Security Intelligence.
Think Integrated.

От реагирования на угрозы информационной безопасности к их предотвращению

Системы информационной безопасности IBM – Guardium, IPS/XGS, QRadar

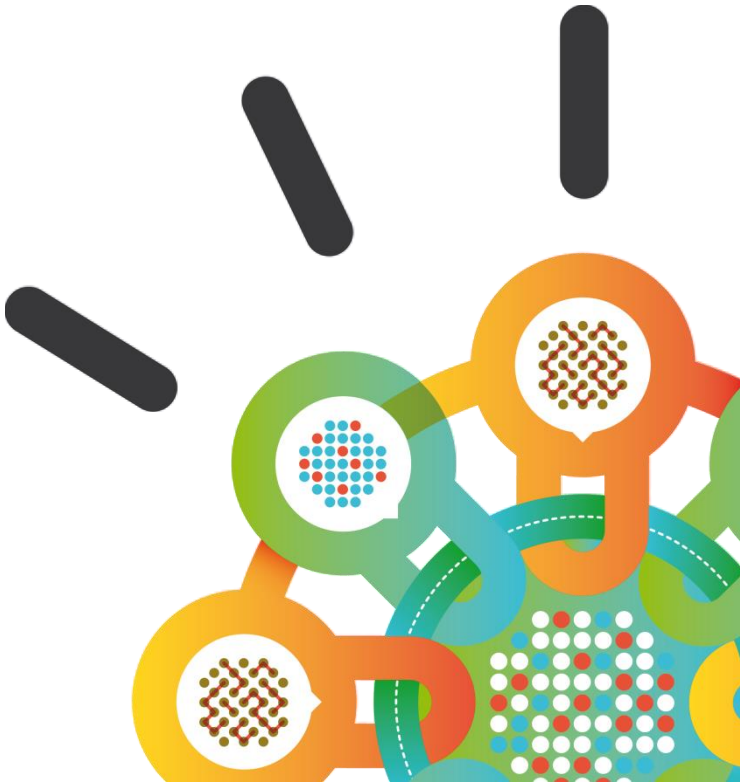
Константин Глушков

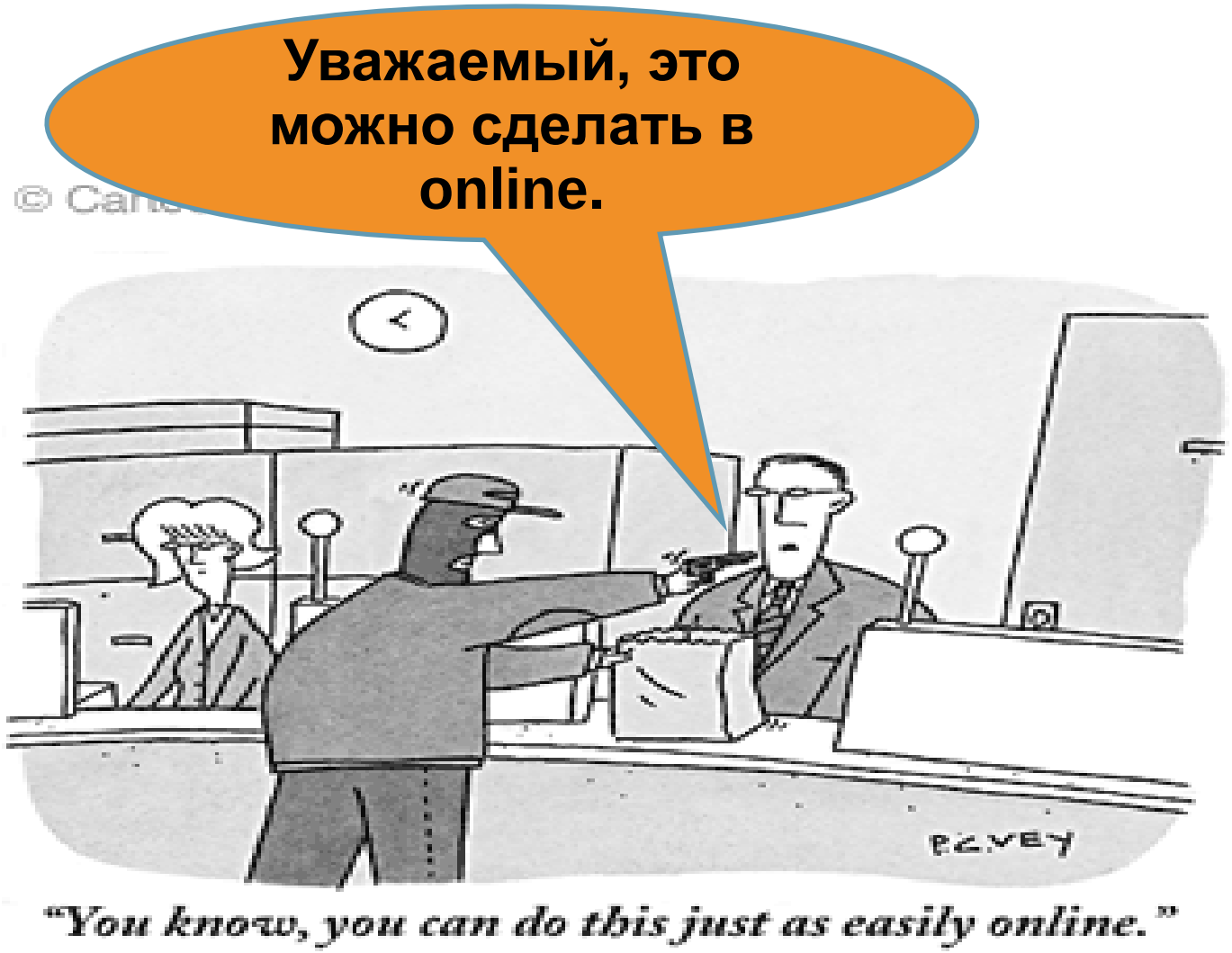
Business Partner Representative in Ural region

Software Group, IBM EE/A

glushkov@ru.ibm.com

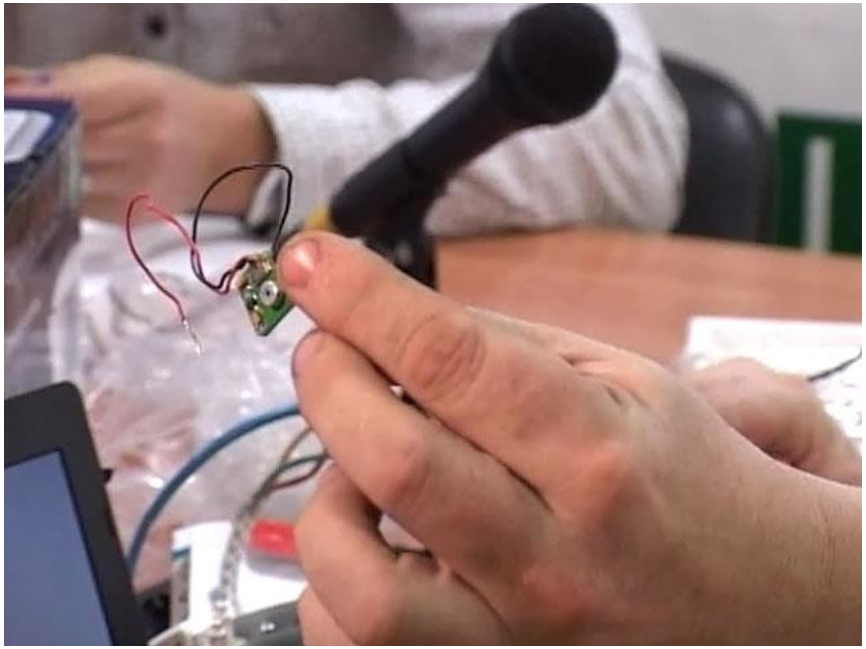
Апрель 2014





УТЮГИ – ШПИОНЫ в СПБ

- Утюги, чайники и телефоны из Китая
- Чип, который подключается по Wi-Fi к незащищенным компьютерам
- Что будет дальше?



Организованная кибер-преступность

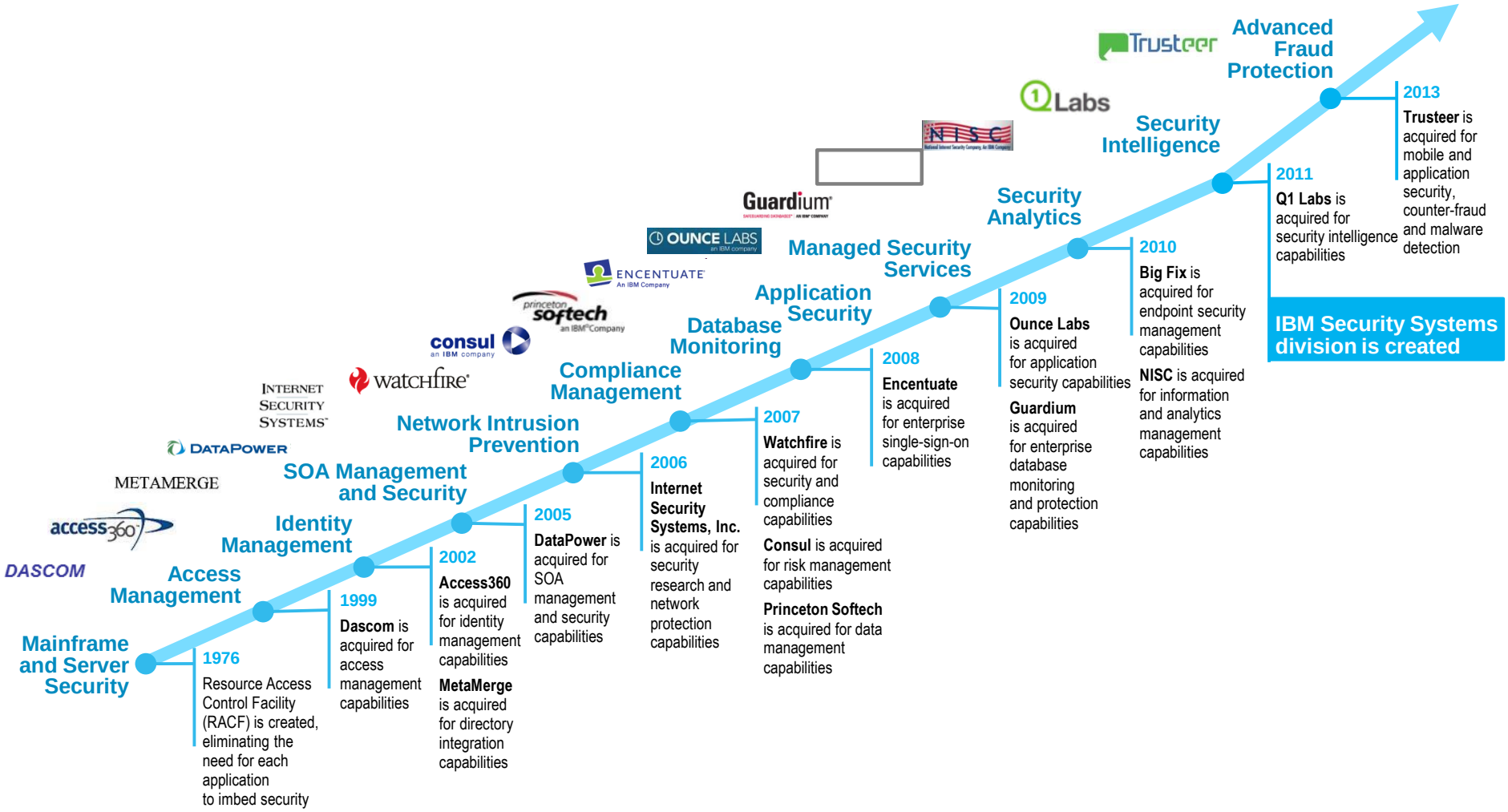
«... кибер-преступность обходится человечеству дороже наркотрафика кокаина, марихуаны и героина вместе взятых...»

