НТЦ ВУЛКАН

Система сбора, анализа и обработки событий безопасности на базе **IBM QRadar Security Intelligence Platform**

Решение НТЦ «Вулкан»

www.ntc-vulkan.ru

Предпосылки внедрения Системы сбора, анализа и обработки событий безопасности

Достижение Компанией определенного уровня зрелости в сфере управления ИТ и ИБ формирует объективную необходимость:

- Централизации сбора информации о событиях ИБ
- Централизации функций мониторинга состояния ИБ
- Наличия механизма для фиксации и управления инцидентами ИБ
- Наличия средств для уменьшения «окна возможностей» нарушителя ИБ
- Современного инструментария для анализа причин нарушений и источников рисков ИБ
- Совершенствования процессов управления системами и средствами защиты информации, контроля эффективности процессов ИБ

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (February 2020)

Для повышения эффективности процессов ИБ и обеспечения требуемого уровня оснащенности инструментами контроля ИБ в организации НТЦ «Вулкан» предлагает внедрение Системы сбора, анализа и обработки событий безопасности (SIEM) на базе IBM QRadar Security Intelligence Platform (IBM QRadar SIP)

Внедрение SIEM на базе IBM QRadar SIP позволяет повысить эффективность в сфере ИБ

SIEM на базе IBM QRadar SIP – инструмент поддержки решения ключевых задач ИБ организации:

создания единой точки сбора, хранения и анализа информации о событиях ИБ, генерируемых ИТ-инфраструктурой и СЗИ

получения «фактуры» для расследования инцидентов, когда требуется обеспечить глубокую ретроспективу лого» (годы, месяцы)

оперативного выявления аварийных ситуаций и инцидентов ИБ по данным корреляционного анализа событий

автоматизации процессов оценки соответствия требованиям (Compliance)

внедрения/совершенствования процессов управления ИТ на основе ITSM

создания центра оперативного управления ИБ (SOC)

Результаты внедрения

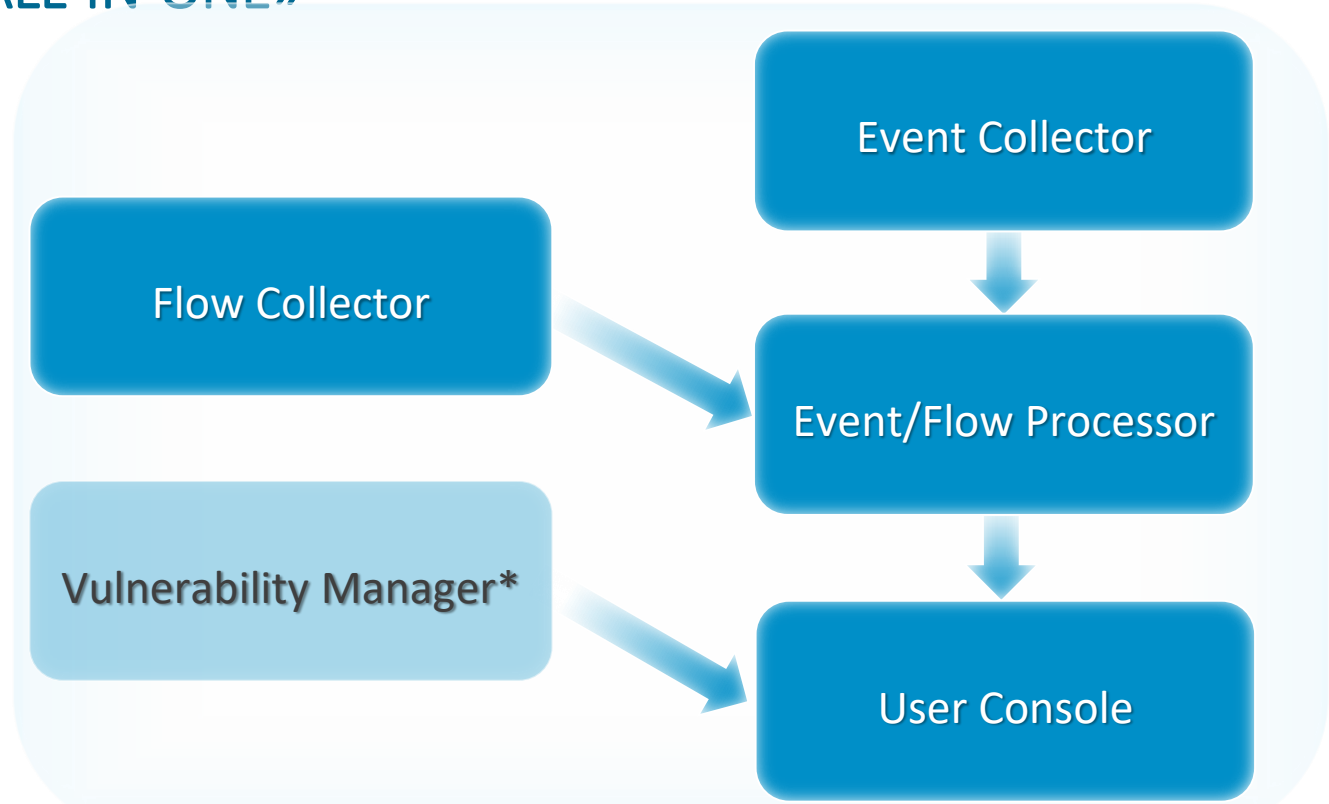
Внедрение SIEM-системы на платформе IBM QRadar SIP обеспечивает Заказчику возможности:

Возможности платформы IBM QRadar SIP

IBM QRadar Security Information and Event Management:	Сбор событий	Журналы событий; Flow (транспортный уровень модели OSI); QFlow/VFlow (уровень приложений модели OSI)
	Обработка и анализ событий	Нормализация; Корреляция; Выявление активов; Классификация; Визуализация и уведомления; Анализ и работа с данными от сканеров безопасности
	Хранение событий	Централизованное хранение; Исходный вид (RAW); Нормализованный вид
Data Store:		Лицензия неограниченного сбора и хранения событий без корреляции
Vulnerability Manager (в т.ч. Risk Manager):		Выявление уязвимостей на найденных активах
	Анализ сетевых устройств	Анализ конфигураций; Соответствие политикам; Построение топологии сети; Отслеживание путей атак
Network Insights:		Выявление угроз в потоке сетевого трафика (глубокий анализ)
Incident Forensics:		Детальное расследование, в т.ч. с реконструкцией сессий
Advisor with Watson:		Искусственный интеллект, повышающий эффективность и скорость расследования инцидентов
User Behavior Analytics:		Анализ поведения/действий пользователей по набору поведенческих правил и использованием машинного обучения (ML)

НТЦ ВУЛКАН

Архитектура – «ALL-IN-ONE»

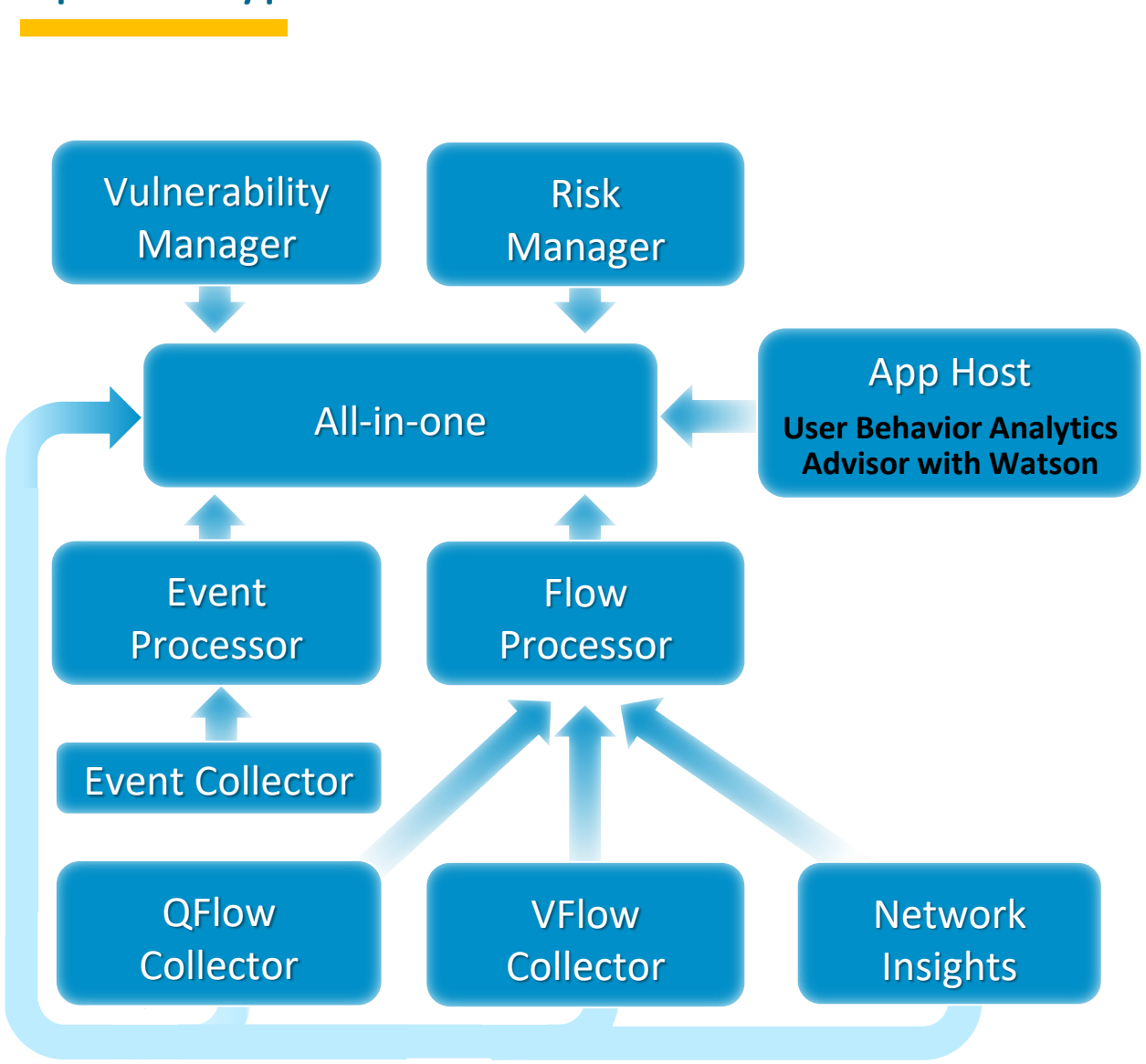


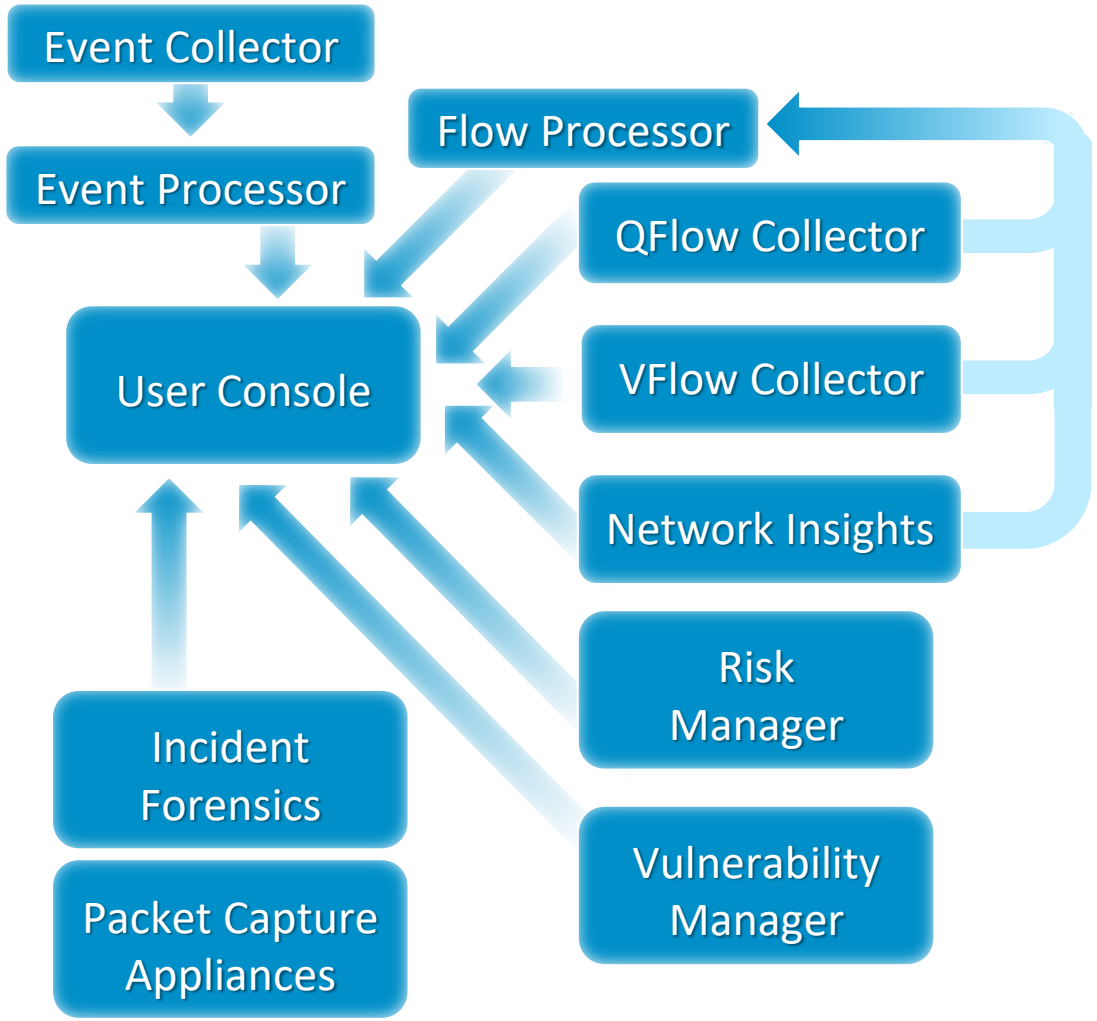
**Vulnerability Manager не входит в стандартные лицензии «All-in-one»*

Варианты исполнения:

- ПАК на базе Lenovo System x3xxx M5 или IBM xSeries M4;
- VM для виртуальных сред (от 24 Gb RAM и от 256 GB HDD):
  - VMWare ESXi (hardware версия 13);
  - KVM на базе CentOS/RHEL V7.5 с QEMU KVM 1.5.3-141;
  - Hyper-V на базе Windows Server 2016.

Архитектура – «DISTRIBUTED»





- Vulnerability Manager не требует отдельного ПАК/VM
- VFlow Processor только в виде VM

Принципы, реализованные в QRadar SIP

- Средства защиты информации
- Серверное оборудование
- Сетевая и виртуальная активность
- Базы данных
- Приложения
- Конфигурационная информация
- Уязвимости и угрозы
- Пользователи и учетные записи
- Глобальная база угроз

Интеллектуальная обработка

- Автоматический сбор данных
- Корреляция (логи/события, потоки данных сети, репутационные данные по IP, географическое положение)
- Расследование нарушений и профилирование
- Автоматизированная и интегрированная аналитика
- Уменьшение массивов данных
- Выявление аномалий и тенденций активности (пользователи, БД, приложения, сеть)

Выявление инцидентов

Реальное нарушение

Подозрительные инциденты

Обширный перечень источников + Развитая интеллектуальная обработка = **Практически применимые выводы**

