



СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

DALLAS LOCK 8.0



СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

DALLAS LOCK LINUX

**ЭВОЛЮЦИЯ ЗАЩИТЫ КОНЕЧНЫХ ТОЧЕК
СОП. НОВЫЙ МОДУЛЬ В ПРОДУКТОВОЙ ЛИНЕЙКЕ**

ОБЗОР



КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

САНКТ – ПЕТЕРБУРГ, 2026



СОДЕРЖАНИЕ

Введение 1

Эволюция решений 2

Модуль COP в решениях Dallas Lock..... 2

Заключение 6



Размещаемая в данном документе информация предназначена для свободного ознакомления. Центр защиты информации ООО «Конфидент» оставляет за собой право вносить без уведомления любые изменения в данный документ, а также в ПО, которое описано в документе.

ВВЕДЕНИЕ Конечные точки (ПК, ноутбуки и серверы) обеспечивают доступ к корпоративной сети и бизнес-приложениям, являясь одним из основных векторов проникновения в инфраструктуру организации.

Базовые средства защиты, такие как спам-фильтры, антивирусы и брандмауэры, эффективно противостоят типовым и массовым угрозам. Однако при более сложных и целенаправленных атаках их возможностей может быть недостаточно. Для решения этой задачи ЦЗИ ООО «Конфидент» разработал модуль «Средство обнаружения и реагирования», который доступен в решениях Dallas Lock 8.0, Dallas Lock Linux и Едином центре управления (ЕЦУ) Dallas Lock.

ЭВОЛЮЦИЯ РЕШЕНИЙ

Антивирусы (AV) и платформы защиты конечных точек (EPP) обеспечивают проактивную защиту, используя сигнатуры, машинное обучение и дополнительные механизмы безопасности для предотвращения известных угроз. Однако при целевых атаках или уязвимостях нулевого дня такие решения могут оказаться недостаточно эффективными. Для выявления сложных угроз в реальном времени, анализа инцидентов и быстрого реагирования используется **Endpoint Detection and Response (EDR)**, или в терминах ФСТЭК России — **Средство обнаружения и реагирования (COP)**¹.

COP для Windows, Linux и отечественных ОС
Решения Dallas Lock 8.0 и Dallas Lock Linux стали еще эффективнее с добавлением модуля COP. Он помогает обнаруживать признаки взлома и атаки², анализировать угрозы и автоматически реагировать на инциденты, обеспечивая быструю и своевременную защиту от сложных атак.

МОДУЛЬ COP В РЕШЕНИЯХ DALLAS LOCK



1. Не является полной заменой антивирусного решения, а служит хорошим дополнением.
2. Функциональная возможность реализована и уже доступна для бета-тестирования, а также будет включена в следующие сертифицированные версии продуктов.

1. Выявление признаков взлома.

Решения Dallas Lock 8.0 и Dallas Lock Linux используют механизмы обнаружения индикаторов компрометации (IoC) — цифровых артефактов, свидетельствующих о несанкционированном доступе, которыми могут быть хэши файлов, IP-адреса и домены и т. д. COP работает с актуальными базами IoC.

2. Выявление признаков атаки³.

В Dallas Lock 8.0 и Dallas Lock Linux применяется механизм обнаружения индикаторов атаки (IoA) — правил, содержащих описание подозрительного поведения в системе, которое может быть признаком целевой атаки, например, необычный сетевой трафик или неожиданные соединения с известными вредоносными IP-адресами, аномальный доступ к файлам или изменения в критических файлах ОС, попытки эскалации привилегий и т.п. COP работает с актуальными наборами IoA, которые сгруппированы по тактикам матрицы MITRE ATT&CK.

3. Автоматическая локализация инцидента.

В Dallas Lock 8.0 и Dallas Lock Linux модуль COP гарантирует быстрое принятие решений с помощью правил автоматического реагирования. В зависимости от платформы и типа угрозы доступны различные действия для нейтрализации:

- **блокировка IP-адреса** — заблокирует IP-адрес атакующего.
- **блокировка учётной записи** — остановит выполнение вредоносных действий;
- **блокировка APM** — прервёт атаки на рабочей станции.
- **изоляция узла** — отключит скомпрометированное устройство от сети передачи данных;
- **завершение процесса** — завершит вредоносный или подозрительный процесс;
- **удаление файла³** — ликвидирует обнаруженный вредоносный объект;
- **запуск командного сценария³** — выполнит сложные, пользовательские сценарии реагирования;
- **выключение APM³** — позволит сохранить состояние APM для дальнейшего расследования инцидента.

