LibraSoft

LibraSIEM

Система мониторинга и корреляции событий информационной безопасности

www.librasoft.by

Проблема и решение

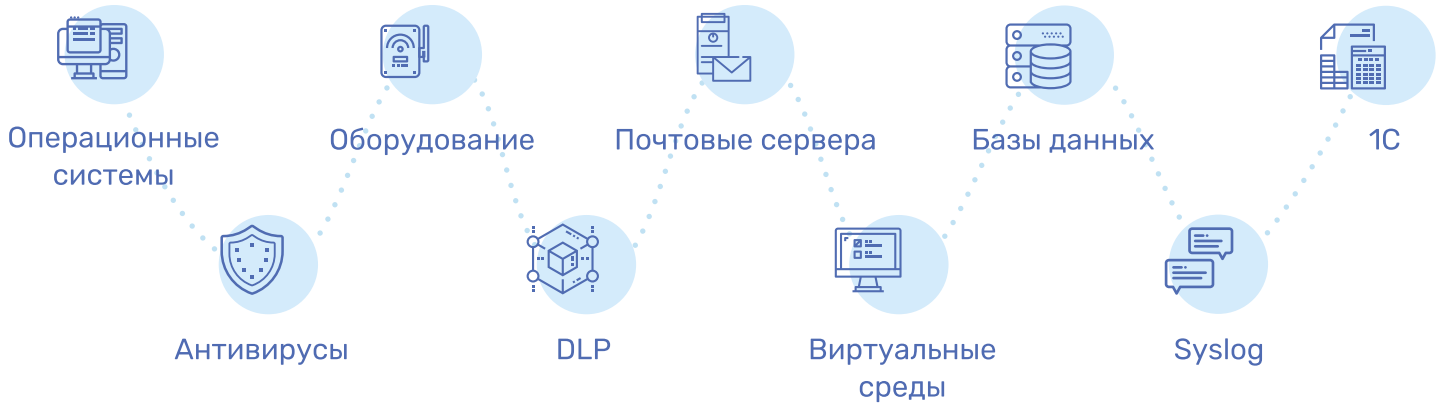
СКРЫТЫЕ УГРОЗЫ

Инцидентам в IT-инфраструктуре компании всегда предшествуют некие «симптомы» (события), значение которых может стать ясно только постфактум:

- подбор учетных данных;
- выход из строя или неверная работа оборудования;
- избыточные настройки доступа;
- временное изменение привилегий – получение расширенных прав доступа.

Вовремя обнаружить связь между событиями и принять меры служба безопасности может не всегда - поскольку количество рядовых информационных событий в сети может измеряться тысячами в секунду.

IT-инфраструктура большинства организаций состоит из ряда систем, нуждающихся в постоянном контроле.



Чтобы не упустить важное, службе безопасности нужен особый инструмент.

LIBRASIEM – ОБРАБОТКА СОБЫТИЙ И ВЫЯВЛЕНИЕ УГРОЗ

Система в режиме реального времени осуществляет сбор и анализ событий безопасности, выявляя инциденты и предоставляя ИБ-специалисту всю необходимую информацию для принятия решения. SIEM-система – это многофункциональный инструмент, который обеспечивает прозрачность функционирования IT-инфраструктуры.

ЧТО НАХОДИТ LIBRASIEM?

- потенциально опасные действия пользователей или администраторов;
- критические события в средствах защиты;
- попытки несанкционированного доступа к информации;
- неполадки в корпоративных системах;
- аппаратные и программные сбои.

Как устроена LibraSIEM?

