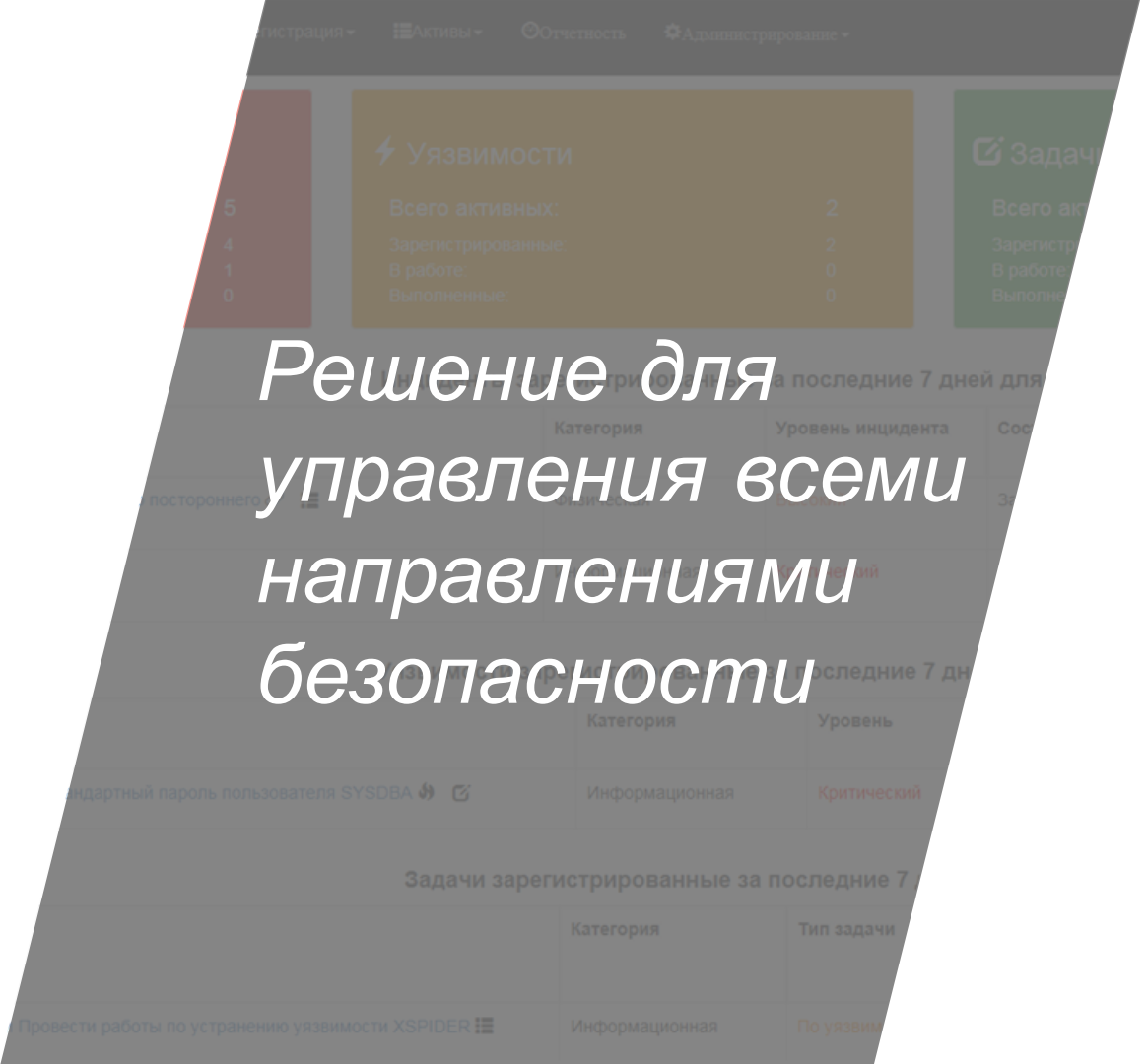
SecurityDesk

Автоматизированная система управления безопасностью



Решение для управления всеми направлениями безопасности

SecurityDesk

Все под контролем

SecurityDesk

Система относится к классу систем **Incident Response Platform (IRP)** и предназначена для создания центра мониторинга и реагирования на инциденты и уязвимости, а также управления работой сотрудников по выявлению и нейтрализации угроз.

