Aether Platform

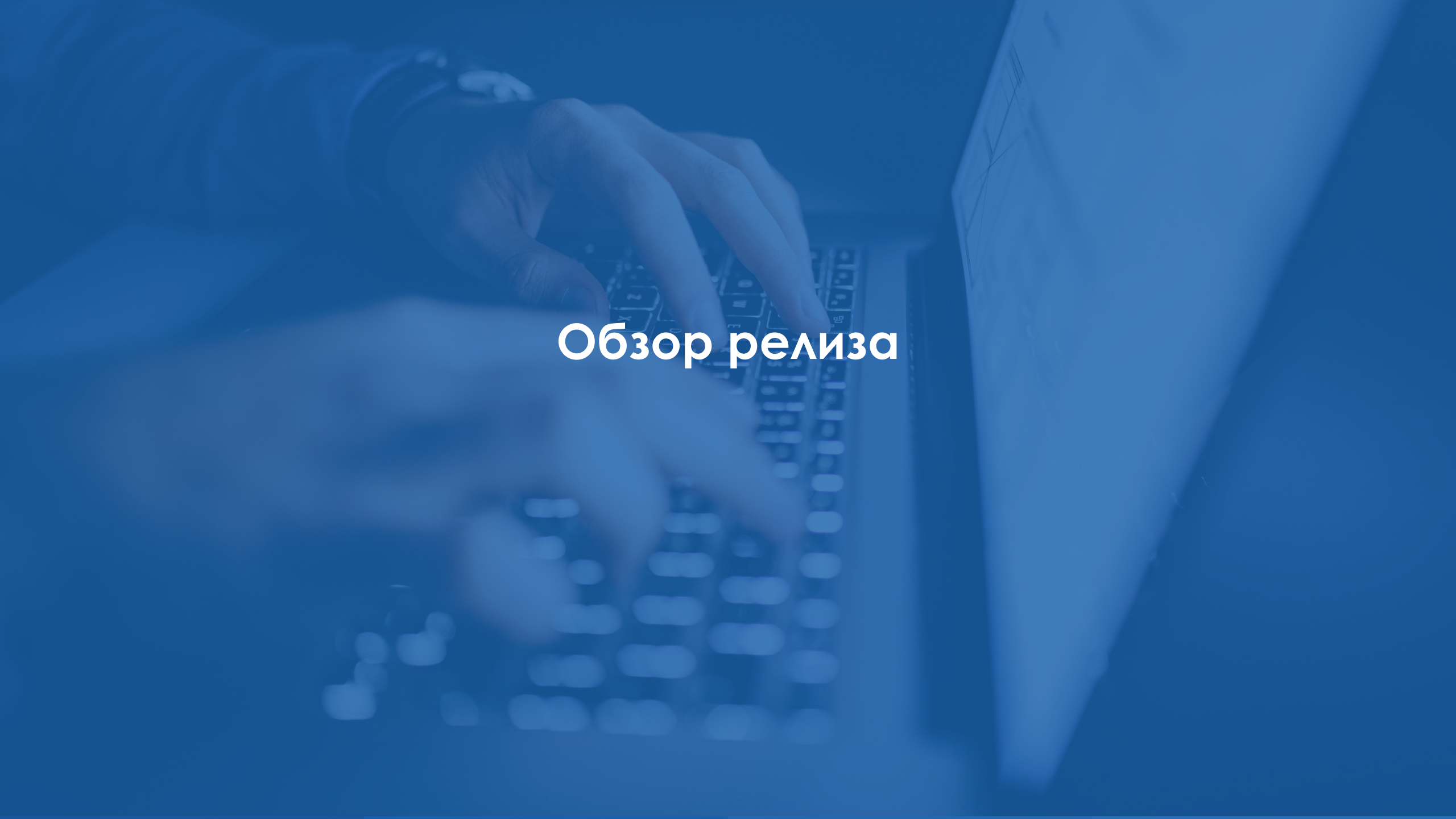
Aether Релиз XII
Что нового

21.07.2021

panda

www.pandasecurity.com
www.cloudav.ru

Содержание



Обзор релиза

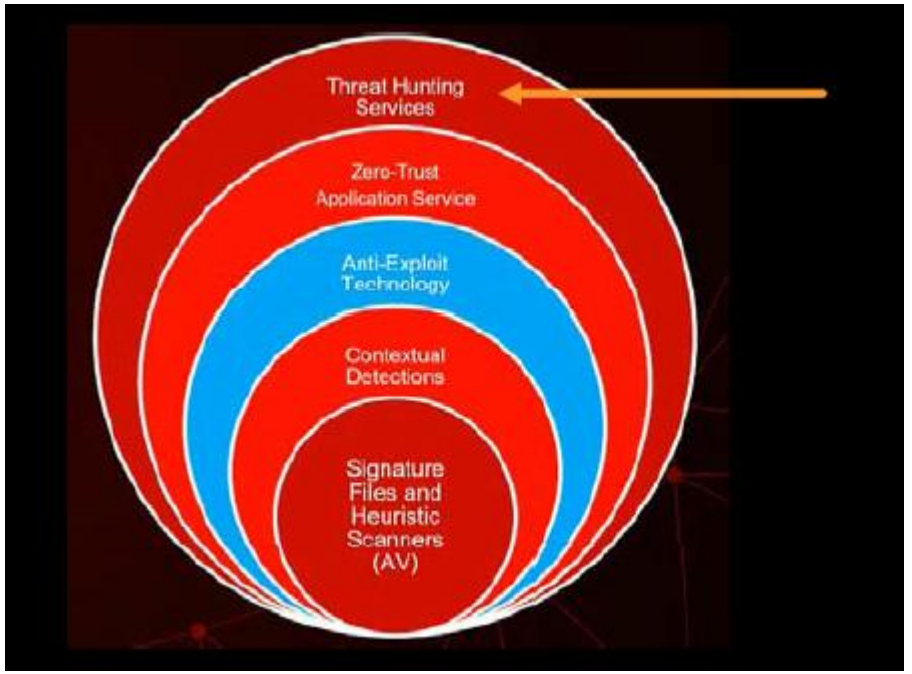
Обзор релиза

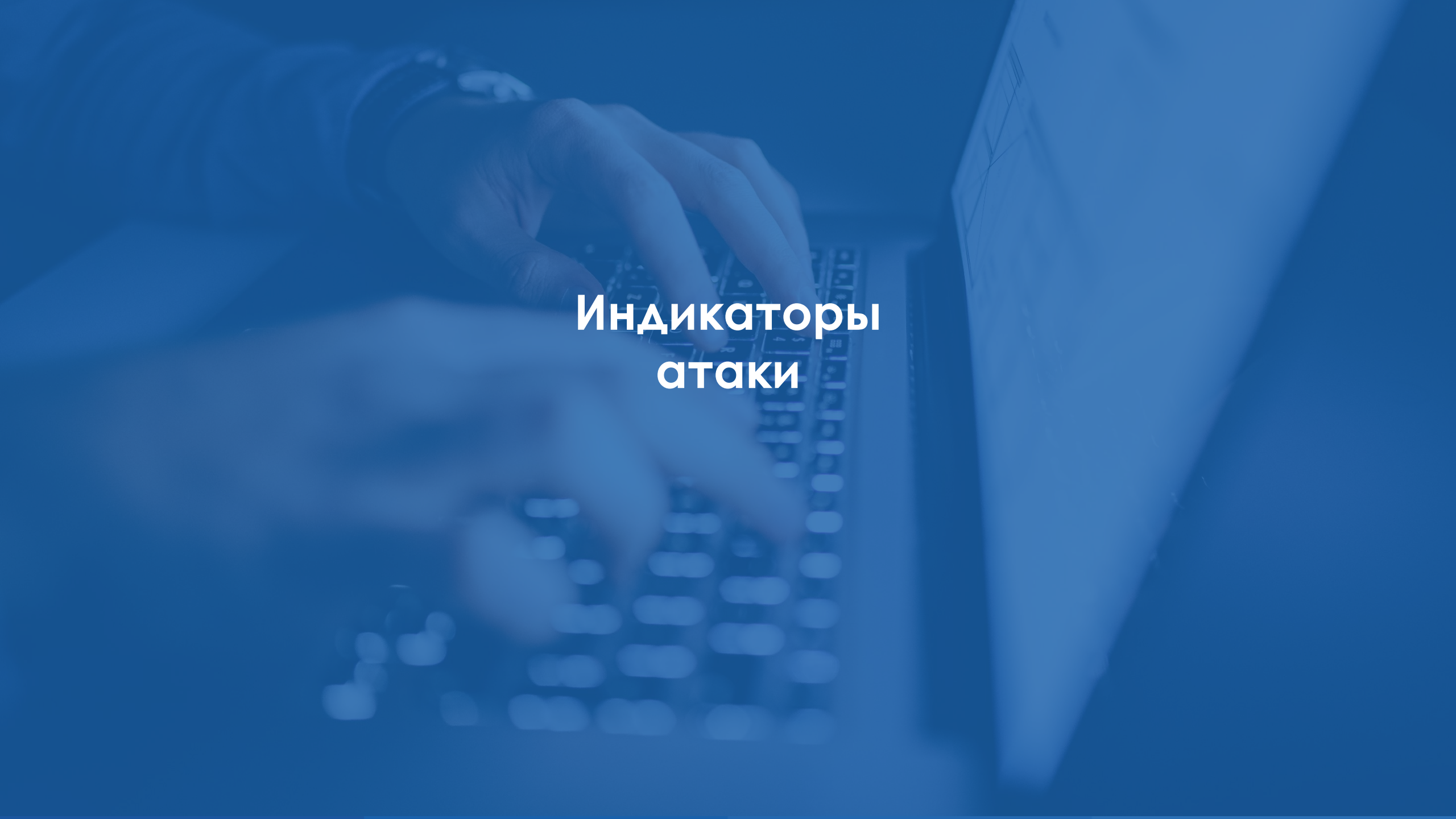
- Сервисы Threat Hunting позволяют администраторам обнаруживать скомпрометированные машины, ранние стадии атак и подозрительную активность

- Сервисы Threat Hunting помогают обнаруживать:
  - RDP-атаки на подключение к удаленному рабочему столу
  - Атаки без использования вредоносных программ
  - Скомпрометированные компьютеры
  - Хакеров и инсайдеров

- Новый релиз XII платформы Aether предоставляет администраторам доступ к инструментам сервиса Threat Hunting, включая индикаторы атак, расширенное расследование, графики и сопоставление с матрицей MITRE

- В новом релизе XII можно автоматически останавливать RDP-атаки





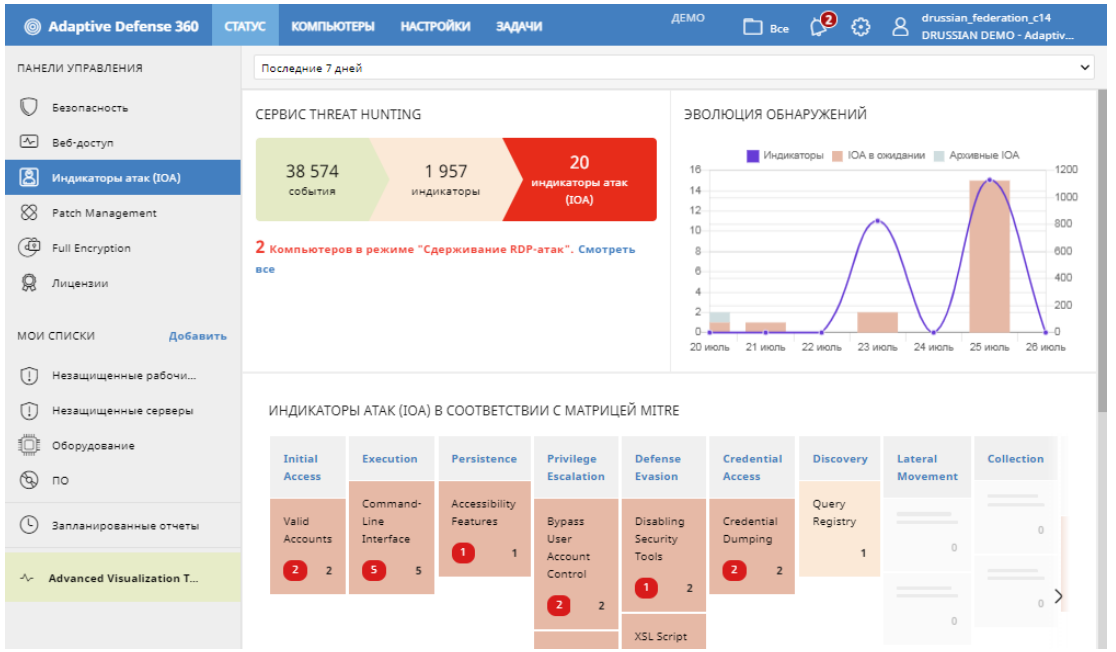
Индикаторы атаки

Что такое индикатор атаки?

