Кибербезопасность здесь и сейчас

Шутбаев Жанибек

Руководитель отдела развития кибербезопасности в Softline в Центральной Азии

Повестка

1. Softline - эксперты в кибербезопасности
2. Современные киберугрозы в промышленном секторе
3. Карта услуг и сервисов
4. Вызовы ИБ и как SL на них отвечает
5. Реальные кейсы
6. Безопасность как сервис

1

SOFTLINE – ЭКСПЕРТЫ В КИБЕРБЕЗОПАСНОСТИ

Группа Компаний Softline

ГК Softline – ведущий поставщик решений и сервисов в области цифровой трансформации и ИБ, обладающий публичным статусом (MOEX, Ticker: SOFL)

Краеугольный камень цифровой трансформации (DX)

25+
Компаний в группе

> 5000
Производителей

> 100 000
Клиентов

Полный набор
Услуг и решений для цифровой трансформации

Ведущая ИТ компания в России

30+
Представительств в 6 странах

30
Лет на ИТ-рынке

> 1.3 млрд $
Оборот 2024

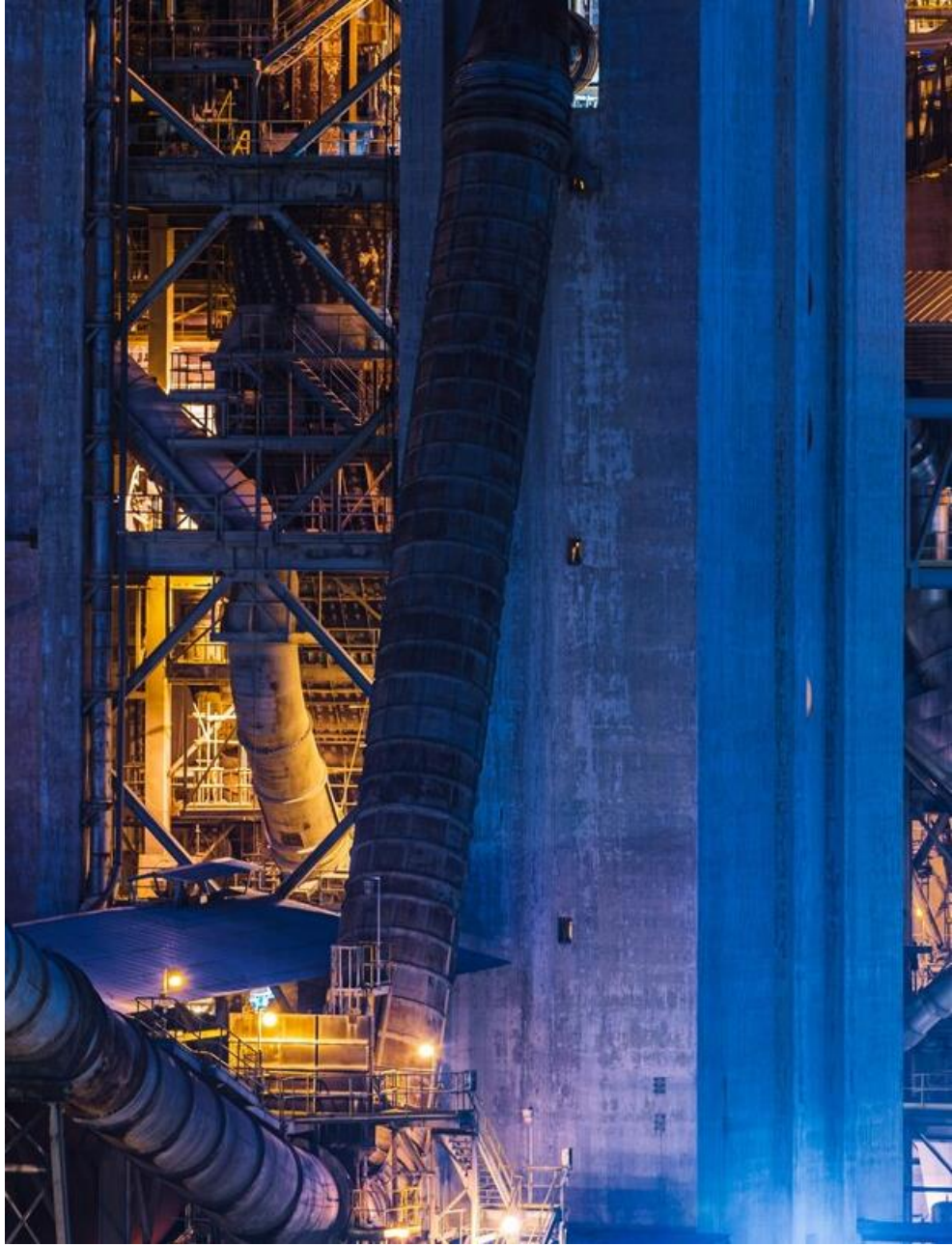
> 11100
Сотрудников

ГК Softline: Сервисы и решения

- Отраслевые решения
- Собственное ПО и аппаратные продукты
- Облачные решения
- Заказная разработка
- Информационная безопасность
- Премьер сервисы
- Softline Finance
- Системная интеграция
- Обучение и сертификация
- Техподдержка и аутсорсинг
- Современная гибридная инфраструктура
- ВКС
- СУБД
- САПР и ГИС
- Бизнес-решения