Сбор событий из различных источников: сетевое оборудование, ПО, средства защиты, ОС

Анализ данных и выявление угроз

Фиксация инцидентов и оповещение в реальном времени

СИСТЕМА РАБОТАЕТ ПОЭТАПНО:

- **Собирает логи из различных источников: оборудование, программное обеспечение, операционные системы.**
- **Анализирует сведения, согласно настройкам (политикам безопасности).**
- **Обнаруживает инциденты и сообщает об этом специалисту по безопасности.**

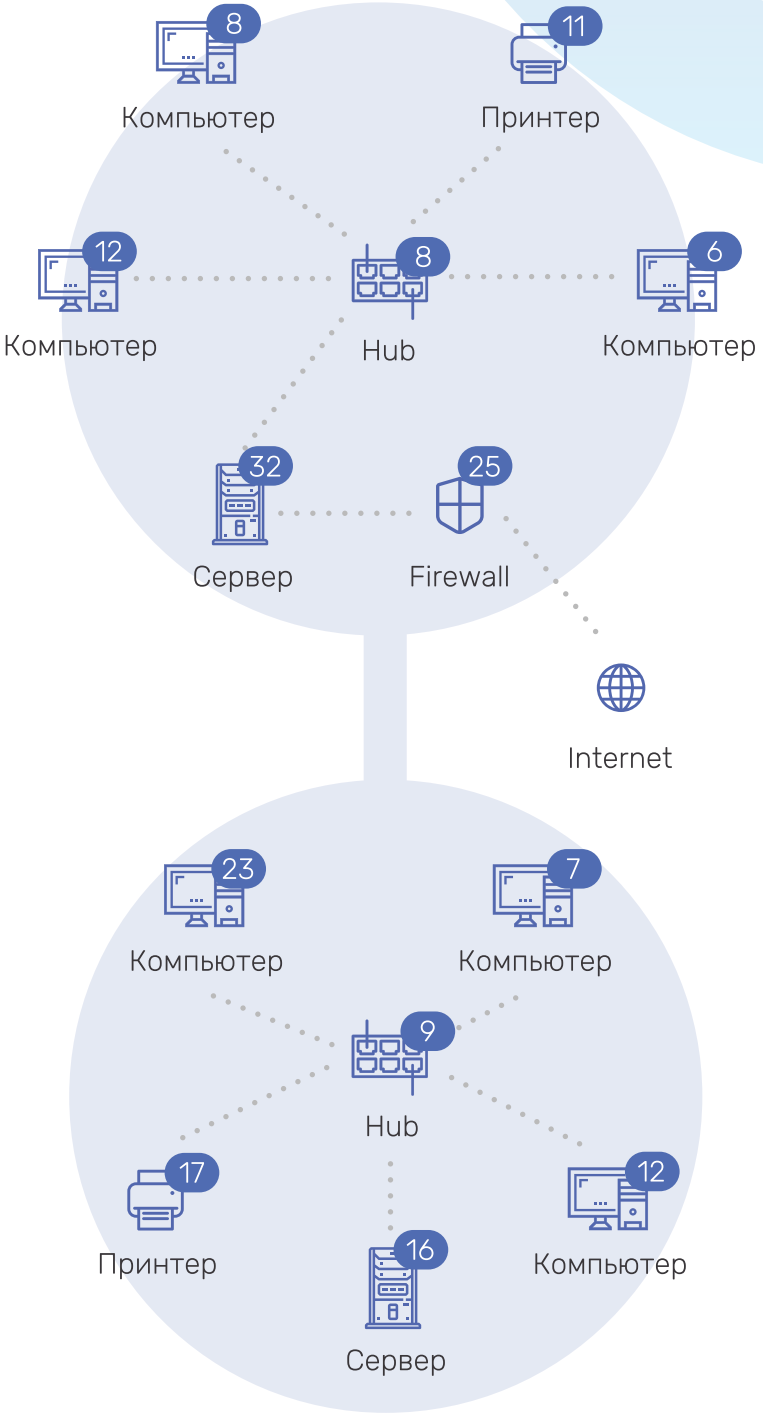
Настройка и управление LibraSIEM осуществляется через рабочую консоль. Здесь указываются параметры подключения к источникам данных, настраиваются оповещения и резервирование данных.

