CITIC TELECOM CPC

Безопасная трансформация: ваше спокойствие как услуга

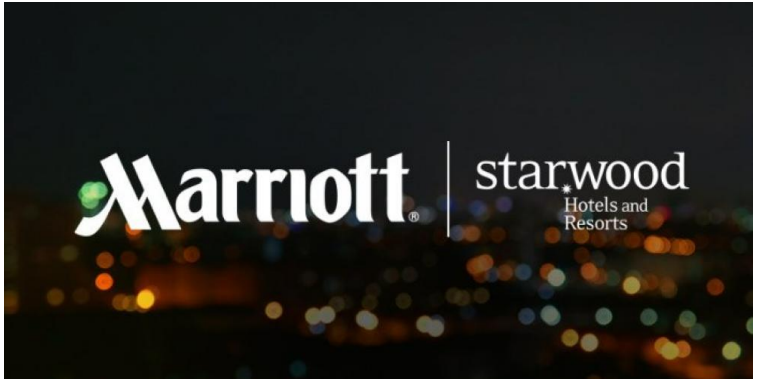
Игорь Селиверстов

30 Мая 2019

Innovation Never Stops

Самые громкие случаи утечки данных 2018

- 30,000,000 аккаунтов похищены
- Атака началась 14 Сентября 2018
- Обнаружена 25 Сентября 2018
- Опубликована 28 Сентября 2018

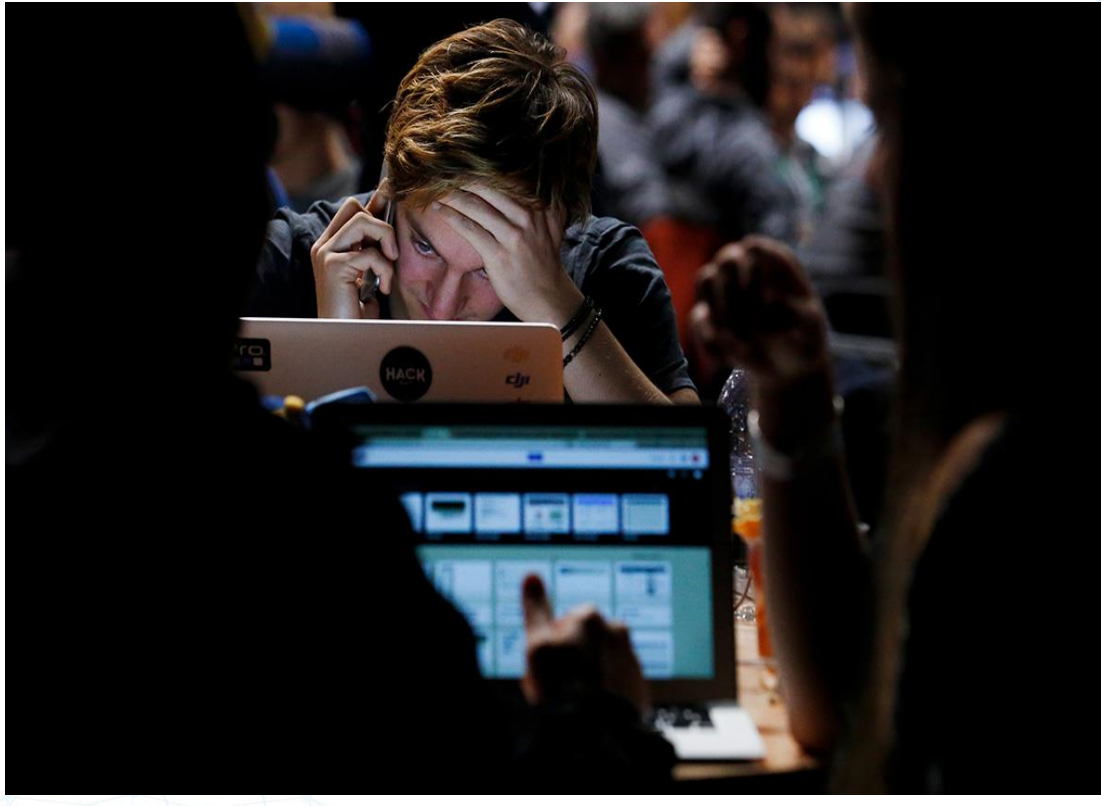


- 500,000,000 гостевых аккаунтов
- Опубликовано в 2018
- Несанкционированный доступ с 2014

Атаки на банковский сектор в России

Ущерб российских банков от кибератак за 2017 год составил **1,078 млрд руб.**

Общая сумма хищений с карт физлиц в 2018 году составила **1,4 млрд руб.**, что в **1,4 раза** больше показателя 2017-го, говорит статистика ЦБ.