Решаемые задачи:

Контроль процессов

Контролируйте процессы расследования инцидентов, устранения уязвимостей, исполнения поручений

Управление сотрудниками

Эффективно управляйте сотрудниками через выстроенную систему

Совместная работа

Организуйте совместную работу сотрудников с максимальной производительностью

Отчетность

Быстро формируйте и предоставляйте необходимую отчетность руководству, оценивайте риски

Автоматизация реагирования

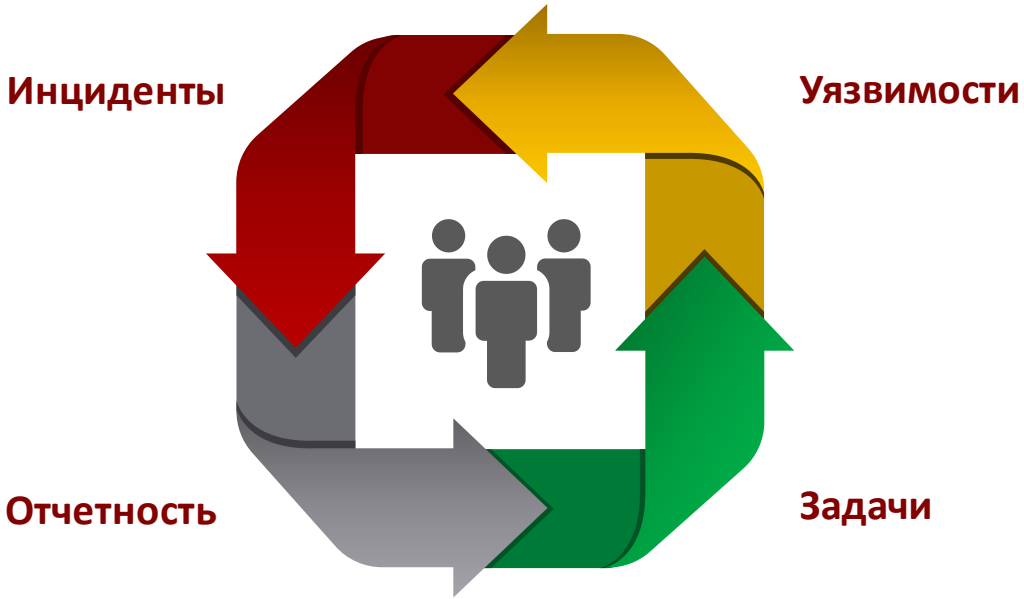
С помощью настроенных сценариев обеспечьте быструю скорость реагирования на инциденты

Архив данных

Создайте полное упорядоченное хранилище данных по всем инцидентам в одной системе

Интеграция с внешними источниками и обработка:

Подразделение безопасности, не важно к какому направлению оно относится, строит свою работу на расследовании инцидентов, выявлении уязвимостей, а также планирования и выполнения работ направленных на обнаружение и нейтрализацию угроз.



- По мере развития компании, растут и требования к ее безопасности
- Сначала покрываются базовые потребности
- В конечном итоге приходят к решению о внедрении SIEM

НО ТАК ЛИ ОНА НЕОБХОДИМА ?

