(<https://threats.kaspersky.com/>).

Глава 5. Установка Endpoint-агента

5.1. Типы Endpoint-агентов



В решении Kaspersky EDR Expert Центральный узел получает от Endpoint-агентов телеметрию для анализа и посыпает им команды реагирования от имени сотрудника службы безопасности. Но инструментов для удаленной установки, активации и настройки Endpoint-агентов у Центрального узла нет. Для развертывания и управления Endpoint-агентами можно воспользоваться средством централизованного управления, к примеру Kaspersky Security Center, или разворачивать Endpoint-агенты и управлять ими локально.

Варианты Endpoint-агентов для работы с KEDR:

- Kaspersky Endpoint Agent
- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac

Принципы установки и управления различными Endpoint-агентами в целом схожи, в данном курсе остановимся на общих моментах, а также на некоторых важных нюансах для различных типов Endpoint-агентов. Более подробная информация об установке, настройке, подключению к центральному узлу доступно в онлайн справке к соответствующим продуктам.

Как Endpoint-агент пересыпает телеметрию для анализа.

События телеметрии поступают от компьютеров почти непрерывно. Отправка событий регулируется политикой или локальными настройками Endpoint-агента, если компьютер не управляемся через KSC.

В политике соответствующие параметры находятся в различных разделах, в зависимости от типа Endpoint-агента. Сами параметры это:

- Event transmission period (sec) — задает максимальный интервал между последовательными сеансами передачи событий и по умолчанию имеет значение 30 секунд. Если после предыдущего сеанса передачи событий прошло 30 секунд, Endpoint-агент начинает новый сеанс передачи событий.
- Event limit per package — задает максимальное количество событий в буфере на отправку и по умолчанию имеет значение 1024 события. Как только в буфере накапливается 1024 события, Endpoint-агент начинает новый сеанс передачи событий (даже если 30 секунд после прошлого сеанса еще не прошло).

Иными словами, Endpoint-агент начинает новый сеанс отправки событий при выполнении любого из двух условий: либо после завершения предыдущего сеанса прошло больше, чем Event transmission period, либо в буфере на отправку накопилось число событий, равное Event limit per package.

События также записываются в очередь отправки, которая хранится на диске в папке с данными Endpoint-агента. Таким образом, если связи с Центральным узлом нет, события накапливаются в очереди. При восстановлении связи Endpoint-агент отправляет события из очереди в хронологическом порядке: сначала старые, потом более новые.

Настройки по умолчанию не гарантируют доставку всех собранных локально событий на Центральный узел. Приоритет отдается бесперебойности работы Центрального узла, который может оказаться перегружен слишком большим потоком телеметрии. Если на компьютере происходит слишком много событий, часть из них может быть отброшена самим Endpoint-агентом.

Для установки и управления работой Endpoint-агентов предназначен Kaspersky Security Center. Это не значит, что без KSC развернуть и настроить Endpoint-агенты нельзя, но с помощью KSC это делать значительно проще.

Kaspersky Security Center позволяет:

- Создавать инсталляционные пакеты для Kaspersky Endpoint Agent и Kaspersky Endpoint

Security.

- Удаленно устанавливать Endpoint-агенты.
- Активировать Endpoint-агенты ключом или кодом активации.
- Распространять на Endpoint-агенты настройки подключения к центральному узлу.
- Получать от Endpoint-агентов события об их работе и состоянии.

Kaspersky Security Center даже дублирует часть функций реагирования, к примеру можно создавать и выполнять задачи поиска индикаторов компрометации.

Установка средства сбора телеметрии

127

	Через Kaspersky Security Center	Без Kaspersky Security Center
Удаленно	<ul style="list-style-type: none">▪ Задачей установки отдельного пакета Kaspersky Endpoint Agent▪ Задачей установки Kaspersky Endpoint Security for Windows/Linux/Mac	<ul style="list-style-type: none">▪ Из MSI-пакета с помощью GPO или другой системы распространения ПО
Локально	<ul style="list-style-type: none">▪ Из автономного пакета Kaspersky Endpoint Agent или Kaspersky Endpoint Security for Windows/Linux/Mac	<ul style="list-style-type: none">▪ Из MSI-пакета с помощью мастера установки▪ Из MSI-пакета через командную строку

Установить Kaspersky Endpoint Agent возможно как удаленно через KSC, так и отдельно из MSI-пакета локально или удаленно. Даже если в компании не используется KSC, то его целесообразно развернуть для распространения Endpoint-агента. KSC не требует приобретения дополнительных лицензий.

5.2. Установка средствами Kaspersky Security Center

Пакет установки для Kaspersky Security Center

Discovery & deployment / Deployment & assignment / Installation packages

Downloaded In progress (0)

+ Add × Delete ⌘ Refresh + Deploy View the list of stand-alone packages

Current application versions

Group by: Operating system (change grouping using filter)

Category	Type	Name	Version	Enabled	Operating system
Embedded systems	Web plug-in	Kaspersky Embedded Systems Security 3.3 for Windows	3.3.0.87	Yes	Windows
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (12.3.0) (English) (Lite encryption)	12.3.0.493	Yes	Windows
> Linux					
< macOS					
Workstations	Administration	Kaspersky Network Agent for Mac (English)	15.0.0.9323	Yes	
Workstations	Distribution package	Kaspersky Endpoint Security for Mac (English)	12.0.0.325	Yes	
Workstations	Plug-in	Kaspersky Endpoint Security for Mac Administration Plugin 12.0	12.0.0.25	Yes	
Workstations	Web plug-in	Kaspersky Endpoint Security for Mac Web Console Plugin 12.0	12.0.0.28	Yes	

Kaspersky Endpoint Agent 3.16 (English) ×

Area to secure Workstations
Type Distribution package
In use in managed network No
Version 3.16.0.195
Added 12/13/2023 5:00:01 am
Operating system Windows

Kaspersky Endpoint Security 12.0 for Linux (English) ×

Area to secure Workstations
Type Distribution package
In use in managed network Yes
Version 12.0.0.6672
Added 12/13/2023 5:00:01 am
Operating system Linux
Language en
Download complete

Download and create installation package

Чтобы централизованно установить один из возможных вариантов Endpoint-агентов с использованием Kaspersky Security Center, нужно использовать задачу или мастер удаленной установки.

В Kaspersky Security Center есть много способов запустить мастер удаленной установки и его шаги будут немного отличаться в зависимости от контекста. Подробности можно найти в курсе KL 002 Kaspersky Endpoint Security and Management или в документации Kaspersky Security Center.

Здесь рассмотрим, как установить Endpoint-агент на компьютер, предполагая, что на этом компьютере уже есть Агент администрирования Kaspersky Security Center, который необходим для связи Endpoint-агента и Kaspersky Security Center.

Детали установки и работы с Агентом администрирования Kaspersky Security Center
можно прочитать в справке по ссылке <https://support.kaspersky.com/KSC/14.2/ru-RU/3305.htm> либо в курсу kl002.

Для начала мы загрузим выбранный пакет в Kaspersky Security Center.

Добавьте плагин в веб-консоль Kaspersky Security Center

129

The screenshot shows the 'Discovery & deployment / Deployment & assignment / Installation packages' interface. On the left, a sidebar includes 'Deployment & assignm...', 'Moving rules', 'Protection deployment wiz...', 'Quick start wizard', 'Installation packages' (selected), 'Device selections', 'Marketplace', and 'Settings'. The main area displays a table of current application versions, including various Kaspersky products like Embedded systems, Workstations, and Distribution packages. A detailed view of 'Kaspersky Endpoint Agent 3.16' is shown in a modal window, with an 'Install plug-in' button at the bottom right.

Далее необходимо добавить соответствующий плагин. Это позволит создавать политики управления Endpoint-агентом.

Создайте задачу удаленной установки

130

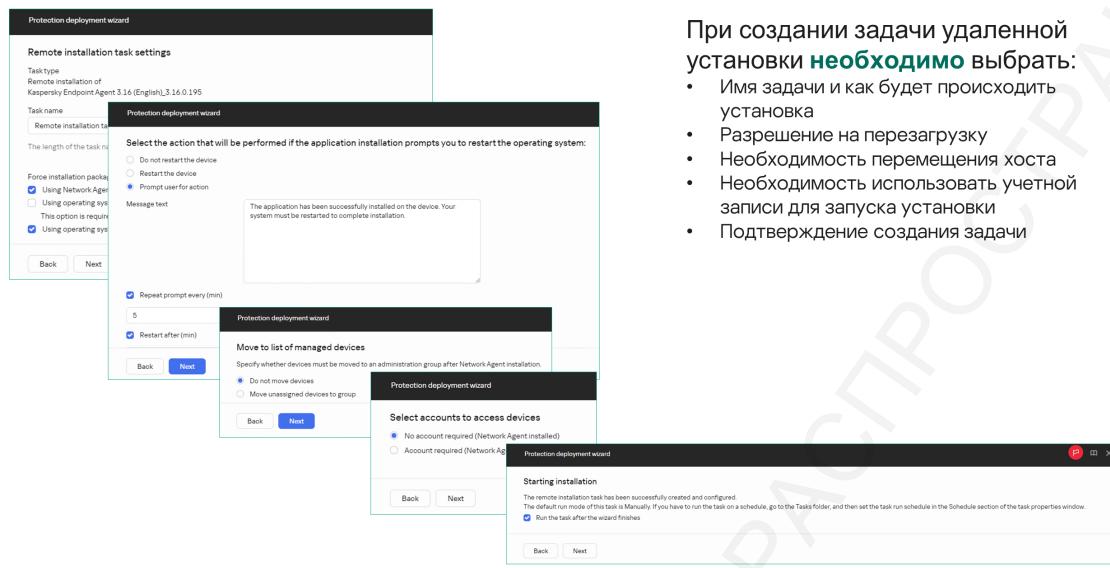
The screenshot shows the 'Protection deployment wizard' process. Step 1: 'Select the deployment method for the selected installation package' (radio buttons for 'Using the remote installation task' and 'Using a stand-alone package'). Step 2: 'Protection deployment wizard' (checkboxes for 'Installation packages', 'Devices', 'IP range', and 'IP addresses'). Step 3: 'Properties: Kaspersky Endpoint Security for Mac (English) 12.0.0.325' (tabbed view: General, Settings, Stand-alone packages, Revision history). Under 'Packages to install', several checkboxes are checked, including 'Scan', 'Endpoint Detection and Response', 'File Threat Protection', 'Web Threat Protection and Web Control', and 'Network Threat Protection'. A note at the bottom states: 'Есть небольшие **различия** в задачах в зависимости от выбранной **операционной системы**'.

Необходимо создать задачу для удаленной установки Endpoint-агентов. При создании задачи удаленной установки необходимо выбрать: * Пакет установки, * Способ распространения, * Агент администрирования, * Целевой узел.

Настройки задач различаются в зависимости от выбранной операционной системы и типа Endpoint-агента.

Создайте задачу удаленной установки

131

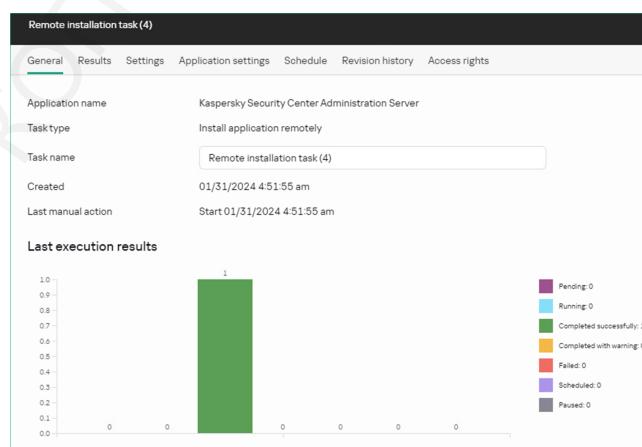


При создании задачи удаленной установки необходимо выбрать:

- Имя задачи и как будет происходить установка
- Разрешение на перезагрузку
- Необходимость перемещения хоста
- Необходимость использовать учетной записи для запуска установки
- Подтверждение создания задачи

Результат выполнения задачи удаленной установки

132



В результате успешной установки приложение появится в списке управляемых приложений в свойствах компьютера в консоли Kaspersky Security Center.

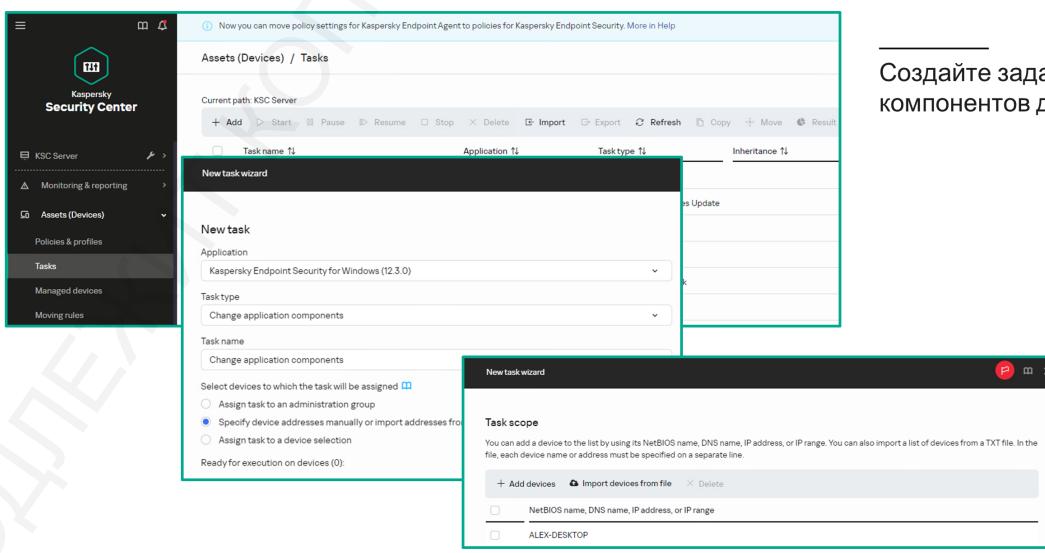
В свойствах управляемого компьютера в консоли Kaspersky Security Center можно:

- Отобразить события Endpoint-агентов кнопкой **Events**. События могут помочь в выяснении причин некорректной работы. События работы Endpoint-агентов доступны только в Kaspersky Security Center, и не доступны в веб-консоли Центрального узла Kaspersky Endpoint Detection and Response.
- Посмотреть настройки Endpoint-агентов можно в разделе **Applications | <Выбранный тип агента> | Application Settings**. В свойствах Endpoint-агента стоит обратить внимание на раздел Components, где необходимо найти модуль, отвечающий за взаимодействие с Центральным узлом Kaspersky Endpoint Detection and Response. В KES это Endpoint Detection and Response (KATA), в других Endpoint-агентах наименование модуля может отличаться. После того, как вы настроите подключение к центральному узлу и активируете Endpoint-агент лицензионным ключом, этот модуль должен будет перейти в запущенное состояние.
- Остановить и запустить Endpoint-агент можно кнопками сверху от списка в разделе Applications. Чтобы остановить или запустить Endpoint-агент сразу на нескольких компьютерах, используйте задачу KSC: Start or stop application.

Чтобы отобразить события Endpoint-агентов от всех (или некоторых) компьютеров, создайте выборку событий на вкладке **Monitoring & Reporting | Event Selections** веб-консоли Kaspersky Security Center, и настройте подходящие условия фильтрации событий.

Если у вас уже установлен и используется KES

133



Создайте задачу смены компонентов для KES

В случае, если у вас уже установлен и используется Kaspersky Endpoint Security, то вы можете доустановить модуль сбора телеметрии. Для этого создайте задачу смены компонентов для KES.

Установка компонента Endpoint Detection and Response (KATA) в составе KES

134

В свойствах **задачи** указываем необходимость установки **компонента Endpoint Detection and Response (KATA)**

В свойствах задачи укажите необходимость установки компонента Endpoint Detection and Response (KATA).

Создайте политику управления

135

Для КЕА политика не создается по умолчанию, ее должен создать администратор

Нужен плагин для KES или KEA:

- Доступен для загрузки стандартными средствами из инфраструктуры «Лаборатории Касперского»
- Доступен для установки из файлов, входящих в поставку KES или KEA для автономной установки

Чтобы настроить параметры подключения к центральному узлу через Kaspersky Security Center, нужно создать политику управления Endpoint-агентами. Для KEA автоматически она не создается, ее должен создать администратор вручную.

Чтобы настроить подключение для всех Endpoint-агентов, достаточно одной политики в узле Managed devices. Если же вы установили второй (третий и т.д.) Центральный узел и хотите переподключить только часть Endpoint-агентов к новому адресу, выделите их в отдельную группу на сервере KSC и создайте политику для этой группы.

Чтобы создать политику KEA или KES, в консоли KSC должен быть установлен плагин управления.

Проверить, что плагин установлен можно в свойствах узла Сервера администрирования в разделе **Console Settings | Web Plug-ins**.

Если плагин не установлен, его можно установить через интерфейс загрузки новых версий приложений в консоли KSC:

- Откройте раздел **Console Settings | Web Plug-ins** в боковом меню слева;
- Нажмите кнопку **Add** и выберите необходимый плагин;
- Установите плагин нажав кнопку **Install plug-in**.

После того как плагин установлен, создайте политику управления:

- В боковом меню откройте **Devices | Policies and profiles** и выберите требуемую группу устройств;
- Запустите мастер создания политики кнопкой **Add**;
- Выберите в списке приложение соответствующее типу используемого Endpoint-агента;
- **Выберите Endpoint Detection and Response Expert (KATA EDR)**;
- Дайте политике узнаваемое имя;
- Укажите, что создаете активную политику и отметьте флаг **Policy status – Active**.

Только настройки активных политик распространяются на компьютеры. Неактивные политики можно использовать как шаблоны. Вы всегда можете открыть свойства политики вручную и всегда можете изменить статус политики с активной на неактивную или наоборот.

Настройте подключение к центральному узлу

136

Обязательные параметры

- Переключатель в положении **Enforce**
- Параметр **Enable KATA integration** включен
- Адрес и порт сервера (центрального узла или сенсора) заданы верно

Опциональные параметры

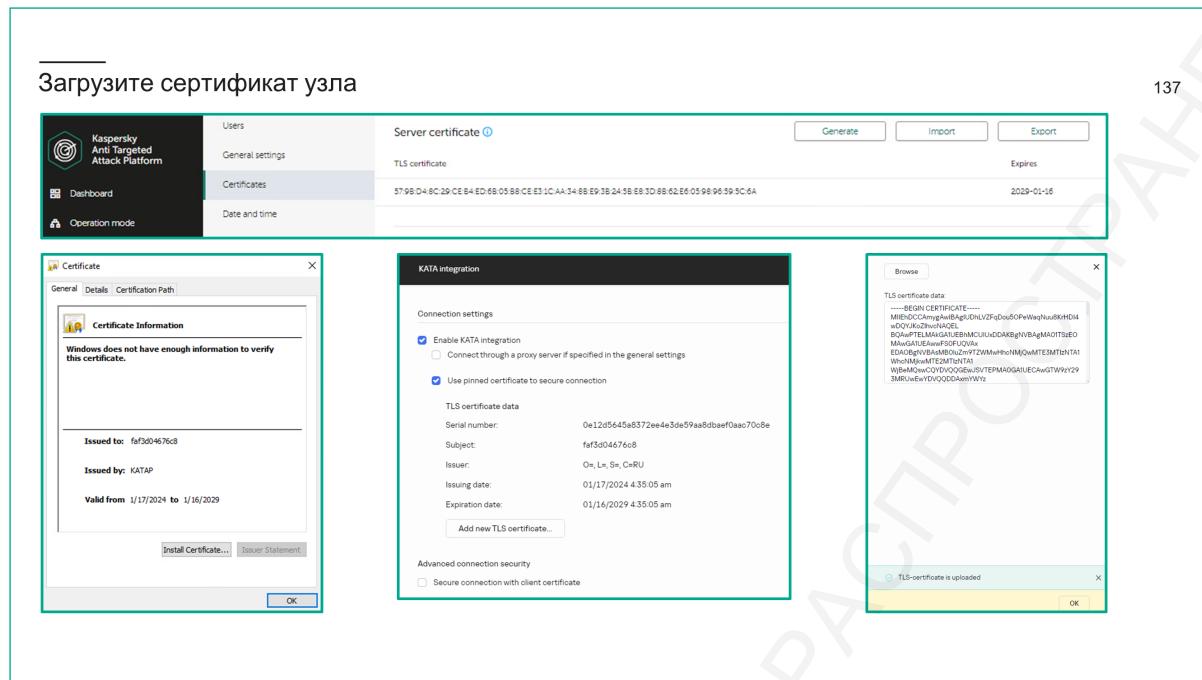
- Добавить сертификат **центрального узла**
- Добавить сертификаты **клиентских узлов**

Чтобы настроить подключение Endpoint-агентов к центральному узлу:

- Откройте окно свойств политики управления КЕА или КЕС;
- Перейдите в соответствующий раздел Telemetry Collection servers | KATA integration;
- Отметьте параметр Enable KATA integration;
- Ведите адрес Центрального узла в поле List of KATA servers; Можно вводить как IP-адрес, так и DNS-имя. Порт подключения в большинстве случаев менять не нужно. Он по умолчанию имеет значение 443 и в настройках Центрального узла и в политике Endpoint-агента.
- Сохраните настройки политики.

Предварительно полезно проверить, что переключатель в правом верхнем углу окна находится в положении Enforce со значком закрытого замка. Если он находится в положении Undefined, настройки не применяются.

Это все, что нужно задать в политике, чтобы Endpoint-агенты подключились к центральному узлу и отобразились в его веб-консоли.



Центральный узел может принимать защищенные соединения от Endpoint-агентов. В свою очередь Endpoint-агенты устанавливают защищенные соединения только с доверенным Центральным узлом. Это защищает Endpoint-агенты от команд реагирования из нелегитимных источников.

Чтобы Центральный узел считался доверенным, сертификат Центрального узла должен совпадать с сертификатом, заданным в настройках Kaspersky Endpoint Agent.

Адрес и сертификат узла можно задать политикой Kaspersky Security Center или запуском утилиты agent.exe с параметрами.

Скачать сертификат Центрального узла можно в веб-интерфейсе в разделе Settings | Certificates | Server Certificate.

После этого в политике KEA в разделе Telemetry Collection servers | KATA integration нужно выбрать Use pinned certificate to secure connection и добавить скачанный сертификат. В политике отобразится информация о данном сертификате.

Создайте или загрузите на сервер агентский сертификат

138

Сервер генерирует сертификат и **секретный ключ** в формате PFX **без пароля**

Можно иметь **несколько разных** сертификатов для разных групп **клиентов**

При обычном подключении Центральный узел при этом принимает соединения от любых Endpoint-агентов.

Эту схему можно сделать более безопасной, если включить проверку агентского сертификата Центральным узлом. В этом случае не только Endpoint-агент будет проверять подлинность сертификата Центрального узла, но и Центральный узел будет проверять подлинность сертификата, с которым подключается Endpoint-агент. И в результате Центральный узел не будет принимать соединения от незнакомых ему Endpoint-агентов (т.е. от агентов, которые подключаются с неизвестным сертификатом).

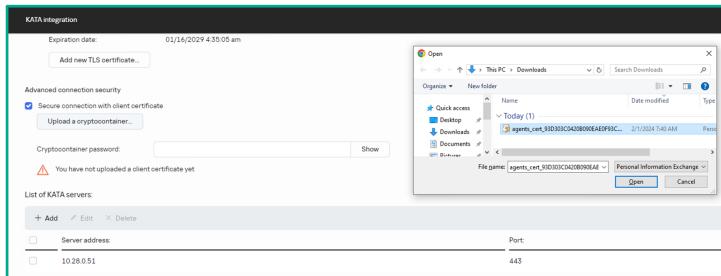
Чтобы использовать такой режим подключения, его нужно синхронно включить на центральном узле и в настройках Endpoint-агентов. По умолчанию этот режим выключен и там, и там.

Дополнительно нужно создать сертификат для Endpoint-агентов (сертификат и секретный ключ к нему), после чего синхронно указать этот сертификат в настройках Центрального узла и в настройках Endpoint-агентов. В этой схеме Endpoint-агенты используют один и тот же сертификат.

Скачать клиентский сертификат можно в веб-интерфейсе Центрального узла в разделе **Settings | Certificates | Endpoint Agent Certificates**. Сертификат будет скачан в формате pfx.

Добавьте агентский сертификат в политику

139



Пароль может быть нужен для сертификатов, сгенерированных сторонними средствами

Включите параметр

- Secure connection with client certificate**

Загрузите PFX-сертификат кнопкой

- Upload your crypto container**

Получите сообщение

- Client certificate successfully uploaded**

После этого в политике управления в разделе Telemetry Collection servers | KATA integration нужно выбрать Secure connection with client certificate и добавить скачанный сертификат.

Защита от вмешательства в работу КЕА-агентов

140

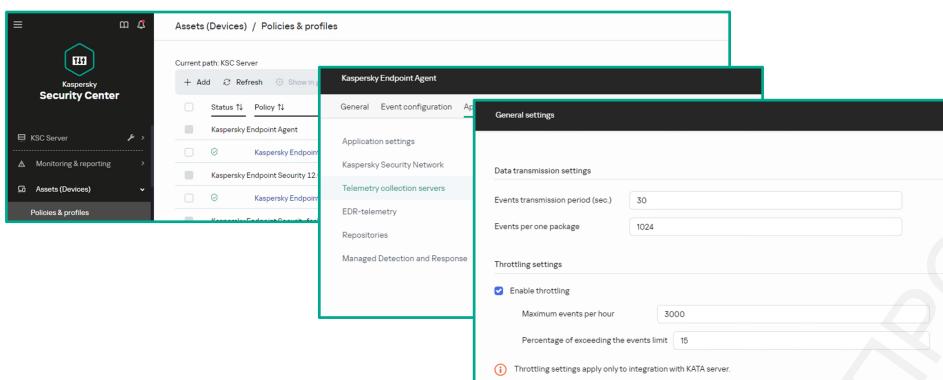
Задайте пароль на использование утилиты **agent.exe**

Права пользователей **по умолчанию** разрешают доступ к служебным файлам агента только учетной записи **службы агента** и учетной записи **локальной системы**

Так как утилита agent.exe в составе Kaspersky Endpoint Agent обладает широким функционалом, то хорошей практикой является защитить её паролем. Для этого необходимо открыть политику КЕА, перейти в раздел Application Settings | Application settings | Security settings и выбрать Apply password protection, после чего задать пароль.

Throttling

141



Функция регулирования количества запросов позволяет **ограничить** поток событий **низкой важности** от Kaspersky Endpoint Agent к компоненту Центрального узла

Функция регулирования количества запросов позволяет ограничить поток событий низкой важности от Kaspersky Endpoint Agent к компоненту Центрального узла.

Это поведение регулируется настройками политики КЕА в том же разделе KATA integration | General settings в секции Throttling settings:

- Event throttling — флаг, включающий или выключающий отброс «лишних» событий; по умолчанию включен.
- Maximum events per hour — максимальное количество событий в час, по умолчанию равно 3 000 событий. Все события, превышающие этот лимит, будут отброшены.
- Percent of exceeding the limit of events — максимальная доля событий одной категории, по умолчанию равно 15%. Если доля каких-то событий превышает указанный порог, все остальные события этой же категории начинают отбрасываться (пока доля категории не уменьшится по мере сбора событий других категорий).

