Современные аналитические инструменты на страже бизнеса

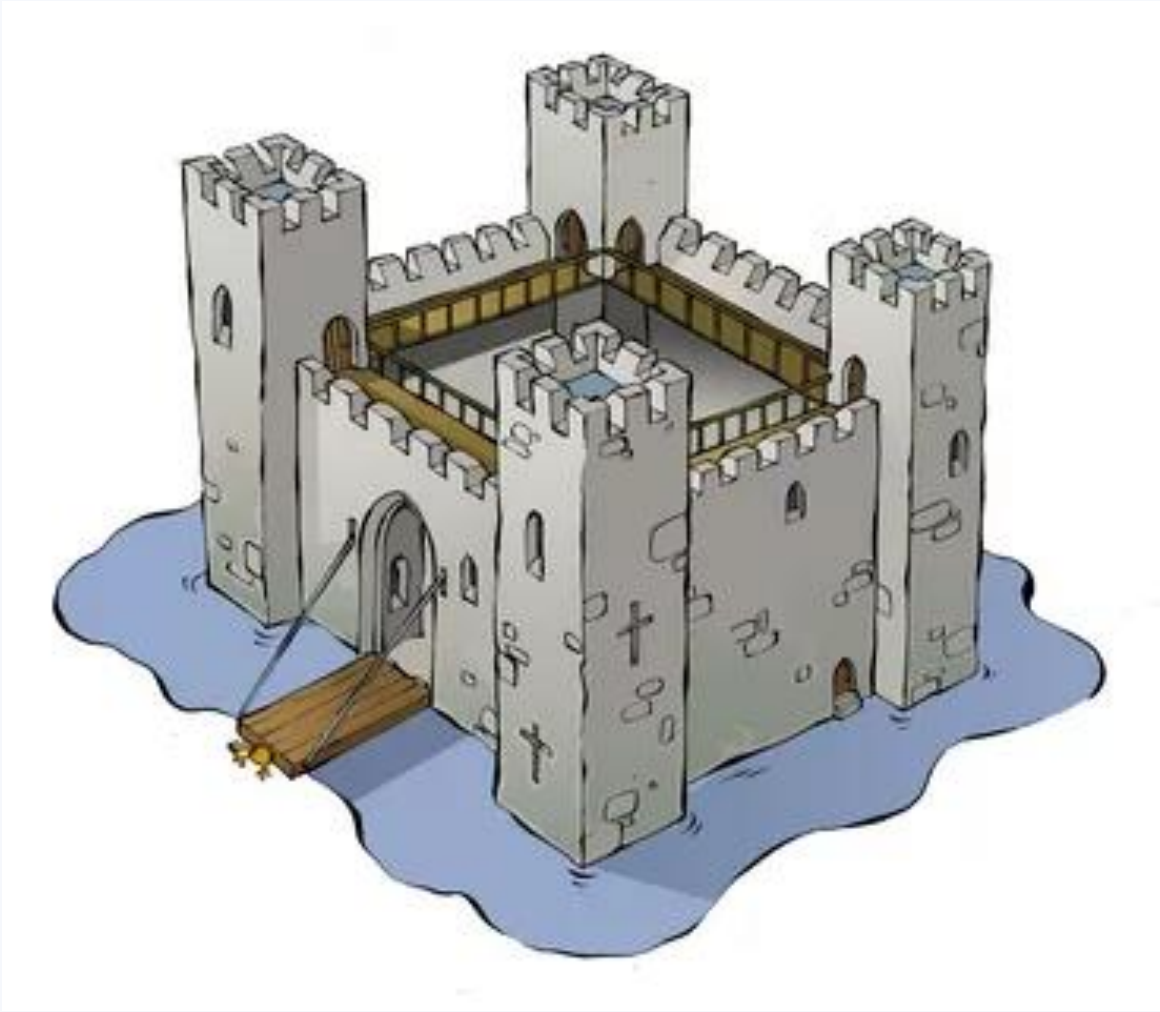
Вураско Александр

ведущий аналитик
Infosecurity a Softline company

INFOSECURITY
a Softline company

Традиционная концепция обеспечения ИБ

и ее минусы…



INFOSECURITY
a Softline company

Типовые угрозы бизнесу

- Утечки конфиденциальной информации
- Целевые атаки
- Нарушения бизнес-процессов
- PR-атаки
- Неправомерное использование бренда
- Атаки на клиентов организации
- Недобросовестные контрагенты

Что такое ETHIC?