Средства QRadar SIP позволяют реализовать полный цикл управления событиями ИБ

До атаки

Прогнозирование и предотвращение

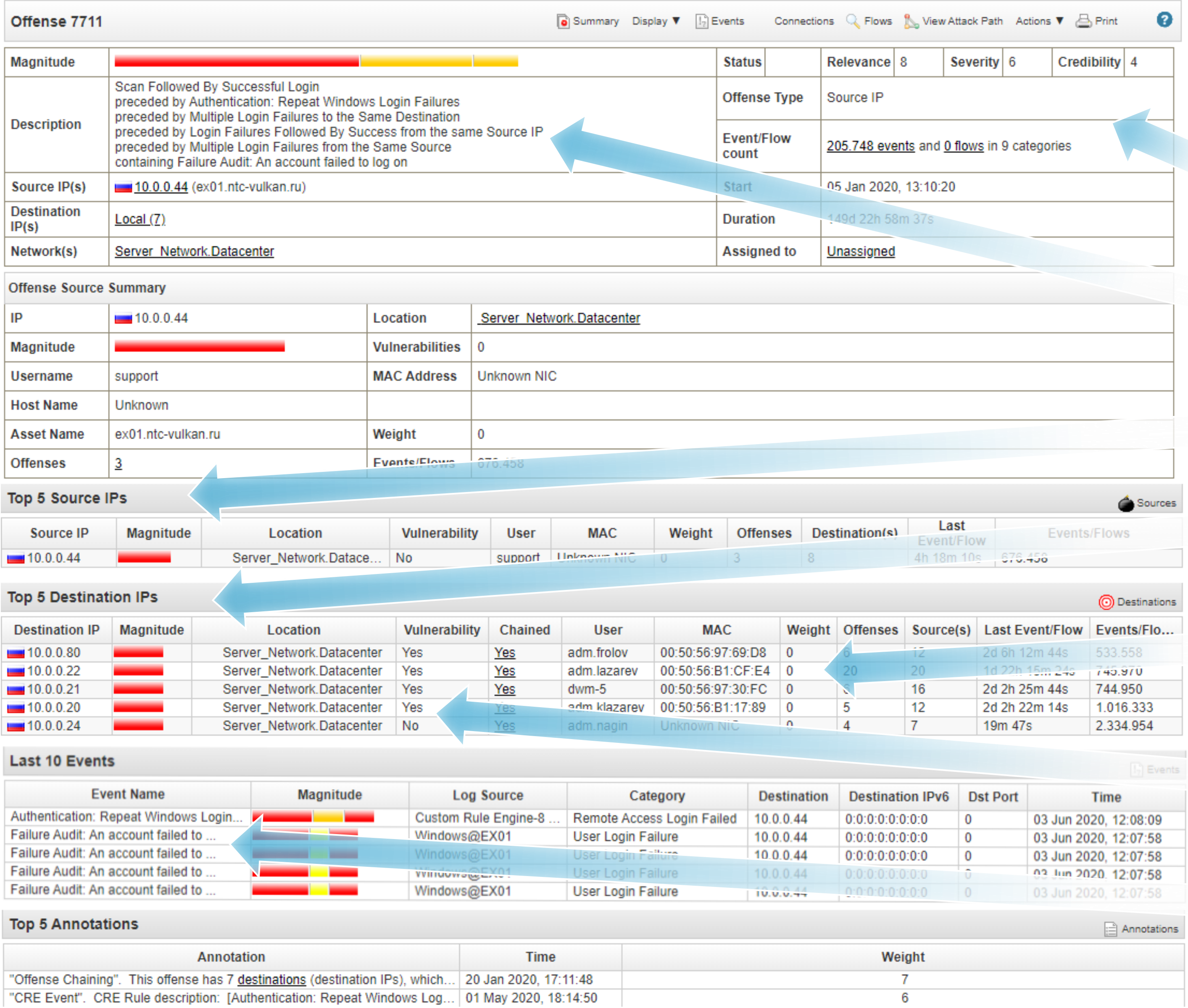
Risk Management
Vulnerability Management
Configuration Monitoring
Patch Management
X-Force Research and Threat Intelligence
Compliance Management
Reporting and Scorecards

