BlockchainKZ community

CSAI Group

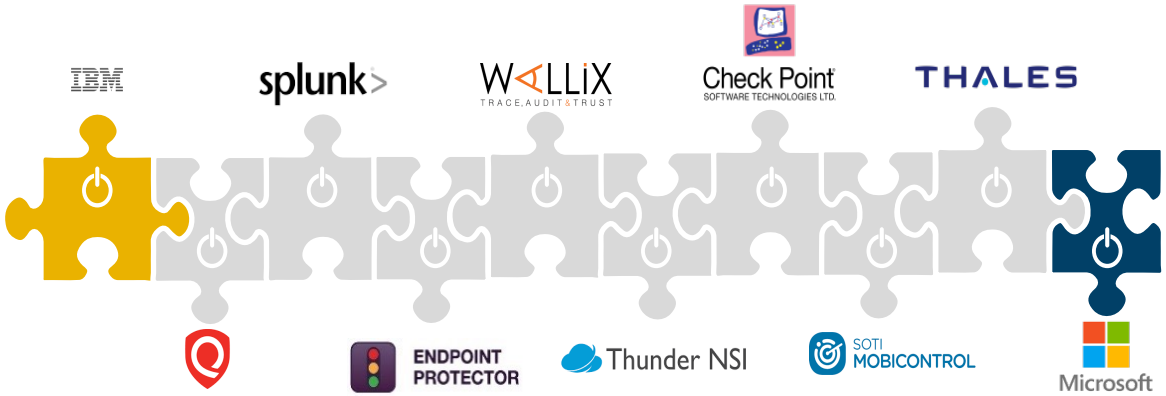
Ваш партнер кибер-защиты

Экспертиза. Опыт. Надежность

О нас

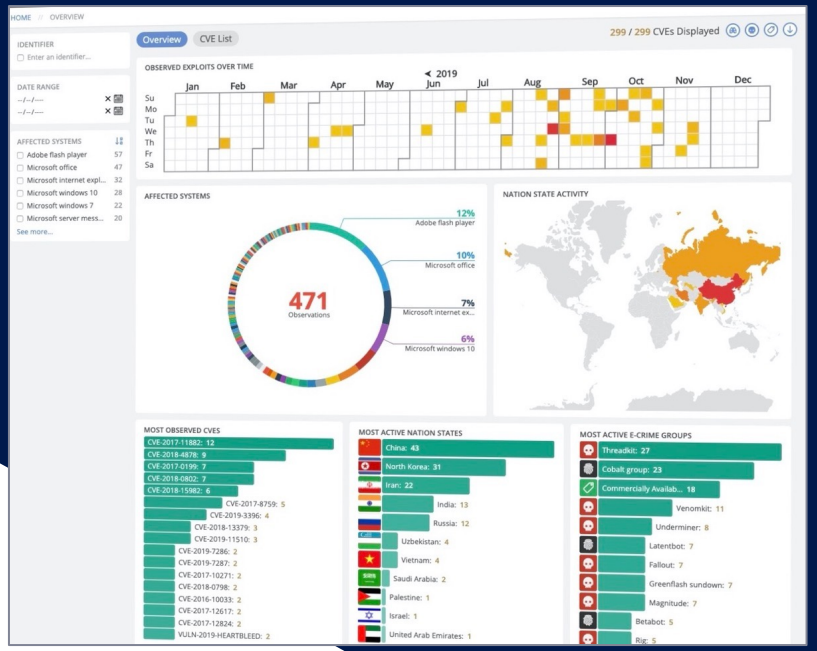
комплексный интегратор —
нам доверяют IBM, Microsoft, Checkpoint

- ✓ Наши специалисты имеют более семи лет сфокусированного опыта в кибер-безопасности
- ✓ Простые, надежные и интеграционные решения внедрены в более чем 20 проектах в СНГ
- ✓ Наши решения отразили более 1 млрд. атак



О нас

- Мы имеем собственную разработанную платформу в области Кибербразведки



CSAI GROUP - ведущая компания в области исследования и предотвращения киберугроз. Мы успешно расследуем высокотехнологичные преступления за счет использования собственной уникальной платформы, применения проверок безопасности компьютерных систем и внедрения решений собственной разработки в области разведки угроз

OFFENSIVE security OSCP

Open Source Intelligence Reconnaissance Surveillance Report OSINT Investigations

CISSP® Certified Information Systems Security Professional

European Bank for Reconstruction and Development
Аккредитованный консультант

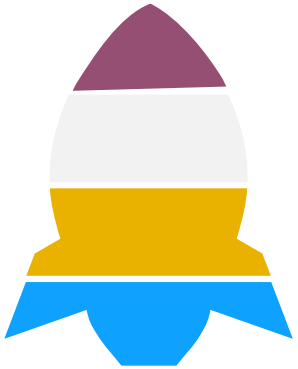
cisco Solution Partner

CARNEGIE MELLON UNIVERSITY CERT IS A REGISTERED TRADEMARK OF CERT AUTHORIZED TO USE CERT Software Engineering Institute Carnegie Mellon University

Наши стратегические партнеры

BlockchainKZ community

Kcell



European Bank
for Reconstruction and Development

Аккредитованный консультант

Глобальные риски

Хакер — это не один человек,
вас атакуют организованные группы

288 млрд $

Рынок наркотиков

2,1 трлн $

Международный рынок киберпреступлений

+

114 млрд $

Рынок краденых кредитных карт

56 млрд $

Рынок краденных машин

30 млрд $

Рынок краденных смартфонов

?

Ущерб от правительственных атак

Актуальные угрозы

Угрозы для порталов операторов связи и сопряженных веб-ресурсов

- Атаки отказа в обслуживании (DDoS-атаки);
- Компрометация данных клиентов при использовании web-сервисами;

Угрозы, связанные с организацией внутренних процессов

- Отсутствие четкого плана реагирования на инциденты;
- Слабая защищенность персонала от социотехнических воздействий;

Угрозы репутаций и бренду операторов связи

- Поддельные аккаунты и группы в социальных сетях;
- Фишинговые и мошеннические сайты, незаконно использующие бренд или схожее доменное имя;
- Мошеннические опросники, собирающие деньги с обманутых клиентов от имени компании;

Целевые атаки на внутреннюю сеть телекоммуникационной компании

- Распространение вредоносного ПО;
- Компрометация конфиденциальных данных;
- Остановка или нарушение работы внутренних систем и сервисов;

Атаки на устройства на данные клиентов операторов связи

- Угрозы финансово мотивированного мошенничества;
- Несанкционированный доступ в личные кабинеты пользователей;

Угрозы финансового мотивированного мошенничества

- Вывод, кража и обналичивание цифровой валюты клиентов;

Вирус уже здесь!

Кибератаки в Казахстане: с 2018 года зафиксировано более 2 миллиардов кибератак
На 2021 год по статистике KZ CERT кибератак увеличилось в 4 раза

Основные шаги в достижении Информационной безопасности

Предупреждение атак, постоянное обновление систем, цифровая гигиена сотрудников – основа защиты. Каждая новая ИТ-технология — это угроза!

Инфраструктурные факторы: кибер-террористы каждый день изобретают новые зловредные ПО, способные вывести из строя промышленные объекты. Важно:

- ✓ Регулярно проводить аудит на анализ уязвимостей системы;
- ✓ Независимыми силами анализировать возможность проникновения хакерами и новые каналы утечки информации;
- ✓ Регулярно обновлять программные обеспечения;
- ✓ Развивать и поддерживать эффективную инфраструктуру.

Человеческий фактор: большая часть крупнейших современных атак была результатом неосторожности или недостаточной компетентности сотрудников. Важно:

- ✓ Постоянное повышение компетентности сотрудников по кибер-безопасности;
- ✓ Обучение всех работников цифровой гигиене и регулярное тестирование знаний;
- ✓ Проведение «тестового» аудита с рассылкой «зараженного» письма и анализом ситуации.

Наши решения

- Сетевая безопасность
- Защита от целенаправленных атак
- Промышленная безопасность
- Threat Intelligence (собственная разработка)
- Контроль привилегированных пользователей (администраторов, контрагентов, удаленных разработчиков)
- Видение атак, системы анализа и сбора логов
- Автоматизация реагирования на угрозы
- Системы идентификации, аутентификации, контроля доступа
- Защита от утечки данных
- Защита и управления конечными устройствами
- Сканер уязвимостей
- DevOps Security
- Корпоративное аналитическое хранилище данных
- Системы противодействию мошенничества
- Платформа для обучения осведомленности информационной безопасности
- Шифрование баз данных, почты, чувствительной информации

Check Point SOFTWARE TECHNOLOGIES LTD.