- Индикаторы атаки (IoA) – это подтвержденные события, которые с высокой степенью вероятности говорят о наличии атаки
  - Наша команда ИБ подтверждает события, получаемые с конечных устройств, если они соответствуют созданным ею гипотезам
- Как правило, сведения об атаке можно получить на ее самые ранних стадиях, когда еще не используется какое-либо вредоносное ПО
- Мы настоятельно рекомендуем Вам сдерживать атаки и восстанавливать конечные устройства как можно быстрее

Панель индикаторов атаки

- В разделе **Статус** > **Индикаторы атак** Вы можете увидеть сводную информацию по обнаружениям сервиса **Threat Hunting**.
- Панель показывает информацию за период времени, выбранный в верхней части страницы
- Для получения более подробной информации необходимо нажать на соответствующие ссылки в панели

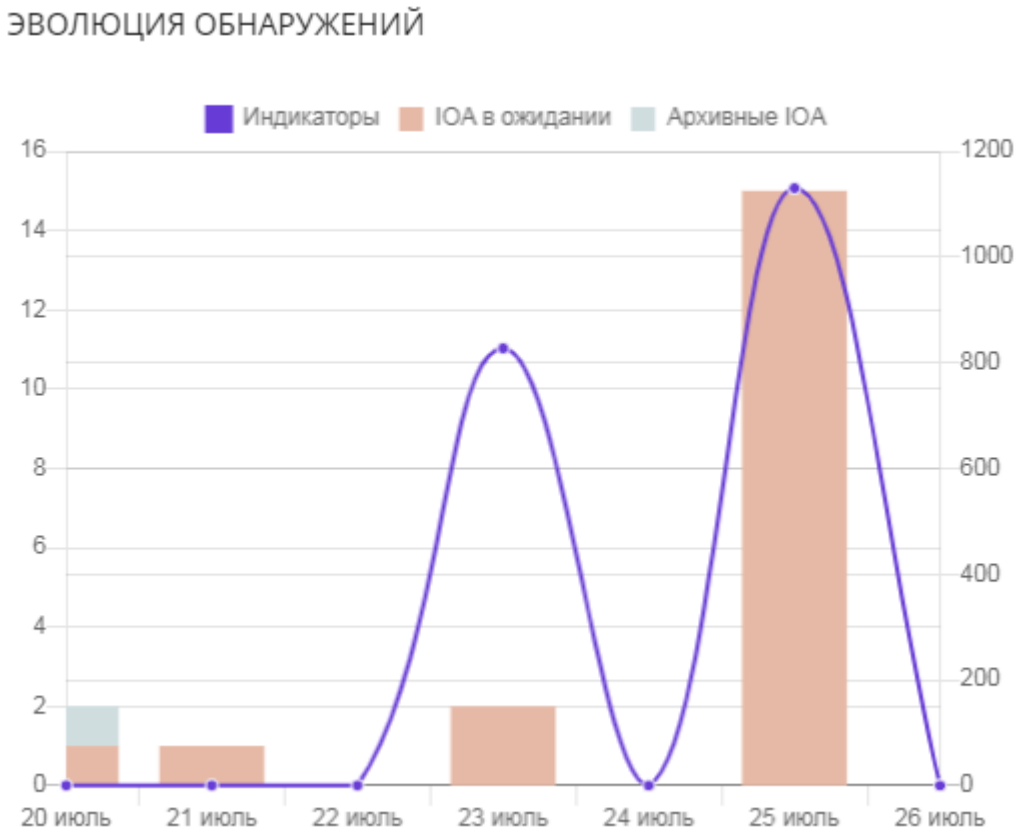


Виджет Threat Hunting

- **Виджет Threat Hunting** показывает сводную информацию по событиям, индикаторам и индикаторам атак (IoA) для всех компьютеров и устройств в сети за выбранный период времени
  - События – количество действий, выполненных программами, установленными на защищаемых компьютерах, и отслеживаемых решением Adaptive Defense 360 / Adaptive Defense
  - Индикаторы – количество подозрительных событий, обнаруженных в потоке данных событий
  - Индикаторы атак – количество индикаторов, которые с высокой степенью вероятности характеризуют наличие атаки
- Чтобы открыть статус защиты компьютеров и увидеть компьютеры, которые подверглись RDP-атаке, необходимо нажать ссылку **Смотреть все**
- Локальный кеш невредоносных программ (goodware)

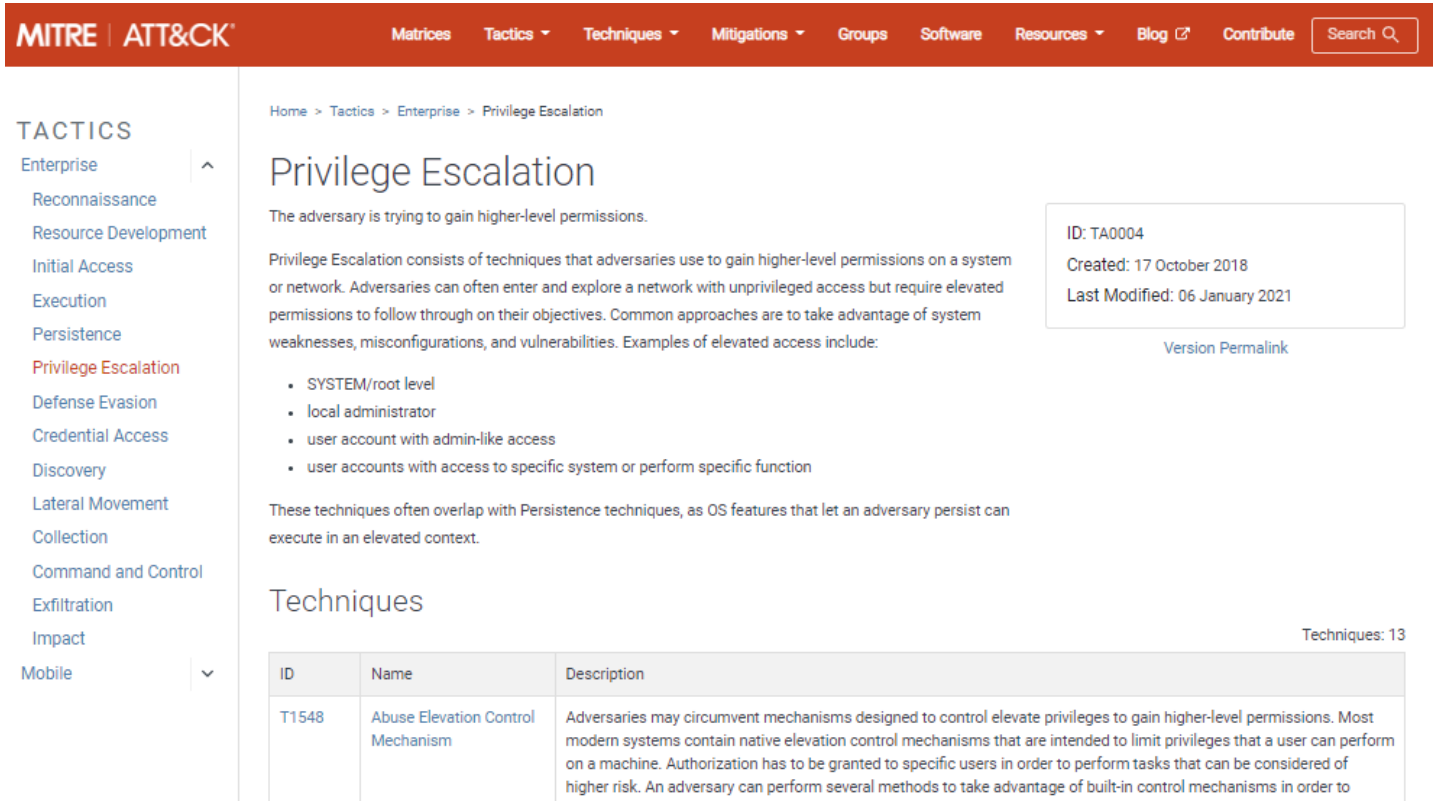
Виджет Эволюция обнаружений

- **Виджет Эволюция обнаружений** гистограмму обнаружений индикаторов, IOA в ожидании и архивных IOA за определенный период времени
  - Индикаторы – количество подозрительных элементов, обнаруженных в потоке данных событий
  - IOA в ожидании – количество подозрительных элементов, которые с высокой степенью вероятности являются индикаторами атак (IOA). При этом администратор еще не проанализировал их
  - Архивные IOA - количество подозрительных элементов, которые с высокой степенью вероятности являются индикаторами атак (IOA). При этом администратор уже проанализировал их и решил связанные с ними вопросы
  - Левая ось Y показывает количество IOA (архивные и в ожидании)
  - Правая ось Y показывает обнаруженные индикаторы
- Чтобы открыть список индикаторов атаки, необходимо нажать на виджете



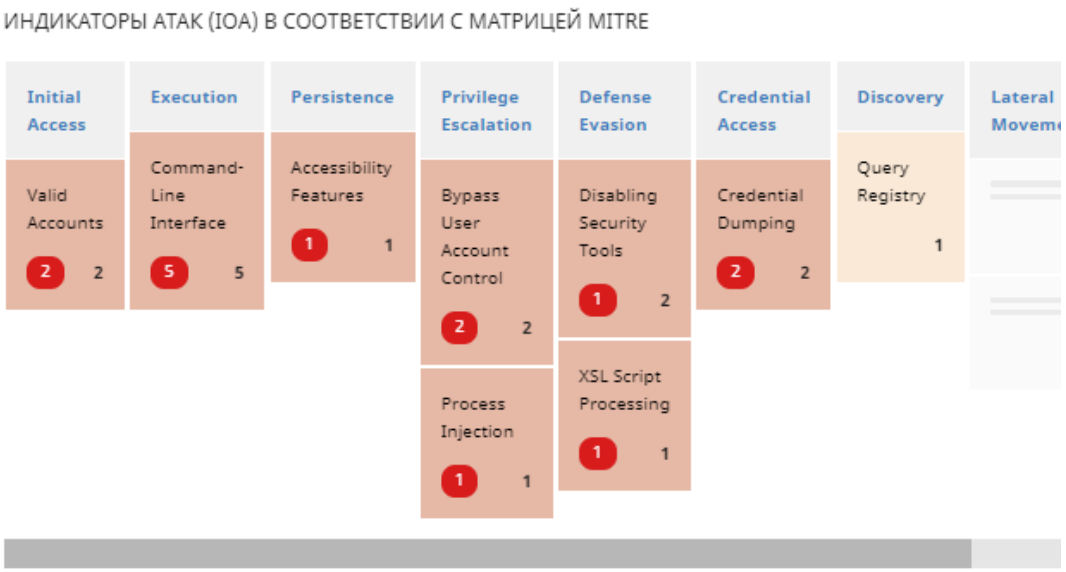
О матрице MITRE ATT&CK

- MITRE ATT&CK – это стандарт в индустрии для классификации тактик и техник атак
- Охотники за угрозами (threat hunting) используют ее для оценки рисков организации



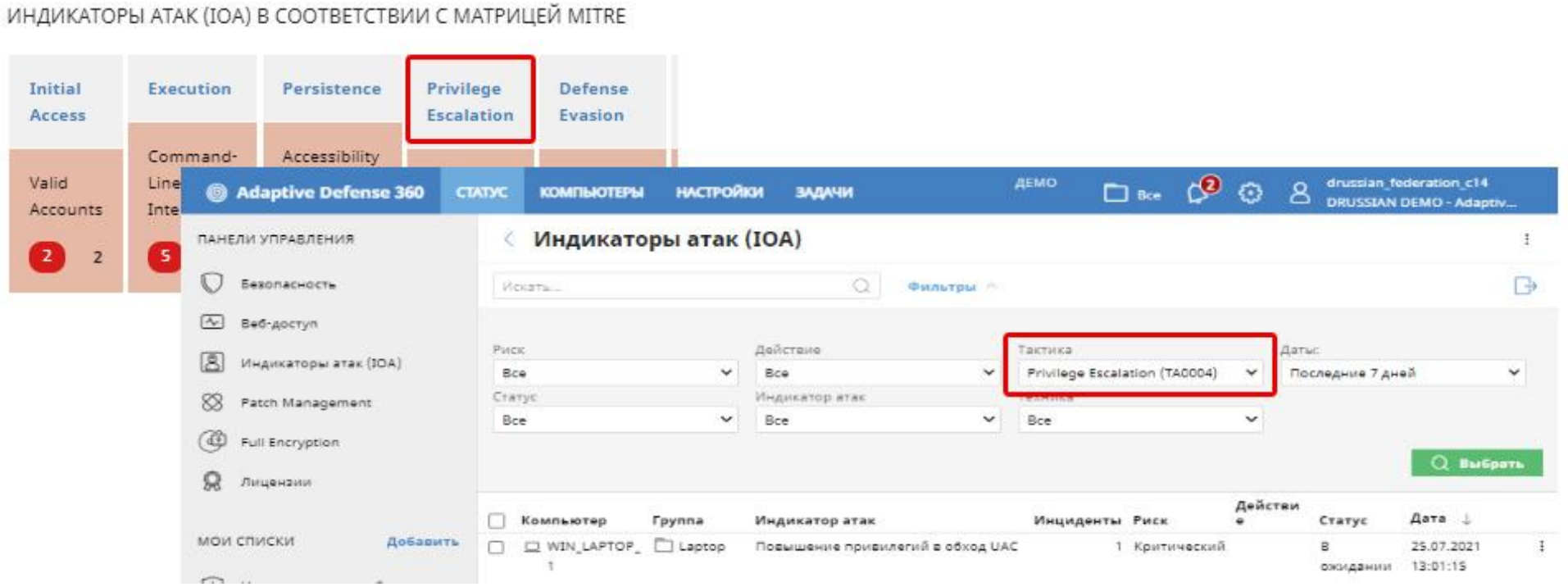
Индикаторы атак в соответствии с матрицей MITRE

- Данный виджет в панели индикаторов атак показывает количество индикаторов атак, обнаруженных за выбранный период времени, в соответствии с тактиками и техниками MITRE
- Чтобы посмотреть название и код техники или общее количество обнаружений, наведите мышку на столбец или блок
  - Заголовки столбцов – это тактики
  - Техники показываются ниже тактики
  - Чтобы увидеть IOA в ожидании, наведите мышку на число в красном кружке



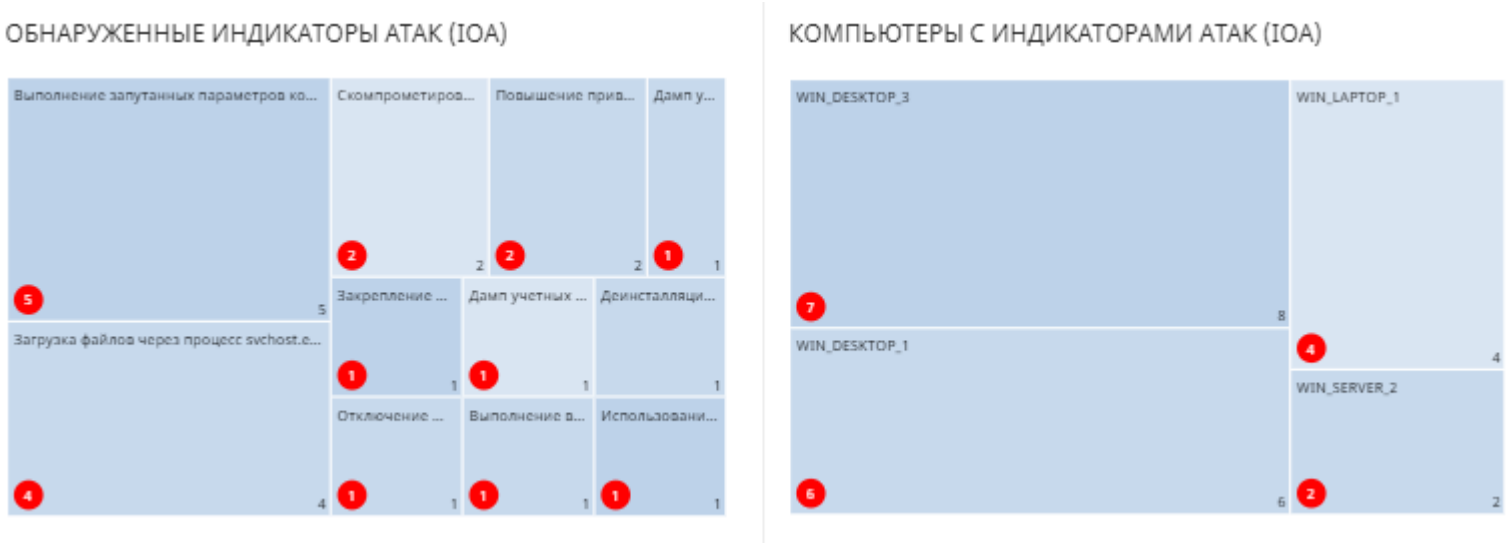
Индикаторы атак в соответствии с матрицей MITRE

