Решения на базе Aether

Релиз XII

июль 2021

Что нового

Версии агентов и защиты

Adaptive Defense / Adaptive Defense 360: 4.00.00
Endpoint Protection / Endpoint Protection Plus: 9.00.00

- Защита Windows: 8.00.19.0000
  Агент Windows: 1.18.00.0000
- Защита MacOS: 2.00.08.0000 и 2.00.08.1000 для Catalina и Big Sur
  Агент MacOS: 1.10.08.0001
- Защита Linux: 3.01.00.0001
  Агент Linux: 1.10.10.0001
- Агент и защита для Android: 3.5.33

Новые функции

Threat Hunting Service, индикаторы атаки

- Новая панель мониторинга, обеспечивающая видимость **индикаторов атаки (IOA)**, обнаруженных с помощью сервиса поиска угроз Threat Hunting Service, бесплатно включенного в наши EDR-решения. Индикаторы атаки (IOA) - это обнаруженные на компьютерах аномальные поведения, которые, скорее всего, могут указывать на выполнение атаки против них. Непрерывный мониторинг действий, выполняемых на компьютерах, позволяет нам предоставлять этот сервис
- Виджеты с количеством событий, индикаторов и индикаторов атаки. События – это количество действий, отслеживаемых EDR- решением, индикаторы – это аномальное поведение, обнаруженное в сети, а индикаторы атаки – это индикаторы, которые с большой вероятностью могут быть признаками атаки.
- Индикаторы атаки (IOA), сопоставленные с матрицей **MITRE**. Каждый индикатор атаки сопоставляется с тактикой и техникой из матрицы MITRE. Это позволяет организациям легко идентифицировать стадию атаки и ее характеристики. Данная информация также предоставляет организациям индивидуальные рекомендации по реагированию и позволяет им принимать меры по сдерживанию и устранению с необходимой срочностью.

- Просмотр индикаторов атак по типам индикаторов позволяет легко определить наиболее распространенные типы атак, которым подвергается организация, и определить приоритеты превентивных мер для предотвращения будущих атак.
- Просмотр индикаторов атаки с помощью компьютера позволяет легко идентифицировать компьютеры, которые с высокой долей вероятности были взломаны (скомпрометированы).
- Возможность архивировать индикаторы атаки, которые уже были обработаны, чтобы легко идентифицировать индикаторы, ожидающие каких-либо действий управления. Они отображаются красным цветом в виджетах.
- Подробная информация о каждом индикаторе атаки: дата, риск, описание типа атаки, рекомендации по локализации и устранению, если атака подтверждена, и полное описание типа атаки на основе сопоставления тактики и техники, используемых злоумышленником, с базой данных MITRE.
- Прямой доступ к расширенной информации об индикаторе атаки со страницы описания обнаруженного индикатора. На этой странице в секции **MITRE** нажмите на ссылку у параметра «Тактика» или «Техника», чтобы открыть веб-сайт MITRE с подробной информацией, помогающей устранить атаку и сократить площадь атаки.
- **Расширенное расследование атаки**. Доступно со страницы описания обнаруженного индикатора атаки. Расширенное расследование автоматически сообщает о взломанных пользователях и компьютерах, помогает определить основную причину атаки, предоставляет такую информацию, как URL-адреса и IP-адреса, участвующие в атаке, и дает представление об общем воздействии атаки на всю организацию.
- **График атаки**. Доступно со страницы описания обнаруженного индикатора атаки. Представляет собой графическое отображение всех элементов, участвующих в атаке, помогая расследованию основной причины атаки, ее последствий и т.д.
- **График атаки**. Узлы на графике показывают классификацию файлов. Оранжевые узлы указывают на неизвестные файлы и потенциально нежелательные программы (ПНП / PUP), в то время как красные узлы указывают на вредоносное ПО. Кроме того, иконки узлов могут показывать иконки популярных приложений, что облегчает их идентификацию.
- **График атаки**. Вы можете взаимодействовать с элементами графика и даже выполнять действия в отношении нескольких узлов одновременно.
- **График атаки**. График позволяет просматривать сведения об активности конкретных процессов.

- **График атаки**. На графике показана последовательность событий, вызванных процессом, для идентификации всех событий, произошедших с течением времени. Каждому событию присваивается порядковый номер, основанный на дате, когда произошло событие.
- Обнаружение и сдерживание **атак типа brute force на протокол RDP**. Возможность вручную завершить режим сдерживания RPD-атак на требуемых компьютерах.
- Настройка индикаторов атаки и выбор действий, которые необходимо предпринять, настройка списка надежных IP-адресов и отключение любого индикатора атаки, который генерирует ложные срабатывания, на любом компьютере в организации.
- Добавлено новое разрешение для ролей пользователей, позволяющее настраивать роли для тех пользователей, которые могут изменять настройки индикаторов атаки.
- Добавлен новый тип оповещений в настройки «Мои оповещения» для отправки уведомлений по электронной почте при обнаружении индикаторов атаки.
- Добавлена информация об индикаторах атаки в отчеты для руководителей.

Расширенная защита

- **Возможность удаления заблокированных программ в процессе классификации**. Администраторы могут удалять заблокированные программы из списка заблокированных элементов. Эта опция полезна в том случае, когда есть заблокированные файлы, которые не могут быть отправлены в облако из-за их слишком большого размера или недоступности. Статус файла отображается в списке заблокированных программ. Все предпринятые действия регистрируются в журнале действий и в истории заблокированных элементов.
- Теперь по умолчанию антиэксплойтная защита включена и установлена в режим блокировки. Параметры защиты от эксплойтов, созданные до нового релиза XII, не изменяются, хотя рекомендуется включить защиту во всех профилях настроек.
- Расширенная защита для Linux теперь по умолчанию установлена в режим блокировки. Таким образом, теперь все вредоносные действия, обнаруженные поведенческим сканером, будут по умолчанию блокироваться, что позволяет обеспечивать максимальную защиту.
- Контекстные обнаружения расширенной защиты для Linux обновляются динамически, когда это необходимо.