FORTINET

WALLIX BASTION

FUDO SECURITY

CSAI Group

IBM

Microsoft

splunk>

MICRO FOCUS

SOTI

FireEye

exabeam

TREND MICRO

CROWDSTRIKE

Как мы можем вам помочь

Мы готовы предоставить весь спектр услуг
в области кибер-безопасности.

Тест на проникновение (Pentest)

Оценка зрелости процессов управления безопасностью

Анализ и оценка рисков

Формирование стратегии создания и развития кибербезопасности в организации

Внедрение решений и их поддержка

Обучение ваших специалистов

Тренинги офисных сотрудников кибербезопасности, отражение фишинговых атак

Кибербезопасность SCADA систем

Единственная интегрированная платформа безопасности по всему Казахстану!

CLAROTY

Check Point
SOFTWARE TECHNOLOGIES LTD.

АСУ ТП уязвима по умолчанию

Старая версия ОС

Отсутствие встроенной безопасности

Невозможно патчить

Слабый или пароль по умолчанию

Ландшафт угроз и векторы атак

Целевой фишинг

Таргетированный атаки

Традиционные ИТ угрозы

Криптомайнеры

Традиционные решения по ИБ бесполезны...

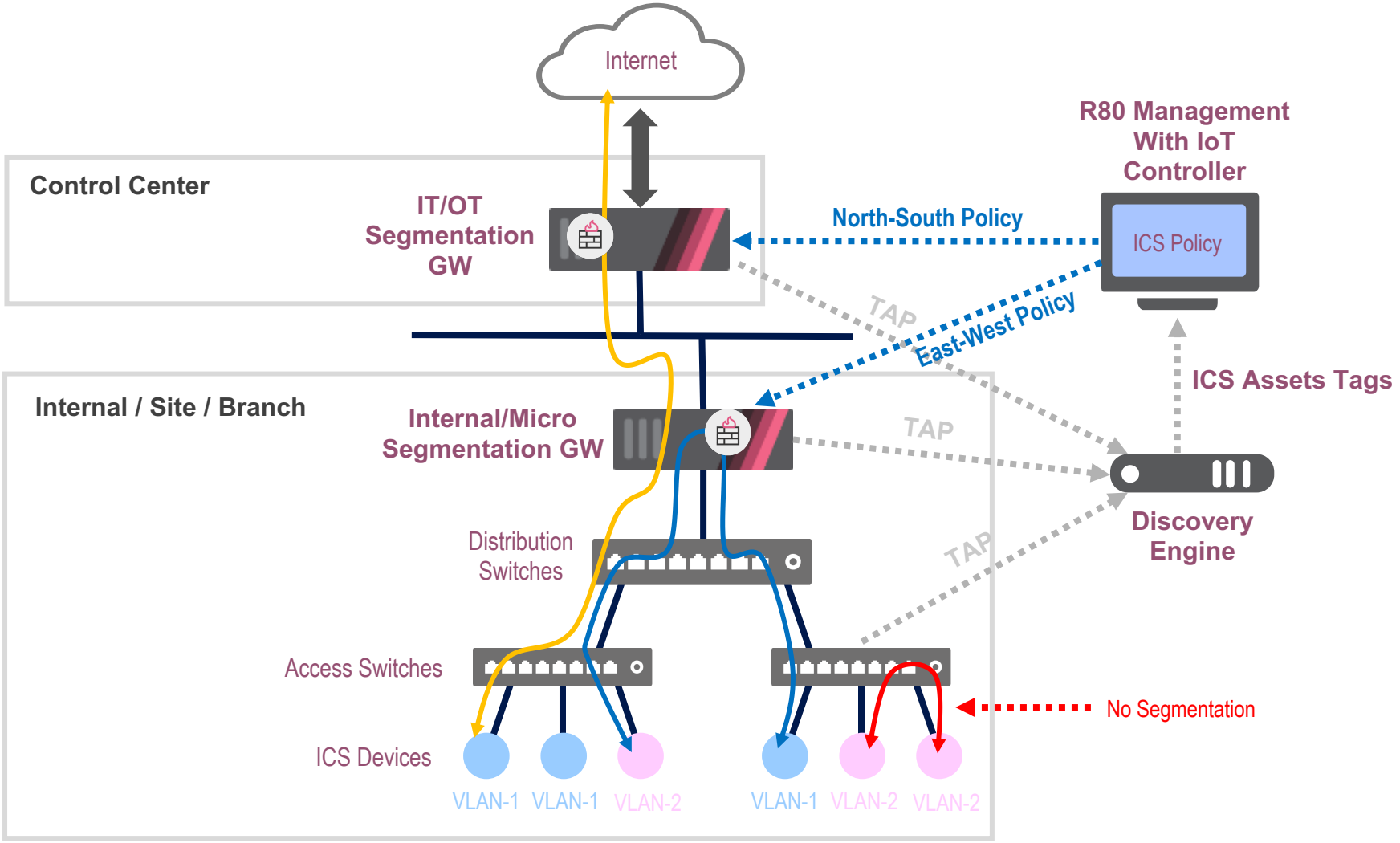
Какие риски для АСУ ТП в моей организации?
Нет информации об устройствах в АСУ ТП сети и их уязвимостям

Что передается по сети АСУ ТП?
Нет контроля целостности, контроля передаваемых команд, инспекции АСУ ТП трафика

Нет возможности детектировать и блокировать атаки
Отсутствует информация об угрозах для АСУ ТП

Ты не можешь защитить
то что ты не видишь и не понимаешь...

Топология решения



Мониторинг промышленной сети

Информация о взаимодействии

- Протоколы и команды
- Внутрисистемные связи
- Открытые и проприетарные протоколы

Информация об устройствах

- IP- и MAC-адреса
- Производитель устройства
- Тип устройства (PLC, HMI, рабочая станция, коммутатор, итд)
- Модель и серийный номер
- Версия прошивки

Информация о сети

- Какие устройства работают в вашей сети?
- Каким образом эти устройства взаимодействуют между собой и внешним миром?
- Существуют ли ошибки конфигурации и уязвимости?

Комбинированная защита

Настраиваемые политики

- **Фаза обучения** – анализ сетевого трафика и логов
- Ручная конфигурация нормального режима работы
- Специализированные политики для команд и значений
- Политики на основе временны*х* шаблонов трафика

Обнаружение аномалий

- **Фаза обучения** – автоматическое обнаружение устройств
- Поведенческий анализ на основе обнаружения аномалий
- Создание базисного профиля производственного процесса

Комбинированная защита на основе настраиваемых политик и обнаружения аномалий

Check Point 1570R

Производительность:

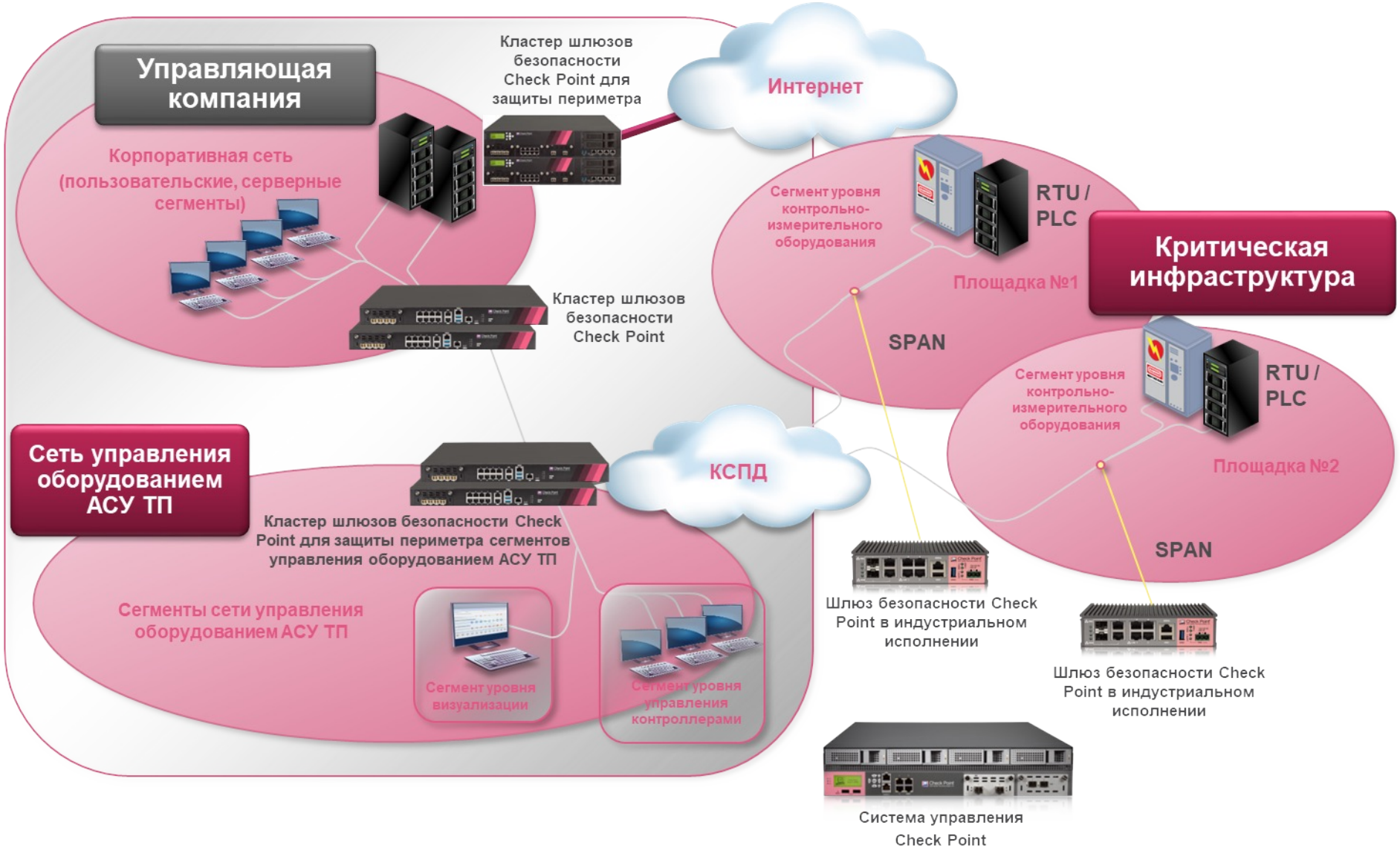
- 49 SecurityPower[1] Units
- Пропускная способность МСЭ 2 Гбит/с, 1518 байт UDP
- 700 Мбит/с МСЭ, смешанный трафик
- 60 Мбит/с МСЭ и IPS, смешанный трафик
- Пропускная способность VPN 450 Мбит/с
- 400,000 одновременных соединений

Соответствие требованиям:

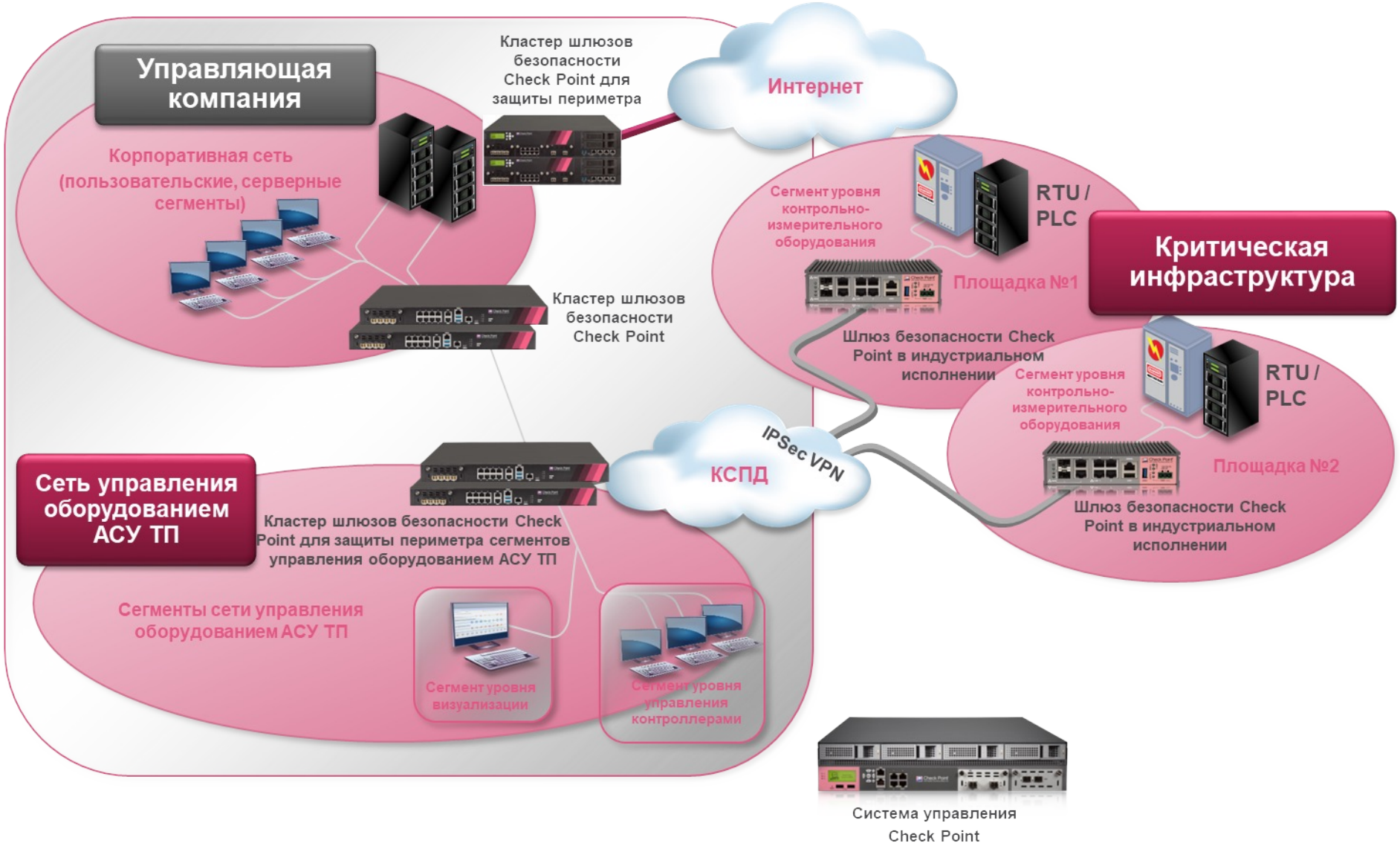
- IEEE 1613 , IEC 61850-3
- CE, EN 55024, EN 55022
- EN 61000-3, EN 61000-4
- CB, IEC 60950, UL 60950

- Температура и влажность:
  - от -40 до 75°C,
  - 20%-90%
- Соответствует промышленным стандартам по температуре, вибрациям, влажности и ЭМИ
- Отсутствие движущихся частей
- Гибкие варианты монтажа устройства
- Различные опции по питанию:
  - AC: 100-240V, 50 – 60 Hz
  - DC: 12V-72V, -48V DC

Архитектура индустриальной сети



Архитектура индустриальной сети



ПРОДУКТЫ И СЕРВИСЫ РАЗРАБОТАННЫ НАШЕЙ КОМАНДОЙ

- FS TI
- CROSSLINK
- FS MNG
- PATCH MANAGEMENT INTELLIGENCE (PMI)
- FS IRT
- FS PHISHING

Клиенты

- Мировые

European Bank
for Reconstruction and Development

Клиенты

- Казахстан

kaspi

HALYK BANK
НАРОДНЫЙ БАНК КАЗАХСТАНА

NITEC

europharma
СЕТЬ АПТЕК

СК-ФАРМАЦИЯ

САМҰРЫҚ-ҚАЗЫНА КОРПОРАТИВТІК УНИВЕРСИТЕТІ

KEGOC

TARLAN
PAYMENTS

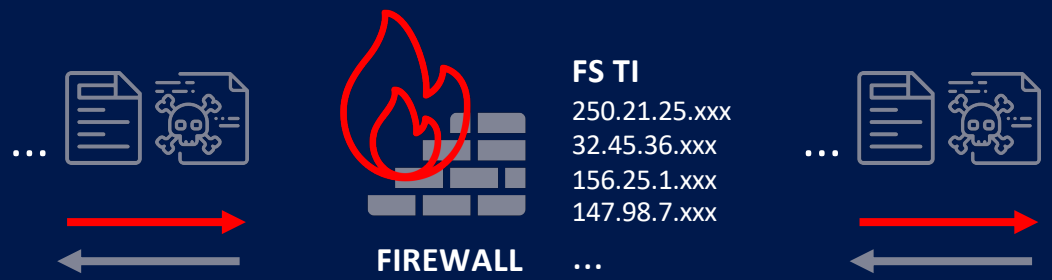
BASEL
СТРАХОВАЯ КОМПАНИЯ

FS TI

FS TI - это список из 30+ млн IP-адресов, который содержит анонимизированные IP-адреса в категориях TOR, PROXY & VPN, продающиеся как в публичном пространстве, так и в даркнете

