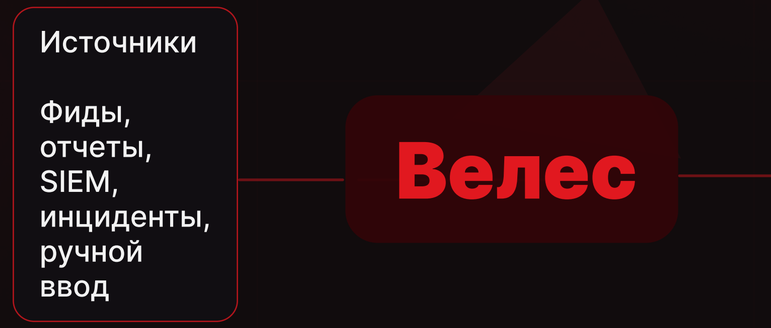
ВЕЛЕС

платформа кибербразведки и обмена индикаторами компрометации для SOC

Что такое Велес?

Велес — платформа
для централизованного хранения,
обработки и обмена данными
о киберугрозах, включая события, IoC,
атрибуцию, отчеты, фиды и сведения,
используемые командами SOC.



Ключевой принцип работы: аналитик управляет жизненным циклом знания об угрозе, а не набором разрозненных файлов.

Задачи, решаемые продуктом

Разрозненные источники

Индикаторы поступают из почты, отчетов, SIEM, внешних фидов и ручного ввода. При отсутствии единой модели данные сложнее сопоставлять, проверять и использовать в рабочих процессах SOC.

Ручная обработка

Аналитики вынуждены вручную выполнять нормализацию, проверку дубликатов, обогащение и передачу данных между инструментами.

Медленная реакция

При ручной обработке критичные IoC могут несвоевременно попадать в подключенные средства защиты и аналитические системы.

Велес объединяет разрозненные данные о киберугрозах в управляемый рабочий контур SOC.

Ключевые возможности

1 События и IoC

Хранение, поиск, связывание и управление жизненным циклом индикаторов компрометации.

2 Фиды и обмен

Подключение источников данных и контролируемое распространение индикаторов.

3 Отчеты

Формализация выводов аналитиков и привязка результатов анализа к событиям.

4 Таксономии

Единые классификаторы, уровни доверия, TLP-маркировка и правила категоризации данных.

5 API и интеграции

Интеграция с SOC-инструментами через REST API и форматы обмена STIX/TAXII при наличии соответствующих коннекторов.