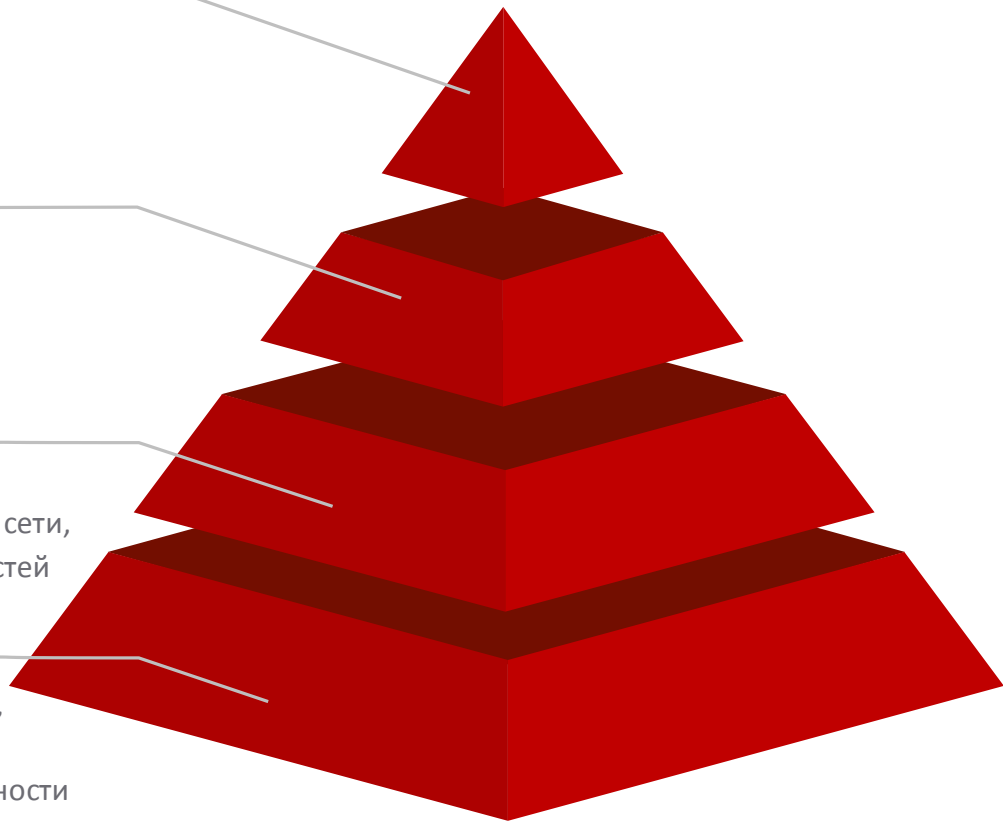
Технический уровень обеспечения

Высший
SIEM ?

Высокий
DLP, IPS,
MDM, IDM

Средний
FW, AD GPO,
сегментирование сети,
сканеры уязвимостей

Базовый
Антивирусное ПО,
встроенные
средства безопасности



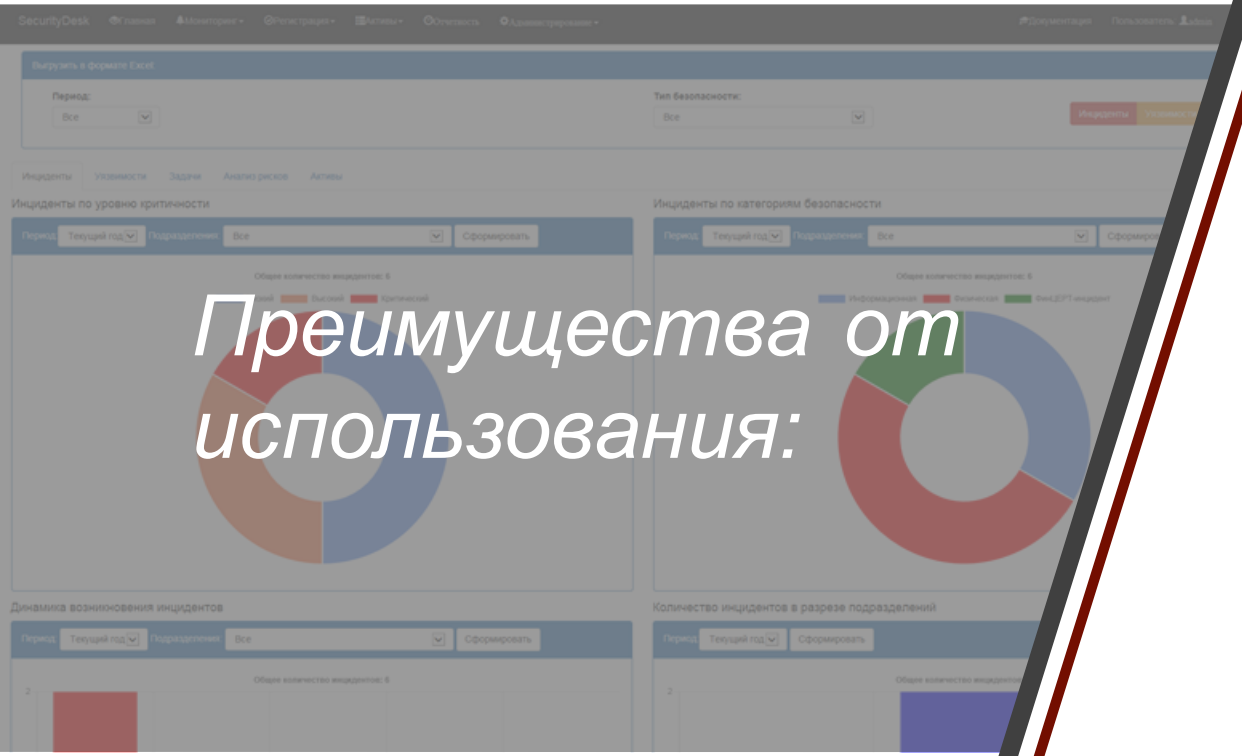
SIEM или IRP ?

