UDV SIEM

Система сбора и корреляции
событий безопасности

РОССИЙСКИЙ РАЗРАБОТЧИК РЕШЕНИЙ ДЛЯ КОМПЛЕКСНОЙ КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

udv|group

РОССИЙСКИЙ РАЗРАБОТЧИК РЕШЕНИЙ ДЛЯ КОМПЛЕКСНОЙ КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

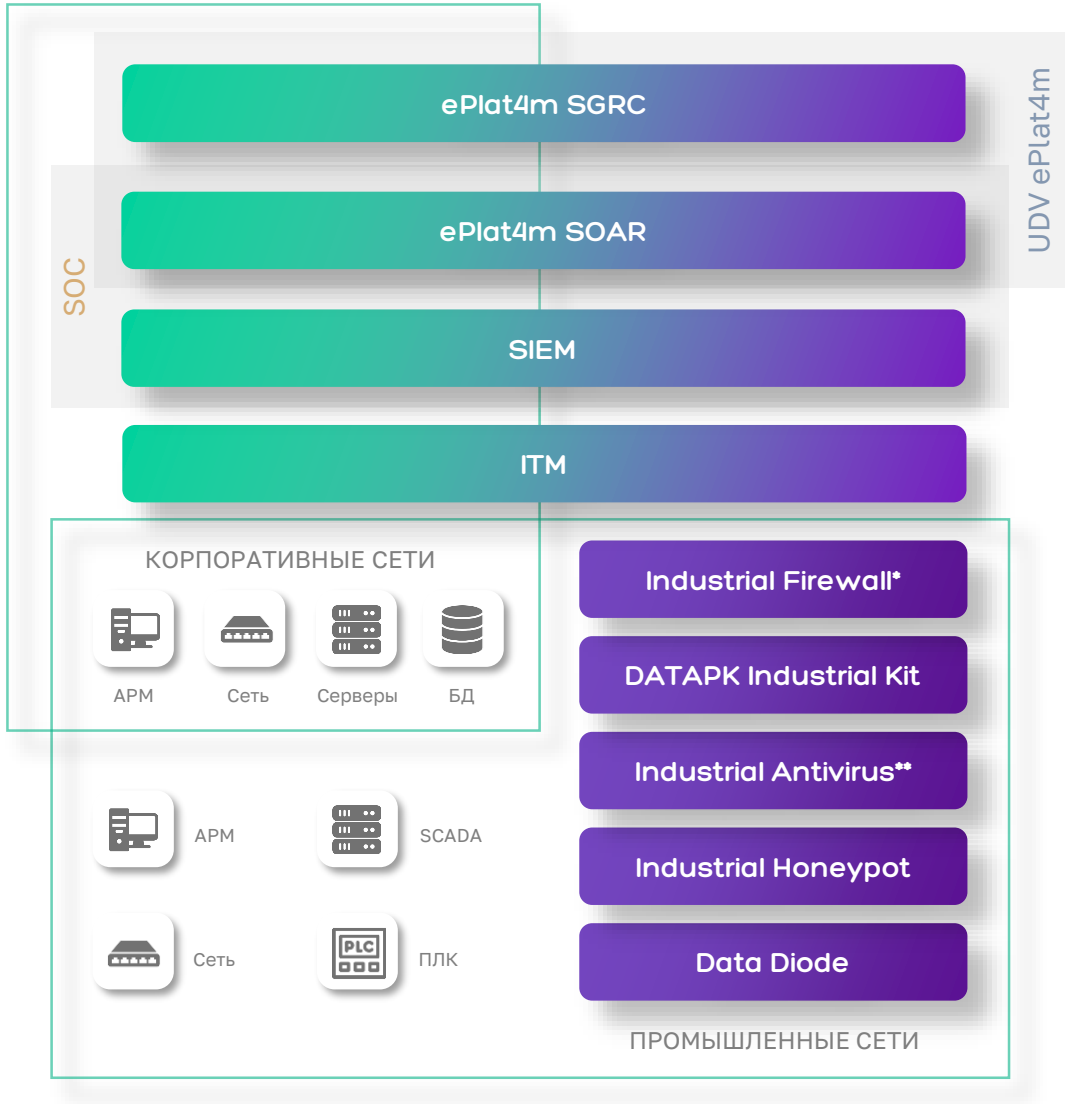
БОЛЕЕ 10 ЛЕТ ЭКСПЕРТИЗЫ ИБ АСУ ТП

КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