«... 80% интернет-преступлений совершается транснациональными организованными бандами...»

«... ориентировочная стоимость киберпреступности в Европе составила 979 млрд долл. в год...»

Бун Хуэй Ху,
Конференция Интерпола,
2012

IBM Security. 15 компаний за 37 лет

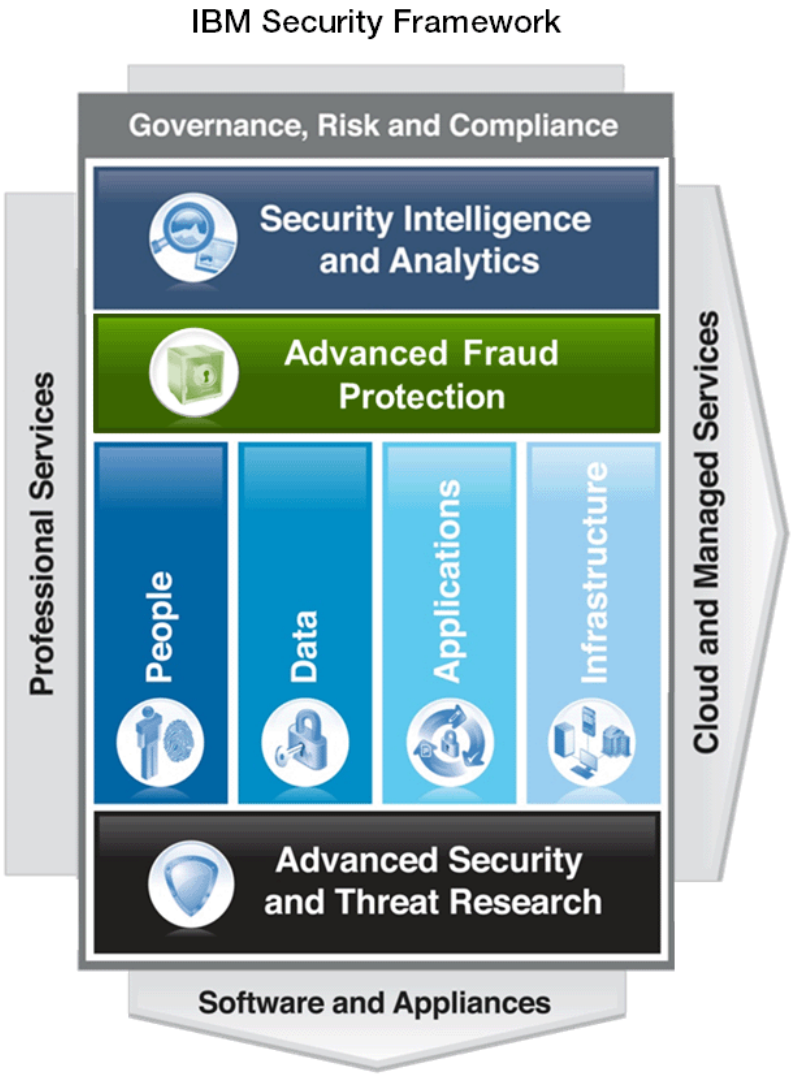


IBM Security. Портфель решений

IBM Security Systems

- Новое название, объединяющее все предложения IBM в области безопасности
- Широкий набор продуктов, покрывающий все основные домены ИБ
- Глобальный уровень инвестиций в технологии ($1.8мрлд), 6K+ специалистов по ИБ
- Исследовательская группа X-Force®

Intelligence • Integration • Expertise



X-Force это основа всех продуктов IBM Security

X-FORCE

Миссия X-Force это:

- **Мониторинг** и оценка быстро меняющегося ландшафта ИБ
- **Изучение** новых техник атак и разработка защиты от завтрашних угроз
- **Информирование** наших клиентов и общественности

Обнаружение и анализ угроз. Исследования в области безопасности

Покрытие

20,000+ устройств под контролем

3,700+ клиентов на управлении по всему миру

15B+ обрабатываемых событий в день

133 страны присутствия (MSS)

1,000+ патентов в области ИБ

X-FORCE

IBM Research

Точность

20B проанализированных web страниц и образов

40M спам и фишинг атак

76K задокументированных уязвимостей

Billions попыток вторжений каждый день

Millions уникальных образцов зловреда

Обнаружение и анализ угроз беспрерывно

8 центров управления + 9 центров исследования + в 133 странах + 20000+ устройств под контролем + 3700+ клиентов на управлении + 4 млрд + событий ежедневно

Достаточно ли средств защиты?

Мы используем Firewall

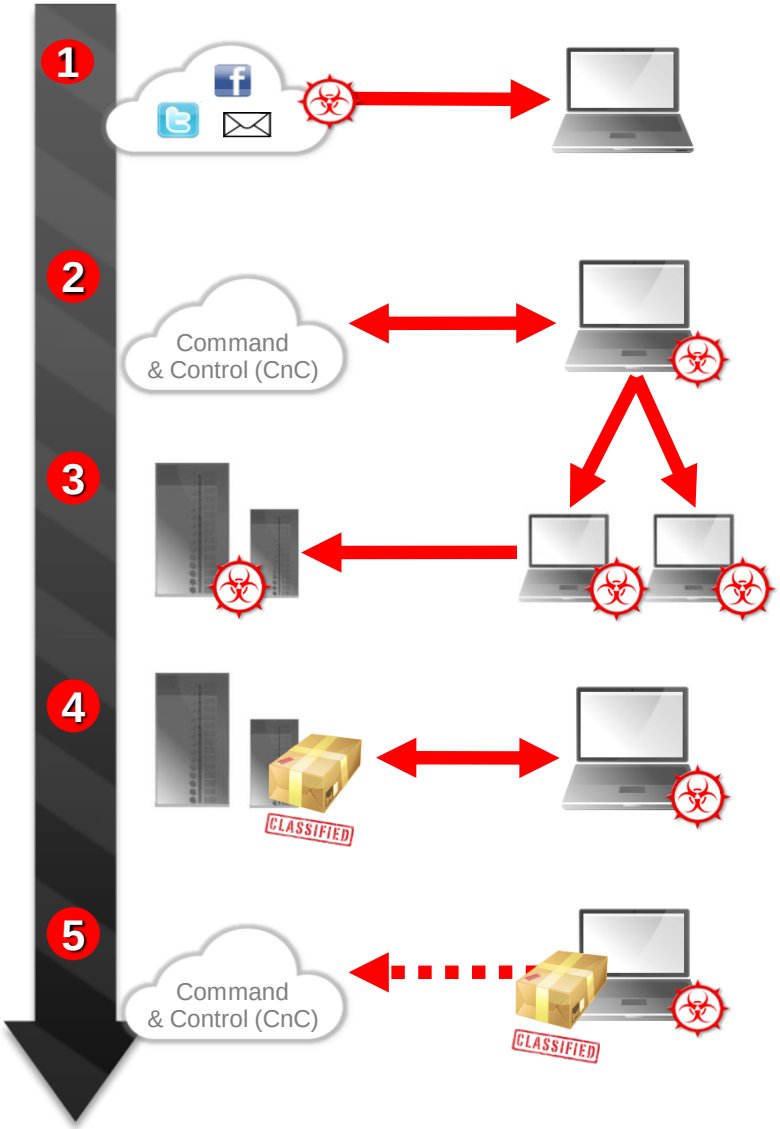
Да кому мы нужны?

Мы используем сетевые сканеры

Мы уже используем SSL

Угрозы становятся более организованными

5 этапов современной атаки



Разведка — Подготовка к проникновению в сеть

Проникновение — Коммуникация с центром

Распространение — Расширение присутствия в сети организации

Сбор — Поиск и консолидирование важных данных

Выгрузка — Передача данных в центр

Подход IBM для защиты от сложных атак

Network and Endpoint Security
Использование технических контролей для безопасности сети и управления хостами

Network Security Использование SIEM + SP + IPS для детектирования неизвестных угроз

Secure Users Обеспечение безопасности пользователей, мониторинг и детектирование подозрительной активности

Data Security Обеспечение безопасности данных, постоянный мониторинг и контроль доступа к критичными данным

Network Security Постоянный мониторинг сетевого трафика и предотвращение нелегитимных соединений

Security Analytics
Интеллектуальный анализ по всей инфраструктуре…

Использование исследовательских данных для детектирования новых угроз…

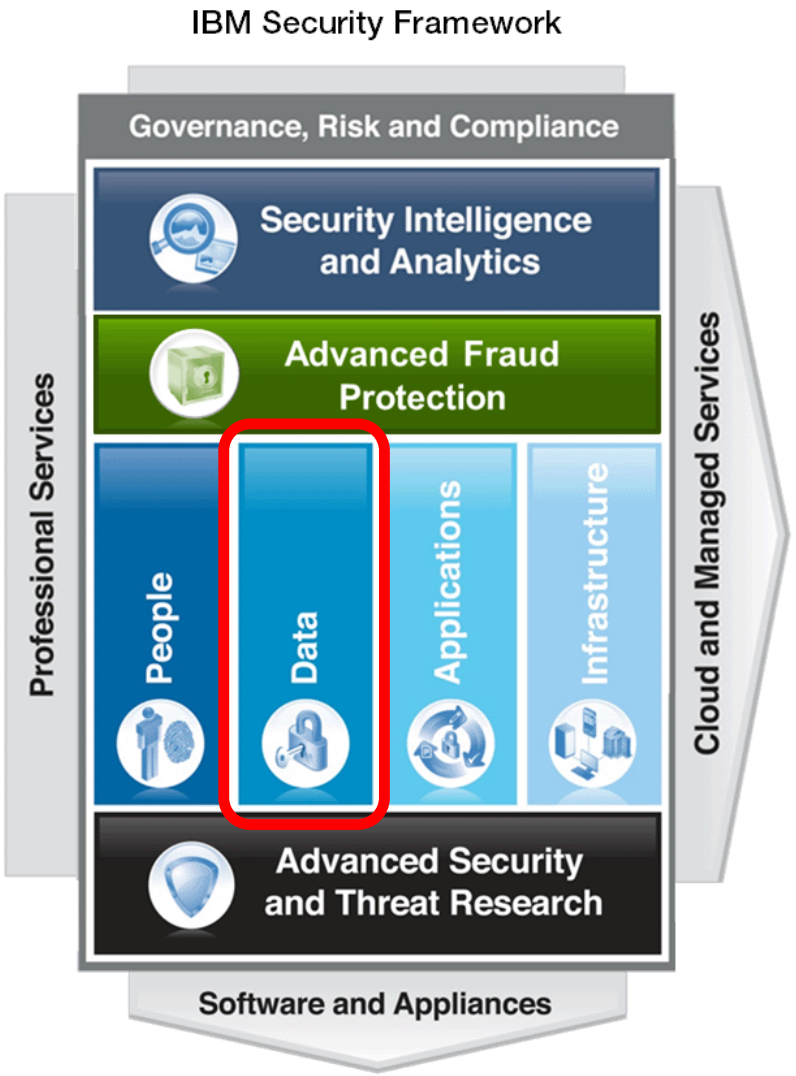
Использование сервисов безопасности для устранения риска

Security **Intelligence**. Think **Integrated**.

