

Подход IBM к созданию SOC



Владимир Потапов

CISSP-ISSAP, CISM

Ведущий консультант IBM Security Services

IBM Security в России и СНГ



SECURITY TRANSFORMATION SERVICES

Management
Consulting

Systems
Integration

Managed
Security

Security Strategy, Risk and Compliance

Security Intelligence and Operations

IBM® X-Force® Red Offensive Security

X-Force Incident Response and Intelligence

Identity and Access Management

Data and Application Security

Infrastructure and Endpoint Security

Уровень экспертизы, недоступный на локальных рынках

- Доступ к глобальной сети всемирно известных экспертов по безопасности
- Огромный проектный опыт по всему миру
- Возможность вести и выполнять большие проекты по трансформации



Целостный интегрированный подход

- Интегрированное портфолио сервисов и технологий по безопасности
- Открытая экосистема с 100+ технологических партнёров и 30+ сервисных партнёров
- 800+ технических сертификатов вендоров и 150+ профессиональных сертификатов по ИБ



Определение стратегии

Потребности
бизнеса в ИБ

Проверка уровней
зрелости

Планы развития

Уровень
соответствия

Первый шаг - определение правильной стратегии развития кибербезопасности



Определение ключевых областей информационной безопасности



3 Безопасность мобильных и социальных средств



4 Безопасная разработка ПО



5 Соблюдение гигиены ИБ и ИТ



6 Создание защищенной и контролируемой сети



1 Построение культуры ИБ



Цель: построение системы управления рисками и системы защиты от кибератак на основе сравнительного анализа угроз



2 Внедрение центров обработки и реагирования на инциденты ИБ, аналитика ИБ



7 Безопасность применения облачных технологий и виртуализации



8 Требования к третьим сторонам

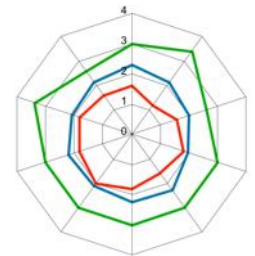


9 Безопасность данных и конфиденциальность



10 Управление доступом и учетными записями

Модель возможных уровней зрелости Capability maturity model (CMM)





Построение когнитивного SOC

Выявление
сложных атак

Активный
поиск угроз

Планы
реагирования

Обмен
базами угроз

Терминология SOC

- **SOC (Security Operations Center), Центр оперативного реагирования на инциденты ИБ** – это организационная единица подразделения информационной безопасности, объединяющая в себе людей, процессы и технологии, предназначенные для получения ситуационной осведомлённости в процессе обнаружения, локализации и предотвращения угроз информационной безопасности.
- **SOC** представляет собой эволюцию понятия CERT (Computer Emergency Response Team) – группу реагирования на чрезвычайные ситуации в области IT технологий
 - Одно из ключевых отличий – использование аналитических технологий для создания единого оперативного видения текущей ситуации в компании с точки зрения ИБ. “Стеклянная кабина” для самолёта информационной безопасности.

Традиционно понятие SOC имеет множество наименований. Только в английском языке это:

- *security defense center;*
- *security analytics center;*
- *security intelligence center;*
- *cyber security center;*
- *threat defense center,*
- *security intelligence and operations center*



Как выиграть гонку со временем при расследовании инцидентов ИБ?

