IBM Security

Ростелеком

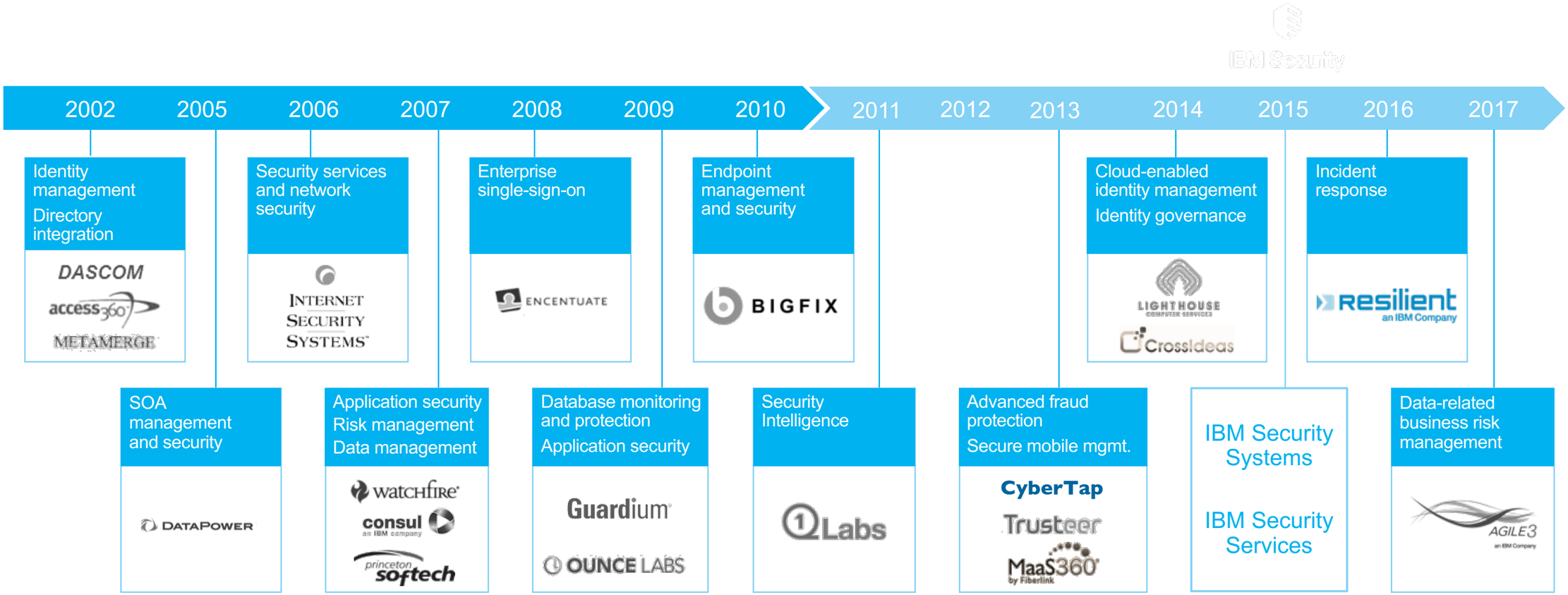
Этапы развития SOC в финансовых организациях

Илья Кравцов, руководитель IBM Security Россия, СНГ

Владимир Шадрин, директор SOC Ростелеком

История развития IBM Security

IBM Security



История IBM в области ИБ

IBM Security

Поглощения **Организация IBM Security**

1964

- IBM выпускает IBM System/360, новое семейство компьютеров класса Mainframe со встроенными функциями безопасности

1968

- Начало разработки национального стандарта шифрования данных U.S. Data Encryption Standard

1972

- IBM инвестирует $40 млн. в изучение и развитие функционала безопасности в решениях IBM

1976

- IBM выпускает Resource Access Control Facility (RACF) – решение для управления доступом и аудита на платформе Mainframe

1977

- Национальное бюро стандартов США принимает стандарт шифрования данных Data Encryption Standard (DES), разработанный IBM

