GO GLOBAL GO CLOUD GO INNOVATIVE

Будущее облачного потребления услуг

Сок в банке и в разлив

Гулевич Виктор
“Руководитель практики MSSP и теории SOC”

Творцы будущего

1	Apple
2	Amazon.com
3	Bank of America
4	JPMorgan Chase
5	Samsung Electronics
6	Facebook
7	Tencent
8	Charter Communications
9	Alibaba
10	Microsoft
11	Alphabet
12	Berkshire Hathaway
13	Citigroup
14	China Construction
15	Johnson & Johnson
16	HSBC
17	Unitedhealth Group
18	Wells Fargo
	TSMC
	ncast

CNews100: Крупнейшие ИТ-компании Росси

№ 2016	№ 2015	Название компании		
1	1	НКК		
2	2	Ланит		
3	–	Epam*		
4	5	Softline		
5	4	Техносерв		
6	3	Газпром Автоматизация***		
7	7	Luxoft *		
8	6	Лаборатория Касперского*		
9	8	1С**		
10	9	ITG (Inline Technologies Group)(3)		
	11	Ай-Теко	Моск	
	12	Крок	Москва	ИТ-услуги

Крупнейшие компании России в сфере

#2016	Название компании	Город	Специализация	Выручка от направления ИБ в 2016 г., ₽тыс, включая НДС	напра 2015 вклю
1	Лаборатория Касперского (1) (2) (3)	Москва	разработка ПО, сервисы ИБ	43 083 600	37 5
2	Softline	Москва	дистрибуция ПО и ПАК, сервисы ИБ, интеграция	12 810 496	11 2
3	Акронис* (3)	Москва	разработка ПО	10 046 000	9 0
4	Информзащита (4)	Москва	разработка ПО и ПАК, дистрибуция ПО и ПАК, сервисы ИБ, интеграция	6 867 682	5 2
5	ИнфоТеКС (5)	Москва	разработка ПО и ПАК, сервисы ИБ	3 704 000	4 0
6	Техносерв	Москва	интеграция	3 251 422	3 1
7	Инфосистемы Джет	Москва	разработка ПО, сервисы ИБ, интеграция	3 100 000	2 5
	ICL-КПО ВС	Казань	интеграция, разработка ПО и ПАК, сервисы ИБ	2 765 504	2 1

Корпорации будущего

Задача - Самуил Маркович, Вы сильный, Вы справитесь!

Решениие

- Яша, я - умный, я даже не возьмусь!

РБК: «Ростелеком» намерен купить конкурента InfoWatch — Solar Security

7 февраля в 10:46
Читатель Roem.ru, через: roem.ru/fe

«Ростелеком» договаривается
работающей в сфере информ
менеджеры двух ИТ-компаний

> Solar Security разрабатыва
> и сканер проверки мобиль
> предоставляет сторонним
> от киберугроз. Компания о
> системного интегратора «
> ООО «Солар Секьюрити» п
> гендиректору Solar Securit
> 2016 год составила 361 м

Softline купила долю в российской «Инфосекьюрити»