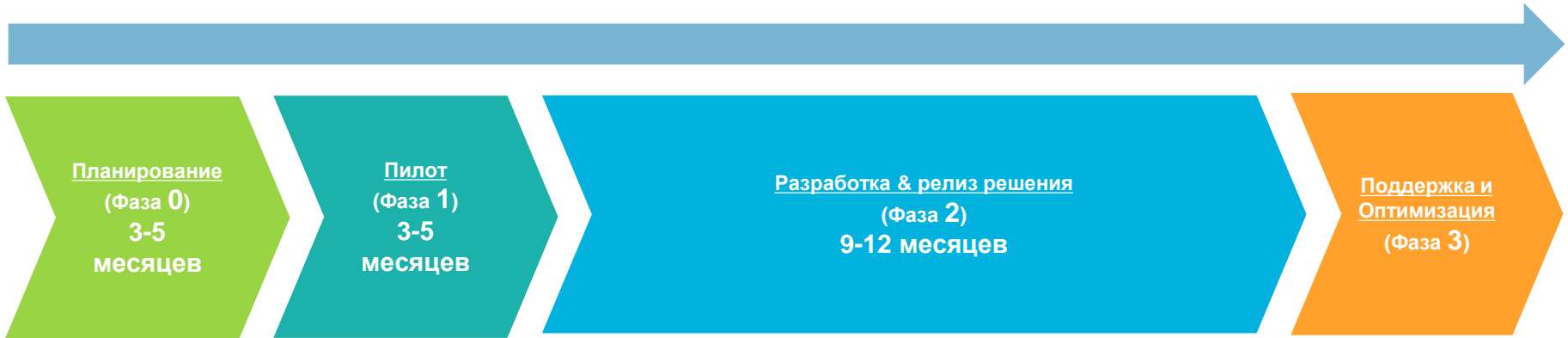


Задачи, стоящие перед SOC



План программы трансформации SOC – теория и практика

SOC Нового поколения – новейшая инфраструктура для наблюдения и реагирования на инциденты информационной безопасности. Эксперты и разработчики систем ИБ смогут воспользоваться самыми современными и инновационными инструментами в соответствии с выработанными процедурами для управления угрозами ИБ и снижения уровня риска.





Sneak Peak. SOC изнутри

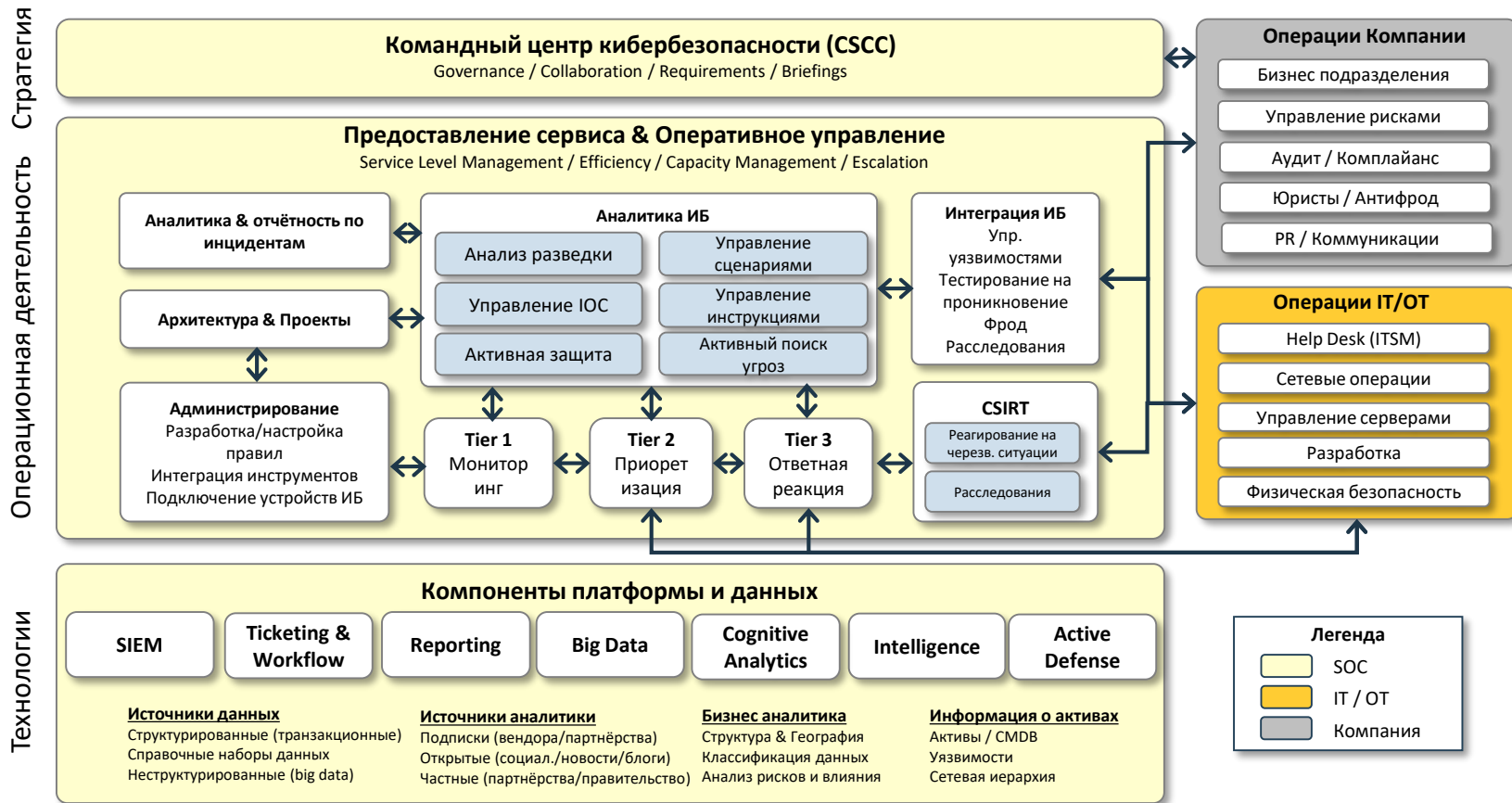
Операционная
модель

Техническая
архитектура

Оргструктура

Процессы,
методологии

Операционная модель для построения SOC нового поколения (типовая модель IBM)