Сервис ETHIC предназначен для выявления на ранних стадиях цифровых угроз бизнесу в глобальных информационных и телекоммуникационных сетях, что позволяет своевременно реагировать на угрозы, не допуская наступления негативных последствий или минимизируя их.

Какие задачи решает ETHIC?

- снижение рисков информационной, экономической безопасности и репутационных потерь
- предотвращение неправомерного использования бренда
- выявление утечек информации, компрометации учетных записей, мобильного фрода

- защита от фишинга
- противодействие мошенникам
- защита от социальной инженерии
- выявление и пресечение информационных атак
- проверка контрагентов

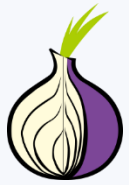
В чем заключаются преимущества ETHIC?

- простота работы и автоматизация рабочих процессов
- отсутствие нагрузки на инфраструктуру заказчика
- многоступенчатая верификация угроз опытными аналитиками
- модульность сервиса

- широкий перечень объектов мониторинга
- удобный интерфейс
- гибкость настройки с учетом специфики бизнеса заказчика
- оперативное реагирование на инциденты

INFOSECURITY
a Softline company

Источники данных ETHIC



Ресурсы DarkNet – анонимные сайты и форумы, размещенные в распределенных сетях Tor, i2p

Реестры доменных имен

«Черные списки» (реестр дисквалифицированных лиц, иностранных агентов, санкционные списки, перечень террористических организаций и т.п.)

Ресурсы Deep Web - веб-страницы «Всемирной паутины», неиндексируемые поисковыми системами

Государственные информационные системы и интеграторы данных

Социальные сети (Вконтакте, Facebook, Instagram, Мой Мир, Twitter, Одноклассники) и мессенджеры (Skype, Telegram и т.д.)

Базы данных публичных утечек

Сервисы поиска работы (hh.ru, avito.ru и т.д.)

Магазины мобильных приложений (Google Play Market, Apple Store, Windows Store, Яндекс.Store)

Торговые площадки (avito.ru, youla.ru и аналоги)

Порядок работы сервиса

МОНИТОРИНГ

Автоматический анализ источников вне периметра компании: от соцсетей до ресурсов DarkNet

ОЦЕНКА

Аналитическая экспертиза уровня опасности и определение тактики реагирования

ОПОВЕЩЕНИЕ

Отправка предупреждений об угрозах для бизнеса или инцидентах через специальный веб-портал

РЕАГИРОВАНИЕ

Блокировка источников, изменение технических настроек сервисов, проведение расследования

Модули ETHIC

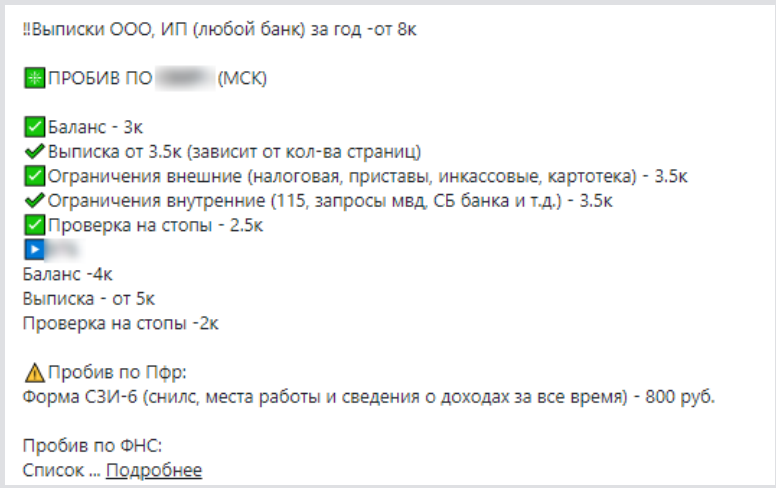
В состав сервиса входит 12 модулей:

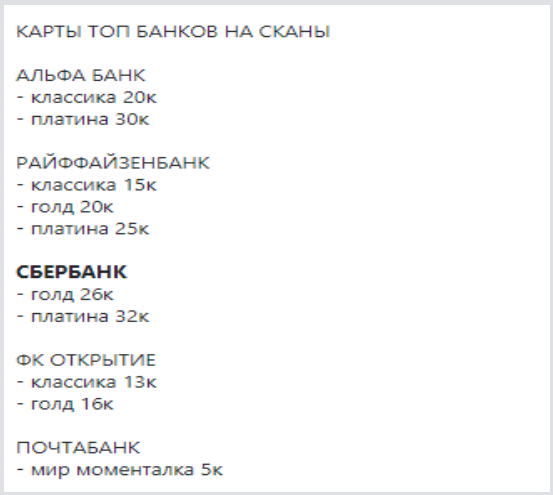
- УСЛУГИ
- ФИШИНГ
- УТЕЧКИ
- НЕГАТИВ
- БРЕНД
- МЕНЕДЖМЕНТ
- СОТРУДНИКИ
- ЮР. ЛИЦА
- МОБИЛЬНЫЙ ФРОД
- КОНТРАГЕНТЫ
- ПРОВЕРКА
- РЕПОЗИТОРИИ

Модульность сервиса позволяет заказчику получать услуги в требуемом ему объеме, избегая тем самым лишних затрат

Модуль «Услуги»

Выявленные события





Анализ угрозы:

- вероятное наличие инсайдера в организации
- риски для клиентов
- риски утечки конфиденциальной информации
- репутационные риски
- риски санкций со стороны регулятора

Действия со стороны «Инфосекьюрити»*:

- установление лица, разместившего объявление
- проведение «проверочной закупки»
- блокирование аккаунтов и удаление сообщений
- подготовка материалов для проведения внутренней проверки или направления в правоохранительные органы

Возможные действия со стороны Заказчика:

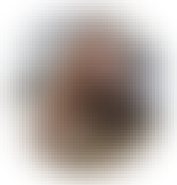
- проведение внутренней проверки
- выявление сотрудников, причастных к противоправной деятельности
- обращение в правоохранительные органы (при необходимости)
- совершенствование мер внутреннего контроля на основе результатов анализа инцидента

Результат:

- устранение каналов утечки информации
- выявление неблагонадежных сотрудников
- снижение финансовых и репутационных рисков

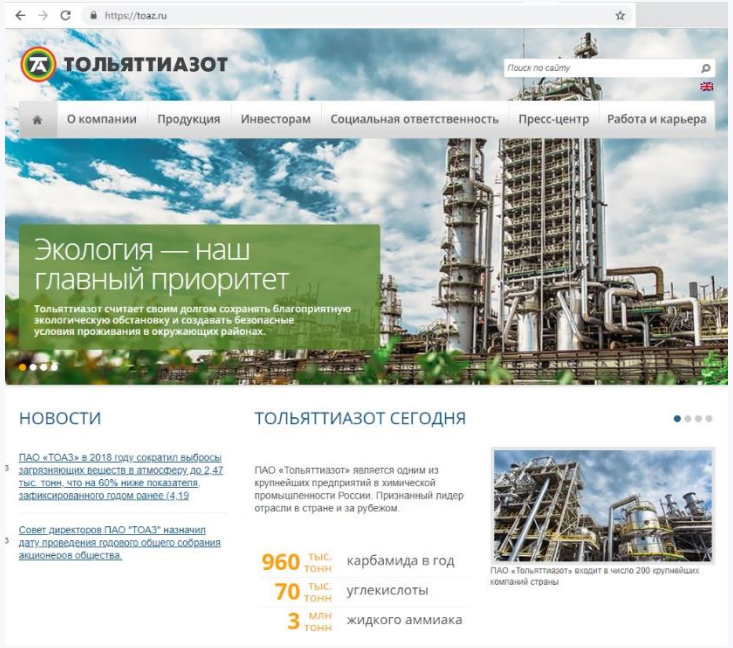
*В рамках услуги «Оперативное реагирование на инциденты»