1978

- IBM выпускает первый банкомат со стандартом DES

1995

- IBM участвует в разработках Java Security technologies

1996

- IBM запускает SecureWay Key Management Framework – набор приложений, сервисов и криптографических механизмов для безопасной интернет-торговли
- IBM участвует в разработке Secure Electronic Transaction (SET) протокола и запускает пилот с MasterCard в целях обеспечения безопасности карточных транзакций в интернете.
- Исследователи IBM Research изобретают keyed-hash message authentication code (HMAC) – стандарт шифрования интернет протоколов
- IBM выпускает первый LDAP Directory Server класса enterprise

1998

- IBM расширяет Secure Electronic Transaction (SET) - протокол, базирующийся на разработках IBM Research и принятый основными игроками на рынке кредитных карт
- IBM выпускает безопасное почтовое open-source решение Postfix

1999

- IBM приобретает Dascom, основу портфолио IBM Access Manager
- Исследователи IBM участвуют в разработке TLS 1.0 – индустриального стандарта защиты веб-трафика

2000

- IBM получает патент на систему и метод оповещения пользователей о проникновении
- IBM назначает первого Chief Privacy Officer

2002

- IBM приобретает Access 360, основу портфолио IBM's Identity Manager
- IBM приобретает MetaMerge (Directory Integrator)

2005

- IBM выпускает первый ноутбук со считывателем отпечатка пальцев

2006

- IBM приобретает Internet Security Systems, Inc.
- Smart cards, высокоэффективная технология JavaCard™ разработана IBM Research в Цюрихе и лицензирована ведущими производителями smart cards. Технология до сих пор используется в кредитных картах.
- IBM выпускает первую ленточную библиотеку со встроенным функционалом шифрования.

2007

- IBM приобретает Consul для усиления data and governance strategy
- IBM приобретает Princeton Softech
- IBM приобретает Watchfire
- Исследователи IBM играют ключевую роль в разработке стандартов шифрования IEEE 1619. Эти стандарты являются основой большинства storage encryption продуктов на рынке.

2008

- IBM получает патент на защищенную систему и метод усиления политик конфиденциальности
- IBM приобретает Encentuate, основу IBM Enterprise Single-sign-on (ESSO)
- Zone Trusted Information Channel: решение для безопасных онлайн-транзакций

2009

- IBM приобретает Ounce Labs - **AppScan family**
- IBM приобретает **Guardium**,
- Исследователи IBM успешно применяют технологии Big Data для кибербезопасности

2010

- IBM приобретает Big Fix,
- Прорыв IBM Research в области Fully Homomorphic Encryption

2011

- Организация подразделения IBM Security
- IBM приобретает Q1 Labs (QRadar)

IBM Security сегодня

IBM Security

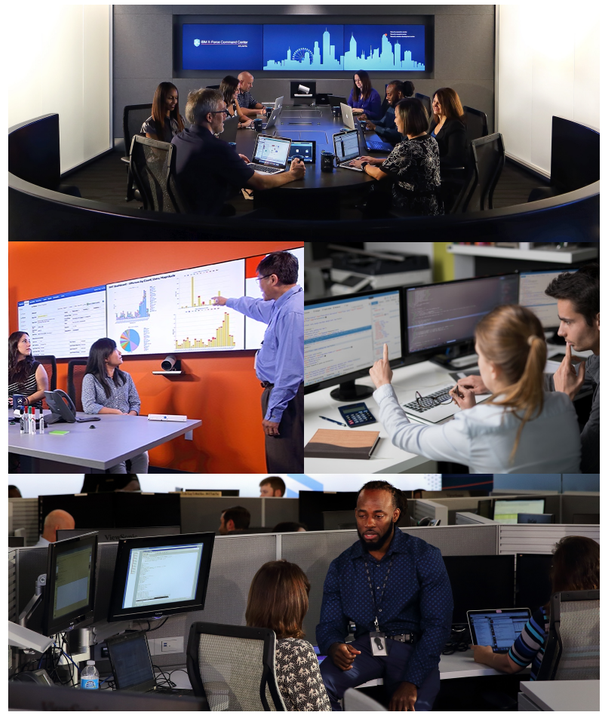
- Мировой разработчик технологических решений в области ИБ
- Консалтинговая компания с мировым опытом построения SOC для своих ключевых клиентов
  - Более 50 компаний входящих в список Fortune Global 500 имеют SOC, построенные IBM
  - Проекты в крупнейших организациях Российской Федерации.
- Провайдер услуг коммерческих SOC с 20-летним опытом