После этого LibraSIEM отслеживает события операционных систем (WinEvent, Linux), почтовых серверов (Exchange, Domino), антивирусов (Kaspersky, Mcafee, Eset, Symantec), оборудования (Fortigate, Palo Alto, Check Point, CWA, Cisco), DLP (LibraDLP), баз данных (MS SQL, Oracle, PostgreSQL), виртуальные среды (VMware), Syslog, 1С (1С Connector, 1С AD Integrator).

Полученные данные система анализирует в реальном времени, проверяя на соответствие политикам безопасности. Если обнаружен инцидент, LibraSIEM уведомляет об этом сотрудника службы безопасности.

Все инциденты хранятся в базе данных MongoDB, что обеспечивает доступ к ним для проведения расследований. ИБ-специалист может строить отчеты по найденным инцидентам и экспортировать их в другие форматы для дальнейшего изучения.

Карты корпоративной сети



IT-ИНФРАСТРУКТУРА НА ЭКРАНЕ И КАРТА ИНЦИДЕНТОВ

LibraSIEM – наглядный инструмент для контроля за событиями в корпоративной сети. На карте в рабочей консоли можно отобразить все устройства, подключенные к сети, и связи между ними. На значке объекта отображаются его характеристики: имя, IP- и MAC-адрес, операционная система.

Данные об устройствах и открытых на них портах отображаются не только на карте, но и в боковом меню. Благодаря карте сотрудник службы безопасности может в реальном времени следить за подключением и отключением устройств в IT-инфраструктуре.

В случае обнаружения инцидента специалист по безопасности может установить связь между событием и устройствами. На карте инцидентов в виде графа отношений отображается выбранная часть IT-инфраструктуры в связке с другими компонентами.

Политики безопасности

300+
готовых политик безопасности

список правил постоянно пополняется

ПРИМЕРЫ ПРЕДУСТАНОВЛЕННЫХ ПОЛИТИК LIBRASIEM

ДЛЯ КОНТРОЛЛЕРОВ ДОМЕНА ACTIVE DIRECTORY:

- временное переименование учетной записи;
- подбор паролей и устаревшие пароли;
- временное включение/добавление учетной записи.

ДЛЯ ОБОРУДОВАНИЯ:

- отказ системы охлаждения;
- вход с повышенными привилегиями;
- ошибки при работе системы.

ДЛЯ SYSLOG:

- события пользовательского уровня;
- события почтовых систем;
- события системных демонов.

ДЛЯ БАЗ ДАННЫХ:

- временное создание учетных данных;
- статистика изменения прав доступа;
- попытки входа в систему.

ДЛЯ FTP-СЕРВЕРОВ:

- соединение клиента с FTP;
- скачивание файла с FTP;
- создание/удаление файла на FTP.

ДЛЯ 1С:

- создание нового пользователя;
- использование привилегированного режима;
- изменение права администрирования пользователя.

ДЛЯ ПОЧТОВЫХ СЕРВЕРОВ:

- доступ к почтовому ящику не владельцем;
- смена владельца почтового ящика;
- предоставление доступа к ящику.

ДЛЯ АНТИВИРУСОВ:

- самозащита антивируса отключена;
- обнаружен вирус;
- выявлена сетевая атака.

ДЛЯ ВИРТУАЛЬНЫХ СРЕД:

- неправильные пароли;
- неудачные попытки входа;
- создание группы пользователей.

ДЛЯ СЕРВЕРОВ И РАБОЧИХ СТАНЦИЙ LINUX:

- неудачная попытка авторизации;
- события входа/выхода SSH;
- открытие/закрытие сессии.

Кейсы

ИЗМЕНЕНИЕ КОНФИГУРАЦИИ СЕТЕВОГО ОБОРУДОВАНИЯ

Некорректная настройка сетевого оборудования может нарушить работоспособность сети. LibraSIEM укажет сотруднику службы безопасности на связь между действиями системного администратора и работой конкретного устройства.