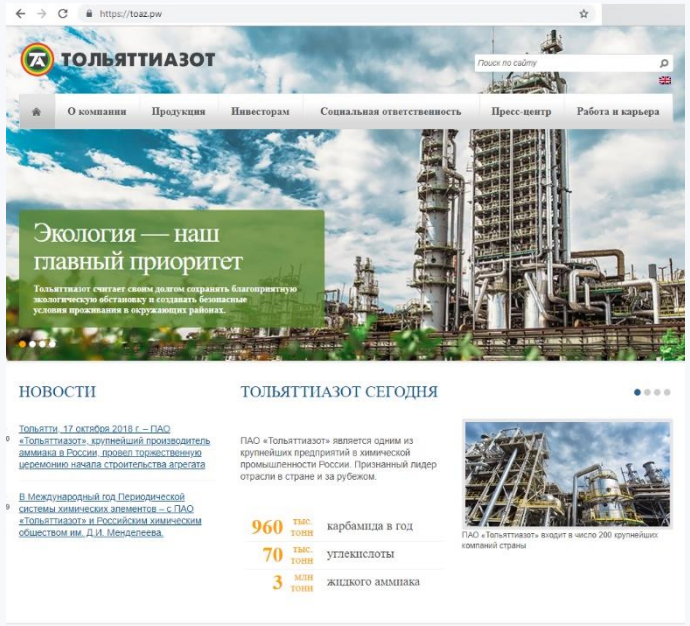
Пример объявления о поиске сотрудников банка



СОДЕЙСТВИЕ в Открытие счёта в МОСКВЕ ИЗ ПЕРВЫХ РУК НЕ ПОСРЕДНИК!
А так же в Регионах по запросу (в т ч организациям которые в блоке других банках 550 115фз)с директором и без ,закрытие , пробив остатка счёта,выписки со счёта,вывод средств без пометок на контрагента А так же Приглашаем к сотрудничеству работников банковской сферы для совместной плодотворной работы в направлении открытия расчетных счетов . Мы гарантируем стабильный поток клиентов, большой объем продаж сопутствующих доп. услуг , хорошее вознаграждение
Все конфиденциально!

Модуль «Фишинг»





Действия со стороны «Инфосекьюрити»*:

- идентификация владельца ресурса, хостера и регистратора домена
- формирование уведомления о нарушении прав заказчика
- составление и отправка обоснованной претензии администратору сайта
- направление жалобы хостинг-провайдеру и регистратору доменного имени
- обращение к поисковым системам для удаления ресурса из поисковой выдачи
- работа с регуляторами по имеющимся претензиям со стороны правообладателей

Действия со стороны заказчика:

- согласование перечня необходимых действий
- предоставление доверенности
- предоставление необходимых документов, подтверждающих права на интеллектуальную собственность и средства индивидуализации

Результат:

- блокирование фишингового ресурса
- снижение финансовых и репутационных рисков
- повышение лояльности клиентов

*В рамках услуги «Оперативное реагирование на инциденты»

Модуль «Утечки»

Учетная запись	vk.com, Anti Public Combo List, Exploit.In		og[redacted]@[redacted].ru	Компрометация учетной записи "Ольга [redacted]"
Документы	https://vk.com/doc75232830_476534394	 vk.com		Документ содержащий подпись и печать официального представителя партнера Банка и конфиденциальные данные клиента.

Анализ угрозы:

- информация может использоваться для атаки на организацию
- персональные данные клиента могли оказаться в общем доступе по вине сотрудников организации

Действия со стороны «Инфосекьюрити»*:

- установление источника компрометации данных
- установление лица, разместившего информацию
- анализ распространения информации (количество скачиваний и т.д.)
- блокирование аккаунтов и удаление сообщений (при необходимости)

Действия со стороны заказчика:

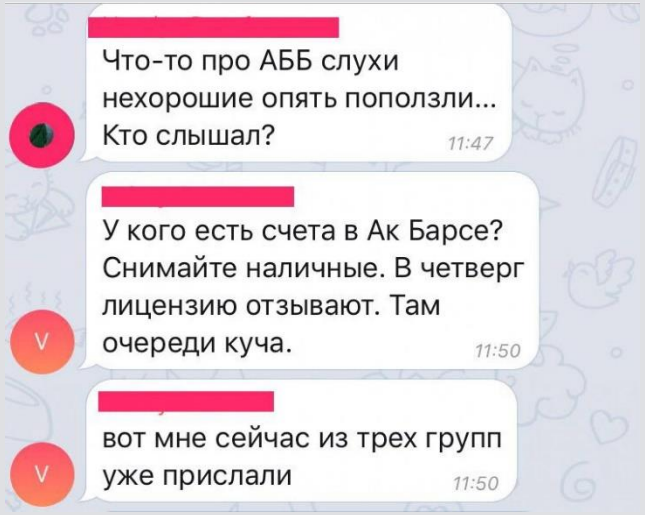
- оценка возможного вреда от распространения информации
- защита скомпрометированных учетных записей

