БЕЗОПАСНО, НАДЁЖНО, КОМПЛЕКСНО

Управление инцидентами информационной безопасности

rusiem.com

Security Information and Event Management (SIEM)

Это эволюция и интеграция двух независимых технологий:

Security Event Management

Основной упор на сбор и агрегирование событий безопасности;

Security information Management

Сфокусирован на обогащении, нормализации и корреляции событий безопасности.

SIEM это совокупность технологии для:

- Сбора журналов безопасности
- Корреляции событий
- Агрегирования информации
- Нормализации информации
- Анализа содержимого трафика
- Анализа и технологического процесса управления событиями

ДВИЖУЩИЕ ФАКТОРЫ ДЛЯ ВНЕДРЕНИЯ SIEM

Выполнение требований регуляторов по обнаружению и реагированию на инциденты ИБ

Визуализация угроз в режиме реального времени

Операционная эффективность службы ИБ

РЕЗУЛЬТАТЫ РЕАЛИЗАЦИИ УГРОЗ

rusiem.com

ПРИМЕРЫ РЕАЛИЗАЦИИ:

- Сетевые атаки
- Фрод и мошенничество
- Отсутствие антивирусной защиты
- Повышение привилегий
- Изменение критичных конфигураций
- Аудит изменений конфигураций
- Обнаружение НСД

Вход в систему под пользователем, отсутствующим в офисе

Аномальная активность пользователя

Обнаружение распределенной атаки или вирусной эпидемии

Влияние отказа в инфраструктуре на бизнес - процессы

Обнаружение распределенных по времени атак

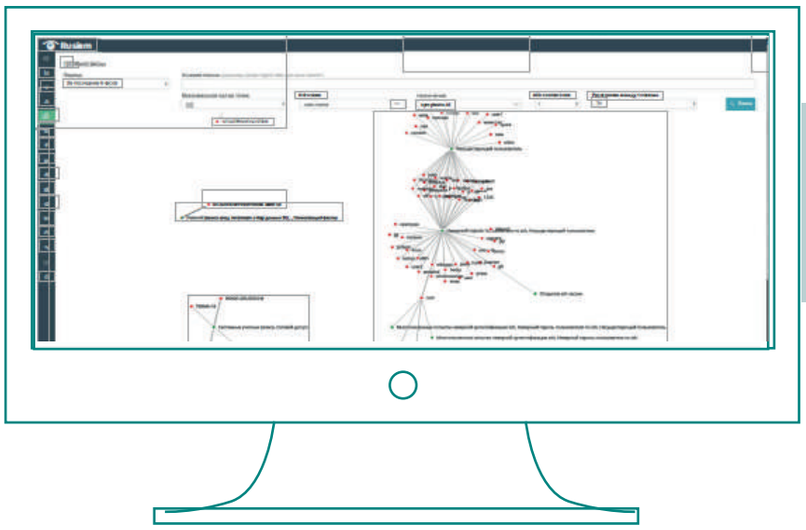
Оповещение об активной уязвимости по запуску ранее отключенной службы

Российская разработка

Полная поддержка русского языка

Высокая производительность

Возможность предоставления безлимитной лицензии



Коннекторы от производителя!

rusiem.com