Опыт создания Infosecurity SOC

Олег Вяткин

Директор по развитию продуктов

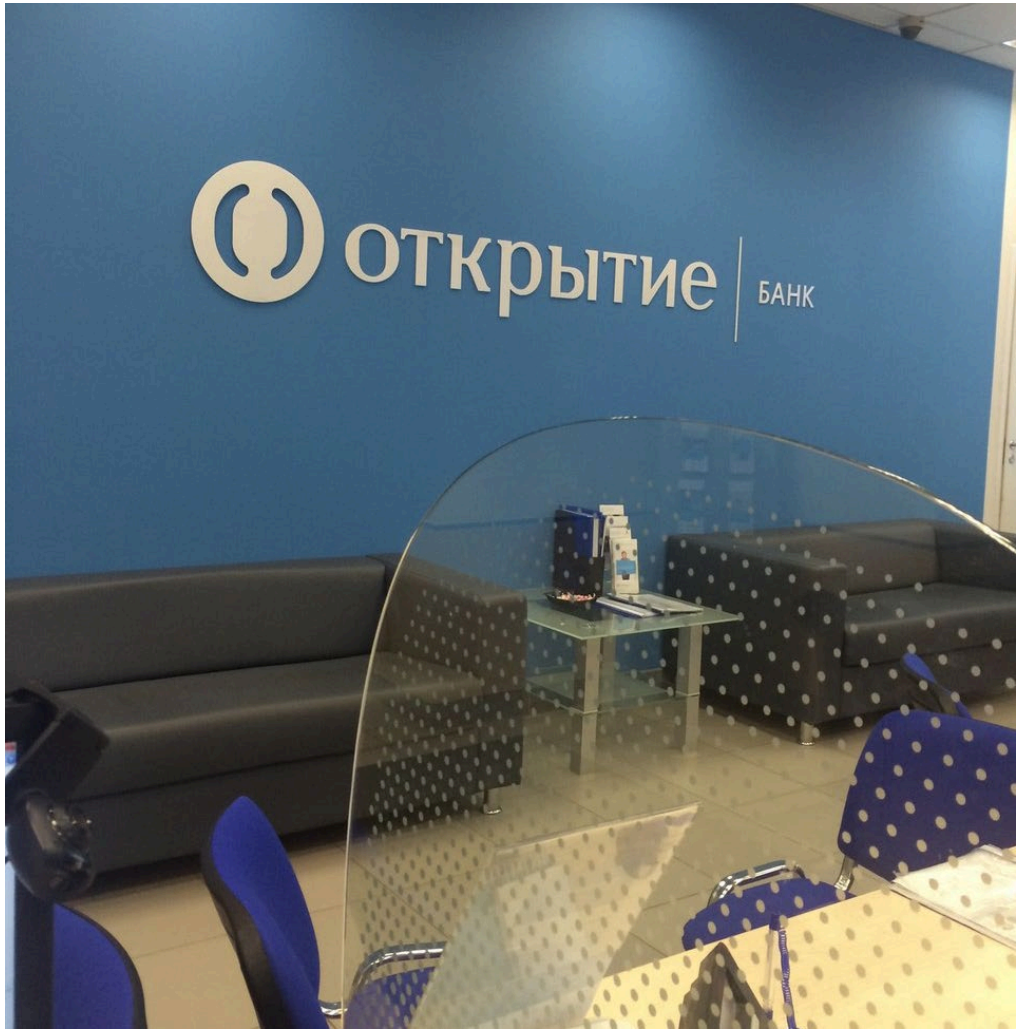
vyatkin@in4security.com

Cloud | Security | Big Data | Mobility

INFOSECURITY

softline® 25 Years in IT

Первый кейс ISOC: финансовая группа «Открытие»



100
событий/день
для разбора
аналитиками

24/7
режим
сопровождения
Infosecurity SOC

3 000
источников
событий ИБ

35 000
хостов
в сети клиента

Классический состав и цели SOC

ЦЕЛИ:

Снижение рисков хищения данных и денежных средств

Обеспечение непрерывности бизнеса

Снижение тяжести последствий инцидентов

ПОДХОД:

Выявление кибератак на ранних стадиях

Быстрый разбор инцидентов в большем количестве информационных систем

Команда ISOC

15
разработчиков и специалистов сопровождения

7
сотрудников круглосуточного мониторинга

4
аналитика второй линии

2
аналитика-эксперта

Путь развития технологической платформы

2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019

Возможности технологической платформы

Высокая надежность, отказоустойчивость
и автоматизированное горизонтальное масштабирование
до требуемой производительности

Разработка сценариев любой сложности
благодаря использованию полноценного
языка программирования (Scala)

Высокая производительность на потоковых
данных и ретроспективных запросах

Автоматическое реагирование
на атаки и инциденты

Максимальное количество инцидентов разбирается автоматически или на первой линии

Поток данных:

2 Тб/сутки

Сжатие данных:

1 : 50

Быстрая аналитика по Big Data*:

2 мин поиск по IP-адресу

8 мин GroupBy + Sort

** на тестовой выборке 3 мес. Netflow: 17 млрд событий, 24 Тб данных.*

Формирование процессов SOC

Описание типовых сценариев разбора инцидентов, формирование собственной базы знаний

Регламенты взаимодействия с департаментами IT и ИБ заказчика

Аналитика собранных данных, выделение атомарных действий, сведение разбора инцидента к алгоритму

Формирование процессов SOC

Эффективно
работающий
коммерческий SOC

Более 6 лет экспертизы
по внедрению и
обслуживанию SOC

Свыше 10 клиентов из различных
отраслей — от финансовых
корпораций до госструктур

Готовность к динамическому
масштабированию и подключению
новых клиентов


INFOSECURITY
a Softline company


GO GLOBAL
GO CLOUD
GO INNOVATIVE