Интеллектуальная система управления киберугрозами

SCS SBER CYBER SECURITY

МОДУЛЬ ОБОГАЩЕНИЯ

Использует механизмы обогащения информации о киберугрозах из платных и открытых источников, а также из смежных систем мониторинга, учета и защиты инфраструктуры банка

МОДУЛЬ АНАЛИТИКИ И ИНТЕГРАЦИИ

Позволяет проецировать обнаруженные киберугрозы на инфраструктуру банка (индикаторы компрометации, YARA-правила, SIGMA-правила, CVE/BDU) и оценивать возможный масштаб их влияния

МОДУЛЬ «GRAPH»

Позволяет проводить аналитику с использованием интерактивного графа, выявляя в автоматическом режиме неявные связи между объектами киберугроз

МОДУЛЬ СБОРА

Отвечает за сбор структурированных и неструктурированных данных, нормализацию и постоянную актуализацию информации о киберугрозах в сети интернет, включая теневой сегмент (DarkNet)

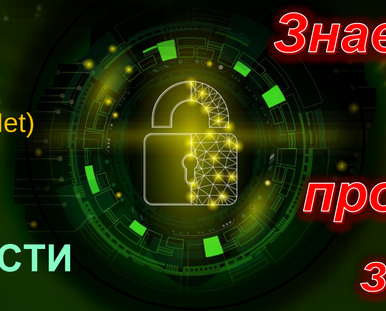
SBERBANK TIP

МОДУЛЬ УЧЁТА

Позволяет хранить информацию о результатах аналитики и атрибуты киберугроз (Case, Actor, Campaign, Malware, Vulnerability, TTP, IOC, DataLeaked, Phishing и др.)

МОДУЛЬ BRAND MONITORING

Выявляет фишинговые ресурсы и контент, дискредитирующий бренд банка в сети интернет, включая теневой сегмент (DarkNet) с последующим оповещением CERT



Знаете ли ВЫ, что произойдет завтра?

МОДУЛЬ УПРАВЛЕНИЯ СКАНИРОВАНИЕМ

Отвечает за полную автоматизацию процесса сканирования элементов инфраструктуры в режиме Vulnerability и Compliance и последующую обработку полученных результатов

МОДУЛЬ УПРАВЛЕНИЯ СЦЕНАРИЯМИ БЕЗОПАСНОСТИ

Связывает киберугрозы со сценариями детектирования, что позволяет обнаруживать и минимизировать киберугрозы в инфраструктуре банка на разных стадиях кибератаки

МОДУЛЬ УПРАВЛЕНИЯ РИСКАМ

Позволяет автоматизировать работу с рисками: заведение рискА в учетной системе HPSM, расчет рейтинга риска, обновление полей риска, связь риска с уязвимыми элементами, контроль исполнения риска по данным сканирования

МОДУЛЬ АДМИНИСТРИОВАНИЯ

Позволяет управлять ролевой моделью, словарями для хранения описаний разных сущностей, либо настройками системы

МОДУЛЬ ВИЗУАЛИЗАЦИИ

Создает оперативные виджеты на основании хранимых атрибутов описания киберугроз либо результатов их анализа

Преимущества продукта:

- Использование ML-подходов для анализа и приоритезации киберугроз.
- Реализация полного цикла работы с киберугрозами от обнаружения, расширенного анализа и проецирования на ИТ-инфраструктуру до последующей оценки влияния и создания сценариев реагирования.
- Встроенный модуль управления уязвимостями, содержащий полную информацию об элементах ИТ-инфраструктуры, позволяющий в автоматическом режиме определить векторы.
- Возможность работы со структурированной и неструктурированной информацией за счет поддержки известных форматов (STIX/TAXII, JSON, XML и др.), а также механизмов нормализации.
- Гибкость разработанного продукта для расширения функциональных возможностей существующих модулей
- Независимость от конкретных коммерческих решений: реализовано большое количество универсальных коннекторов для подключения.
- Отсутствие аналога разработанной системы анализа киберугроз, которая в одной платформе объединяла бы в себе совокупность созданных модулей и аналитических алгоритмов.
- Система обладает патентом на территории РФ.

Результаты внедрения продукта:

- Сокращено времени сбора информации и увеличен объем обрабатываемых данных за счет средств автоматизации сбора и постоянной актуализация информации о киберугрозах.
- Сокращено время анализа обрабатываемой информации за счет автоматизации обогащения информации о киберугрозах за счет интеграции с подписками и внутренними системами защиты и мониторинга инфраструктуры.
- Сокращено время анализа на первичную обработку актуальных киберугроз из всего поступающего потока информации за счет применения ML-подходов, выполняющих приоритезацию (скоринг) поступающей информации.
- Сокращено времени анализа информации за счет централизованного учета информации о киберугрозах и гибких инструментов аналитики (неявные связи, интерактивный граф, фильтры, агрегации).
- Своевременное обнаружение и оценка масштаба влияния за счет проецирования обнаруженных киберугроз на инфраструктуру.
- Сформирован централизованный банк знаний о киберугрозах, позволяющий повышать компетенции профильных подразделений и уровень осведомленности об актуальных киберугрозах.