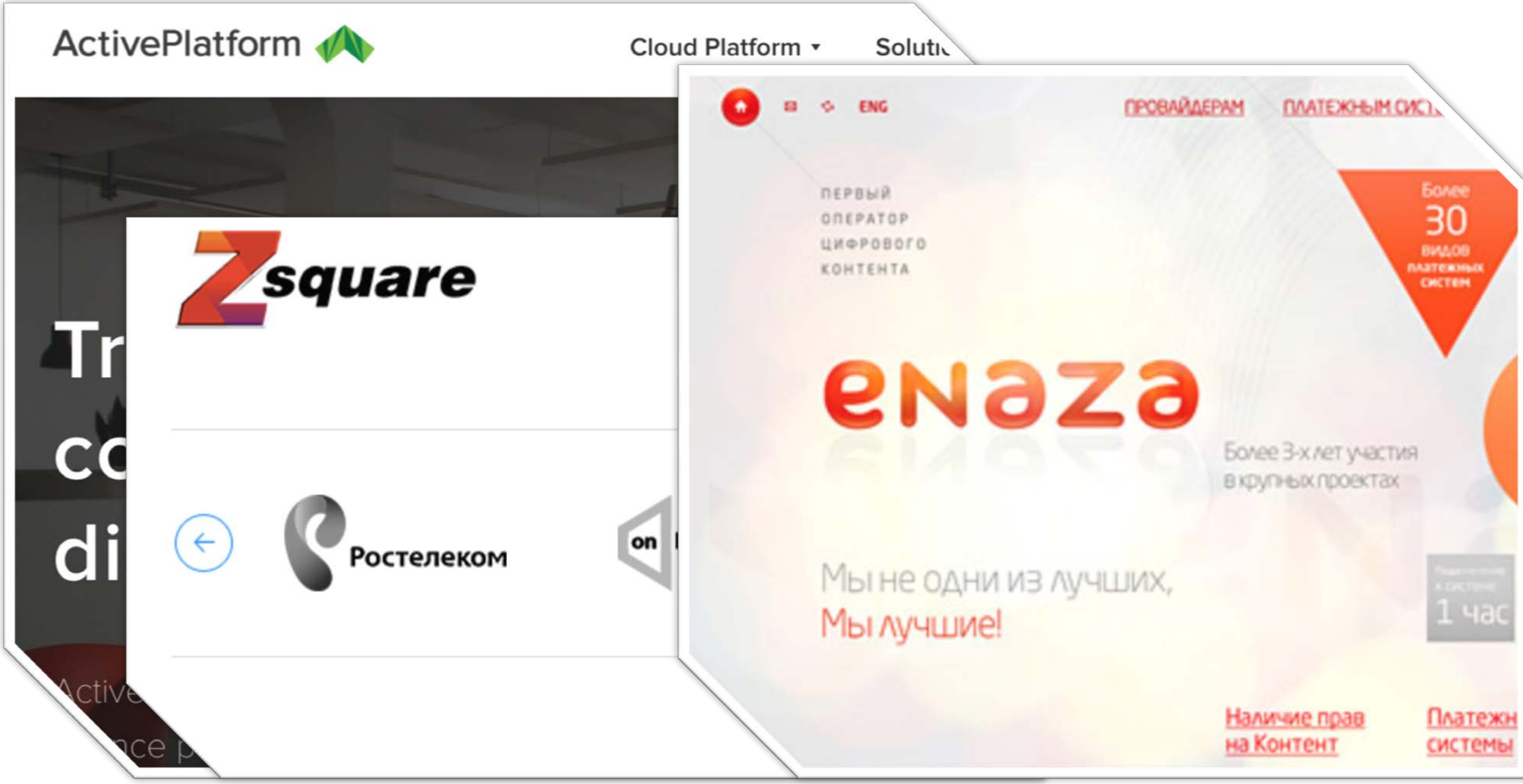
Бизнес **Инвестиции и M&A** мобильная ве

13.02.2018, ВТ, 16:54, Мск , Текст: Владимир Бахур

Softline объявила о покупке контрольного пакета в ГК «Инфосекьюрити» - сервис-провайдере услуг информационной безопасности, системной интеграции и консалтинга.

Цель покупки – усиление позиций Softline на рынке кибербезопасности и расширение спектра услуг за счет сервисов центра управления информационной безопасностью (Security Operation Center, SOC) и компьютерной криминалистики. Softline намерен предлагать новые решения заказчикам как на российском, так и на зарубежных рынках. «Инфосекьюрити» будет постепенно интегрирована в структуру группу Softline. Бренд «Инфосекьюрити» сохранится. Команда, включая высших руководителей, продолжит развивать бизнес «Инфосекьюрити» уже в рамках ГК Softline.

«Мы уверены, что сделка с «Инфосекьюрити» в среднесрочной перспективе поможет Softline занять лидирующие позиции на быстрорастущем рынке сервисов информационной безопасности таких, как Security Operation Center и managed security services. На данный момент в портфеле «Инфосекьюрити» олее 60 сервисов. Объединение наших команд поможет масштабировать бизнес «Инфосекьюрити» на основные рынки присутствия Softline, где компания имеет исторически сильные позиции. Помимо «Инфосекьюрити» активно разрабатывает собственные решения в сфере информационной сти, которые, мы уверены, будут крайне востребованы нашими клиентами на этих рынках», -


ActivePlatform
Cloud Platform
Zsquare
Ростелеком
ENG
ПРОВАЙДЕРАМ
ПЕРВЫЙ
ОПЕРАТОР
ЦИФРОВОГО
КОНТЕНТА
Более
30
ВИДОВ
платежных
систем
enaza
Более 3-х лет участия
в крупных проектах
Мы не одни из лучших,
Мы лучшие!
Наличие прав
на Контент