- Нажмите на тактику или технику, чтобы открыть список Индикаторы атак с выборкой по выбранной тактике или тактике и технике



Обнаруженные IOA и компьютеры с IOA

- Виджет **Обнаруженные индикаторы атак** показывает распределение по типу обнаруженных IOA за выбранный период времени
  - Чем больше количество обнаруженных IOA определенного типа (относительно других типов), тем крупнее его квадратик
- Виджет **Компьютеры с индикаторами атак** показывает распределение обнаруженных IOA по компьютерам в сети за выбранный период времени
- Нажмите на требуемый квадратик в виджетах, чтобы открыть список Индикаторы атак с выбранной информацией

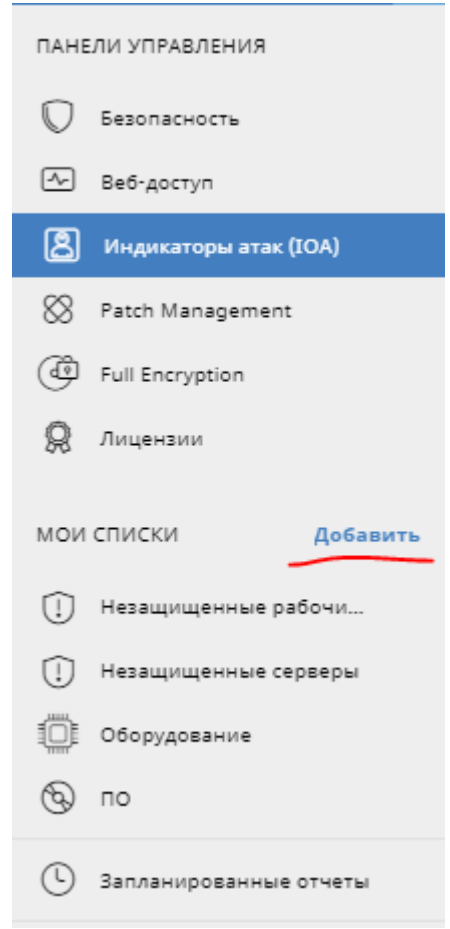


Список Индикаторы атак

- Список **Индикаторы атак** показывает сведения по IOA, обнаруженным решениями Adaptive Defense 360 или Adaptive Defense на рабочих станциях и серверах

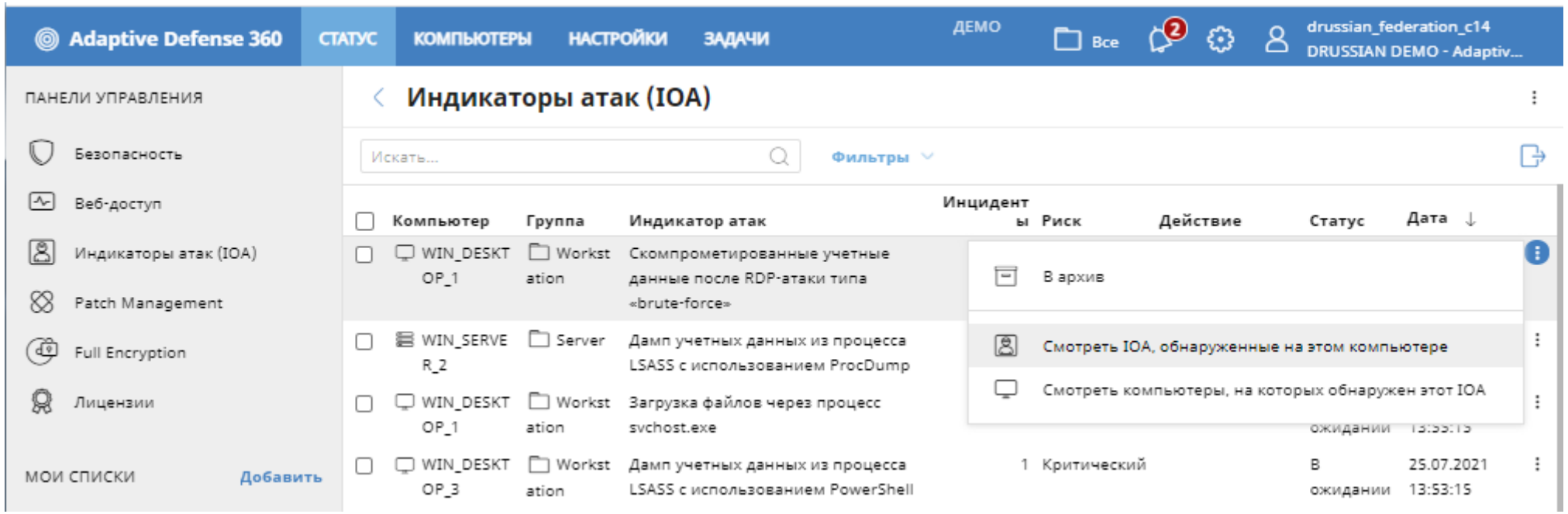
- Чтобы открыть список, в панели Индикаторы атак необходимо нажать на количество IOA (виджет Сервис Threat Hunting) или на любые другие виджеты (и их элементы) в данной панели (в этом случае откроется отфильтрованный список)

- Чтобы добавить список в **Мои списки**:
  - В левом меню «Мои списки» нажмите ссылку Добавить
  - В секции Безопасность выберите Индикаторы атак (IOA)
  - При необходимости настройте фильтр и нажмите Сохранить



Список Индикаторы атак

- Для просмотра сведений по всем доступным IOA, Вы можете экспортировать список в CSV-файл
- В списке индикаторов атак можно применить фильтр для более узкого поиска
- В контекстном меню у каждого индикатора атаки Вы можете отправить данный индикатор в архив, посмотреть IOA, обнаруженные на данном компьютере или посмотреть компьютеры, на которых обнаружен данный IOA



Сведения по индикатору атаки

- Для просмотра сведений по конкретному индикатору атаки, нажмите на нем в списке индикаторов атак
- Чтобы отправить индикатор атаки в архив или перевести в статус «В ожидании», нажмите синюю кнопку рядом с датой обнаружения
- Для просмотра описаний тактики и техники, используемых на пострадавшем компьютере, нажмите кнопку **Расширенное исследование атаки**
  - Включает рекомендации по смягчению последствий атаки и последовательность событий, приведших к появлению индикатора атаки

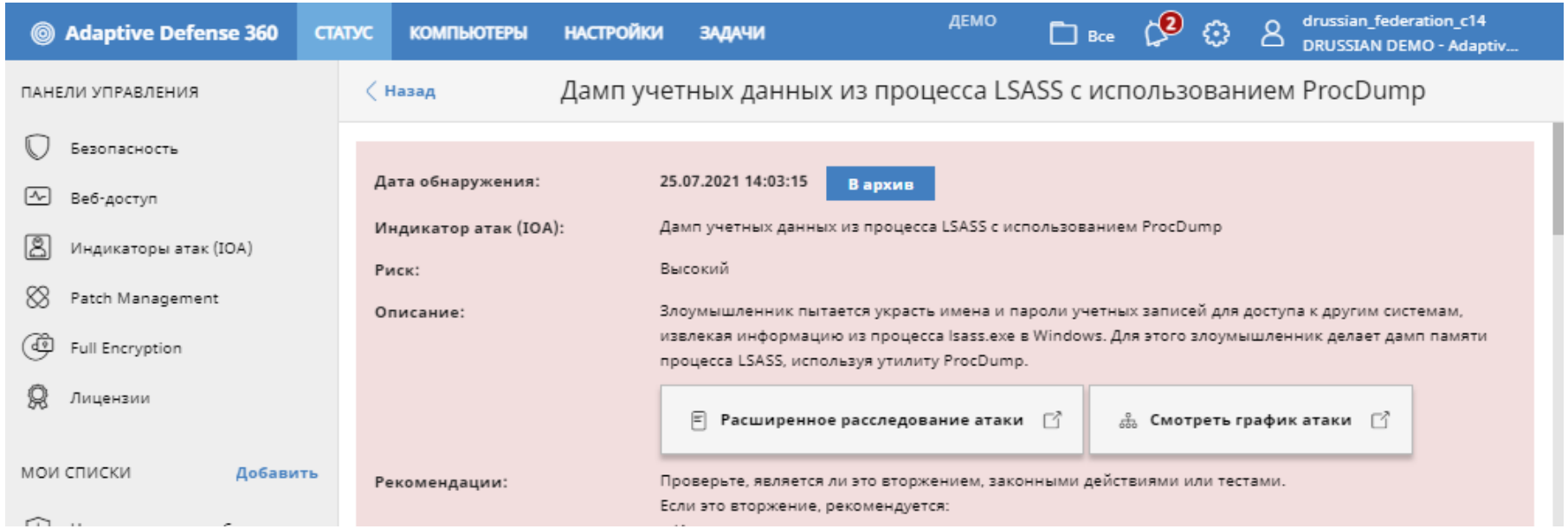
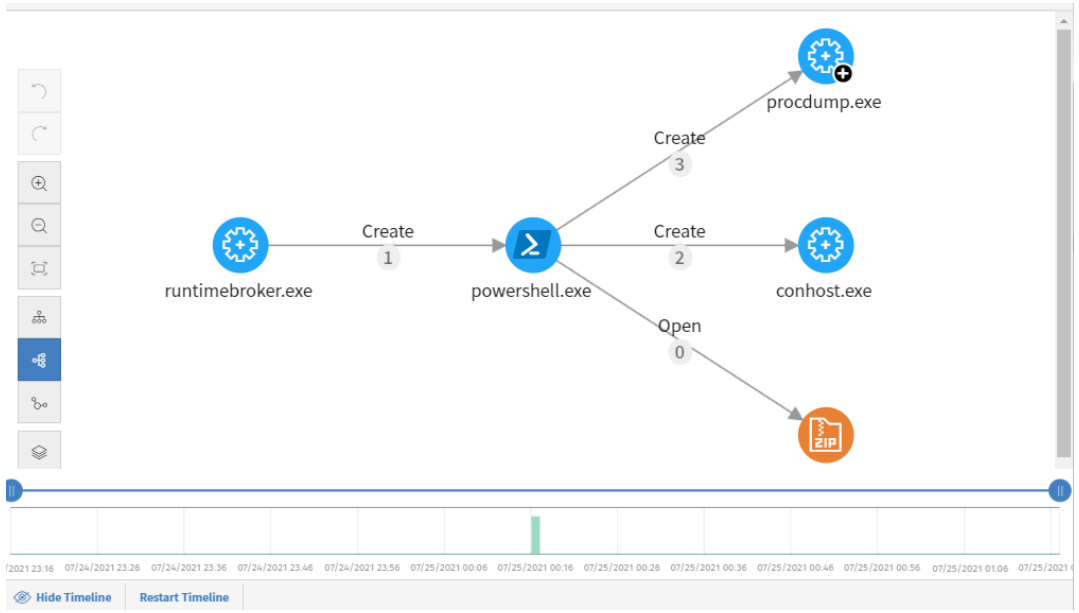


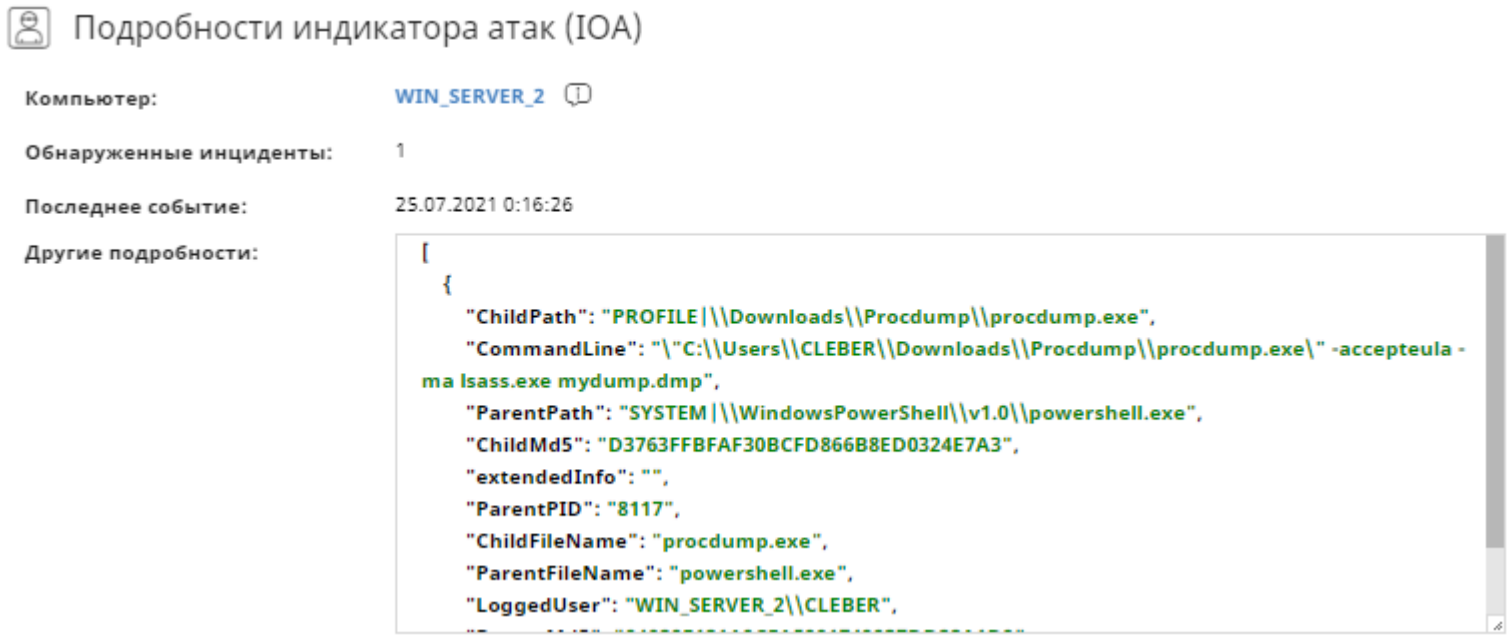
График атаки IOA

- Для просмотра графического представления дерева выполнения атаки, по которому появился данный индикатор атаки, на странице со сведениями IOA нажмите на кнопку **Смотреть график атаки**
  - Узлы – это элементы, которые участвуют в операции (например, процессы, файлы, и т.д.)
  - Стрелки показывают направление операции
- График помогает идентифицировать причину атаки