СОБСТВЕННЫЙ R&D И ЛАБОРАТОРИЯ КИБЕРБЕЗОПАСНОСТИ

ДЕЛОВЫЕ И ТЕХНОЛОГИЧЕСКИЕ ПАРТНЁРЫ

Экосистема решений UDV Group

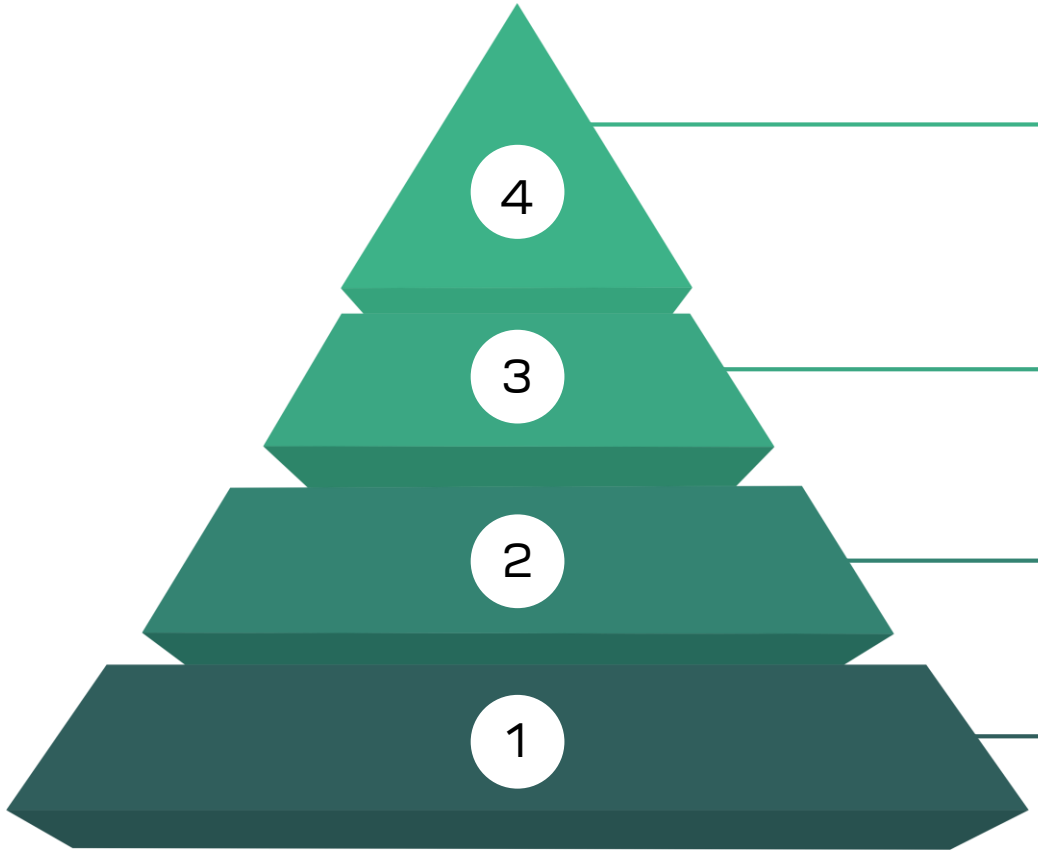


- Защита АСУ ТП и объектов КИИ
- Мониторинг ИБ и реагирование на инциденты
- Автоматизация бизнес-процессов по ИБ

* Включено в дорожную карту развития продуктовой линейки на 2023 год. ** Партнёрское решение.