Решение от IBM Security

Guardium

Защита и аудит баз данных



3 основые причины мониторинга СУБД

1. Внутренние угрозы
   - Неавторизованные изменения
   - Предотвращение утечек данных

2. Внешние угрозы
   - Предотвращение кражи данных

3. Нормативные требования
   - Упрощение процессов
   - Сокращение затрат

О компании Guardium

Компания Guardium специализируется на решениях по защите СУБД. Решения компании используются более чем в 350-ти центрах обработки данных, а также в ведущих компаниях по всему миру.

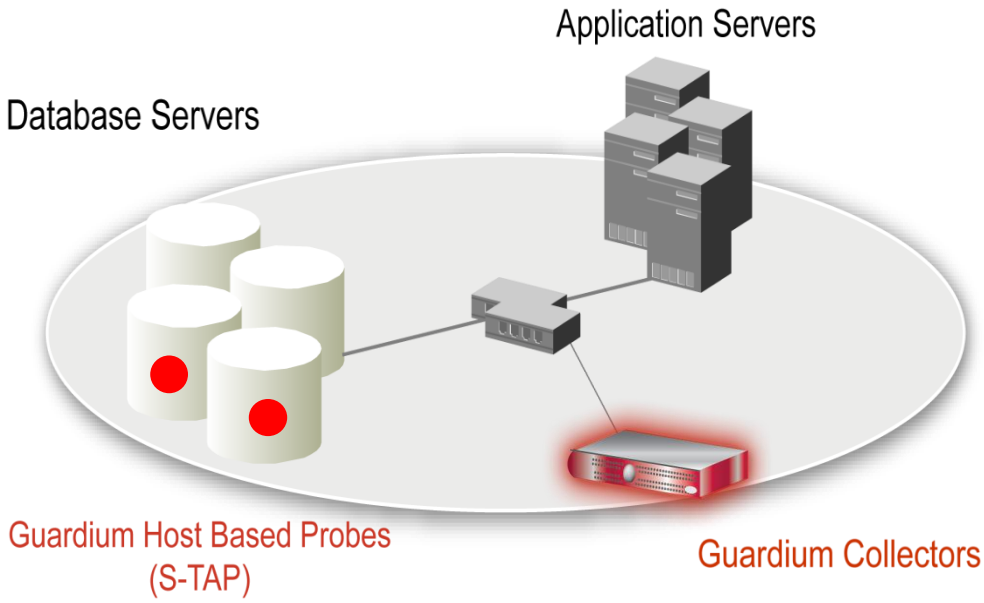
Основанная в 2002 году, Guardium была первой в мире компанией, производящей решения для устранения уязвимостей в защите баз данных бизнес-систем в режиме реального времени.

Компания Cisco – стратегический инвестор Guardium.

Guardium – партнер компании IBM (сегодня часть IBM), Oracle, Microsoft, Sybase, BMC, EMC, RSA, Accenture, NetApp, McAfee и NEON. Является членом IBM Data Governance Council и PCI Security Standards Council.

Guardium®
SAFEGUARDING DATABASES™

Мониторинг БД в реальном времени



- Продуманная архитектура
  - Вне базы данных
  - Минимальное влияние на производительность (3 - 5%)
  - Не нужно менять БД и приложение
- Универсальное решение для разных СУБД
- 100% контроля, включая локальный доступ DBA

- Обеспечивает разграничение полномочий
- Не полагается на логи в БД, которые могут быть стерты злоумышленниками
- Детальные политики и аудит в реальном времени
  - *Кто, что, когда, как*
- Автоматическая отчетность (SOX, PCI, NIST, и т.д.)

Соответствие законам и стандартам: ФЗ №152

Требование	Функционал Guardium
Обеспечение конфиденциальности ПДн (ст. 7)	Аудит запросов к объектам БД с ПДн Аудит действий DBA Блокирование неавторизованных действий
Наличие технических мер по защите ПДн от (ст. 19): . неправомерного или случайного доступа . уничтожения . изменения . блокирования . копирования . распространения	Аудит выборок из объектов БД с ПДн Аудит действий DBA Блокирование неправомерных действий Аудит DML-команд
Функции СЗПДн ИС (п.2.2 приказа ФСТЭК России №58): . управление доступом . регистрация и учёт . обеспечение целостности . анализ защищённости	Блокирование неправомерных действий Аудит запросов к БД Аудит исключений СУБД Аудит DML-команд Анализ уязвимостей
Регистрация попыток доступа к записям и полям записей (п. 4.2 и 4.3 приказа ФСТЭК России №58)	Аудит всех запросов к объектам БД с ПДн

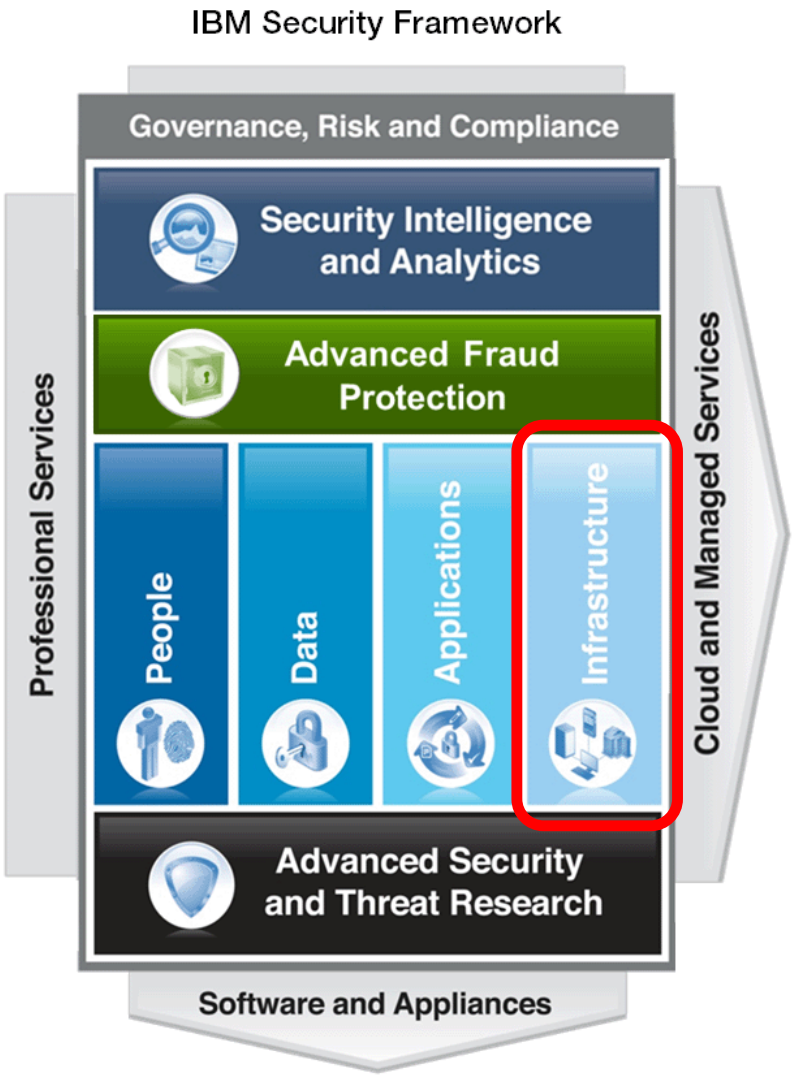
Решение Guardium – защита данных

- Мониторинг транзакций СУБД в реальном времени
- Упрощение прохождения аудита и соответствия SOX, PCI-DSS
- Управление изменениями БД
- Управление уязвимостями СУБД
- Предотвращение утечки данных из БД
- Мониторинг транзакций СУБД для мейнфреймов

Guardium®
SAFEGUARDING DATABASES™

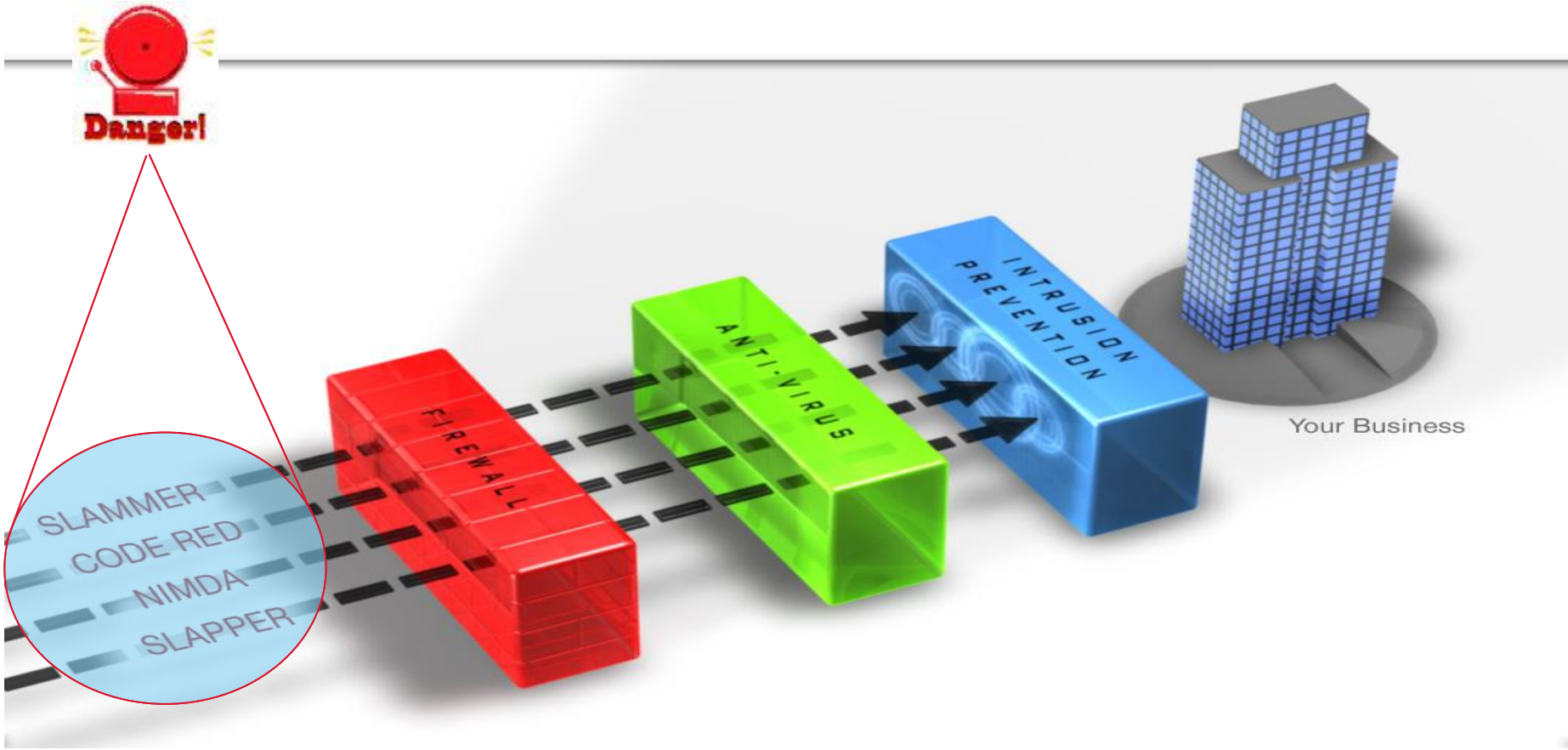
Intrusion Prevention System (IPS и XGS)