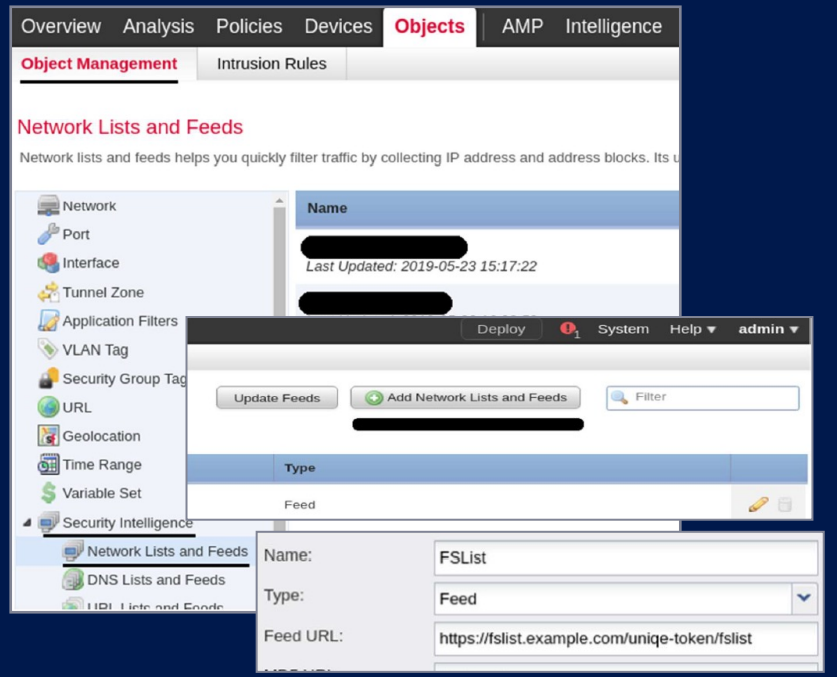
FS TI позволяет идентифицировать аномалии в сетевом трафике и трафике приложений и может быть использован различными способами

КАК FS TI ДОПОЛНЯЕТ КЛАССИЧЕСКИЕ РЕШЕНИЯ?



- Мгновенная интеграция в любую систему (VMWare ESXI, Firewalls, anti-fraud systems)

- Данные FS TI доступны через feed в форматах TXT, STIX, JSON, которые можно загрузить через API



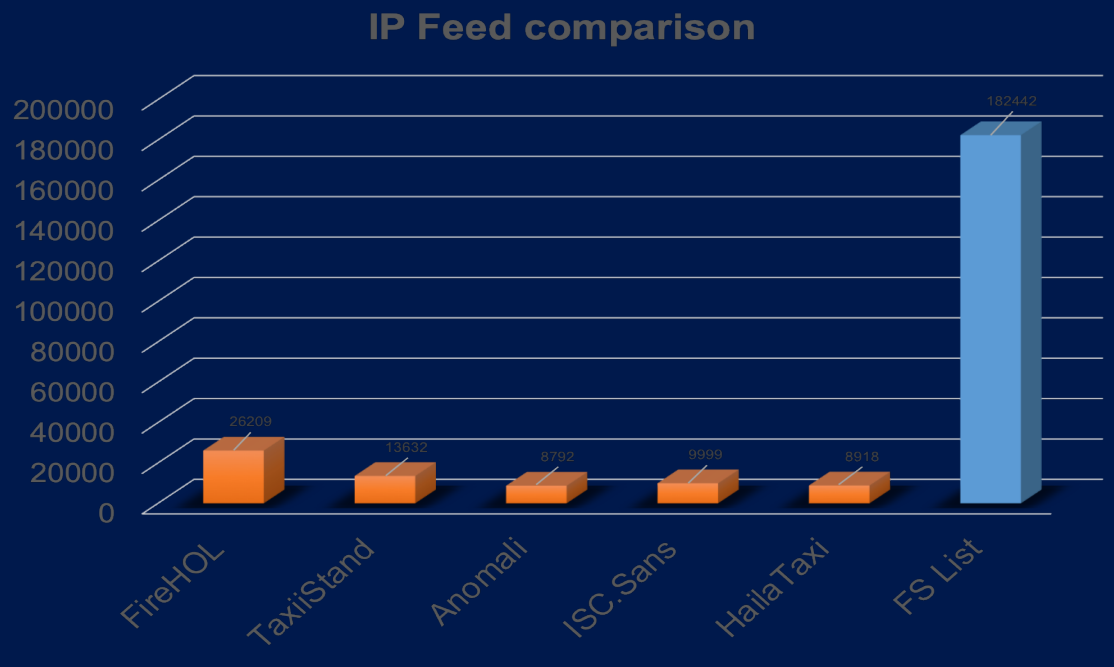
КАК FS TI ДОПОЛНЯЕТ КЛАССИЧЕСКИЕ РЕШЕНИЯ?

- Проактивный подход к сбору TI
- Больше информации для принятия решения
- Более раннее предоставление данных и тем самым предотвращение атаки
- Совместимость с решениями большинства вендоров
- Комплементарность с другими фидами

FS TI предоставляет anonymization IP, которые еще не внесены в black-листы других вендоров в качестве IOC/IOA
Данные IP начинают фигурировать в таких black-листах через 2-6 недель после того, как были опубликованы в FS TI

- ПЕРЕСЕЧЕНИЕ БАЗ ПОПУЛЯРНЫХ ВЕНДОРОВ С ИНФОРМАЦИЕЙ ОТ FS GROUP

32%	28%	7%	35%
CISCO per day	CISCO per week	PALOALTO Webroot	IBM X-Force



CROSSLINK

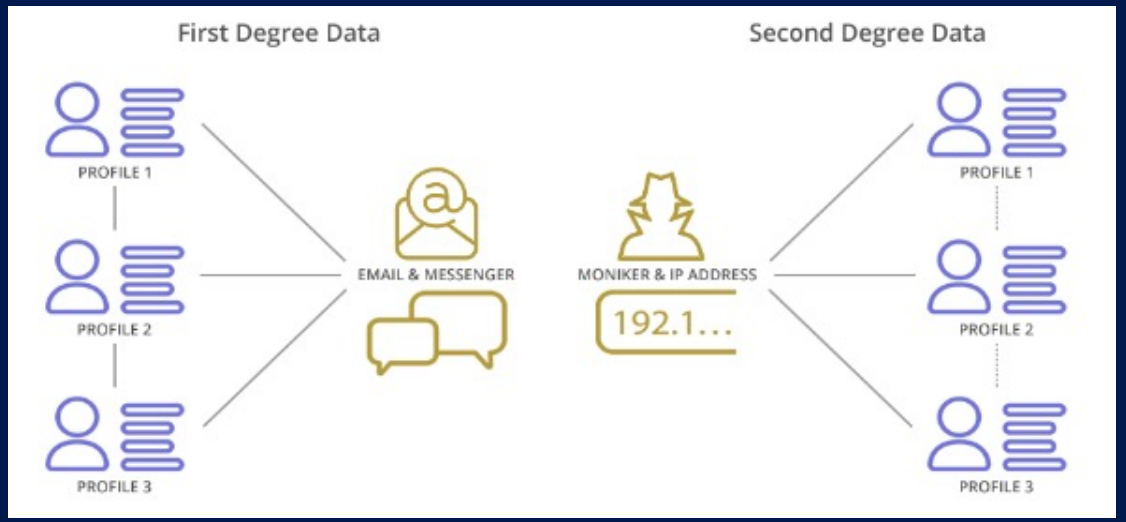
CROSSLINK - уникальная платформа, позволяющая аналитикам в сфере информационной безопасности исследовать индикаторы и находить информацию по ним в различных базах данных и ресурсах. Ресурсы могут включать сведения о профилях на общедоступных сайтах, сообщениях в мессенджерах, домены, которые зарегистрированы эктором, и другие