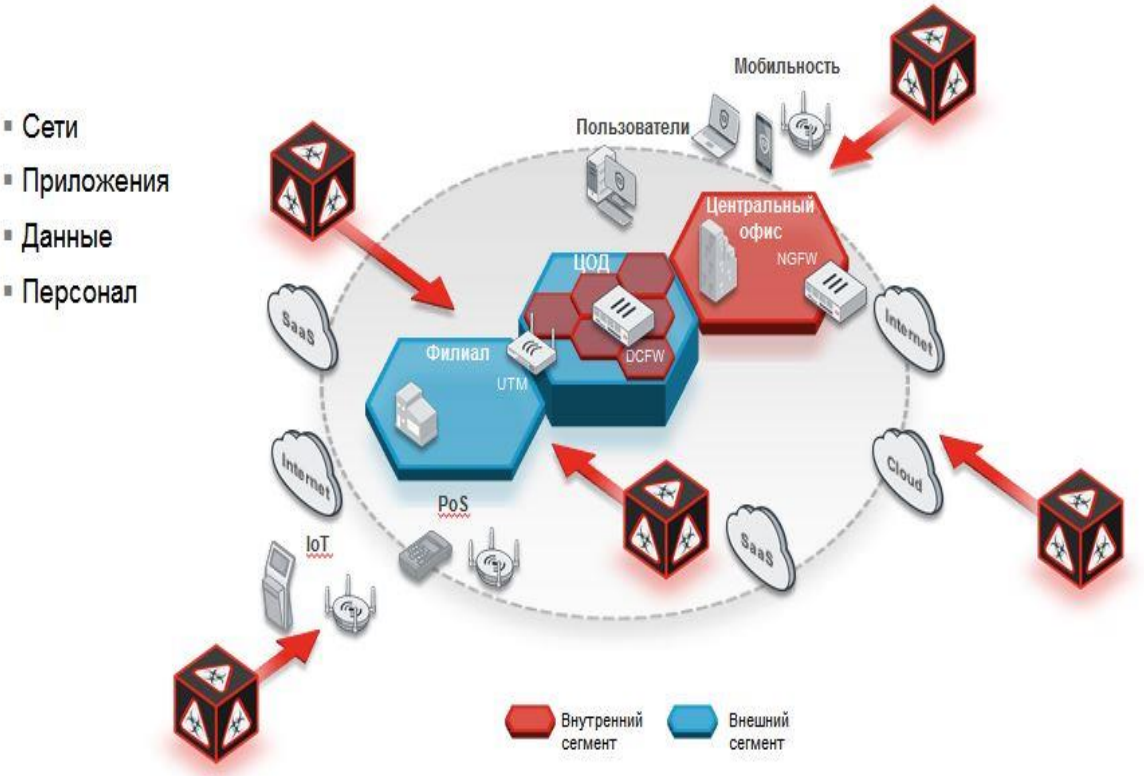


Тенденция увеличения атак на корпоративный сегмент

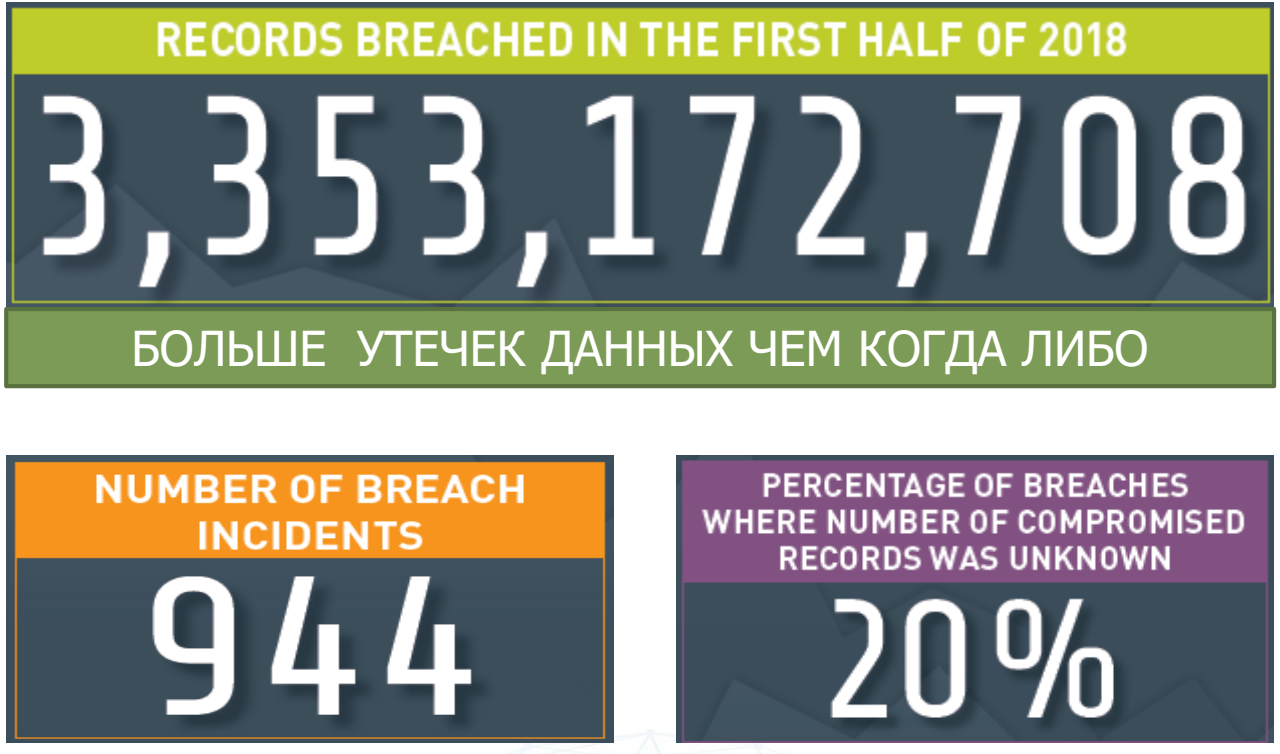
Во второй половине 2018 г. количество атак, направленных на получение контроля над ИТ-инфраструктуру, выросло на 20%.

