

SecurityDesk



Автоматизированная система
управления безопасностью

Решение для
управления
обеспечения
безопасности
всех направлений



SecurityDesk

Все под контролем



SecurityDesk

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

Решаемые задачи:

Контроль процессов

Контролируйте процессы расследования инцидентов, устранения уязвимостей, исполнения поручений



Единый центр управления

Организируйте единый центр управления процессами безопасности любого направления



Совместная работа

Организируйте совместную работу сотрудников с максимальной эффективностью



Отчетность

Быстро формируйте и предоставляйте необходимую отчетность руководству и оценивайте риски



Автоматизация реагирования

С помощью настроенных сценариев обеспечьте максимальную скорость реагирования на инциденты и уязвимости



Упорядоченный архив

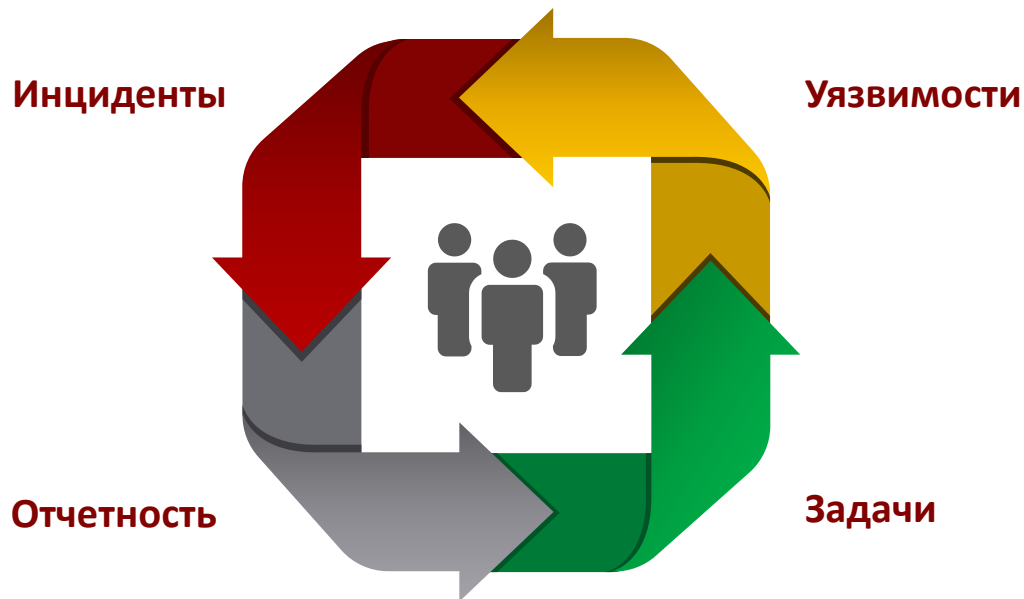
Создайте аналитическое хранилище данных по всем инцидентам, уязвимостям и работам в одной базе данных



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, также растут и требования к обеспечению ее безопасности
- Сначала обеспечиваются базовые потребности
- В конечном итоге приходят к решению о внедрении IRP и SIEM систем