Категории событий можно найти в онлайн-справке или отобразить командой:

```
agent.exe --message-broker stats:
-
- AccountLogon,
- ConsoleInput,
- FileChange,
- HttpRequest,
- HttpResponse,
- ListenPort,
- LoadImage,
- NetworkConn (Network connection),
- ProcessCreate,
- ProcessExit,
- ProcessTkChange (Process token change),
```

- AllThreatDtkt (KES Detections),
- WinEventLog,
- WinRegistry.

Если при анализе истоков подозрительных событий в Threat hunting явно не хватает событий для восстановления полной картины произошедшего, это может быть результатом настройки Event throttling. Попробуйте увеличить общий лимит или относительный лимит для событий одной категории. На компьютерах, не управляемых Kaspersky Security Center, это можно сделать через утилиту agent.exe.

Задача обновления агентов
142

The screenshot shows the Kaspersky Security Center interface. On the left, the navigation pane includes 'Assets (Devices)', 'Monitoring & reporting', 'Policies & profiles', and 'Tasks'. Under 'Tasks', there's a list of existing tasks like 'Task name T1' (Kaspersky Endpoint Security 12.0 for Linux), 'Malware Scan', 'System Integrity Check', 'Update', 'Critical Areas Scan', and 'Kaspersky Endpoint Security for Windows (12.3.0)'. A 'New task wizard' dialog is open in the center, titled 'New task'. It shows the 'Application' field set to 'Kaspersky Endpoint Agent' and the 'Task type' field set to 'Databases and Modules Update'. In the 'Task name' field, 'Databases and Modules Update' is entered. Below this, there are options for selecting devices: 'Assign task to an administration group' (selected) and 'Specify device addresses manually or import addresses from a list'. At the bottom of the wizard is a 'Next' button. To the right of the wizard, a 'Databases and Modules Update' configuration window is open, showing the 'Schedule' tab. This tab has a 'Run by schedule' toggle switch turned on, a 'Frequency' dropdown set to 'Every day', and a 'Every' field with '1 day(s)'. The 'Start time' is set to '00:44' and the 'Start date' is '2/1/2024'.

Обновляет

- Фильтры для сбора телеметрии
- Параметры подключения к KSN

По умолчанию не создается для KEA

- Создайте вручную
- Назначьте регулярное расписание

Мы рекомендуем создать задачу обновления Endpoint-агентов. Эта задача обновляет:

- Фильтры для сбора телеметрии.
- Параметры подключения к KSN.

По умолчанию для Endpoint-агентов типа Kaspersky Endpoint Agent она создается. Рекомендуем создать ее вручную и назначить регулярное расписание.

Ожидаемый результат успешной установки агентов

143

Отчет об установленных приложениях Лаборатории Касперского

The screenshot shows a report titled 'Report on Kaspersky software versions' from February 1, 2024, at 12:14:23 AM. It lists the current versions of Kaspersky software installed for a single group: 'Managed devices'. A chart displays the number of devices for each version. A modal dialog box is open, titled 'Filter enabled', with the condition set to 'Equal' and the value set to 'Kaspersky Endpoint Agent'.

Application	Version number	Number of devices	Number of groups
Kaspersky Endpoint Agent	3.16.0.195	1	1

Отфильтруйте отчет по приложению:

- Kaspersky Endpoint Agent
- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux

Вы можете создать отчет об установленных приложениях, чтобы получить текущую картину состояния установки Endpoint-агентов на компьютеры организации. Отчет можно фильтровать по типу желаемого Endpoint-агента:

- Kaspersky Endpoint Agent.
- Kaspersky Endpoint Security for Windows.
- Kaspersky Endpoint Security for Linux.
- Kaspersky Endpoint Security for Mac.

Распространите лицензионный ключ через Kaspersky Security Center

144

The screenshot shows the 'Operations / Licensing / Kaspersky licenses' section of Kaspersky Security Center. A license key dialog box is open, displaying details for license key '11A4-0007B8-577A1AC5'. The dialog includes tabs for General, Devices, About the client, Technical Support, and Limits. The General tab shows the license key, name ('Kaspersky Endpoint Detection and Response Advanced International Edition, 10-14 Node 1 year RPR License KEDR'), type ('Commercial'), term (367 days), expiration date (07/26/2024 5:00:00 pm), end date of license key (07/26/2024 5:00:00 pm), limit (10), and status ('Not in use'). There is also a checkbox for 'Automatically distribute license key to managed devices'.

Ключ/код автоматически распространяется на все узлы во время плановых синхронизаций агента Kaspersky Security Center с сервером Kaspersky Security Center

В Kaspersky Security Center есть и другие способы распространить ключ

- Распространить ключ отдельной задачей Kaspersky Endpoint Agent типа Activation of Application
- Добавить ключ в инсталляционный пакет перед установкой

Чтобы активировать Endpoint-агент через Kaspersky Security Center можно использовать один из следующих методов:

- Включить функцию автоматического распространения; Так ключ будет установлен на все управляемые компьютеры;
- Распространить ключ специальной задачей установки ключа; Так можно контролировать, на какие компьютеры будет распространен ключ;
- Добавить ключ в инсталляционный пакет перед установкой; Так Endpoint-агент будет активирован сразу после установки. Это метод хорошо подходит при первоначальном развертывании, но не очень подходит для замены устаревшего ключа.

Во всех трех случаях сначала нужно добавить ключ в хранилище ключей Лаборатории Касперского на сервере администрирования KSC:

- Выбрать в консоли KSC в боковой панели Operations | Licensing | Kaspersky Licenses;
- Нажать кнопку Add | Add key file;
- Кнопкой Select key file указать файл ключа;

Здесь же можно включить автоматическое распространение ключа на управляемые компьютеры флагом Automatically distribute license key to managed devices. Этот же флаг можно установить или снять позже в свойствах ключа.

Ключ, для которого включено автоматическое распространение, будет автоматически доставлен на все компьютеры, подключенные к серверу администрирования, на которых есть соответствующий компонент (Kaspersky Endpoint Agent или Kaspersky Endpoint Security). Распространение ключа происходит по мере синхронизаций Агента администрирования KSC с сервером KSC (по умолчанию раз в 15 минут).

Автоматическое распространение не приводит к замене ранее установленного ключа новым ключом, если старый ключ еще действителен.

Автоматическое распространение легче всего настроить, но оно не обладает гибкостью. Если нужно именно заменить ранее установленный ключ новым ключом, при том, что старый ключ еще не истек, или если нужно адресно установить ключ только на некоторые выбранные компьютеры, автоматическое распространение ключа не подходит.

Когда может понадобиться установить ключ только на некоторые компьютеры? Это может быть нужно поставщику услуг, который обслуживает сразу несколько клиентов. В этом случае у него будет несколько лицензий по одной для каждого заказчика и ему важно активировать Endpoint-агент на компьютерах заказчика лицензией этого заказчика. KSC предоставляет несколько

способов решить эту проблему и один из них — это использовать задачи установки ключа, в которых можно задать список целевых компьютеров.

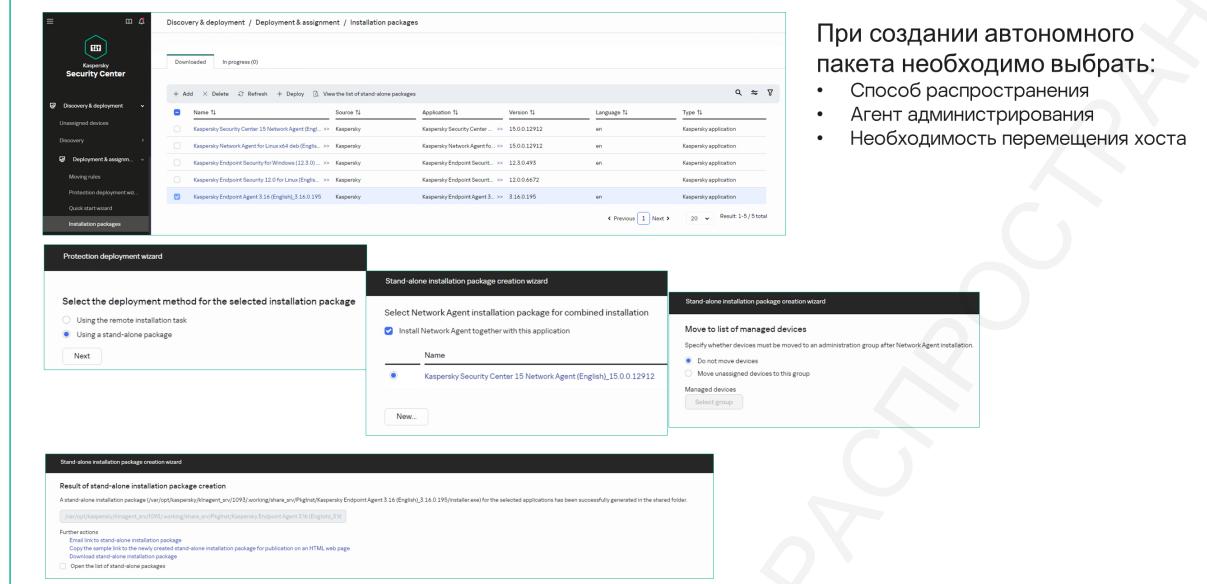
Чтобы установить ключ задачей:

- Выберите Devices | Tasks в дереве объектов KSC.
- Создайте новую задачу кнопкой Add.
- В мастере выберите тип задачи Activation of application для соответствующего приложения.
- Выберите компьютеры, на которых нужно активировать приложение. Здесь можно либо выбрать индивидуальные компьютеры из структуры управляемых компьютеров KSC (верхняя кнопка), либо выбрать какую-то группу компьютеров целиком (нижняя кнопка), либо задать компьютеры по именам или IP-адресам (средняя кнопка).
- Выберите Activate with a key file or key и затем выберите ключ с помощью кнопки Select. Ключ можно выбрать как из хранилища сервера администрирования, так и непосредственно с диска, указав путь к файлу. Мастер проверяет, подходит ли ключ выбранному приложению, и не истек ли его срок действия. Создать задачу с неподходящим ключом нельзя. На этом же шаге можно установить флаг Add this key as an additional. Это механизм для обеспечения беспрерывной работы Endpoint-агента, когда срок действия старого ключа заканчивается. Если заранее установить новый ключ в качестве дополнительного, Endpoint-агент продолжит использовать старый ключ до самой даты окончания и затем сразу начнет использовать дополнительный ключ.
- Завершите создание задачи, запустите ее и дождитесь результатов.

Еще одна возможность активировать приложение с помощью Kaspersky Security Center — это поместить ключ в инсталляционный пакет.

Установка из автономного пакета

145

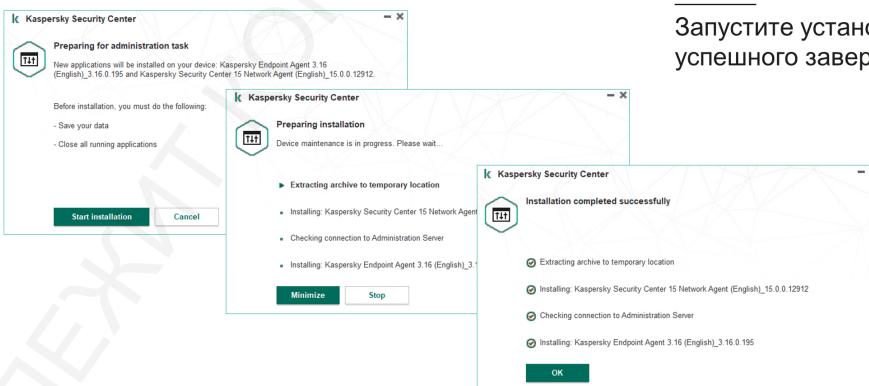


Автономный инсталляционный пакет представляет собой исполняемый файл (installer.exe), который можно разместить на Веб-сервере, в общей папке или передать на клиентское устройство другим способом. Можно также отправить ссылку на автономный инсталляционный пакет по электронной почте. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки программы без участия Kaspersky Security Center. Чтобы установить Endpoint-агент из автономного пакета необходимо сначала сформировать автономный пакет, используя KSC, после чего необходимо доставить данный пакет на хост и запустить установку.

Установка из автономного пакета для Windows

146

Запустите установку и дождитесь успешного завершения



Установка из автономного пакета не требует дополнительных настроек, так как все необходимые конфигурации уже содержатся в пакете.

Установка из автономного пакета Kaspersky Endpoint Security 12.0 for Linux

147

```
administrator@corpserv:~$ sudo chmod +x ./kesl_12.0.0-6672.sh
[sudo] password for administrator:
administrator@corpserv:~$ sudo ./kesl_12.0.0-6672.sh
Unpack archive to '/tmp/01.02_09.23.33.771595241'...
Found installer...
Found parameters...
Run package installer 'akinstall.sh' ...
Mode of '/var/log/kaspersky/klnagent/19112cb2-31ae-4566-b52c-ffba70c8909a' changed
from 0644 (rw-r--r--) to 0660 (rw-rw----
```

Выдаем права на выполнение файл и запускаем установку:

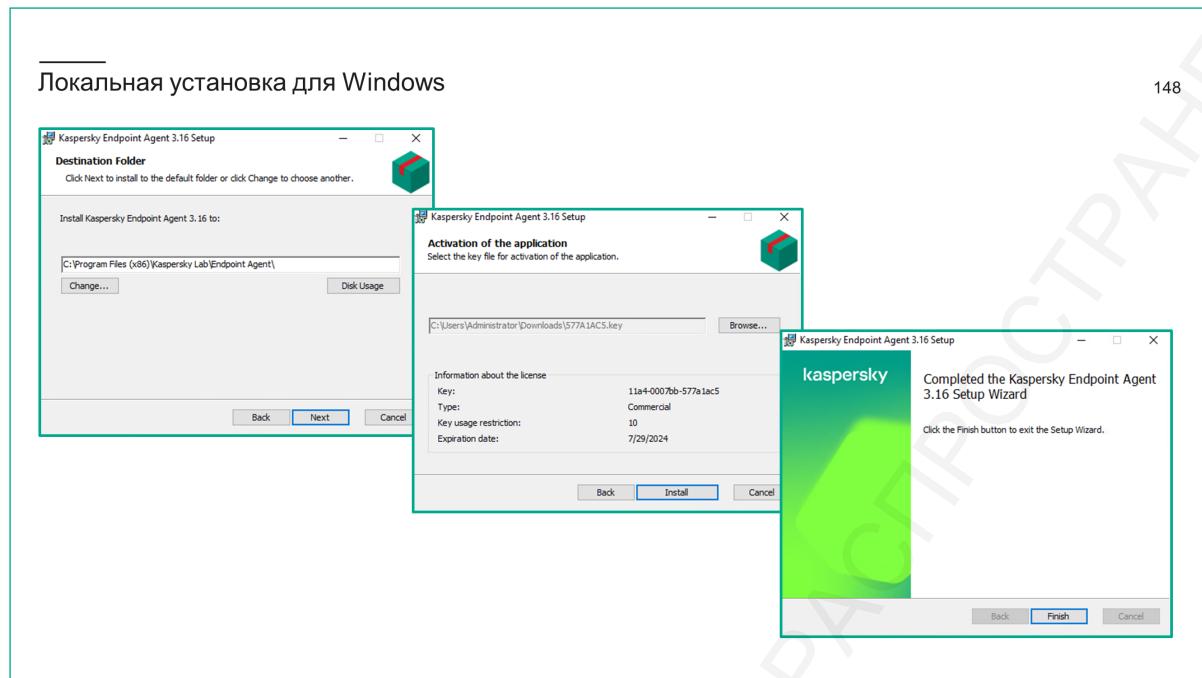
- sudo chmod +x ./kesl_12.0.0-6672.sh
- sudo ./kesl_12.0.0-6672.sh

Установка из автономного пакета для Linux требует запустить файл с правами админа.

Например:

```
sudo chmod +x ./kesl_12.0.0-6672.sh
sudo ./kesl_12.0.0-6672.sh
```

5.3. Установка без Центрального управления



Локально на компьютере можно установить Endpoint-агент с помощью мастера установки или с помощью командной строки.

Мастер установки запускается при запуске исполняемого файла и на примере установки KEA состоит из четырех шагов:

- На первом шаге нужно принять лицензионное соглашение и положение о защите данных.
- Второй шаг установки позволяет изменить папку для установки исполняемых модулей Kaspersky Endpoint Agent.

По умолчанию Kaspersky Endpoint Agent устанавливает свои исполняемые файлы и библиотеки в папку %Program Files (x86)%\Kaspersky Lab\Endpoint Agent. Если по какой-то причине нужно, чтобы файлы KEA находились в другой папке, путь к ней нужно указать в поле окна Destination folder. Расположение файлов настроек и прочих служебных файлов Kaspersky Endpoint Agent от этого не зависит, служебные файлы всегда хранятся по пути %ProgramData%\Kaspersky Lab\Endpoint Agent

- Третий шаг установки позволяет указать ключ для активации функций KEDR в Kaspersky Endpoint Agent. Если ключ находится в папке, из которой был запущен EndpointAgent.msi, инсталлятор подхватит его автоматически. Активировать KEA можно и после установки.
- Четвертый шаг завершает установку.

Установка КЕА с помощью командной строки

149

Журнал установки

- %TEMP%\MSIxxxx.log

File Home Share View
This PC > Local Disk (C) > Users > Administrator > AppData > Local > Temp

Name	Date modified	Type	Size
MSIb896	1/31/2024 1:58 PM	Text Document	2,392 KB
MSI104	1/31/2024 2:00 PM	Text Document	2,423 KB
offline	1/25/2024 3:53 PM	File	24 KB
offline.session64	1/25/2024 3:53 PM	SESSION64 File	65 KB
StructuredQuery	1/26/2024 8:08 AM	Text Document	10 KB

Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Administrator>msiexec /i C:\Users\Administrator\Downloads\endpointagent.msi /qn EULA=1 PRIVACYPOLICY=1

MSI (s) (00:50) [14:28:44:389]: Product: Kaspersky Endpoint Agent 3.16 -- Configuration completed successfully.
MSI (s) (00:50) [14:28:44:389]: Windows Installer reconfigured the product. Product Name: Kaspersky Endpoint Agent 3.16. Product Version: 3.16.0.195. Product Language: 1033. Manufacturer: AO Kaspersky Lab. Reconfiguration success or error status: 0.

Если нужно установить Kaspersky Endpoint Agent в неинтерактивном режиме, можно использовать команду:

```
msiexec /i <Путь к MSI файлу> /qn EULA=1 PRIVACYPOLICY=1
```

- где EULA и PRIVACYPOLICY — обязательные параметры.

Дополнительные параметры MSI-пакета:

- LICENSEKEYPATH=<путь к файлу лицензионного ключа> — позволяет активировать Kaspersky Endpoint Agent сразу после установки.
- SKIPCVERWINDOWS10=1 — позволяет пропустить проверку наличия на компьютере требуемого обновления Windows.
- ADDLOCAL=<Core, KATA, SB, All> — позволяет выбрать устанавливаемые компоненты. По умолчанию используется значение All.

В результате установки создается журнал с подробным описанием процесса. По умолчанию он находится в папке %TEMP% пользователя, от имени которого была запущена установка. В случае успешной установки в конце журнала появятся записи: "Product: Kaspersky Endpoint Agent – Installation completed successfully" и "Installation success or error status: 0".

Локальная установка Kaspersky Endpoint Security 12.0 for Linux

168

```
administrator@corpserv:~$ sudo apt-get install ./kesl_12.0.0-6186_amd64.deb
Reading package lists... Done
Building dependency tree... Done
The following NEW packages will be installed:
  kesl
0 upgraded, 1 newly installed, 0 to remove and 16 not upgraded.
Need to get 0 B/54.8 MB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 /home/administrator/kesl_12.0.0-6186_amd64.deb kesl amd64 12.0.0-6186 [54.8 MB]
Selecting previously unselected package kesl.
(Reading database ... 118750 files and directories currently installed.)
Preparing to unpack .../kesl_12.0.0-6186_amd64.deb ...
Unpacking kesl (12.0.0-6186) ...
Setting up kesl (12.0.0-6186) ...

The application 'Kaspersky Endpoint Security 12.0 for Linux' was successfully installed but must be configured before use.

Please run script '/opt/kaspersky/kesl/bin/kesl-setup.pl' for application configuration

Processing triggers for man-db (2.10.2-1) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.

Restarting services...
systemctl restart smbd.service packagekit.service smbd.service
No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
N: Download unsandboxed as root as file '/home/administrator/kesl_12.0.0-6186_amd64.deb' couldn't
be accessed by user 'apt' - pkAcquire::Run ([10: Permission denied])
administrator@corpserv:~$ sudo /opt/kaspersky/kesl/bin/kesl-setup.pl
Kaspersky Endpoint Security 12.0 for Linux version 12.0.0.6186
```

Запустите установку:

- sudo apt-get install ./kesl_12.0.0-6186-amd.deb

Запустите скрипт первоначальной конфигурации:

- sudo /opt/kaspersky/kesl/bin/kesl-setup.pl

Чтобы запустить локальную установку KES для Linux, заранее скопируйте архив с решением на целевой узел. Далее запустите установку командой:

```
sudo apt-get install ./kesl_12.0.0-6186-amd.deb
```

И запустите скрипт первоначальной конфигурации:

```
sudo /opt/kaspersky/kesl/bin/kesl-setup.pl
```

Инсталляционный пакет может иметь расширение .rpm для установки на соответствующую операционную систему.

Интерфейс управления из командной строки agent.exe

151

```

:C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent>agent.exe --help
You are using the Kaspersky Endpoint Agent 3.16.0.195 command line utility.
(c) 2023 AO Kaspersky Lab.

Available options:
--help arg           Show help for available options
--trace arg          Enable/disable tracing in the product
<enable|disable>[show]
--dump arg           Enable/disable writing in the product
<enable|disable>[show]
--password arg       Password protection management <set|reset|state>
Product service management <start|stop|state>
--ppl arg            PPL tag management for product <enable|show>
Prevention management <enable>[show]
--prevention arg    Scan autostart entries task management
--scan-autostart    Scan IOC task management
--scan-loc           Scan Network isolation management <enable|disable>[show]
Connection to message broker management
<enable|disable>[show]<stats>[global]
--isolation arg     Turn on/off system events
<on|off>[parameters] <eventlog>[registry|network|eventlog|filechange|activity|accountlogon|codeinject|autostartentry>
--message-broker arg Quarantine operations <add|delete|restore>[show]<limi
ts>[clear]
--quarantine arg    Make disk image
--disk-image         Make system memory dump
--memory-dump        Scan OVAL rules management
--scan-oval          Sandbox cluster integration management
--sandbox arg        Kernel module management
--update arg         Update management <bases|modules>
Product license management
<add|delete>[show]<reserve>
--license arg        Product self-defense management <enable|disable>
Product proxy management <enable|disable>[show]
--selfdefense arg   Product traces folder
--proxy arg          Product traces rotation mode <yes|no>
--rotate-file-size arg Product traces file maximum size
--rotate-files-count arg Product traces rotates files count

```

Расположение

- C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\agent.exe

Справка

- agent.exe --help

Статус основной службы

- agent.exe --product state

Остановить и запустить агент

- agent.exe --product stop
- agent.exe --product start

Включить или выключить трассировку

- agent.exe --trace enable --folder <путь к существующей папке>
- agent.exe --trace disable

Ниже рассмотрим интерфейсы командной строки для различных типов Endpoint-агентов.

Начнем с КЕА.

Вы можете управлять настройками Endpoint-агента локально с помощью командной строки. На примере КЕА это:

Расположение утилиты:

C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\agent.exe

Примеры использования:

- agent.exe --help (справка)
- agent.exe --product state (статус основной службы)

Остановить и запустить Endpoint-агент:

- agent.exe --product stop
- agent.exe --product start

Включить или выключить трассировку:

- agent.exe --trace enable --folder <путь к существующей папке>
- agent.exe --trace disable

В частности, чтобы настроить параметры подключения КЕА к центральному узлу нужно

запускать agent.exe с ключом --message-broker=enable. Адрес и сертификат Центрального узла задаются дополнительными параметрами:

- --type=kata — указывает тип подключения, обязательен
- --servers=<адрес центрального узла>:<порт для подключения агентов>
- --pinned-certificate=<путь к файлу TLS-сертификата Центрального узла в формате crt>

Полная команда будет выглядеть так (в одну строку):

```
agent.exe --message-broker=enable --type=kata  
--servers=10.10.10.10:443 --pinned-certificate=kata.crt
```

Чтобы включить использование клиентского сертификата, нужно дополнительно задать параметр:

```
--client-certificate=<путь к файлу с клиентским сертификатом в  
формате pfx>
```

Даже если вы хотите просто поменять один параметр, нужно повторять основной ключ --message-broker=enable и параметр --type=kata. Например, чтобы просто добавить клиентский сертификат, используйте команду:

```
agent.exe --message-broker=enable --type=kata --client  
-certificate=client.pfx
```

Чтобы показать настроенные параметры КЕА, используйте команду:

```
agent.exe --message-broker=show
```

В выводе этой команды кроме значений перечисленных выше параметров обращайте внимание на параметры:

- kata.tls — ожидаемое значение true, если включено безопасное соединение
- kata.use_pinned_certificate — ожидаемое значение true, если включена проверка сертификата Центрального узла
- kata.use_client_certificate — ожидаемое значение true, если на стороне Центрального узла включена валидация клиентского сертификата; в противном случае ожидаемое значение false

В большой сети без Kaspersky Security Center настройку Endpoint-агентов можно

организовать с помощью скрипта входа в систему, распространяемого групповой политикой.

Чтобы активировать Kaspersky Endpoint Agent без KSC, используйте интерфейс командной строки agent.exe на компьютере. Активировать можно и ключом, и кодом:

```
agent.exe --license add=<код активации или путь к файлу ключа>
```

Чтобы активация кодом была успешной, нужно чтобы у компьютера был доступ к серверам активации Лаборатории Касперского в интернете.

Чтобы установить дополнительный ключ (или код), используйте команду:

```
agent.exe --license reserve=<код активации или путь к файлу ключа>
```

Чтобы отобразить информацию об установленной лицензии, используйте команду:

```
agent.exe --license show
```

Чтобы удалить установленный ключ или код (с целью заменить другим), используйте команду:

```
agent.exe --license delete=<серийный номер лицензий, который показывает команда show>
```

На самом компьютере проверить, запущен ли Endpoint-агент можно локально, как пример для KEA:

```
agent.exe --product state
```

Чтобы проверить настройки подключения к центральному узлу, используйте команду:

```
agent.exe --message-broker show
```

Чтобы проверить статус активации Endpoint-агента, используйте команду:

```
agent.exe --license show
```

Чтобы проверить, что Endpoint-агент собирает телеметрию для отправки на Центральный узел, используйте команду:

```
agent.exe --message-broker stats
```

Эта команда показывает сколько и каких событий зарегистрировал КЕА. Отдельно стоит обратить внимание на категорию Throttled. Это события, превысившие установленные квоты на сбор телеметрии, и отброшенные Endpoint-агентом без отправки на Центральный узел. Квоты для событий можно настроить в политике Kaspersky Endpoint Agent.

