udv|group

UDV SIEM

Система сбора и корреляции
событий безопасности

UDV Group — ведущий разработчик в области кибербезопасности

UDV Group предоставляет единый портфель решений для защиты технологических сетей, корпоративного сегмента и автоматизации в области объектовой безопасности:

- защита АСУ ТП и объектов КИИ
- мониторинг инфраструктуры
- реагирование на инциденты ИБ
- автоматизация работы SOC
- выполнение требований регуляторов

200+

Разработчиков в штате

Распределённая команда
со штаб-квартирой в Екатеринбурге

1000+

Инсталляций

Проекты по защите АСУ ТП
и корпоративных сетей

10+

Патентов

Собственный исследовательский
центр в области кибербезопасности

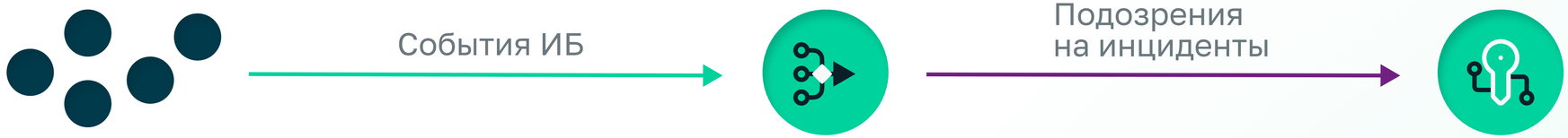
10

Лет на рынке

Подтвержденный опыт интеграции
в крупных предприятиях
нефтегазовой отрасли, энергетики,
металлургии и других

Техническая инфраструктура SOC

Назначение UDV SIEM



СЗИ и другие источники событий

- События от различных СЗИ, включая хостовые и сетевые средства
- Логи событий инфраструктурного уровня

UDV SIEM

- Мониторинг и управление событиями ИБ в режиме реального времени
- Сбор и корреляция событий безопасности
- Долгосрочное хранение событий для анализа

UDV SOAR

- Обогащение данных о возможных инцидентах
- Автоматизация процесса реагирования
- Плейбуки и скрипты автоматического реагирования
- Оценка последствий инцидентов
- База знаний и рекомендации по реагированию
- Контроль SLA и отчетность

Поддерживаемые источники в UDV SIEM

Поддерживаются любые источники данных по протоколу Syslog.

> 350

систем-источников

У агента имеются универсальные транспорты, позволяющие собирать события с:

- Windows event log (любые журналы)
- Checkpoint LEA
- Cisco SDEE
- File logs
- Logs on ftp servers
- WMI logs
- Hash logs
- Logs on MySQL/Oracle/ MS SQL таблицах и представлениях
- Информация об установленном ПО и патчах
- Информация об открытых процессах и портах

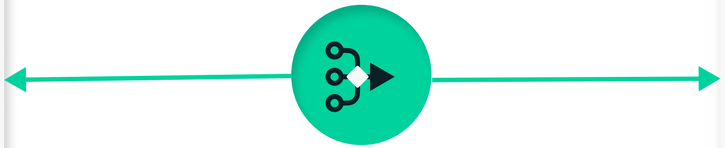
Гарантированная обработка всех событий

Микросервисная архитектура с применением очередей сообщений (MQ) для гарантированной доставки и обработки всех поступающих событий при любой нагрузке и в случае сбоев

Высокая производительность UDV SIEM

Корреляция событий безопасности

- Более 400 готовых правил корреляции
- Дополнительный пакет экспертизы для выявления инцидентов в промышленных сетях
- Автоматическое создание кратких описаний событий и назначение веса (приоритета) каждого события
- Лёгкое создание собственных пользовательских правил корреляции в интерфейсе SIEM-системы



UDV SIEM

Применение параллельных вычислений для достижения максимальной производительности

Сохранение событий в базе даных

- Применение специализированных СУБД для сжатого хранения данных и быстрого доступа к данным
- Оптимизация ресурсов хранилища в зависимости от важности событий
- Гибкие возможности по географически распределённому хранению данных
- Удобный поиск событий по ключевым словам и критичности, не прибегая к сложным запросам

Сохранение событий в базе данных UDV SIEM

- Предупреждения
- Дашборды
- Журнал событий
- Отчеты
- Мониторинг

Интеграция с UDV SOAR / UDV IRP Lite

Автоматическая передача инцидентов
(подозрений на инциденты)
из UDV SIEM в UDV IRP Lite

При закрытии инцидента в UDV IRP Lite он
автоматически закрывается в UDV SIEM

Преимущества UDV SIEM

Мониторинг событий в реальном времени

- UDV SIEM позволяет проводить сбор, нормализацию, корреляцию и сохранение событий информационной безопасности в реальном времени, что позволяет оперативно реагировать на возможные угрозы безопасности.
- В системе предусмотрена 100%-защита от потерь данных при пиковых нагрузках и возможных сбоях, поэтому обеспечивается гарантированная обработка всех поступающих событий.
- Архитектура системы оптимизирована для применения в распределённых инфраструктурах.

Правила корреляции для промышленных сетей

- UDV SIEM содержит множество преднастроенных правил корреляции событий информационной безопасности, каждое из которых может быть изменено пользователем по своему усмотрению.
- Благодаря многолетней экспертизе в защите АСУ ТП в UDV SIEM добавлены правила корреляции, специфичные для промышленных (технологических) сетей. Они позволяют оперативно выявлять в том числе инциденты информационной безопасности в АСУ ТП.

Преимущества UDV SIEM

Автоматическое выставление тегов для событий

Для удобства пользователя все события из большого количества разнородных источников помечаются специальными тэгами с весовыми коэффициентами. Это позволяет быстро ориентироваться в потоке событий, получая их краткие описания и совокупный вес (приоритет) каждого события.

Использование тэгов позволяет искать события по ключевым словам и критичности, не прибегая к сложным запросам с применением специфичных для источников событий технических параметров.

Интеграция с другими системами ИБ

UDV SIEM интегрируется с другими системами, что позволяет обеспечить более эффективное управление информационной безопасностью предприятия.

Поддерживается возможность получать события из сотен разнотипных источников (log-файлы, события от серверов, рабочих станций, приложений, а также других сторонних решений).

На выходе формируется информация об инцидентах информационной безопасности, которая может передаваться в SOAR/IRP для обработки (реагирования) с последующим автоматическим закрытием инцидента в SIEM.

udv|group

Спасибо!

Закажите пилотный проект или персональную демонстрацию наших решений

Контакты

commercial@udv.group
8-800-511-65-51

Адрес

620100, г. Екатеринбург,
ул. Сибирский тракт, 12,
строение 7, этаж 4

Сайт

udv.group

Telegram

@udv_group