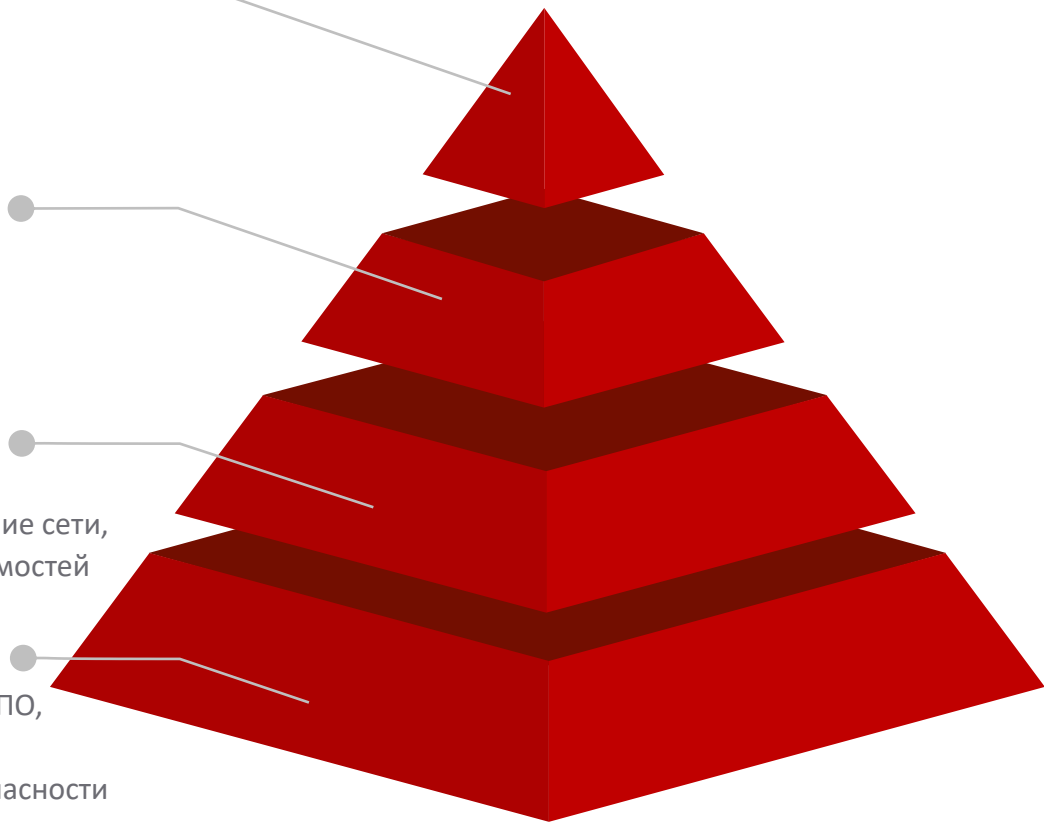
Высший
SIEM, IRP

Высокий
DLP, IPS,
MDM, IDM,
EDR

Средний
FW, AD GPO,
сегментирование сети,
сканеры уязвимостей

Базовый
Антивирусное ПО,
встроенные
средства безопасности

Технический уровень обеспечения



Сравнение функциональности IRP и SIEM?

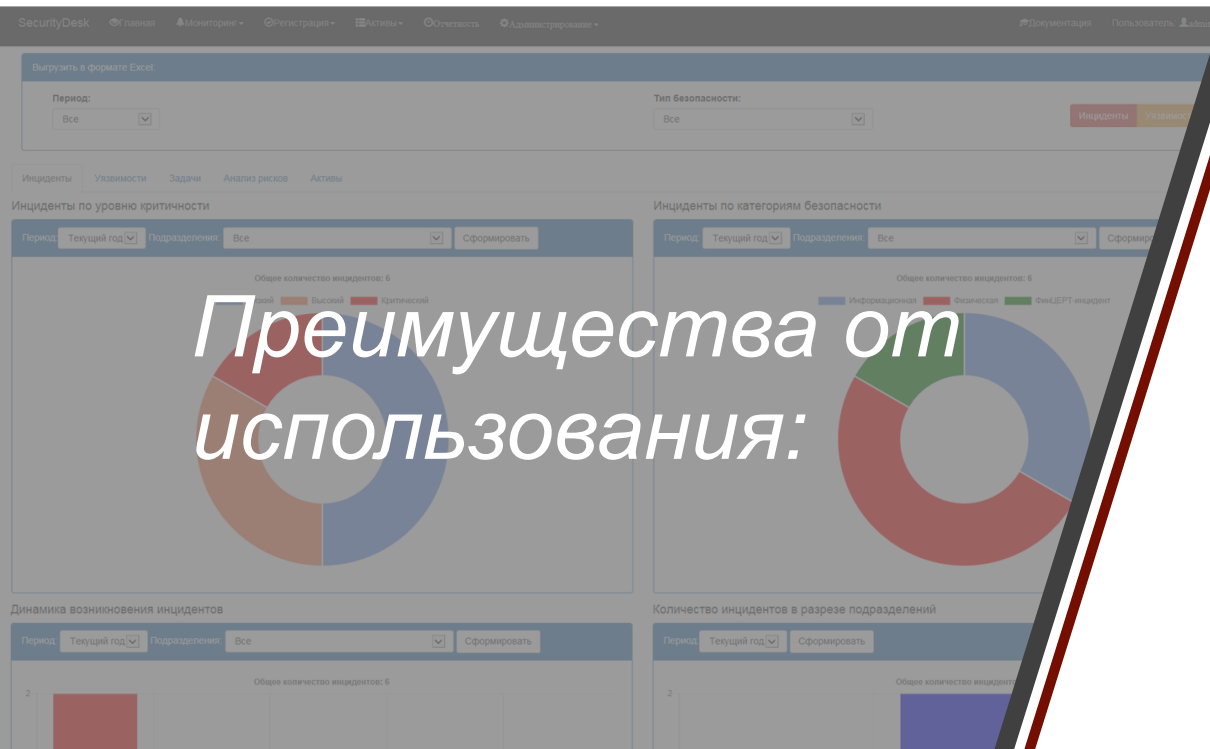
Функциональность	IRP	SIEM
Обработка большого объема событий от систем безопасности		✓
Формирование инцидентов/уязвимостей/задач	✓	✓
Возможность гибкой настройки обработки инцидентов/уязвимостей/задач	✓	
Обогащение дополнительной информацией инцидентов из различных источников	✓	
Привязка инцидентов, уязвимостей и задач к активам	✓	✓
Создание долговременного аналитического хранилища данных по инцидентам	✓	