Чтобы увидеть возможные ошибки подключения Endpoint-агента к центральному узлу, включите трассировку командой:

```
agent.exe --trace enable --folder <путь к существующей папке для хранения отладочных журналов>
```

Интерфейс управления из командной строки KES

156

```
C:\Program Files (x86)\Kaspersky Lab\KES.12.3.0\avp.com edrkata /show  
Server endpoints:  
    - 10.28.0.51:443  
Server connection timeout: 10 seconds  
Server request timeout: 10 seconds  
Synchronization period: every 60 seconds  
Events send period: every 30 seconds  
Events count limit, enabled: 1  
Events count limit, max events per hour: 3000  
C:\Program Files (x86)\Kaspersky Lab\KES.12.3.0>
```

Расположение:

C:\Program Files (x86)\Kaspersky Lab\KES 12.3.0\avp.com

Команды:

- avp.com START EDRKATA
- avp.com STOP EDRKATA
- avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
- avp.com edrkata /show
- avp.com LICENSE <operation> [/login=<user name> /password=<password>]

В случае, если вы управляете KES локально, то вы также можете управлять модулем сбора телеметрии с помощью командной строки. Утилита командной строки по умолчанию находится в папке:

C:\Program Files (x86)\Kaspersky Lab\KES 12.3.0\avp.com

Примеры команд для запуска модуля сбора телеметрии:

```
avp.com START EDRKATA  
avp.com STOP EDRKATA
```

Примеры команды для настройки модуля сбора телеметрии и указания сервера решения:

```
avp.com edrkata /set /servers=<server address>:<port> /server-
certificate=<path to the TLS certificate> [/timeout=<Central Node
server connection timeout (s)>] [/sync-period=<Central Node server
synchronization period (min)>]
```

Примеры команды для вывода настроек и задания лицензии:

```
avp.com edrkata /show
avp.com LICENSE <operation> [/login=<user name>
/password=<password>]
```

Интерфейс управления из командной строки KESL

157

```
administrator@corpserv:~$ kesl-control --help
Command Help:
[-A] --get-app-list           get application list
                               --json in json format
[-A] --get-categories         get application categories
                               --json in json format
[-B] --mass-remove            delete files from Storage
                               --query <filter> object filter
                               get information about objects in Storage
                               -n <number> display last 'number' of records. Default value is 30. Use
n 0 to display all elements.
[-B] --restore <object ID>    restore an object from Storage
                               --file <path> path for restoring
[-D] --get-device-list         get list of devices connected to the host
                               --json in json format
-E                            get application events
                               --query <filter> object filter
                               -n <number> number of items from the end
                               --query -d<db-file> database file to use
                               --db <db-file> database file
administrator@corpserv:~$ kesl-control --get-settings 24
UseClientPinnedCertificate=No
SynchronizationPeriod=1
ConnectionTimeout=10
RequestTimeout=10
EnableTelemetry=Yes
[Endpoints.item_0000]
Address=10.28.0.51
Port=443
[EventTransferSettings]
MaximumDataTransferTime=30
UseRequestCountLimit=No
MaximumNumberOfEventsInHour=3000
EventLimitExceededPercentage=15
administrator@corpserv:~$ kesl-control --query-kataedr-server-certificate
Serial number: 0E 12 D5 64 5A 83 72 EE 4E 3D E5 9A A8 DB AE F0 AA C7 0C 8E
Subject: C=RU, ST=Moscow, CN=faf3d04676c8, O=faf3d04676c8, OU=InfoSec
Issuer: C=RU, ST=MSK, CN=KATAPI, OU=InfoSec
Valid from: 2024-01-17 12:35:05
Expires on: 2029-01-16 12:35:05
SHA-1 fingerprint: 9A 87 0F B1 5F D5 76 B6 5F 11 7D 6C 64 16 D0 AA E0 D3 A3 88
SHA-256 fingerprint: 57 9B D4 8C 29 CE B4 ED 6B 05 B8 CE E3 1C AA 34 8B E9 3B 24 5B E8 3D 8B 62 E6 05 98 96 59
5C 6A
```

Изучите справку консоли управления:

- `kesl-control --help`

Получите настройки сервиса интеграции:

- `kesl-control -get-settings 24`

Пример получения сертификата сервера:

- `kesl-control --query-kataedr-server-certificate`

В случае, если вы управляете KES для Linux локально, то вы также можете управлять модулем сбора телеметрии с помощью командной строки. Для вызова справки используйте команду:

```
kesl-control --help
```

Получите настройки сервиса интеграции:

```
kesl-control -get-settings
```

Пример получения сертификата сервера:

```
kesl-control --query-kataedr-server-certificate
```

Управление активацией Kaspersky Endpoint Security 12.0 for Linux из командной строки

158

Добавить лицензию

- `kesl-control --add-active-key <код или путь к файлу ключа>`

```
administrator@corpserv:~$ kesl-control --add-active-key /home/administrator/lic.key
```

Удалить лицензию

- `kesl-control --remove-active-key`

```
administrator@corpserv:~$ kesl-control --remove-active-key
```

Вы можете добавить лицензию KESL локально с помощью команды:

`kesl-control --add-active-key <код или путь к файлу ключа>`

Чтобы удалить лицензию KESL выполните команду:

`kesl-control --remove-active-key`

5.4. Результат установки и сбор данных

Службы и драйверы Kaspersky Endpoint Agent

159

```
S C:\Users\Administrator> Get-Service soyuz
status   Name           DisplayName
-----  ---
running  soyuz          Kaspersky Endpoint Agent

S C:\Users\Administrator> Get-Service angara
status   Name           DisplayName
-----  ---
running  angara         Kaspersky Sandbox Integration
```

SOYUZ.exe

- основная служба Kaspersky Endpoint Agent, которая управляет задачами и рабочими процессами программы, обеспечивает взаимодействие между Kaspersky Endpoint Agent и компонентом Central Node

ANGARA.dll

- (исполняется в proton.exe) – это служба, которая обеспечивает взаимодействие между Kaspersky Endpoint Agent и EPP в сценариях интеграции с Kaspersky Sandbox

Module	Name	Display Name	Driver Type	Link Date
klnsnr	Kaspersky Lab Security	File System	File System	9/27/2023 5:20:22 AM
klncap	Klncap	Kernel	Kernel	2/15/2023 10:04:28 PM

klncap.sys — собирает сетевые события

- установление соединений
- открытие портов

klnsnr.sys — собирает системные события

- изменение в реестре
- запущен процесс
- загружен модуль
- изменен файл
- событие OS
- интерактивный ввод команд

По умолчанию КЕА устанавливается в папку %ProgramFiles%\Kaspersky Lab\Endpoint Agent. В списке служб появляются службы, автоматически запускаемые под учетной записью Local System:

- Kaspersky Endpoint Agent (системное имя soyuz);
- Kaspersky Sandbox integration (системное имя angara);
- KATA integration (системное имя vostok).

Исполняемыми файлами этих служб являются soyuz.exe и proton.exe. Ищите ошибки подключения в журнале процесса proton.exe. Например, выполните поиск по IP-адресу Центрального узла или по слову error или failed.

В Kaspersky Endpoint Agent встроен механизм самозащиты, который препятствует воздействию сторонних процессов при попытках:

- Модификации, удаления, изменения прав доступа исполняемых и служебных файлов продукта.
- Модификации и удаления настроек продукта в реестре ОС Windows.
- Остановки и перезапуска сервисной части продукта или изменения учетной записи для запуска сервисной части.
- Модификации загруженных в память исполняемых модулей продукта.

Kaspersky Endpoint Agent устанавливает на компьютер два драйвера для сбора телеметрии:

- klnccap.sys собирает сетевые события такие как установление входящих и исходящих соединений, открытие портов для приема соединений и др.
- klsnsr.sys собирает всевозможные события об активности на компьютере:
 - создание файлов;
 - запуск процессов;
 - изменения в реестре Windows;
 - ввод команд с клавиатуры в командных оболочках;
 - появление событий в журналах Windows;
 - и некоторые другие.

Оба драйвера собирают события с помощью механизма Event Tracing for Windows (ETW).

Сбор данных регулируется специальными фильтрами, которые задают области мониторинга (на диске, в реестре, в журналах событий и пр.) и исключения. Эти фильтры загружаются задачей обновления Kaspersky Endpoint Security. Иными словами, какие именно события Endpoint-агенты собирают и передают на Центральный узел не является запрограммированным поведением, а может меняться с течением времени, например, в результате анализа специалистами Лаборатории Касперского новых целевых атак и методов, используемых злоумышленниками.

Журналы и папки Kaspersky Endpoint Agent

160

Application and Services Logs | Kaspersky | Security:

- Sensor Diagnostics | Operational
- Soyuz | Product

\Program Files (x86)\Kaspersky Lab\Endpoint Agent

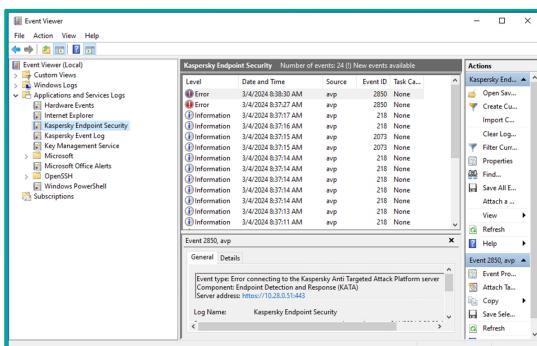
- Программные файлы
- Утилита командной строки agent.exe

Папка с исполняемыми файлами Kaspersky Endpoint Agent по умолчанию расположена по пути %Program Files (x86)%\Kaspersky Lab\Endpoint Agent. Из исполняемых модулей КЕА важно отметить интерфейс для управления из командной строки agent.exe.

Еще одно очевидное место, где можно пытаться понять, ожидаемо ли работает Endpoint-агент, это журнал событий Windows. События Kaspersky Endpoint Agent нужно искать в журналах Applications and services logs\Kaspersky\Security\Soyuz |Product и Applications and services logs\Kaspersky\Security\Sensor Diagnostics\Operational. В основном здесь нужно смотреть на возможные сообщения об ошибках. В частности, здесь можно найти ошибки проверки лицензии.

Журналы и папки Kaspersky Endpoint Security

176



Application and Services Logs | Kaspersky Endpoint Security

События Kaspersky Endpoint Security нужно искать в журналах Applications and services logs\Kaspersky Endpoint. В основном здесь нужно смотреть на возможные сообщения об ошибках. В частности, здесь можно найти ошибки подключения к центральному узлу.

Результат установки Kaspersky Endpoint Security 12.0 for Linux

161

```
administrator@corpserve:-$ sudo systemctl status kesl.service
● kesl.service - kesl
   Loaded: loaded (/lib/systemd/system/kesl.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-02-01 09:48:36 UTC; 3h 52min ago
     Main PID: 1354 (wdserver)
       Tasks: 1 (limit: 4558)
      Memory: 353.6M
        CPU: 1min 6.623s
       CGroup: /system.slice/kesl.service
               └─1354 /var/opt/kaspersky/kesl/install-current/opt/kaspersky/kesl/libexec/wdserver --trace-level

Feb 01 09:48:32 corpserve systemd[1]: Starting kesl...
Feb 01 09:48:36 corpserve kesl[1334]: kesl started
Feb 01 09:48:36 corpserve systemd[1]: Started kesl.

Manifest file: "kl file integrity manifest.xml"
+ echo Running /var/opt/kaspersky/kesl/install-current/opt/kaspersky/kesl/libexec/kesl-starter ...
Running /var/opt/kaspersky/kesl/install-current/opt/kaspersky/kesl/libexec/kesl-starter ...
+ [ -f /opt/kaspersky/kesl/lib64/libjemalloc.so ]
+ LD_PRELOAD=/opt/kaspersky/kesl/lib64/libjemalloc.so:
+ lsmod
+ fgrep -q parsec
+ [ ! -z /opt/kaspersky/kesl/lib64/libjemalloc.so: ]
+ export LD_PRELOAD
+ exec /opt/kaspersky/kesl/libexec/kesl
Integrity Check Result: SUCCEEDED
=====
Summary( failed / skipped / succeeded ):
  Manifests: 0 / 0 / 1
  Files: 0 / 0 / 104
  Directories: 0 / 0 / 0
  Registries: 0 / 0 / 0
  Registry values: 0 / 0 / 0
=====
SUCCEEDED
2024-02-01 09:48:36 launcher (pid:1343): wdserver started!
```

Посмотрите статус сервиса

- sudo systemctl status kesl.service

Изучите журнал установки

- /var/log/kaspersky/kesl

Получить статус установки Kaspersky Endpoint Security для Linux можно введя комманду:

```
sudo systemctl status kesl
```

В случае необходимости, изучите журнал установки:

/var/log/kaspersky/kesl

Подключенные агенты в консоли центрального узла

Host	IP	OS	License	Version	Server	Activity	Last connection
alex-desktop.abc.lab	10.28.0.1	Microsoft Windows Prores	OK	12.0.0.493	Kata	Normal a...	2024-02-01 00...
coroserv	10.28.0.2	Ubuntu	OK	12.0.0.6672	Kata	Normal a...	2024-02-01 00...

162

Проверьте состояние агентов (доступно всем учетным записям)

Threat Hunting

Host name	Count	First event (time)	Last event (time)
alex-desktop.abc.lab	7498	2024-01-31 12:15:54	2024-02-01 08:16:42
coroserv	3633	2024-01-31 01:35:03	2024-02-01 00:05:04

Проверьте поступление событий телеметрии (доступно всем, кроме администраторов)

В консоли Центрального узла подключенные Endpoint-агенты отображаются на вкладке Endpoint Agents, где можно увидеть их статус и наличие лицензий. Отображение Endpoint-агентов в консоли со статусом *Normal* означает только то, что Endpoint-агент смог подключиться к Центральному узлу. Чтобы проверить поступление телеметрии от Endpoint-агентов, на странице Threat Hunting введите запрос, под который точно попадет телеметрия с хостов, к примеру: HostIP != 1.1.1.1

Настройка статуса агентов

The settings are applied to all Endpoint Agent hosts that are connected to this PCN server. The settings do not affect SCN hosts.

Activity indicators

- Warning: 1 days of inactivity
- Critical inactivity: 7 days of inactivity

163

«Соединением» считается синхронизация настроек, а не отправка телеметрии

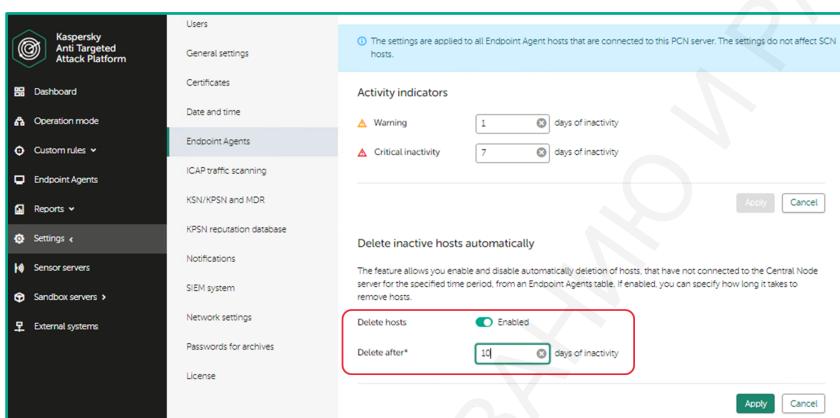
Если Endpoint-агент по какой-то причине перестанет подключаться к центральному узлу, об этом можно будет судить по значению параметра Last connection. Если Endpoint-агент не подключается больше суток, его статус меняется на Warning, а после 7 суток — на Critical.

Кроме этого, в веб-консоли Центрального узла отображается состояние активации Endpoint-агента. Если лицензионный ключ не установлен или истек, значение поля License key status будет отличаться от OK.

Центральный узел не показывает ошибки авторизации, если, например, Endpoint-агент пытается подключиться с не тем клиентским сертификатом, или без клиентского сертификата, или отказывается подключаться из-за несовпадения сертификата Центрального узла.

Удаление из консоли Центрального узла неактивных агентов

164



По истечении указанного времени неактивные хосты будут удалены из консоли. Если хост подключится к Центральному узлу позже, то он снова появится в консоли

В случае, если у вас в организации часто меняются рабочие станции или используется рабочие станции в виде виртуальных машин, то вы можете удалять неактивных клиентов по истечении определенного времени.

По истечении указанного времени неактивные хосты будут удалены из консоли. Если хост подключится к Центральному узлу позже, то он снова появится в консоли.

Глава 6. Эксплуатация KEDR

6.1. Технологии обнаружения KEDR

Технологии Kaspersky Endpoint Detection & Response		165
	Технология	Описание
TAA	Targeted Attack Analyzer	Обнаруживает индикаторы атак (Indicators of attack, IOA) по обновляемым и пользовательским правилам в событиях телеметрии, поступающих от компьютеров
SB	Sandbox	Анализирует исполняемые файлы и активные документы на виртуальных машинах по запросу аналитика или автоматически в результате срабатывания правила ТАА. Применяет обновляемую логику обнаружения
IOC	Indicator of Compromise	Обнаруживает признаки компрометации на компьютерах сети по пользовательским правилам в формате OpenIOC
YARA	YARA Engine	Сканирует файлы (и процессы) на компьютерах, а также файлы в хранилище центрального узла по пользовательским правилам
AM	Anti-malware Engine	Сканирует файлы в хранилище центрального узла по обновляемым сигнатурам

Для детектирования угрозы используется целый набор технологий, среди которых:

- ТАА — Обнаруживает индикаторы атак в событиях телеметрии.
- SB — Анализирует исполняемые файлы и активные документы на виртуальных машинах компонента KATA Sandbox.
- IOC - Обнаруживает признаки компрометации на компьютерах сети по пользовательским правилам в формате OpenIOC.
- YARA - Сканирует файлы (и процессы) на компьютерах, а также файлы в хранилище Центрального узла по пользовательским правилам.
- AM - Сканирует файлы в хранилище Центрального узла по обновляемым сигнатурам.

Targeted Attack Analyzer.

Модуль Targeted Attack Analyzer выполняет анализ данных, полученных в результате наблюдения за активностью конечных узлов, и выявляет признаки целевых атак на ИТ-инфраструктуру организации.

Targeted Attack Analyzer получает информацию о поведении конечных узлов от Endpoint-агентов. Kaspersky Endpoint Agent сообщает центральному узлу о запуске процессов, загрузке исполняемых модулей, используемых исполняемых файлах и устанавливаемых сетевых

соединениях, файловой активности и изменениях в реестре, событиях Windows Event Log, интерактивном вводе с клавиатуры в командных оболочках.

Эти данные добавляются в базу, сопоставляются и анализируются в реальном времени. Targeted Attack Analyzer использует множество разных правил для обнаружения опасной активности и база правил регулярно обновляется. Сотрудники службы безопасности также могут добавлять собственные правила для анализа телеметрии.

Есть два класса правил ТАА, используемых в Kaspersky Endpoint Detection and Response. Часть правил направлена на обнаружение признаков атак. Если активность на узле соответствует одному из таких правил, Центральный узел создает обнаружение от технологии ТАА.

Другая часть правил не создает обнаружения, а добавляет метки к событиям. Эти метки можно увидеть при анализе событий телеметрии в разделе Threat Hunting в веб-консоли. Метки помогают аналитику быстрее ориентироваться в массе событий и делать выводы о том, какая активность требует дальнейшего изучения, а какая нет.

К правилам разметки относятся, например, правила, обнаруживающие действия, подпадающие под классификацию MITRE ATT&CK. Метки с названиями техник дополняют обнаружения от технологии ТАА и помогают принимать решения о том, какие шаги имеет смысл предпринять в ответ на атаку.

Правила обнаружения также являются правилами разметки. У одного события может быть много меток, как от правил разметки, так и от правил обнаружения.

Чтобы проверить работоспособность технологии ТАА, нужно симулировать на одном из компьютеров активность, на которую есть правила обнаружения или правила разметки ТАА.

Если хочется получить несинтетическое обнаружение, можно запустить на компьютере системную утилиту certutil.exe с параметром -decode . Это приведет к обнаружению ТАА с именем suspicious_certutil_usage_decoding.

Что используют технологии Kaspersky Endpoint Detection & Response

166

	Технология	Обновляемые правила	Пользовательские правила
TAA	Targeted Attack Analyzer	Да	Да
SB	Sandbox	Да	Нет
IOC	Indicator of Compromise	Нет	Да
YARA	YARA Engine	Нет	Да
AM	Anti-malware Engine	Да	Нет

Часть технологий обнаружения позволяет использовать пользовательские правила, часть нет. Технологии IOC и YARA используют только пользовательские правила.

Где применяются технологии Kaspersky Endpoint Detection & Response

167

	Технология	На компьютере	На серверах КАТА
TAA	Targeted Attack Analyzer	Нет	Автоматически (все) и по запросу (только пользовательские)
SB	Sandbox	Нет	Автоматически (по правилам TAA) и по запросу
IOC	Indicator of Compromise	По расписанию	По запросу (с ограничениями)
YARA	YARA Engine	По запросу	Автоматически и по запросу
AM	Anti-malware Engine	Нет	Автоматически и по запросу

Часть технологий применяются локально на компьютерах либо на серверах КАТА. Технологии TAA, SB, AM применяются только на серверах КАТА.

Импорт сторонних правил ТАА

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. At the top, there's a header with the platform logo and navigation links like 'ABC Corp' and 'Dashboard'. Below the header, a table lists 'TAA' rules with columns for 'Type', 'Confide...', and 'Name'. A green 'Import' button is visible at the top right of this section. In the center, a modal window titled 'New TAA (IOA) rule' is open, showing fields for 'Name' (set to 'ioc:ioc'), 'Description', 'Importance' (set to 'Low'), 'Confidence' (set to 'Low'), 'Generate alerts' (set to 'Enabled'), and 'Apply to' (checkboxes for 'ABC Corp' and 'kata'). Below the modal, a preview of the imported rule content is shown:

```

It is highly recommended that you test custom TAA (IOA) rules in a test environment before you import them. Custom TAA (IOA) rules may cause performance issues, in which case stable performance of Kaspersky Anti Targeted Attack Platform is not guaranteed.

State: Enabled
Name*: ioc:ioc
Description:
Importance: Low
Confidence: Low
Generate alerts: Enabled
Apply to: ABC Corp, kata
127.0.0.1

```

On the right side of the main interface, there are two status indicators: '1 node' (disabled) and 'All' (enabled). The number '168' is located in the top right corner of the main content area.

Вы можете импортировать файл формата IOC

- **State** — добавляет метки к событиям
- **Generate alerts** — создает обнаружения
- **Importance** — определяет важность обнаружения

Чтобы эффективно использовать Threat hunting, нужно обладать соответствующей квалификацией и опытом. Но даже менее опытный офицер безопасности может использовать Threat hunting для поиска индикаторов компрометации.

Списки индикаторов компрометации часто входят в публичные отчеты об обнаруженных атаках или вредоносных программах. Их можно найти, в частности, в отчетах, публикуемых на сайте securelist.com — веб-сайте Лаборатории Касперского, посвященном актуальной информации об угрозах.

Индикаторы компрометации доступны также вместе с отчетами об APT-атаках на портале Threat Intelligence. По подписке, которая включена в Kaspersky Anti Targeted Attack и Kaspersky Endpoint Detection and Response, доступны только сравнительно старые отчеты. Для доступа к свежим отчетам нужно приобретать полноценную подписку.

Индикаторами могут являться имена и контрольные суммы вредоносных модулей, адреса серверов управления, характерные ключи реестра. Все эти параметры легко перенести в Threat hunting, и проверить, не встречались ли они в событиях, переданных Endpoint-агентами.

При импорте правил ТАА следует учитывать, что они могут повлиять на производительность системы.

Для некоторых правил нецелесообразно создавать алERTы. В таких случаях не включайте опцию Generate alerts.

При импорте возможна ситуация, когда какие-то условия пользовательского правила ТАА не будут поддерживаться. В таком случае, правило будет импортировано, но система

проигнорирует неподдерживаемые условия.

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. On the left, there's a sidebar with 'Custom rules' expanded, showing 'TAA', 'IDS', and 'IOC'. The main area is titled 'IOC' and shows a list with one item: 'Global loc loc'. A modal window titled 'Import IOC file' is open. It has tabs for 'Autoscan' (which is checked) and 'Enabled'. The 'Name' field is set to 'loc.loc'. The 'Importance' dropdown is set to 'Low'. The 'Apply to' dropdown lists 'ABC Corp' and 'kata'. Below these fields, there's a note about unsupported document context and search contexts. The XML code for the IOC file is shown at the bottom:

```

<?xml version="1.0" encoding="utf-8"?><ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="ioc">
<description>My IOC</description>
<keywords/>
<authorized_by>Test Label</authorized_by>
<authorized_date>2018-06-03T06:05:37</authorized_date>
<links/>
<definition>
<indicator operator="OR" id="5f7aee05-cd5c-4bb1-9350-41af44895e8d">
<context document="#RouteEntryItem" search="RouteEntryItem/Destination">
<content type="string">area.athelpdesk.com</content>
</context>
<indicatorItem id="5b219f89-076c-4408-ab8d-4f5ccca85a10" condition="1s">
<context document="#FileItem" search="FileItem/Md5sum" type="md5">
<content type="string">area.athelpdesk.com</content>
</context>
<indicatorItem id="5b219f8d-f808-4cd0-9380-4f5ccb8a5a10" condition="1s">
<context document="#FileItem" search="FileItem/Sha256" type="sha256">
<content type="string">5f17adbd4d129e7b208a4d7f3a0e3e2a8bd77a23cb54</content>
</indicatorItem>
</Indicator>
</definition>
</ioc>

```

Правила IOC применяются для поиска на компьютерах средствами Endpoint-агентов.

Индикаторы можно только импортировать из файла в формате OpenIOC. Сохранить поиск Threat hunting в виде пользовательского правила IOC нельзя.

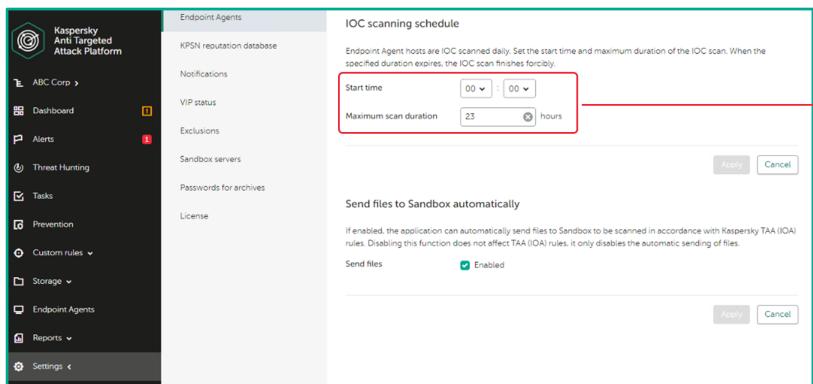
Условия поиска индикаторов компрометации в загруженных правилах редактировать нельзя. Их нужно редактировать перед импортом. В свойствах индикатора можно изменить уровень важности и имя индикатора. Также можно включить или выключить флаг Autoscan.

Правила, для которых включен Autoscan, применяются при поиске индикаторов на узлах сети. Правила, для которых Autoscan выключен, для поиска на узлах не используются. Фактически, Autoscan позволяет выключить правило, но не удалять его. Это может быть полезно, чтобы снизить потребление ресурсов на узлах при выполнении поиска.

Из карточки IOC можно найти все обнаружения, созданные по этому правилу, по ссылке Find alerts. Ссылка Find events загружает условия правила в Threat hunting для ретроспективного поиска по базе телеметрии. С помощью ссылки Download file можно сохранить правило в файл в формате OpenIOC.

Поиск IOС на компьютерах

170



Охват поиска

- Все компьютеры (агенты)

Время запуска

- в зоне UTC +0

Область поиска

- Весь компьютер

Центральный узел поддерживает ровно одну конфигурацию поиска индикаторов компрометации на узлах. Поиск выполняется раз в сутки во время, указанное в разделе Settings | IOC scanning schedule. Параметр Start time задает время запуска в часовой зоне UTC. Изменить зону нельзя. Параметр Maximum scan duration задает максимальное время выполнения поиска в часах.

