

Общество с ограниченной ответственностью
«Инфрасек»

Infrasec Deception

Описание функциональных характеристик экземпляра ПО

Версия 1.0

ОГЛАВЛЕНИЕ

1. Функционал ПО..... 3

.

Infrasec Deception – распределенная платформа ложных целей.

1. Функционал ПО

1.1. Централизованное управление киберловушками

Программное обеспечение обеспечивает централизованную настройку, запуск, остановку и удаление ложных (фиктивных) сетевых сервисов, имитирующих уязвимые узлы в защищаемой инфраструктуре.

1.2. Централизованное распространение киберприманок

Система позволяет формировать и распространять фиктивные аутентификационные данные (логины, пароли, SSH-ключи и т. п.) на защищаемых хостах с целью провокации их использования для обращения в приманки.

1.3. Генерация Canary-токенов

Реализована возможность создания файлов-маячков, URL-ссылок и других типов токенов, активация которых приводит к фиксации события и передачи данных на сервер контроля.

1.4. Сбор телеметрии

Система осуществляет сбор полной информации обо всех взаимодействиях с размещёнными ловушками, включая сессию, IP-адрес атакующего, команды и протоколы взаимодействия.

1.5. Корреляция событий и формирование инцидентов

Автоматическая агрегация событий с последующей корреляцией и формированием инцидентов с присвоением приоритета и стадии обработки.

1.6. Интеграция с внешними системами

Передача информации об инцидентах в сторонние системы мониторинга и SIEM посредством протокола Syslog.

1.7. Уведомления об инцидентах

Поддерживается отправка уведомлений о новых инцидентах через Telegram и e-mail.

1.8. Ролевая модель доступа

В системе предусмотрены роли:

— Администратор: полный доступ ко всем функциям и настройкам.

— Оператор: ограниченный доступ в режиме просмотра.

1.9. Генерация рекомендаций

На основе анализа сетевой инфраструктуры система может формировать рекомендации по размещению новых ловушек.