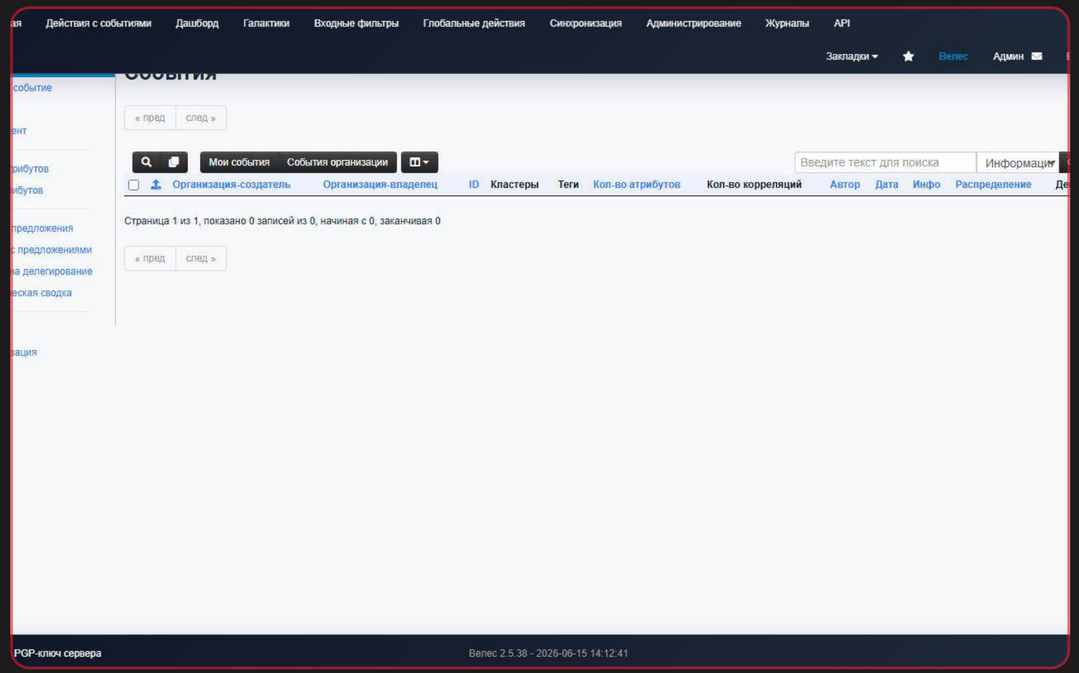
6 Аудит и права

Ролевое разграничение доступа, журналирование изменений и контроль действий пользователей.