Цели атак:
Сети
Приложения
Данные
Персонал

Средства атак:
Фишинг
Троян
DDoS-атаки
Ботнет
Backdoor
Черви
Классические файловые вирусы
Вирус-вымогатель (шифровальщик)
Вредоносная программа (зловред)
Фрод
И др.



Частота и масштаб утечки данных в мире



source: Gemalto Breach Level Index 1H2018

Частота потерянных или украденных записей данных

source: Gemalto Breach Level Index 1H2018

Экспоненциальное увеличение данных и подключенных устройств

Объем **Данных** увеличиться в **10 раз** за последние 6 лет и к **2020** возрастет с 4.4 ЗБ to **44 ЗБ**.

Количество **Устройств** подключенных к интернету более чем в **3х** раза к **2021**, с 17.1 млрд в 2016 до **27.1 млрд** в 2021

Sources: Computerweekly: 'Data set to grow 10-fold by 2020 as internet of things takes off'
The Zettabyte Era: Trends and Analysis (Cisco public white paper)

Нехватка квалифицированных кадров

- 1 мил вакансий в 2018 году… 1,5 мил в 2019 году во всем мире (согласно PwC)

- В России 45% компаний испытывают дефицит специалистов данной отрасли. 15% компаний заявили, что поиск специалистов-кибербезопасников является приоритетной задачей.

- Нехватка квалифицированного персонала затрагивает как региональные так и международные компании

Провайдер MSSP

Managed security service provider (MSSP) - обеспечивает внешний мониторинг и управление устройствами и системами безопасности. Базовая услуга включает управление межсетевым экраном, обнаружение вторжений в виртуальную частную сеть, сканирование на наличие уязвимостей и управление антивирусном.

MSSP используют операционные центры безопасности SOC (либо свои собственные, либо от других поставщиков) для предоставления круглосуточных 24*7 поддержки, что способствует сокращению числа сотрудников по обеспечению оперативной безопасности, которые предприятию необходимо нанимать, обучать и удерживать для поддержания приемлемого уровня безопасности.