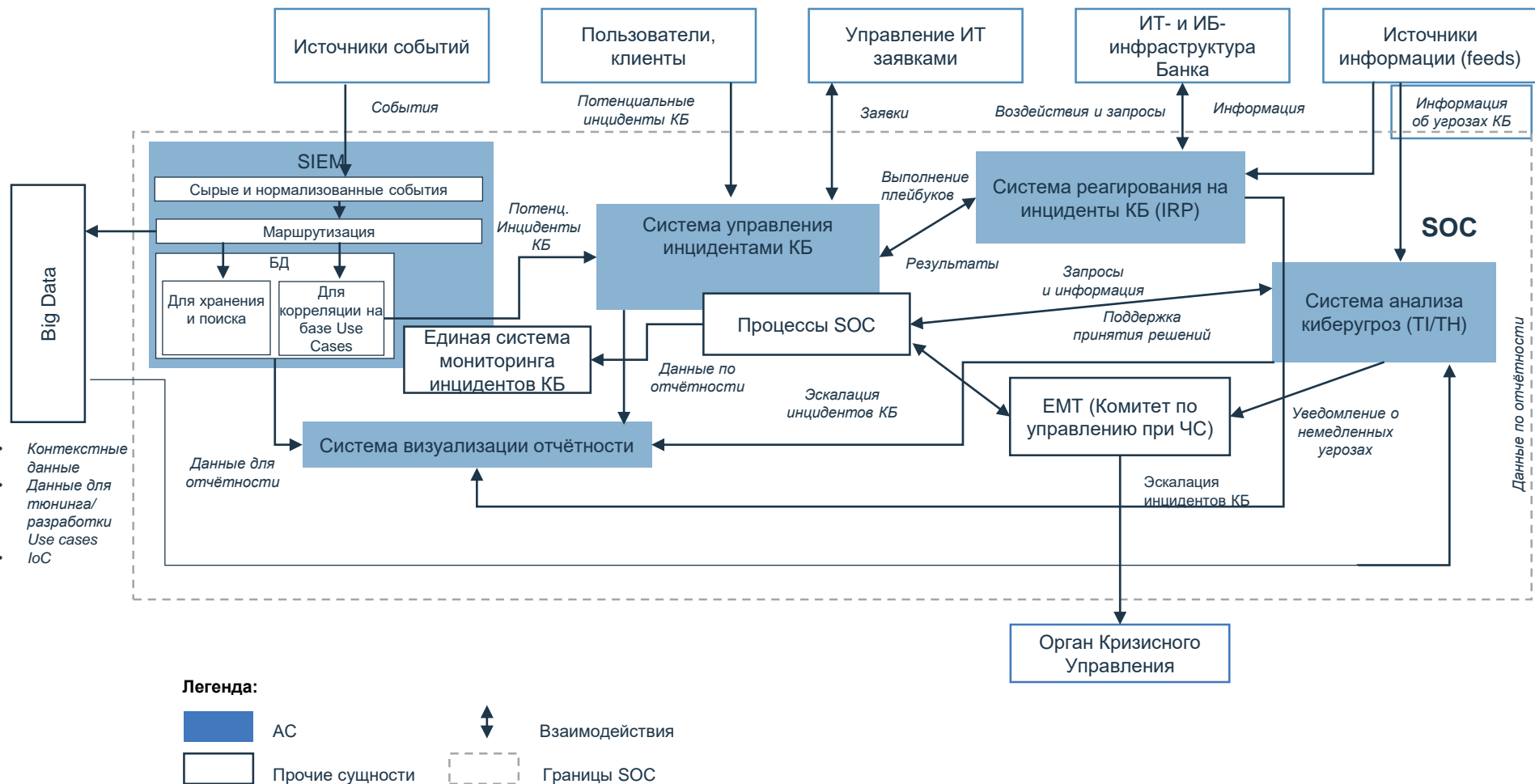


Методология UseCase - подход «Сверху вниз» при разработке сценариев мониторинга



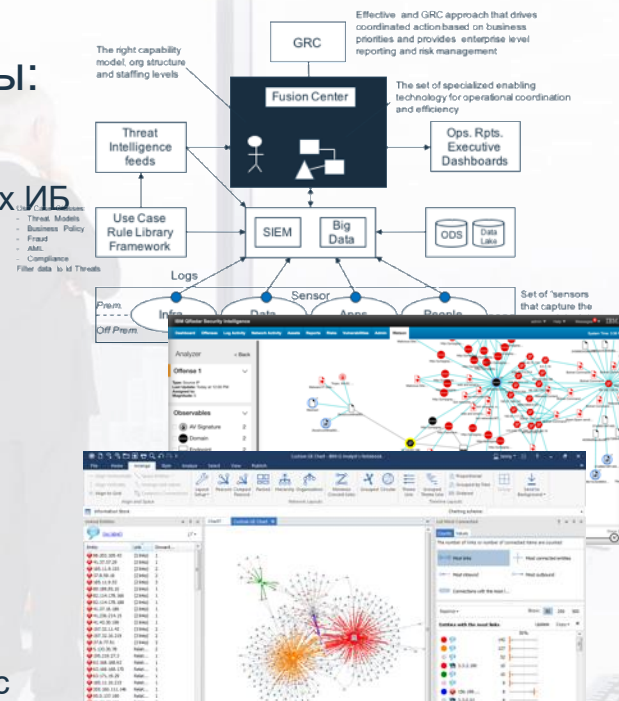
1. Бизнес определяет релевантные риски и угрозы
2. SOC обеспечивает мониторинг реализации этих угроз **посредством сценариев (Use Case) и правил SIEM**
3. При обнаружении реализации угрозы регистрируется инцидент
4. Инцидент обрабатывается согласно определённым приоритетам

Техническая архитектура SOC (пример)



Дальнейшее развитие? SOC 2.0 – Концепция «Fusion Center»

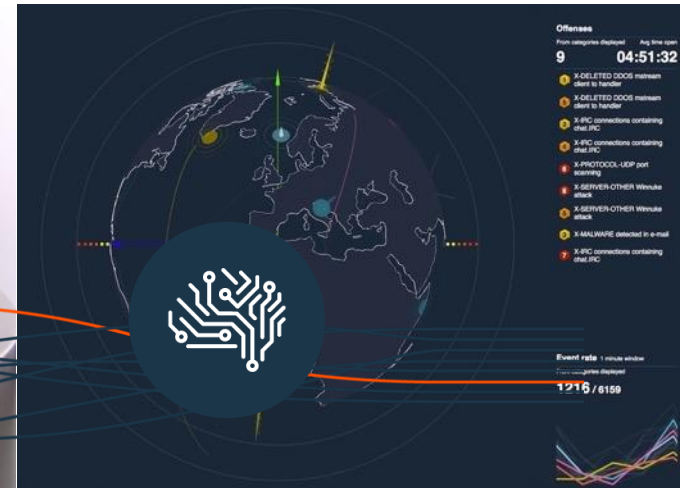
- Термин Fusion Center в применении к Кибербезопасности не является устоявшимся, и применяется различными консультантами в разных значениях.
- Тем не менее, можно выделить общие моменты:
 - **Расширение информации**, с которой работает SOC в рамках аналитики за пределы структурированной информации о событиях ИБ и создания единого «Озера данных безопасности»
 - Смежные события – антифрод, физическая безопасность
 - Неструктурированная информация – соцсети, пресса, публикации
 - Широкий **обмен информацией безопасности** внутри и вовне организации
 - Обмен с смежными внутренними функциями безопасности, 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.



Дальнейшее развитие? SOC 2.x - За пределами внутреннего SOC.

Предоставление услуг мониторинга ИБ сторонним организациям:

- SOC и Fusion Center требуют больших вложений, как на уровне CAPEX так и OPEX, и большого числа обученных, профессиональных сотрудников.
- Один из возможных вариантов развития внутреннего SOC для оправдания финансирования столь сложной структуры – оказание услуг сторонним компаниям, модель Managed Security Services Provider.
- Переход к поставке услуг MSS SOC – опыт как компании IBM, так и её ключевых заказчиков.



SOC как повод для гордости

Центр управления кибербезопасностью
Сбербанка получил сертификат соответствия
международному стандарту ISO/IEC
27001:2013

13.12

По словам представителя Сбербанка, в конце 2017 года на ряд организаций, в том числе финансовых, были организованы массированные кибератаки. Сбербанк отразил 100% попыток атак за счет работы собственного Security Operation Center (SOC).