Современные киберугрозы в промышленном секторе

- **Атаки на АСУ ТП** – 32,5% промышленных систем в РК подверглись кибератакам. (Kaspersky)
- **Наиболее уязвимые отрасли** – нефтегаз (30%), энергетика (32%), логистика (11%). (Inbusiness)
- **Программы-вымогатели** – каждая 4-я атака связана с шифровальщиками, блокирующими работу предприятий. (Positive Technologies Security)
- **Фишинг и социальная инженерия** – основной метод взлома корпоративных систем. (Tengrinews)
- **Рост атак на предприятия** – за 2023 год число атак увеличилось на 25%. (Kapital.kz)



Мысли про «плохое» ИБ

Мешает: от паролей до долгого согласования любой мелочи

Пугает: вечно рассказывает про какие-то несуществующие угрозы

Тратит: инвестиции в те же самые несуществующие угрозы

Другая безопасность

Упрощает работу ИТ/ИБ-подразделений и бизнеса в целом

Окупается в понятные сроки и становится выгодной

Помогает увидеть и решить явные проблемы

2
КАРТА УСЛУГ И СЕРВИСОВ

Карта решений

Услуги и консалтинг

- Защита бренда в сети Интернет
- ISO27001
- Подготовка дорожной карты развития ИБ
- Awareness
- Услуги по аутсорсингу DLP (DLPaaS)
- Услуги по аутсорсингу NGFW (NGFWaaS)
- Услуги центра мониторинга и реагирования на инциденты ИБ (SOC)

Защита инфраструктуры

- Антивирусная защита серверов и рабочих станций
- Сетевая безопасность (NGFW/VPN/AntiAPT/FM)
- Сбор и корреляция событий (SIEM)
- Автоматизация процессов ИБ (SGRC/IRP)
- Защита почты
- Защита виртуальных сред
- Защита мобильных устройств (MDM)
- Защита промышленных сетей и АСУ ТП
- Защита веб-приложений (WAF)
- Управление уязвимостями (VM)
- Анализ кода
- Защита от DDoS

Контроль доступа и защита от утечек

- Защита от утечек информации (DLP)
- Управление жизненным циклом учетных записей (IdM)
- Многофакторная аутентификация (MFA)
- Контроль за привилегированными пользователями (PAM)
- Контроль использования облачных ресурсов (CASB)
- Аудит доступа к файловым ресурсам и управление неструктурированными данными (DAG)

Делаем ставки

- EDR/XDR/Песочницы
- Защита от направленных атак (APT)
- Анализ защищенности/Анализ кода
- Защита от утечки информации DLP
- Защита серверов, раб станций, виртуализации
- Сетевая безопасность (FW,IDS/IPS,VPN,FW management)
- Управление доступом (IDM, SSO,PKI)
- DataProtection as a service
- DLP as a service
- SIEM
- SOC
- Virtual CISO

3

ВЫЗОВЫ ИБ И КАК SL НА НИХ ОТВЕЧАЕТ

Нет ресурсов чтобы реагировать на инциденты ИБ

SOC

Атаки на сайты
+ DDoS

Пентест
WAF
AntiDDoS

Фейки/вбросы
в сети Интернет
про компанию

ETHIC

Слив внутренними сотрудниками ценных данных перед увольнением

DLP/DLPaaS

Отказ в ТП
или плохое
качество услуги

Переход
на ТП от SL

Не реализован проект по многофакторной аутентификации

Сделать проект по MFA

4
РЕАЛЬНЫЕ КЕЙСЫ

Переход на решения Лаборатории Касперского

Отрасль: Производство и продажа

Задача:
Подбор решений для защиты инфраструктуры (сеть, почта, конечные точки).

Решение:
Внедрение продуктов Kaspersky (KATA, KEDR, KSMG, KES и решений для серверов и виртуальных сред).

Результат:
- Успешная миграция без потери уровня защищенности с помощью наших специалистов
- Проект реализован в течение 1 года.

Внедрение PAM-системы для защиты привилегированных учетных записей

Отрасль: Крупный ритейл (торговля пищевыми продуктами)

Задача:
Контроль и защита доступа подрядчиков к критически важным ресурсам компании.

Решение:
Внедрение PAM для контроля привилегированного доступа и минимизации рисков утечек.