Функционал	IRP	SIEM
Обротка событий и журналов работы систем		✓
Формирование инцидентов/уязвимостей/задач	✓	✓
Контроль и обработка инцидентов	✓	
Обогащение и хранение дополнительной информации	✓	
Связь с активами	✓	✓
Создание долговременного аналитического архива	✓	

Главным недостатком SIEM является **стоимость владения системой**, складывающаяся из стоимости аппаратных ресурсов, лицензий, услуг по внедрению и поддержки ее в работоспособном состоянии.
Именно поэтому **неуспешных примеров внедрения SIEM так много**.

IPR напротив проста во внедрении и поддержке, не требовательна к ресурсам, способна приносить пользу даже без интеграции с внешними источниками.
Именно поэтому **все внедрения IRP успешны**.

SecurityDesk



Преимущества от использования:

- Управление подразделениями любого направления безопасности
- Сокращение сроков реагирования на инциденты
- Получение в реальном режиме времени данных по расследованию инцидентов, устранению уязвимостей, выполнению поставленных задач
- Обоснование перед руководством эффективности работы подразделения
- Сокращение сроков формирования отчетности

Ключевые особенности:

01

Простое использование

Быстрое освоение функционала пользователями. Простая настройка, поддержка и администрирование

02

Управление объектами

Регистрация и управление жизненным циклом инцидентов, уязвимостей и задач

03

Гибкость

Возможность дополнять карточки объектов дополнительными параметрами

04

Построение связей

Возможность построения взаимосвязей между инцидентами, уязвимостями и задачами

05

Связь с активами

Возможность импорта активов из внешних источников и связывания их с объектами

06

Сценарии

Создание сценариев автоматического реагирования на инциденты и уязвимости

Ключевые особенности:

07

Классификация

Классификация инцидентов в соответствии с нормативными документами

08

Управление рисками

Оценка качественного и количественного ущерба от инцидентов для оценки рисков

09

Отчетность

Автоматическое формирование отчетов, и диаграмм

10

Обработка сканирования

Регистрация уязвимостей по результатам сканирования на уязвимости

11

Почтовый коннектор

Регистрация объектов на основе полученных данных с универсального коннектора электронной почты

12

Интеграция LDAP

Подключение Active Directory, FreeIPA для импорта активов и аутентификации

Ключевые особенности:

15

Экспорт

Экспорт данных в формат MS Excel и JSON ФинЦЕРТ

14

Коннекторы

С помощью коннекторов возможность интеграции с DLP, ERP и прочими системами

13

Встроенный API

Возможность взаимодействия с системой по встроенному WEB API, построенному на REST-архитектуре

Требования к ресурсам:

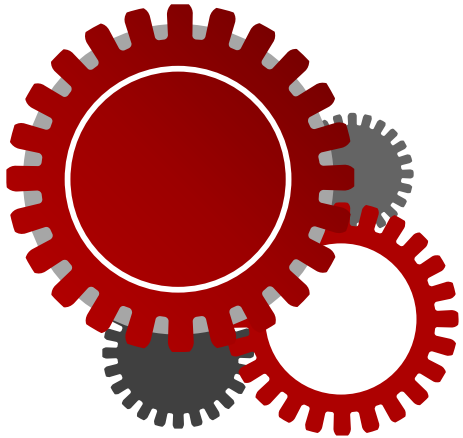
Минимальные программно-аппаратные требования для работы системы:

Для сервера:

- 64-разрядный процессор с тактовой частотой 1 ГГц или выше
- 4 ГБ оперативной памяти
- Свободное место на жестком диске 15 Гб
- Windows Server 2012 R2 (русская версия) и выше
- MS SQL Server 2014 (включая Express) и выше
- IIS 8
- .NET Framework 4.7 и выше

Для клиента:

- Персональный компьютер с установленным браузером Google Chrome, Internet Explorer 11, Microsoft Edge.



Лицензирование и тестирование:

Лицензирование:

- **В настоящий момент мы предлагаем свой продукт в виде приобретения права на простую неисключительную лицензию.**
- **Лицензия приобретается на необходимое количество серверов, не ограничена сроком использования и количеством пользователей.**
- **В поставку с лицензией включена бесплатная техническая поддержка на первый год.**

Демо-доступ:

- **Для тестирования предлагается демонстрационная версия системы с полным функционалом, но с ограничением на количество создаваемых инцидентов и уязвимостей.**
- **В случае принятия решения о приобретении лицензии вы сможете продолжить использовать настроенную в демо-версии базу данных, подключив к ней сервер приложений с приобретенной лицензией.**

Спасибо за внимание!

info@securitydesk.ru

securitydesk.ru

+7(910)-470-35-55