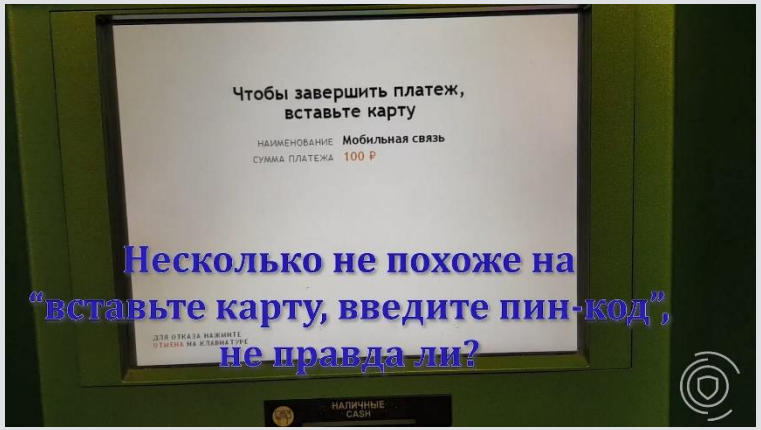
Результат:

- выявление сотрудников, допустивших утечку
- недопущение неправомерного использования конфиденциальной информации
- предотвращение возможных атак на организацию
- совершенствование регламентов обеспечения ИБ

*В рамках услуги «Оперативное реагирование на инциденты»

Модуль «Негатив»





Первое сообщение в VK – 7 мая
Пик сообщений – 18-20 мая

Анализ угрозы: информация может носить заказной характер, выявленные публикации могут содержать сведения об уязвимых элементах бизнес-процессов или деятельности недобросовестных сотрудников

Возможные действия со стороны «Инфосекьюрити»:
- установление лиц, разместивших информацию
- анализ распространения информации
- выявление схожих публикаций на других площадках и их анализ на предмет обнаружения PR-атак
- блокирование аккаунтов и удаление сообщений (при необходимости)

Действия со стороны заказчика:
- оценка возможного вреда от распространения информации
- корректирование PR-политики, своевременное реагирование на PR-атаки
- совершенствование сервисов, повышение качества оказываемых услуг
- выявление недобросовестных сотрудников и принятие мер

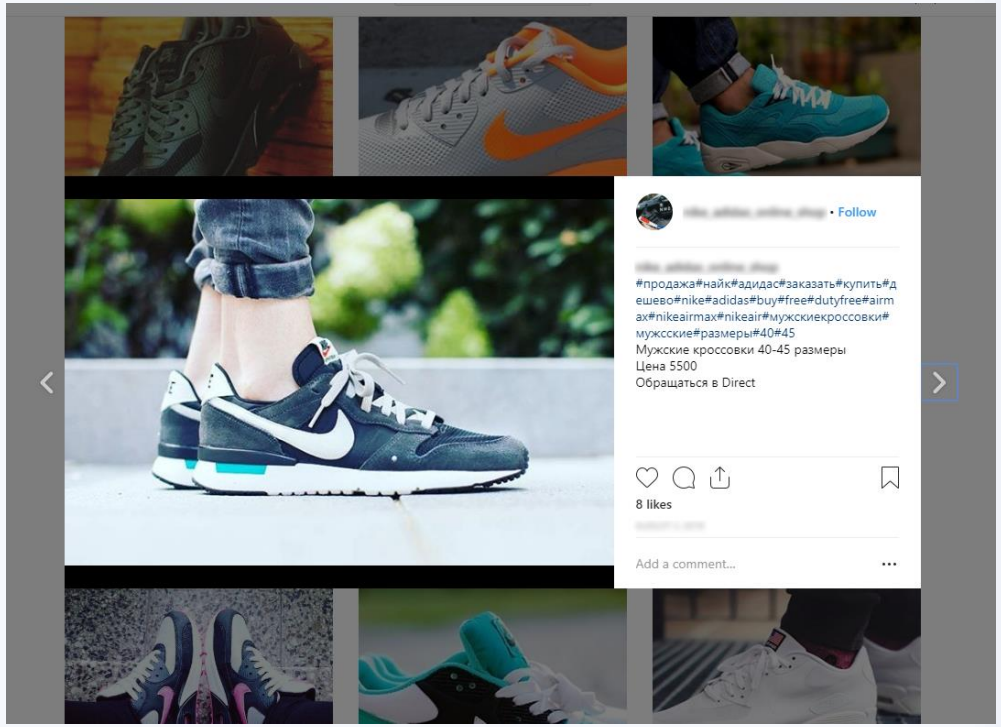
Результат:
- повышение качества сервисов и услуг
- снижение репутационных рисков
- предотвращение PT-атак на организацию