Результат:
- Централизованная система управления доступом.
- Снижение риска утечек и атак.
- Высокая удовлетворенность заказчика: дальнейшая закупка лицензий и дополнительных модулей.

Подключение к облачному SOC (ISOC 3.0) для банка

Отрасль: Финансовый сектор

Задача:
Внедрение процессов мониторинга и реагирования на инциденты ИБ в соответствии с требованиями регуляторов.

Решение:
Подключение к облачному SOC Softline, обработка угроз на мощностях провайдера.

Результат:
- Успешное соответствие требованиям ЦБ.
- Существенная экономия на поддержке собственного SOC.
- 24/7 мониторинг и реагирование

5

БЕЗОПАСНОСТЬ КАК СЕРВИС

Что о нас знает сеть?

Сервис **ETHIC** (External Threats & Human Intelligence Center) предназначен для выявления на ранних стадиях цифровых угроз бизнесу в глобальных сетях, что позволяет своевременно реагировать на угрозы, не допуская наступления негативных последствий или минимизируя их

Как работает?

Собирает информацию о компании

Изучает компанию и ее информационные активы

Выявляет угрозы и мониторит различные источники

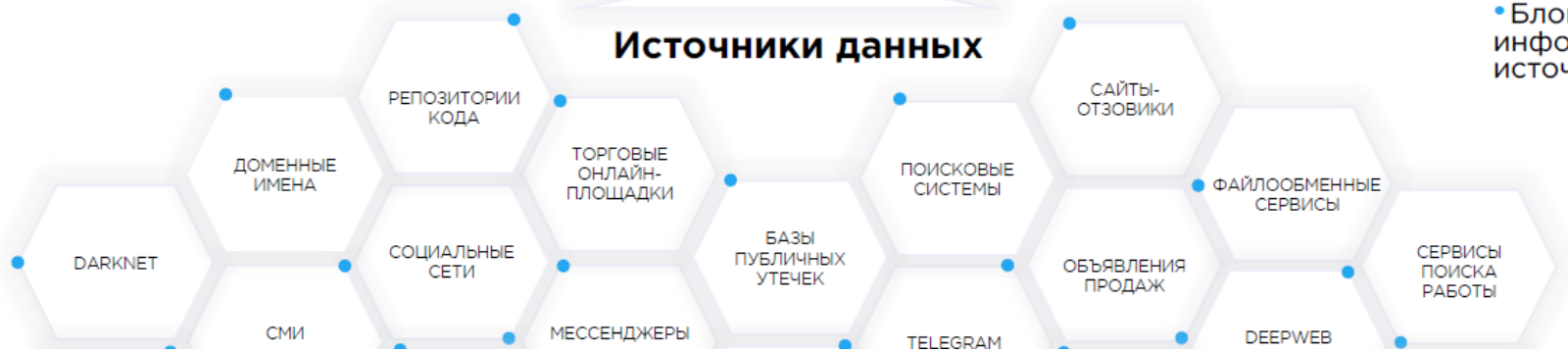
Использует автоматизированные средства для сбора, агрегации и первичного анализа данных

Обрабатывает данные и проводит кибер-расследования

Анализирует и верифицирует обнаруженные угрозы с помощью команды экспертов

Принимает меры реагирования на инциденты

- Оперативно уведомляет ответственных лиц Заказчика
- Взаимодействует с хостинг-провайдерами, регистраторами доменных имен, регуляторами и администраторами сетевых площадок
- Блокирует ресурс или изымает информацию из открытых источников (до 3 часов)



Сервис включает

DRP-платформу

Круглосуточно мониторит десятки миллионов ресурсов, выявляет потенциально опасную информацию, которая может навредить бизнесу, и фиксирует ее в веб-интерфейсе

Команду экспертов

Эксперты Infosecurity постоянно обрабатывают информацию об угрозах, оперативно устраняют найденные нарушения и расследуют сложные мошеннические схемы

Threat Intelligence

Кибербразведка (анализ угроз) является одним из столпов сервиса и направлена на выявление и реагирование на угрозы до того, как они будут реализованы и повлекут за собой ущерб

Примеры модулей

МОДУЛЬ	ОПИСАНИЕ
Домены	выявление фишинговых ресурсов, которые используются для осуществления противоправной деятельности в отношении компании или от его имени
Услуги	выявление объявлений о нелегальных услугах, затрагивающих интересы компании
Утечки	выявление в сети Интернет данных и документов ограниченного доступа, поиск фейковых мобильных приложений на маркетплейсах и иных ресурсах
Базы данных	выявление и анализ фактов продажи и/или размещения массивов данных, содержащих конфиденциальную информацию
Аккаунты	выявление учетных записей, пароли от которых были скомпрометированы и находятся в открытом доступе
Менеджмент	выявление фактов кражи личности ключевых сотрудников в социальных сетях
Медиа	выявление публикаций, содержащих упоминания Заказчика, на публичных ресурсах

