

 sp.group-ib.ru

SECURE PORTAL

Проактивное обнаружение
онлайн-мошенничества на всех
устройствах клиента в режиме
реального времени



Защита личных
кабинетов
пользователей



Выявление
и блокирование
бот-активности



Предотвращение
бонусного
мошенничества



ЗАЩИТА ОТ ВСЕХ ВИДОВ ОНЛАЙН-МОШЕННИЧЕСТВА В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Используя данные из уникальных источников, технологию цифрового “отпечатка” устройства и собственные решения на базе машинного интеллекта, Secure Portal предотвращает ущерб, проактивно выявляя подготовку мошенничества на стороне пользователей интернет-порталов.

Блокирование действий ботов

Shell-боты, веб-боты и бот-сети для сбора данных, подбора паролей и несанкционированных действий на сайте.

Защита личных кабинетов

Несанкционированный доступ в аккаунты пользователей, захват учетной записи.

Обнаружение бонусного мошенничества

Кража бонусных баллов и миль авиакомпаний, множественная регистрация аккаунтов.

Отслеживание кросс-канального мошенничества

Кросс-канальные атаки на онлайн-порталы и мобильные приложения.

Выявление социальной инженерии

Мошенничество через социальные сети, мошеннические рассылки и подложные сайты.

Противодействие платежному мошенничеству

Использование P2P-страниц для хищения, CNP-мошенничество, автоматическая подмена реквизитов платежа, возмещения (chargebacks).

Всего за 24 часа Secure Portal дополнительно обнаружил 150 000 запросов ботов, производивших несанкционированные действия на популярном ecommerce-сайте, который уже использовал средство по блокировке ботов.

В качестве источника данных Secure Portal использует уникальную информацию из GIB Threat Intelligence, включая сведения:

- о скомпрометированных банковских картах и личных кабинетах
- о подозрительных IP-адресах
- о новых мошеннических схемах и методах

ИНДИВИДУАЛЬНЫЕ РЕШЕНИЯ ДЛЯ ИНТЕРНЕТ-БИЗНЕСА ИЗ ЛЮБОЙ ИНДУСТРИИ



Интернет-магазины



Развлекательные сервисы



Госуслуги



Страховые компании



Криптовалютные проекты



Сайты с платным контентом



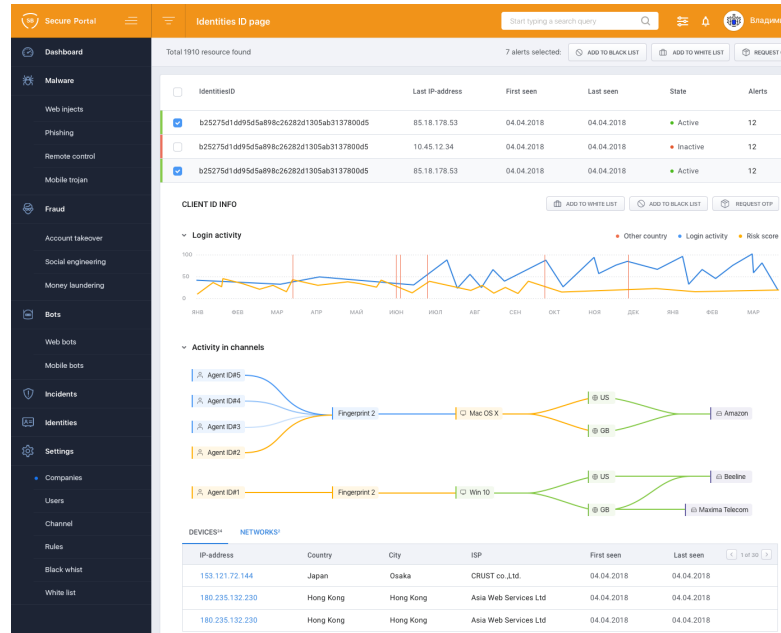
Туристические сервисы



Корпоративные порталы

КАК РАБОТАЕТ **SECURE PORTAL**

- 1** Secure Portal загружается вместе с веб-страницами сайта и мобильным приложением незаметно для пользователя.
- 2** Модуль собирает индикаторы мошеннической активности и передает их по защищенному каналу в серверную часть Secure Portal.
- 3** В случае выявления фактов мошенничества Secure Portal незамедлительно информирует заказчика.