13 декабря 2017 года, Москва — Сбербанк стал первым банком в России, чей центр управления кибербезопасностью (Security Operation Center – SOC) сертифицирован Британским институтом стандартов (BSI) на соответствие международному стандарту ISO/IEC 27001:2013.

В Сбербанке, как заявил зампред, открыта программа «Кибербезопасность 2018». Банк активно совершенствует собственный SOC. Центр функционирует в режиме 24x7 и расположен на 5-ти площадках в Санкт-Петербурге, Самаре, Екатеринбурге, Новосибирске с головным отделением в Москве. Подключено около 18 тысяч устройств безопасности, что позволяет отслеживать в режиме онлайн функционирование порядка 300 тысяч элементов инфраструктуры.

Как отметил Станислав Кузнецов, в день регистрируется и расследуется порядка 200 событий информационной безопасности. В ближайшее время центр перейдет на новую технологию работы с использованием BigData и Machine Learning. Планируется обеспечение мониторинга защиты не только российских подразделений Банка, но и зарубежных дочерних обществ и банков. В ближайшие месяцы к системе фрод-мониторинга будет подключен первый дочерний банк в Хорватии.



Примерно год назад «Банковское обозрение» опубликовало интервью с Сергеем Лебедем, руководителем службы кибербезопасности Сбербанка. За прошедший год команде ИБ Сбербанка удалось достичь многого. В преддверии Форума Finopolis 2017 мы попросили Сергея Васильевича подробнее рассказать о результатах проделанной работы.

— Сергей Васильевич, что было сделано за прошедший год по повышению уровня зрелости SOC? На какие методики оценки вы при этом опирались?

В этом году мы уже дважды провели оценку уровня зрелости по всем направлениям кибербезопасности, в том числе и по направлениям работы SOC. Для оценки использовалась шкала CMMI (Capability Maturity Model Integration) — так называемая методология совершенствования процессов. Эта шкала предполагает пятибалльную оценку. В начале года наша оценка в части управления инцидентами ИБ составляла 2,2, а в середине — уже 3,2. Это хороший темп. Уровень мировых лидеров среди финансовых организаций сейчас составляет 3,6, и мы будем стараться его превзойти.

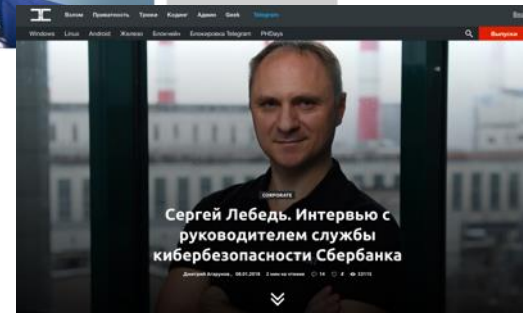
Герман Греф: «Мы начинаем
монетизировать свою компетенцию в
области кибербезопасности»



Сбербанк не прерывал свою деятельность из-за хакерских атак в 2017 г.

Александр Амосов, 22 ноября 2017
КОММЕНТАРИИ

Сбербанк не прерывал бизнес-процессы и обслуживание клиентов банка из-за хакерских атак в 2017 г., сообщил на пресс-брифинге SOC-форума 2017 руководитель службы кибербезопасности Сбербанка Сергей Лебедь.




Если говорить о процессах, то раньше у нас был один процесс, а сейчас двадцать семь процессов в рамках операционной деятельности. В качестве основы мы выбрали операционную модель Security Operation Center, разработанную компанией IBM. Перед этим мы изучили все существующие в мире модели, глубоко погрузились в решения Hewlett-Packard, Dell, Microsoft, Cisco и в итоге выбрали модель IBM, как наиболее зрелую и способную к жизни.

Работа RedTeam очень важна, потому что в прошлом году мы запустили крупнейший в Европе проект по строительству Security Operation Center. Для нас SOC — это не экраны и не консоли управления. Для нас это прежде всего процессы и правила действия наших сотрудников. Для нас это огромная трансформация сознания. Если раньше задача дежурной службы заключалась в том, чтобы подсчитать и доложить, сколько операций на средствах защиты, связанных с внесением изменений, они провели за сутки, то относительно недавно мы начали действительно управлять рисками безопасности в нашей инфраструктуре, и RedTeam помогает отлаживать наши же процессы.



СПАСИБО

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.