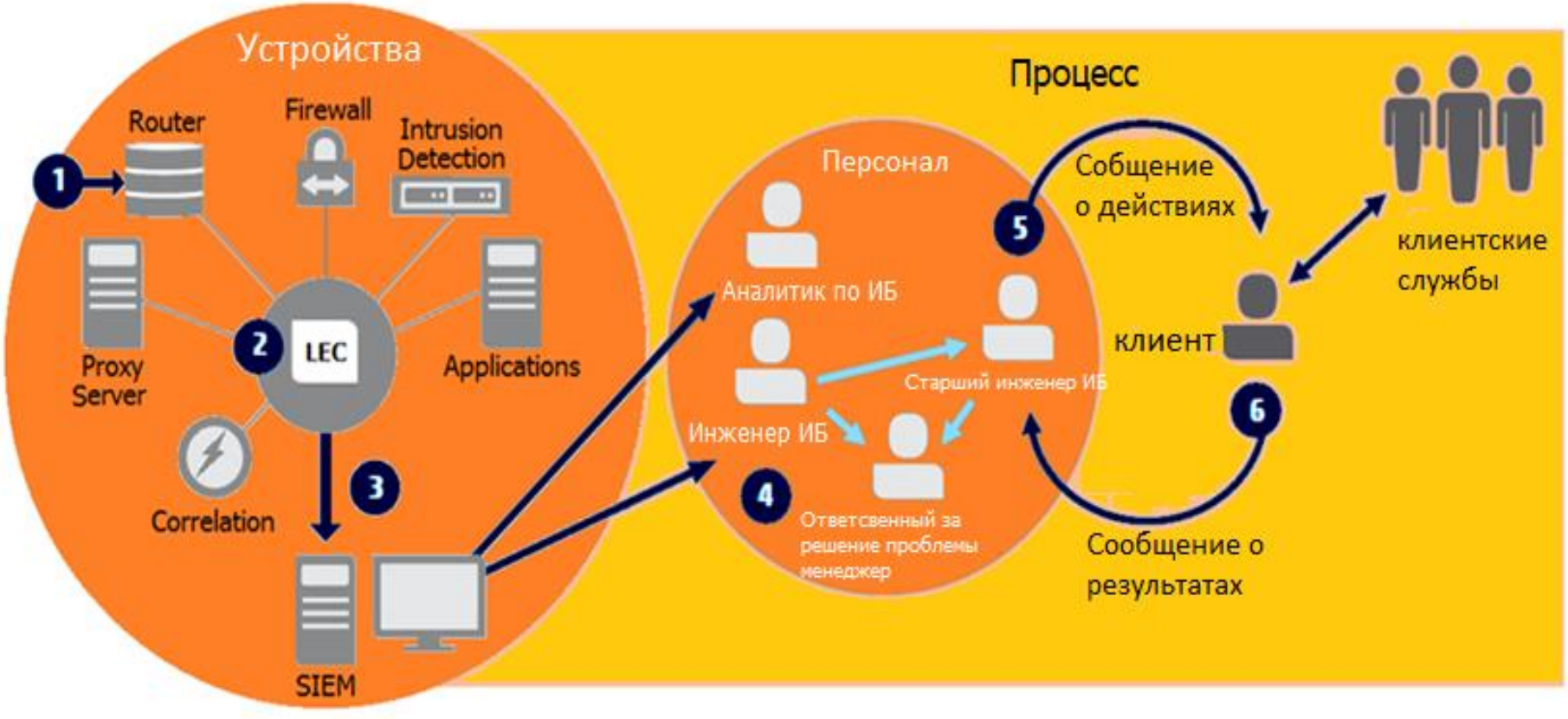
- Gartner

MSSP увеличивает прибыльность инвестиций Security ROI

- **Предположим, что стоимость устройства безопасности составляет $ x**

Модель управления	Самостоятельное управление	Управление от системного интегратора	MSSP
Затраты на управление	0	10% of $x	20% of $x
Состав работ	➢ Эксплуатация оборудования ➢ Изменение конфигурации ➢ Устранение неполадок зависит от поставщика ➢ Замена оборудования (только RMA) ➢ Мониторинг и устранение неисправностей устройства 7x24 ➢ Мониторинг инцидентов безопасности 7x24 и проактивное реагирование ➢ Интернет-портал для мониторинга инцидентов безопасности в режиме реального времени ➢ Индивидуальный отчет	➢ Эксплуатация оборудования ➢ Изменение конфигурации ➢ Устранение неполадок по запросу. ➢ Замена оборудования ➢ Мониторинг и устранение неисправностей устройства 7x24 ➢ Мониторинг инцидентов безопасности 7x24 и проактивное реагирование ➢ Интернет-портал для мониторинга инцидентов безопасности в режиме реального времени ➢ Индивидуальный отчет	➢ Эксплуатация оборудования ➢ 7x24 Изменение конфигурации ➢ 7x24 Устранение неисправностей ➢ Обмен оборудования ➢ Мониторинг и устранение неисправностей устройства 7x24 ➢ Мониторинг инцидентов безопасности 7x24 и проактивное реагирование ➢ Интернет-портал для мониторинга инцидентов безопасности в режиме реального времени ➢ Индивидуальный отчет
Итог	➢ Не хватает навыков, чтобы полностью использовать устройство ➢ Медленный или неэффективный ответ на инцидент безопасности	➢ Системный интегратор предоставляет поддержу по запросу как дополнительный сервис ➢ Медленный или неэффективный ответ на инцидент безопасности	➢ Полностью управляемый сервис с технической поддержкой 7x24 ➢ Проактивное реагирование на инциденты безопасности, чтобы минимизировать влияние на бизнес
Эффективность использования устройства	**30%**	**50%**	**100%**