ВЗЛОМ ПК В ХОДЕ КИБЕРАТАКИ

LibraSIEM оповестит службу безопасности, если один из ПК корпоративной сети был атакован вредоносной программой. Своевременное обнаружение инцидента позволит вывести зараженное устройство из сети, блокируя масштабную атаку.

ХРАНЕНИЕ УЧЕТНЫХ ЗАПИСЕЙ УВОЛИВШИХСЯ СОТРУДНИКОВ

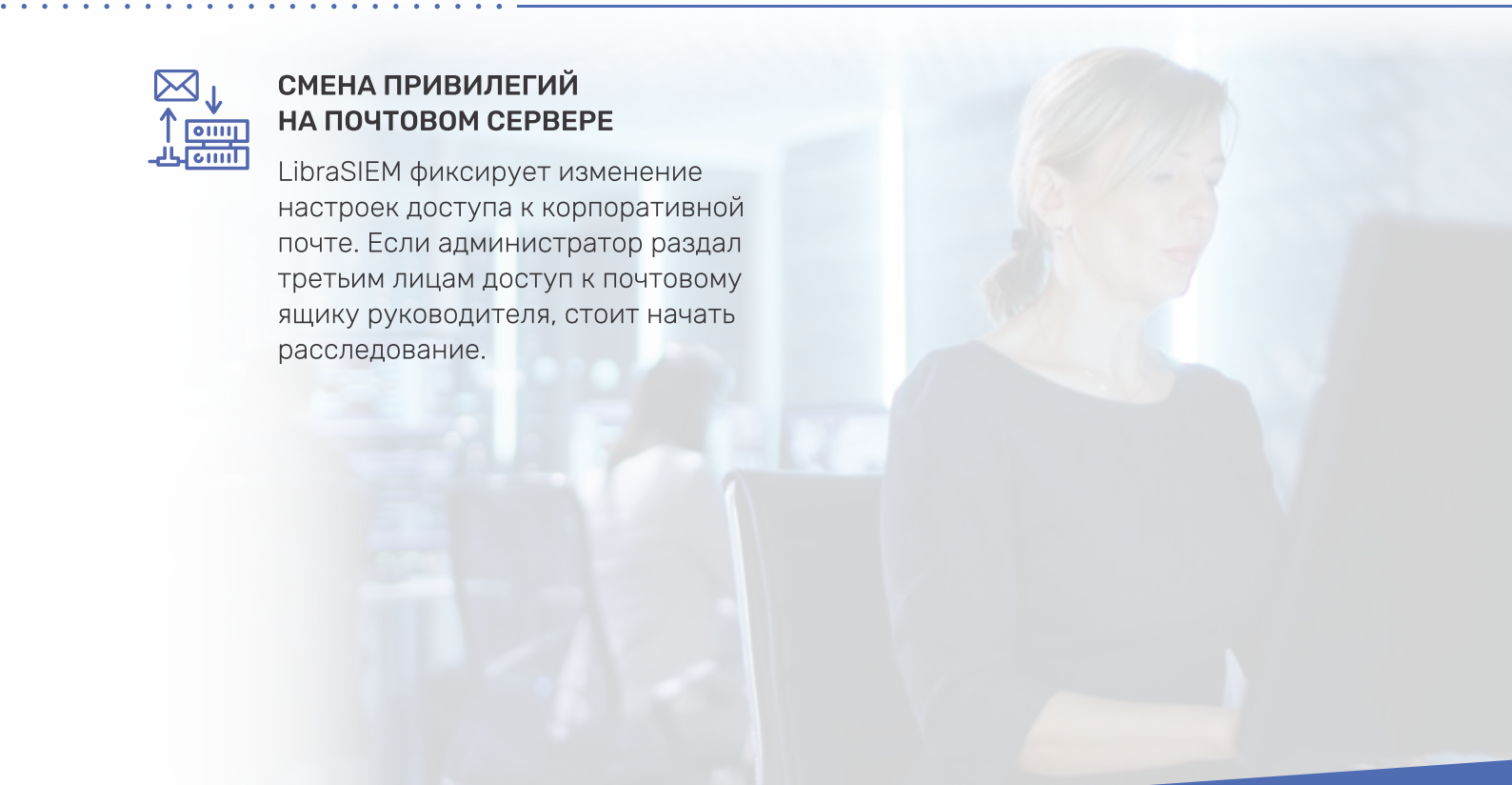
В соответствии с правилами информационной безопасности IT-отдел должен отключать записи сотрудников, которые больше не работают в компании. Однако «мертвые души» не всегда покидают корпоративную сеть. LibraSIEM обнаруживает подобные нарушения, о чем сообщает службе безопасности.