udv|group

Техническая инфраструктура SOC



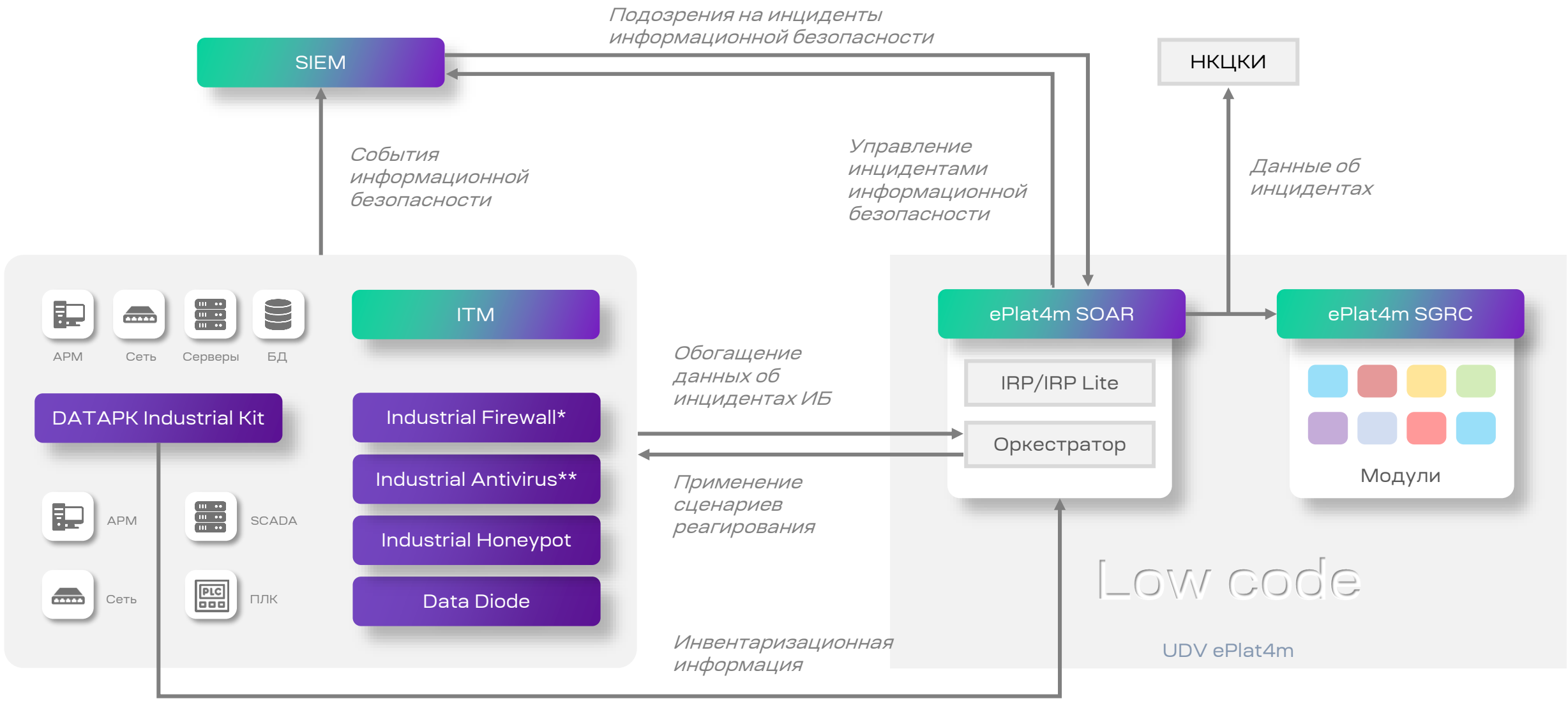
УРОВЕНЬ УПРАВЛЕНИЯ
UDV ePlat4m SOAR

УРОВЕНЬ АГРЕГАЦИИ
SIEM

ИНСТРУМЕНТАЛЬНЫЙ УРОВЕНЬ
Антивирусная защита, МЭ, WAF, СЗИ от НСД, IDS/IPS, СКЗИ, DLP, anti-DDoS и т.д.

ИНФРАСТРУКТУРНЫЙ УРОВЕНЬ
Серверное оборудование, сетевое оборудование, АРМ, ОС, СПО, ППО и т.д.

Экосистема решений UDV Group



* Включено в дорожную карту развития продуктовой линейки на 2023 год. ** Партнёрское решение.

udv|group

Назначение UDV SIEM

Источники событий

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

События

UDV SIEM

- мониторинг и управление событиями ИБ в режиме реального времени;
- сбор и корреляция событий безопасности;
- долгосрочное хранение событий для анализа.

Подозрения на инциденты

UDV ePlat4m 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

> 350
систем-
источников

Поддерживаются любые источники данных по протоколу Syslog.