Супермаркеты услуг ИБ

THREAT MANAGEMENT

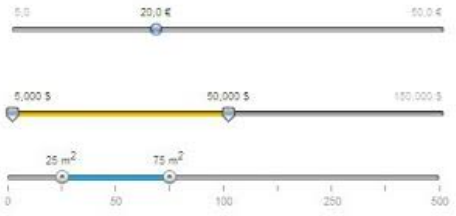
Managed Threat Detection	Managed Application Control
Managed SIEM	Managed IDS/IPS
Managed Secure Web Gateway	Managed DDoS Protection
Managed Network Access Control	MDR for Endpoints
Managed Email Security	Detection, Analytics & Response
Managed UTM	Firewall Management
Managed Two Factor Authentication	Incident Readiness & Response
Managed Endpoint Protection	SSL Certificate Lifecycle Management

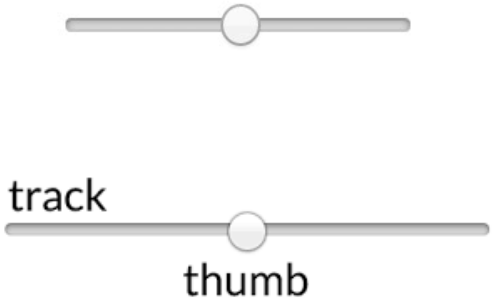
VULNERABILITY MANAGEMENT

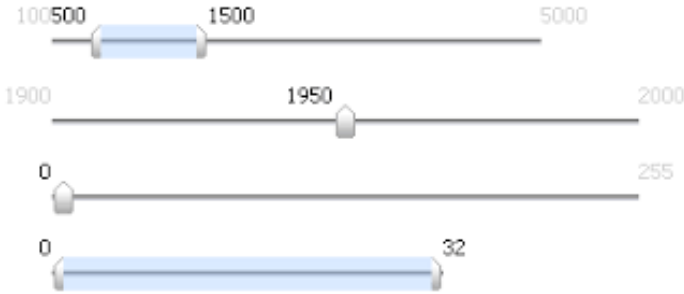
- Managed Security Testing
- Managed Web Application Firewall
- Database & Big Data Scanning
- Application Scanning
- Network Vulnerability Scanning

COMPLIANCE MANAGEMENT

- Risk Assessment
- PCI Compliance
- Security Awareness Education
- Secure Development Training
- Merchant Risk Management







Банк: А что внутри?

Инфраструктура

Сетевое оборудование

Серверы

Рабочие станции

Каналы связи

Мобильные устройства

Прикладные / бизнес системы

FRONT и BACK

Платежные шлюзы

Публикации

Файловые хранилища

СУБД

Терминальная сеть

Процессы

Корректное проведение платежей

Коммуникации с клиентами и контрагентами

Выполнение требований регулятора (организационные и технические)

Обеспечение удобной работы с системами банка для клиентов и сотрудников

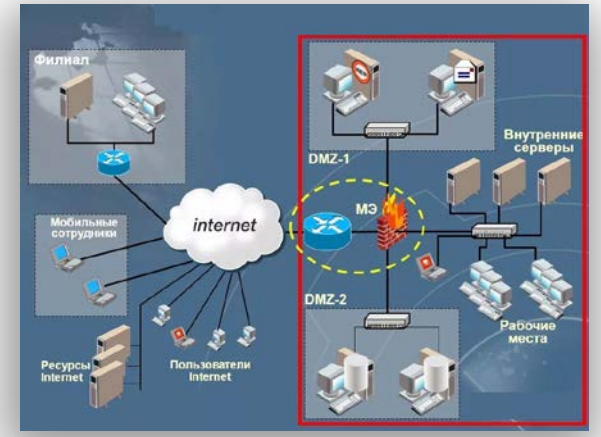
Минимизация прямых и косвенных финансовых рисков

Банк: Что нужно защищать? **Периметр!**

- Фильтрация Интернет-трафика.