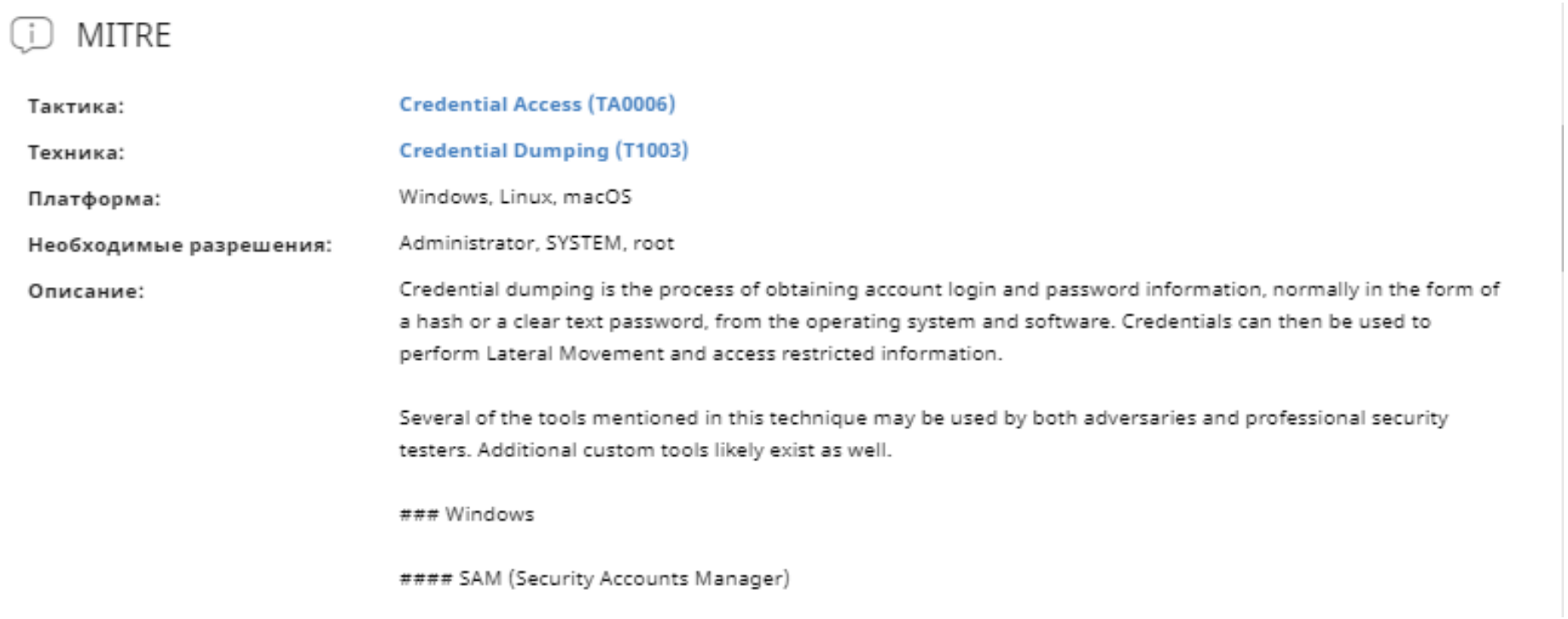
Подробности индикатора атаки

- Секция **Подробности индикатора атаки (IOA)** показывает пострадавший компьютер, количество обнаруженных инцидентов, а также дату и время последнего события
- Блок Другие подробности предоставляет пример JSON с полями, соответствующими событию, которое привело к появлению данного индикатора атаки



Подробности MITRE

- Секция **MITRE** показывает тактику и технику, а также подробное описание техники
- Нажмите на тактику или технику, чтобы увидеть их описания на веб-сайте MITRE

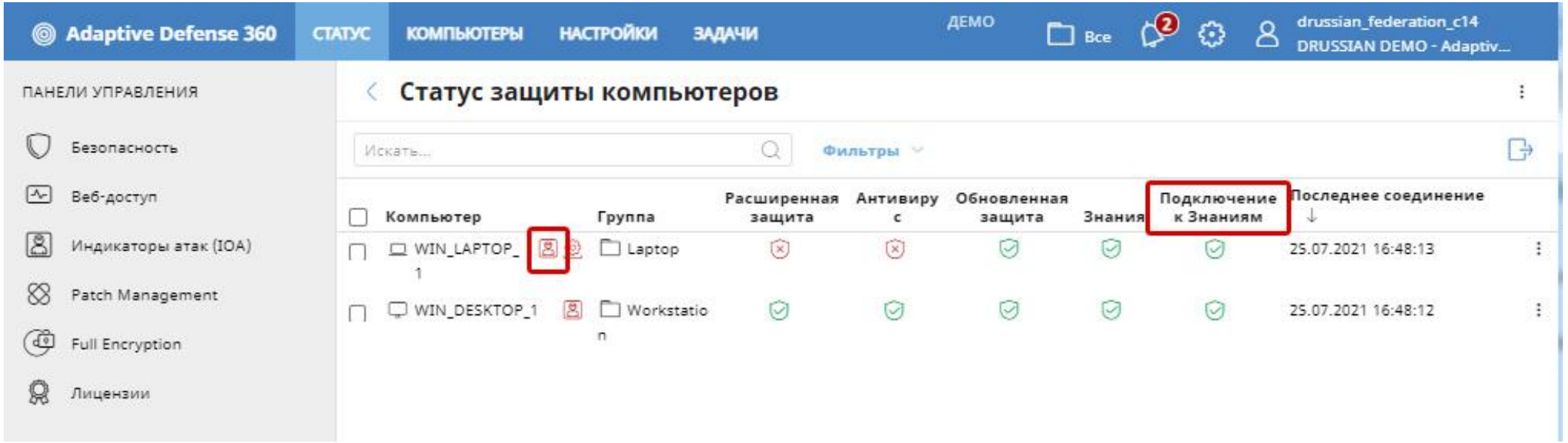


Список Статус защиты компьютеров

- В панели **Индикаторы атаки** виджет **Сервис Threat Hunting** показывает количество компьютеров в режиме сдерживания RDP-атак
- Режим сдерживания RDP-атак защищает от тех сценариев, когда хакер проникает в ИТ-сеть через уязвимый компьютер, затем осуществляет горизонтальные перемещения на другие незащищенные устройства, и использует RDP для перехода с одного устройства на другое
- Нажмите на ссылку **Смотреть все**, чтобы открыть список Статус защищенных компьютеров с выборкой по компьютерам с включенным режимом сдерживания RDP-атак

Изменения в списке Статус защищенных компьютеров

- Список **Статус защищенных компьютеров** включает новую иконку RDP для отображения того, что данный компьютер работает с включенным режимом сдерживания RDP-атак
- Новый столбец **Подключение к Знаниям** показывает, может ли установленный агент подключаться к серверам знаний и обновлять сигнатурные файлы

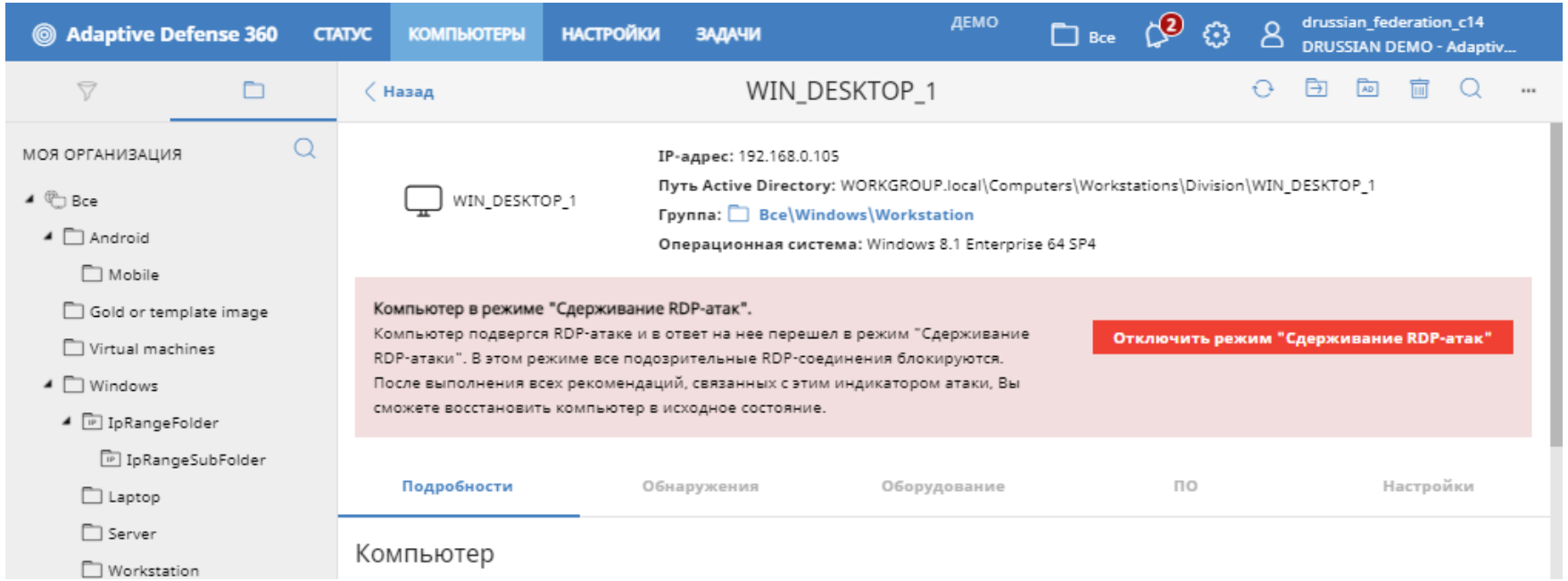


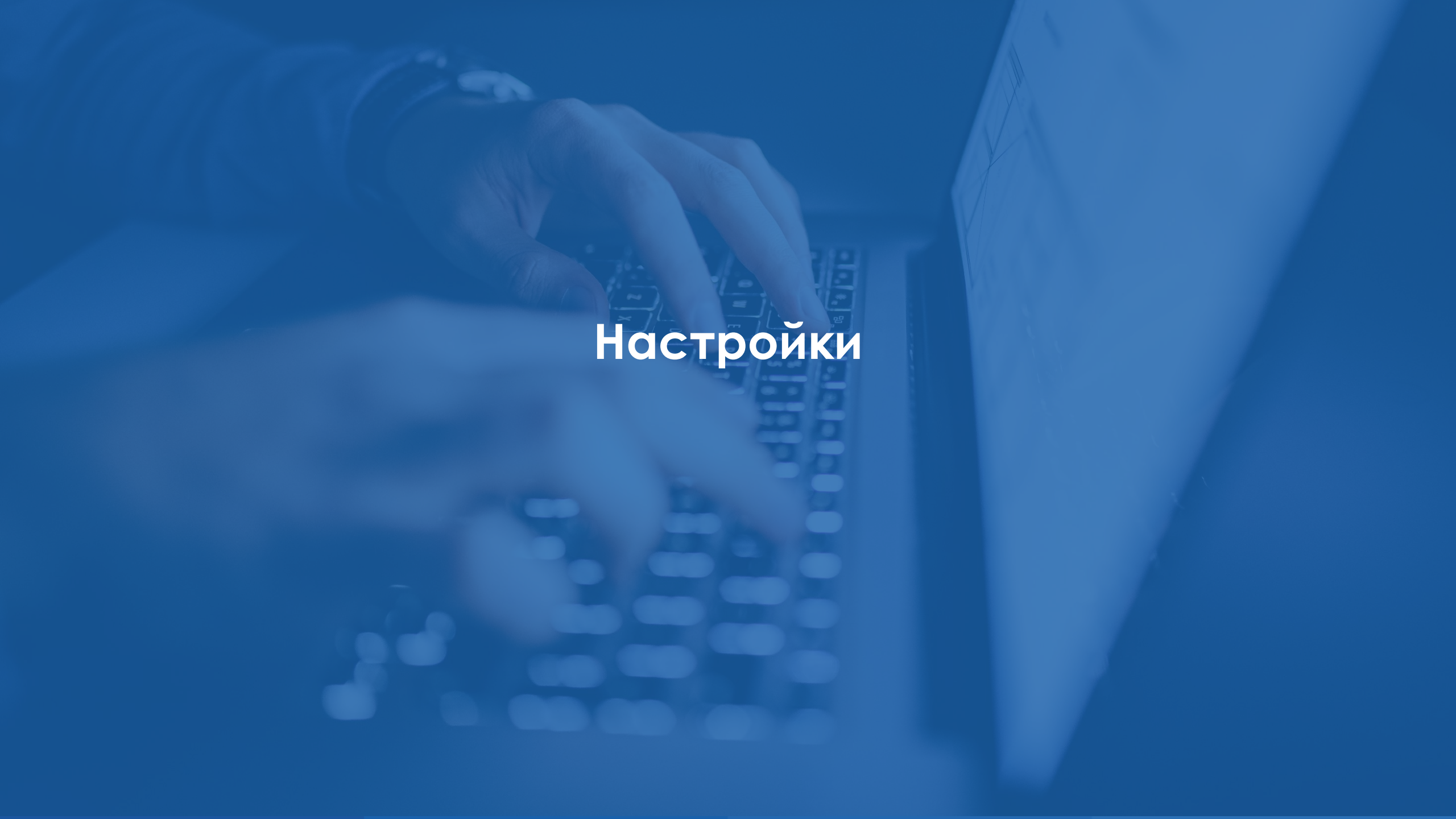
Режим сдерживания RDP-атак

- Новый релиз XII платформы Aether отслеживает попытки подключения к компьютеру в сети через службу RDP
- Если свыше 50 неудачных попыток подключения были с одного и того же IP-адреса, то включается режим **Сдерживание RDP-атак**
  - Запрещаются все IP-адреса, которые имеют свыше 23 подключений
  - Если злоумышленник способен удачно подключиться с правами администратора, то идентифицируются все коммуникации с внешних IP-адресов за последние 24 часа с более одной ошибкой, при этом эти внешние IP-адреса запрещаются
  - Если свыше 50 неудачных попыток подключения были с одного и того же IP-адреса, то включается режим **Сдерживание RDP-атак**
- Вы можете добавить разрешенные IP-адреса в разрешенный список, чтобы подключения с этих IP-адресов не блокировались