У агента имеются универсальные транспорты, позволяющие собирать события с:

- Windows event log (любые журналы)
- Checkpoint LEA
- Cisco SDEE
- File logs
- Logs on ftp servers
- Hash logs (запущенные процессы их sha1/md5/sha256)
- Logs on Mysql/Oracle/MS SQL таблицах и представлениях
- WMI logs
- Информация об установленном ПО и патчах
- Информация об открытых процессах портах

UDV SIEM

Гарантированная обработка всех событий

Поддерживаются любые источники данных по протоколу Syslog.

У агента имеются универсальные транспорты, позволяющие собирать события с:

- Windows event log (любые журналы)
- Checkpoint LEA
- Cisco SDEE
- File logs
- Logs on ftp servers
- Hash logs (запущенные процессы их sha1/md5/sha256)
- Logs on Mysql/Oracle/MS SQL таблицах и представлениях
- WMI logs
- Информация об установленном ПО и патчах
- Информация об открытых процессах портах

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

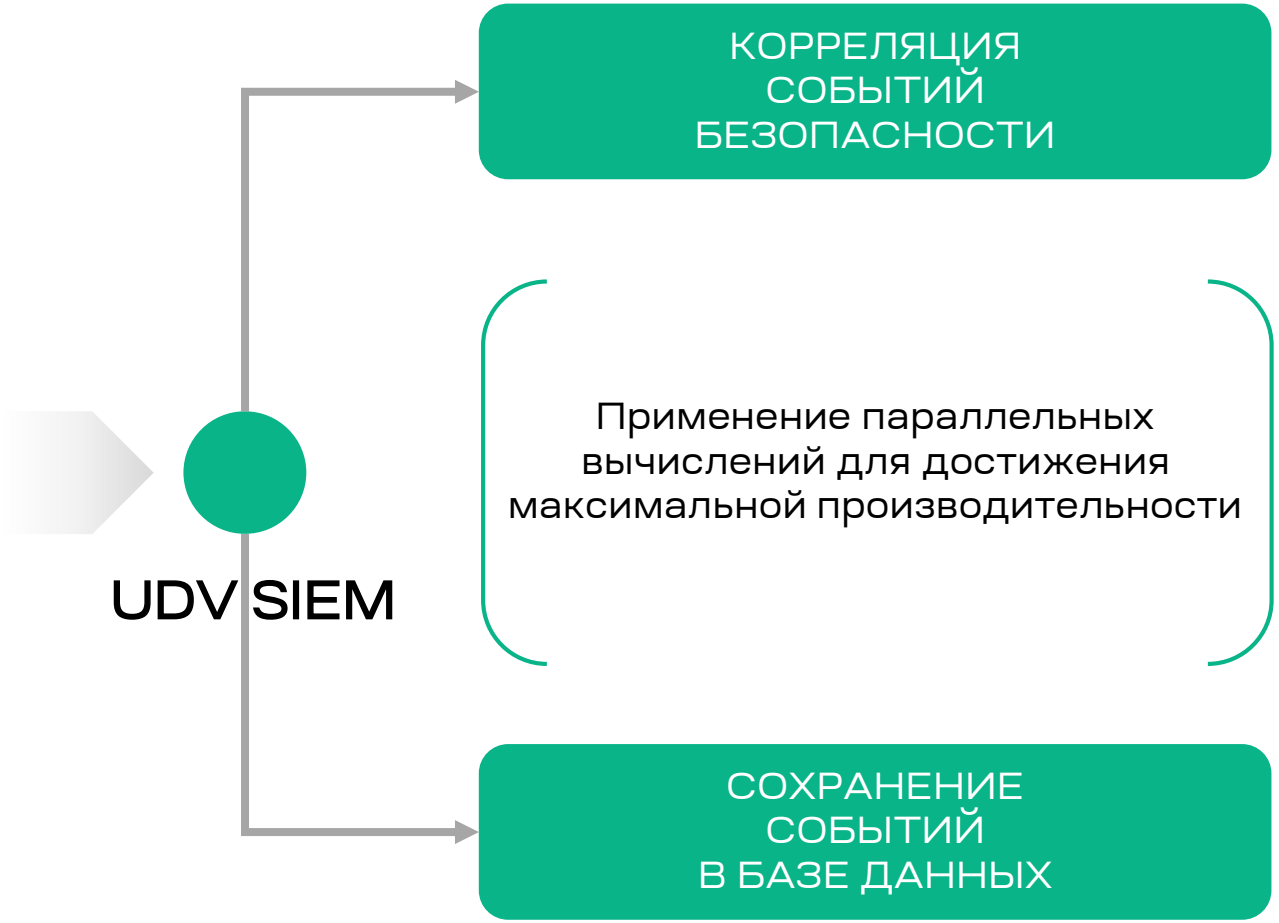
UDV SIEM

Высокая производительность UDV SIEM

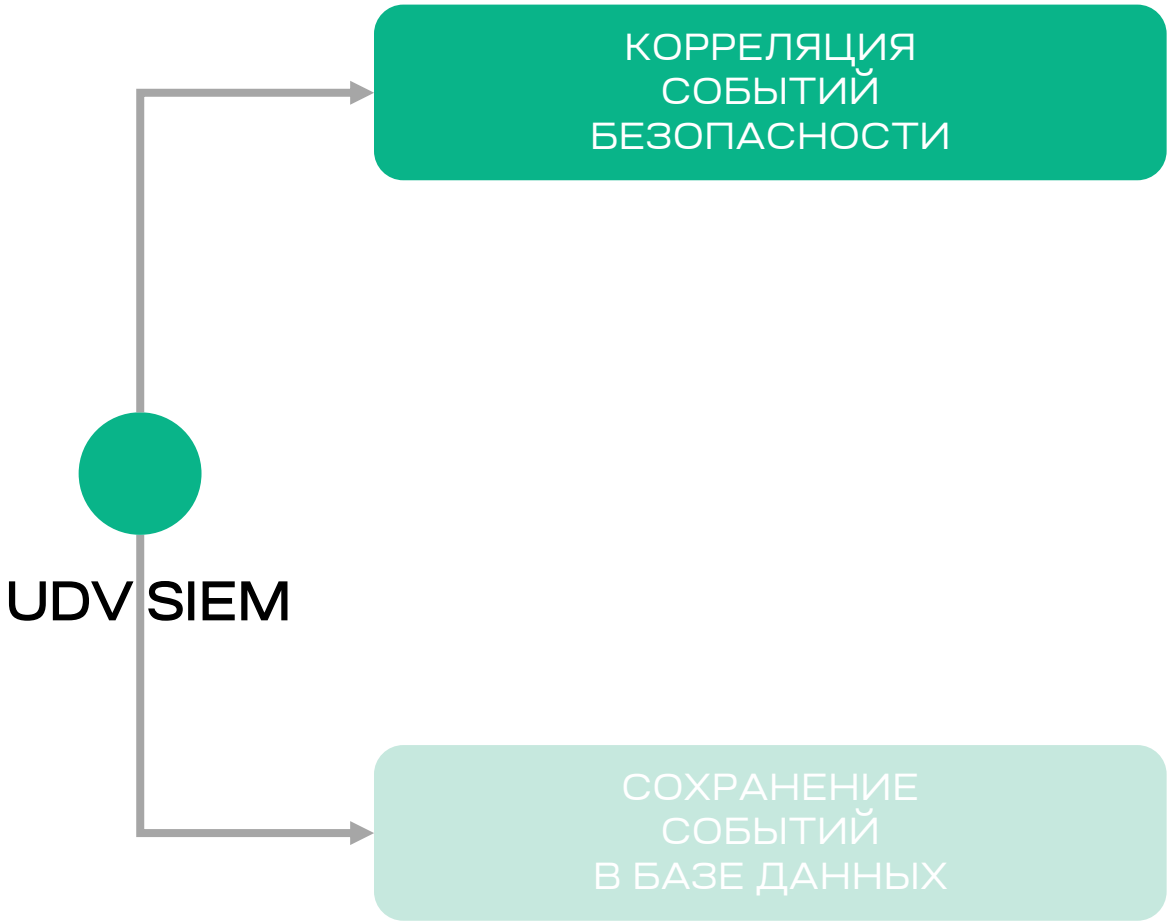
Поддерживаются любые источники данных по протоколу Syslog.