Цель **CROSSLINK** - помочь аналитикам деанонимизировать преступника и провести расследование

ИНДИКАТОРЫ

- Moniker (e.g. a nickname, alias, or username)
- Email
- IP Address
- Messenger (i.e. chat client address)
- Domain Name
- Phone Number
- Full Text

Используя корреляционные данные появляется возможность строить цепочки связей, иерархические структуры и обоснованно связывать цифровую личность с реальным человеком



CROSSLINK

CROSSLINK предоставляет доступ как через WEB-интерфейс, так и через ReSTful API. Это дает возможность, в том числе, взаимодействовать с платформой на программном уровне, например, ввести автоматическую проверку по e-mail сотрудников на предмет того, не задействованы ли они в противоправной киберактивности

Наличие информации о человеке в CrossLink не обязательно свидетельствует о том, что человек вовлечен в противоправную деятельность. Некоторые данные появляются в системе только потому, что они были скомпрометированы и продавались в Даркнете

CROSSLINK - РЕШЕНИЕ, КОТОРОЕ ВКЛЮЧАЕТ НА СЕГОДНЯ:

- Профили фигурантов киберинцидентов, вплоть до номеров паспортов и физического адреса
- Дампы ug форумов, джаббер-серверов, информация о публичных и приватных сообщениях из открытых и закрытых площадок и телеграм/IRC-каналов, используемых киберпреступниками для общения и координации своей деятельности
- Информацию о паролях киберпреступников в открытом виде, которая получена с использованием собственного кластера для получения паролей из хешей, что позволяет идентифицировать связанные аккаунты путем анализа открытого пароля либо корня пароля
- Информацию о регистраторах доменов (Whois)
- Passive DNS
- Геолокации IP и репутационные данные

CROSSLINK 4.22.1

Know More.

Choose your search type

KEYWORD(S) CONTAINS Enter a keyword or phrase...

- KEYWORD(S)
- FULL NAME
- MONIKER
- EMAIL
- PASSWORD
- PHONE NUMBER
- IP ADDRESS
- DOMAIN

ooking for more options? Try the new Advanced Search section.

USER GUIDES

Read the guides to learn the ins and outs of the application, enabling you to make the most of this tool.

START INVESTIGATING

Choose your search type and term in the bar above and hit enter or click the search button to begin.

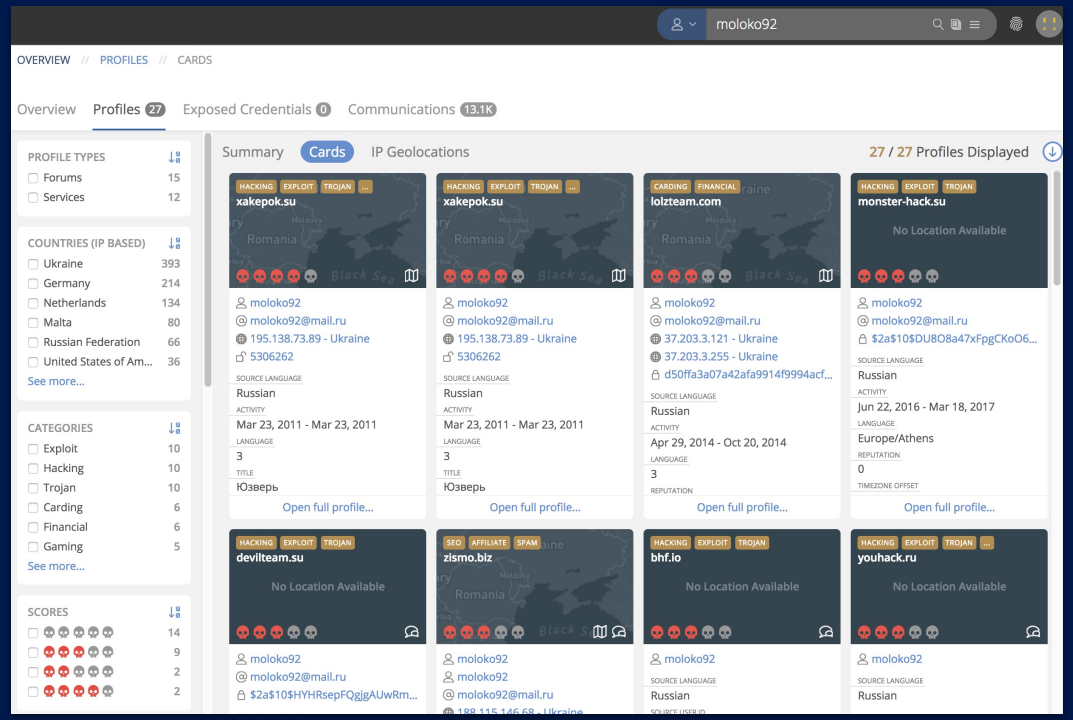
GLOSSARY

Find definitions for commonly used terms within the application.