Сетевые системы предотвращения вторжений



Три рубежа защиты сети

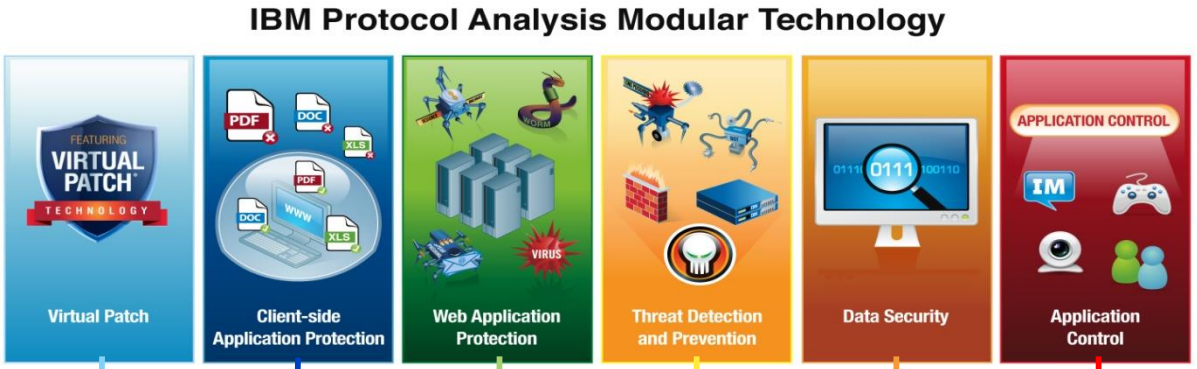
Intrusion Detection / Prevention



IBM X-Force Research

Возможности Protocol Analysis Module

С использованием информации из X-Force, защита становится надежнее



Virtual Patch

Возможность закрывать узявимости, не устанавливая патчей и не изменяя конфигурации систем

Client-Side Application Protection

Защита поль-зователей от уязвимостей прикладного ПО: Microsoft Office, Adobe PDF, Multimedia files and Web browsers

Web Application Protection

Защита веб приложений от атак (Web Application Firewall)

Threat Detection & Prevention

Защита от неизвестных типов уязвимостей и атак, используя Shellcode Heuristics (SCH)

Data Security

Борьба с утечкой данных

Application Control

Контроль приложений и сервисов

IBM Security Network Protection XGS 5100

ЗАЩИТА ОТ УГРОЗ	КОНТРОЛЬ СЕТЕВОЙ АКТИВНОСТИ	ИНТЕГРАЦИЯ
Защита от угроз, благодаря уникальной базе X-Force®	Определение аномалий в трафике, гибкие политики доступа	Интеграция с решениями IBM Security

XGS5100. IPS нового поколения

Новый IPS XGS 5100 помогает защититься от всего спектра целевых атак, от системных атак до атак и рисков, связанных с пользователями

Инфраструктура

System-level Attacks

Service-level Attacks

Web Application Attacks

Пользователи

Spear Phishing

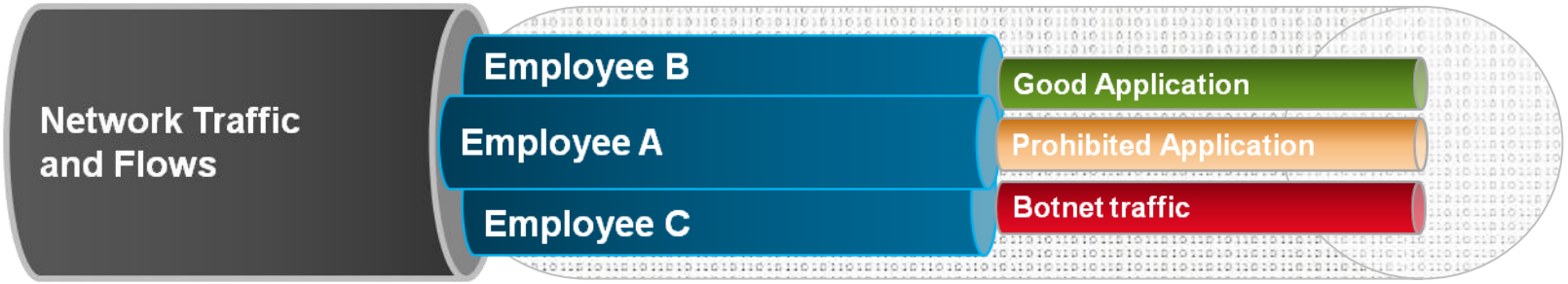
Malicious Attachments

Web/Social Media Risks

Расширяемые модули защиты и непрерывные апдейты от *IBM X-Force® Research and Development Team*

Анализ трафика и защита на 7 уровне сети

XGS это уникальная комбинация продвинутой системы защиты от атак и высокопроизводтельного прокси



DPI

Аутентификация

Разграничение доступа

400+	1,950+	20 Млрд+
Протоколов и форматов файлов	Приложений	Сайтов и 70 категорий

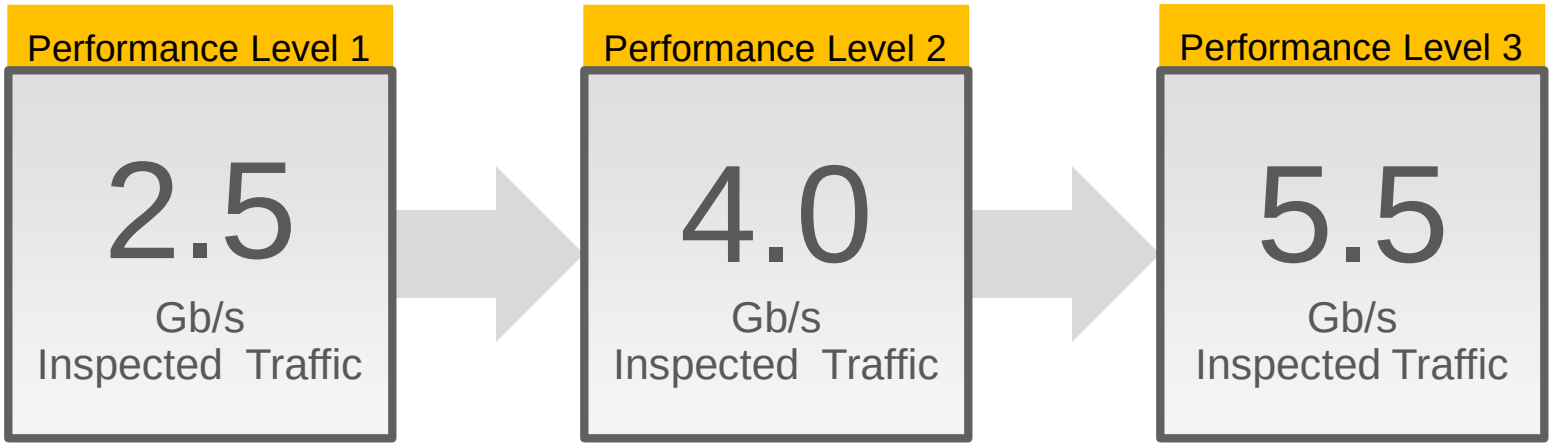
Сетевые интерфейсные модули

Два модуля с семью различными вариантами интерфейсов позволяют XGS 5100 быть более гибким для подключения

Interface Type	Ports
RJ-45 copper w/ built-bypass	8
Fixed fiber (SX) w/ built-bypass	4
Fixed fiber (LX) w/ built-bypass	4
10GbE (SR) w/ built-bypass	2
10GBE (LR) w/ built-bypass	2
SFP (requires transcievers)	4
10GbE SFP+ (requires transcievers)	2

Гибкое лицензирование производительности

Три уровня производительности позволяют производить апгрейд лицензионно, без необходимости менять «железо»



Новый отдельно лицензируемый функционал XGS 5100

1. **SSL/TLS Инспекция**
   Помогает защитить от атак, содержащихся в пользовательских зашифрованных сессиях

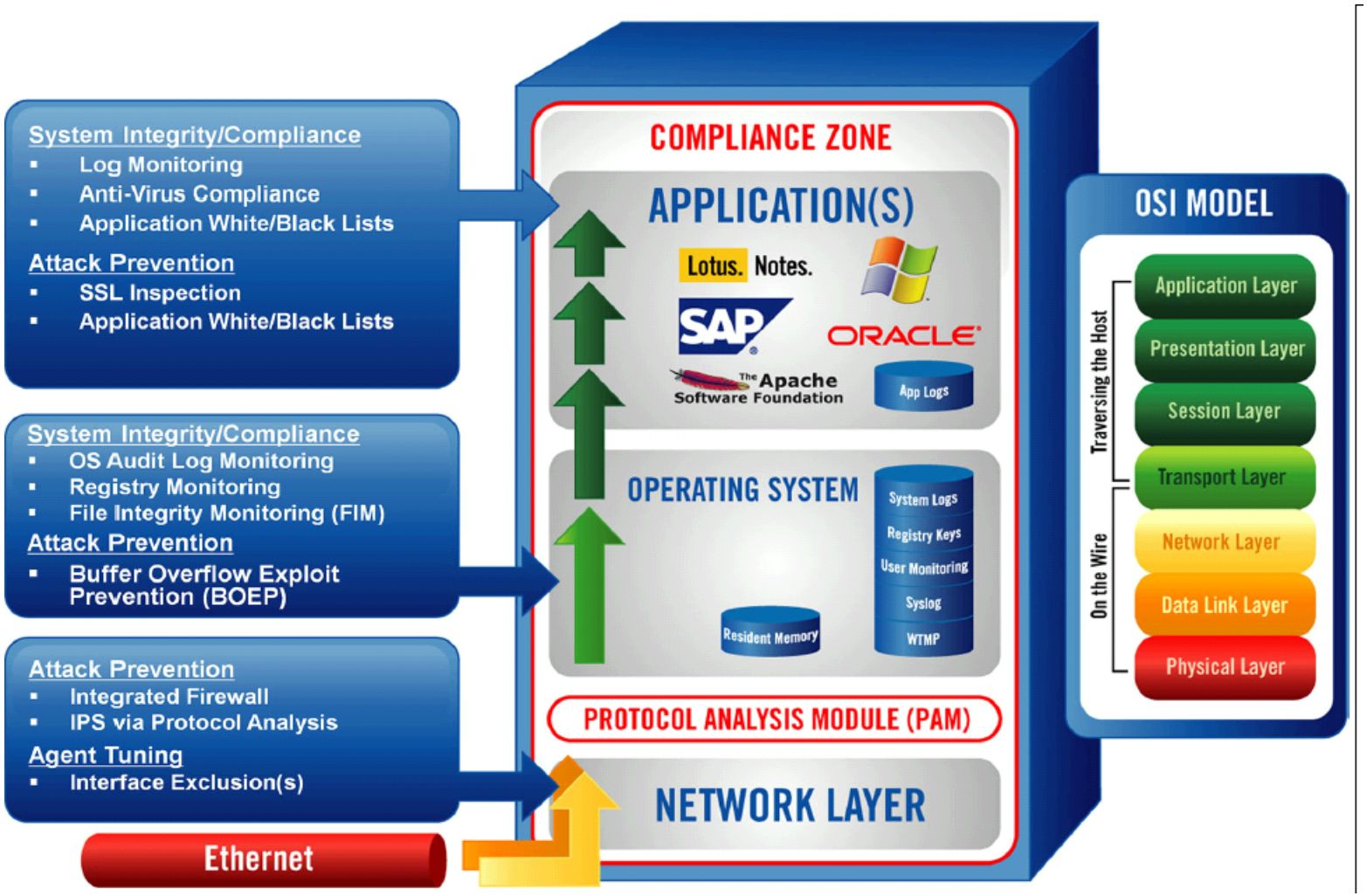
2. **База IP-репутации**
   Использует X-Force базу IP-репутаций, чтобы добавить дополнительную информацию в событие безопасности

3. **База URL-фильтрации и Контроль приложений**
   Использует X-Force базу Web-ресурсов и возможности контроля действий приложений для грунулированного управления и безопасного пользовательского доступа к Web ресурсам и приложениям