Основным недостатком SIEM является **стоимость их владения**, которая складывается из стоимости аппаратных ресурсов, лицензий, затрат на услуги по внедрению и поддержке 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**.



Преимущества от использования:

- Обеспечение совместной эффективной работы сотрудников
- Единый центр управления процессами в подразделениях всех направлений безопасности
- Повышение уровня безопасности за счет сокращения сроков реагирования на инциденты
- Доступ в режиме online ко всей информации по устранению инцидентов, уязвимостей, выполнению поставленных задач
- Сокращение времени и затрат на формирование отчетности
- Автоматизированная регистрация инцидентов и передача данных в ФинЦЕРТ

Ключевые особенности:

03

Гибкость

Возможность расширять карточки объектов дополнительными параметрами

02

Управление

Гибкая настройка жизненного цикла инцидентов, уязвимостей и задач

01

Простое использование

Быстрое освоение функционала пользователями. Простая настройка, поддержка и администрирование

04

Построение связей

Возможность построения взаимосвязей между инцидентами, уязвимостями и задачами

05

Связь с активами

Импорт активов из внешних источников и привязка их к инцидентам, уязвимостям, задачам

06

Сценарии

Создание сценариев автоматического реагирования на инциденты и уязвимости

Ключевые особенности:

09

Отчетность

Мощные конструкторы построения отчетов и диаграмм любой сложности, полнотекстовый поиск

08

Управление рисками

Оценка качественного и количественного ущерба от инцидентов для проведения оценки рисков

07

Классификация

Классификация инцидентов в соответствии с нормативными документами

10

Обработка сканирования

Регистрация уязвимостей по результатам сканирования на уязвимости

11

Почтовый коннектор

Регистрация инцидентов, уязвимостей и задач на основе данных полученных по электронной почте

12

Интеграция LDAP

Подключение Active Directory, FreeIPA для импорта активов и аутентификации

Ключевые особенности:

15

Экспорт данных

Экспорт данных в формат MS Excel, Word, PDF, CSV и JSON, JSON ACOI ФинЦЕРТ

14

Коннекторы

Интеграция по API с помощью встроенных коннекторов ACOI ФинЦЕРТ, SIEM, DLP, ERP и прочими системами

13

Встроенный API

Возможность взаимодействия с системой по встроенному WEB API, на основе REST-архитектуры

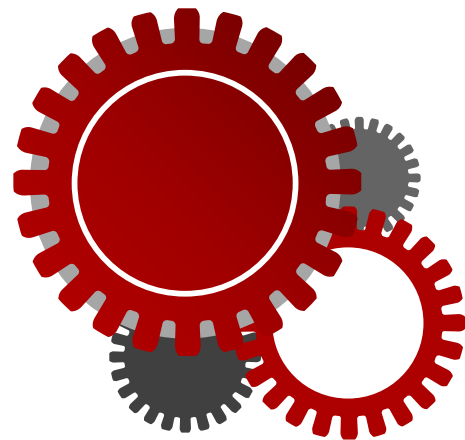
Требования к ресурсам:

Минимальные программно-аппаратные требования для работы системы:

- Сервер SecurityDesk**
- 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 4.8

- Сервер бизнес-процессов (опционально)**
- 64-разрядный процессор с тактовой частотой 1 ГГц или выше
 - 4 ГБ оперативной памяти
 - Свободное место на жестком диске 10 Гб
 - Linux Ubuntu Server 20.04 LTSC
 - Postgres SQL 14
 - Apache Webserver
 - .NET CORE 3.1

- Пользователь**
- Персональный компьютер с установленным браузером Google Chrome, Microsoft Edge и др.



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 1 год с момента приобретения.

Демо-доступ:




- Для тестирования предлагается демонстрационная версия системы с полным функционалом, но с ограничением количества 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