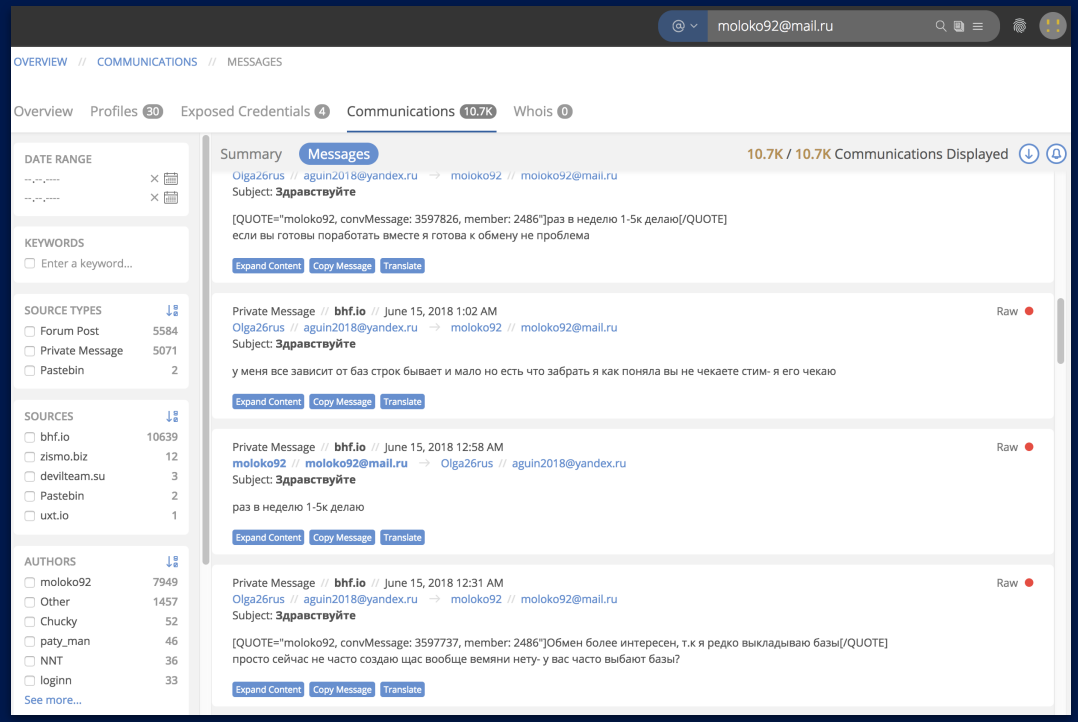
CROSSLINK

ПРИМЕРЫ ПОИСКА ПО РЕАЛЬНЫМ КЕЙСАМ

1. Производим поиск по интересующему псевдониму



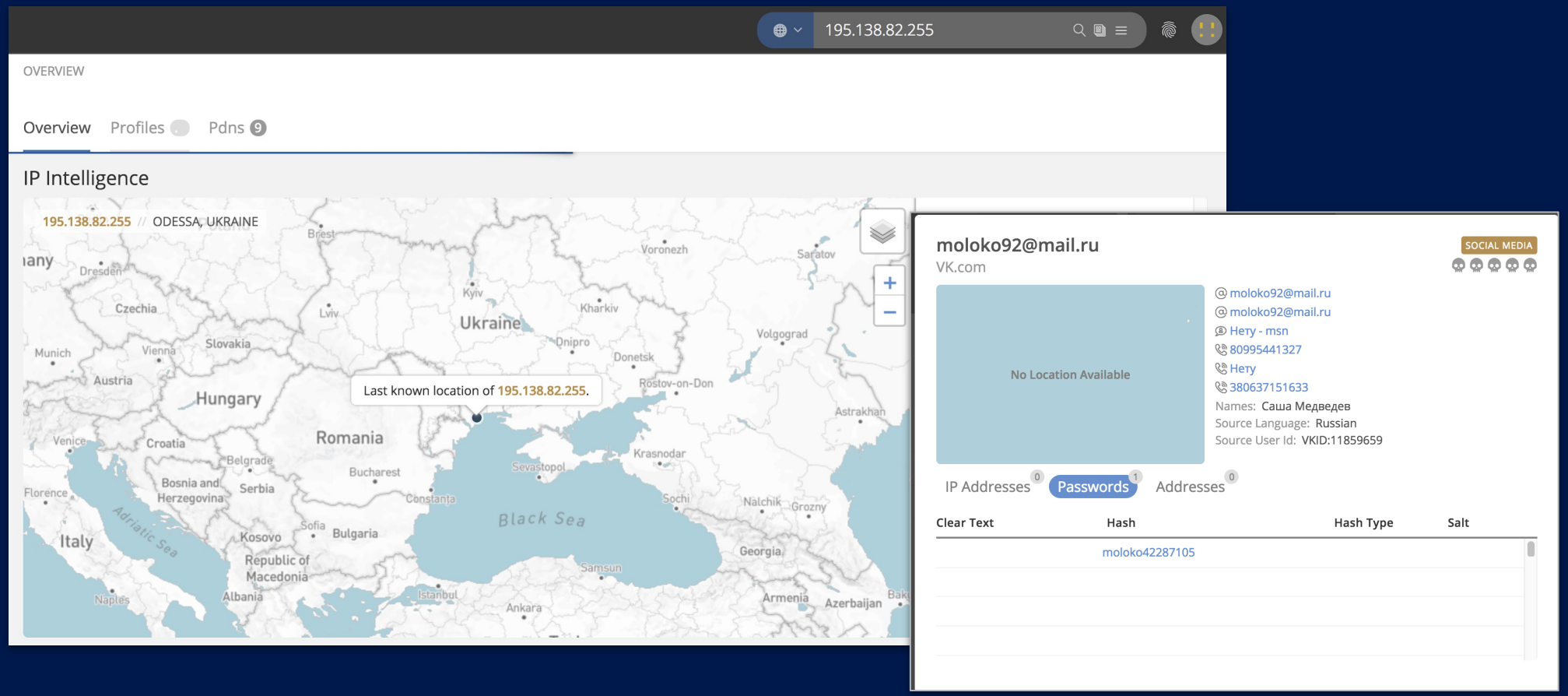
2. Получаем выдачу всех его сообщений на форумах и дополнительную информацию



CROSSLINK

ПРИМЕРЫ ПОИСКА ПО РЕАЛЬНЫМ КЕЙСАМ

3. Находим информацию, которая связывает человека, псевдоним и его IP-адрес



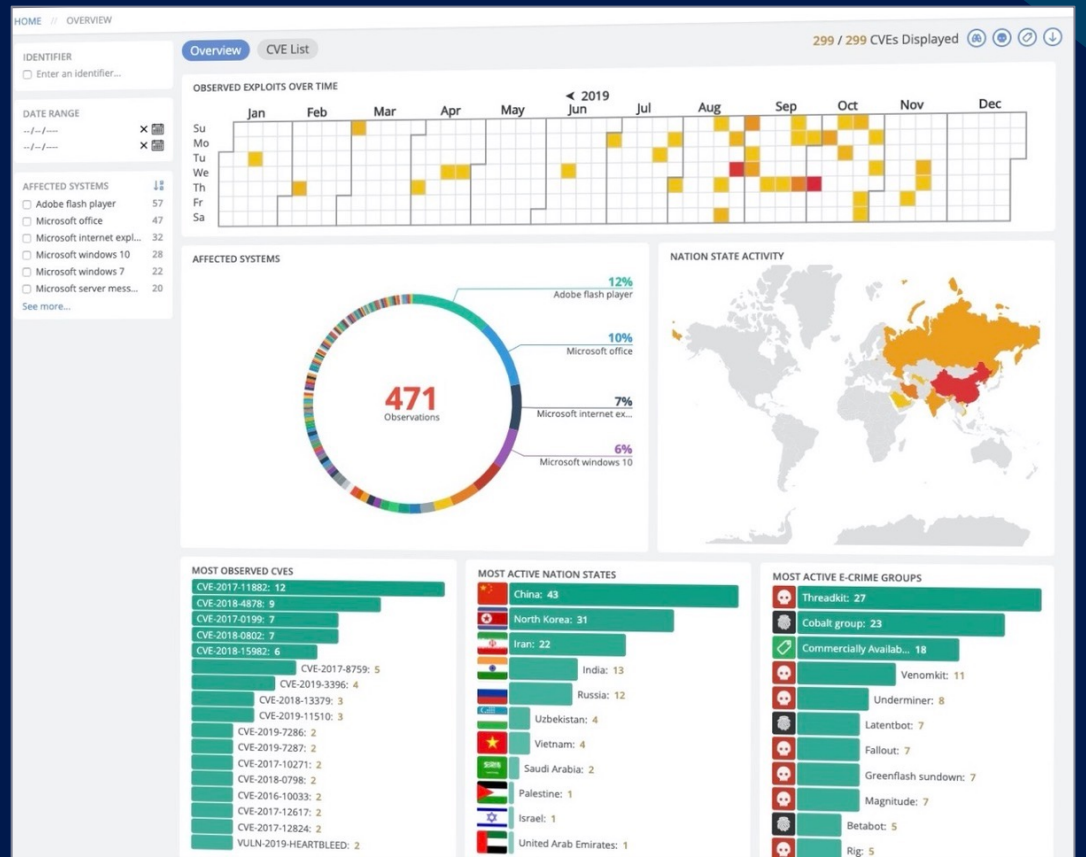
PATCH MANAGEMENT INTELLIGENCE

PATCH MANAGEMENT INTELLIGENCE (PMI) - продукт, состоящий из совокупности данных о текущих Vulnerabilities and Exploitations (CVEs) (общеизвестных уязвимостях ИБ), используемых APT-группами, с указанием географической принадлежности этих групп. Продукт объединяет экспертизу и результаты исследований CSAI Group в отношении киберпреступных групп и специализированных хакерских подразделений силовых структур по всему миру. Также продукт соотносит известные уязвимости с конкретными агентами угроз (людьми или организациями) из нашей базы данных

Для выявленных уязвимостей PMI поставляет данные о:

- результатах разведки хакерской активности, пораженных системах и версиях ПО
- информацию о патчах и способах устранения уязвимостей
- информацию об агентах угроз (людях или группах), использующих данные уязвимости

В отличие от других продуктов на рынке, PMI предоставляет не весь список уязвимостей, существующих на данный момент, а список уязвимостей, активно используемых киберпреступниками и государственными хакерскими группами в своих атаках



FS MNG

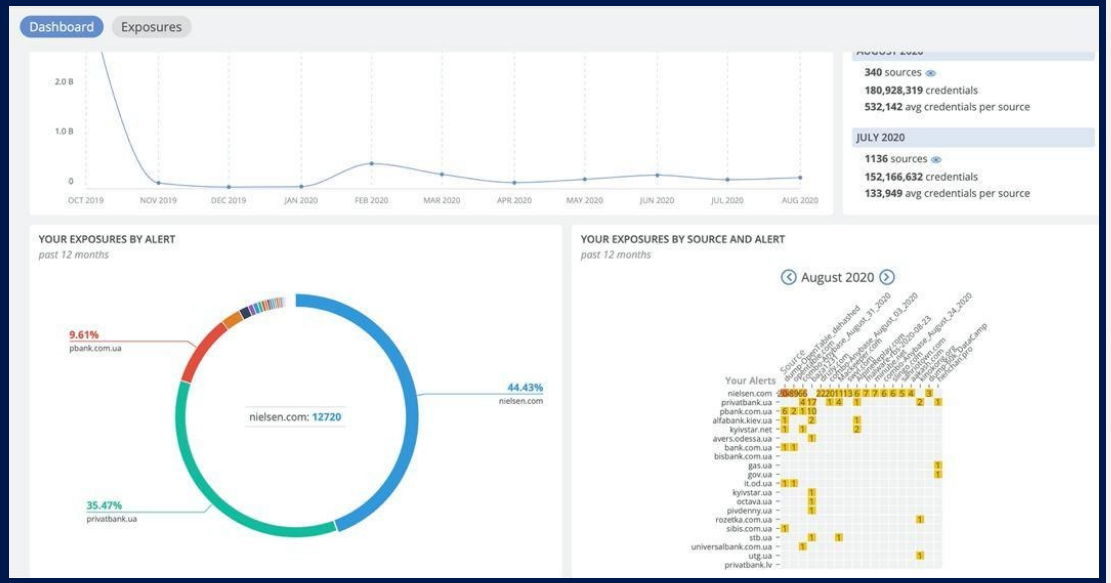
FS MNG - мониторинг наличия скомпрометированных аккаунтов, хостов или учетных данных клиента в открытых и закрытых источниках