Работа SOC


Устройства
Router
Firewall
Intrusion Detection
Proxy Server
LEC
Applications
Correlation
SIEM
1
2
3
Процесс
Персонал
Аналитик по ИБ
Старший инженер ИБ
Инженер ИБ
Ответсвенный за решение проблемы менеджер
4
5
Собщение о действиях
клиентские службы
клиент
6
Сообщение о результатах

Эффективность решение проблем (KPIs)

Непрерывное улучшение производительности

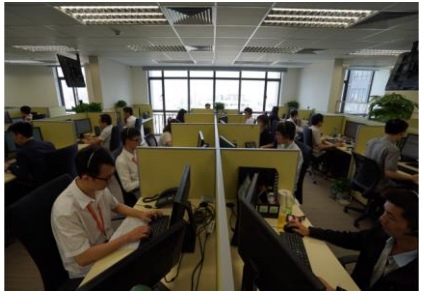
Ответ
- **6 секунд** тел. звонок
- **99%** доступность
- **15 мин.** email

Оповещение
- **8 минут** SMS
- **15-30минут** email

Решение проблем
- **< 4 часа** на устранение
- **Час** оповещение о ходе решения
- **Минута** проверка

Цели

* **Про активность**
* **Быстрота**
* **Эффективность**



Работа SOC – на примере атаки WannaCry в 2017

В период с 12 Мая по 14 May 2017,

Наш оперативный центр по безопасности(SOC) предотвратил Более 225,000 попыток атак на всех наших клиентов в течение 48 часов во время атаки The WannaCry.

Наши клиенты были хорошо защищены от WannaCry и НЕ потеряли ДАННЫЕ и ДЕНЬГИ!

Почему CPC?

- **Десятилетний опыт в сфере управления сервисами информационной безопасности**

> 24x7 SOC поддержка, мониторинг доступности устройств, мониторинг инцидентов безопасности с уведомлением по электронной почте

> Постоянная поддержка и консультации по вопросам безопасности сертифицированным специалистом

> Управления изменениями (обновление версии встроенного ПО) для максимальной эффективности безопасности

> Регулярное резервное копирование конфигурации устройств

Почему CPC?

- **ISO 9001, 20000, 27001: Использование стандартных процедур ISO для защиты интересов клиентов и предоставления услуг**
- **Сертификация от поставщиков: Профессиональные инженеры знакомые с оборудованием производителей**
  - > Palo Alto Networks Certified Network Security Engineer (PCNSE)
  - > NSE 4 – FortiGate Network Security Professional
  - > NSE 6 – FortiGate Network Security Specialist

  В случае инцидента безопасности :

  Более быстрое выявление проблемы и ее устранение→Более эффективная связь с поставщиком → Меньшее влияние на бизнес клиента → Меньше $$$ потерь;
- **Другие профессиональные сертификаты в области информационной безопасности :**
  - > GIAC Penetration Tester (GPEN)
  - > Сертифицированный аудитор информационных систем
  - > Сертифицированный специалист по безопасности информационных систем