Страница со сведениями по компьютеру

- В списке выберите требуемый компьютер, чтобы перейти на страницу со сведениями о данном компьютере
- В блоке с уведомлениями показывается предупреждение о том, что у компьютера включен режим сдерживания RDP-атак
- Чтобы отключить данный режим, нажмите на кнопку **Отключить режим «Сдерживания RDP-атак»**



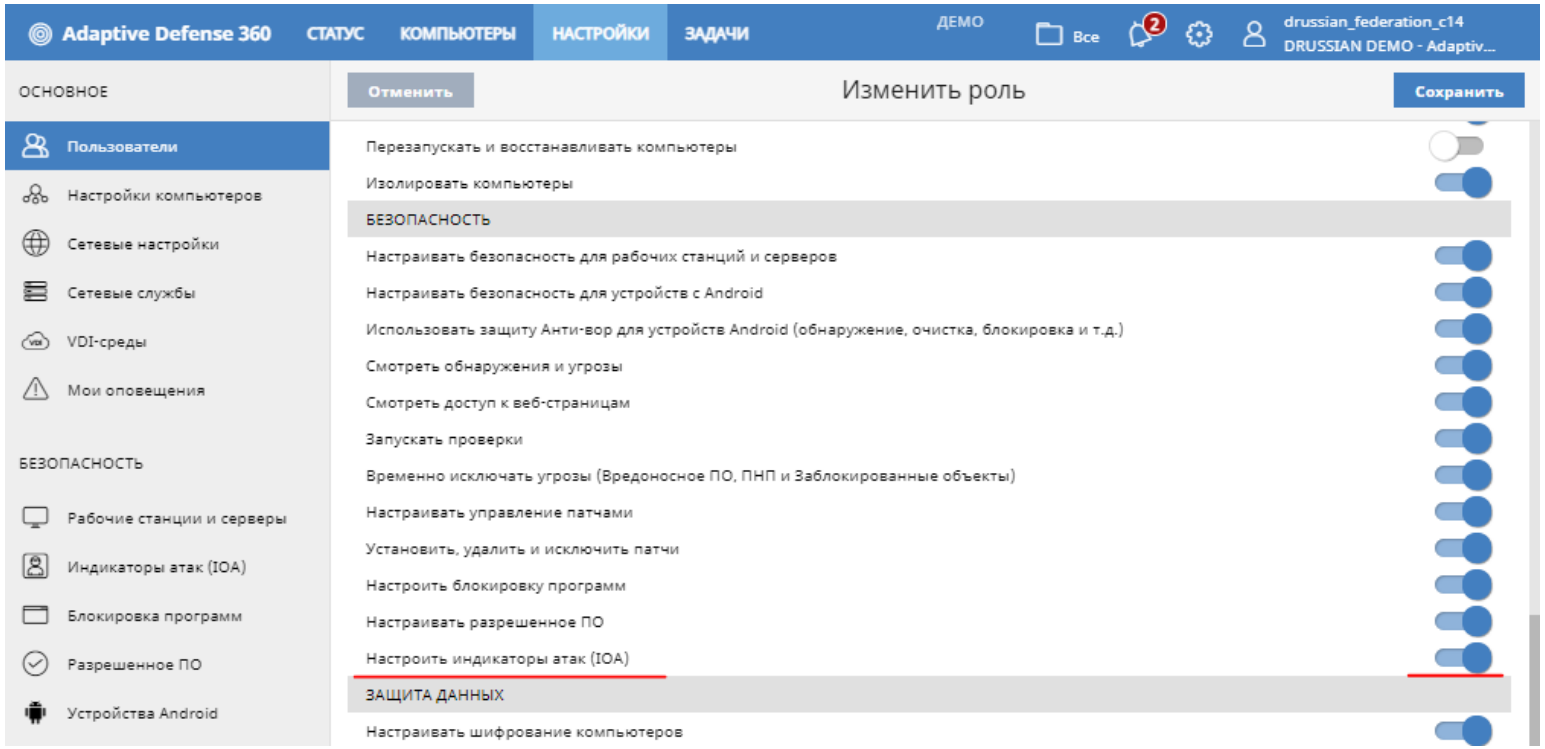


Настройки

Права в ролях пользователей

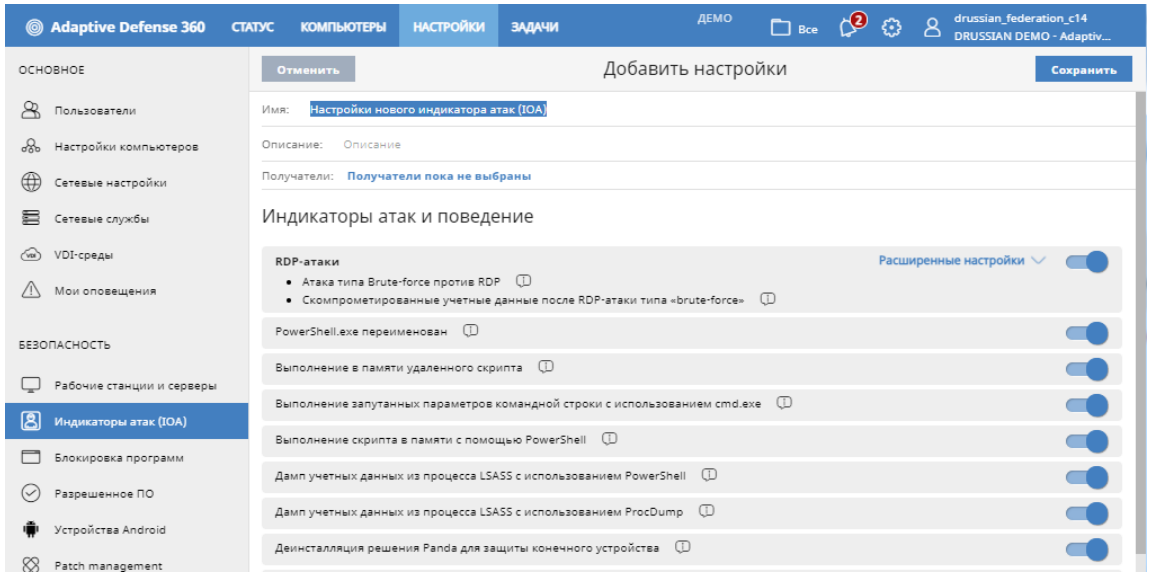
- Вам необходимо настроить новые права безопасности для той роли пользователей, которые смогут настраивать параметры индикаторов атак

- В разделе Настройки > Пользователи на закладке Роли у требуемой роли необходимо включить разрешение **Настроить индикаторы атак (IOA)**



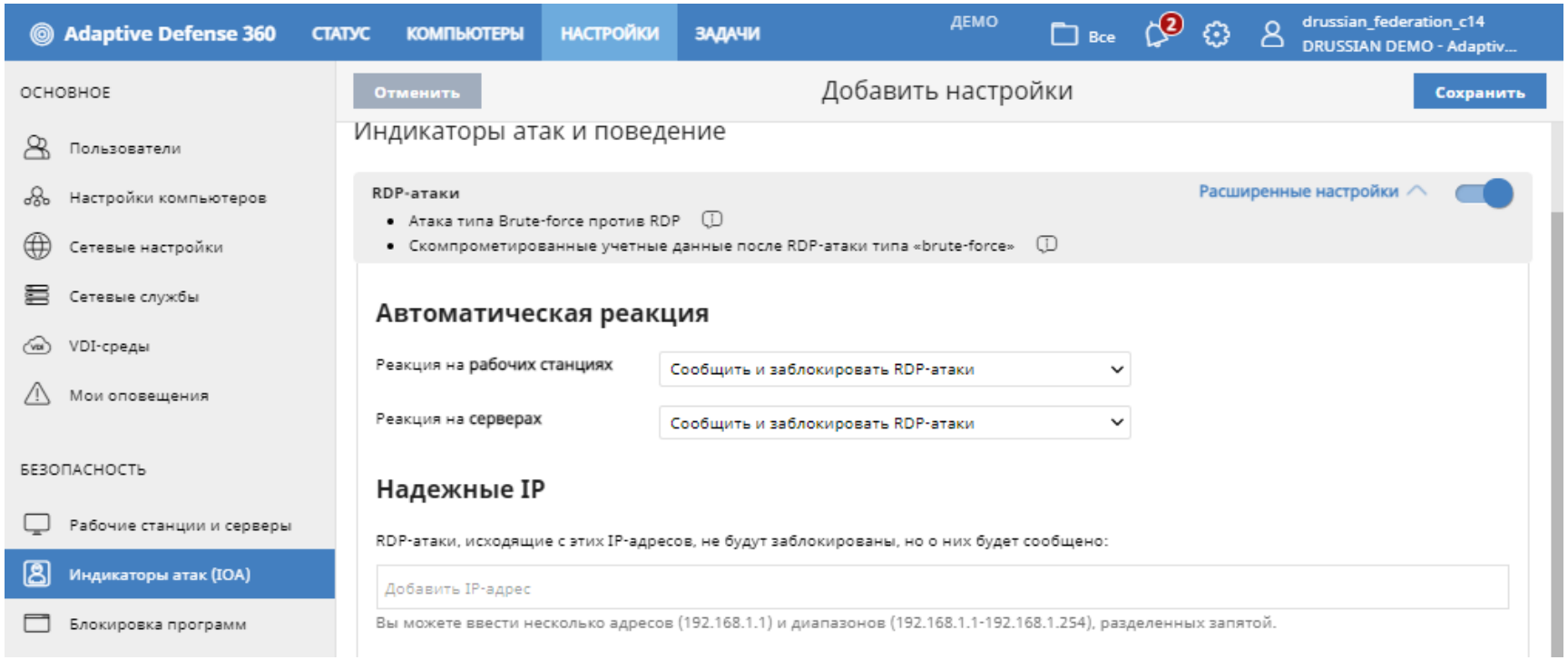
Настройки безопасности – Индикаторы атак

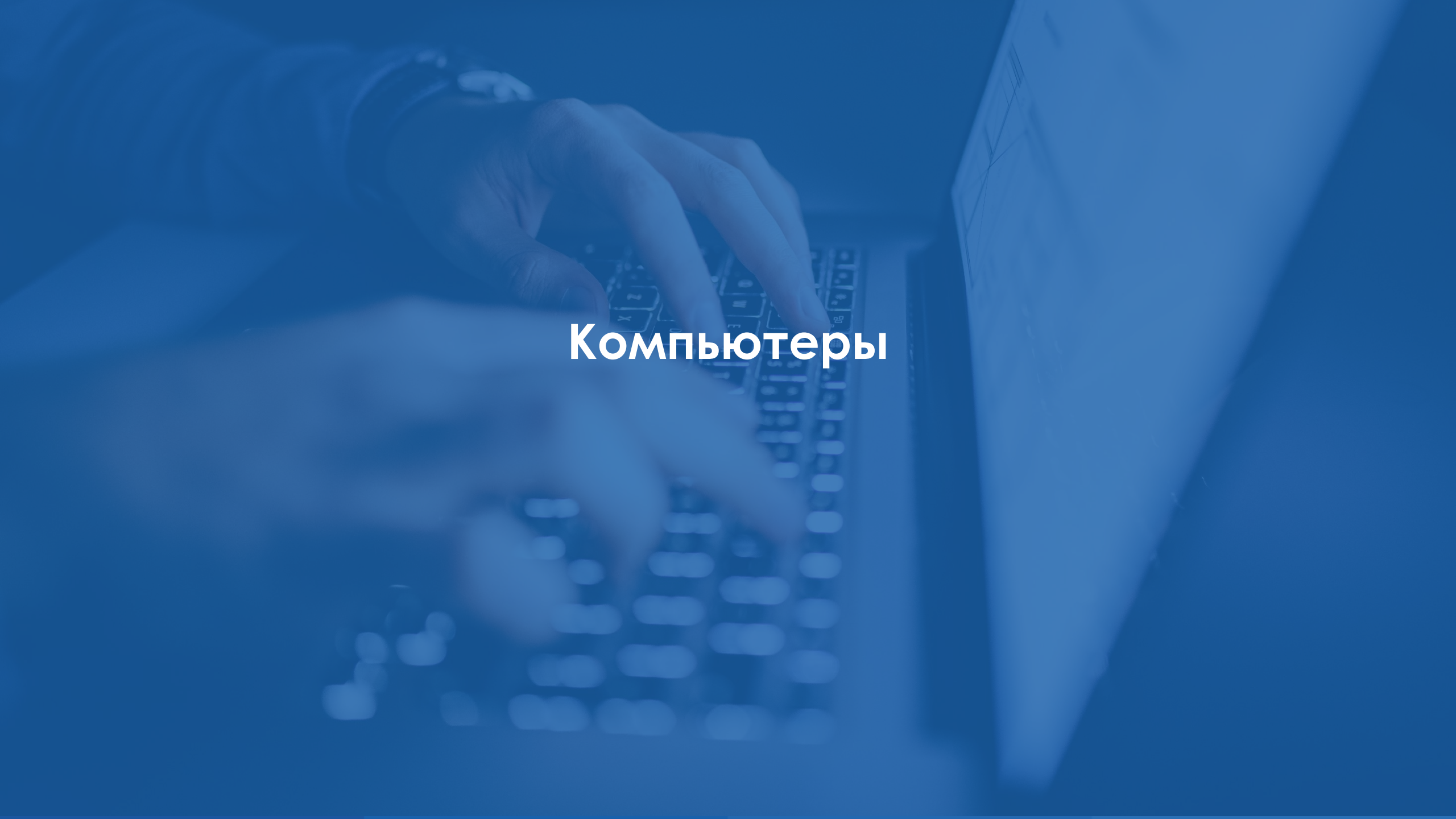
- В разделе **Настройки > Индикаторы атак (IOA)** Вы можете включить защиту от RDP-атак и других индикаторов атак
- Чтобы посмотреть описание индикатора атаки, нажмите на иконку с восклицательным знаком у требуемого индикатора в списке
- Вы можете отключить индикаторы атак для ложных срабатываний и применить профиль с настройками безопасности для группы компьютеров, конкретных компьютеров или для всей организации



Расширенные настройки для RDP-атак

- Когда Вы включаете опцию **RDP-атаки**, Вы можете настройки **Расширенные настройки**
  - **Автоматическая реакция –** в этой секции Вы можете выбрать, какие действия будут применяться автоматически отдельно для рабочих станций и серверов (Только сообщить или Сообщить и заблокировать RDP-атаки)
  - **Надежные IP** – в этой секции Вы можете указать IP-адреса и диапазоны IP-адресов в качестве исключений. О них будет сообщаться, но они не будут блокироваться