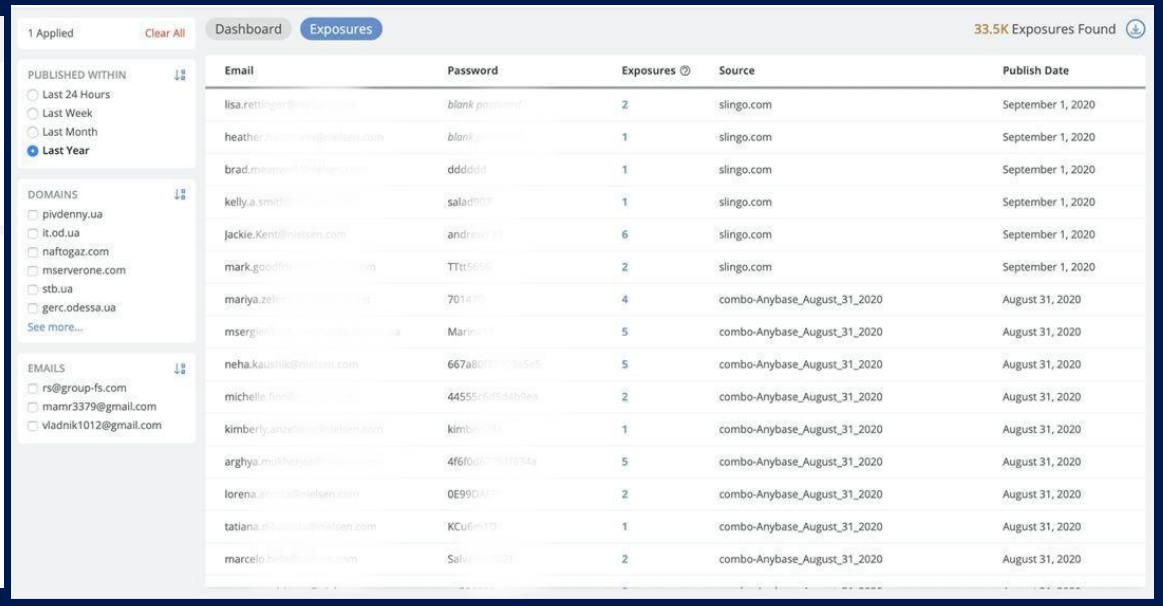
ACTIVE FEED

Новые данные постоянно добавляются в фид, по мере того, как они обнаруживаются в DarkNet

REAL-TIME ALERTS

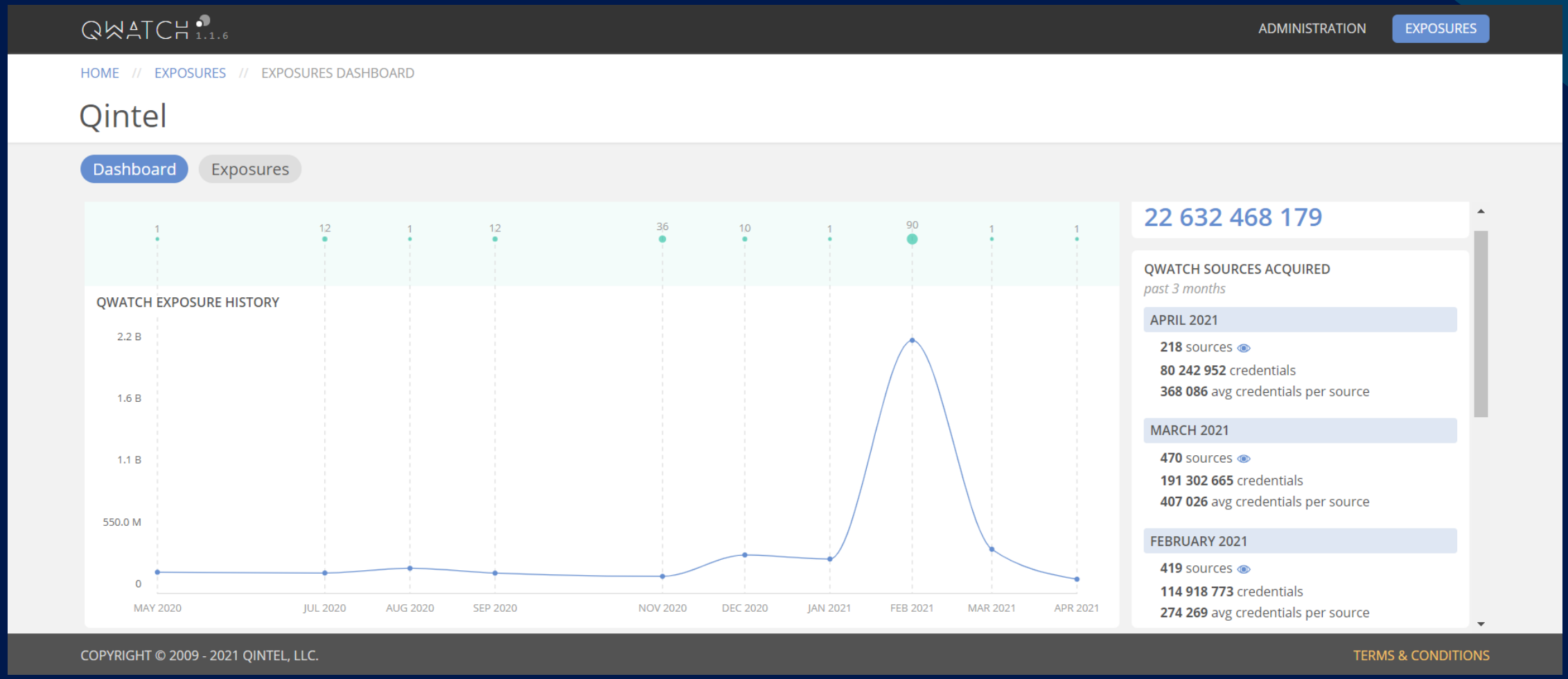
Мониторинг конкретных емейлов и доменных имен, чтобы отслеживать, не были ли соответствующие аккаунты скомпрометированы





FS MNG

Графическая отчетность по утечкам



FS PHISHING

FS PHISHING - симулятор рассылки фишинговых писем с целью понимания вероятности успешной фишинговой атаки на клиента и планирования активностей для повышения уровня образованности сотрудников для противодействия фишинговым атакам.