В рамках одного правила реагирования можно использовать индикаторы только одного типа (IoA или IoC). Выбор типа индикаторов доступен перед созданием нового правила автоматического реагирования³.

За счет гибкости в настройке правил реагирования модуль адаптируется под различные сценарии угроз.

Новые возможности Dallas Lock 8.0 и Dallas Lock Linux:

- сканирование системы по запросу, по расписанию или централизованно через ЕЦУ Dallas Lock;
- управление базой IoC с возможностью добавления пользовательских индикаторов;
- регулярное обновление базы индикаторов.

При этом механизм обладает высокой производительностью и при пиковой нагрузке использует не более 30% системных ресурсов конечной точки.

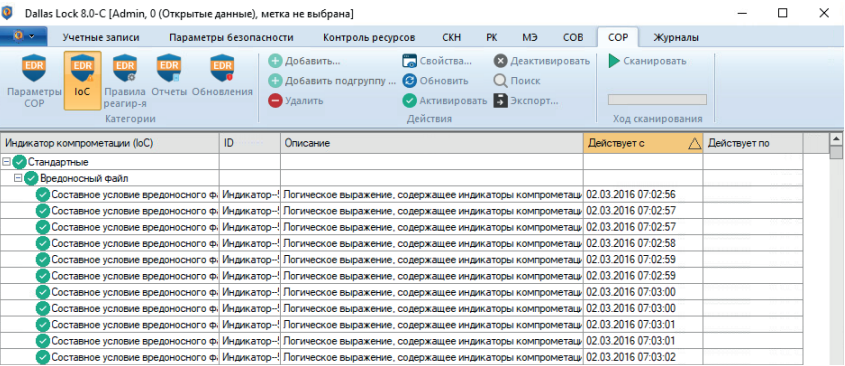


Рисунок 1. Dallas Lock 8.0. Модуль «Средство обнаружения и реагирования»

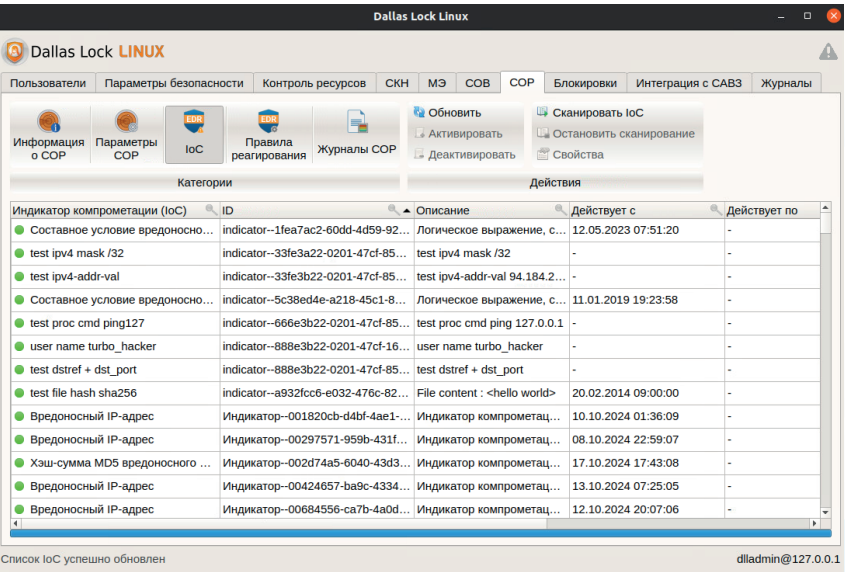


Рисунок 2. Dallas Lock Linux. Модуль «Средство обнаружения и реагирования»

3. Функциональная возможность реализована и уже доступна для бета-тестирования, а также будет включена в следующие сертифицированные версии продуктов.