NGFW (Next-Generation Firewall) – МЭ нового поколения с возможностью поведенческого анализа и анализа в облаке.

paloalto NETWORKS · Check Point SOFTWARE TECHNOLOGIES LTD. · FireEye SECURITY REIMAGINED · websense



- **Фильтрация почты.**

CISCO · IRONPORT · FireEye SECURITY REIMAGINED

- **Защита публикаций.**

WAF (Web Application Firewall) – класс обучаемых систем, предотвращающих взлом бизнес-приложений, опубликованных в Интернете.

IMPERVA · POSITIVE TECHNOLOGIES · FORTINET

- **Контроль сети и корректная сегментация, сканеры безопасности**

skybox security · REDSEAL · algosec · CISCO · Nessus vulnerability scanner · POSITIVE TECHNOLOGIES · acunetix WEB APPLICATION SECURITY · QUALYS

Банк: Что нужно защищать? **Серверы с прикладными системами!**

- Защита СУБД.

• DAM (Database activity monitoring) – класс систем для мониторинга действий с СУБД.

IBM IMPERVA

- **Контроль целостности на серверах / терминалах.**

Класс систем, которые позволяют в режиме реального времени отслеживать все изменения в конфигурации серверов. Возможен активный режим работы (блокировка). Контроль уязвимостей и обновлений.

tripwire symantec

- **Контроль обращений к файлам и работа в файловых хранилищах (требования PCI DSS).**

VARONIS FireEye SECURITY REIMAGINED

- **Управление жизненным циклом учетных записей в прикладных системах.**

IDM (Identity Management System) — это класс систем, предназначенных для автоматизации процессов управления учетными записями и правами доступа пользователей в информационных системах, организации управления доступом пользователей на основе ролевых моделей, автоматизации процедур контроля и аудита имеющихся доступов.

Банк: Что нужно защищать? **Рабочие места сотрудников и их мобильные устройства!**

- Защита от утечки конфиденциальной информации.

• DLP (Data Leak Prevention) – класс систем для мониторинга действий пользователей и реагирования на попытки совершения противоправных действий.

SearchInform INFOWATCH® Dozor

- **Антивирусная защита рабочих мест.**

symantec. KASPERSKY lab McAfee paloalto NETWORKS

- **Защита мобильных устройств (корпоративных и личных)**

MDM (mobile device manager) – класс систем, позволяющий контролировать мобильное устройство (удаленное управление, безопасный доступ к неопубликованным приложениям и пр.).

Good airwatch by vmware CITRIX XenMobile MobileIron

- **Контроль работы привилегированных пользователей (в т.ч. на терминальных серверах)**

SearchInform WALLIX TRACE,AUDIT&TRUST CYBERARK

Банк: Что нужно контролировать? **Внутренние критичные процессы!**

- Финансовые транзакции.
- Антифрод (от англ. fraud — «мошенничество», противодействие мошенничеству) – класс систем, которые позволяют скоррелировать различные источники и с высокой вероятностью определить легитимность проводимой операции.

Внешние / внутренние коммуникации сотрудников.

Мониторинг каналов утечки и реагирование на инциденты. Корректная фиксация инцидентов (результаты должны быть валидны для предоставления в суде).

Организационное и документарное обеспечение ИБ.

Написание необходимых НПА и ОРД по требования регуляторов. Регулярные технические и документарные аудиты. Обучение сотрудников.

Защитили всё правильно, но нет ресурсов на сопровождение и контроль ИБ?

У нас обычно для этого берут SOC!

БИЗНЕС, 25 СЕН, 2017 17:35 14 808

Хакеры проникли в «облако» с миллионами сообщений клиентов Deloitte

По данным Guardian, хакерам удалось взломать глобальный почтовый сервис одной из крупнейших аудиторских компаний мира, что открыло им «потенциальный доступ» ко «всем областям информации» о клиентах

Фото: Hannah McKay / Reuters

Чем характеризуется услуга SOC?

- Отсутствует реальная конкуренция на рынке услуг SOC
- Практически невозможно определить SLA
- Сложно оценить эффективность услуги
- Практически невозможно возложить ответственность за реальный инцидент на компанию, предоставляющую услугу SOC

Чего там у ripple

accenture

Santander InnoVentures

MUFG · RBC · Santander · Standard Chartered · Westpac · CRÉD. AGRICOLE

tures

Ripple's Board of Directors lend their deep experience in finance, policy and regulation in advising Ripple.








AMERICAN EXPRESS · UniCredit · transferGo · ALLEX · d·t

GO GLOBAL

GO CLOUD

GO INNOVATIVE