- **ИНТЕГРАЦИЯ ВНУТРИ КОРПОРАТИВНОЙ СЕТИ**
  Важно для крупных компаний, которые не желают передавать информацию о сотрудниках в облачные решения

- **ПОЛЬЗОВАТЕЛЬСКИЕ ТЕКСТЫ В ПИСЬМАХ**
  Формирование фишинговых писем максимально универсально. Система не ограничивает вид писем

- **РАЗРАБОТКА ФИШИНГОВЫХ СТРАНИЦ ПОД КЛИЕНТА**
  Гибкая настройка системы под ресурсы компании, чтобы атака проходила наиболее реалистично

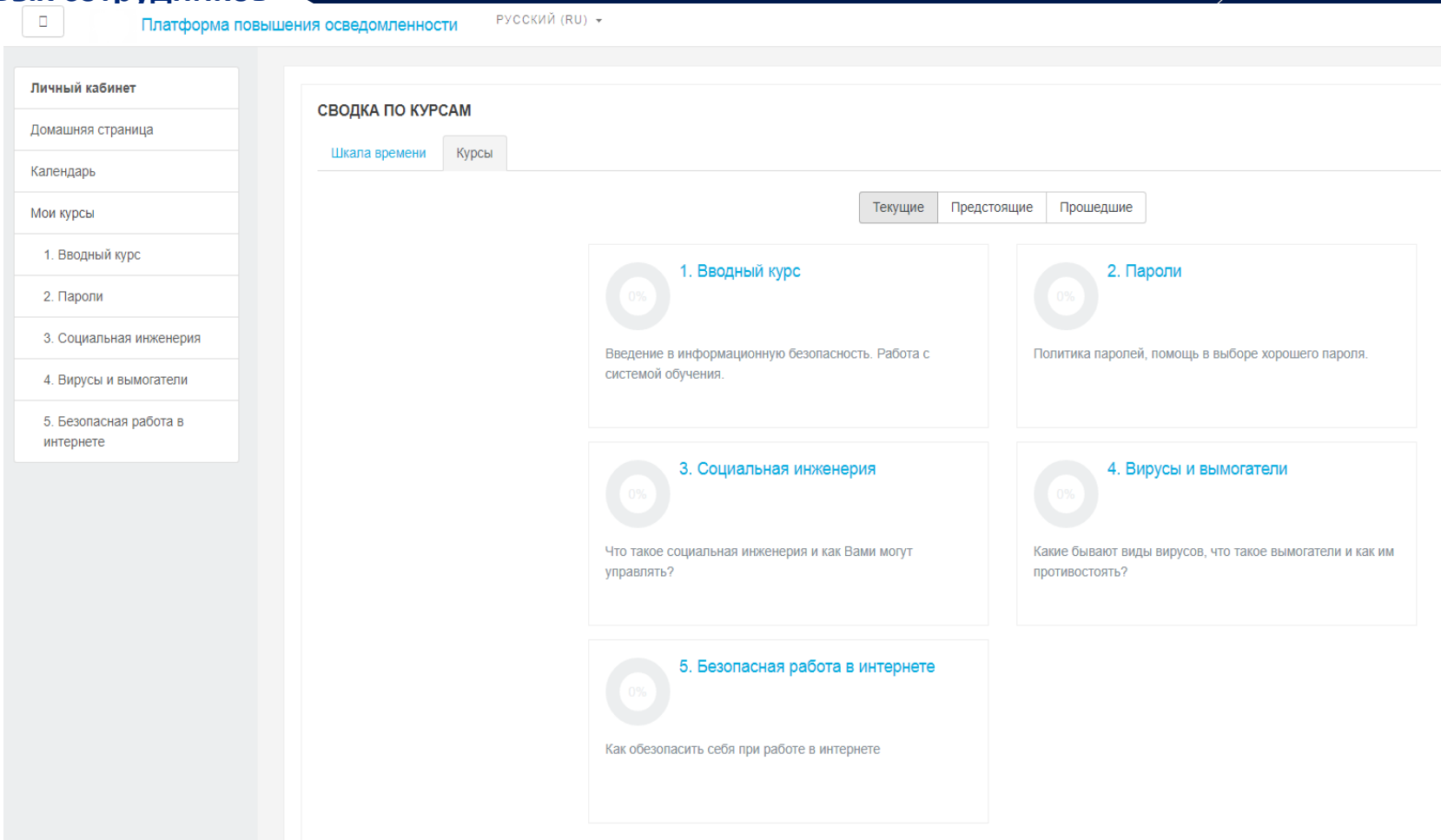
- **НАСТРОЙКА СИСТЕМЫ ПОД ПОЧТОВЫЙ СЕРВЕР ИЛИ КЛИЕНТ**
  При интеграции клиента мы настраиваем взаимодействие с корпоративными почтовыми решениями для максимальной эффективности работы системы

АҚПАРАТТЫҚ САНА

• Казахстанская Платформа для повышения осведомлённости в области Информационной безопасности – «Ақпараттық сана»

ПЛАТФОРМА – это виртуальный класс, где можно одновременно развивать сотрудников из разных отделов, повышая их осведомленность по необходимым разделам, а также обучить новых сотрудников

1	Повышение знаний и осведомленности персонала
2	Систематизация контроля знания сотрудников
3	Выбор направления и материала по вашему усмотрению
4	Экономия средств - не нужно закладывать в бюджет командировочные расходы
5	Экономия времени - нет необходимости искать помещение для проведения обучения и контролировать явку учащихся
6	Возможность проводить массовое обучение в очень короткие периоды времени



IRT – Кибер армия

- Мы с Вами 24x7, лучшие специалисты в расследовании инцидентов кибербезопасности

В рамках минимального пакета услуг предоставляется:

КОНСАЛТИНГ СО СПЕЦИАЛИСТАМИ
От 10 часов в месяц:

- Предоставление информации с описанием и рекомендациями о наиболее актуальных и критических угрозах в киберсети;
- Практические рекомендации по защите систем в соответствии с методикой ISO27001 (услуга предоставляется единоразово при активации подписки);
- Intelligence (OSINT/CSINT) - информация о сотрудниках /потенциальных злоумышленниках из открытых и закрытых источников

- INCIDENT INVESTIGATION (расследование инцидентов)

До 60 часов работы фокус-группы по каждому инциденту

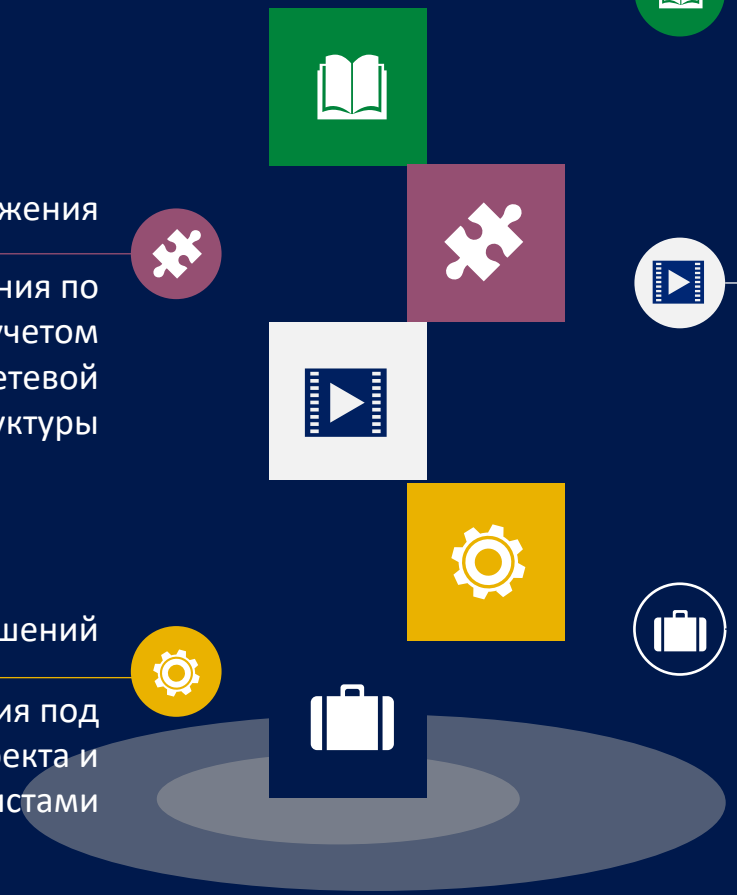
- CS CVE

Информация о уязвимостях с рекомендациями для повышения уровня защиты

- PENETRATION TESTING

(тестирование на проникновение)
От 2 тестов в год

Как мы работаем



1. Аудит

Проведения аудита на уязвимости существующей сети с помощью тестирования

2. Предложения

Формирование предложения по выявленным уязвимостям и с учетом планов компании по развитию сетевой инфраструктуры

3. Выбор решений

Подбор и согласование решений наиболее отвечающие требованиям компании заказчика и ликвидации существующих уязвимостей

4. Внедрение решений

Полный цикл внедрения решения под ключ, с нашим менеджментом проекта и техническими специалистами

5. Поддержка

Ежегодная поддержка внедренных решений на уровне L1, L2. Мы готовы предоставить поддержу 8x5 по локальному времени заказчика, а так же 24x7 на все внедренные нами решения

BlockchainKZ
community

CSAI Group

Контакты

+7777 619 2222

info@bkz.kz