У агента имеются универсальные транспорты, позволяющие собирать события с:

- Windows event log (любые журналы)
- Checkpoint LEA
- Cisco SDEE
- File logs
- Logs on ftp servers
- Hash logs (запущенные процессы их sha1/md5/sha256)
- Logs on Mysql/Oracle/MS SQL таблицах и представлениях
- WMI logs
- Информация об установленном ПО и патчах
- Информация об открытых процессах портах

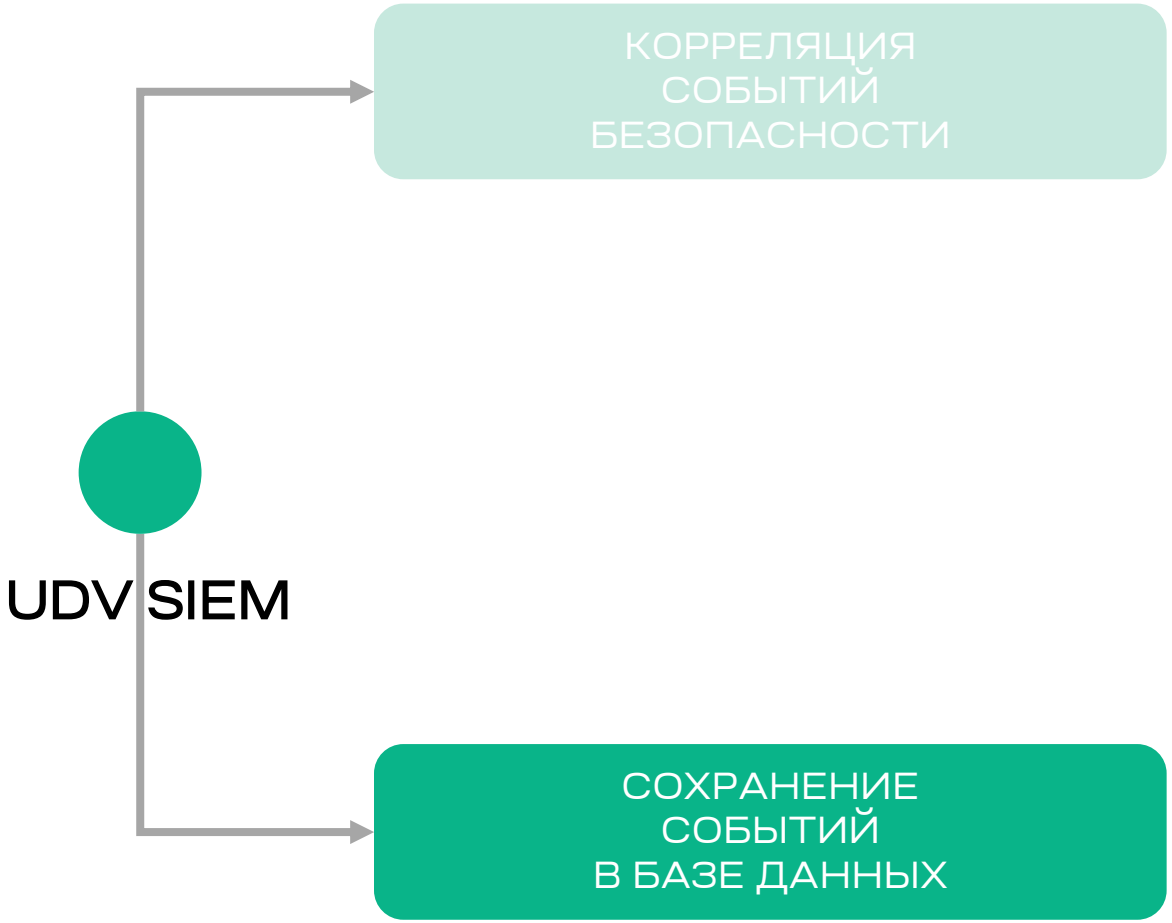


Корреляция событий безопасности в UDV SIEM



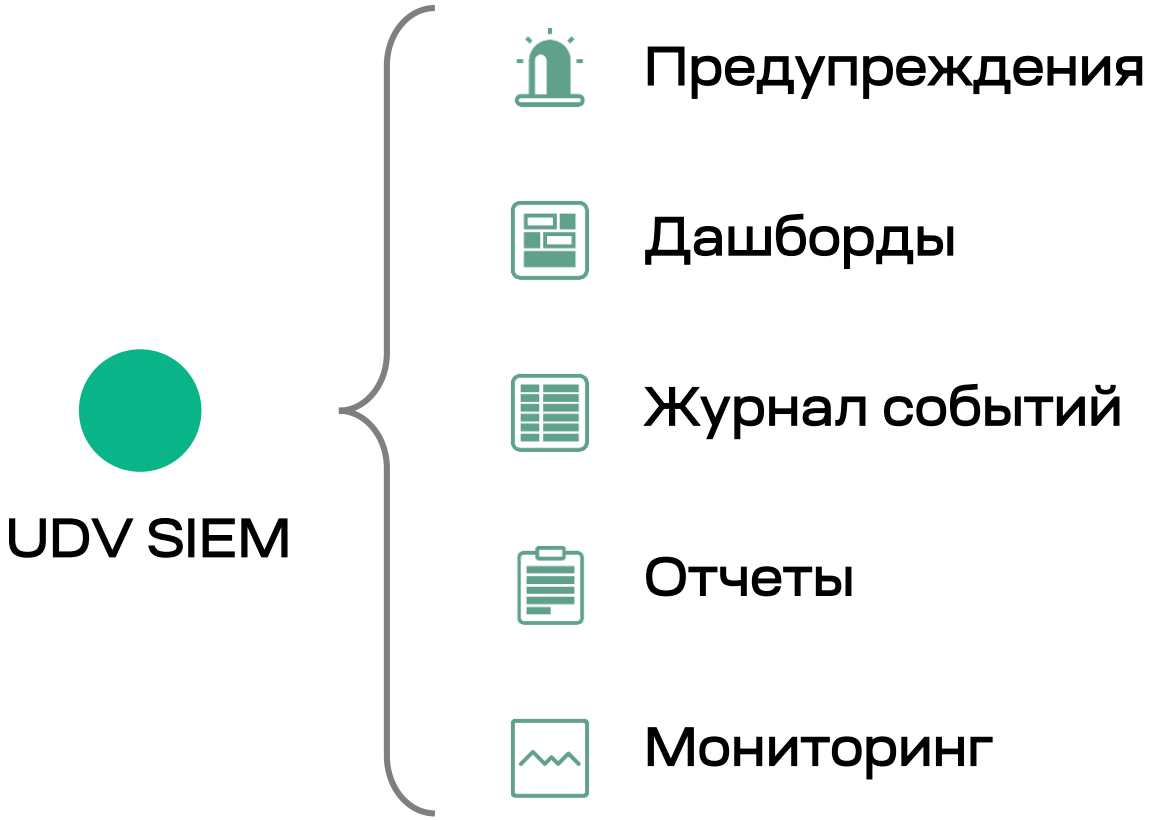
- Более 400 готовых правил корреляции
- Дополнительный пакет экспертизы для выявления инцидентов в промышленных сетях
- Автоматическое создание кратких описаний событий на человеко-понятном языке и назначение веса (приоритета) каждого события
- Лёгкое создание собственных пользовательских правил корреляции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

Сохранение событий в базе данных UDV SIEM



- 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



Интеграция с UDV ePlat4m SOAR / UDV ePlat4m IRP Lite

Автоматическая передача инцидентов (подозрений на инциденты) из UDV SIEM в UDV ePlat4m IRP Lite

При закрытии инцидента в UDV ePlat4m IRP Lite он автоматически закрывается в UDV SIEM

Преимущества UDV SIEM

- Мониторинг событий в реальном времени
- Правила корреляции для промышленных сетей
- Автоматическое выставление тэгов для событий
- Интеграция с другими системами ИБ

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.

Преимущества UDV SIEM

- Мониторинг событий в реальном времени
- **Правила корреляции для промышленных сетей**
- Автоматическое выставление тэгов для событий
- Интеграция с другими системами ИБ

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

- Мониторинг событий в реальном времени
- Правила корреляции для промышленных сетей
- **Автоматическое выставление тэгов для событий**
- Интеграция с другими системами ИБ

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 на человеко-понятном языке и совокупный вес (приоритет) каждого события. Использование тэгов позволяет делать поиск событий по ключевым словам и критичности, не прибегая к сложным запросам с применением специфичных для источников событий технических параметров.

Преимущества UDV SIEM

- Мониторинг событий в реальном времени
- Правила корреляции для промышленных сетей
- Автоматическое выставление тэгов для событий
- 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, рабочий 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 ЗА ВНИМАНИЕ!

Закажите пилотный проект или персональную демонстрацию наших решений

commercial@udv.group

8-800-511-6551

udv.group