Описание функциональных характеристик Платформы управления информационной безопасностью «Эгида»

Аннотация

Настоящий документ содержит сведения о функциональных характеристиках Платформы «Эгида» (далее — ПО).

Описание и назначение ПО

ПО — российская платформа, автоматизации управление информационной безопасностью. Позволяет:

- реагировать на инциденты;

- осуществлять мониторинг;

- повышать зрелость информационной безопасности компании на основе метрик и данных.

ПО включает функционал SGRC-система для создания автоматизированной среды управления информационной безопасностью, объединяя в себе функционал SIEM, IRP, SOC, IDS, GRC, Сетевых СЗИ и модули управления соответствием.

ПО позволяет*:*

- Проводить инвентаризацию инфраструктуры;
- Анализировать инфраструктуру на соответствие требованиям регуляторов и внутренних нормативных документов;
- Учитывать информационные активы;
- Осуществлять управление событиями информационной безопасности;
- Производить оценку оборудования на соответствие требованиям при подключении к корпоративным сетям или защищенным контурам;
- Предоставлять отчетность о проделанных работах;
- Осуществлять управление сетевыми СЗИ;

Функциональные характеристики:

- Управление событиями и инцидентами информационной безопасности

- Контроль за исполнением сроков
- Механизм контроля исполнения
- Возможность переводить события ИБ в инциденты
- Отчетные материалы по различным разрезам
- Инвентаризация и учет физических активов
- Инвентаризация и учет цифровых активов
- Инвентаризация и учет систем
- Анализ конфигураций оборудования, операционных систем и прикладного программного обеспечения
- Управление конфигурациями сетевого оборудования и СЗИ
- Предоставление отчетности
- Проверка конфигураций на соответствие требованиям регуляторов и внутренних нормативных документов
- Управление сетевым доступом на основании результатов проверки соответствия
- Разграничение прав и ролей пользователей ПО
- Информационная панель
- Инструмент для управления правилами проверки

Основные компоненты платформы

Система состоит из следующих компонентов:

1. Система управления ПО – Веб приложение, выполняющее роль панели администратора ПО и пользовательского интерфейса ПО
2. База данных – хранит все данные и конфигурацию ПО
3. ACMS – Модуль управления сетевыми доступами
4. Агент ПО – сервис на конечных устройствах для осуществления сбора локальных проверок и взаимодействия с пользователем.

Руководство администратора и пользователя см. Приложение 1. Руководство администратора и пользователя.

Сведения о разработчике

Тел.: +7 (962) 577-24-67

e-mail: mail@infozont.com

Фактический адрес разработчиков и тех поддержки: *420500, г. Иннополис, ул.Университетская 5, офис 122*