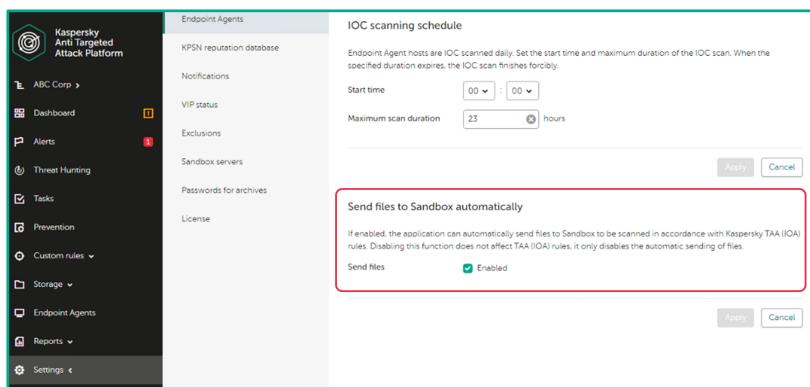
Ни какие другие параметры поиска задать нельзя. Поиск файлов по файловым признакам выполняется на всех дисках компьютера. Поиск ключей реестра выполняется по всему реестру. Следовательно, поиск может занимать продолжительное время и лучше планировать его на ночь.

Если поиск обнаруживает на компьютере индикаторы компрометации, результаты отображаются как обнаружения в веб-консоли Центрального узла. Для каждого правила IOCs создается отдельное обнаружение с уровнем важности, заданным для этого правила. Endpoint-агенты передают результаты поиска после окончания выполнения задачи, а не по ходу выполнения задачи.

Если поиск обнаруживает признаки компрометации на компьютерах, Центральный узел создает предупреждение от технологии IOCs с уровнем важности равным уровню важности сработавшего индикатора.

Проверка подозрительных файлов технологиями анализа файлов

171



Файлы отправляются на проверку при срабатывании **определенных** (не любых) **системных** (не пользовательских) правил ТАА

Проверка выполняется всеми технологиями анализа файлов

- Anti-Malware
- Sandbox
- YARA

У пользователя системы есть возможность включить автоматическую отправку подозрительных файлов на углубленную проверку.

Файлы отправляются на проверку при срабатывании определенных (не любых) системных (не пользовательских) правил ТАА.

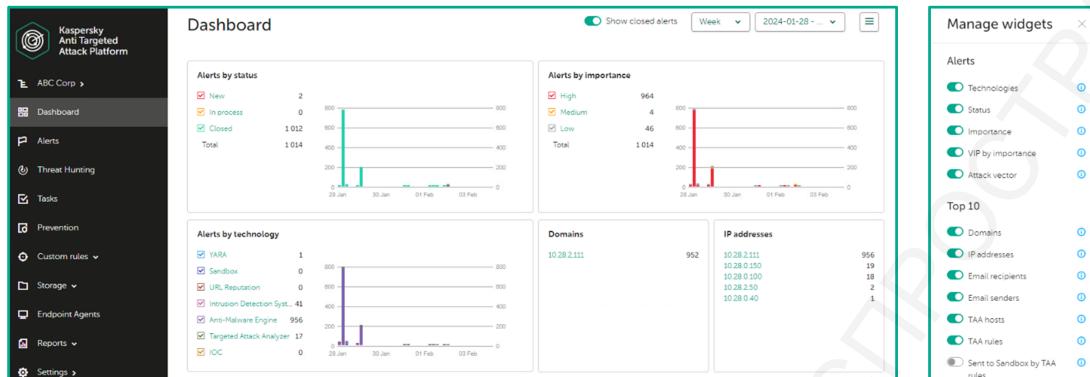
Проверка выполняется всеми технологиями анализа файлов

- Anti-Malware,
- Sandbox,
- YARA.

6.2. Расследование инцидента

Страница мониторинга Kaspersky Anti Targeted Attack

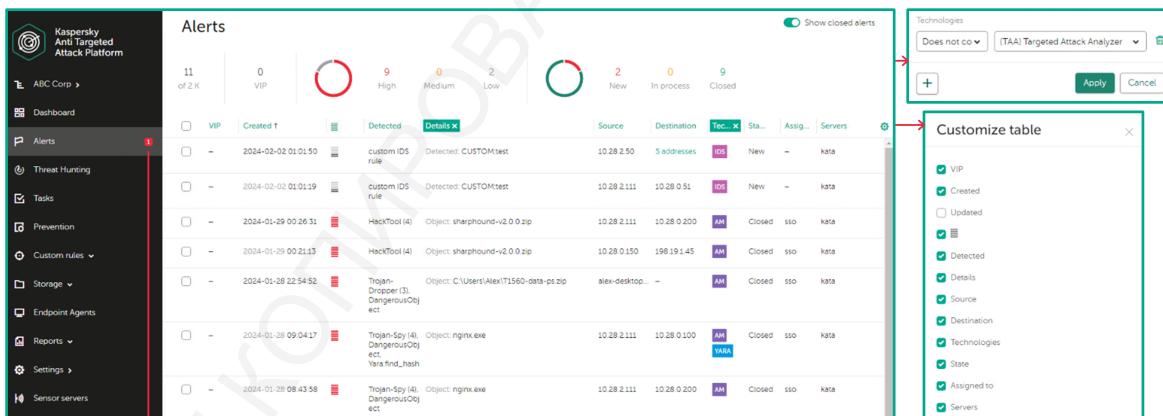
172



Стартовая страница представляет из себя настраиваемое полотно. На странице отображается статистика обнаружений и их детали. Вы можете сортировать статистику по типу, количеству и отрезку времени сборки данных.

Обнаружения Kaspersky Anti Targeted Attack

173



Количество новых обнаружений высокой важности (без учета фильтра)

Центральный узел исследует активность на конечных узлах с помощью компонента Targeted Attack Analyzer. Для этого собираются данные с Endpoint-агентов, затем они группируются и подвергаются анализу с целью выявления подозрительного поведения. Все данные для Targeted Attack Analyzer хранятся на центральном узле в специальной базе и доступны аналитикам для анализа вручную.

Чтобы посмотреть все обнаружения выберите Alerts в меню навигации слева.

Обработка обнаружений

Заголовок:

- **Статус обработки**
- **Важность** (согласно сработавшему правилу)
- **Источник** (Sensor или Endpoint)
- **Время создания**
- **Время обновления** (карточка пополняется событиями до закрытия обнаружения или 24 часа)

Поиск связанных обнаружений

История изменения состояния и комментарии

Change log

Выбрав любое обнаружение откроется его карточка. В карточка будет представлена детальная информация об обнаружении:

- Статус обработки
- Важность (согласно сработавшему правилу)
- Источник (Sensor или Endpoint)
- Время создания
- Время обновления (карточка пополняется событиями до закрытия обнаружения или 24 часа)

Вы можете искать связанные обнаружения и просматривать историю изменения состояний обнаружения и комментарии офицеров безопасности.

Обнаружение Targeted Attack Analyzer

175

Имя правила (ссылка на описание угрозы и рекомендации)

Список узлов, на которых сработало правило

Поиск связанных событий телеметрии

Технология **TAA** обнаруживает индикаторы атак в телеметрии узлов по обновляемым правилам

Одно обнаружение может включать события с разных узлов сети, и все эти узлы перечислены ниже в секции Hosts в подробностях обнаружения.

В качестве источника в обнаружении ТАА указывается ENDPOINT и время первого события, на котором сработало правило ТАА.

В секции Scan results в обнаружениях Targeted Attack Analyzer приводится имя правила ТАА, которое сработало на телеметрии с компьютеров. При клике по имени правила открывается описание правила, которое содержит:

- Описание опасной активности;
- Рекомендации по реагированию на инцидент;
- Классификацию активности по матрице MITRE ATT&CK и ссылку на соответствующий раздел на сайте attack.mitre.org;
- Описание техники MITRE ATT&CK и рекомендации по реагированию;
- Описание возможного легитимного использования операций, на которых сработало правило.

Рекомендации в обнаружении ТАА

176

The screenshot shows two main windows. The left window is titled 'All alerts > Event details #128' and displays alert information: State (New), Importance (High), Data source (ENDPOINT), Time created (2023-02-11 09:30:51), and Time updated (2023-02-11 09:34:19). A red box highlights the 'Scan results' section, which contains a link to 'TAA rule: using_msieexec_to_install_package_from_url'. An arrow points from this link to the right window. The right window is also titled 'All alerts > Event details #128' and shows a detailed view of the IOA ('using_msieexec_to_install_package_from_url'). It includes sections for 'Description', 'Recommendations', and 'MITRE ATT&CK(R) techniques'. The 'Recommendations' section provides guidance on how to handle such packages. The 'MITRE ATT&CK(R) techniques' section lists T1107 (Application Layer Protocol [D] Command and Control) and T1105 (Ingress Tool Transfer [C] Command and Control).

Имя правила ссылается на подробное описание с рекомендациями

В случае обнаружения правилом ТАА, вы можете получить детальные рекомендации по реагированию. Для этого выберите название сработавшего правила ТАА.

Обнаружение Sandbox

177

Сработавшее правило

Имя файла

Результаты проверки

The screenshot shows the 'All alerts > Event details' window for an 'in process' alert. The 'Object information' section shows the file 'c:\test_automob.exe'. The 'Scan results' section shows the file was not detected by AM (Not detected), but was detected by SB (IDS:Trojan-Spy:Quasar_UDP.C!C) and YARA (Not detected). A red box highlights the file name 'c:\test_automob.exe' in the object information and the scan results table.

Часть правил ТАА автоматически отправляет файлы на проверку технологией Sandbox

Часть правил ТАА автоматически отправляет файлы на проверку технологией Sandbox. Если Sandbox-сервер обнаружит подозрительную активность, то создаст новое обнаружение.

В деталях вы увидите:

- Сработавшее правило ТАА.

- Имя файла, на который сработало обнаружение.
- Результаты проверки файла.

Обнаружение индикатора компрометации на компьютере 178

Сработавший индикатор выделен маркером ←

В случае, если обнаружение создано индикатором компрометации на компьютере, то сработавший индикатор будет выделен маркером.

События, связанные с обнаружением 179

После имени правила в карточке обнаружения ТАА перечисляются узлы сети, на которых обнаружены события, соответствующие правилу. Для каждого узла указано его имя и количество событий, соответствующих правилу.

Центральный узел накапливает в карточке обнаружения ТАА все события, соответствующие правилу ТАА, от всех узлов сети в течение 24 часов после первого события такого типа. Если обнаружение было обработано и появились новые события, Центральный узел переназначает обнаружение обработавшему его сотруднику в статусе In process.

Детали активности, такие как имена файлов или параметры запуска, в карточке не отображаются. Чтобы их узнать, нужно формировать поиск в базе Threat hunting. Ссылка Find events под таблицей узлов сети в карточке автоматически формирует поиск по идентификатору правила ТАА за период, который охватывает карточка: 24 часа от времени регистрации первого события. Такой поиск покажет события ото всех компьютеров. События от одного компьютера можно найти, щелкнув мышью по имени компьютера в карточке.

Либо можно изменить условия поиска уже в результатах Threat Hunting: щелкнуть мышью по любому значению в любом столбце и либо добавить его к условиям поиска, либо исключить его из поиска.

Граф расследования

Разметка правилами TAA:

- Не все правила создают обнаружения
- Часть правил просто добавляет информационные метки к событию

180

Граф процессов

Свойства выбранного события на графике

Параметр	Значение
ID	10410 = "e07b0e2c-4cf2-a5d4-942d-8ac43b9b25c4"
Host	"alex-desktop.abc.lab"
Event time	2023-02-11 09:30:19E
Event type	Process started
Host name	alex-desktop.abc.lab
File	C:\Windows\system32\cmd.exe
Importance	High
Hash	SHA256
MDS	400f1c14bd9f90a8002271c18504779f41e3e4e40951deaa851e
Launch parameters	cmd.exe
Parent process	File: C:\Windows\system32\cmd.exe
Process ID	4688
Launch parameters	cmd.exe
System info	Host name: alex-desktop.abc.lab Host IP: 10.28.1.10 Account type: Non-administrator Logon type: Interactive User name: ABC\Alex OS name: Microsoft Windows 10 Pro 10.0.19045 N/A Build 19045
Details	Program name: Microsoft Windows® Operating System Vendor: Microsoft Corporation File description: Windows Command Processor

При клике мышью по событию в результатах поиска отображается карточка с подробностями о событии и визуализация дерева событий. Исходно и в карточке, и на панели визуализации отображаются выбранное событие и его родительский процесс.

Карточка содержит многочисленные атрибуты события, такие как тип операции, имя файла и контрольные суммы файла, размер, цифровая подпись, пользователь, выполнивший операцию и другие. Полный список отображаемых атрибутов зависит от типа события (типа операции) и есть в онлайн-справке KATA Platform.

Большинство значений атрибутов в карточке события интерактивны. По щелчку мыши

открывается контекстное меню, которое позволяет искать другие события с таким же атрибутом или обнаружения с таким атрибутом. Результаты поиска открываются в новой вкладке, чтобы не мешать основному анализу.

Вверху карточки события сразу под панелью визуализации располагается панель быстрого доступа к командам реагирования. Отсюда можно изолировать от сети компьютер, на котором была выполнена отображаемая операция, создать правило запрета доступа для файла, создать задачи для удаленного реагирования: удалить файл, остановить процесс и другие.

Граф событий над карточкой события тоже интерактивен. Простой клик мышью по процессу на графике отображает карточку события запуска процесса и сразу же отображает следующий по цепочке родительский процесс. Так, кликая по родительским процессам, можно полностью «размотать» последовательность запуска процессов от самого старта операционной системы.

Возле каждого имени процесса на графике приводится число событий, хранящихся в базе Threat hunting, которые относятся к этому процессу. Это могут быть файлы, созданные процессом, другие процессы, которые он запустил, выполненные сетевые соединения, обращения к реестру и другие типы событий.

Если кликнуть по стрелке справа от индикатора числа событий на графике, открывается контекстное меню, в котором перечислены типы событий и количество событий каждого типа. Аналитик может кликнуть по категории событий или по пункту All events и отобразить перечень событий процесса под графиком.

Для каждого события указано время его регистрации, тип события и подробности, которые зависят от типа события. Например, для события Process started приводится имя исполняемого файла дочернего процесса, его контрольные суммы MD5 и SHA256 (скрытые под ссылками) и маркер TAA, который указывает, что у этого события есть метки TAA того или иного уровня важности. Наличие маркера TAA означает, что активность дочернего процесса соответствует одному или нескольким правилам TAA.

Список событий можно фильтровать, чтобы скрыть менее интересные события и оставить более интересные. Для этого можно либо кликнуть в один из заголовков и настроить условия вручную, либо кликнуть по любому атрибуту события в таблице и из контекстного меню выбрать, либо показывать только события с таким же значением атрибута, либо скрыть события с таким значением атрибута.

Аналитик может вывести интересующие его события на график для более наглядного представления развития активности на компьютере. Для этого нужно навести (но не нажимать) курсор мыши на строку с событием, в результате чего слева от времени регистрации события появится тусклый значок глаза. Если теперь кликнуть по глазу, он из тусклого станет ярким, а

событие будет закреплено на графе и связано линией со своим родительским процессом.

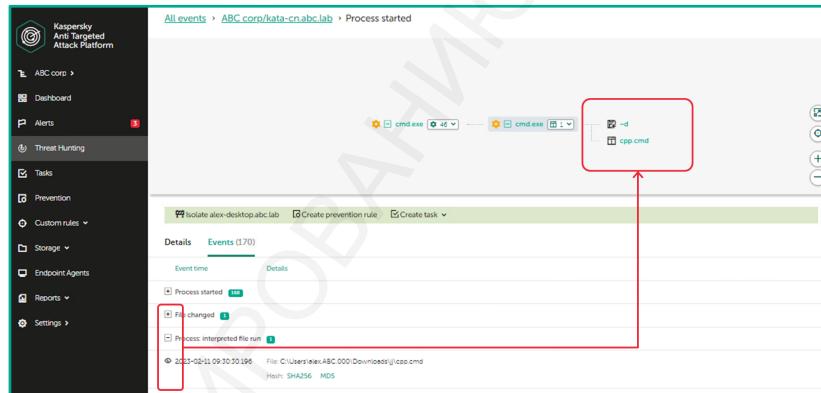
Чтобы убрать событие с графа, нужно либо повторно кликнуть по глазу в списке событий, либо навести курсор мыши на событие на графике, подождать пока появится красный значок с диагональным крестом возле имени события, и кликнуть по этому значку.

Таким образом аналитик может изучать подробности событий, связанных с исходным обнаружением: раскручивать цепочку родительских процессов назад во времени, находить другие дочерние процессы, созданные файлы, сетевые соединения.

В любой момент аналитик может кликнуть по любому атрибуту любого события и сформировать новый поиск по этому атрибуту в базе Threat hunting, чтобы начать новую цепочку расследования. Результаты поиска открываются в новой вкладке, чтобы не мешать нарушать уже идущему расследованию.

Восстановление цепочки событий

181



Существует возможность по каждому процессу отобрать перечень связанных с ним событий и при необходимости добавить их на график расследования. Некоторые события отображаются на графике автоматически.

Корреляция с событиями средств защиты узлов

182

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. On the left, there's a sidebar with navigation options like ABC Corp, Dashboard, Alerts, Threat Hunting, Tasks, Prevention, Custom rules, Storage, Endpoint Agents, Reports, Settings, and SSO Primary Central Node. The main area has a title bar "All events > ABC Corp/kata > Scan: detect". Below it, there's a timeline with two entries: "nginx.exe" and "PDM:Trojan.Win32.Bazon.a". The "nginx.exe" entry is highlighted with a red box. The "PDM:Trojan.Win32.Bazon.a" entry is also highlighted with a red box. The details for the "Scan: detect" event are shown in a table:

Scan: detect		Event initiator	
Detect	PDM:Trojan.Win32.Bazon.a	File	"C:\Users\Alex\Downloads\nginx.exe"
Last action	2024-02-02 11:31:11:947	Process ID	8772
Object name	c:\users\alex\downloads\nginx.exe	Launch parameters	"C:\Users\Alex\Downloads\nginx.exe"
MDS	78aaae9e74f77896c94b5c83992e0b1bf		Find events
SHA256	1a141682b211260c62d15130308954ca5da0525dac88fd49581b2ad97185d9612e	MDS	78aaae9e74f77896c94b5c83992e0b1bf
Object type	Unknown	SHA256	1a141682b211260c62d15130308954ca5da0525dac88fd49581b2ad97185d9612e
Detect mode	Default		
Event time	2024-02-02 11:31:11:947	System info	

Если Endpoint-агент установлен в составе Kaspersky Endpoint Security, кроме активности процессов он будет также пересыпать детекты Kaspersky Endpoint Security, причем в том числе и так называемые «тихие» детекты, которые не видны в журналах самого Kaspersky Endpoint Security.

Обнаружения KES попадают в базу ТАА как обычные события от Endpoint-агентов. Их можно найти через Threat hunting, но не нужно ожидать их увидеть в списке Alerts.

Информация о детектах KES может помочь оценить ущерб от угроз или добавить веса связанным событиям. Или, наоборот, подскажет аналитику, что локальное средство защиты успешно заблокировало атаку и инцидент можно считать исчерпанным.

События Kaspersky Endpoint Security можно искать по условию EventType = Detect processing result. В описании таких событий приводится время обнаружения, имя угрозы по классификации Kaspersky Endpoint Security и последнее примененное действие.

Создание исключений ТАА

183

Исключение **отключает** и **обнаружение** и **разметку**

Если правило ТАА производит много малополезных обнаружений, для него можно создать исключение. Исключения поддерживаются только для обновляемых правил ТАА. Если возникает необходимость отключить пользовательское правило ТАА, его можно выключить или удалить в разделе User rules | ТАА.

Чтобы создать исключение для правила ТАА, поступившего с обновлениями, в карточке обнаружения кликните по имени правила в секции Scan results. В открывшемся описании правила используйте кнопку Add to exclusions в шапке карточки.

Исключения ТАА с дополнительными условиями

184

При необходимости можно создать исключение из правила ТАА с дополнительными условиями,

для этого при создании исключения необходимо выбрать **Exclude rule – Based on conditions** и задать необходимые условия.

Управление исключениями ТАА

Исключения можно **удалить** или **перенастроить**

Создать исключение можно **только из свойств** правила

Позже все исключенные правила можно найти в разделе **Settings | Exclusions** на вкладке **TAA exclusions**. Здесь можно удалить исключение, чтобы правило снова применялось к поступающей телеметрии.

Конструктор запросов поиска угроз

Position 6 : 2 CTRL+SPACE for autocomplete CTRL+ENTER to search Autoformat

Поиск угроз — это мощный инструмент детектирования в умелых руках. Опытный аналитик может формировать сложные условия поиска, и находить как явные индикаторы компрометации, так и неявные индикаторы атак.

Endpoint-агенты сообщают на Центральный узел о всевозможных событиях на узлах: запуске процессов, загрузке библиотек, установке служб и драйверов, изменении файлов, создании и изменении ключей реестра, установлении соединений. Все это доступно для поиска сотрудникам службы безопасности.

В условиях поиска аналитик настраивает атрибуты событий, операторы сравнения и значения, с которыми нужно сравнивать выбранный атрибут.

Атрибутами могут быть имя компьютера, его адрес, имя файла, путь к файлу, контрольная сумма, время изменения или создания, имя родительского процесса, имя загруженной библиотеки и многое другое, включая, среди прочего, типы событий в журнале Windows и события обнаружения угроз Kaspersky Endpoint Security.

Операторы сравнения могут быть строгими, такими как «равняется» или «не равняется», или нестрогими, такими как «включает», «начинается», «заканчивается». Доступные операторы зависят от выбранного атрибута поиска.

Значением в условии поиска может быть произвольная строка или число в зависимости от типа атрибута. Для некоторых атрибутов значения фиксированы и доступны в виде списка.

Аналитик может объединять несколько условий операторами И и ИЛИ. Для более сложного поиска можно сначала объединить условия в группы и затем объединить группы операторами И и ИЛИ.

Отдельно от условий поиска можно задать временной интервал в верхнем правом углу раздела Threat hunting. По умолчанию задано значение Last day. Аналитик может ограничить поиск одним часом или задать любой произвольный интервал для поиска.

Пользовательские правила ТАА из результатов поиска 187

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. On the left, there's a sidebar with 'ABC corp' selected. The main area is titled 'Threat Hunting' with a search bar containing the query: 'RegistryOperationType = "Registry modified" AND host = "alex-desktop.abc.lab" AND (RegistryKey CONTAINS "\REGISTRY\USER\S-1-5-21-325402544-36615148-1514834948-1104\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" OR Operation type Registry modified Value name failed_count Value data 0)'.

Below the search bar, it says 'All events > ABC corp/kata-cn.abc.lab > Registry modified (5 events)'. A table lists the events: 'Event time', 'Event type', 'Host name', and 'Details'. One event is shown: '2023-03-11 Registry modified alex-desktop.abc.lab Key path: \REGISTRY\USER\S-1-5-21-325402544-36615148-1514834948-1104\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Operation type Registry modified Value name failed_count Value data 0'.

To the right, a modal window titled 'New TAA (IOA) rule' is open. It contains a note: 'It is highly recommended that you test custom TAA (IOA) rules in a test environment before you import them. Custom TAA (IOA) rules may cause performance issues, in which case stable performance of Kaspersky Anti Targeted Attack Platform is not guaranteed.' Below this, there are fields for 'Name*' (My_TAA_rule), 'Description', 'Importance' (Low), 'Confidence' (Low), 'Generate alerts' (Disabled), and 'Apply to' (ABC corp, kata-cn.abc.lab). The bottom right of the modal shows '127.0.0.1'.

Удачные комбинации условий можно сохранять как пользовательские правила для разметки или создания обнаружения

Любые условия поиска в Threat hunting можно сохранить как пользовательское правило для технологии Targeted Attack Analyzer. Правила ТАА, в сущности, и являются условиями для поиска событий с подозрительными атрибутами, как, например, запуск certutil с параметром urlcache, что позволяет сохранить файл на компьютер с помощью системной утилиты.

Обновляемые правила ТАА составлены экспертами Лаборатории Касперского на основании их опыта в поиске признаков атак в сети Лаборатории Касперского и в сетях клиентов.

Сотрудник службы безопасности вполне может обнаружить новые методы злоумышленников в телеметрии с узлов сети. Например, он может расследовать обнаруженные подозрительные действия и увидеть рядом также подозрительные действия, которые не были обнаружены, поскольку являются новой и ранее не использованной техникой злоумышленников.

В этом случае сотрудник ИБ может описать обнаруженную активность параметрами поиска Threat hunting и сохранить как пользовательское правило ТАА.

Пользовательские правила применяются также, как и загружаемые правила ТАА: в реальном времени ко всем новым поступающим событиям от узлов сети. Если какие-то события соответствуют условиям правила, они получают метку (tag) с именем этого правила. Такие события потом визуально выделяются в результатах поиска Threat Hunting.

Если сотрудник ИБ считает, что его правило характеризует опасную активность и эта активность обязательно требует расследования, он может включить для такого правила флаг Generate alerts. В этом случае Центральный узел будет создавать обнаружения ТАА при срабатывании правила.

Еще сотрудник ИБ может настроить для своих правил уровень важности и уровень уверенности — отдельно для каждого правила. Уверенность призвана отражать вероятность того, что описанная активность может быть не вредоносной.

Например, выполнение certutil с параметром -decode может быть частью скрытной деятельности злоумышленников, но может быть и вполне обычным использованием certutil в скрипте, созданном сотрудниками ИТ. Для такого события уверенность можно установить на среднем уровне. В общем случае уверенность зависит не только от самой активности, но и от практик, принятых в организации. Если практики ИТ не разрешают сотрудникам использовать certutil с параметром -urlcache или -decode, соответствующая активность для этой организации может иметь высокий уровень уверенности.

Важность призвана отражать потенциальную опасность описанной активности. От важности зависит цвет метки на событии, а также уровень важности обнаружения, если для правила ТАА установлен флаг Generate alerts.

Пользовательские правила ТАА можно найти в разделе User rules | ТАА. Здесь сотрудник ИБ может отключить правила, которые больше не приносят пользы, а также изменить атрибуты правила: имя, уровни важности и уверенности, флаг Generate alerts.

Здесь же можно импортировать правила из файла в формате OpenIOC. Такие файлы можно найти в отчетах об атаках, в потоках данных от Лаборатории Касперского или других вендоров, а также в публичных источниках.

Изменить условия поиска в правиле нельзя. Вместо этого нужно загрузить правило в Threat hunting по ссылке Run query в карточке правила, отредактировать условия поиска в Threat hunting, и сохранить как новое правило ТАА.

Run query загружает в Threat hunting оригинальные условия поиска и позволяет найти любые события, удовлетворяющие условиям, во всей базе телеметрии. Ссылка Find events тоже формирует поиск в Threat hunting, но ищет только события, которые имеют метку (tag) от этого правила. Метка есть только у тех событий, которые были обработаны, когда правило было активно. Например, у событий, собранных до того, как правило было создано, не может быть метки правила.

Иными словами, Run query можно использовать для ретроспективного поиска по базе телеметрии. Find events ищет события, размеченные правилом. Find alerts ищет обнаружения созданные по этому правилу.

Для загружаемых правил ТАА можно создавать исключения. Для пользовательских правил ТАА исключения не предусмотрены. Если пользовательское правило генерирует много бесполезных

меток или обнаружений, его следует изменить, отключить или удалить.