- Мониторинг сетевых событий в Linux для получения дополнительной контекстной информации о запущенных приложениях. Смысл заключается в том, чтобы предоставить функциям EDR, включенным в защиту Linux, большую видимость и, следовательно, больше возможностей для обнаружения подозрительных процессов.
- Улучшен мониторинг процессов в Linux для обогащения телеметрии большим количеством данных о выполнении процессов. Это предоставляет модулю EDR, включенному в защиту для Linux, большую видимость и, следовательно, более широкие возможности обнаружения.

Задачи

- Возможность отменить и удалить несколько задач одновременно.
- **Более детальное и гибкое планирование задач**. Вы можете запланировать выполнение задач сканирования или патчинга в любой день недели, например, в последнюю пятницу месяца в выбранное Вами время, и т.д. Предлагается ряд других опций, которые делают процесс планирования задач более гибким. Особенно удобно для установки патчей с помощью модуля **Patch Management**.

Linux

- Поддержка последних версий поддерживаемых дистрибутивов Linux (Fedora, Red Hat, CentOS и т.д.). Смотрите дополнительную информацию обо всех поддерживаемых дистрибутивах Linux.
- **Поддержка SUSE** 11 SP2 и выше, SUSE 12 и SUSE 15.
- Новый параметр при установке агента Linux для настройки параметров прокси-сервера.
- Автоматическое обновление защиты Linux при необходимости после обновления установленного ядра или дистрибутива Linux.
- Повышение производительности защиты Linux, применимое к очень специфическим дистрибутивам, в которых управление несколькими потоками не было оптимальным.

Другое

- Новая **вкладка «Обнаружения» на странице со сведением о выбранном компьютере**. На этой вкладке отображаются все обнаружения,

незакрытые уязвимости, индикаторы атаки и т.д, относящиеся к данному компьютеру. Состав отображаемой информации зависит от приобретенного продукта и дополнительных модулей.

- Возможность выполнять поиск в дереве групп компьютеров.
- Возможность запланировать отправки списков, которые позволяют экспортировать подробную информацию (например, список инвентаризации ПО).
- Новая колонка в списке «Статус защиты». В этом столбце отображается состояние коммуникаций компьютера с серверами платформы Коллективного разума и серверами, используемыми для классификации URL-адресов. В настоящее время эта функция реализована для компьютеров с ОС Windows.
- Новая колонка в экспорте списка «Статус защиты». В этом столбце отображается режим расширенной защиты (Audit, Hardening или Lock).
- **Улучшена интеграция с интерфейсом проверки на наличие вредоносных программ Windows 10 (AntiMalware Scan Interface, AMSI)**. Использование AMSI предоставляет нашим решениям телеметрию и дополнительную информацию о выполнении сценариев и макросов, повышая защиту компьютера без отрицательного влияния на его производительность.
- Сканирование программ, запущенных при запуске Windows, что позволяет убедиться в том, что все программы, загруженные в память, являются надежными.
- Оптимизация кэша модуля управления веб-доступом для уменьшения количества запросов в облако при классификации URL-адресов.
- Фильтрация трафика IPv6 для всех протоколов, поддерживаемых файервольной технологией, встроенной во все наши продукты.
- **Возможность отображения оповещений в веб-консоли**. Эти оповещения носят информационный характер и используются для уведомления клиентов о наличии новых версий, позволяя им обновить свой аккаунт до последней версии. Каждый пользователь веб-консоли может отключить требуемые оповещения, при этом это не будет влиять на отображения оповещений для других пользователей аккаунта.
- При выборе пользовательского диапазона в списках «Веб-доступ» теперь невозможно выбрать данные более чем за один месяц.
- **Защита для серверов Exchange достигла этапа «конец жизни» (Endo of Life, EOL)**, и она больше недоступна для новых клиентов. Данный модуль остается доступным для текущих клиентов вплоть до июня 2024 года (окончание технического обслуживания, EOM).

Устраненные ошибки

- Исправлены некоторые ошибки, способные вызывать BSOD.
- Исправлена ошибка, когда при выборе фильтра “Все” в списке заблокированных элементов показывались только элементы за последний месяц. Сейчас отображаются все элементы.
- Исправлена ошибка, когда в результатах поиска при создании фильтра, в который включались поля по аппаратному и программному обеспечению, не удавалось выбрать несколько компьютеров.
- Если обновления защиты были отключены в настройках, то на странице со сведениями о компьютере вместо указания на отключение обновлений отображалась ошибка обновления.
- Исправлена ошибка, из-за которой если на первом уровне дерева групп было несколько групп, и одна из них была свернута, остальные группы появлялись без названия.
- В разделе Лицензии при наличии нескольких пакетов лицензий в том случае, если срок действия любого из них был близок к истечению, неправильно сообщалось о том, что заканчивались сроки действия всех пакетов лицензий.
- Исправлена ошибка, при которой переход по ссылке VirusTotal открывал не страницу конкретного вредоносного ПО, а страницу поиска.
- Исправлена ошибка, при которой после обновления защиты и перезагрузки компьютера пользователю неверно предлагалось перезагрузить компьютер еще раз для завершения обновления.
- Исправлена ошибка некорректного обнаружения Windows 10 version 21H1.

В данном документе не отражены изменения, связанные с модулем Data Control, в связи с тем, что данный модуль недоступен для продаж на территории стран бывшего СССР. Для получения информации об изменениях в данной модуле, смотрите полный список изменений в версии.