Линейка XGS пополняется

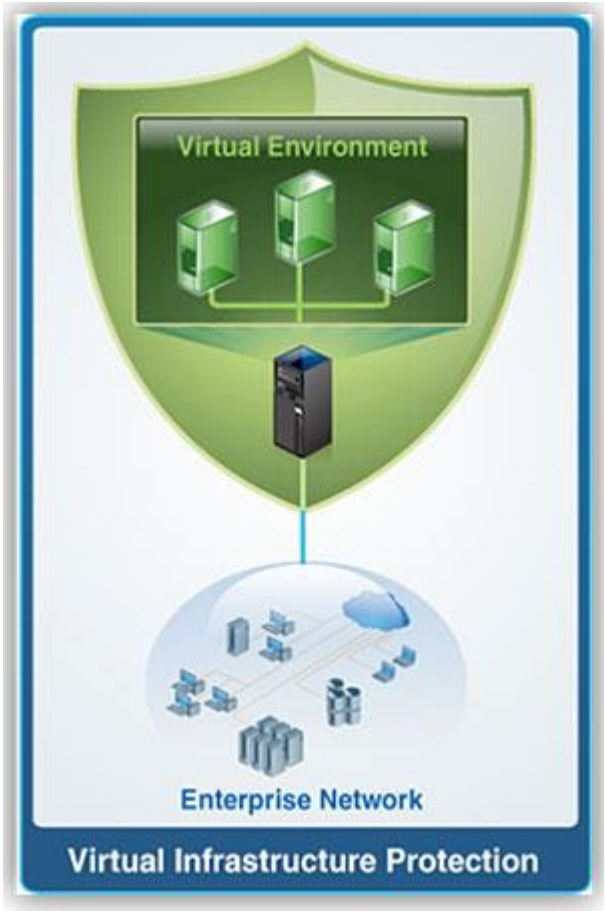
- XGS3100, XGS4100 – уже в продаже.
- XGS7100 – скоро будет...

Защита критичных серверов



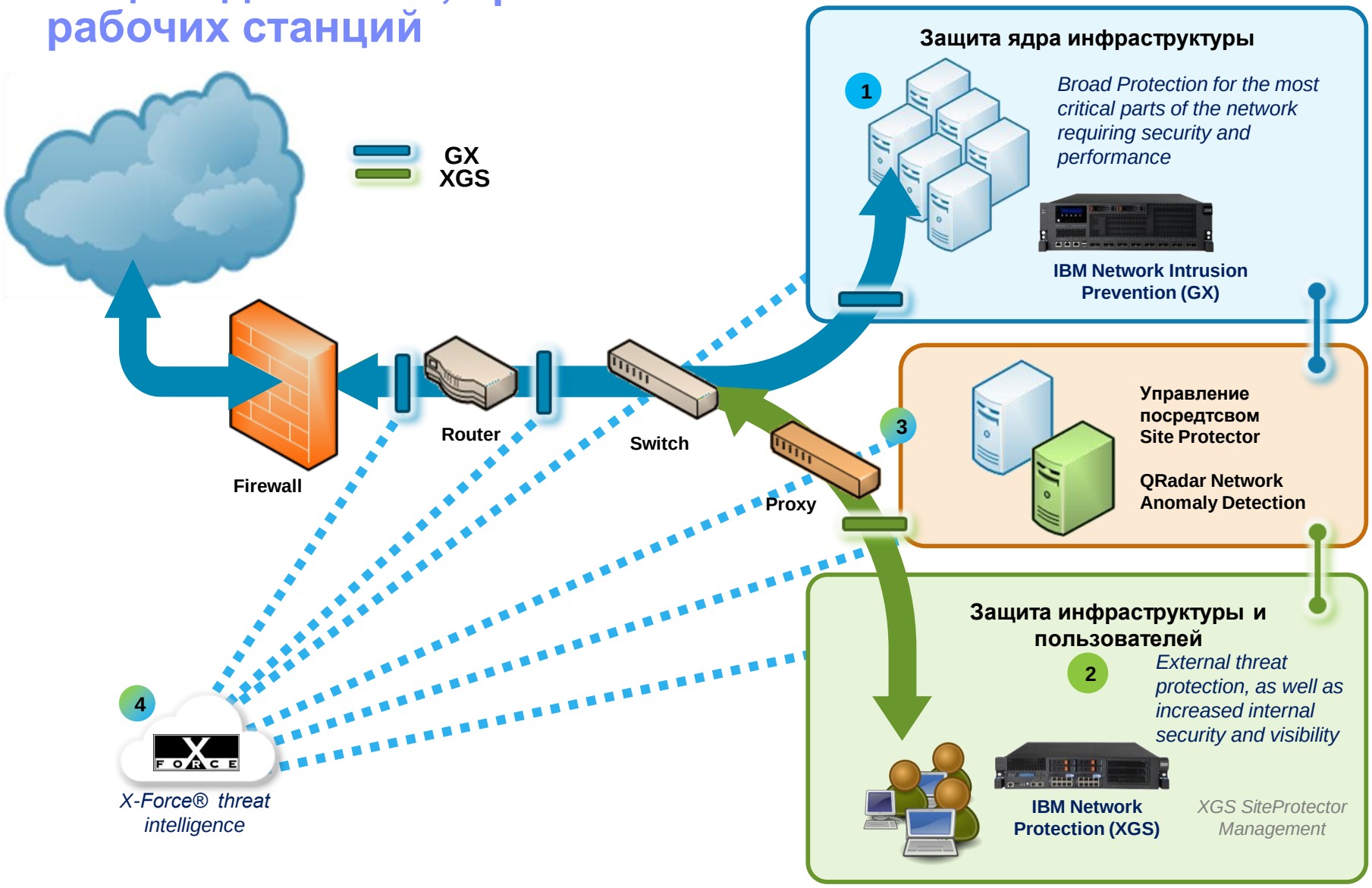
Защита виртуальной инфраструктуры

- Интеграция с VMsafe на уровне гипервизора
- Обнаружение руткитов
- Предотвращение «кражи» ВМ
- Обнаружение поддельных ВМ
- Анализ трафика между ВМ
- Управление разрастанием ВМ
- Аудит доступа администраторов
- Файервол для контроля доступа на сетевом уровне
- Защита виртуальных сегментов
- Централизованное управление
- Виртуальный патч от X-Force



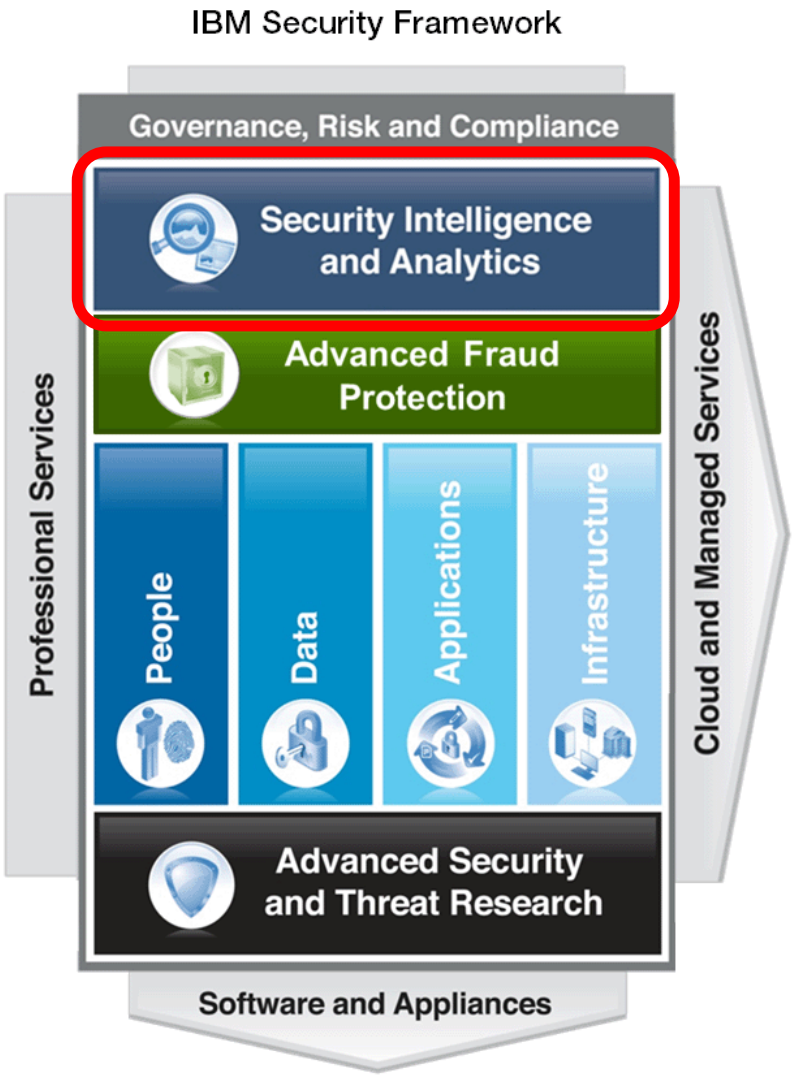
Централизованное управление безопасностью - Site Protector

Защита для сетей, приложений и конечных рабочих станций



QRadar

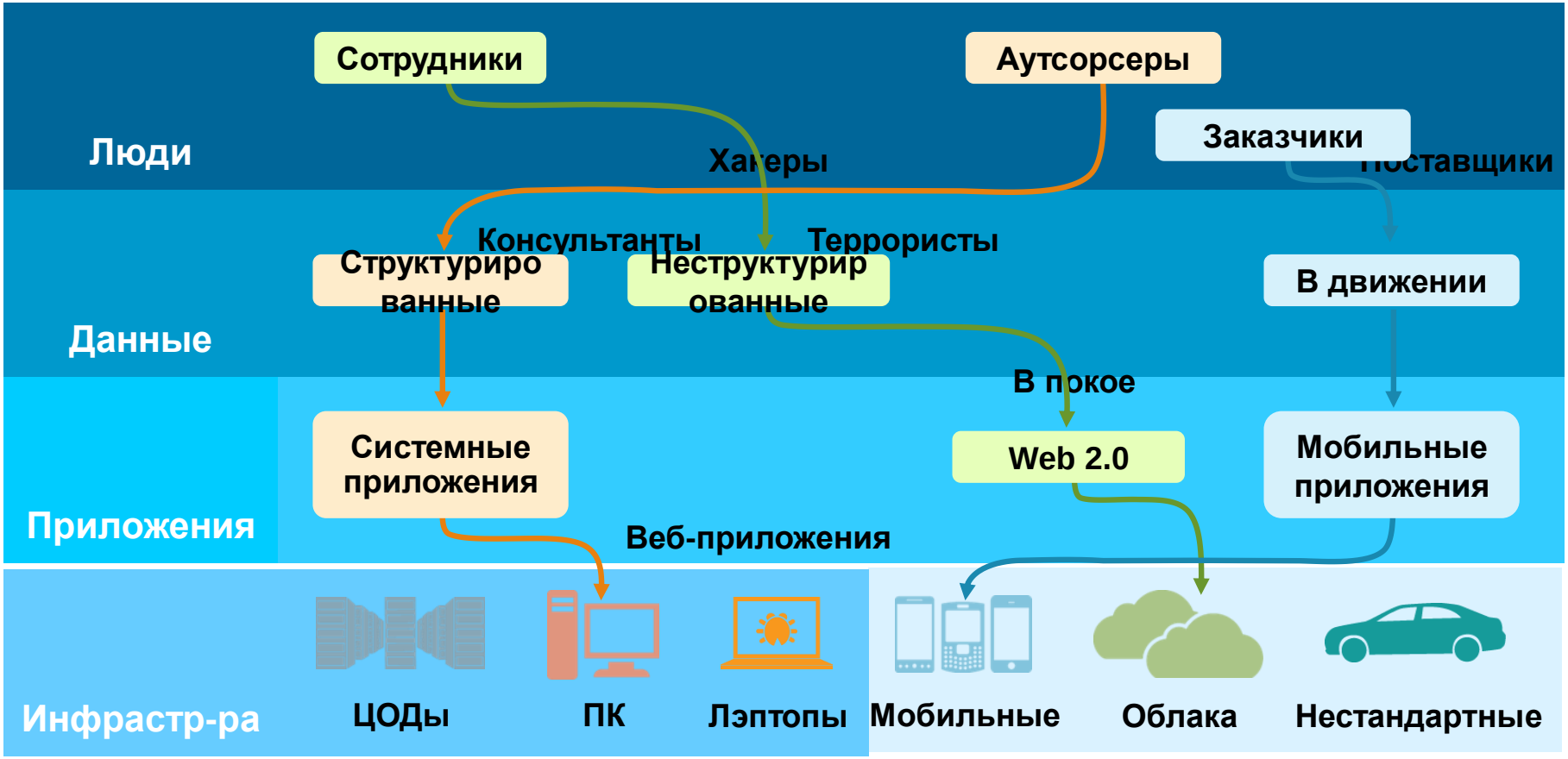
Выявление инцидентов информационной безопасности