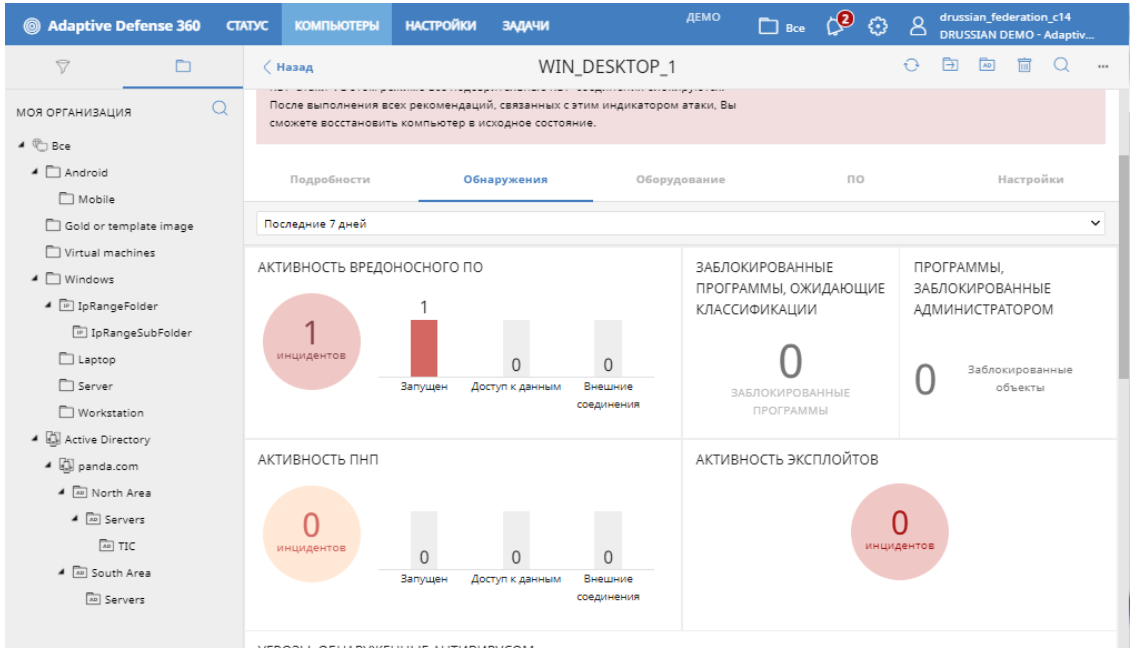


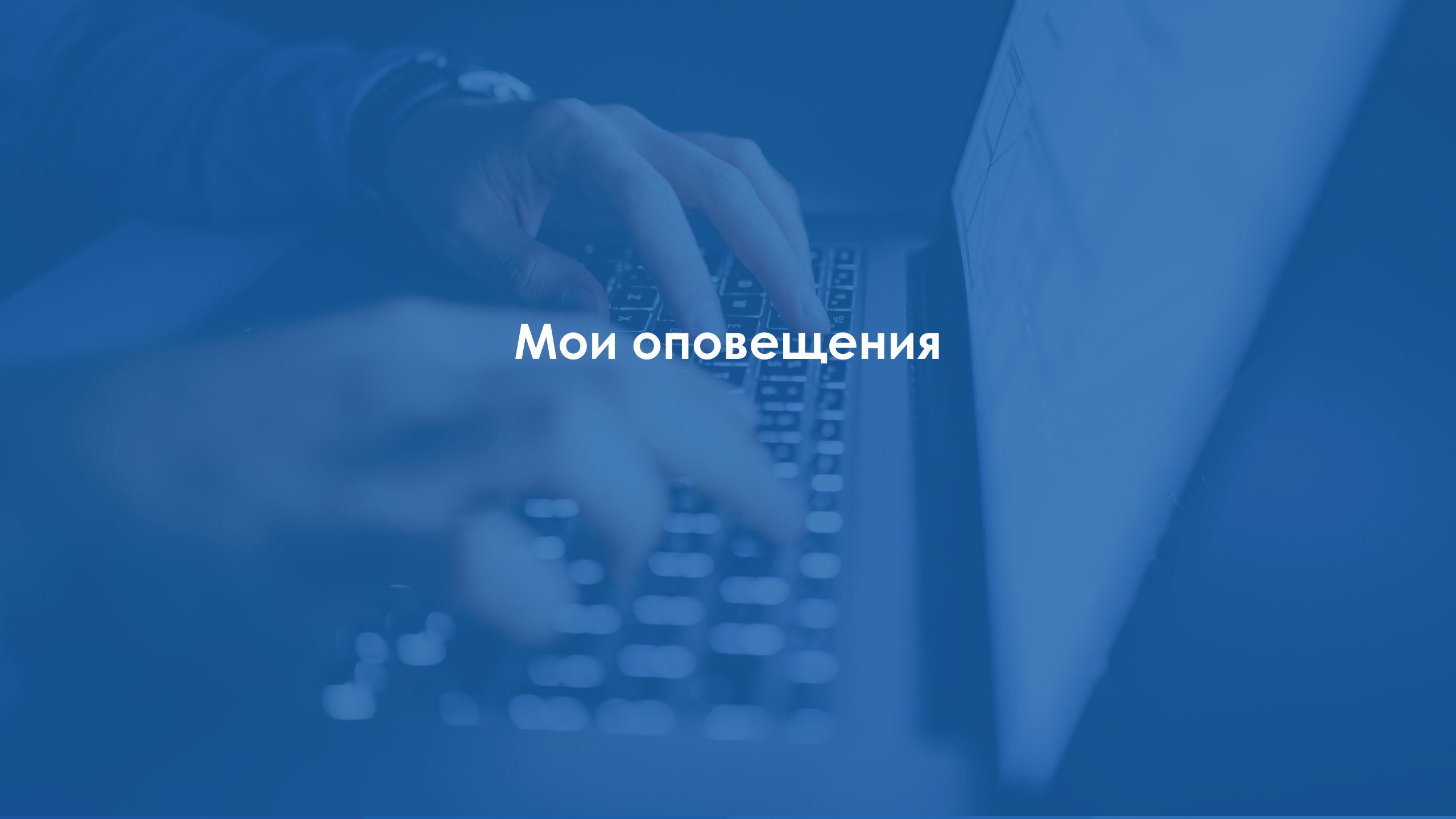


Компьютеры

Закладка Обнаружения

- На странице со сведениями по компьютеру новая закладка **Обнаружения** показывает количество обнаруженных на нем вредоносных программ, ПНП, эксплойтов, уязвимостей и индикаторов атак, отфильтрованных по дате
- Закладка также показывает угрозы, обнаруженные антивирусом, а если у клиента имеются лицензии на модуль Patch Management, то еще и доступные патчи и программы на стадии End-of-Life
- Нажмите на элементы виджетов, связанных с индикаторами атак, чтобы открыть список **Индикаторы атак**, отфильтрованный по данному компьютеру



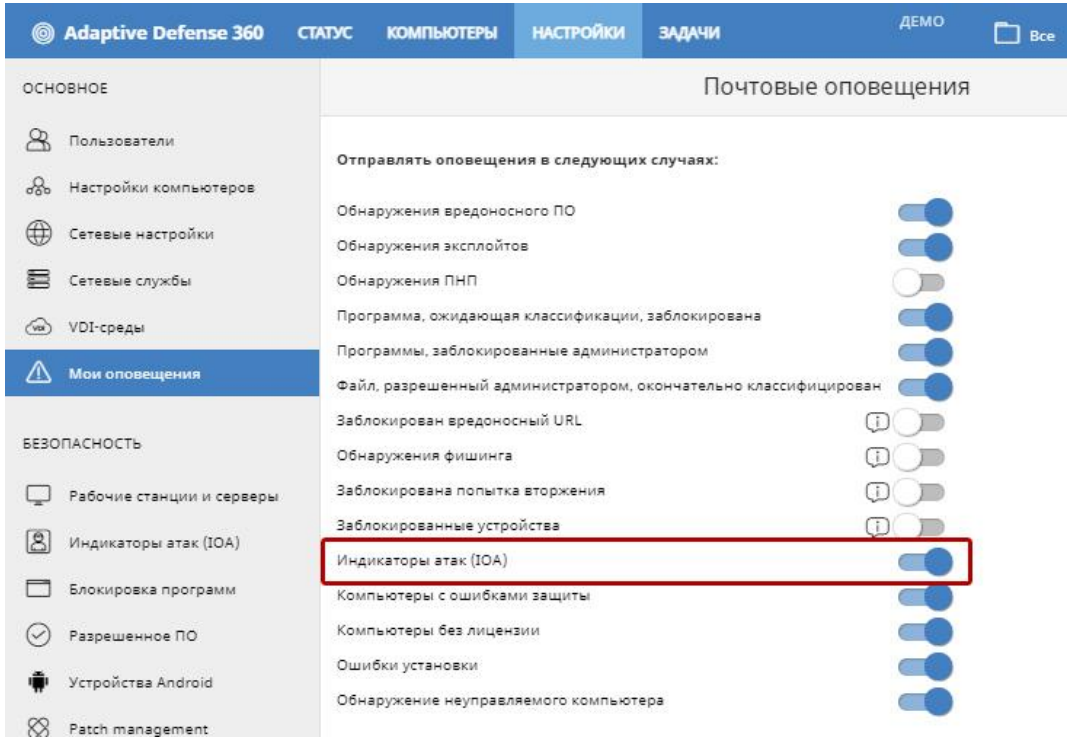


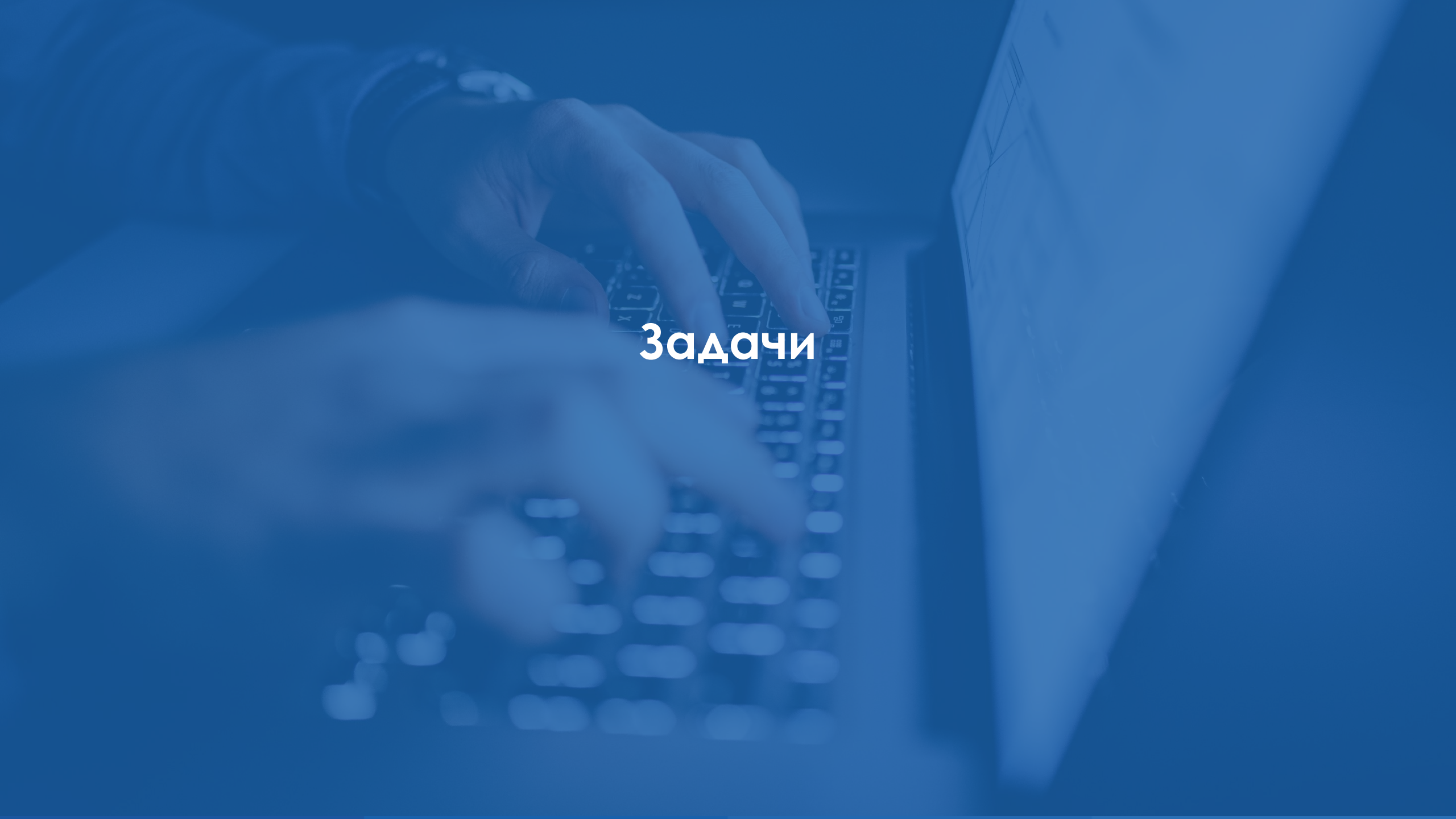
Мои оповещения

Настройки оповещений

- На странице **Настройки** > **Мои оповещения** Вы можете включить опцию **Индикаторы атак (IOA)** для получения почтовых уведомлений при появлении индикатора атаки

- Получатель почтового оповещения сможет нажать на ссылку в письме, чтобы перейти на страницу со сведениями о данном индикаторе атаки в веб-консоли