INFOSECURITY
a Softline company

Модуль «Бренд»

Выявление неправомерного использования бренда в социальных сетях или в мессенджерах

Фейковые страницы могут вводить в заблуждение клиентов, использоваться для кражи конфиденциальных данных или оказания услуг под видом организации



Возможные действия со стороны «Инфосекьюрити»:

- становление лиц администраторов сообществ, владельцев учетных записей или ресурсов
- формирование уведомления о нарушении прав заказчика
- составление и отправка обоснованной претензии администрации ресурса
- работа с регуляторами по имеющимся претензиям

Действия со стороны заказчика:

- оценка возможной угрозы или нарушения прав
- предоставление доверенности
- предоставление необходимых документов, подтверждающих права на интеллектуальную собственность и средства индивидуализации

Результат:

- снижение репутационных рисков
- повышение лояльности клиентов
- выявление атак на организацию, предотвращение мошеннических и иных противоправных схем

INFOSECURITY
a Softline company

Неправомерное использование бренда

https://pochtabanka.site

ПОЧТА БАНКА | Работа курьером по доставке банковских карт

Зарабатывайте до 3400 руб. в день, доставляя документы и карты банка без продаж, вложений и опыта!

Ищете простую работу или подработку с достойной оплатой и свободным графиком?

Начните работать через наше приложение - доставляя документы и банковские карты клиентам банка в своем городе, вы будете получать до 3400 руб. в день не напрягаясь

Хочу работать

Узнать подробнее ...

Неправомерное использование бренда

ПОЧТА БАНКА | Работа курьером по доставке банковских карт

Инструкция по подключению

ШАГ 2. Подготовьте документы и карту банка

Для подключения и заключения договора необходимо иметь полный комплект документов (Без исключения - пакет документов обязательный):

1. Паспорт РФ **(Строго с действующей регистрацией)**
2. СНИЛС (Зеленая карточка)
3. ИНН
4. Банковская карта для расчетов **(Альфа Банк - обязательно)**

ВНИМАНИЕ! С 12.06.2019 г. курьеры могут использовать только карты Альфа Банк. Карты других банков для расчетов не принимаются. Заявки на подключение от курьеров без карты Альфа Банк будут отклоняться без возможности повторной подачи.

ПЕРЕД ПОДАЧЕЙ ЗАЯВКИ НА ПОДКЛЮЧЕНИЕ самостоятельно оформите и получите дебетовую карту Альфа Банк по инструкции ниже.

ИНСТРУКЦИЯ!!! по самостоятельному получению карты АО «Альфа Банк» для работы (Выпуск и обслуживание карты бесплатно) >>>

Важно! Карту оформляете для личных нужд - БЕЗ УКАЗАНИЯ ПОЛУЧЕНИЯ ЗАРПЛАТЫ.

Реквизиты необходимо предоставить при подключении - должны быть у Вас обязательно.

При подаче заявки на подключение, карта должна быть у Вас на руках и активирована.

<<< Назад

Далее >>>

Not Secure | odobrim.ml/cc/

Инструкция по оформлению дебетовой карты «Альфа-Карта»

- *Бесплатный выпуск*
- *Бесплатное обслуживание*
- *Бесплатное снятие наличных*
- *Бесплатные переводы*

Оформить карту >

Шаг 1.

Перейдите на страницу анкеты карты: Ссылка (нажмите) > > >

https://pochtabanka.site/end.html

ШАГ 3. Отправьте запрос на подключение

После того, как подготовите необходимый комплект документов и получите карту на руки, Вам необходимо отправить запрос на электронный адрес:

apps@pochtabanka.site

В теме письма напишите:

Запрос на подключение

В самом письме напишите:

Ваше ФИО (полностью) и Ваш город.

ВАЖНО! Никакие документы отправлять не надо, только ФИО и город!

В течение 3-4 рабочих дней Вам будет предоставлен доступ к приложению и информация по заключению договора и обучению. С Вами свяжется оператор и проведет вводный инструктаж по работе в приложении.

Будем рады видеть Вас в нашей команде!