- **8+1** площадок IBM X-Force Command Center для предоставления круглосуточных услуг Managed Security Services
- **1 триллион** событий безопасности анализируемых по более чем 4500 MSS клиентам по всему миру
- Продуктовая линейка для SOC, включая решения из области искусственного интеллекта (IBM Watson for Cyber Security и др.)
- **8,000+** сотрудников, **17,500+** заказчиков из **133** стран, **3,500+** патента в области ИБ, **20** слияний с 2002 года.

SOC в терминах IBM

IBM Security

SOC (Security Operations Center), Центр оперативного реагирования на инциденты ИБ – организационная единица службы ИБ, объединяющая в себе людей, процессы и технологии многоуровневой защиты и обеспечивающая скоординированную работу с целью обнаружения, предотвращения и реагирования на угрозы информационной безопасности.



Уровни зрелости Security Operations Center

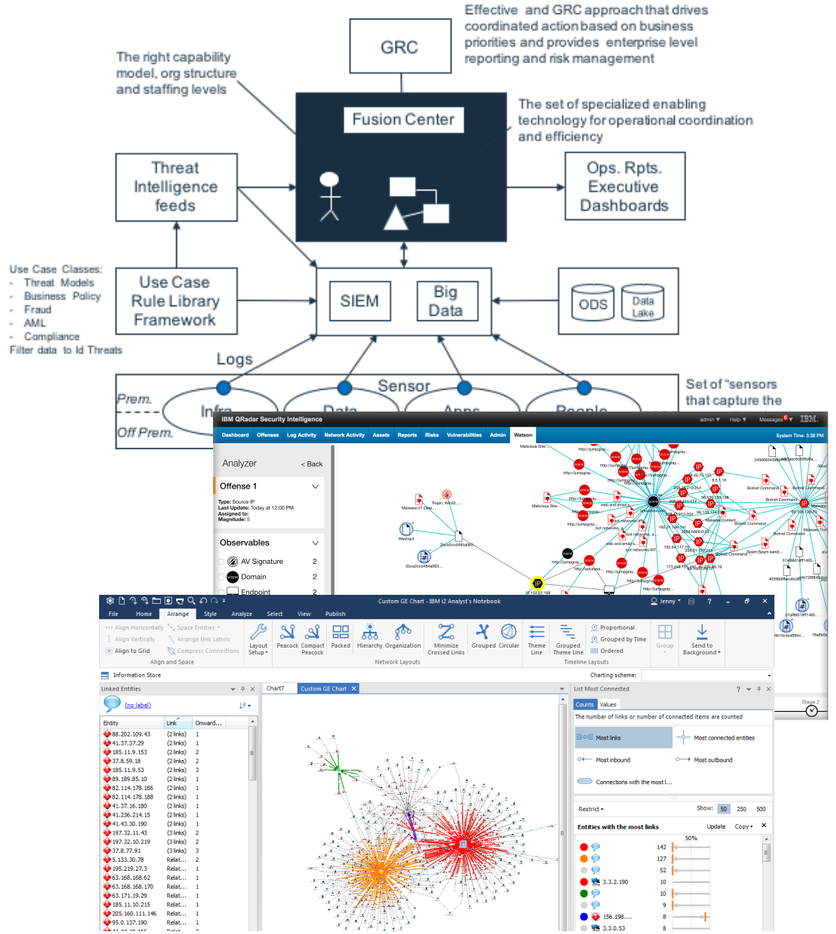
IBM Security

Концепция Fusion Center

IBM Security

Термин Fusion Center в применении к кибербезопасности не является устоявшимся.
Тем не менее, можно выделить общие моменты:

- **Расширение информации**, с которой работает SOC в рамках аналитики за пределы структурированной информации о событиях ИБ и создания единого «Озера данных безопасности»
  - Смежные события – антифрод, физическая безопасность
  - Неструктурированная информация – соцсети, пресса, публикации
- Широкий **обмен информацией** внутри и снаружи организации
  - Обмен со смежными подразделениями, совместная оперативная деятельность с физической безопасностью, борьбой с мошенничеством и финансовым мониторингом.
  - Обмен информацией с правоохранительными органами, регуляторами, ведомственными CERT, центрами по борьбе с мошенничеством.



Вектор на управляемые сервисы

IBM Security

- Растет потребность в сервисах информационной безопасности, предоставляемых профессиональными операторами.
- Развивается российский рынок управляемых сервисов ИБ / MSS (Managed Security Services)

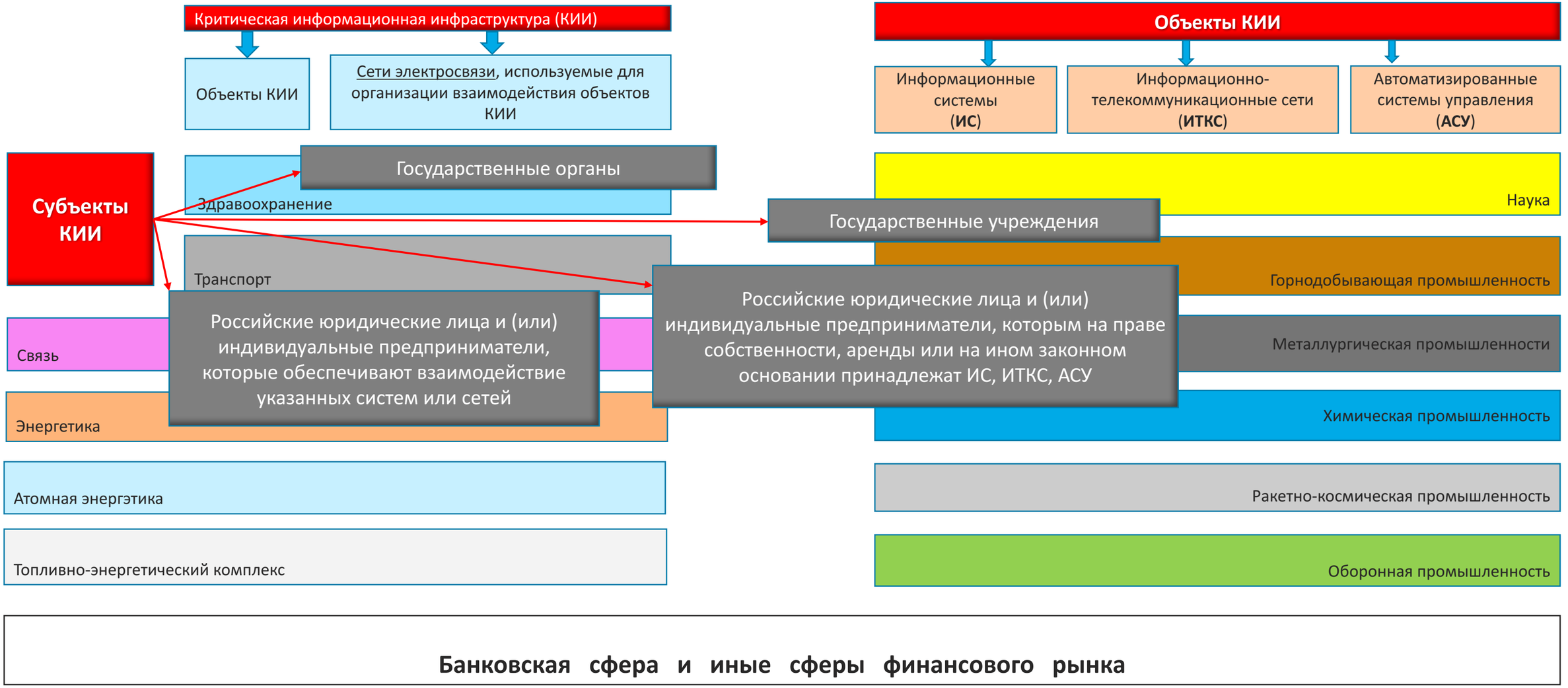
IBM приносит в Россию глобальную экспертизу и опыт в области управляемых сервисов ИБ как крупнейший мировой провайдер услуг Managed Security Services