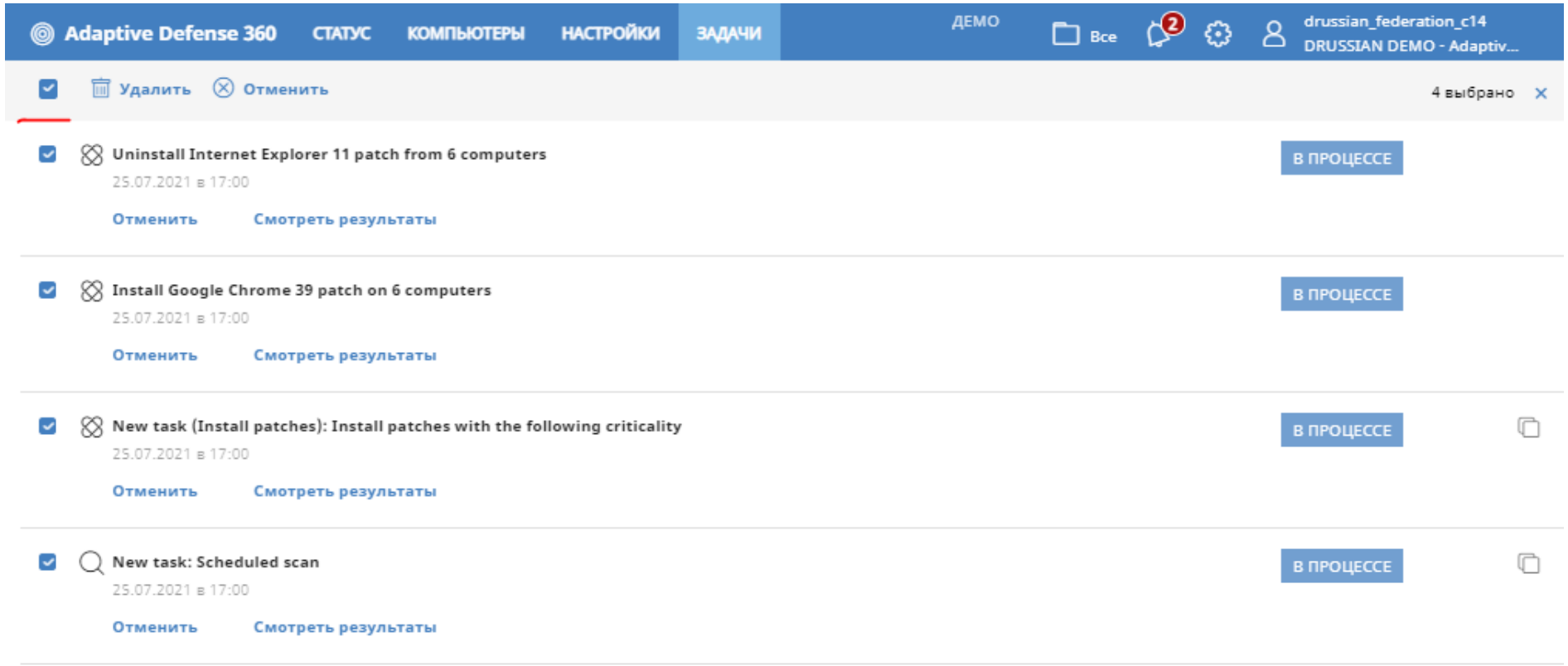




Задачи

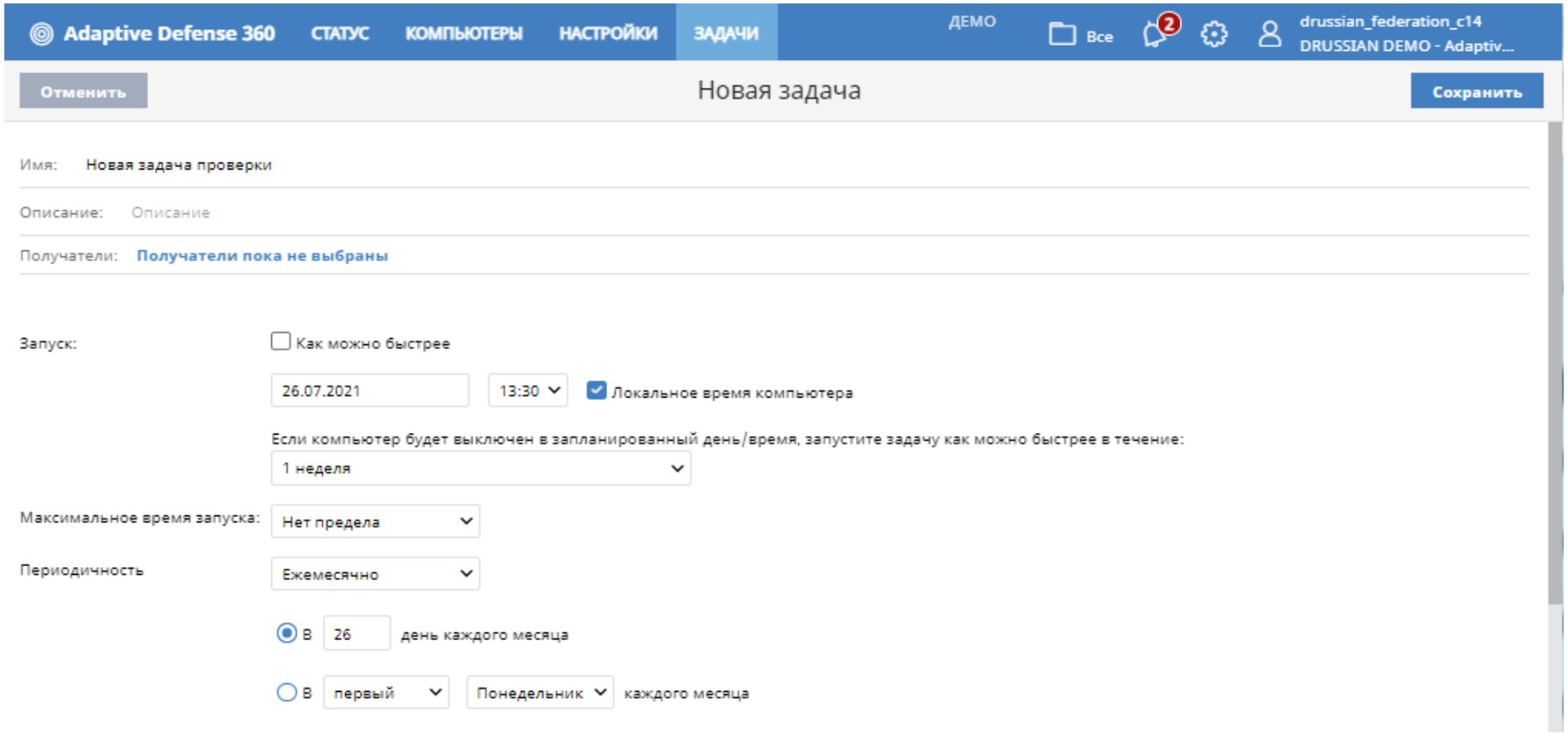
Управление задачами

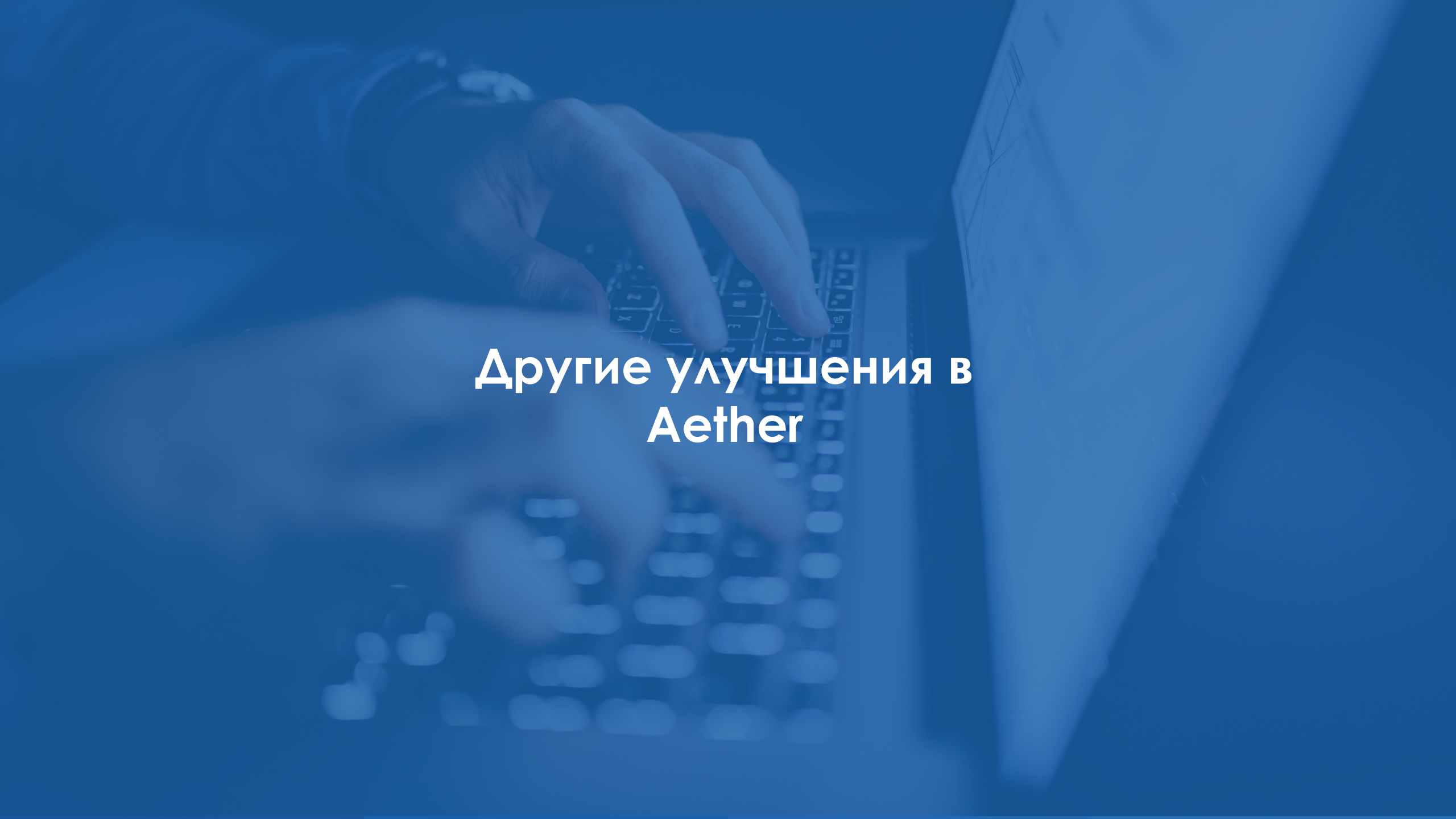
- В разделе **Задачи** теперь можно выбрать все задачи, чтобы затем отменить их или удалить
  - Вы должны сперва отменить задачу, чтобы потом можно было ее удалить



Периодичность выполнения задачи

- Теперь при создании задачи по запланированной проверке или установке патчей Вы можете настроить выполнение задачи на определенный день недели или месяца

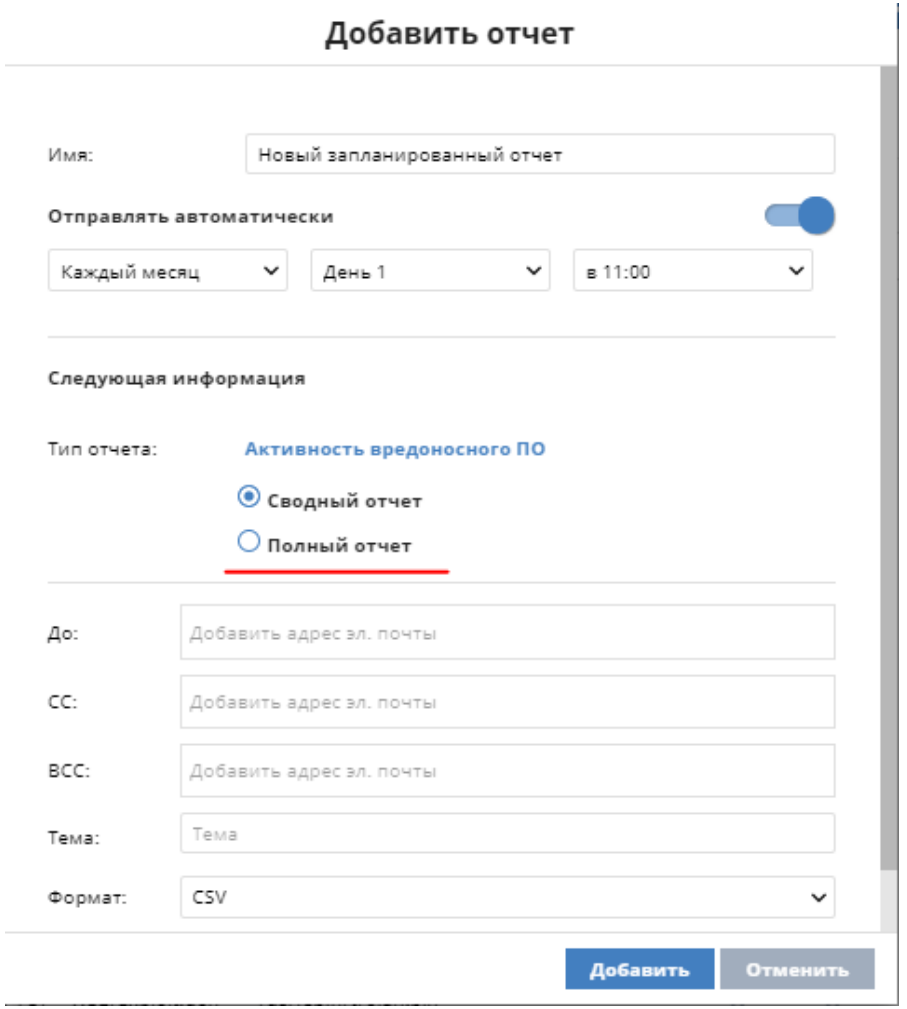




Другие улучшения в Aether

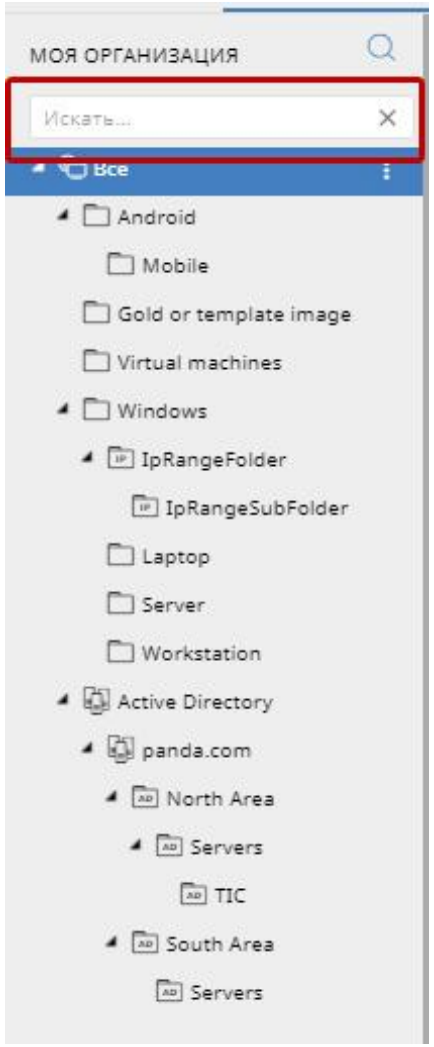
Подробные отчеты

- Теперь можно отправлять полный подробный отчет об активности ПО или вредоносного ПО
- Получатель почтового оповещения сможет нажать на ссылку в письме, чтобы перейти на страницу со сведениями о данном индикаторе атаки в веб-консоли