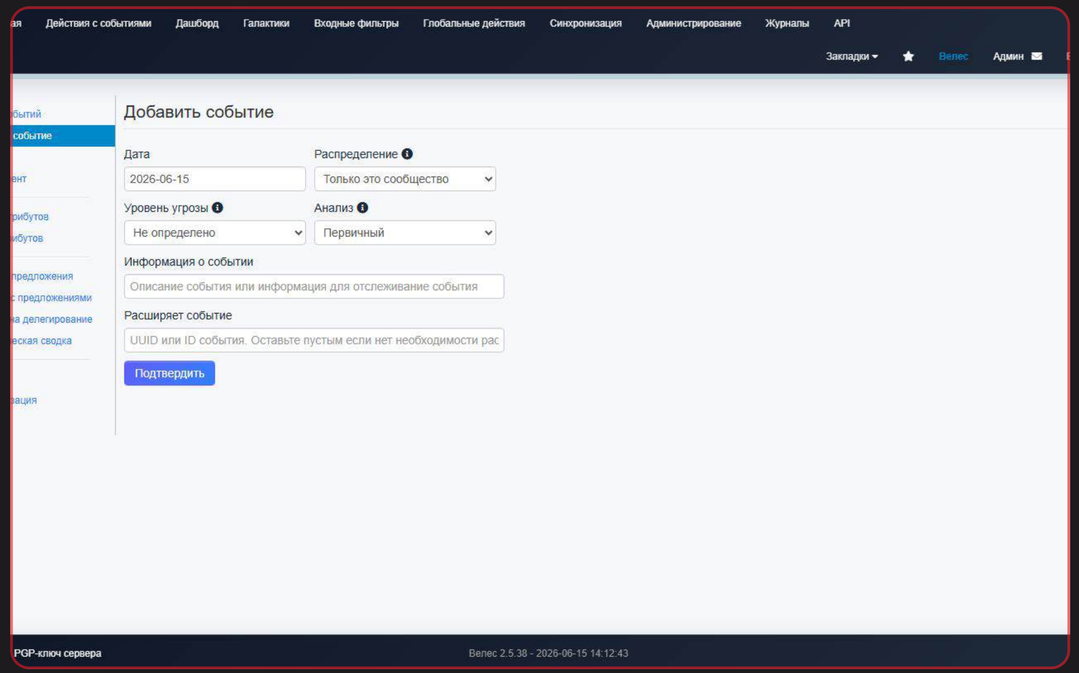
SURTE IT

Работа с событиями и создание IoC

Список событий



Создание IoC

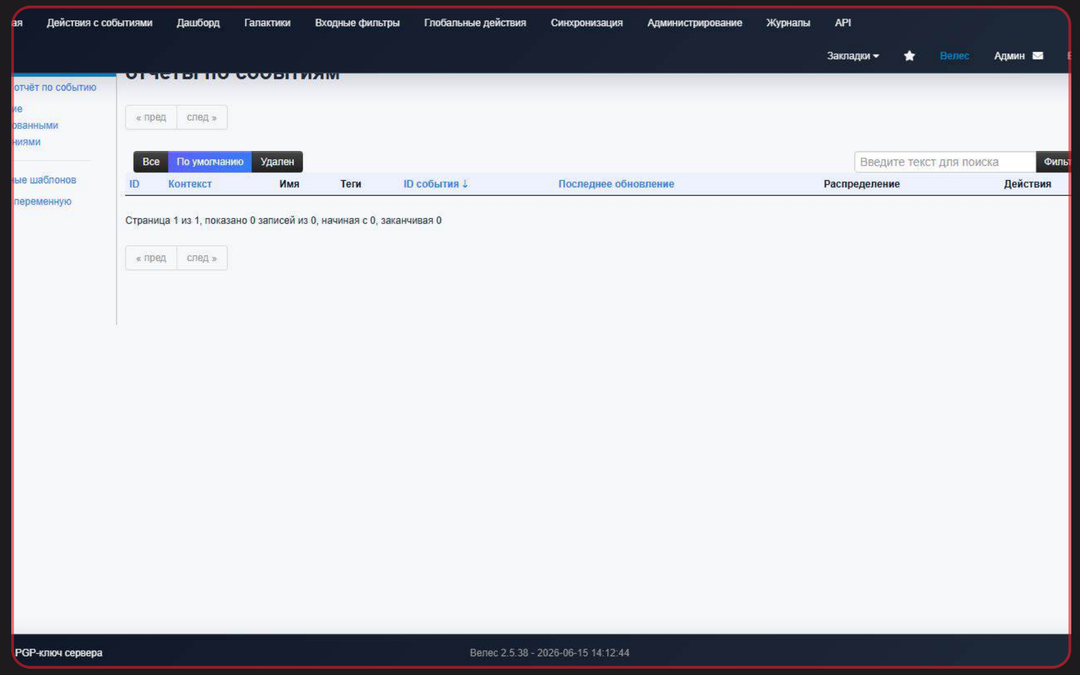


Платформа позволяет вести перечень событий, создавать IoC и связывать их с контекстом расследования.