CITIC TELECOM CPC

Пример решения

Управления 400+ устройствами безопасности в розничной сети магазинов в Китае

Innovation Never Stops

Информация о клиенте

Клиент

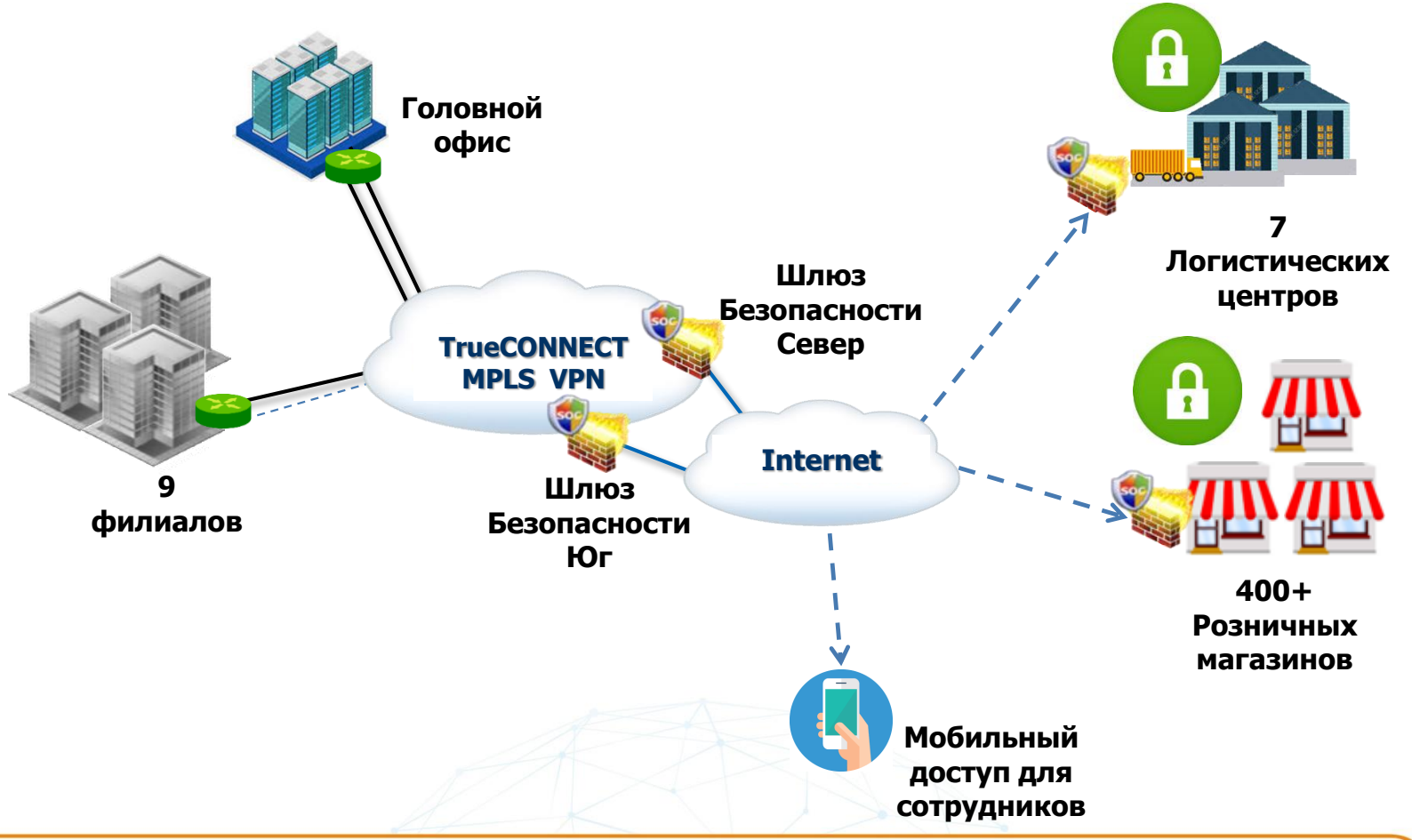
- Ведущая розничная сеть магазинов с более чем 400 магазинами в Китае
- Число магазинов сети растёт на 30% в год на протяжение нескольких лет

Задача

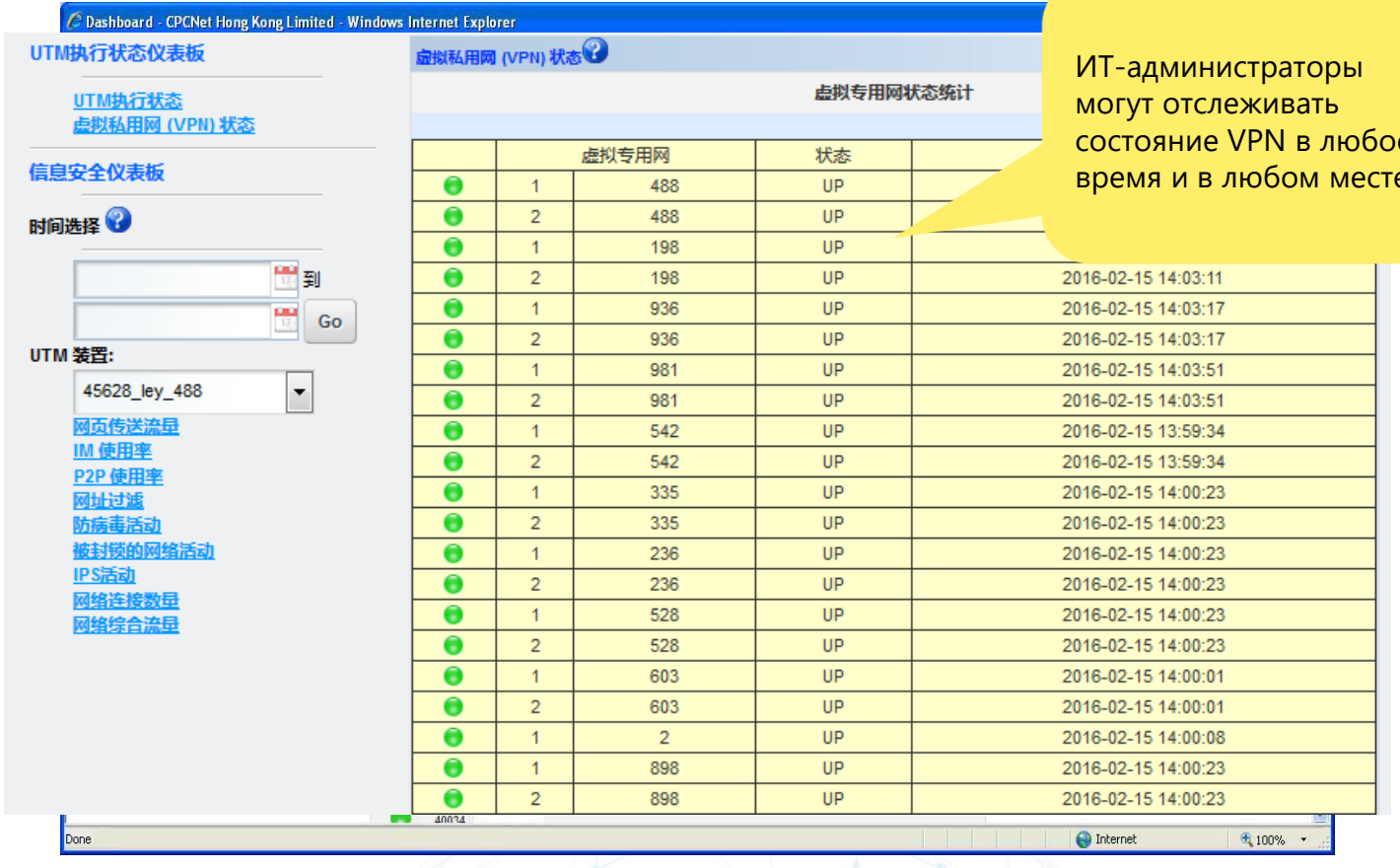
- Предоставить решение по обеспечению безопасности (внедрение и управление) для сотен магазинов по всей стране
- Агрессивное расширение бизнеса требует многочисленных экспертов по безопасности