Технология ТАА на центральном узле в реальном времени сравнивает события, поступающие от Endpoint-агентов, с набором правил ТАА. События, соответствующие условиям правила, получают метку (tag) соответствующего правила. Эти метки видны в карточке события в результатах поиска Threat Hunting. В зависимости от настроек правила, Центральный узел также создает обнаружения.

6.3. Реагирование на инцидент

Инструменты реагирования					188
Инструмент	KEA 3.16	KES 12.3	KESL 12.0	KES for MAC 12	
Получение файла	+	+	+	+	
Сбор форензики	+	+			
Получение ключа реестра	+	+			
Получение метафайлов NTFS	+	+			
Получение дампа памяти процесса	+	+			
Получение образа диска	+	+			
Получение дампа оперативной памяти	+	+			
Завершения процесса / Завершить процесс по PID	+	+	+		
Проверка YARA	+	+			

За обнаружением признаков атаки должна следовать немедленная реакция со стороны сотрудников службы безопасности. В хорошо организованном отделе информационной безопасности должна быть продуманная и отлаженная процедура реагирования на инциденты. Такая процедура среди прочего может включать следующие меры:

- Изолировать скомпрометированные компьютеры от сети.
- Проанализировать недавние события на компьютерах.
- Идентифицировать подозрительные или явно вредоносные файлы.
- Запретить доступ к таким файлам на всех компьютерах сети.
- Остановить выявленные вредоносные процессы и удалить вредоносные файлы.
- Выполнить анализ кода вредоносных файлов и выяснить, что они делают.
- Получить различного рода информацию для анализа и расследования инцидента.

Инструменты реагирования

189

Инструмент	KEA 3.16	KES 12.3	KESL 12.0	KES for MAC 12
Управление службами	+	+		
Запустить приложения	+	+	+	+
Удаление файла	+	+	+	
Помещение/восстановление файла из карантина	+	+		
Сетевая изоляция	+	+	+	
Запрет запуска	+	+		
Поиск IOС	+	+	+	

Возможности реагирования зависят от используемых Endpoint-агентов, включая тип Endpoint-агента и его версию.

Учитывайте это при планировании развертывания Endpoint-агентов и планировании реагирования на возникающие угрозы.

Изоляция компьютера от сети

190

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. On the left, there's a sidebar with navigation links like ABC corp, Dashboard, Alerts, Threat Hunting, Tasks, Prevention, Custom rules, Storage, Endpoint Agents, Reports, and Settings. The main area shows a timeline of events under 'All events > ABC corp/kata-cn.abc.lab > Process started'. A specific event for 'services.exe' is highlighted. To the right, a modal window titled 'Isolation of host alex-desktop.abc.lab' is open, allowing configuration of isolation duration (8 hours), traffic direction (Incoming/Outgoing), and ports. Below the modal, a box titled 'Встроенные исключения' (Built-in exceptions) lists 'DHCP', 'DNS', and 'Программы Лаборатории Касперского' (Kaspersky Lab programs). At the bottom of the modal, there are notes about local administrator access and server certificate changes.

Чтобы изолировать компьютер в сети средствами Kaspersky Endpoint Detection and Response, нужно чтобы на нем был установлен Endpoint-агент с полностью активированными функциями EDR.

Изолировать компьютер может старший сотрудник службы безопасности из свойств компьютера в списке Endpoint-агентов в консоли Центрального узла, или в любом другом разделе консоли, где отображается имя компьютера. Например, старший сотрудник службы безопасности может активировать сетевую изоляцию в контекстном меню имени компьютера в свойствах обнаружения или в свойствах события в Threat hunting.

Сетевая изоляция выполняется Endpoint-агентом с помощью пакетного фильтра операционной системы Windows. Сетевая изоляция блокирует все входящие и исходящие пакеты и соединения кроме тех, для которых заданы исключения.

В Endpoint-агенте есть безусловные исключения для:

- Протоколов DNS и DHCP, чтобы не нарушить работоспособность компьютера и, в частности, способность Endpoint-агента связываться с Центральным узлом.
- Для служб и процессов самого Kaspersky Endpoint Agent, а также других приложений Лаборатории Касперского, которые могут быть установлены на компьютере:
- Kaspersky Endpoint Security,
- Kaspersky Security for Windows Servers,
- Сервера администрирования Kaspersky Security Center,
- Агента администрирования KSC .

Любые другие исключения старший сотрудник службы безопасности должен создать вручную, используя простой список настроек:

- Направление трафика— может принимать значения «Исходящие», «Входящие» или «Входящие/Исходящие» и означает направление пакетов или соединений.
- IP — допускает только отдельные IP-адреса. Означает адрес удаленного компьютера, на который или с которого нужно разрешить пакеты или соединения.
- Ports — допускает номер порта или диапазон портов. Доступно только для направлений «Входящие» и «Исходящие». Если порт задан, будут разрешены TCP-соединения на этот порт, если порт не задан, разрешены любые пакеты и соединения на или с указанного IP.

Например, старший сотрудник службы безопасности может разрешить входящие соединения для подключения к рабочему столу компьютера для более детального расследования.

При применении изоляции Kaspersky Endpoint Agent показывает уведомление локальному пользователю о том, что компьютер будет изолирован от сети, и перечисляет заданные исключения.

Исключения можно настраивать и после того, как изоляция уже включена. Поскольку встроенные исключения не мешают Endpoint-агенту связываться с Центральным узлом, он сможет получить и применить новые настройки.

При включении изоляции старший сотрудник службы безопасности также указывает отсчет времени до отключения изоляции. По умолчанию этот параметр имеет значение 8 часов, чего должно быть достаточно для расследования большинства инцидентов.

Отсчет времени до отключения изоляции сбрасывается (т.е. начинается заново) при любых изменениях параметров изоляции:

- Изменении значения самого отсчета времени;
- Изменении списка исключений.

Отсчет времени до отключения изоляции также сбрасывается при перезагрузке службы Kaspersky Endpoint Agent на компьютере.

Изолированные компьютеры отмечены специальной пиктограммой в списке Endpoint-агентов: красный кирпич в красном круге. Но легко представить, что, если к центральному узлу подключено несколько сотен или тысяч узлов, найти в их списке изолированный компьютер может быть непросто.

Чтобы быстро найти изолированные компьютеры, используйте фильтр, доступный в настройках заголовка Host в списке Endpoint-агентов. Отметьте в окне фильтра опцию Show isolated Endpoint Agents only и список покажет только изолированные компьютеры. В свойствах изолированного компьютера о том, что он изолирован, говорит красное предупреждение вверху окна.

Изолированный компьютер продолжает принимать команды от Центрального узла, потому что соединения Endpoint-агента всегда исключены из изоляции. Это позволяет старшему сотруднику службы безопасности снять изоляцию в любой момент или изменить настройки исключений, не снимая изоляцию.

The screenshot shows two main windows from the Kaspersky Anti Targeted Attack Platform:

- Left Window (Event Details):** Shows an event titled "Process started" for "svchost.exe" (File: "C:\Windows\System32\svchost.exe", Process ID: 4416). The event details include MD5 and SHA256 hashes, launch parameters, and system information.
- Right Window (Prevention Rule Configuration):** A modal dialog titled "New prevention rule" with the following settings:
 - State:** Enabled
 - MD5/SHA256:** d9e577bf078c45954f4531885478d5e9
 - Name:** (empty)
 - Type:** Global
 - Notification:** Notify user about blocking file execution
 - Prevent on:** ABC corp
 - Hosts:** All hosts, Specified servers, Specified hosts (selected)
 - Hosts Filter:** Enter the IP address or host name

Text Overlay:

Можно создать из любого хэша
Поддерживается запрет доступа к
■ Исполняемым файлам
■ Скриптам
■ Документам MS Office и PDF

Изоляция скомпрометированного хоста — это первый шаг по сдерживанию угрозы. Не менее важно запретить доступ к известным опасным объектам на остальных компьютерах сети.

Этой цели служат так называемые политики предотвращения запуска, доступные в разделе Prevention. Старший сотрудник службы безопасности может запретить доступ к файлу из контекстного меню контрольной суммы файла где угодно в консоли Центрального узла, например, в описании угрозы или в свойствах события Threat hunting.

Блокировать доступ к файлам можно только по контрольной сумме. Это может быть и MD5, и SHA256. Дополнительно в свойствах правила блокирования можно задать:

- имя правила (не имя файла);
- показывать ли пользователю сообщение о блокировании доступа;
- область действия правила — все компьютеры или выбранные компьютеры. Чтобы выбрать компьютер, введите часть его имени, подождите, пока появится список компьютеров с подходящими именами и выберите компьютер в списке. Можно выбрать сколько угодно компьютеров.

В распределенной установке дополнительно можно выбрать областью действия все хосты отдельного Центрального узла в рамках компании.

Правила блокирования доступа (политика) 192

Список хешей для блокирования можно импортировать из файла

Каждый хеш в новой строке

До 50000 хешей

Все заданные правила блокирования можно найти в разделе Prevention. Здесь же можно менять их настройки:

- выключать или включать правила;
- менять параметры: значение контрольной суммы, область действия;
- удалять ненужные правила.

Блокирование распространяется не на все типы файлов и операции с файлами, а только на следующие:

- запуск исполняемых файлов;
- запуск скриптов с помощью интерпретаторов (cmd, powershell, java, regsvr32 и др.);
- открытие документов в их родных приложениях:
- doc, docx, rtf и пр. — в Microsoft Word и Wordpad;
- xls,xlsx, csv и пр. — в Microsoft Excel;
- ppt, ppx и пр. — в Microsoft PowerPoint;
- pdf — в Acrobat Reader, Microsoft Edge и Google Chrome.

Блокировать документы для всех приложений большого смысла нет. Доступ к документам блокируется для тех приложений, которые могут быть уязвимы к несанкционированному выполнению кода при работе с документами.

Завершить процессс

193

Для корректного завершения процесса нужен **полный путь** к файлу

Переменные среды и спецсимволы **не поддерживаются**

Когда срочные меры по сдерживанию угрозы приняты, можно в более неспешном порядке начать анализ ситуации на скомпрометированных и изолированных компьютерах. В этом помогут задачи Kaspersky Endpoint Detection and Response.

Для борьбы с активной угрозой поможет задача Kill process. У нее можно задать параметры:

- Путь к файлу — главный параметр задачи, без которого ее нельзя создать. Допускает только полный путь к файлу, переменные среды и спецсимволы не работают.
- MD5/SHA256 — необязательный уточняющий параметр, за счет которого можно отличить вредоносный процесс, который маскируется под одноименный легитимный процесс.
- Описание — произвольный поясняющий текст.
- Область действия — все или выбранные компьютеры.

В распределенной установке также можно выбрать все компьютеры одного Центрального узла или всех Центральных узлов компании.

Задачу Kill process можно создавать из событий в Threat hunting. В описании события запуска процесса есть путь к исполняемому файлу процесса. При щелчке мышью по пути к файлу открывается контекстное меню, где есть возможность создавать задачи. Альтернативно, над карточкой события в Threat hunting есть панель быстрого доступа к инструментам реагирования, и там можно создать задачу Kill process из меню Create a task.

При создании задачи из события не нужно вводить путь к файлу, он подставляется автоматически из атрибутов события.

После запуска задачи Kill process, результаты ее выполнения можно найти в узле Tasks. В карточке задачи для каждого компьютера будет написано, успешно или неуспешно завершилась операция. Чаще всего, если операция завершилась неуспешно, это просто потому, что на компьютере нет такого файла или такого процесса.

194

Завершить процесс по PID

Задачу **Kill unique process** можно создать только из свойств события

Например, чтобы завершить скомпрометированный процесс **svchost.exe** и не затронуть нескомпрометированные

Иногда в результате использования уязвимости злоумышленникам удается внедрить вредоносный код непосредственно в системный процесс в памяти. Нередко таким процессом оказывается svchost.exe, который может быть скомпрометирован в результате сетевой уязвимости.

Обычная задача Kill process позволяет указать только полный путь к файлу и его контрольную сумму, но не позволяет различить несколько процессов с одним и тем же исполняемым файлом. Если в такой задаче указать процесс svchost.exe, она попытается остановить все системные процессы svchost.exe, последствия чего могут быть нежелательными.

Чтобы остановить отдельный процесс по его PID, нужно сначала средствами Threat hunting локализовать скомпрометированный процесс. После этого с помощью кнопки Create a task или из контекстного меню пути к исполняемому файлу в карточке можно будет создать задачу Kill unique process. Задача автоматически заполнит параметры Process ID, File path, MD5/SHA256 и Host значениями из карточки. Получившаяся задача остановит только процесс с совпадающим Process ID, т. е. сможет точно остановить скомпрометированный процесс и не будет мешать работе остальных процессов.

Вручную указать Process ID в задаче Kill process/Kill unique process нельзя.

Получить файл для анализа 195

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. On the left is a sidebar with navigation items like Threat Hunting, Tasks, Prevention, and Reports. The main area shows a timeline of events with several icons for different processes. A context menu is open over one of the event entries, showing options like 'Isolate admin-laptop.abc.lab', 'Create prevention rule', and 'Create task'. A 'Get file' task configuration dialog is open in the foreground. It has fields for 'File path*' (set to 'C:\Windows\security\database\secedit.sdb'), 'MD5/SHA256' (showing two hash values), and a checked checkbox for 'Send for scanning'. There are also fields for 'Description', 'Task for' (set to 'ABC corp'), and 'Host' (set to 'admin-laptop.abc.lab').

Загружает файл в хранилище на центральном узле

File path — обязательный параметр

Маски и переменные среды не поддерживаются

Send for scanning ставит файл в очередь на проверку технологиями

- Antimalware Engine
- Sandbox
- YARA

Если в ходе расследования аналитик обнаруживает подозрительный файл, имеет смысл проверить его технологиями Центрального узла. Особенно информативными могут оказаться результаты проверки файла на сервере Sandbox.

Для этого служит задача Get file. Ее параметры такие же, как у задач Delete file и Quarantine file, с двумя отличиями:

- Флаг Send for scanning позволяет загрузить файл с компьютера и сразу начать его проверку. Если флаг снять, файл просто попадет в хранилище, и его можно будет проверить позже.
- Задача Get file всегда распространяется на один указанный компьютер.

Задача Get file ничего не делает с файлом на компьютере. Если у аналитика есть серьезные основания полагать, что файл может быть опасным, лучше использовать задачу Quarantine file. Если в результате дополнительного анализа подозрения перерастут в уверенность, можно будет добавить задачу Delete file и распространить ее на все компьютеры сети.

Поместить файл на карантин / восстановить файл 196

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. On the left, there's a sidebar with navigation options like ABC corp, Dashboard, Alerts, Threat Hunting, Tasks, Prevention, Custom rules, Storage, Endpoint Agents, Reports, and Settings. The main area shows a timeline of events under 'All events > ABC.corp/kata-cn.abc.lab > File changed'. A specific event for 'cmd.exe' is selected. A context menu is open over this event, with 'Quarantine file' highlighted. A modal window titled 'Quarantine file' is displayed, containing fields for 'File path*', 'MD5/SHA256', 'Description', 'Task for', and 'Host'. The 'Host' dropdown lists two hosts: 'alex-desktop.abc.lab' (IP 10.28.0.150) and 'kata-cn.abc.lab' (IP 127.0.0.1).

Полезно для файлов, опасность которых еще **не** до конца **установлена**

Карантин находится на узлах с агентом

Файлы из карантина можно восстановить

Удалять все выявленные вредоносные файлы может быть преждевременно. По одной копии каждого уникального файла желательно поместить в карантин, чтобы иметь возможность подробно проанализировать код и поведения такого файла, чтобы лучше понять возможный ущерб от атаки, а также найти дополнительные признаки атаки: узнать адреса серверов управления, имена и контрольные суммы дополнительных модулей, методы, которыми злоумышленники выполняют те или иные действия (техники).

Для этого предназначена задача Quarantine file, которая помещает файл в специальное защищенное хранилище на компьютере. Впоследствии файл можно будет запросить для анализа на Центральный узел, сохранить на компьютер аналитика. Если в результате анализа окажется, что файл не был вредоносным, его можно будет восстановить из карантина.

Поместить файл на карантин / восстановить файл

197

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. In the top left, there's a sidebar with 'ABC corp >', 'Dashboard', 'Alerts' (with a red notification dot), 'Threat Hunting', and 'Tasks'. The main area is titled 'Tasks' and lists several entries:

Time	Type	Name	Details	Description	Servers
2023-02-11 12:25:18	Global	Quarantine ...	File path C:\Users\sl...		1 node
2023-02-11 10:45:32	Global	Start YARA s...	Scan All local disks	YARA rules: file_by...	1 node
2023-02-07 13:35:33	Global	Get disk ima...	Share path: \120.28...	Volume E	1 node
2023-02-07 13:24:37	Global	Get disk ima...	Share path: \120.28...	Volume E	1 node
2023-02-07 13:22:26	Global	Get disk ima...	Share path: \120.28...	Volume E	1 node

A context menu is open over the first task, showing options like 'Get data', 'Kill process', 'Start YARA scan', etc. Below the tasks list is a modal window titled 'Restore file from quarantine' with fields for 'Description' and 'File search' containing 'E:\nginx.exe'. At the bottom of the modal is a table with one row:

2023-02-07 11:49:51	E:\nginx.exe	Server: kaspersky	Host: aev-desk01.solo
---------------------	--------------	-------------------	-----------------------

Полезно для файлов, опасность которых еще **не** до конца **установлена**

Карантин находится на **узлах с агентом**

Файлы из карантина можно
восстановить

Восстановить файл из карантина можно отдельной задачей Restore file from quarantine из раздела Tasks.

Увидеть, какие файлы хранятся в локальных карантинах на узлах можно в разделе Storage | Quarantine. Офицер безопасности может удаленно выполнять операции с файлами на карантине:

- Delete — безвозвратно удалить файл.
- Restore — восстановить файл в исходное расположение.
- Get file — загрузить файл с компьютера в хранилище Центрального узла для проверки технологиями Центрального узла.

Операции выполняются при синхронизации Endpoint-агента с Центральным узлом, по умолчанию раз в 5 минут. Результаты выполнения операций доставляются на следующей синхронизации.

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. On the left, there's a sidebar with navigation options like Dashboard, Alerts, Threat Hunting, Tasks, Prevention, Custom rules, Storage, Reports, and Settings. In the center, under Threat Hunting, a 'File removed' event is selected. A context menu is open over the event, with 'Delete file' highlighted. To the right, a 'Delete file' task configuration dialog is open. It shows the file path 'C:\Users\alex\ABC_000\Downloads\|~d'. The 'Task for' dropdown is set to 'ABC corp'. The 'Hosts*' section shows two hosts: 'alex-desktop abc.lab' (IP 10.28.0.150) and 'kata-cn.abc.lab' (IP 127.0.0.1). A note on the right side of the dialog says: 'Полезно для очистки компьютеров после расследования инцидента' (Useful for cleaning computers after investigating an incident).

В ходе расследования инцидента аналитик может выявить на компьютерах вредоносные исполняемые файлы и связанные с ними служебные файлы. Одну копию каждого вредоносного файла имеет смысл поместить в карантин для дальнейшего исследования. Но все остальные копии на других компьютерах можно просто удалить. Также удалить можно неисполнимые файлы, связанные с атакой. Например, файлы с дампом веток реестра, которые злоумышленники могли сохранять для выяснения паролей.

Для этой цели идеально подходит задача Delete file. У нее почти такие же параметры, как и у задачи Kill process: * Путь к файлу — главный параметр задачи, без которого ее нельзя создать. Допускает только полный путь к файлу, переменные среды и спецсимволы не работают. * MD5/SHA256 — необязательный уточняющий параметр, за счет которого можно отличить вредоносный процесс, который маскируется под одноименный легитимный процесс. * Описание — произвольный поясняющий текст. * Область действия — все или выбранные компьютеры.

В распределенной установке также можно выбрать все компьютеры одного Центрального узла или всех Центральных узлов компании.

Задачу Delete file, как и другие задачи, можно создавать из контекста событий в Threat hunting: из панели быстрого доступа над карточкой события или из контекстного меню, которое открывается при щелчке по имени файла в описании события.

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. On the left, there's a sidebar with navigation links like ABC corp, Dashboard, Alerts, Threat Hunting, Tasks, Prevention, Custom rules, Storage, Endpoint Agents, Reports, and Settings. The main area shows a timeline with events: 'cmd.exe' at 46 and 'cmd.exe' at 1. A specific event for 'UDSTrojan' is selected. A context menu is open over this event, with 'Get forensics' highlighted. To the right, a modal window titled 'Get forensics' is displayed. It has several sections: 'Information type*' with checkboxes for 'Processes list', 'Autorun points list', and 'File list' (which is checked); 'Source type' with a radio button for 'Directory' (selected); 'Start directory*' set to 'C:\Users\alex\ABC.000\Downloads\'; 'File mask' set to '*'; 'Alternative data streams' with a checked 'Get data' option; 'Maximum nesting level' set to 'Enter an integer'; 'Exclusions' (empty); 'Description' (empty); 'Task for' set to 'ABC corp'; and 'Host' with two entries: 'alex-desktop.abc.lab' (IP 10.28.0.150) and 'kata-on.abc.lab' (IP 127.0.0.1).

Вы можете получить списки файлов, процессов и точек автозапуска с выбранных хостов Kaspersky Endpoint Agent для Windows. Для этого нужно создать задачу сбора данных.

Тип информации — тип собираемых данных. Установите флажок напротив одного, нескольких или всех параметров:

- Список процессов, если хотите получить список процессов, запущенных на хосте в момент выполнения задачи.
- Список точек автозапуска, если хотите получить список точек автозапуска.

В список точек автозапуска включаются данные о программах, добавленных в папку автозагрузки или зарегистрированных в разделах реестра Run, а также о программах, которые запускаются автоматически при загрузке хоста с Kaspersky Endpoint Agent и при входе пользователя в систему на указанных хостах.

- Список файлов, если хотите получить список файлов, хранящихся в выбранной папке или во всех папках хоста в момент выполнения задачи.

Управлять службой 200

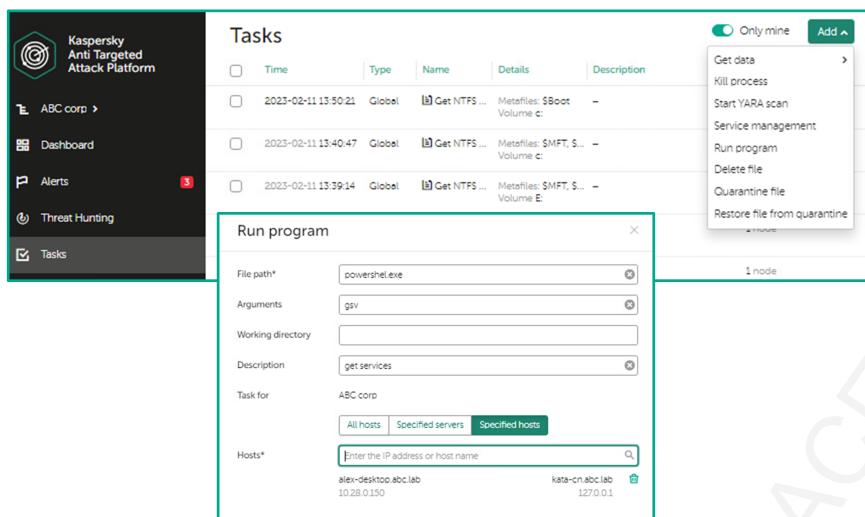
The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. On the left is a sidebar with navigation links: ABC corp, Dashboard, Alerts (with 3 notifications), Threat Hunting, and Tasks (selected). The main area displays a table of tasks with columns: Time, Type, Name, Details, and Description. Three tasks are listed, all of which are Global type. The first task details are: Time 2023-02-11 13:50:21, Type Global, Name Get NTFS..., Details Metafiles: \$Boot, Volume: c:, Description -. The second task details are: Time 2023-02-11 13:40:47, Type Global, Name Get NTFS..., Details Metafiles: \$MFT, \$..., Volume: c:, Description -. The third task details are: Time 2023-02-11 13:39:14, Type Global, Name Get NTFS..., Details Metafiles: \$MFT, \$..., Volume: F:, Description -. An open modal window titled 'Service management' contains fields for Service name (kinagent), MDS/SHA256 (MD5/SHA256), Action (Stop), Description, Task for (ABC corp), and Hosts (Specified servers). The 'Hosts' section includes a search bar and a list of hosts: alex-desktop.abc.lab (10.28.0.150) and kata-cn.abc.lab (127.0.0.1). A context menu is open at the top right, with 'Service management' highlighted. Other menu items include 'Get data', 'Kill process', 'Start YARA scan', 'Service management', 'Run program', 'Delete file', 'Quarantine file', and 'Restore file from quarantine'. A note '1 node' is visible at the bottom of the menu.

Есть возможность производить некоторые действия над службами:

- Запустить,
- Остановить,
- Приостановить,
- Продолжить,
- Удалить,
- Изменить тип запуска.

Выполнить программу

201



Если перечисленных выше задач не хватает для полноценного расследования инцидента, в арсенале Kaspersky Endpoint Detection and Response есть задача Run program, которая позволяет удаленно выполнить на компьютере произвольную команду или запустить произвольную программу.

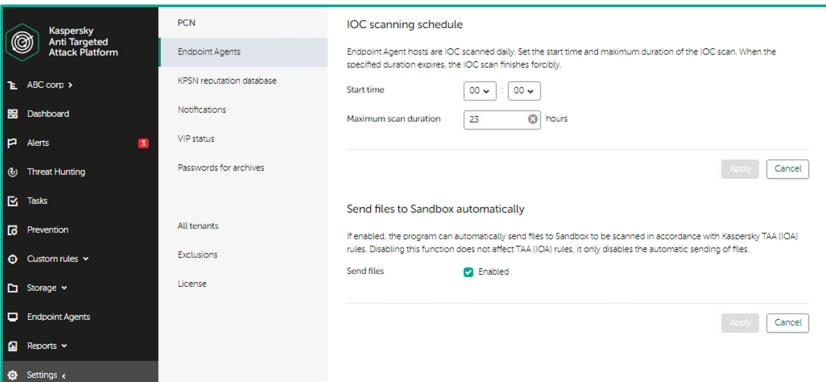
Для выполнения команды нужно указать:

- Исполняемый файл, который будет запущен на компьютере. Файл должен уже быть на целевом компьютере. Задача не позволяет выбрать файл на компьютере аналитика, скопировать его на целевой компьютер и там запустить.
- Параметры командной строки (опционально).
- Рабочую папку для выполнения команды (опционально).

Задачу Run program можно запускать на всех компьютерах сразу или на выбранных компьютерах.

При выполнении задачи Run program Endpoint-агент передает на Центральный узел содержимое кода возврата, а также стандартных потоков вывода и ошибок. Все это доступно отдельно для каждого компьютера в карточке задачи. Так, например, содержимое стандартного потока вывода доступно по ссылке Standard output и открывается в отдельной вкладке.

Поиск IOC на компьютерах



The screenshot shows the 'IOC scanning schedule' configuration for 'Endpoint Agents'. It includes fields for 'Start time' (00:00), 'Maximum scan duration' (23 hours), and a checkbox for 'Send files to Sandbox automatically' which is checked and labeled 'Enabled'. There are 'Apply' and 'Cancel' buttons at the bottom right.

202

Охват поиска

- Все компьютеры (агенты)

Время запуска

- в зоне UTC +0

Область поиска

- Весь компьютер

Чтобы запустить поиск индикаторов компрометации (IOC) на хостах, необходимо прежде всего для каждого IOC, которое необходимо искать на хостах, выставить значение параметра Autoscan – Enabled в разделе Custom rules | IOC.