ПОПЫТКА НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

LibraSIEM обнаруживает попытки подобрать пароль к учетным записям, зарегистрированным в корпоративной системе. Выявление нарушителя предупредит утечку конфиденциальной информации.

СМЕНА ПРИВИЛЕГИЙ НА ПОЧТОВОМ СЕРВЕРЕ

LibraSIEM фиксирует изменение настроек доступа к корпоративной почте. Если администратор раздал третьим лицам доступ к почтовому ящику руководителя, стоит начать расследование.



Простое решение

LibraSIEM отличается от аналогов, которые нередко доставляют неудобства IT-отделу компании сложностью внедрения и конфликтностью с существующей инфраструктурой.

ПРЕИМУЩЕСТВА СИСТЕМЫ:

30 ДНЕЙ ДЛЯ ТЕСТИРОВАНИЯ LIBRASIEM С ПОЛНЫМ ФУНКЦИОНАЛОМ

1 ПРОСТОЕ ВНЕДРЕНИЕ

LibraSIEM является решением «из коробки». Заказчик получает готовый к запуску и использованию продукт с предустановленными политиками безопасности. Система изначально учитывает задачи компаний из различных сфер бизнеса.

2 ПРОСТАЯ ЭКСПЛУАТАЦИЯ

Для работы с LibraSIEM не нужны навыки программирования. В распоряжении специалиста по безопасности - готовые правила корреляции событий. Система работает на привычной ОС Windows и использует встроенную базу данных. А значит, заказчику не нужно переплачивать сторонним специалистам за настройку системы и обучение персонала.

3 ПРОСТАЯ ИНТЕГРАЦИЯ С IT- ИНФРАСТРУКТУРОЙ КОМПАНИИ

LibraSIEM отличается гибкостью – ее легко настроить под нужные задачи с учетом технических характеристик корпоративной сети. Система не конфликтует с установленным в компании программным обеспечением.