Ландшафт угроз сегодня невероятно сложен, динамичен и целенаправлен – требуется иной уровень интеллекта, чтобы понимать и управлять им

- Угрозы сегодня динамичны
  - Ежедневно создаются десятки тысяч экземпляров вредоносного ПО
  - Новые классы угроз непрерывно создаются и совершенствуются
  - Топология угроз изменяет форму и превращается в сеть серверов и конечных точек, соединения между которыми динамически создаются и разрываются
- Угрозы сегодня сложны
  - Полиморфные программы преобразуют вредоносное ПО при каждом использовании
  - Распространение мобильных устройств, облачных вычислений, виртуализации (и взаимопроникновение этих технологий) обеспечивает плодородную среду для новых угроз и вредоносного ПО
- Угрозы сегодня целенаправлены
  - Это не случайные атаки, а организованные, целеустремленные и мотивированные
  - Существует целый “черный рынок”, производящий вредоносное ПО и автоматизированные средства

Вызовы ИБ – это сложный четырехмерный паззл…



…, который требует нового подхода


Виден шум

Что такое Security Intelligence

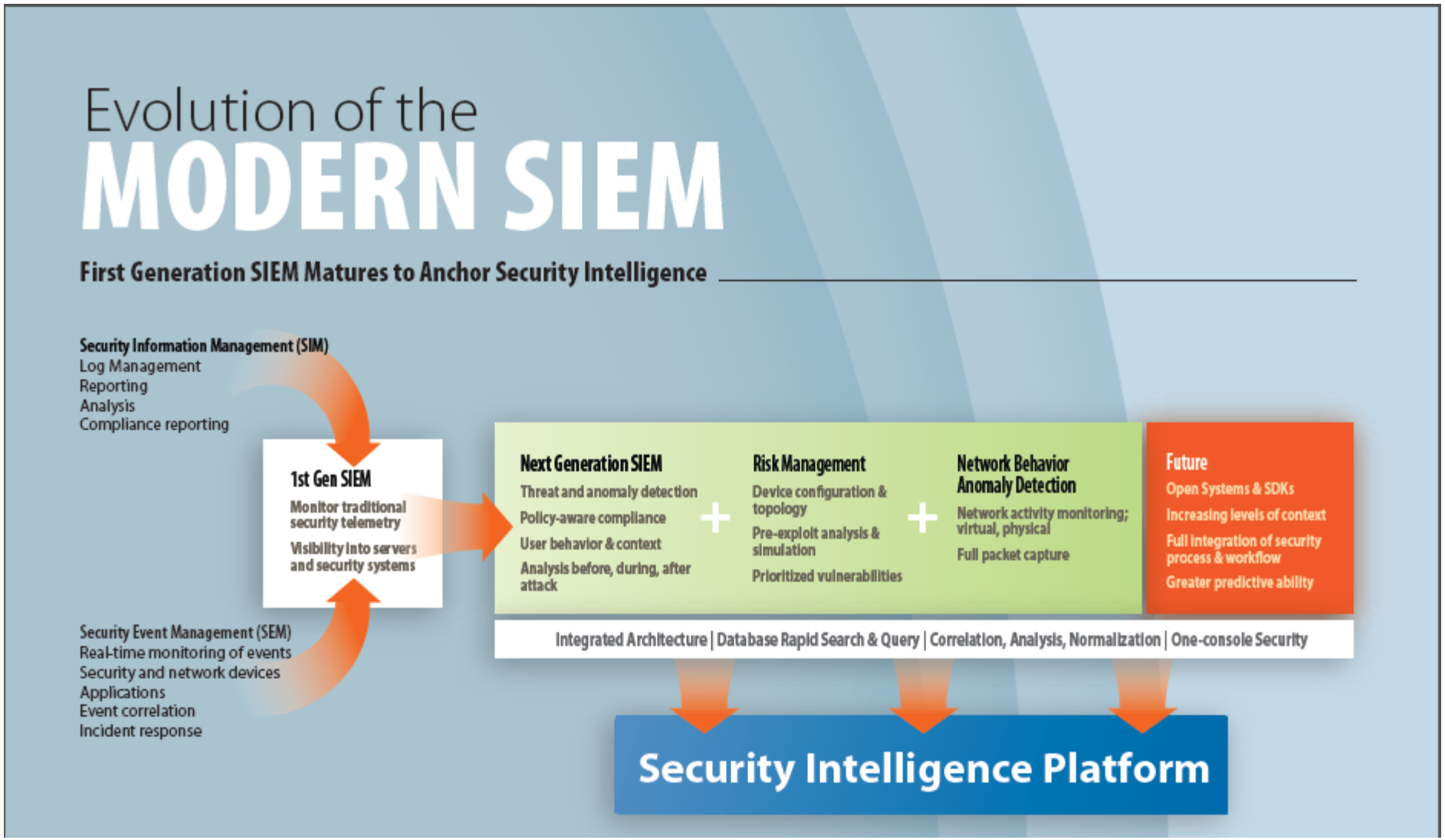
Security Intelligence

--существительное

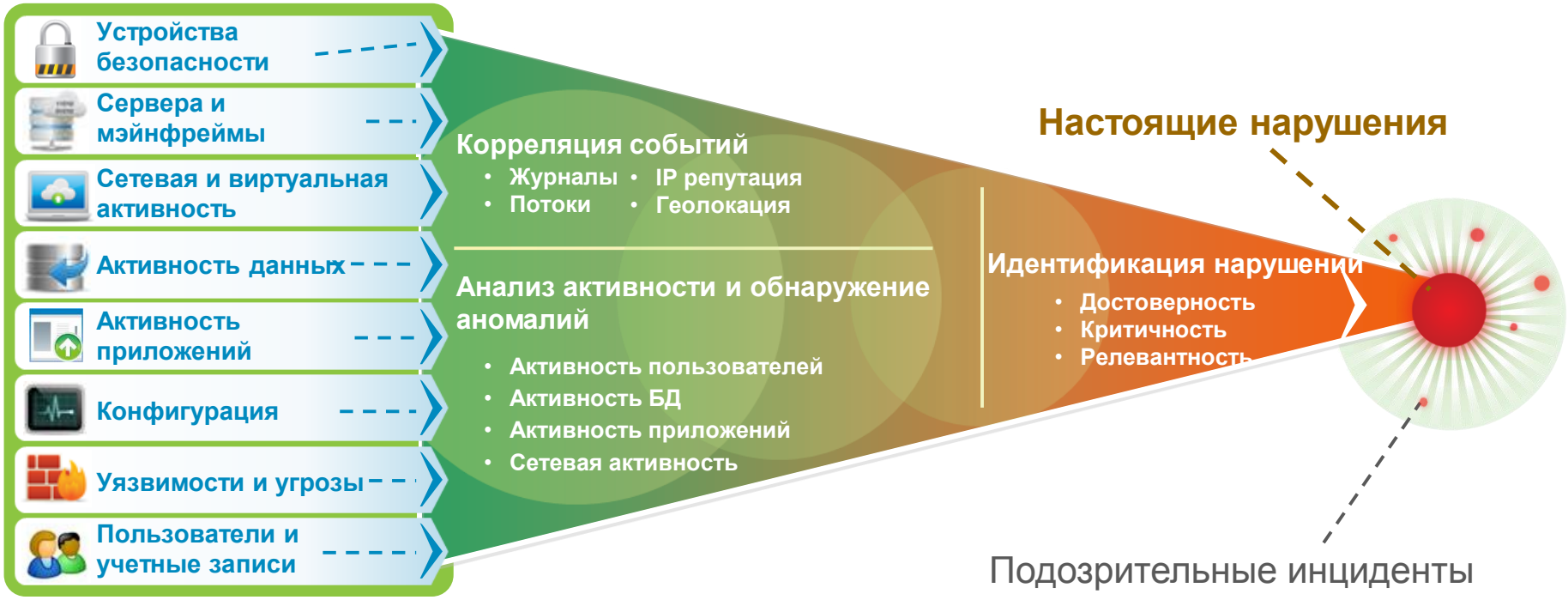
1. Сбор, нормализация и анализ в реальном времени данных, сгенерированных пользователями, приложениями, инфраструктурой и влияющих на информационную безопасность и риски предприятия

Security Intelligence предоставляет исчерпывающую и практически применимую информацию, необходимую для управления рисками и угрозами, от обнаружения и защиты до устранения

Эволюционируя вместе с изменяющимся ландшафтом



Контекст и корреляция позволяют понять суть происходящего



Обширный перечень источников + Глубокий интеллект = Исключительно точные и практически применимые выводы

Полностью интегрированная платформа Security Intelligence

Log Management	Radar Log Manager 	• Log management и отчеты, включив вилку в розетку • От СМБ до масштаба предприятия • Расширяется до SIEM
SIEM	Radar SIEM 	• Корреляция журналов, потоков, уязвимостей, identity • Передовое профилирование активов • Offense management и workflow
Управление конфигурацией и уязвимостями	Radar Risk Manager 	• Мониторинг конфигурации средств сетевой безопасности • Приоритезация уязвимостей • Прогнозирующее моделирование угроз и симуляция
Обнаружение аномалий сетевой активности	Radar SIEM  Radar QFlow 	• Анализ сетей • Обнаружение поведенческих аномалий • Полностью интегрирован с SIEM
Видимость сети и приложений	Radar QFlow  Radar VFlow 	• Мониторинг приложений на Уровне 7 • Захват контента для глубокого анализа и расследований • Физические и виртуальные среды
Масштабируемость		• Процессоры Событий • Процессоры Потоков • Отказоустойчивость и Катастрофоустойчивость • Горизонтальное масштабирование