Отчётность

В КОНЦЕ КАЖДОГО ОТЧЕТНОГО ПЕРИОДА

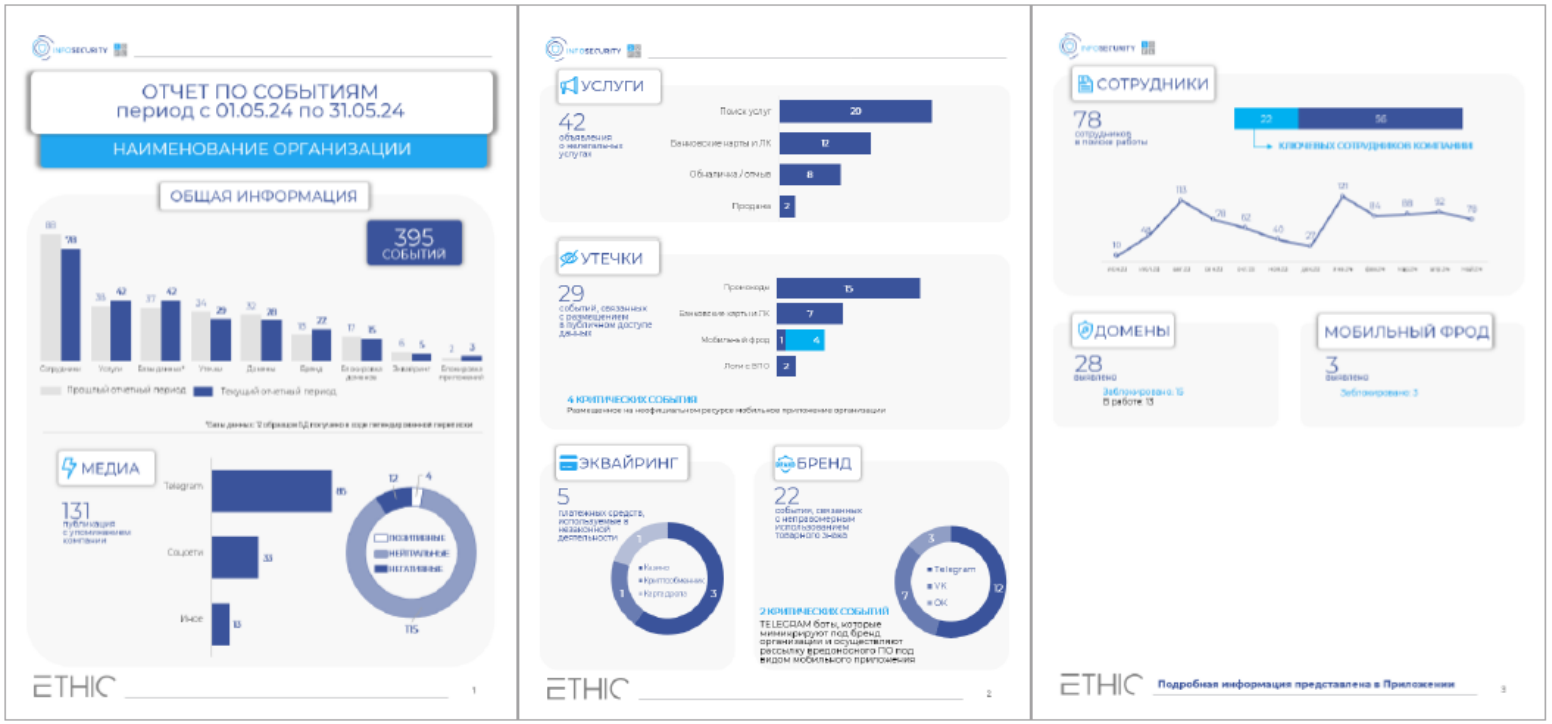
Вы получаете комплексный аналитический отчет, содержащий сведения о результатах работы каждого модуля и выявленных угрозах

В ЛЮБОЕ ВРЕМЯ

В личном кабинете сервиса вы можете всего за пару кликов сформировать статистический отчет за выбранный промежуток времени и сделать выгрузку выявленных событий в удобном формате

БУДЬТЕ В КУРСЕ ВСЕГО, ЧТО ПРОИСХОДИТ, ДАЖЕ НЕ ЗАХОДЯ В СЕРВИС

Настройте рассылку и ежедневно получайте статистические данные и выгрузку выявленных событий за минувшие сутки



Шутбаев Жанибек

Руководитель отдела развития
кибербезопасности в Центральной Азии

+7 701 786 97 70
Zhanibek.shutbaev@softline.com

softline®

Цифровая Трансформация.
Успешная. Эффективная.