Расписание проверки можно выставить в разделе Settings | Endpoint Agents | IOC scanning schedule.

Охват поиска - все компьютеры (Endpoint-агенты).

Время запуска - в зоне UTC +0.

Область поиска - весь компьютер.

Проверка компьютеров YARA-правилами

203

Сканирование выполняется по запросу

При срабатывании создается обнаружение

Никакие действия к файлу не применяются

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. On the left, there's a sidebar with 'Custom rules' expanded, showing 'YARA' selected. In the center, a 'YARA' section displays a rule named 'file_by_md5_hash'. The 'Details' tab shows the rule configuration, including 'Rule name: file_by_md5_hash', 'Traffic scan: Enabled', 'Importance: High', and 'Type: Global'. The 'Apply to*' field contains 'ABC corp' and 'kata-cn.abc.lab'. Below the configuration is the YARA rule code:

```
rule file_by_md5_hash {
    condition:
        hash.md5 (0, filesize) == "4e4c76f78bcaa32b95cd82ec67d4d828"
}
```

To the right, a 'Start YARA scan' dialog is open. It shows the selected rule 'file_by_md5_hash' and the 'my_yara_rules.txt' file. The 'Scan scope*' section has 'RAM' selected. The 'Processes' section contains the command 'Start each entry on a new line'. The 'Exclusions' section contains the command 'Start each entry on a new line'. The 'Maximum scan duration*' field is set to 23 hours. The 'Task for' field is set to 'ABC corp'. At the bottom, there are 'Add' and 'Cancel' buttons.

Чтобы запустить проверку компьютеров YARA-правилами, необходимо перейти в раздел Custom rules | YARA и далее выбрать нужные правила и нажать Start YARA Scan. В появившемся окне будет возможность добавить дополнительные правила к задаче, выбрать область сканирования, исключения, максимальное время выполнения, перечень компьютеров, на которых будет выполняться задача.

Так же задачу проверки компьютеров YARA-правилами можно создать из раздела Tasks, нажав Add и выбрав Start YARA Scan.

Получить дамп памяти процесса / дамп памяти системы

204

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. On the left, there's a sidebar with 'Tasks' selected. In the center, a 'Tasks' table lists several tasks, including a task named 'Start YARA s...' which is currently running. To the right of the table, a context menu is open over one of the tasks, showing options like 'Get data', 'Kill process', 'Start YARA scan', etc.

Задачу получения дампа памяти процесса или дампа памяти системы можно создать из

The bottom part of the screenshot shows a detailed view of a task configuration. It includes fields for 'Process ID*', 'MD5/SHA256', 'Description', 'Task for', and 'Host'. The 'Description' field contains a command-line for volatility: 'C:\Users\Ozz\Downloads\volatility_2.6.win64_standalone\volatility_2.6.win64_standalone.exe -f C:\Users\Ozz\Downloads\volatility_2.6.win64_standalone\MemoryDump_ksc_2023-01-30T07.27.44Z.dmp --profile=Win2016x64_pslist'. The 'Task for' field is set to 'ABC corp' and the 'Host' field to 'alex-desktop.abc.lab'. A table at the bottom shows memory dump details for three processes: System, smss.exe, and csrss.exe.

PID	PPID	Thds	Hnds	Sess	Wow64 Start	Exit
4	0	127	0	-----	0 2023-01-30 06:49:54 UTC+0000	
396	4	2	0	-----	0 2023-01-30 06:49:54 UTC+0000	
492	488	12	0	0	0 2023-01-30 06:50:02 UTC+0000	

Задачу получения дампа памяти процесса или дампа памяти системы можно создать из

раздела Tasks, нажав Add и выбрав Get data | Memory dump или Process memory dump.

Для задачи Process memory dump необходимо указать:

- Process ID (обязательный параметр);
- MD5/SHA256;
- Description;
- Host (хост, на котором будет запущена задача).

Для задачи Memory dump необходимо указать:

- Share path (сетевая папка, где будет сохранен дамп);
- User name (имя учетной записи для доступа к сетевой папке);
- Password (пароль учетной записи для доступа к сетевой папке);
- Description;
- Host (хост, на котором будет запущена задача).

После получения дампов с ними можно работать, используя сторонние средства, к примеру WinDBG или Volatility Framework.

**для ознакомления с особенностями работы WinDBG или Volatility Framework
обратитесь к справке по соответствующему продукту.**

The screenshot displays the Kaspersky Anti Targeted Attack Platform interface. On the left, there's a sidebar with navigation links like ABC corp, Dashboard, Alerts, Threats, and Tasks. The main area shows a 'Tasks' table with three entries. A context menu is open over the third entry, listing options such as 'Get data', 'Kill process', 'Start YARA scan', etc. Below the table, a 'Get disk image' dialog box is open, prompting for a share path ('\\10.20.100\Users\Administrator\Downloads'), user name ('ABC Administrator'), and password. It also allows selecting disk type (Logical or Physical) and volume. In the bottom right corner, a separate window titled 'PassMark OSFMount' shows a list of 'Mounted virtual disks'. One disk is mounted at 'E:' with the path 'C:\Users\Administrator\Downloads\ksc.abc.lab'. The status bar at the bottom right of the main interface shows the number '205'.

Задачу получения образа диска можно создать из раздела Tasks, нажав Add и выбрав Get data | Disc image.

Для задачи Disc image необходимо указать:

- Share path (сетевая папка, где будет сохранен образ диска);
- User name (имя учетной записи для доступа к сетевой папке);
- Password (пароль учетной записи для доступа к сетевой папке);
- Disk type ;
- Volume;
- Description;
- Host (хост, на котором будет запущена задача).

После получения образа диска с ним можно работать, используя сторонние средства, к примеру OSFMount.

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. On the left, there is a sidebar with navigation links: ABC corp >, Dashboard, Alerts (with 3 notifications), Threat Hunting, and Tasks. The Tasks section is currently selected. In the main area, there is a table titled "Tasks" with columns: Time, Type, Name, Details, and Description. There are five entries in the table. To the right of the table, a context menu is open over the last entry, which has a "Get disk image" action highlighted. Below the table, a modal window titled "Get registry key" is open. It contains fields for "Registry key*" (set to "HKLM\Software\Microsoft\WindowsUpdate\Orchestrator"), "Description" (empty), "Task for" (set to "ABC corp"), and "Host" (a dropdown menu with "Enter the IP address or host name" placeholder, showing options like "alex-desktop.abc.lab" and "10.28.0.150").

Задачу получения ключа реестра можно создать из раздела Tasks, нажав Add и выбрав Get data | Registry Key. Для задачи Registry Key необходимо указать:

- Registry Key;
- Description;
- Host (хост, на котором будет запущена задача).

Получить метафайлы NTFS

207

Задачу получения метафайлов NTFS можно создать из раздела Tasks, нажав Add и выбрав Get data | NTFS metafiles.

Для задачи NTFS metafiles необходимо указать: * Метафайлы, * Том, * Описание, * Хост (на котором будет запущена задача).

Задачи

208

Все задачи, созданные сотрудником службы безопасности, отображаются в разделе Tasks.

Здесь можно увидеть задачи, созданные из карточек обнаружения и карточек событий, а также можно создать задачу любого типа, кроме Kill unique process. (Задачу Kill process создать можно.)

Все задачи в Kaspersky EDR Expert одноразовые. У них нет расписания и их нельзя повторно запустить вручную. Если нужно повторить какую-то операцию, в свойствах задачи есть кнопка **Duplicate**, которая создает новую задачу и копирует в нее настройки оригинала. Настройки новой задачи можно откорректировать перед запуском.

Поскольку задачи являются одноразовыми, список задач заодно является и журналом выполнения задач. По списку можно судить, какие задачи создавали и выполняли различные сотрудники. Впрочем, список задач не является надежным инструментом аудита, т.к. задачи из него можно удалять.

Щелчком мыши по задаче открывается карточка задачи, где видны результаты выполнения задачи. Ошибки, как правило, отображаются в виде кодов возврата Windows . Вот значения некоторых кодов, которые могут встречаться в результатах задач:

- 3 — The system cannot find the path specified.
- 5 — Access is denied.
- 123 — The filename, directory name, or volume label syntax is incorrect.
- 1168 — Element not found.

Хранилище файлов и результаты проверки

Если в ходе расследования аналитик выполнял задачу **Get file** с флагом **Send for scanning**, результаты можно будет найти в разделе **Tasks** в карточке задачи **Get file**. В свойствах задачи можно будет увидеть результаты проверки файла различными технологиями. Если в файле обнаружена угроза, предупреждение о ней попадет и в список предупреждений.

Полные результаты проверки отображаются всегда, даже если угрозы не были обнаружены. В частности, если файл проверялся технологией **Sandbox**, аналитику будут доступны все подробности о запуске файла внутри виртуальных машин. Даже если автоматический анализ ничего не нашел, опытный вирусный аналитик сможет идентифицировать подозрительные действия в отчетах о выполнении файла.

Результаты проверки можно посмотреть также в разделе **Storage | Files**. Все файлы, запрошенные задачами **Get file**, попадают в это хранилище, и если аналитик запрашивал проверку файла, то здесь же отображаются результаты — в карточке файла.

Чтобы проверить файл вручную, не обязательно запрашивать его с одного из компьютеров задачей **Get file**. Загрузить файл можно кнопкой **Upload** в верхнем правом углу раздела **Storage | Files**. Загруженные таким образом файлы будут проверены, но предупреждения по ним не генерируются.

Файлы в хранилище Storage | Files можно:

- Сохранить на компьютер старшего сотрудника службы безопасности;
- Проверить повторно;
- Удалить.

Еще можно запрашивать файлы из раздела Storage | Quarantine, где отображаются файлы, находящиеся в локальных карантинах на компьютерах сети.

Особенности реагирования в распределенной установке

В распределенном режиме предполагается что сотрудники службы безопасности в основном работают в консоли первичного Центрального узла. В этой консоли данные от всех вторичных Центральных узлов компании объединяются в единое представление.

Для этого списки обнаружений, компьютеров, задач, правил блокирования доступа и других объектов консоли реплицируются между базами данных вторичных Центральных узлов и первичного Центрального узла. После этого они доступны в консоли первичного Центрального узла, даже если связи с вторичным Центральным узлом временно нет.

Базы телеметрии от Endpoint-агентов занимают большой объем и реплицировать их нецелесообразно. Вместо этого все запросы в базу телеметрии из консоли первичного Центрального узла передаются в реальном времени на вторичные Центральные узлы. Результаты запроса передаются обратно в рамках того же соединения.

В настройках учетных записей можно дать доступ сотруднику службы безопасности к индивидуальным веб-консолям вторичных Центральных узлов компании. Это позволит, например, сохранить возможность реагирования, если первичный Центральный узел недоступен.

Поиск событий в распределенном режиме

База данных событий телеметрии между Центральными узлами в распределенной установке не реплицируется. Данные об активности, которые поступают от Endpoint-агентов, хранятся в базе того Центрального узла, к которому они подключены.

Сотрудник службы безопасности в веб-консоли первичного Центрального узла может искать события в базах телеметрии всех узлов выбранной компании. Первичный узел перепосыпает запрос поиска на вторичные Центральные узлы и таким образом получает от них результаты. Если в момент выполнения поиска связи с вторичным Центральным узлом нет, результаты поиска на нем доступны не будут.

Endpoint-агенты

Список Endpoint-агентов в консоли первичного Центрального узла отображает компьютеры, подключенные ко всем Центральным узлам компании (или всех компаний, если речь идет о сервис-провайдере). Старший сотрудник службы безопасности может применять к ним все инструменты EDR, в том числе изолировать от сети, при условии, что у первичного Центрального узла есть связь со вторичным Центральным, к которому подключен компьютер.

Хранилище объектов

В хранилище на первичном центральном узле видны объекты хранилищ со всех Центральных узлов выбранной компании. Старший сотрудник службы безопасности может их сохранять на свой компьютер, независимо от того, к какому центральному узлу подключен Endpoint-агент, в локальном хранилище которого хранится объект.

Задачи, правила блокирования, правила обнаружения

В распределенной установке могут быть учетные записи старших сотрудников службы безопасности, которые имеют право входа в веб-консоль отдельного вторичного Центрального узла компании. Они могут создавать задачи реагирования и правила блокирования файлов в консоли вторичного Центрального узла. Эти задачи и настройки являются локальными и распространяются только на один Центральный узел, в консоли которого они созданы.

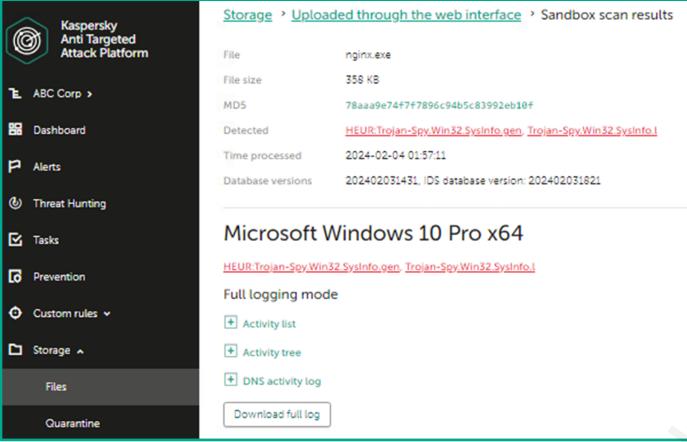
В то же время задачи и правила для всей компании может создавать и старший сотрудник службы безопасности в общей консоли первичного Центрального узла. Эти правила и задачи являются глобальными и распространяются на все Центральные узлы компании.

Списки задач и правил в консоли первичного Центрального узла показывают как глобальные задачи и правила, так и локальные, указывая к какому вторичному центральному узлу они относятся. В консоли первичного Центрального узла отключать или изменять можно только глобальные правила. Локальные правила можно отключить только в локальной консоли вторичного Центрального узла. В консоли вторичного Центрального узла отображаются его локальные задачи и правила, а также глобальные задачи и правила, созданные для компании в консоли первичного Центрального узла. Отключить или изменить тут можно только локальные правила. Глобальные правила можно только читать.

Глава 7. Результаты анализа Sandbox

7.1. Карточка обнаружения Sandbox

Обнаружения Sandbox
209



The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. On the left is a sidebar with navigation links: ABC Corp, Dashboard, Alerts, Threat Hunting, Tasks, Prevention, Custom rules, Storage (selected), Files, and Quarantine. The main area displays a file analysis result for 'nginx.exe'. The details are as follows:

- File: nginx.exe
- File size: 358 KB
- MD5: 78aaa9e7447f7896c94b5c83992eb10f
- Detected: HEUR:Trojan-Spy.Win32.SysInfo.gen, Trojan-Spy.Win32.SysInfo.I
- Time processed: 2024-02-04 01:57:11
- Database versions: 202402031431, IDS database version: 202402031821

Below this, it says 'Microsoft Windows 10 Pro x64' and lists 'HEUR:Trojan-Spy.Win32.SysInfo.gen, Trojan-Spy.Win32.SysInfo.I'. Under 'Full logging mode', there are three options: 'Activity list', 'Activity tree', and 'DNS activity log'. A 'Download full log' button is at the bottom.

Full logging mode

- собирает больше деталей за более короткое время выполнения образца

Quick scan mode

- собирает меньше деталей, но за более длительный период наблюдения

Как проверять, решает модуль AM согласно обновляемой логике

Если угрозу обнаружил сервер Sandbox, в секции Scan results файлового обнаружения будут перечислены все обнаруженные угрозы. Под перечнем названий угроз от сканирующих технологий находится кнопка Sandbox detect, которая открывает более подробное описание результатов. В подробном описании видно, на каких виртуальных машинах проверялся файл и какие опасные действия были обнаружены.

Большинство объектов обрабатывается на нескольких типах виртуальных машин. Если обнаружения от Sandbox нет, то никакие данные в веб-интерфейсе не отображаются. Если Sandbox обнаружил вредоносный объект или подозрительное поведение, то при нажатии на кнопку Sandbox detect откроется дополнительная карточка результатов анализа Sandbox, которая содержит:

- Информацию об объекте (имя файла, размер файла, md5 файла, цифровую подпись);
- Названия обнаруженных угроз;
- Время проверки и версию баз компонентов Scanner и IDS, которые анализировали журналы и артефакты выполнения объекта в виртуальной среде.

Ниже приводятся результаты обработки на каждой из виртуальных машин, которые включают:

- Журнал опасной активности;

- Граф опасной активности, который показывает зависимости между опасными действиями и исходным объектом;
- Журналы сетевой активности (HTTP, DNS и IDS);
- Полный журнал исследования поведения файла в операционной системе.

7.2. Результаты анализа в виртуальной среде

Опасная активность, обнаруженная Sandbox

210

Microsoft Windows 10 Pro x64

File: Trojan-Spy-World-Win32.Trojan-Spy-World.Syphn1

Full logging mode

Activity list

- The process Swindn!System32\systeminfo.exe has tried to discover the system information via the standard Windows Utilities: systeminfo (MITRE T1082 System Information Discovery).
- The process Swindn!System32\cmd.exe has run the wildcard search c:\\$RECYCLE.BIN\\$-f-1-1811.txt (MITRE T1005 Data from Local System).
- The process Swindn!System32\cmd.exe has run the wildcard search c:\\$RECYCLE.BIN\\$-f-1-94006402-10021*txt (MITRE T1005 Data from Local System).
- The process Swindn!System32\cmd.exe has run the wildcard search c:\\$RECYCLE.BIN\\$-f-1-21-423098884-2617871557-94006402-10021*txt (MITRE T1005 Data from Local System).
- The process Swindn!System32\cmd.exe has run the wildcard search c:\\$RECYCLE.BIN\\$-f-1-21-423098884-2617871557-94006402-10021*txt (MITRE T1005 Data from Local System).
- The process Swindn!System32\cmd.exe has run the wildcard search c:\Config.Mal*.txt (MITRE T1005 Data from Local System).

Microsoft Windows 10 Pro x64

File: Trojan-Spy-World-Win32.Trojan-Spy-World.Syphn1

Full logging mode

Activity list

Run sample

Список активности показывает **только подозрительные действия и не претендует на полноту**

Дерево процессов **показывает цепочку** от анализируемого файла до действий, повлиявших на результат анализа

В списке Activity list будут отображены подозрительные действия, обнаруженные при выполнении файла. У каждого действия есть уровень важности, показанный значком слева. Для большинства действий также приводится классификация по матрице MITRE ATT&CK.

В журнале опасных действий можно увидеть такие описания, как:

- самораспаковывающийся архив был запущен в скрытом режиме;
- процесс создал несколько файлов в системной папке system32;
- процесс создал службу;
- процесс создал настройки для автоматического запуска;
- процесс выполнил массовый поиск файлов;
- и т. п.

Активность файла можно отобразить и в виде дерева. Самое левое событие — это запуск файла на виртуальной машине. Все последующие действия файла: запуск дочерних процессов, сохранение новых файлов и запуск их, активность дочерних процессов

разворачивается в виде дерева. Для опасных операций также приводится их классификация по MITRE ATT&CK.

Ниже располагаются три журнала сетевой активности, информация в которых во многом пересекается, но при этом содержит разные аспекты сетевой активности.

HTTP activity log показывает HTTP-запросы из виртуальной машины. Для каждого запроса приводится URL, IP-адрес сервера и тип запроса (GET, POST и т. п.) IP-адреса и URL интерактивны: по щелчку мыши можно выполнить поиск связанных событий и обнаружений, а также перейти на Kaspersky Threat Intelligence Portal, где могут быть географические данные об адресе или имени сервера.

Поиск связанных обнаружений открывает новую вкладку с отфильтрованным списком обнаружений. Поиск связанных событий является функционалом Kaspersky Endpoint Detection and Response. Он также открывает новую вкладку с автоматически заданными параметрами поиска. Аналитик может редактировать условия, чтобы расширить или сузить поиск.

Контекстный поиск по URL ищет по всему URL и не обязательно найдет обращения к тому же серверу, но на другую страницу, или обращения к другому вредоносному серверу с аналогичным запросом. При анализе угроз может быть полезно выполнить контекстный поиск по URL, и, если он ничего не найдет, изменить параметры поиска, оставив только имя сервера или только часть URL.

Сетевая активность за время наблюдения

211

DNS name	Type	Host
settings-win.data.microsoft.com	A	
settings-win.data.microsoft.com	A	
settings-win.data.microsoft.com	CNAME	atm-settingse-prod-geo2.trafficmanager.net
atm-settingse-prod-geo2.trafficmanager.net	CNAME	settings-prod-scs-1.southcentralus.cloudapp.azure.com
settings-prod-scs-1.southcentralus.cloudapp.azure.com	A	52.185.211.133

В сетевую активность часто попадают
рутинные действия
операционной системы

Отличить опасную активность можно за счет запроса в **KL TIP**

IDS activity log во многом повторяет HTTP activity log, но приводит относительные URL без имени сервера, поиск по которым может дать другие результаты, чем поиск по полному URL.

В журнале IDS-активности также есть Source IP, но это IP-адрес виртуальной машины в изолированной служебной сети на сервере Sandbox, и большого интереса он не представляет.

В журнале DNS-активности видно, что была успешная попытка разрешить имя удаленного хоста.

Во всех сетевых журналах может попадаться легитимная активность операционной системы виртуальной машины.

7.3. Отладочная информация Sandbox

Полный журнал активности
212

```

{
    "name": "wildcard_search",
    "id": 19381,
    "parent_id": 909,
    "severity": 290,
    "record_id": 27783372,
    "detect_required": 1,
    "interest_level": 100,
    "description": "Wildcard Searching Data (MITRE: T1005 Data from Local System)",
    "ktz_only": 0,
    "count": 1,
    "class": "susp",
    "keywords": "",
    "properties": {
        "Pid": 3056,
        "process": 100,
        "Image_path": "$windir\\$system32\\cmd.exe",
        "File_path": "$programfiles\\Java\\jre1.8.0_351\\legal\\*.txt"
    },
    "techniques": [
        {
            "technique": "T1005",
            "tactics": [
                "TA0009"
            ]
        }
    ]
}

```

Журнал содержит все запротоколированные события за время выполнения в формате **json**

В карточке анализа объекта технологией Sandbox под списком журналов каждой виртуальной машины находится кнопка Download full log. Она сохраняет в формате JSON полный список операций, запротоколированных на виртуальной машине за время анализа. Этот журнал может помочь аналитику полнее воспроизвести последовательность действий, которая предшествовала явно вредоносной активности.

Sandbox debug info

213

Debug info содержит абсолютно все артефакты, имеющие отношение к запуску и анализу файла

sandbox_config.json

- на каких виртуальных машинах и с какими настройками проверялся объект

multitask_result.json

- все обнаружения, в том числе **SILENT**

task0, task1, task2, task3

- данные собранные с виртуальных машин

пароль: **infected**

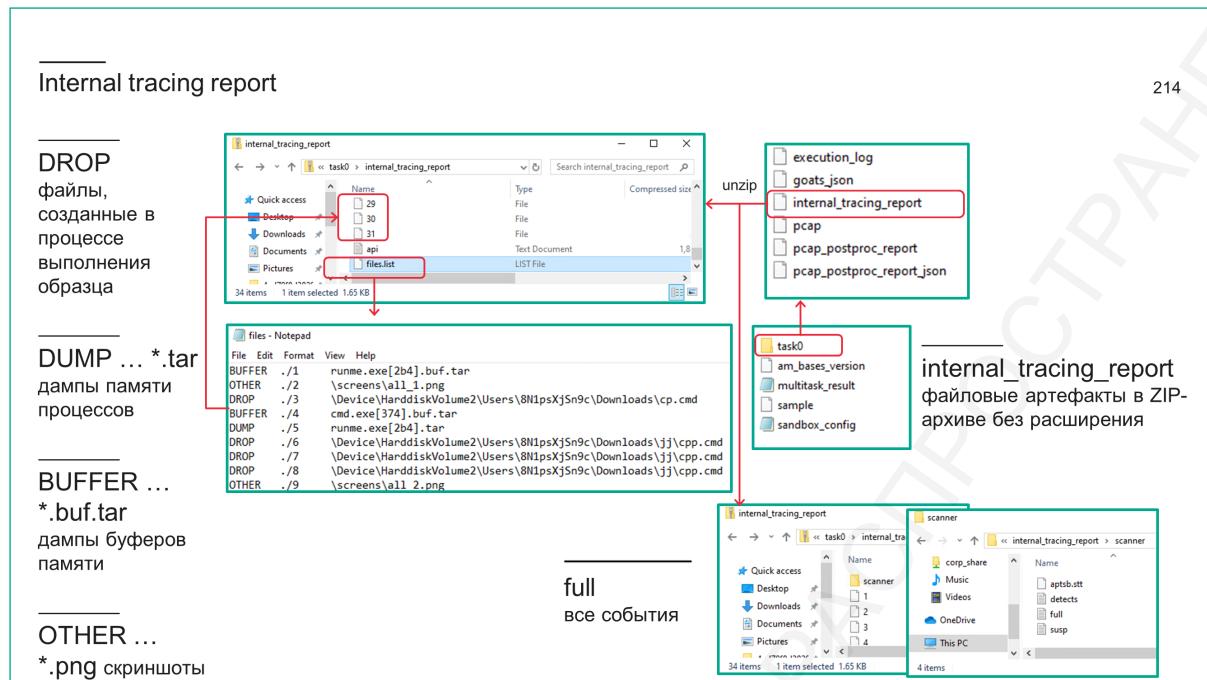
task0
am_bases_version
multitask_result
sample
sandbox_config

Если отображаемых в веб-интерфейсе интерпретированных результатов проверки файла на Sandbox-сервере недостаточно для понимания происходящего и принятия решения в отношении инцидента, то аналитик может обратиться к сведениям об отладке (Debug info). Сведения об отладке также включают в себя все журналы и артефакты, полученные в результате наблюдения за активностью файла в виртуальной среде.

Сведения об отладке — это zip-архив, защищенный паролем, который содержит набор артефактов по результатам проверки файлов в «песочнице». Чтобы распаковать содержимое, используйте пароль **infected**. Название папки соответствует md5-хешу файла.

Внутри архива вы найдете:

- Папки task0, task1, task2 и task3 — результаты проверки после запуска на разных виртуальных машинах и в разных режимах. Файл не всегда запускается на всех типах виртуальных машин, поэтому в архиве может быть менее четырех папок, а иногда и просто одна папка task0.
- multitask_result.json — форматированный результат проверки на всех виртуальных машинах.
- meta — файл со ссылкой, если проверяется ссылка.
- sandbox_config.json — конфигурация Sandbox: на каких виртуальных машинах запускать образец, как именно его запускать (как исполняемый файл, скрипт, документ, или как ссылку, которую надо открыть в браузере), как долго проверять и в каком режиме (полного журналирования или быстрого сканирования).