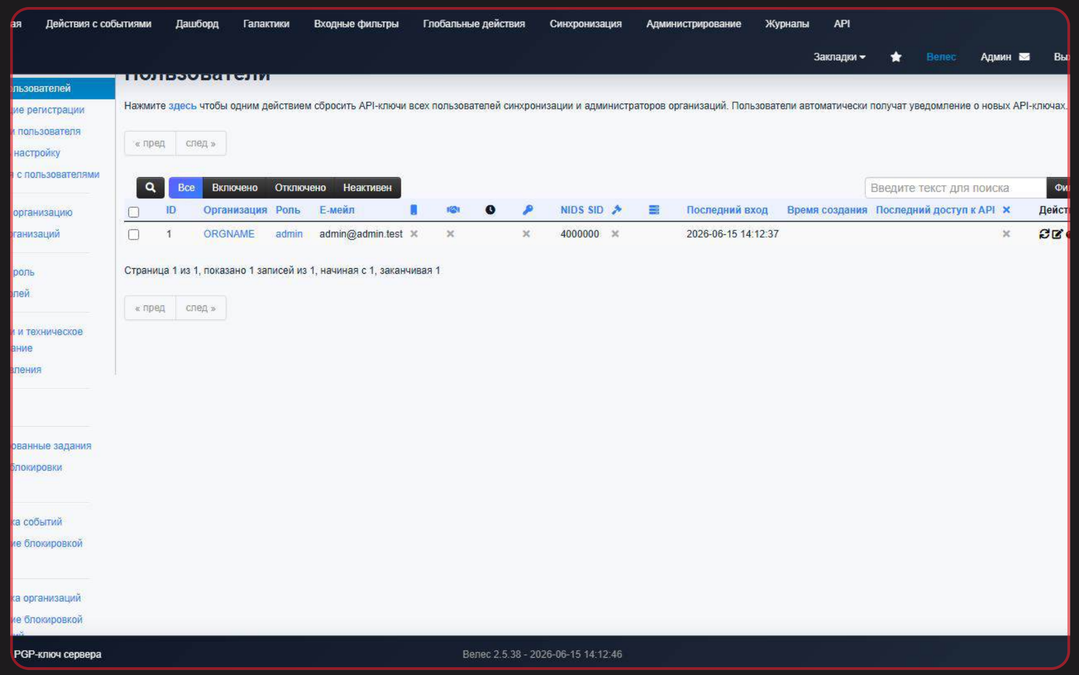
SURTE IT

Отчетность и администрирование

Отчеты по событиям



Управление пользователями

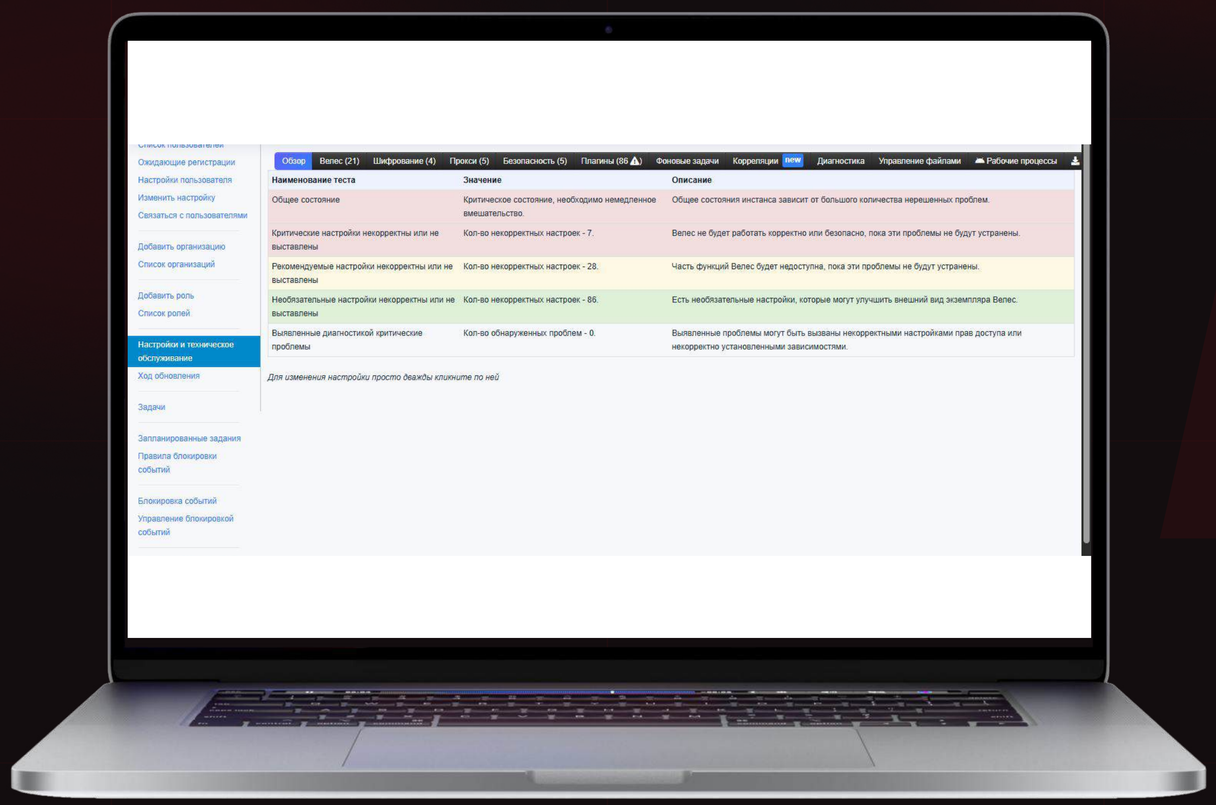


Разделы отчетности и администрирования обеспечивают оформление результатов анализа, управление пользователями и контроль доступа.

SURTE IT

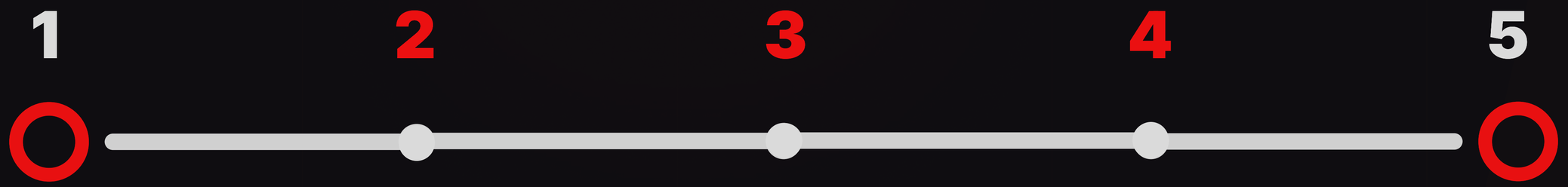
Администрирование сервера

Раздел администрирования сервера предназначен для контроля состояния системы, диагностики, управления фоновыми задачами, плагинами, параметрами безопасности и серверными настройками.