Полностью интегрированная архитектура и интерфейс

Log Management

SIEM

Управление конфигурацией и уязвимостями

Обнаружение аномалий сетевой активности

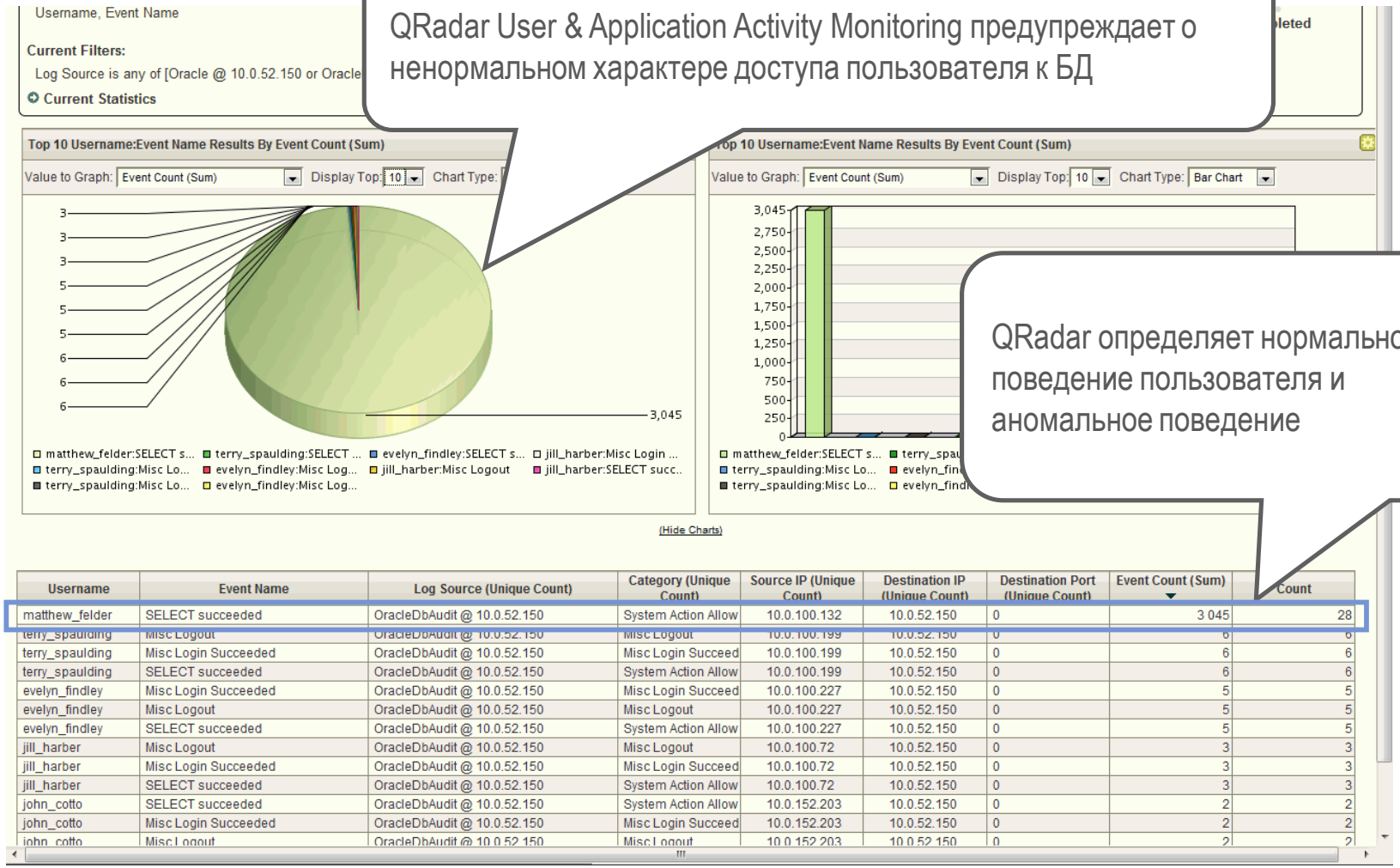
Видимость сети и приложений

Единая консоль безопасности

Построена на унифицированной архитектуре данных

Профилирование поведения пользователей и обнаружение отклонений от нормы

QRadar User & Application Activity Monitoring предупреждает о ненормальном характере доступа пользователя к БД



Username	Event Name	Log Source (Unique Count)	Category (Unique Count)	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Count (Sum)	Count
matthew_felder	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.100.132	10.0.52.150	0	3 045	28
terry_spaulding	Misc Logout	OracleDbAudit @ 10.0.52.150	Misc Logout	10.0.100.199	10.0.52.150	0	6	6
terry_spaulding	Misc Login Succeeded	OracleDbAudit @ 10.0.52.150	Misc Login Succeed	10.0.100.199	10.0.52.150	0	6	6
terry_spaulding	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.100.199	10.0.52.150	0	6	6
evelyn_findley	Misc Login Succeeded	OracleDbAudit @ 10.0.52.150	Misc Login Succeed	10.0.100.227	10.0.52.150	0	5	5
evelyn_findley	Misc Logout	OracleDbAudit @ 10.0.52.150	Misc Logout	10.0.100.227	10.0.52.150	0	5	5
evelyn_findley	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.100.227	10.0.52.150	0	5	5
jill_harber	Misc Logout	OracleDbAudit @ 10.0.52.150	Misc Logout	10.0.100.72	10.0.52.150	0	3	3
jill_harber	Misc Login Succeeded	OracleDbAudit @ 10.0.52.150	Misc Login Succeed	10.0.100.72	10.0.52.150	0	3	3
jill_harber	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.100.72	10.0.52.150	0	3	3
john_cotto	SELECT succeeded	OracleDbAudit @ 10.0.52.150	System Action Allow	10.0.152.203	10.0.52.150	0	2	2
john_cotto	Misc Login Succeeded	OracleDbAudit @ 10.0.52.150	Misc Login Succeed	10.0.152.203	10.0.52.150	0	2	2

QRadar определяет нормальное поведение пользователя и аномальное поведение

Корреляция доступа к данным с сетевой активностью

Потенциальная утечка данных?

Кто? Что? Куда?

Magnitude	
Description	Potential Data Loss/Theft Detected
Attacker/Src	10.103.14.139 (dhcp-workstation-103.14.139.acme.org)
Target(s)/Dest	Local (2) Remote (1)
Network(s)	Multiple (3)
Notes	Data Loss Prevention Use Case. Demonstrates QRadar DL authentication ...

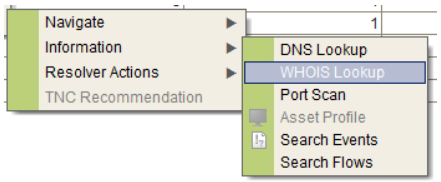
Attacker Summary Details

Magnitude		**User**	scott
Description	10.103.14.139	**Asset Name**	dhcp-workstation-103.14.139.acme.org
Vulnerabilities	0	**MAC**	Unknown
Location	NorthAmerica.all	**Asset Weight**	0

Кто?
Внутренний пользователь

	Event Name	Source IP (Unique Count)	Log Source (Unique Count)	Username (Unique Count)	Category (Unique Count)
	Authentication Failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	Multiple (2)	Misc Login Failed
	Misc Login Succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Login Succeeded
	DELETE failed	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Deny
	SELECT succeeded	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	System Action Allow
	Misc Logout	10.103.14.139	OracleDbAudit @ 10.101.145.198	scott	Misc Logout
	Suspicious Pattern Detec	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Suspicious Pattern Detected
	Remote Access Login Fa	10.103.14.139	Custom Rule Engine-8 :: qradar-vn	N/A	Remote Access Login Failed

Что?
Данные из БД Oracle



QRadar Has Completed Your Request

Go to APNIC results

[Querying whois.arin.net]
[whois.arin.net]

OrgName: Google Inc.
OrgID: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View

Куда?
Gmail

Анализ сетевых потоков **уровня приложения**, анализ содержимого пакетов

Offense 2849 Summary | Attackers | Targets | Categories | Annotations | Networks | Events | Flows | Rules | Actions | Print

Magnitude		Relevance	3
Description	Malware - External - Communication with BOT Control Channel containing Potential Botnet connection - QRadar Classify Flow	Event count	6 events in 1 categories
Attacker/Src	10.103.6.6 (dhcp-workstation-103.6.6.acme.org)	Start	2009-09-29 11:21:01
Target(s)/Dest	Remote (5)	Duration	0s
Network(s)	other	Assigned to	Not assigned
Notes	Botnet Scenario This offense captures Botnet command channel activity from an internal host. The botnet node communicates with IRC servers running on non-standard ports (port 80/http), which would typically bypass many detection techniques. This sc...		

View flows for this offense

First Packet Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Application	ICMP Type/Code	Source Flags	Destinat Flags	Source QoS	Destinat QoS	Flow Sourc
11:19	tcp_ip	10.103.6.6	48667	62.64.54.11	80	IRC	N/A	S,P,A	F,S,P,A	Best Effor	Class 1	qradar
11:19	tcp_ip	10.103.6.6	50296	192.106.224.13	80	IRC	N/A	S,P,A	S,A	Best Effor	Class 1	qradar
11:19	tcp_ip	10.103.6.6	51451	62.181.209.201	80	IRC	N/A	S,P,A	F,S,P,A	Best Effor	Class 1	qradar
11:19	tcp_ip	10.103.6.6	47961	62.211.73.232	80	IRC	N/A	F,S,P,A	F,S,P,A	Best Effor	Class 1	qradar

Source Payload
108 packets,
8850 bytes

UTF | Hex | Base64

```
NICK IamaZombie
USER IamaZombNICK IamaZombie
USER IamaZombNICK IamaZombie
USER IamaZombPROTOCTL NAMESX
PROTOCTL NAMESX
PROTOCTL NAMESX
NOTICE Defender :VERSION xchaNOTICE Defender :VERSION x
JOIN #botnet_command_channel
JOIN #botnet_command_channel
```

Destination Payload
70 packets,
5996 bytes

UTF | Hex | Base64

```
:Lexington.KY.US.AccessIRC.Net:Lexington.KY.US.AccessIRC.Net:1
```

Обнаружена ботсеть?

Максимум, что может сделать SIEM первого поколения

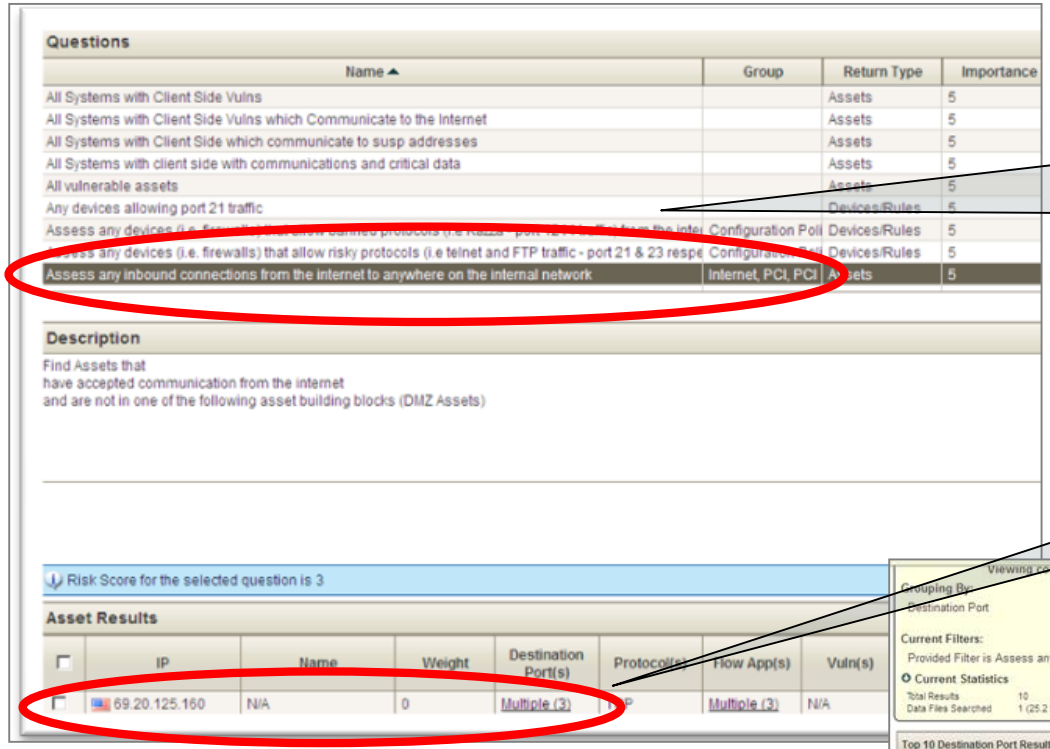
IRC на порту 80?