4 ПРОСТЫЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

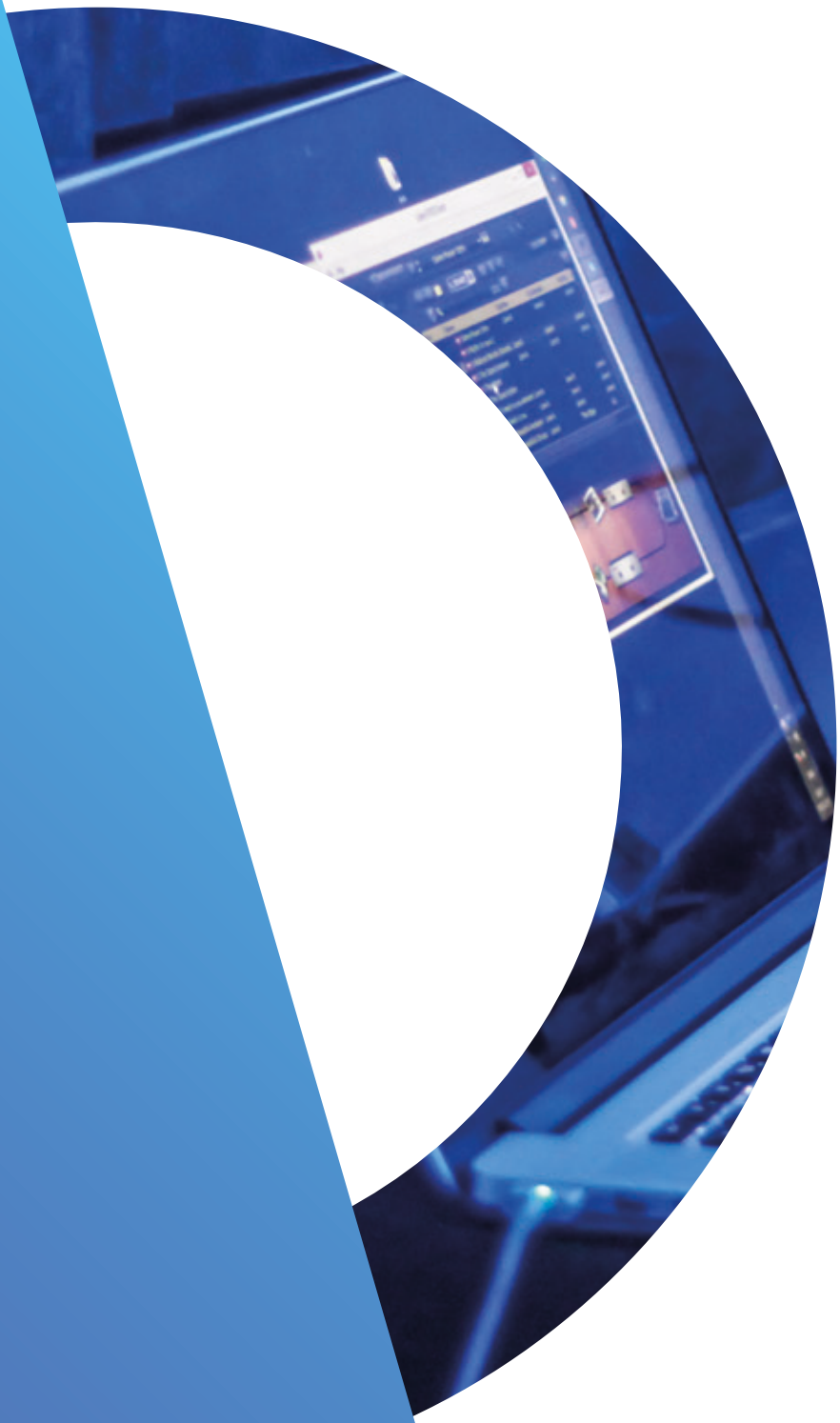
LibraSIEM нетребовательна к программно-аппаратным средствам. Система подойдет как крупному, так и малому и среднему бизнесу – по техническим характеристикам и цене.

5 ПРОСТАЯ ИНТЕГРАЦИЯ С ДРУГИМИ ИБ-РЕШЕНИЯМИ

Если компания уже использует средства защиты от информационных угроз, LibraSIEM четко впишется в ряд. Внедрение системы укрепит границы корпоративной сети, которую уже защищают DLP, IDS, IDM. Гармоничным и эффективным сочетанием станет последовательное или параллельное внедрение LibraSIEM и LibraDLP.

Минимальные системные требования к серверу SIEM

Процессор: **4-ядерный, частотой 2,1 ГГц**
Оперативная память: **4 ГБ**
Винчестер: **200 ГБ**
Сетевая карта: **100 Мбит/с**



Беларусь, Минск
220040, пер. М. Богдановича, д. 1, эт. 2, каб. 3
Телефон: + 375 (17) 227-56-80
Email: official@librasoft.by

LibraSoft