Source: IDC, 2017

Для бизнеса

RT SOC

RT SOC: ГосСОПКА



RT SOC: ГосСОПКА

Федеральный закон от 27.07.2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры РФ»

Указ Президента РФ о внесении изменений в Указ ПРФ №31с **(22.12.17 №620)**

ФСТЭК

Постановление Правительства РФ утверждает **показатели критериев** значимости объектов КИИ и их значения, а также **порядок и сроки осуществления их категорирования**

Приказ ФСТЭК утверждает требования к обеспечению безопасности значимых объектов КИИ

Приказ ФСТЭК утверждает требования к созданию системы безопасности значимых объектов КИИ

Минкомсвязь

Постановление Правительства РФ утверждает **порядок** подготовки и **использования** ресурсов единой сети электросвязи РФ для обеспечения функционирования значимых объектов КИИ»

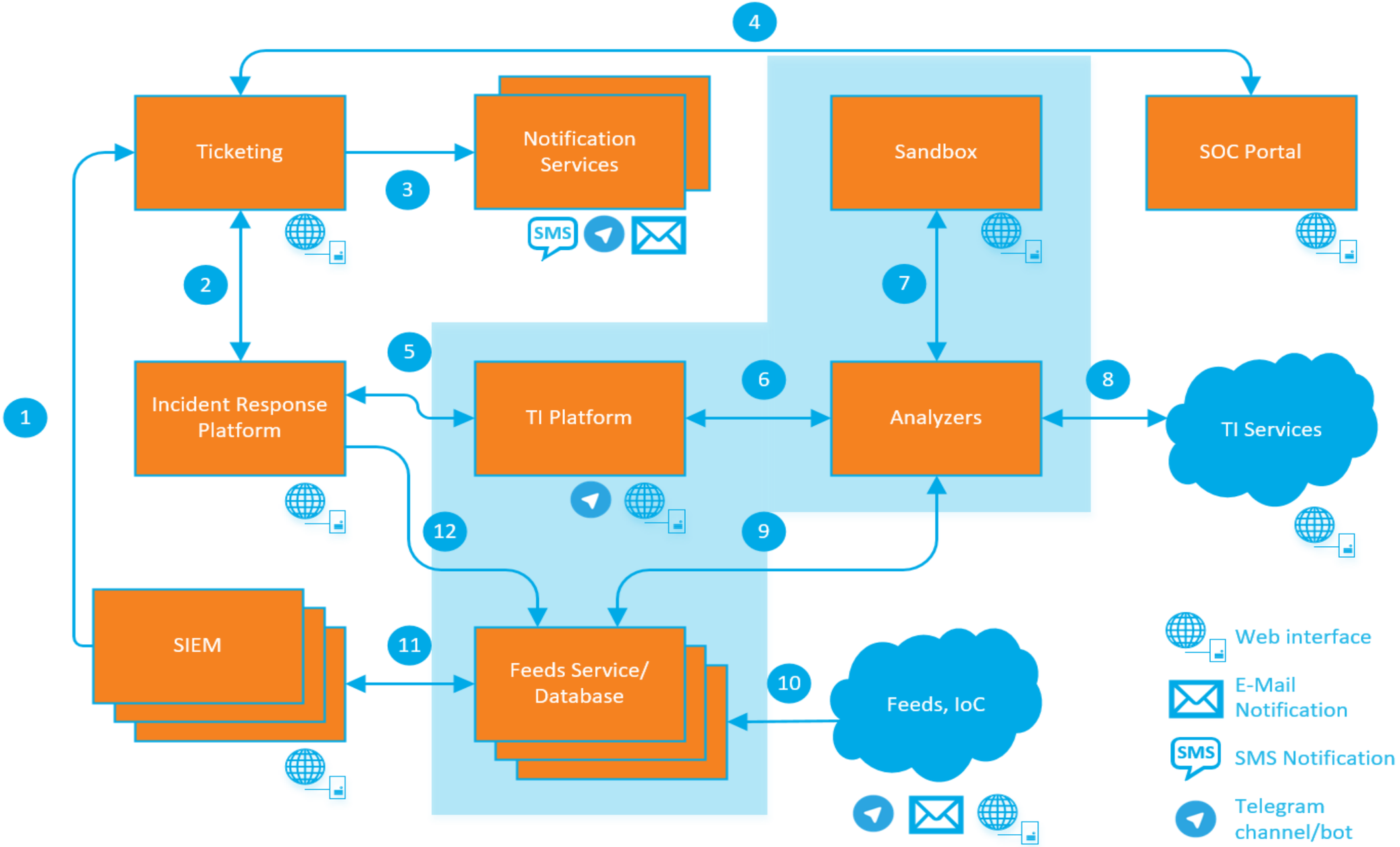
Приказ Минкомсвязи утверждает **порядок, технические условия установки и эксплуатации средств**, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ

ФСБ

Приказ ФСБ утверждает **порядок, технические условия установки и эксплуатации средств**, предназначенных для поиска признаков компьютерных атак на объектах КИИ

Приказ ФСБ утверждает требования к средствам ГосСОПКА

RT SOC: Информационные потоки



RT SOC: Информационные потоки

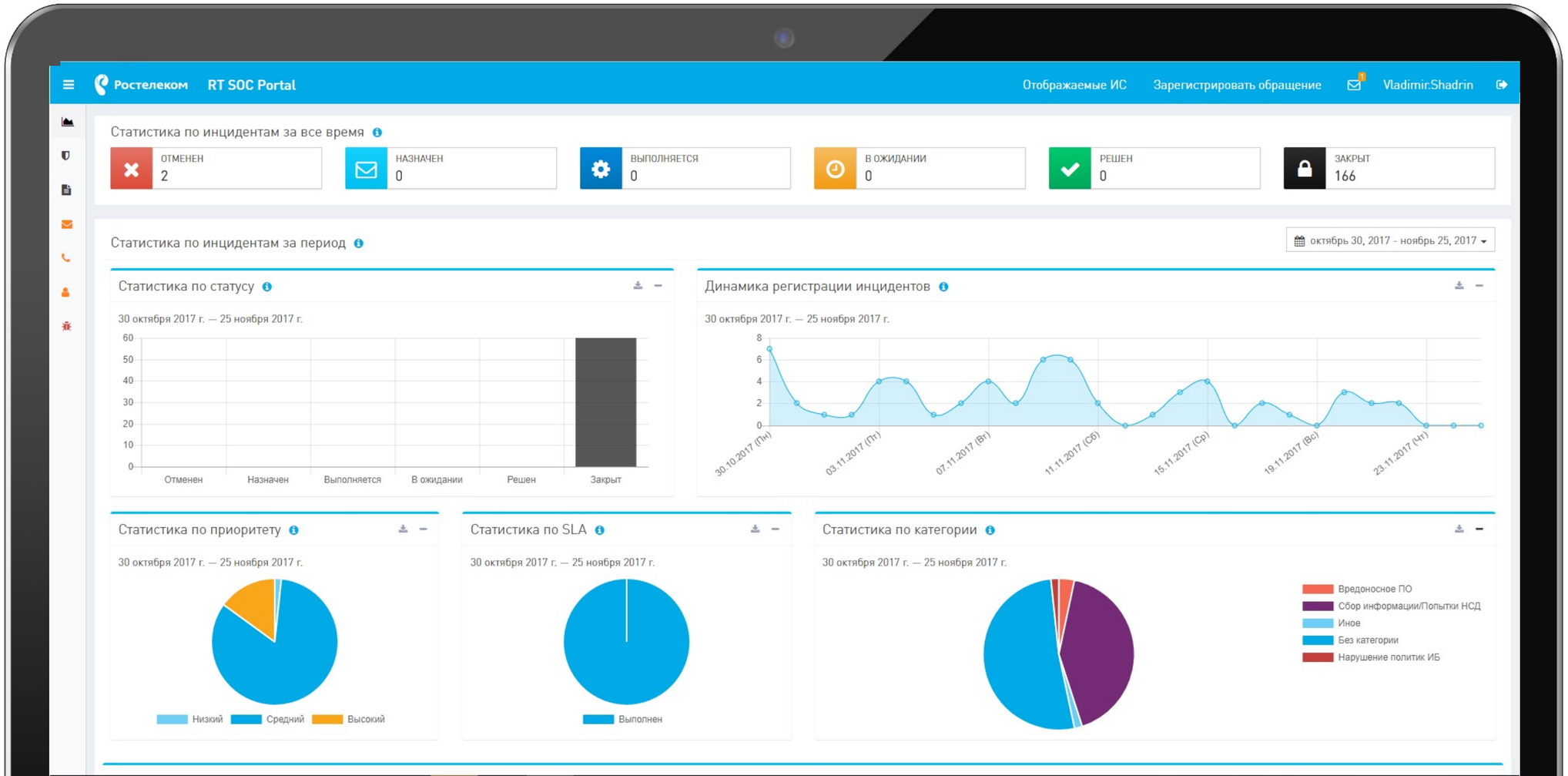
1. Регистрация инцидентов в ticketing системе по срабатыванию кейсов в SIEM. Классификаци, категоризация, приоритизация, SLA
2. Передача инцидента в IRP для реагирования
3. Оповещение задействованных лиц (в т.ч заказчика) через эл.почту, по СМС или через телеграмм канал
4. Синхронизация данных об инциденте с SOC порталом
5. Обогащение инцидента информацией из TI платформы (TheHive <-> Cortex)
6. Запуск доспуных для указанного типа данных (IP, URL, Hash, Domain Name, File, etc) анализаторов и агрегация ответов
7. Локальная песочница (Cuckoo) доступна как через веб-интерфейс, так и как один из анализаторов
8. Запросы к различным поставщикам сервисов (как публичным, так и приватным): Threat lookup, GeoIP, VirusTotal, Google SafeBrowsing, Shodan, Spam etc
9. Запрос к локальным сервисам поиска по фидам и IoC с учетом агрегации, категоризации, весов и т.п.
10. Наполнение баз фидов (FireHol, Public/Private feed bases) и IoC'ов в MISP (через встроенные подписки, Telegram каналы, email рассылки или вручную)
11. Взаимодействие SIEM с фидами и IoC'ами двумя сопсобами:
    - загрузка листов в SIEM (например, майнинг пулы, IoC)
    - форвардинг потока событий в платформу работы с фидами и возврат информации о срабатывании в SIEM
12. Загрузка обнаруженных IoC по различным инцидентам из IRP в MISP

RT SOC: Клиентский портал

ВОЗМОЖНОСТИ

- Статистика по инцидентам (по приоритету, категориям, SLA)
- Динамика регистрации инцидентов
- Возможность получения статистики за любой период, отчеты
- Получение информации по произошедшим инцидентам (общее описание, статус и т.д.)
- Регистрация обращений/инцидентов
- Просмотр контактной информации, список подключенных услуг

RT SOC: Клиентский портал. Интерфейс.



Спасибо за внимание!