QFlow обнаруживает скрытый канал коммуникаций при помощи потоков Уровня 7 и анализа содержимого пакетов

Несомненно ботсеть

Данные потоков Уровня 7 содержат команды ботсети

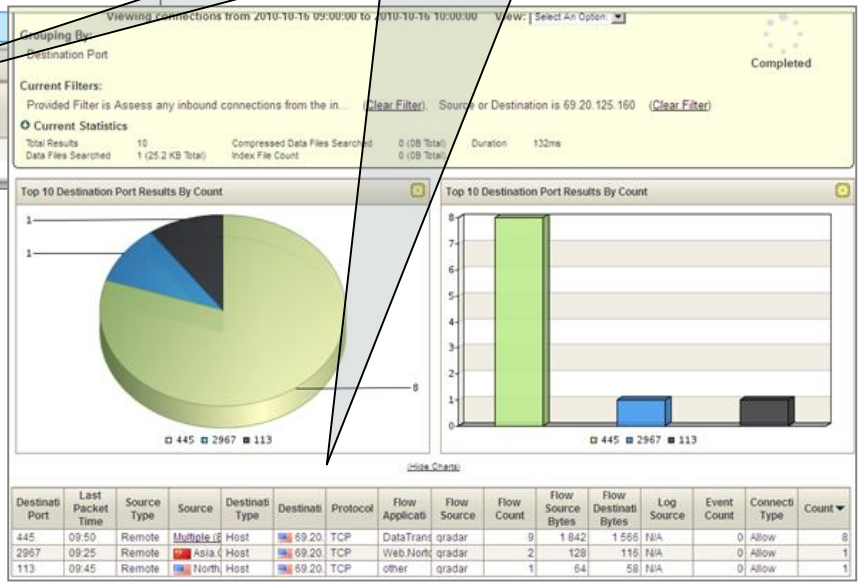
Анализ конфигураций сетевых устройств



Найти устройства с опасными настройками

Использовать знания о сетевом трафике и уязвимостях

Быстро оценить и проанализировать опасный трафик



Найти бреши, прежде чем это сделает нападающий

Постоянная видимость и мониторинг на все 360º

Точечное связывание информации в огромных массивах данных

Offense 3063 Summary | Attackers | Targets | Categories | Annotations | Networks | Events

Magnitude		Relevance	3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Proceeded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan	Event count	1428 events in 3 cate
Attacker/Src	202.153.48.66	Start	2009-09-29 16:05:01
Target(s)/Dest	Local (717)	Duration	1m 32s
Network(s)	Multiple (3)	Assigned to	Not assigned
Notes	Vulnerability Correlation Use Case Illustrates a scenario involving correlation of vulnerability data with I China (202.153.48.66) sweeps a subnet using the Conficker worm exploit (CVE 2008-4250). The first s		

Звучит неприятно…

Но как мы об этом узнали?

Доказательство — всего в одном клике мышью.

Сканирование сети

Обнаружено QFlow

Переполнение буфера

Попытка запуска эксплойта обнаружена Snort

	Event Name	Source IP	Destination IP	Destination Port	Log Source	Low Level Category
	Network Sweep - QRadar Classify Flow	202.153.48.66	Multiple (716)	445	Flow Classification E	Network Sweep
	NETBIOS-DG SMB v4 srvsvc NetrpPathConon	202.153.48.66	Multiple (8)	445	Snort @ 10.1.1.5	Buffer Overflow

Port	Service	OSVDB ID	Name	Description	Risk / Severity
445	unknown	49243	Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution	Microsoft Windows Server Service contains a flaw that may allow a malicious user to remotely execute arbitrary code. The issue is triggered when a crafted RPC request is handled. It is possible that the flaw may allow remote code execution resulting in a loss of integrity.	3

Целевой хост уязвим

Обнаружено Nessus

Total Security Intelligence

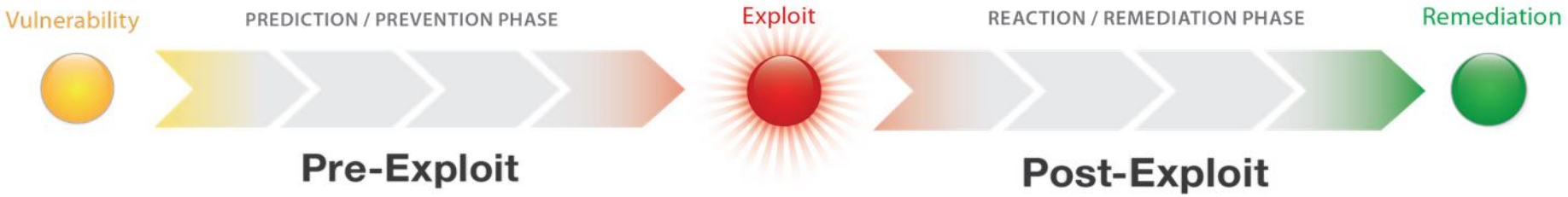
Конвергенция данных сети, событий и уязвимостей

Решая реальные задачи

Крупная электро-компания	ОБНАРУЖИВАЕТ УГРОЗЫ, КОТОРЫЕ ДРУГИЕ НЕ МОГУТ	Обнаружение 500 хостов с **вирусом “Here You Have”**, чего не смогли сделать антивирусные продукты
Крупная нефтяная компания	ИЗВЛЕКАЕТ ЦЕННУЮ ИНФОРМАЦИЮ ИЗ НАГРОМОЖДЕНИЯ ДАННЫХ	2 миллиарда событий в день сведены в **25 высоко-приоритетных нарушений**
Производитель модных товаров	ОБНАРУЖИВАЕТ ИНСАЙДЕРСКИЕ УГРОЗЫ	**Обнаружение инсайдера**, воровавшего и изменявшего конфиденциальные данные
Между-народный холдинг	ПРЕДСКАЗЫВАЕТ РИСКИ ДЛЯ БИЗНЕСА	Автоматизация процесса мониторинга конфигурационных **изменений в инфраструктуре**
Промышлен-ный дистри-бьютор	ВЫПОЛНЯЕТ ТРЕБОВАНИЯ РЕГУЛЯТОРОВ	Мониторинг сетевой активности **в реальном времени** (PCI)

Решения для полного цикла

Каковы внешние и внутренние угрозы? → **Защищает ли текущая конфигурация от этих угроз?** → **Что происходит прямо сейчас?** → **Каков результат?**



Прогнозирование и предотвращение

Risk Management. Vulnerability Management.
Configuration Monitoring. Patch Management.
X-Force Research and Threat Intelligence.
Compliance Management. Reporting and Scorecards.

Реакция и исправление

SIEM. Log Management. Incident Response.
Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Loss Prevention.

Уникальные преимущества QRadar

- Корреляция в реальном времени и обнаружение аномалий на основе широчайшего спектра данных, с учетом контекста
  - *Эффект: Более точное обнаружение угроз в реальном времени*

- Интегрированный анализ потоков, включая контент Уровня 7 (приложений)
  - *Эффект: Превосходная ситуационная информированность и идентификация угроз*

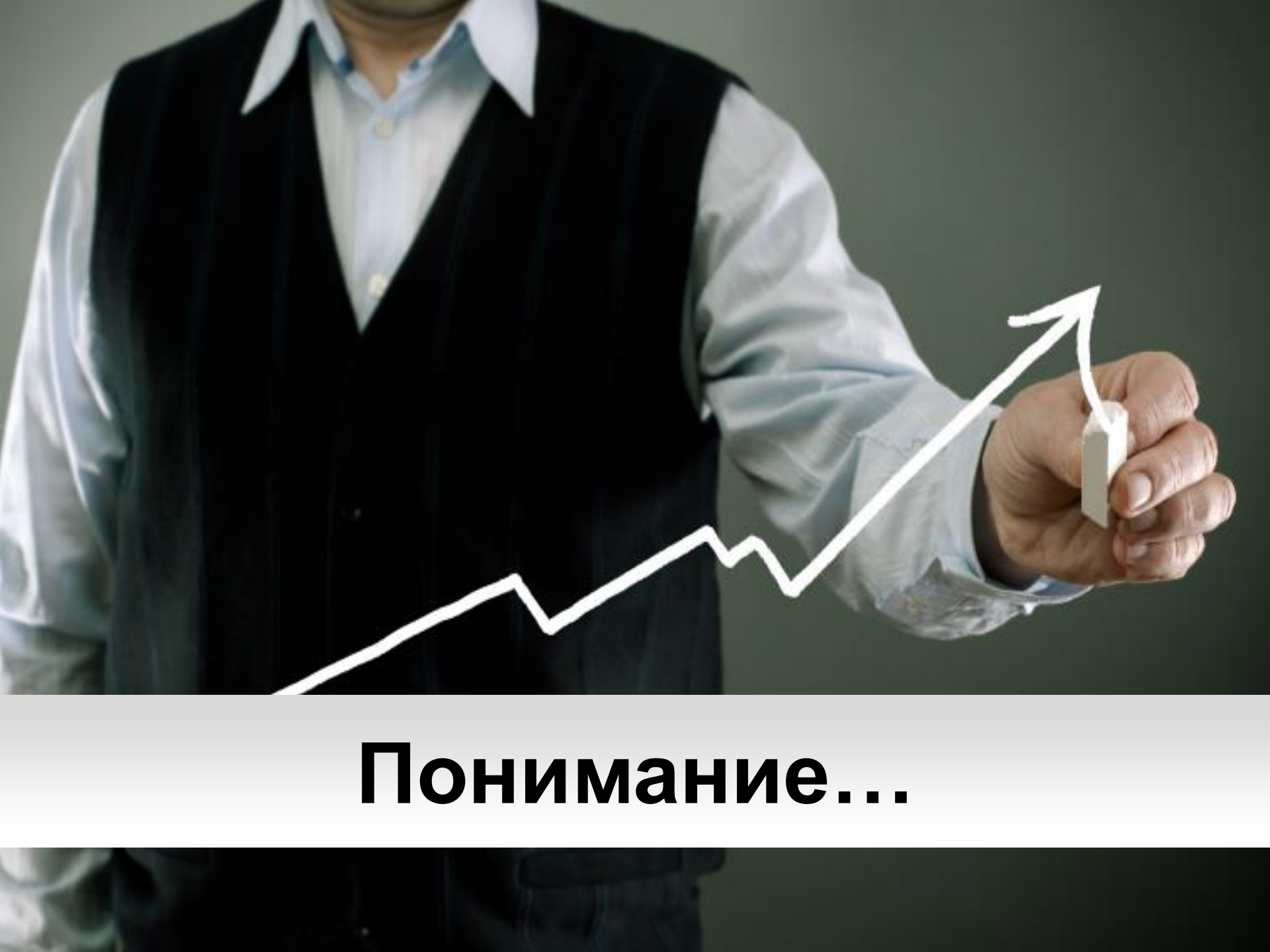
- Интеллектуальная автоматизация сбора данных, обнаружения активов, профилирования активов и т.д.
  - *Эффект: Сокращение ручного труда, быстрый time to value, низкая стоимость эксплуатации*

- Гибкость и простота использования, позволяющая относительно просто создавать и редактировать правила корреляции, отчеты, информационные панели
  - *Эффект: Максимальная эффективность, низкая стоимость владения*

- Масштабируемость для самых больших внедрений благодаря встроенной БД и унифицированной архитектуре данных
  - *Эффект: QRadar поддерживает потребности Вашего бизнеса любого масштаба*

Ваша команда ИБ видит...

Четкость…



Понимание…

Все

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 or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a 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 SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security