Процесс обработки данных

От поступления данных до передачи в подключенные средства защиты и аналитические процессы.



Сбор

Получение данных из фидов, отчетов, инцидентов и ручного ввода.

Нормализация

Приведение событий, атрибутов и меток к единому формату.

Корреляция

Установление связей между IoC, кампаниями, инцидентами и объектами.

Обогащение

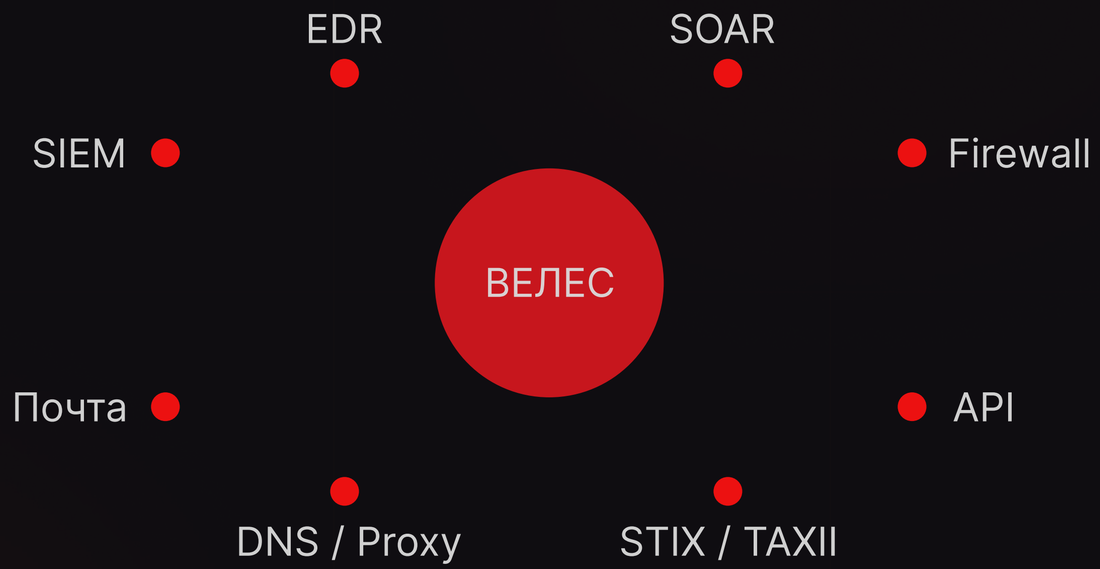
Добавление контекста, уровня доверия, критичности и TLP-маркировки.

Распространение

Передача данных в SOC, SIEM, SOAR, EDR и отчетные материалы.

Интеграции

Велес используется как центральный узел обмена между источниками данных, аналитиками SOC и подключенными средствами защиты.



Сценарии применения платформы Велес

Корпоративный SOC

Централизованный репозиторий IoC, обмен данными между сменами, привязка индикаторов к инцидентам и отчетным материалам.

Финансовый сектор

Мониторинг фишинговых ресурсов, мошеннических доменов, вредоносной инфраструктуры и цепочек атак.

Промышленность

Работа в локальных контурах, контролируемое распространение индикаторов и обработка данных из закрытых источников.

MSSP / интегратор

Управляемый обмен данными с несколькими заказчиками, сегментация информации и применение единой методики обработки индикаторов.

Велес поддерживает разные роли в рабочем процессе: аналитик работает с содержанием, руководитель контролирует процесс и отчетность, интегратор управляет обменом данными.

Спасибо!

surte.by vz@surte.by +375 (29) 114 81 69