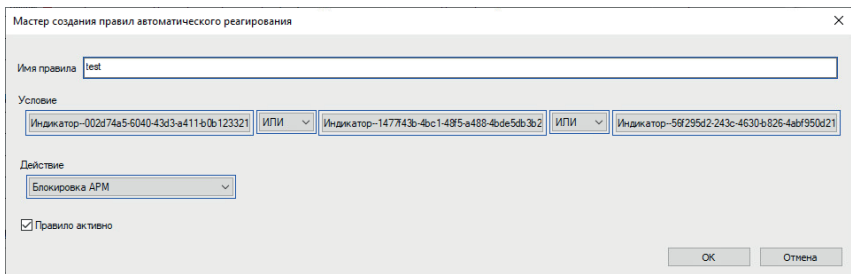


Рисунок 3. Dallas Lock 8.0. Мастер создания правил автоматического реагирования

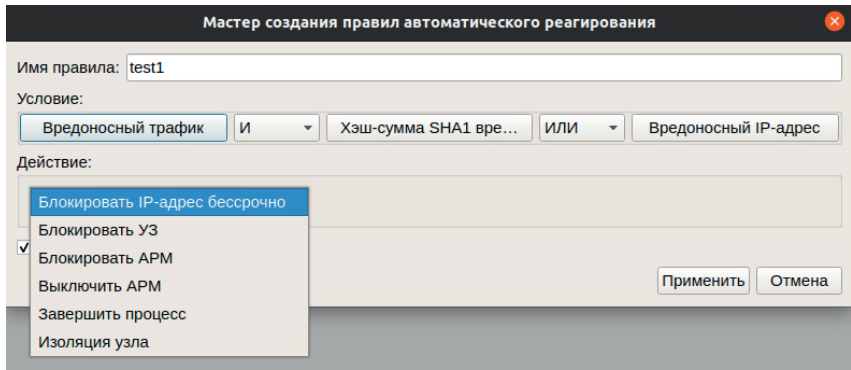


Рисунок 4. Dallas Lock Linux. Мастер создания правил автоматического реагирования

4. Централизованное управление.

В ЕЦУ Dallas Lock предусмотрено **централизованное управление модулем COP** для клиентов Dallas Lock 8.0 и Dallas Lock Linux. Это решение позволяет:

- редактировать параметры COP;
- просматривать информацию о событиях по сканированию систем на индикаторы компрометации с клиентов;
- управлять базой индикаторов компрометации (IoC), включая добавление пользовательских индикаторов;
- создавать правила автоматического реагирования для всего домена безопасности;
- запускать сканирование системы (по запросу или по расписанию);
- обновлять базу индикаторов компрометации.

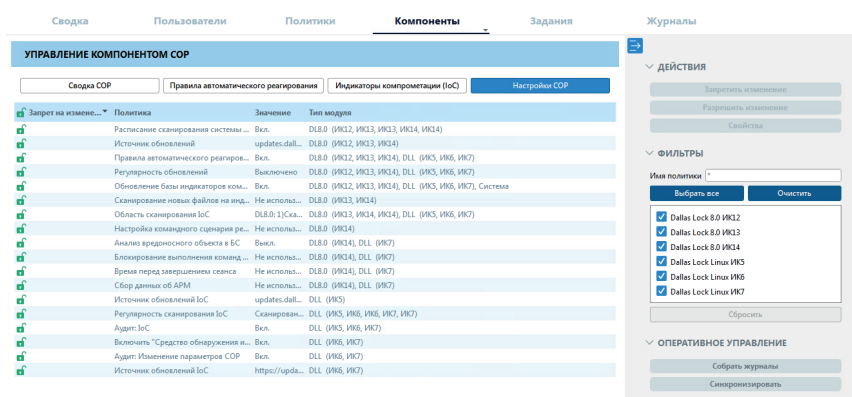


Рисунок 5. ЕЦУ Dallas Lock. Настройки «Средства обнаружения и реагирования»

ЗАКЛЮЧЕНИЕ

Мы продолжаем расширять перечень индикаторов компрометации (IoC) и индикаторов атаки (IoA), что позволит выявлять более сложные и целевые атаки. В будущем модуль COP дополнится новыми возможностями: анализом и расследованием инцидентов, а также визуализацией цепочек атак.

Продлевайте техническую поддержку, чтобы получать актуальные обновления и использовать все новые функции для защиты вашей инфраструктуры.







192029, г. Санкт-Петербург
пр. Обуховской Обороны, д. 51, лит. К
телефон/факс: (812) **325-1037**

<http://www.confident.ru/>
<http://www.dallaslock.ru/>
e-mail:

isc@confident.ru - коммерческие вопросы
helpdesk@confident.ru - техническая поддержка

Схема проезда:



www.confident.ru



www.dallaslock.ru



Telegram-канал