Если открыть любую из папок taskX, то внутри будут следующие данные:

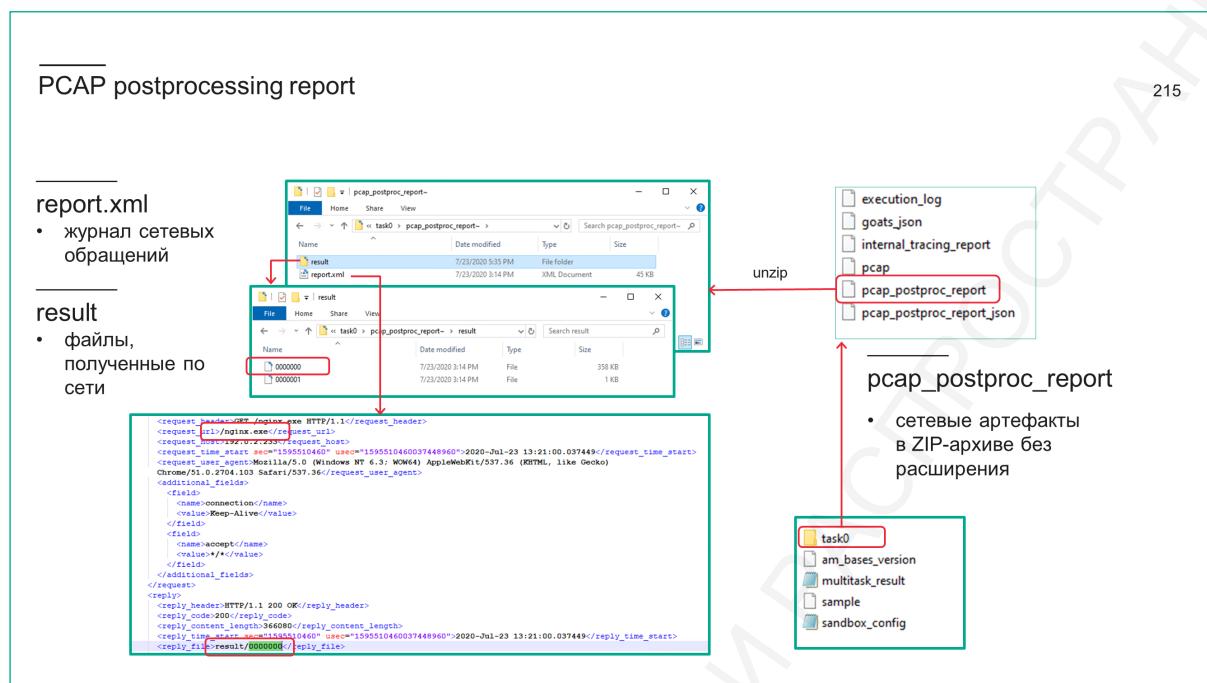
- execution_log — краткий журнал исполнения в json-формате.
- internal_tracing_report — ZIP-архив с системными артефактами (скриншоты, dll-библиотеки, созданные файлы и другое).
- pcap — дамп сетевого трафика.
- pcap_postproc_report — ZIP-архив с сетевыми артефактами (журнал сетевых обращений, загруженные по http файлы).
- goats.json — файл, необходимый для детектирования вредоносной активности.

Если распаковать архив internal_tracing_report, можно найти список файлов, извлеченных из виртуальной машины. Среди этих файлов могут быть новые файлы, сохраненные на диск, скриншоты экрана виртуальной машины, дампы памяти и содержимое буферов в памяти.

Файлы анонимизированы и представлены порядковыми номерами. Что это за объекты, можно найти в файле files.list. Во второй колонке находится анонимизированное имя файла, в третьей его исходное имя, а в первой тип файла:

- DROP — файлы, появившиеся в процессе выполнения образца (извлеченные им из себя, преобразованные из других объектов или загруженные из Internet).
- DUMP — tar-архив с дампом памяти процесса (имя процесса является именем архива).
- BUFFER — tar-архив с дампом буфера памяти процесса.

- OTHER — снимок экрана виртуальной машины в формате PNG.



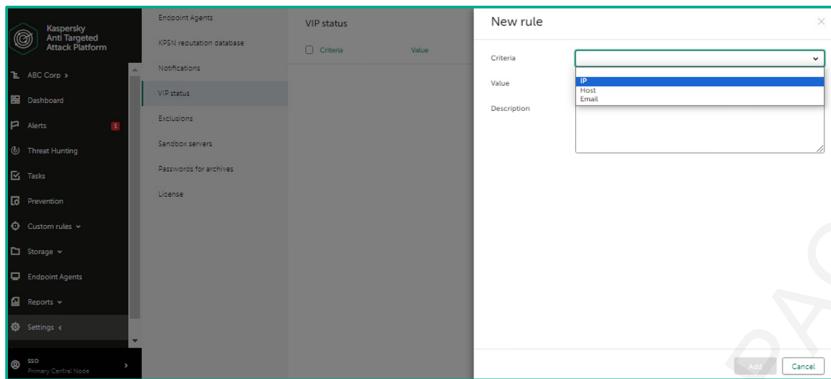
Если распаковать архив pcap_postproc_report, можно найти подробный журнал сетевой активности файла. report.xml содержит информацию о сетевых соединениях. В папке result находятся файлы, загруженные из Internet. Файлы обезличены и представлены номерами. Если выполнить поиск по имени (номеру) обезличенного файла в журнале report.xml, можно найти оригинальное имя файла и URL, по которому он был загружен.

Глава 8. Обслуживание платформы КАТА

8.1. VIP-статус

VIP-узлы

216



Старший сотрудник службы безопасности может

- настроить условия для автоматического назначения статус VIP
- назначить или снять статус VIP вручную

VIP-группа нужна, если нежелательно показывать обычным сотрудникам службы безопасности детали обнаружений, связанных с топ-менеджментом компании или с работой тех или иных отделов. В заголовках почтовых сообщений может содержаться информация, для ознакомления с которой нужен специальный уровень доступа.

VIP-статус можно использовать и просто, чтобы выделить важные обнаружение. Таким обнаружениям посвящена отдельная панель Dashboard, и под них выделен отдельный показатель в статистике над списком обнаружений.

Старший сотрудник службы безопасности настраивает условия присвоения VIP-статуса в разделе **Settings | VIP status**. Условия можно настраивать на основе следующих атрибутов: * IP-адрес; * Имя хоста; * Адрес электронной почты получателя.

Доступ к VIP-обнаружениям

217

The screenshot displays two side-by-side views of the Kaspersky Anti Targeted Attack Platform's 'Alerts' section. Both views show a total of 5 alerts, with 1 being VIP. The left view, under 'VIP', highlights the first alert as VIP (blue star icon). The right view, under 'Hosts', does not highlight any specific alert as VIP. This visual comparison illustrates that only senior security staff can identify and manage VIP alerts.

Старший служащий безопасности обрабатывает **VIP-обнаружения** как обычные

Обычный служащий безопасности **не видит** содержимого VIP-обнаружения и **не может** их обрабатывать

VIP-обнаружение выделяется значком . Их может просматривать только старший сотрудник службы безопасности. Младшие сотрудники будут видеть такие обнаружения в списке, но не смогут просмотреть их содержимое.

Старший сотрудник службы безопасности, помимо того, что видит все детали VIP-обнаружений, может вручную назначать и снимать VIP-статус. Отметить VIP-обнаружение как обработанное может только старший офицер безопасности.

8.2. Проверка архивов с паролем

Пароли к архивам

218

The screenshot shows the 'Passwords for archives' configuration page. On the left, a sidebar lists various settings like 'General settings', 'Certificates', and 'Network settings'. The 'Passwords for archives' option is selected. On the right, a main panel titled 'Passwords for archives' contains a text input field with the value 'KaSoeSKy'. Below the input field, there is a note: 'Start each entry on a new line' and 'You can add 49 more entries'. At the bottom right of the panel are 'Apply' and 'Cancel' buttons.

Основной сценарий использования: **проверка файлов** распространяемых (по **ftp**, **http** или **электронной почте**) в системах документооборота, которые используют архивы с паролем как метод шифрования

Можно задать до **50 паролей**, которые будут применяться для распаковки **защищенных архивов**

Kaspersky Anti Targeted Attack и Kaspersky Endpoint Detection and Response может проверять архивы и документы, защищенные паролем. Проверку защищенных архивов выполняет антивирусный модуль Центрального узла. Проверку защищенных документов выполняет Sandbox: вместе с документом передается список возможных паролей и Sandbox указывает пароль при открытии документа в соответствующем редакторе.

Если защищенный объект находится в письме, анализирующий модуль пытается подобрать пароль на основе текста сообщения.

В дополнение к этому старший сотрудник службы безопасности может настроить список паролей, которые будут применяться ко всем защищенным объектам, не только в почте. Подбор паролей по списку требует значительных вычислительных затрат, поэтому в список можно добавить не больше 50 паролей.

50 паролей слишком мало, чтобы охватить сколько-нибудь заметную долю типичных паролей, встречающихся на просторах Интернет. Поэтому цель такого списка не столько в том, чтобы обнаружить угрозы в файлах, загруженных из Интернет.

Основной сценарий использования такого списка — проверка документов в системах документооборота внутренней разработки. В организациях, особенно в финансовых учреждениях, вроде банков, нередко используются системы внутренней разработки как для обмена документами, так и для защиты этих документов. Также нередко такие системы построены на архаичных методах. Для обмена может использоваться модифицированная почтовая система, а для защиты — архивирование с паролем. Пароли в такой системе меняются регулярно и централизовано. Добавляя пароли в настройки Центрального узла, сотрудник службы безопасности сможет обнаруживать распространение вредоносных документов внутри организации.

8.3. External API

Сценарий использования

Поддерживается несколько типов операций:

- Проверка объектов внешних систем
- Получение внешними системами информации об обнаружениях программы
- Получение информации о событиях
- Управление действиями по реагированию на угрозы

Чтобы отправлять файлы через REST API, нужно зарегистрировать компьютер, который будет это делать, как внешний сенсор на центральном узле:

- Идентификатор стороннего сенсора в формате UUID. Подойдет любой UUID, например, с сайта <https://uuidgenerator.net>
- Пара ключей шифрования (публичный и секретный ключ) для аутентификации и защиты передаваемых файлов.
- Поддерживается RSA с длиной ключа 2048 бит

Взаимодействие внешних систем с Kaspersky Anti Targeted Attack Platform осуществляется с помощью интерфейса API. Вызовы методов API доступны только для авторизованных внешних систем.

В KATA/KEDR REST API поддерживает несколько типов операций:

- Проверка объектов внешних систем.
- Получение внешними системами информации об обнаружениях программы.
- Получение информации о событиях
- Управление действиями по реагированию на угрозы.

Для авторизации администратору приложения необходимо создать запрос на интеграцию внешней системы с приложением. После этого администратор должен обработать запрос в веб-интерфейсе Kaspersky Anti Targeted Attack Platform. Для этого потребуется:

- Идентификатор стороннего Сенсора в формате UUID. Подойдет любой UUID, например, с сайта <https://uuidgenerator.net>
- Пара ключей шифрования (публичный и секретный ключ) для аутентификации и защиты передаваемых файлов. Подойдет пара ключей RSA с длиной ключа 2048 бит, которую можно создать, например, командами:

```
openssl genrsa -out server.key 2048
openssl rsa -in server.key -out server.key
openssl req -sha256 -new -key server.key -out server.csr -subj
'/CN=localhost'
openssl x509 -req -sha256 -days 365 -in server.csr -signkey
```

```
server.key -out server.crt
cat server.crt server.key > cert.pem
```

Авторизация API-клиента

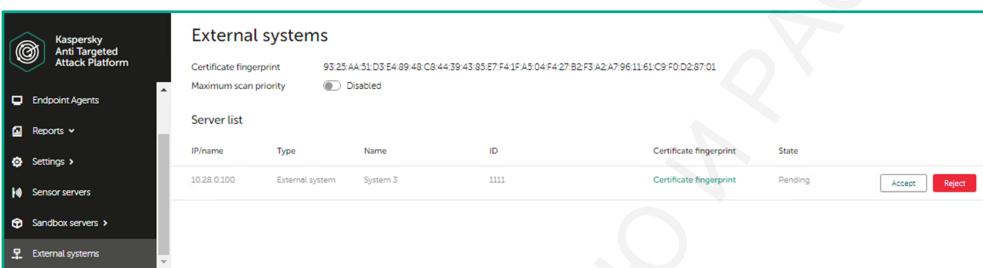
Запрос на подключение по API

220

В API **нет специальной команды** для запроса подключения. Вместо этого запросом становится **любая из команд** API, отправленная с ранее незарегистрированного адреса.

Ожидаемый ответ для первой отправленной команды: **401 Unauthorized**. При этом в консоли администратора центрального узла в разделе External systems **появится запрос** подключения.

Проверьте что **IP-адрес, UUID и отпечаток сертификата** в запросе совпадают с тем, которые использовались в команде REST API. Если все совпадает, примите запрос.



Имея идентификатор и пару ключей шифрования, можно отправлять запрос подключения на Центральный узел. В API Kaspersky Anti Targeted Attack нет специальной команды для запроса подключения. Вместо этого запросом становится любая из команд API, отправленная с ранее незарегистрированного адреса.

Самая простая команда, которую можно отправить, это запрос результатов проверки. Он выполняется методом HTTP GET, отправленным на определенным образом составленный URL с адресом Центрального узла:

```
https://<адрес центрального
узла>:443/kata/scanner/v1/sensors/<UUID>/scans/state
```

- где UUID это идентификатор, который вы сгенерировали для своего внешнего Сенсора.

Вручную такой запрос можно отправить утилитой curl:

```
curl -X GET
https://<IP>:443/kata/scanner/v1/sensors/<UUID>/scans/state -k
--cert cert.pem --key server.key
```

- где cert.pem и server.key — это подготовленный сертификат и секретный ключ для внешнего Сенсора.

Ожидаемый ответ для первой отправленной команды: 401 Unauthorized. При этом в консоли администратора Центрального узла в разделе External systems появится запрос подключения. Проверьте что IP-адрес, UUID и отпечаток сертификата в запросе совпадают с тем, которые использовались в команде REST API. Если все совпадает, примите запрос.

По умолчанию внешние системы получают имена System <ID>. Администратор может изменять имена внешних систем.

Примеры использования API

Пример использования API

221

Проверка файла:

```
curl --cert /root/cert.pem --key /root/server.key -X POST "https://<KATA_IP>:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans?sensorInstanceId=instance1" -F "content=@/tmp/test" -F scanId=1 -F objectType=file"
```

Получение результатов проверки:

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://<KATA_IP>:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans/state?sensorInstanceId=instance1&state=detect,not detected,processing,error,timeout"
```

Вывод информации об обнаружениях:

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://<KATA_IP>:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/detects?detect_type=am,sb&limit=100&token=7b226f6666736574223a20307d"
```

Получение списка хостов Kaspersky Endpoint Agent:

```
curl -k --noproxy '*' --cert ./cert.pem --key ./server.key -X GET "https://<KATA_IP>:443/kata/response_api/v1/ <UUID>/sensors?ip=<ENDPOINT_IP>"
```

Ниже рассмотрим несколько примеров использования API.

Пример использования API

222

```

https://10.28.0.51:443/kata/scanner/v1/sensors/1111/scans/state
GET https://10.28.0.51:443/kata/scanner/v1/sensors/1111/detects?detect_type=ids&limit=5
This request does not have a body
200 OK 44 ms 2.26 KB
1 {
  "detects": [
    {
      "alertId": "128",
      "detect": {
        "detectDateTime": "2023-02-11T06:29:15.0831922",
        "ids": [
          {
            "dataBaseVersion": "20230208112004"
          }
        ],
        "importance": "Low",
        "technology": "ids",
        "threaths": [
          {
            "customIDSrule"
          }
        ],
        "networkEventDateTime": "2023-02-11T06:29:15.0831922",
        "objectSource": {
          "sourceType": "web",
          "web": {
            "destinationIp": "10.28.0.52"
          }
        }
      }
    }
  ]
}
  
```

```

https://10.28.0.51:443/kata/response_api/v1/1111/sensors
GET https://10.28.0.51:443/kata/response_api/v1/1111/sensors
This request does not have a body
200 OK 1065 ms 1.19 KB
1 {
  "server": {
    "version": "4.1"
  },
  "sensors": [
    {
      "sensorId": "11ff0642-84e2-5517-7824-af42a63e67b7",
      "hostIp": "10.28.0.100",
      "hostDn": "admin-laptop.abc.lab",
      "lastAccessTimestamp": "2023-02-11T12:15:31.6685892",
      "version": "3.14.0.273",
      "selfDefenseState": true,
      "licenseStatus": "valid",
      "osFamily": "windows",
      "osName": "Microsoft Windows 10 Pro",
      "capabilities": [
        "prevention",
        "network_isolation",
        "run_process"
      ]
    }
  ]
}
  
```

Также не забываем, что запросы можно отправлять не только стандартной утилитой Curl, но и любыми другими средствами, к примеру используя Postman, что может быть удобнее на этапе тестирования запросов.

Проверка файлов и обработка результатов.

Чтобы отправить на Центральный узел задачу проверки файла, используется метод HTTP POST на адрес <https://<адрес центрального узла>:443/kata/scanner/v1/sensors/<UUID>/scans> с дополнительными параметрами:

- scanId — идентификатор задачи, который может быть произвольным числом или строкой. Главное, чтобы он отличался от идентификаторов уже отправленных задач.
- objectType — file.
- content — содержимое файла (при использовании curl передается в формате @<путь к файлу>).

Вручную такой запрос можно отправить утилитой curl:

```

curl --cert "путь к файлу TLS-сертификата" --key "путь к файлу закрытого ключа" -X POST "URL-адрес сервера с компонентом Central Node:порт, по умолчанию 443"/kata/scanner/v1/sensors/"идентификатор sensorId"/scans?sensorInstanceId="идентификатор sensorInstanceId" -F content="путь к файлу, который вы хотите проверить" -F scanId="идентификатор запроса на проверку" -F "objectType=file"
  
```

- Ожидаемый ответ на правильно сформированную команду: OK.

Отправленные файлы проверяются всеми доступными технологиями Центрального узла. Если в файле обнаружена угроза, Центральный узел сформирует обнаружение с источником EXTERNAL <имя внешней системы>.

В сценарии, когда организация использует API, чтобы отправлять документы из своей внутренней системы документооборота, интересно не только обнаружить опасные файлы, но и автоматически удалить их из системы.

Получить результаты проверки внешняя система может уже рассмотренным методом HTTP GET на адрес:

```
https://<адрес центрального  
узла>:443/kata/scanner/v1/sensors/<UUID>/scans/state
```

или в примере с утилитой curl:

```
curl --cert "путь к файлу TLS-сертификата" --key "путь к файлу  
закрытого ключа" -X GET "URL-адрес сервера с компонентом Central  
Node":<порт, по умолчанию  
443>/kata/scanner/v1/sensors/идентификатор  
sensorId/scans/state?sensorInstanceId=<идентификатор>  
sensorInstanceId&state=<один или несколько статусов проверки,  
которые вы хотите отобразить в результатах проверки>"
```

- Ответом на такой запрос будет список (в формате json) пар scanId, state.

Обрабатывать результаты должна сама сторонняя система. Предполагается также, что сторонняя система будет удалять задачи, результаты которых были обработаны, командой DELETE на адрес:

```
https://<адрес Центрального  
узла>:443/kata/scanner/v1/sensors/<UUID>/scans/<scanId>
```

И пример с утилитой Curl:

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу  
закрытого ключа> -X DELETE "<URL-адрес сервера с компонентом  
Central Node>:<порт, по умолчанию  
443>/kata/scanner/v1/sensors/<идентификатор  
sensorId>/scans/<идентификатор scanId>"
```

Ожидаемый ответ: OK

Пример использования API

223

GET "<URL Центрального узла>:<порт>/<external_system_id>/events"

Параметры:

- external_system_id
- filter
- max_timeout
- max_events
- continuation_token

Получение деталей обнаружений.

Запрос результатов проверки по идентификатору задачи дает только бинарный результат. Этого достаточно для обработки файла на стороне системы, отправившей его на проверку.

Если для каких-то целей нужно получить расширенную информацию об обнаружениях, она также доступна по REST-команде detects (на примере использования утилиты curl):

```
curl --cert <путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X GET "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию 443>/kata/scanner/v1/sensors/<идентификатор sensorId>/detects?detect_type=<одна или несколько технологий, с помощью которых выполнено обнаружение>&limit=<количество обнаружений в ответе на запрос>&token=<идентификатор запроса>"
```

В ответ на такой запрос Центральный узел возвращает все обнаружения, включая обработанные, от самых старых к новым, но не больше 1000. Ответ содержит все атрибуты обнаружений в формате json, в том числе, например, информацию о результатах проверки файла на виртуальных машинах для обнаружения Sandbox (но не архив с отладочными данными).

1000 обнаружений, причем в первую очередь самых старых и уже обработанных, это не обязательно то, что нужно стороне, отправившей запрос. Поэтому команда detects поддерживает дополнительные параметры для фильтрации обнаружений:

- detect_type позволяет фильтровать по технологии обнаружения и принимает значения am, sb, ids, url_reputation, yara; можно указать несколько технологий через запятую.

- limit позволяет запросить ограниченное количество обнаружений и принимает значения от 0 до 10000 (по умолчанию 1000, если лимит не указан явно).

Для запроса новых обнаружений служит параметр token той же команды detects. Принцип его использования немного сложнее, чем простые фильтры, рассмотренные выше.

Любой ответ на команду detects содержит параметр token с некоторым значением. Если повторить запрос и указать в качестве параметра token со значением из предыдущего ответа, то новый ответ будет содержать только новые обнаружения, которых не было в ответе со значением токена, указанном в запросе.

Если в новом ответе есть обнаружения, то значение параметра token в нем будет другое, и его можно будет использовать в следующем запросе, чтобы получить еще более новые обнаружения.

Получение списка хостов Kaspersky Endpoint Agent.

Для последующего реагирования на угрозы может потребоваться получение списка хостов Kaspersky Endpoint Agent. Для создания запроса на вывод информации о хостах с Kaspersky Endpoint Agent используется HTTP-метод GET:

```
curl -X GET https://<Центральный  
узел>/kata/response_api/v1/<UUID>/sensors
```

При успешной обработке запроса отобразится список хостов с Kaspersky Endpoint Agent.

Вы можете создать запрос на вывод информации о хостах с указанными параметрами: IP-адресом, именем или идентификатором хоста. Вы можете указать один, несколько или все параметры:

- sensor_id — уникальный идентификатор хоста Kaspersky Endpoint Agent.
- ip — IP-адрес хоста Kaspersky Endpoint Agent.
- host — имя хоста Kaspersky Endpoint Agent.

или в примере с утилитой curl:

```
curl -k --noproxy '*' --cert ./cert.pem --key ./server.key -X GET  
"https://<KATA_IP>:443/kata/response_api/v1/<UUID>/sensors?ip=<END  
POINT_IP>"
```

Запрос на включение сетевой изоляции.

После того, как мы получили список хостов с КЕА, нам может потребоваться выполнить какое-либо действие на целевом хосте для реагирования на угрозу. К примеру, рассмотрим отправку запроса на включение сетевой изоляции.

Для создания запроса используется HTTP-метод POST и команды передаются в теле запроса в формате JSON.

Синтаксис команды в примере с утилитой curl:

```
CURL -k --<путь к файлу TLS-сертификата> --key <путь к файлу закрытого ключа> -X POST "<URL-адрес сервера с компонентом Central Node>:<порт, по умолчанию 443>/kata/response_api/v1/<идентификатор external_system_id>/settings?sensor_id=<идентификатор sensor_id>&settings_type=network_isolation" -H 'Content-Type: application/json' -d '
{
"settings": {
"autoTurnoffTimeoutInSec": <время действия сетевой изоляции>
}
'
'
```

Ожидаемый код ответа об успешном выполнении: 200 Операция выполнена успешно.

8.4. Отчеты

The screenshot shows the Kaspersky Anti Targeted Attack Platform web interface. On the left, there's a sidebar with navigation links: Reports (Reports, Generated Reports, Templates), Settings (Threat Hunting, Prevention, Custom rules, Storage, Endpoint Agents), and SSO (Primary Central Node). The main area has two windows. One window titled 'Templates' shows a list of existing templates and an 'Add' button. The other window, titled 'Reports > New report template', shows fields for 'Template name' (set to 'weeks'), 'Report title', 'Report description', and a rich-text editor. Below these is a donut chart titled 'alerts_state' with the following data:

Slice name	Percentage
Slice name: 95 (95%)	95%
Slice name: 24 (20%)	20%
Slice name: 10 (11%)	11%
Slice name: 5 (5%)	5%
Slice name: 1 (1%)	1%
Slice name: 0 (< 1%)	< 1%

Веб-консоль Центрального узла позволяет настраивать и создавать пользовательские отчеты. Общий принцип такой: сначала нужно настроить шаблон отчета, затем из шаблона можно создать отчет.

Шаблоны создаются в разделе Reports на закладке Templates. После установки никаких шаблонов нет. Все шаблоны предстоит создать сотруднику службы безопасности.

При создании шаблона открывается редактор, который позволяет добавить в шаблон произвольный статический текст, статические изображения, а также динамические таблицы и диаграммы, которые будут строиться из данных в таблице обнаружений.

В настройках таблицы можно выбрать, какие атрибуты обнаружений в ней будут отображаться, а также настроить фильтр для обнаружений по таким параметрам, как состояние обнаружения, его уровень важности, VIP-статус и технология, обнаружившая угрозу.

В настройках диаграммы можно выбрать только ее тип. Все диаграммы показывают распределение обнаружений по какому-то параметру: уровню важности, источнику, технологии. Содержимое диаграммы не зависит от содержимого таблицы. Диаграмма показывает распределение всех обнаружений за некий период. Период не является настройкой шаблона и выбирается при формировании отчета.

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. On the left, there's a sidebar with 'Reports' selected. The main area is titled 'Reports' and shows a circular chart labeled 'alerts_state' with segments for 'Processed: 3', 'New: 8 (17%)', and 'In process: 1'. Below the chart is a table with columns: Time created, Assigned to, State, and Technologies. The table data is as follows:

Time created	Assigned to	State	Technologies
07.02.2023 13:35:53	sso	Processed	TAA
07.02.2023 14:33:48	sso	Processed	SB
07.02.2023 16:08:09	sso	Processed	iOS
06.02.2023 11:34:02	sso	Processed	AM

To the right, a modal window titled 'New report' is open, showing options for 'Template' (set to 'weeks'), 'Period' (set to 'Last 7 days'), and 'Servers' (set to 'ABC corp' and 'kata-on-abc.lab'). There are 'Create' and 'Cancel' buttons at the bottom.

Имея шаблон, можно создавать по нему отчеты за разные периоды времени. При этом следует понимать, что предупреждения в базе хранятся не вечно, и по мере накопления новых предупреждений, старые предупреждения удаляются из базы. Если поток новых предупреждений очень большой, эффективное время хранения предупреждений может быть около одного месяца или даже меньше.

Созданные отчеты можно сохранить в формате HTML.

8.5. Почтовые уведомления

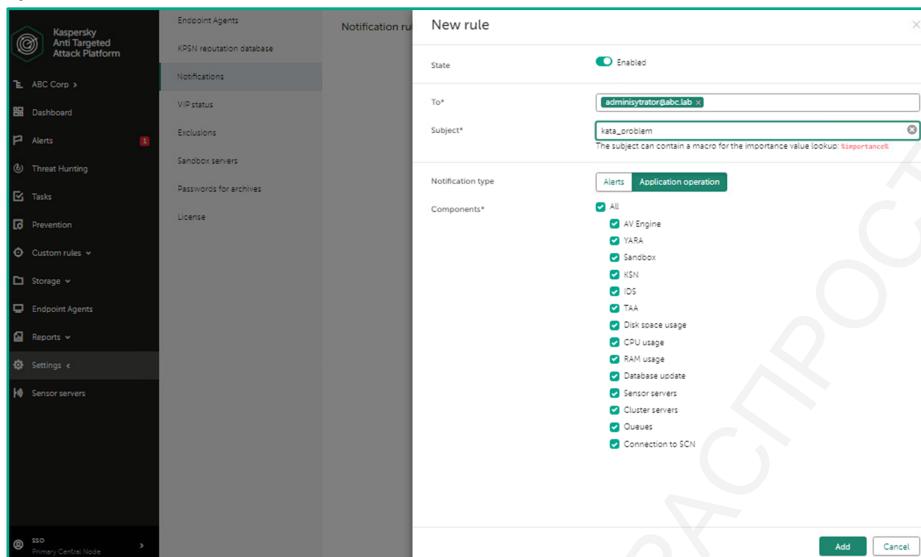
The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. On the left is a navigation sidebar with various sections like Dashboard, Alerts, Threat Hunting, Tasks, Prevention, Custom rules, Storage, Endpoint Agents, Reports, Settings, and Sensor servers. The 'Notifications' section is selected. On the right, a modal window titled 'New rule' is open, showing fields for 'To*', 'Subject*', 'Notification type' (set to 'Alert'), 'Alert importance' (set to 'High'), 'Source or destination' (IP subnet), 'Email' (Recipient/Sender email), and 'Components' (checkboxes for All, YARA, Sandbox, URL Reputation, Intrusion Detection System, Anti-Malware Engine, Targeted Attack Analyzer, and IOC). The status is set to 'Enabled'. There are 'Add' and 'Cancel' buttons at the bottom right of the modal.

Чтобы настроить уведомления об обнаружениях, перейдите в раздел **Settings | Notifications** в веб-интерфейсе старшего сотрудника службы безопасности и добавьте правило. В правиле укажите:

- Адреса электронной почты получателей (уведомления об обнаруженных угрозах могут содержать персональные данные, поэтому рекомендуется настраивать отправку уведомлений на адреса уполномоченных сотрудников);
- Тему сообщения (можно добавить макрос %importance% для подстановки важности обнаружения);
- Минимальную важность обнаружения (низкую, среднюю или высокую);
- IP-адрес или подсеть источника или назначения (опционально);
- Отправителя или получателя сообщения (опционально);
- Технологии обнаружения (все или некоторые из списка: Anti-Malware Engine, Sandbox, Yara, URL Reputation, Intrusion Detection System, Targeted Attack Analyzer, IOC).

Почтовые уведомления о сбоях

227

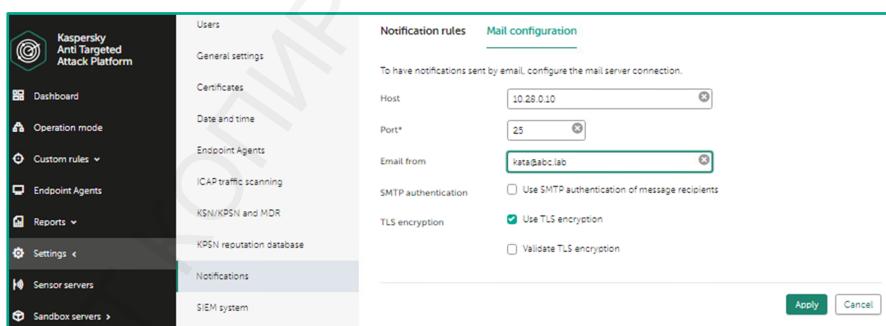


Чтобы настроить уведомления о сбоях в работе компонентов, перейдите в раздел **Settings | Notifications** в веб-интерфейсе администратора Центрального узла и создайте новое правило отправки уведомлений.

В настройках уведомления о работе компонентов администратор указывает адресатов, тему и компоненты, о работе которых нужно уведомлять.

Параметры отправки почтовых уведомлений

228



Центральный узел может отправлять уведомления об обнаруженных угрозах и о сбоях в работе серверных компонентов на адреса электронной почты. По умолчанию уведомления выключены. Адресатов уведомлений об обнаружениях настраивает старший сотрудник службы

безопасности. Адресатов уведомлений об ошибках и параметры доступа к почтовому серверу для отправки всех уведомлений настраивает администратор.

Чтобы указать, как отправлять, откройте веб-консоль администратора Центрального узла и перейдите в раздел **Settings | Notification | Mail configuration**. Укажите:

- Адрес почтового сервера (IP или имя);
- Порт SMTP;
- Почтовый адрес отправителя;
- Пользователя и пароль для аутентификации;
- Использовать ли TLS для защиты соединения.

Флаг **Validate TLS encryption** позволяет выполнить соединение с почтовым сервером с указанными параметрами и загрузить его сертификат. Впоследствии при отправке уведомлений Центральный узел будет проверять соответствие сертификата почтового сервера, загруженному при настройке.

8.6. Интеграция с SIEM

Центральный узел Kaspersky Anti Targeted Attack/Kaspersky Endpoint Detection and Response позволяет отправлять информацию об обнаруженных угрозах и событиях о состоянии (Heartbeat) во внешнюю систему мониторинга и выявления событий информационной безопасности (Security Information and Event Management, SIEM) по протоколу Syslog.

Передача данных в SIEM 229

SIEM system Integration	
Data to send	<input checked="" type="checkbox"/> Activity log <input checked="" type="checkbox"/> Alerts
Host/IP*	10.26.0.222
Port*	601
Protocol	TCP
Host ID	kata The server with this ID will be shown as the source of the alert in the SIEM system log
Heartbeat	10 minutes
TLS encryption	<input type="button"/> Disabled
<input type="button"/> Apply <input type="button"/> Cancel	

Чтобы включить передачу событий в SIEM:

- Войдите в веб-консоль Центрального узла от имени администратора.
- Откройте раздел **Settings | SIEM Settings**.
- Выберите, какие данные необходимо пересылать в SIEM (Activity log и/или Alerts).
- Укажите адрес, протокол и порт для подключения к серверу SIEM в полях Host/IP, Protocol и Port
- Задайте произвольный идентификатор в поле Host ID, чтобы проще находить события KATA/KEDR в консоли SIEM.
- Укажите периодичность отсылки Heartbeat сообщений в SIEM, по умолчанию — 10 минут.
- (Опционально) Загрузите TLS-сертификат, если SIEM требует строгую аутентификацию источников событий.

После этого Центральный узел будет отправлять на SIEM-сервер все новые обнаружения в формате Common Event Format.

Кроме обнаружений, Центральный узел отправляет в SIEM информацию о состоянии серверных компонентов. Информация о состоянии Endpoint-агентов не отправляется. По умолчанию информация о состоянии отправляется с интервалом 10 минут. Это значение можно изменить в поле Heartbeat.

События в SIEM

Информация о каждом обнаружении передается как отдельное syslog-сообщение формата CEF. Если обнаружение выполнено модулем Targeted Attack Analyzer, то информация о нем передается как несколько отдельных syslog-сообщений формата CEF.

Максимальный размер syslog-сообщения об обнаружении по умолчанию составляет 32 Кб. Сообщения, превышающие максимальный размер, обрываются в конце.

В заголовке каждого syslog-сообщения об обнаружении содержится следующая информация:

- Версия формата. Номер текущей версии: 0. Текущее значение поля: CEF:0.
- Производитель. Текущее значение поля: AO Kaspersky Lab.
- Название программы. Текущее значение поля: Kaspersky Anti Targeted Attack Platform.
- Версия программы. Текущее значение поля: 5.0.0-5201.
- Тип обнаружения. Подробности в онлайн документации.

- Наименование события. Подробности в онлайн документации.
- Важность обнаружения. Допустимые значения поля: Low, Medium, High или 0 (для сообщений типа heartbeat).
- Дополнительная информация.

8.7. Мониторинг сервера по SNMP

The screenshot shows the 'General settings' section of the Kaspersky Anti Targeted Attack Platform. On the left, there's a sidebar with various navigation options like Dashboard, Operation mode, Reports, Settings, and External systems. The main area has tabs for Users, General settings (which is selected), Certificates, and Monitoring. Under Monitoring, it says 'If one of the values is over the limit for the Central Node or Sensor servers, a notification is displayed on the Dashboard. You can set different values.' There are two sections: 'Warning of CPU usage above [90] % for [5] minutes' and 'Warning of RAM usage above [95] % for [5] minutes'. Below this is the 'SNMP' section. It has a note: 'Specified values are used in the external system to gain access to Kaspersky Anti-Targeted Attack Platform data.' A checkbox 'Use SNMP' is checked and labeled 'Enabled'. The 'Protocol version' dropdown is set to 'v2c'. In the 'Community string*' field, there is a red asterisk and a tooltip: 'Does not match the user name' and 'Is at least 8 characters long'. Below the field, there are several validation rules: 'Contains at least three of the following four types of characters: Upper-case character (A-Z), Lower-case character (a-z), Numerical character, Special character' and 'No character is repeated 3 or more times in a row'. At the bottom of the 'SNMP' section are 'Apply' and 'Cancel' buttons. To the right, there's a separate window titled 'SNMP' with fields for 'Protocol version' (set to 'v3'), 'Authentication protocol' (set to 'SHA256'), 'Username*' (set to 'kata'), 'Password*' (set to '*****'), and 'Privacy protocol' (set to 'AES'). It also lists validation rules for the password. Both windows have 'Apply' and 'Cancel' buttons at the bottom.

Есть возможность отправлять данные о загрузке центрального процессора и оперативной памяти Центральных узлов и Сенсоров во внешние системы, поддерживающие протокол SNMP. Чтобы настроить SNMP в интерфейсе Центрального узла:

- Перейдите в раздел **Settings | General settings**.
- В области настроек SNMP включите параметр **Use SNMP – Enabled**. Выберите версию протокола **Protocol version** - v2c или v3. Укажите дополнительные параметры для интеграции.

Если вы выбрали версию протокола v2c, в поле **Community string** укажите пароль, который будет использоваться для подключения к Kaspersky Anti Targeted Attack Platform.

Если вы выбрали v3, выполните следующие действия:

- В поле **Authentication protocol** выберите один из следующих вариантов проверки достоверности и целостности данных, переданных во внешнюю систему:

- MD5.
- SHA256.
- В поле User name укажите имя пользователя.
- В поле Password укажите пароль для аутентификации.
- В поле Privacy protocol выберите один из следующих типов шифрования:
 - DES.
 - AES.
- В поле Password укажите пароль для шифрования.

Чтобы настроить SNMP в интерфейсе Сенсора, введите параметры, указанные выше в интерфейсе в разделе System administration | SNMPd monitoring setting.

8.8. Сбор информации о системе

Журналы

Для обнаружения неисправностей администратор Kaspersky Anti Targeted Attack/Kaspersky Endpoint Detection and Response может просмотреть системные журналы и/или запустить скрипт для сбора диагностических данных.

Чтобы просмотреть системные журналы, перейдите в режим технической поддержки и используйте инструменты операционной системы для анализа журналов. В операционной системе журналы модулей Kaspersky Anti Targeted Attack/Kaspersky Endpoint Detection and Response расположены в папке /var/log/kaspersky/. Журналы хранятся отдельно на каждом из серверов.

К примеру, журналы установки лежат по пути /var/log/kaspersky/installation:

- install.log,
- post-install/log,
- per-install.log.

Сбор информации для обращения в поддержку

Сбор данных для обращения в поддержку на центральном узле или сенсоре

231

```
root@l.srv.node1.dyn.kata:~# kata-collect
Running with inactivity timeout: 900 sec

Running collect task: Copy product configs from /etc/kaspersky (CopyConfigsTask)
Starting collect task: Copy product configs from /etc/kaspersky (CopyConfigsTask)
copy: /etc/kaspersky
Collect task "Copy product configs from /etc/kaspersky (CopyConfigsTask)" completed successfully, elapsed time: 0.04 sec
Running with inactivity timeout: 900 sec

Running collect task: Copy logs (product, system, atop, installation, docker) (CopyLogsTask)
Starting collect task: Copy logs (product, system, atop, installation, docker) (CopyLogsTask)
copy: /var/log/kaspersky
copy: /var/log/atop
copy: /var/log/dockerd.log
copy: /var/log/syslog.3.gz
copy: /var/log/syslog.2.gz
copy: /var/log/syslog

-----
collect task "Show confidentiality warning (ShowWarningTask)" completed successfully, elapsed time: 0.00 s
sc
Archiving collected data...
all done: /tmp/collect/collect-l.srv.node1.dyn.kata-2024-02-04T11-08-36
root@l.srv.node1.dyn.kata:~#
```

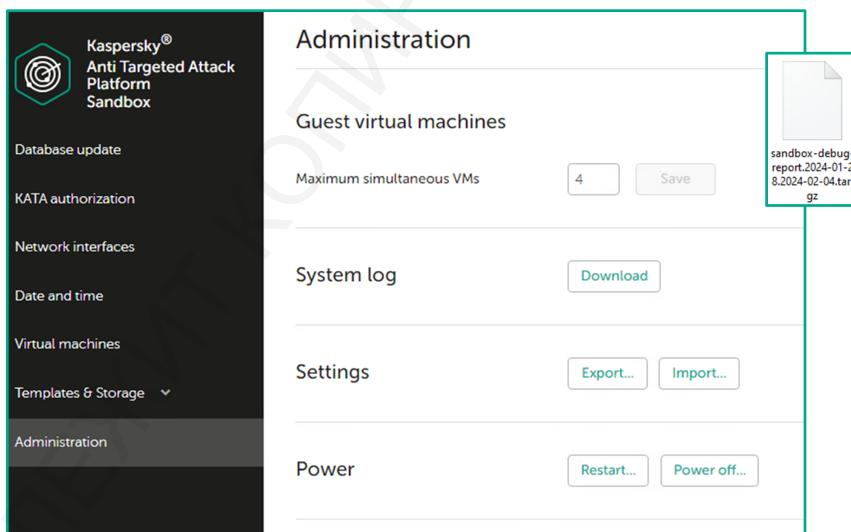
Name	Size	Packed Size
configs	82 804	84 480
diagnostic	580 467	596 992
dumps	163 427 944	163 429 888
environment	1 059 917	1 078 784
logs	2 013 312 162	2 013 356 544

Чтобы запустить скрипт для сбора диагностических данных, откройте текстовую консоль управления Центрального узла или Сенсора, перейдите в Technical Support Mode и запустите утилиту `kata-collect`.

Результат будет сохранен в папке `/tmp/collect` в файле с именем `collect.tar.gz`. Перед отправкой информации в службу технической поддержки удалите из архива данные, которые вы считаете конфиденциальными.

Сбор данных для обращения в поддержку на Sandbox

232



Журналы Sandbox можно сохранить через веб-интерфейс. В разделе Administration напротив секции System log нажмите кнопку Download и подождите. Веб-консоль запускает скрипт для

сбора журналов в архив и на выполнение операции может потребоваться несколько минут. Когда архив с журналами будет готов, браузер, в котором открыта веб-консоль, предложит сохранить файл.

Экспорт деталей обнаружения

Иногда детали обнаружения нужны для отправки запроса в техническую поддержку Лаборатории Касперского. Внизу карточки обнаружения есть ссылка, которая позволяет скопировать все детали сообщения в виде текста.

8.9. Обновление

Обновление Центрального узла

Обновление 233

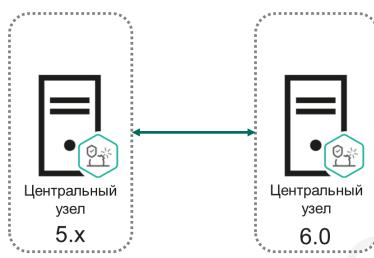
После обновления нужно заново **добавить** лицензионные **ключи**

Допускается кратковременный **перерыв в работе**, в том числе для отказоустойчивой версии

Если в роли компонента Sensor используется решение **KSMG**, параметры интеграции с ним **сохраняются**

Данные компонентов Sensor и Sandbox **не сохраняются**

Совместимость с компонентами более ранней версии **не поддерживается**



Вы можете обновить приложение Kaspersky Anti Targeted Attack Platform с версии 5.1 до версии 6.0.

Миграция с неотказоустойчивой версии приложения на отказоустойчивую с помощью обновления не предусмотрена: если вы используете неотказоустойчивую версию приложения, при обновлении вы можете установить только неотказоустойчивую версию, и наоборот.

Если вы используете режим распределенного решения и мультитенантности, вам нужно подготовить серверы PCN, SCN и отдельные серверы с компонентом Sensor к обновлению.

Обновление поставляется в виде пакета обновлений. Пакет входит в комплект поставки приложения.

Чтобы обновить компонент Central Node, установленный на сервере:

- Поместите пакет с обновлением приложения на сервер с компонентом Central Node в директорию /data
- Войдите в консоль управления сервера Central Node, на котором вы хотите обновить компонент, по протоколу SSH или через терминал
- Убедитесь, что размер свободного дискового пространства в файловой системе /dev/sda2 составляет более 100 ГБ
- Распакуйте архив с обновлением
- Установите пакет с обновлением
- Установите обновление
- Смонтируйте iso-образ с Kaspersky Anti Targeted Attack Platform версии 6.0 и перезагрузите сервер
- Загрузитесь с устройства, на котором находится смонтированный iso-образ
- В меню загрузчика GRUB выберите пункт Upgrade KATA 5.1
- Следуйте дальнейшим шагам мастера до завершения обновления на сервере
- Установите пакет обновлений приложения до версии 6.0.1.

Обновление Сенсора и Sandbox

Обновление

234

Обновление компонента Sandbox и компонента Sensor, установленного на отдельном сервере **не предусмотрено**

Вам требуется **установить** компонент версии **6.0**

Обновление компонента Sandbox и компонента Sensor, установленного на отдельном сервере

не предусмотрено.

Вам требуется установить компонент версии 6.0.

8.10. Обновление с предыдущих версий



Обновление компонента до версии 6.0 возможно только с версии 5.1. Если вы используете более раннюю версию, требуется последовательно обновить версии компонента до версии 6.0: 3.7 → 3.7.1, 3.7.1 → 3.7.2, 3.7.2 → 4.0, 4.0 → 4.1, 4.1 → 5.0, 5.0 → 5.1

Обновление Endpoint Agent описано в соответствующей документации и отличается в зависимости от типа установленного продукта*

8.11. Сохранение и восстановление настроек

У серверов Kaspersky Anti Targeted Attack/Kaspersky Endpoint Detection and Response есть возможность сохранить резервную копию настроек, чтобы была возможность легко их восстановить, если конфигурация будет испорчена. Настройки экспортируются отдельно на каждом из серверов из консоли управления.

Резервную копию параметров Central Node (PCN или SCN в режиме распределенного решения и мультитенантности), можно выполнить из меню администратора сервера или в режиме Technical Support Mode.

Резервная копия Kaspersky Anti Targeted Attack Platform будет содержать только базы

данных (базу обнаружений, сведения о статусе VIP, список данных, исключенных из проверки, уведомления) и параметры Central Node или PCN.

8.12. Изменение системных настроек

Замена сертификата

В ходе эксплуатации Центрального узла может возникнуть необходимость замены сертификата. Во-первых, самоподписанный сертификат, который создается при установке, имеет срок годности 5 лет. Рано или поздно его придется менять. Во-вторых, некоторые организации предпочитают использовать сертификат, выписанный их внутренней системой управления сертификатами. В-третьих, регулярная замена сертификатов может быть прописана в политике безопасности.

Заменить (или создать новый самоподписанный) сертификат можно в веб-консоли администратора Центрального узла в разделе *Settings | General settings*.

Чтобы использовать на центральном узле свой сертификат, нужно подготовить файл в формате PEM. Файл должен содержать и публичную и секретную часть сертификата, с длиной секретного ключа не меньше 2048 бит.

После замены сертификата Центрального узла потребуется заново подключить к нему все смежные сущности: серверы Sandbox, Сенсоры, серверы KWTS и KSMG, Endpoint-агенты — в зависимости от развернутого решения.

Изменение времени

Часто причиной труднодиагностируемых проблем взаимодействия между компонентами KATA или KEDR оказывается рассинхронизация времени. Поэтому так важно, чтобы время на серверах было синхронизировано. Проще всего этого добиться, если все серверы настроены получать время из одного и того же доверенного источника.

Если адрес NTP-сервера организации меняется, не забывайте обновлять настройки времени на серверах.

Параметры времени можно задать как через веб-консоль (для тех серверов, у которых она есть), так и через текстовую консоль.

Изменение настроек сети

В ходе эксплуатации решений может также возникать необходимость менять настройки сети для серверов. Это можно сделать в веб-консоли администратора или в текстовой консоли.

Как правило, изменение настроек сети не несет никаких негативных последствий. Но из соображений предосторожности рекомендуется не менять адрес сервера, пока к нему подключены узлы с активной политикой изоляции от сети.

8.13. Kaspersky Private Security Network (KPSN)

Зачем нужен KPSN

Продукты Kaspersky Anti Targeted Attack и Kaspersky Endpoint Detection and Response, как многие другие решения и продукты Лаборатории Касперского, тесно интегрированы с сетью информационной безопасности Kaspersky Security Network (KSN), которая представляет собой репутационные базы данных с файлами и URL-адресами, находящимися в облачной инфраструктуре Лаборатории Касперского. KSN обеспечивает более быструю реакцию на новые угрозы, повышает эффективность работы компонентов обнаружения и защиты, а также снижает вероятность ложных срабатываний.

KSN — важный компонент, решение об использовании которого лежит на стороне администратора системы. Если принято положительное решение, то при участии в KSN в Лабораторию Касперского автоматически передаются некоторые данные, полученные в результате работы продукта. Перечень передаваемых данных указан в Положении о KSN. В основном это контрольные суммы проверяемых файлов, ссылки, информация об обнаруженных вредоносных объектах и статистические данные о работе продукта.

Несмотря на эти факты, в некоторых отраслях и компаниях встречаются требования, в соответствии с которыми никакие данные не могут быть отправлены за пределы организации. Такое требование может стать серьезным ограничением для использования KSN. Чтобы обойти это ограничение, Лаборатория Касперского предлагает локальную реплику Kaspersky Security Network в виде продукта Kaspersky Private Security Network (KPSN). Этот подход позволяет получить все преимущества KSN, не отсылая никакие данные за пределы организации.

KPSN-серверы на стороне заказчика имеют постоянную связь с глобальными KSN-серверами. Как только в глобальном каталоге происходят изменения, KPSN-серверы уведомляются об этом и начинают скачивать данные. Таким образом, базы данных на стороне клиента всегда находятся в актуальном состоянии, а ответы от KPSN совпадают с ответами, которые бы пришли из KSN.

Kaspersky Private Security Network поддерживает несколько вариантов развертывания, в том числе для работы в физически изолированной сети. Данный курс не рассматривает установку KPSN. Здесь будут рассмотрены только аспекты работы KPSN, которые касаются интеграции с Kaspersky Anti Targeted Attack/Kaspersky Endpoint Detection and Response.

Файлы, необходимые для интеграции с KPSN

Чтобы подключить KATA/KEDR к KPSN, нужны определенные файлы с адресами служб KPSN. Эти файлы вы получаете в процессе развертывания KPSN.

В ходе развертывания нужно будет сохранить файл с настройками KPSN (configuration.json), отправить его в Лабораторию Касперского, и получить в ответ несколько файлов, которые нужны, чтобы подключить KPSN к KSN, и чтобы подключить KATA/KEDR и другие приложения Лаборатории Касперского к KPSN:

- cert.tar.gz — сертификат для аутентификации KPSN в KSN, который необходимо указать в настройках KPSN, чтобы начать загружать данные из KSN.
- kc_<имя компании>.xml, kh_<имя компании>.xml, ksncli_<имя компании>.dat — файлы с адресами служб KPSN, которые нужно добавить в настройки KATA/KEDR.
- <имя компании>_settings.pkcs7 — файл, который нужно загрузить в настройки Kaspersky Security Center, чтобы использовать KPSN в Kaspersky Endpoint Security и других приложениях для защиты сети.

Тройку файлов (kc_<имя компании>.xml, kh_<имя компании>.xml, ksncli_<имя компании>.dat) нужно преобразовать к правильному виду, прежде чем загружать в настройки KATA/KEDR:

- Сжать .xml файлы в .xms файлы утилитой squeeze.exe (можно получить в Лаборатории Касперского)
- Заменить <имя компании> в имени файлов на private, чтобы получились имена
 - kc_private.xms,
 - kh_private.xms,
 - ksncli_private.dat.

Подключение Центрального узла к KPSN

Модуль KSN входит в состав Центрального узла и Сенсора. Sandbox-сервер не взаимодействует с KSN напрямую, но Центральный узел дополнительно проверяет в KSN файлы, признанные опасными по результатам анализа на сервере Sandbox. Взаимодействие с KSN/KPSN настраивается через консоль управления отдельно для каждого из серверов.

Центральный узел подключается к KPSN в веб-консоли администратора. В разделе Settings | KSN/KPSN and MDR выберите тип подключения KPSN, загрузите файлы kc_private.xms, kh_private.xms и ksncli_private.dat и нажмите Apply.

Результат подключения отображается в сообщении внизу окна.

Сенсоры получают настройки KPSN от Центрального узла и отдельной настройки не требуют.

Интеграция с репутационной базой

KPSN не только снабжает продукты Лаборатории Касперского расширенными данными из публичной инфраструктуры KSN, но и создает для компании локальную репутационную базу, подконтрольную администраторам.

Ни одно защитное решение не является одновременно на 100% эффективным в обнаружении угроз и на 100% точным в определении неопасных объектов. Всегда есть небольшой риск и ложных срабатываний, и пропуска угрозы.

При использовании публичной версии KSN статистика обработки файлов попадает в Лабораторию Касперского, где обрабатываются алгоритмами и экспертами. В результате неизвестные ранее файлы быстро получают корректную классификацию: опасен или нет.

KPSN не передает никакие сведения в Лабораторию Касперского. Поэтому задача классификации неизвестных файлов ложится на специалистов заказчика. И именно для этого нужна локальная репутационная база KPSN. Специалисты заказчика могут внести в нее контрольную сумму любого файла и вручную указать, опасен он или нет.

Центральный узел KATA Platform может интегрироваться с репутационной базой KPSN и автоматически заносить в нее все файлы, которые были признаны опасными технологией Sandbox с высоким уровнем важности.

Чтобы настроить передачу в KPSN контрольных сумм файлов, обнаруженных технологией Sandbox, потребуется сертификат пользователя KPSN с правом использовать API KPSN.

Сертификат (обе части, публичную и секретную) пользователя KPSN с правами доступа к KPSN API загрузите из профиля этого пользователя в веб-консоли KPSN. У администратора KPSN есть нужные права, но подойдет пара ключей шифрования любого пользователя с доступом KPSN API.

Чтобы отправлять обнаружения Sandbox в KPSN:

- в консоли администратора Центрального узла в разделе **Settings | KPSN reputation database** укажите:
 - HOST — IP-адрес сервера KPSN, на котором хранится локальная репутационная база KPSN;

- TLS Certificate — файл сертификата для аутентификации пользователей в KPSN;
- TLS encryption key — файл, содержащий закрытый ключ шифрования;
- в консоли старшего сотрудника службы безопасности Центрального узла в разделе Settings | KPSN reputation database отметьте флаг Assign the ‘Untrusted’ status to alerts.

В результате этих настроек Центральный узел будет отправлять контрольные суммы объектов, которые были обнаружены технологией Sandbox, в раздел Reputation database в KPSN. Для каждого объекта отправляются две контрольные суммы: MD5 и SHA256.

Администратор KPSN может вручную создавать записи в KPSN reputation database. Записи от Kaspersky Anti Targeted Attack/Kaspersky Endpoint Detection and Response можно узнать по маркеру KATA в описании. Удалить записи KATA нельзя, но их можно отключить.

Другие приложения Лаборатории Касперского смогут блокировать объекты по контрольным суммам, которые есть в KPSN reputation database. В частности, Kaspersky Endpoint Security блокирует исполняемые файлы с плохой репутацией компонентами File Threat Protection и Host Intrusion Prevention.