ЭЛЕКТРОННОЕ ОБЛАКО

CLOUSERVER.RU

SIEM

Мониторинг информационной безопасности

Наш опыт

- 15 лет в сфере IT безопасности
- Ключевые клиенты - авиа, торговые, финансовые, юридические компании, научные центры
- Построение и поддержка облачных сервисов на более чем 10000 рабочих мест

Наша команда

- CEH - Certified Ethical Hacker
- PT - Licensed Penetration Tester Master
- ESCA - Certified Security Analyst
- CHFI - Forensic Investigator
- CCISO – Security Officer

Наши услуги

- Пентест
- Аудит безопасности
- Защита от dos и ddos атак
- SIEM (комплексные решения по мониторингу)
- Обучение персонала
- Построение защищенной инфраструктуры

Основные компоненты SIEM

- Единый интерфейс управления
- Система сбора событий безопасности
- Система анализа происходящего
- Сканер безопасноси
- Квалифицированный персонал

Единый интерфейс управления мониторингом

- Система вывода информации на широкоэкранные мониторы
- Визуализация угроз
- Отображение событий в реальном времени
- Наглядные отчеты по инцидентам

Система сбора событий безопасности

- Получает информацию с сотен датчиков
- Обрабатывает тысячи параметров
- Производит предварительный анализ информации
- Сохраняет в базу данных все подозрительные события

Система анализа событий безопасности

- Обнаружение атак в реальном времени
- Анализирует потенциальные угрозы на основании базы знаний
- Уведомляет о наличии угрозы

Сканер безопасности

- Регулярная проверка узлов сети на уязвимости
- Контроль устранения выявленных проблем
- Классификация уязвимостей по уровню угрозы

Модель использования

- Облачный сервис под ключ от компании «Электронное облако»
- Развертывание внутри инфраструктуры заказчика и передача под его управления

Результат

- Единый центр управления информационной безопасностью
- Увеличение скорости реагирования
- Предотвращение инцидентов
- Повышение уровня зрелости системы информационной безопасности