Наглядные отчеты с обогащенным контекстом угроз позволяют отслеживать изменения в динамике и характере атак

SECURE PORTAL ПОМОЖЕТ **ЗАЩИТИТЬ ВАШ БРЕНД**

Для хищения учетных записей и данных банковских карт мошенники создают поддельные сайты портала. Многие из них просто делают копию сайта.

Если код оригинального сайта содержит модуль Secure Portal, при заходе первого пользователя на мошенническую копию, модуль сообщит доменное имя этого сайта.

Мы передадим доменное имя Центру круглосуточного реагирования CERT-GIB, который, после вашего подтверждения, оперативно заблокирует фишинговый ресурс.

КОМПЛЕКС АНТИФРОД-ТЕХНОЛОГИЙ ДЛЯ ВЫЯВЛЕНИЯ ВСЕГО СПЕКТРА УГРОЗ

- Поведенческий анализ
- Цифровой «отпечаток» устройства
- Безагентное обнаружение вредоносных программ
- Продвинутый конструктор правил
- Адаптивная аутентификация
- Кросс-канальная аналитика

**ПРОСТАЯ
ИНТЕГРАЦИЯ**



GBG

ArcSight
An HP Company

Intellinx
Insider Threat Intelligence

POSITIVE TECHNOLOGIES



ssas





Group-IB – один из ведущих мировых разработчиков решений для детектирования и предотвращения кибератак, выявления фрода и защиты интеллектуальной собственности в сети

15 лет

**ПРАКТИЧЕСКОГО
ОПЫТА**

55 000+

**ЧАСОВ
РЕАГИРОВАНИЯ**

1 000+

**РАССЛЕДОВАНИЙ
ПО ВСЕМУ МИРУ**

300+

**СПЕЦИАЛИСТОВ
И РАЗРАБОТЧИКОВ**

Официальный
партнер



Group-IB входит в число лучших мировых поставщиков Threat Intelligence по версии Gartner, IDC, Forrester, Cyber Defense Magazine и SC Media.

Эксперты Group-IB проводили тренинги профессионального развития для специалистов Europol, INTERPOL, правоохранительных органов, корпоративных команд безопасности и преподавателей университетов в Великобритании, Германии, Нидерландах, Бельгии, Франции, Таиланде, Бахрейне и Ливане.

УЗНАЙТЕ БОЛЬШЕ

о возможностях
Secure Portal
sp.group-ib.ru

СВЯЖИТЕСЬ С НАМИ

Чтобы провести
тест-драйв Secure Portal
sp@group-ib.ru

ПОЗНАКОМЬТЕСЬ С GROUP-IB

group-ib.ru
facebook.com/GroupIB

СЕРВИСЫ GROUP-IB

Укрепите кибербезопасность с помощью опытных специалистов, погруженных в реагирование и расследование актуальных атак и имеющих доступ к одной из самых современных систем слежения за киберугрозами в мире.

АУДИТ И ОЦЕНКА РИСКОВ

- Тестирование на проникновение
- Исследование уязвимостей
- Анализ исходного кода
- Compromise Assessment
- Red Teaming
- Pre-IR Assessment
- Оценка соответствия

THREAT HUNTING И РЕАГИРОВАНИЕ

- Managed Threat Hunting
- АРТ-мониторинг
- Криминалистическое реагирование (целевые атаки, утечки и др.)
- Оперативное реагирование (фишинг, DDoS, нарушение прав на интеллектуальную собственность и др.)
- Реагирование «по подписке»

КРИМИНАЛИСТИКА

- Сбор цифровых доказательств
- Криминалистический анализ
- Анализ вредоносного кода

РАССЛЕДОВАНИЯ

- Целевые атаки
- Инциденты информационной безопасности
- Финансовые и корпоративные преступления