Модуль «Менеджмент»

Выявление поддельных профилей топ-менеджмента и ключевых сотрудников Заказчика в социальных сетях

Аккаунты-двойники могут использоваться для мошеннических действий, информационных и целевых атак на организацию

Возможные действия со стороны «Инфосекьюрити»:

- взаимодействие с администрацией соцсетей в целях оперативного блокирования учетных записей
- выявление случаев использования учетных записей в противоправных целях

Действия со стороны заказчика:

- верификация легитимности учетных записей ключевых сотрудников организации

Результат:

- снижение репутационных рисков
- снижение рисков мошенничества
- предотвращение атак с использованием социальной инженерии

INFOSECURITY
a Softline company

Модуль «Сотрудники»

Выявление ключевых сотрудников или специалистов, имеющих доступ к критически важной информации Заказчика, находящихся в активном поиске работы

Возможные действия со стороны заказчика:

- дополнительная мотивация ценных сотрудников
- ограничение доступа к конфиденциальной информации
- аудит условий труда и взаимоотношений в коллективе

Результат:

- предотвращение потери ценных кадров
- предотвращение утечки конфиденциальной информации
- выявление конфликтов
- улучшение морально-психологического климата в коллективе

Модули ETHIC

ЮРИДИЧЕСКИЕ ЛИЦА

Сведения о продаже юридических лиц и ИП. Данные лица могут быть незаконно использованы в качестве фиктивных контрагентов Заказчика или иметь расчетные счета, используемые для легализации (отмывания) доходов, полученных преступным путем, финансирования терроризма и иной нелегальной деятельности

МОБИЛЬНЫЙ ФРОД

Выявление фишинговых программ в магазинах мобильных приложений (Google Play Market, Apple App Store, Microsoft Store, Яндекс.Store), а также официальных телефонных номеров Заказчика, используемых в связке со сторонними приложениями или ресурсами

РЕПОЗИТОРИИ

Мониторинг GitHub, Pastebin и прочих ресурсов на предмет выявления потенциально опасного кода, в т.ч. вредоносных программ, скриптов и эксплойтов, нацеленных на инфраструктуру или продукты Заказчика

Информационно-справочные модули ETHIC

КОНТРАГЕНТЫ (скоринг юридического лица)

Автоматизированный поиск и анализ информации о юридическом лице в открытых источниках, а также в собственном реестре неблагонадежных компаний.

Модуль позволяет выявлять не только фирмы-однодневки, но и выставленные на продажу юридические лица, имеющие долгую и хорошую репутацию, необходимые лицензии и коды ОКВЭД, не замеченные ранее в участии в сомнительных схемах

ПРОВЕРКА

Получение сведений об электронных идентификаторах на основе анализа общедоступных онлайн-источников информации.

Формирование отчета занимает от нескольких секунд до двух-трех минут. Возможна пакетная загрузка и обработка массивов данных

ВАЖНО: Модули «Контрагенты» и «Проверка» представляют собой автоматизированные информационно-справочные системы. Достоверность информации, предоставляемой данными модулями, напрямую зависит от достоверности сведений, содержащихся в соответствующих реестрах и базах данных. Основное назначение модулей – сокращение времени, требуемого на сбор и анализ информации из публичных источников. В случае, если предоставленная в рамках работы модулей информация требуется для принятия ответственного решения, мы рекомендуем заказывать комплексный аналитический отчет

INFOSECURITY
a Softline company

Оцените возможности модуля «Проверка»

Для доступа к сервису используйте адрес: HTTP://SCORING.CENTER

Секретный ключ доступа для слушателей вебинара: 1408

INFOSECURITY
a Softline company

Преимущества ETHIC

- простота работы и автоматизация рабочих процессов
- отсутствие нагрузки на инфраструктуру заказчика
- многоступенчатая верификация угроз опытными аналитиками
- модульность сервиса
- широкий перечень объектов мониторинга
- удобный интерфейс
- гибкость настройки с учетом специфики бизнеса заказчика
- оперативное реагирование на инциденты

У нас есть инструмент… и умелые руки!

INFOSECURITY
a Softline company

Спасибо за внимание!

По вопросам использования сервиса Вы можете обращаться:

Сергей Трухачев
руководитель блока специальных сервисов

раб.: +7 (499) 677-10-00 доб. 10-4972
моб.: +7 (926) 229-45-40 |
e-mail: trukhachev@in4security.com

INFOSECURITY
a Softline company