Системы
Информационной
Безопасности

Log Management & SIEM

Управление событиями и инцидентами ИБ

Log Management & SIEM

Системы Информационной Безопасности

Подразделение информационной безопасности в современной организации невозможно представить без тщательно настроенной системы оповещения об инцидентах, уязвимых точках инфраструктуры и сети, подозрительной активности как на сетевом периметре, так и на внутренних ресурсах, базах данных и бизнес приложениях.

Процессы и технические средства обработки и реакции на события безопасности являются важнейшим компонентом системы информационной безопасности.

Место SIEM в инфраструктуре организации

Системы Информационной Безопасности

Инфраструктура

Сетевое оборудование
- маршрутизаторы
- коммутаторы

Серверы
- СПО
- гипервизоры
- ОС
- ППП

АРМы
- СПО
- ППП
- ОС

сенсоры SIEM-систем

МЭ

СОВ (IDS)

DLP

антивирусы

МДЗ

криптошлюзы

сканеры защищенности

сенсоры SIEM-системы

Средства защиты информации

АРМ ИБ, ситуационный центр (SOC)

Консоль управления

SIEM

Системы Информационной Безопасности

Наше решение
как работает?

- Определим критичные узлы инфраструктуры, полезные источники журналов и модель киберугроз для организации.
- Разработаем единые требования к наличию и формату журналов аудита
- Выберем и внедрим необходимые технические средства для сбора, нормализации и корреляции логов.
- Построим процессы обработки и реакции на события безопасности.
- Внедрим простую и прозрачную систему оперативной отчетности для подразделения ИБ и бизнес-отчетности для руководителей.

Log Management & SIEM
– что дает?

Системы Информационной Безопасности

- Сбор и агрегация журналов аудита.
- Корреляция событий безопасности с различных средств защиты, автоматизированное выявление инцидентов, снижение количества ложноположительных срабатываний.
- Защищенное хранение исторических данных для расследования инцидентов ИБ.
- Обнаружение проблем в функционировании инфраструктуры и корпоративной сети.
- Внедрение и настройка систем журналирования во всех критичных узлах инфраструктуры.
- Антифрод, выявление подозрительной активности в финансовых и бизнес-системах.
- Проактивное устранение уязвимостей и предотвращение инцидентов.
- Визуализация текущего состояния информационной безопасности организации
- Снижение операционных расходов

Наше решение
– как начать?

Системы
Информационной
Безопасности

- Подписать NDA.
- Заполнить анкету по подбору SIEM.
- Прислать данные нам на почту.

Системы
Информационной
Безопасности

Как с нами связаться?

+7 495 766-05-38
info@is-systems.org