Проблемы клиента

Предложенное решение



Решение от CITIC Telecom CPC – Онлайн портал



ИТ-администраторы могут отслеживать состояние VPN в любое время и в любом месте.

Решение от CITIC Telecom CPC– Real-time Email Alert

From: CITIC Telecom CPC Security Operations Centre [mailto:soc@citictel-cpc.com]
Sent: Monday, July 13, 2014 9:06 AM
To: johnny.yeung@citictel-cpc.com
Subject: Trust-CSI Managed UTM Alert

Dear Valued Customer,

Our TrustCSI UTM device has detected the following attack to your network.
The following is a summary of the incident captured :

Incident Detected At : 13 Jul 2014 09:05:18 HKT

Network Attack Detected: VIRUS: W32/MYDOOM.M@MM BLOCKED ()

UTM Action: blocked

Other related information:

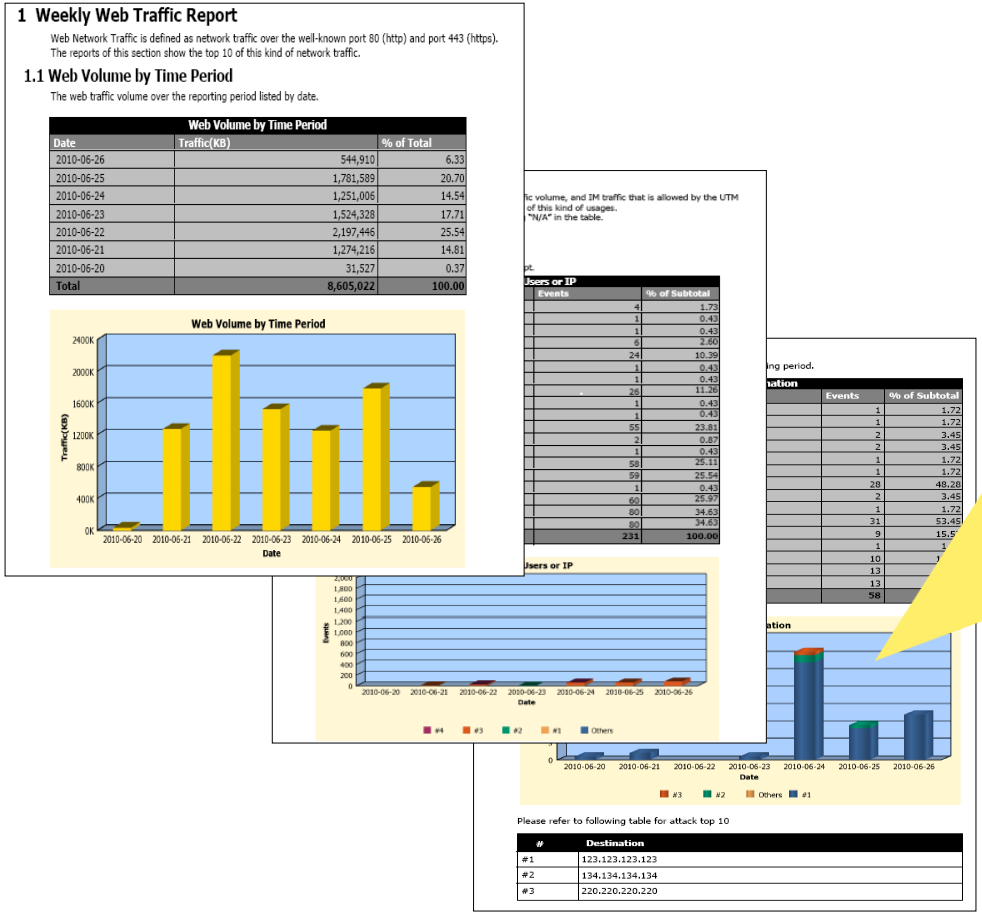
Source IP Address: 192.168.0.58
Destination IP Address: 218.213.242.168
Application Protocol:

Do you like to have professional recommendations on how to handle these security events in future?
By subscribing TrustCSI(TM) Managed Security Service (MSS),
you can consult our security experts and get recommendation from them directly based on our state of the art SIEM technologies and event correlation.
To subscribe, please contact our CS hotline at +852 23318930 or email to help@citictel-cpc.com.

Best regards,
Security Operations Centre
CITIC Telecom International CPC Limited
20/F, Lincoln House, Taikoo Place, 979 King's Road, Quarry Bay, Hong Kong
D: (852) 2811 2852 F: (852) 2219 9610
E: soc@citictel-cpc.com W: www.CITICTEL-CPC.com

UTM перед поставщиком облачных услуг и UTM в головном офисе обеспечивает предотвращения вторжений в IPS. ИТ-администратор может своевременно узнавать об угрозах, встречающихся в сети.

Решение от CITIC Telecom CPC– Еженедельный отчет



1 Weekly Web Traffic Report

Web Network Traffic is defined as network traffic over the well-known port 80 (http) and port 443 (https). The reports of this section show the top 10 of this kind of network traffic.

1.1 Web Volume by Time Period

The web traffic volume over the reporting period listed by date.

Web Volume by Time Period

Date	Traffic(KB)	% of Total
2010-06-26	544,910	6.33
2010-06-25	1,781,589	20.70
2010-06-24	1,251,006	14.54
2010-06-23	1,524,328	17.71
2010-06-22	2,197,446	25.54
2010-06-21	1,274,216	14.81
2010-06-20	31,527	0.37
Total	8,605,022	100.00

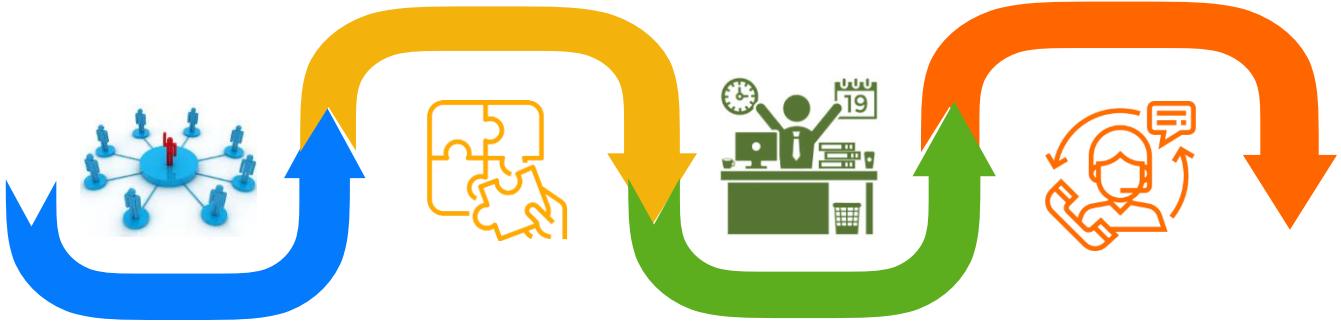
#	Destination
#1	123.123.123.123
#2	134.134.134.134
#3	220.220.220.220

UTM перед поставщиком облачных услуг и UTM в головном офисе обеспечивает предотвращения вторжений в IPS. ИТ-администратор будет получать сводку состояния сети каждую неделю, чтобы анализировать проблемы на корпоративной сети.

Преимущества для клиента

Единый контакт для управления более чем 400 магазинами по всей стране

Облегчает работу клиента, улучшая безопасность, видимость и контроль



Шлюз безопасности высокой доступностью обеспечивает надежность для сети клиентов

24 x 7 сервис управления и технической поддержки клиентов

Спасибо!

Innovation Never Stops

www.citictel-cpc.com