UDV SIEM

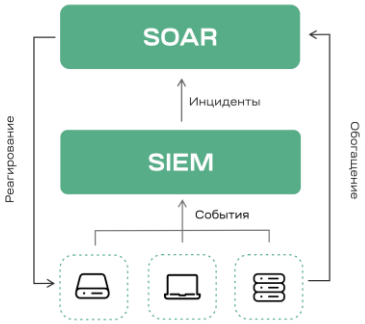
Система сбора и корреляции событий безопасности

UDV SIEM осуществляет мониторинг и управление событиями ИБ в режиме реального времени. Реализует сбор и корреляцию событий безопасности.

РЕШАЕМЫЕ ЗАДАЧИ

- Мониторинг, сбор и корреляция событий безопасности в реальном времени.
- Отображение и поиск данных о событиях компьютерной безопасности.
- Долгосрочное хранение событий для ретроспективного анализа.

ВОЗМОЖНОСТИ



- **Анализ и мониторинг безопасности распределённой ИТ-инфраструктуры предприятия**. Система оповещает о событиях безопасности в режиме реального времени. Производит обнаружение угроз и инцидентов информационной безопасности.
- **Продвинутый пакет экспертизы «из коробки» и интеграция с другими ИБ-решениями.** Более 400 готовых правил корреляции, а также дополнительный пакет экспертизы для выявления инцидентов в промышленных сетях. Поддержка более 350 систем-источников.
- **Визуализация данных и построение отчетов.** Система имеет интуитивно понятный интерфейс, в котором содержится более 75 предустановленных шаблонов отчетов, а также удобные дашборды с индикацией предупреждений.

ПРЕИМУЩЕСТВА

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.

Автоматическое выставление тэгов 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 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.

Интеграция с другими системами информационной безопасности

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 UDV ePlat4m SOAR или UDV ePlat4m IRP Lite для обработки (реагирования) с последующим автоматическим закрытием инцидента в UDV SIEM.

Закажите пилотный проект или персональную демонстрацию решения: commercial@udv.group

udv group