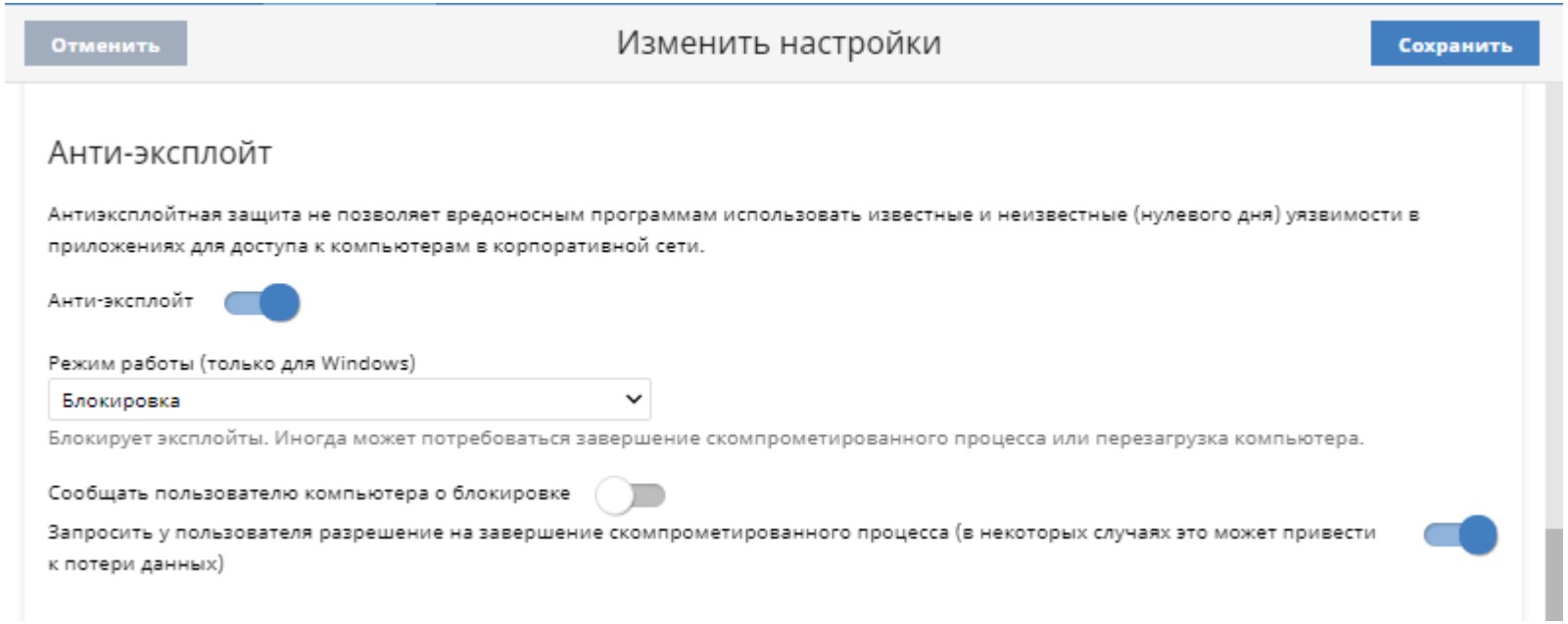
Поиск в Моя организация

- В разделе Компьютеры в блоке Моя организация теперь можно осуществлять поиск по группам в дереве



Блокировка эксплойтов по умолчанию

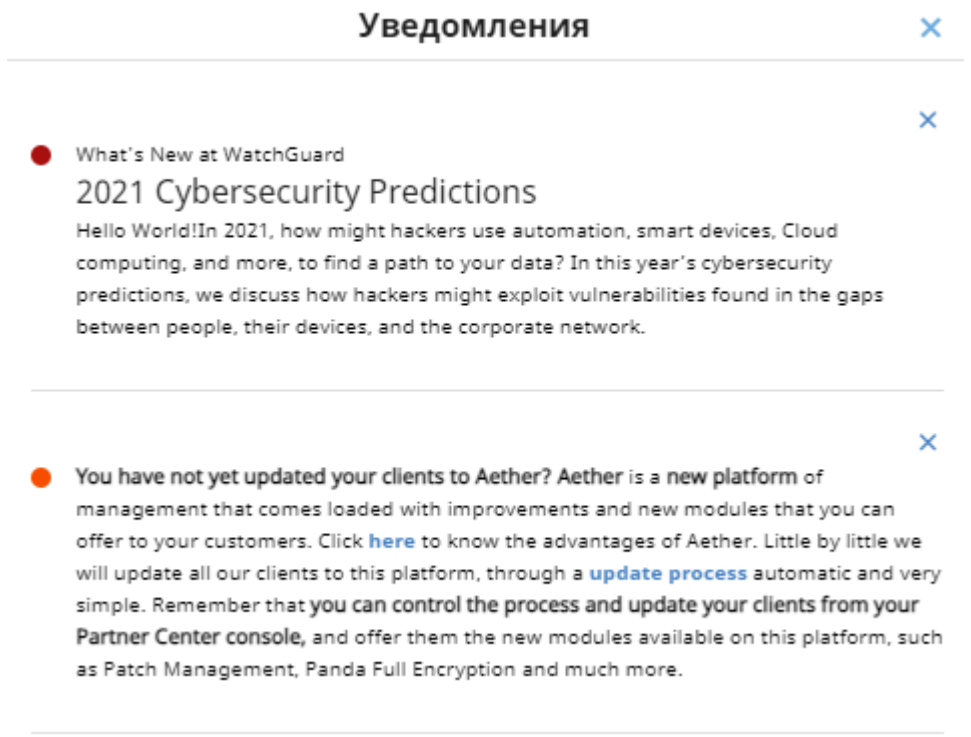
- Теперь у новых клиентов, если в разделе **Настройки** > **Рабочие станции и серверы** включена **Расширенная защита**, то режим работы **Анти-эксплойта** по умолчанию устанавливается в **Блокировка**
- Также у опции **Обнаруживать вредоносную активность (только для Linux)** по умолчанию теперь устанавливается режим **Блокировка**



Уведомления в веб-консоли

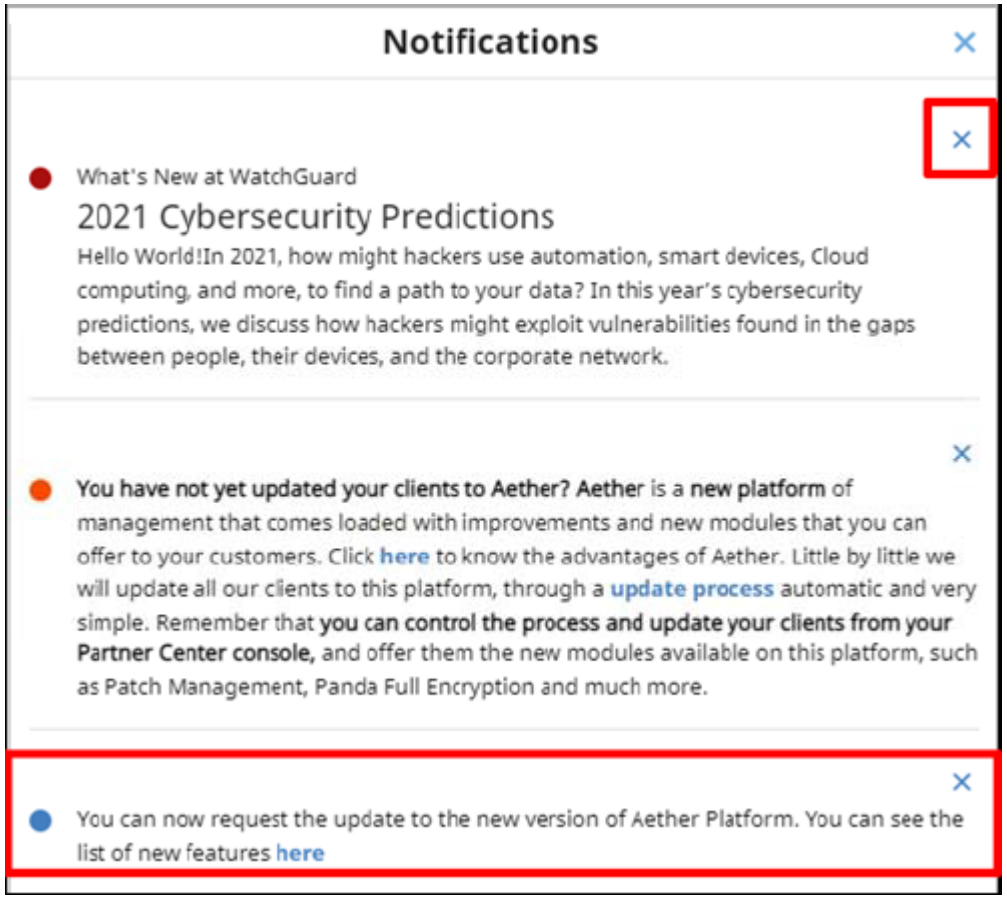
- В веб-консоли теперь могут публиковаться уведомления Panda Security, предназначенные для выборочных групп клиентов или пользователей определенных продуктов.

- Иконка уведомлений в виде звоночка показывается в панели инструментов в правом верхнем углу веб-консоли. В красном кружочке у этой иконке показывается количество новых уведомлений. При нажатии на иконку открывается окно со списком уведомлений



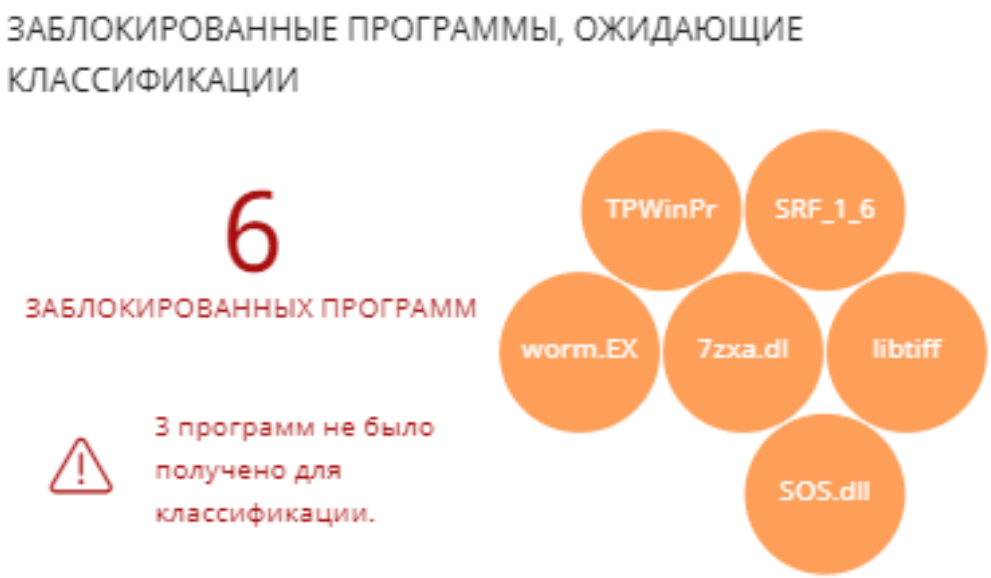
Уведомления по апгрейду продукта

- Когда доступна новая версия продукта, то в списке уведомлений показывается отдельное уведомление по апгрейду продукта.
  - Если пользователь веб-консоли обновит свою версию Aether, то все другие пользователи этого аккаунта (клиента) будут отключены от веб-консоли на период выполнения апгрейда



Заблокированные программы

- Если у Вас есть заблокированные программы, ожидающие классификации, то Вы можете удалить их из списка заблокированных программ в веб-консоли
  - Новый столбец Статус показывает файлы, которые не могут быть получены для классификации, и которые могут быть удалены из списка
  - Когда Вы удаляете программу из списка, это не влияет на уровень защиты
- Если программа запущена повторно, то она снова будет заблокирована
  - Когда файл поступит в Panda Security, он будет классифицирован сервисом Zero-Trust Application
- Список **История заблокированных программ** показывает также, какие программы были удалены из списка



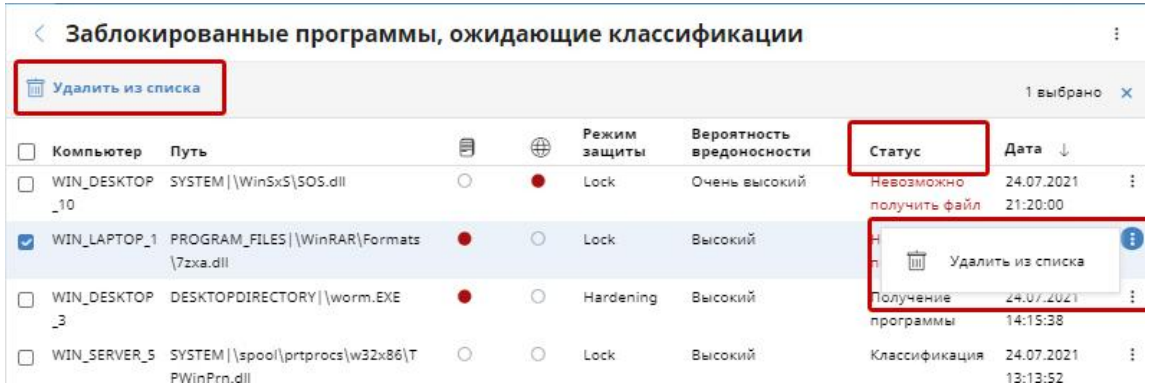
Удаление заблокированной программы из списка

- Чтобы удалить заблокированную программу из списка:

1. В разделе **Статус** > **Безопасность** нажмите на виджете **Заблокированные программы, ожидающие классификации**

2. В появившемся списке выберите программу, которую Вы хотите удалить

3. Нажмите кнопку **Удалить из списка** или в контекстном меню у данной программы выберите пункт **Удалить из списка**



Интеграция Windows 10 AMSI

- Новый релиз XII платформы Aether включает более глубокую интеграцию с Windows 10 AMSI (Antimalware Scan Interface)
- AMSI предоставляет:
  - Телеметрию и дополнительную информацию о выполнении скриптов и макросов
  - Больше контекстных сведений для повышения уровня защиты

Исключение модуля защиты Exchange

- Защита серверов Exchange перешла в режим End of Life, и теперь этот модуль исключен в аккаунтах новых клиентов
  - Обновленные аккаунты существующих клиентов пока еще видят модуль защиты Exchange и связанные с ним виджеты
  - Клиенты, у которых были настроены опции защиты Exchange до июля 2021, смогут ими пользоваться дальше до июня 2024 года

Спасибо!