После атаки

Реакция и исправление

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

Расследование инцидента с помощью инструментария QRadar SIP

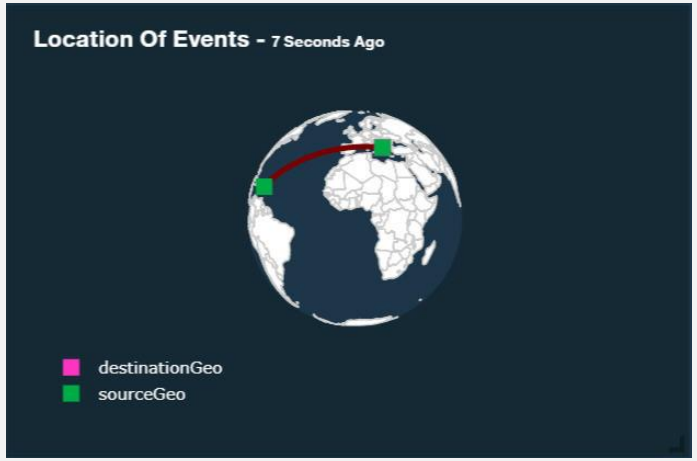


Ответы на вопросы

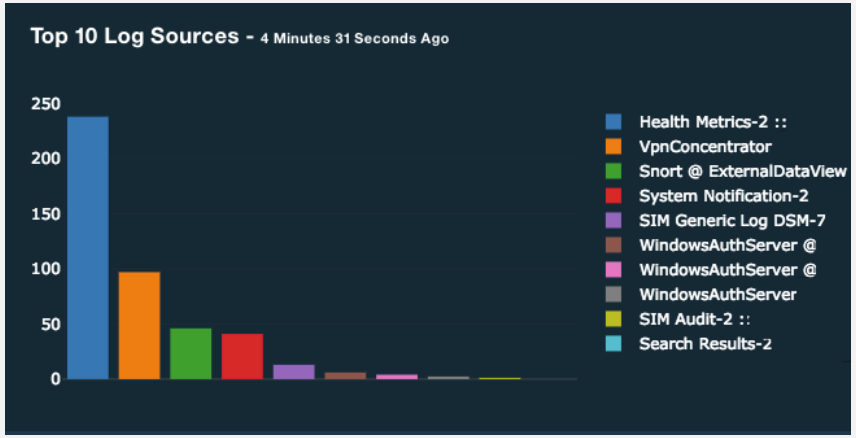
- Была ли атака успешной?
- Какого вида была атака?
- Источник атаки?
- Что затронула атака?
- Какая критичность актива?
- Были ли уязвимости?
- Где доказательства?

QRadar SIP позволяет реализовать кастомизацию пользовательских панелей

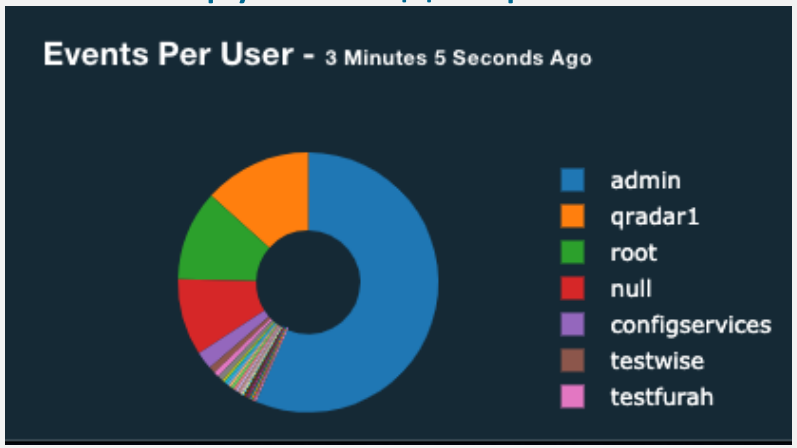
Географические диаграммы



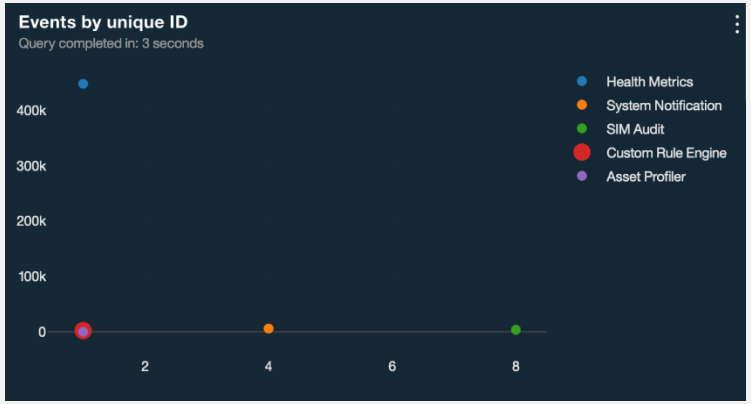
Гистограммы



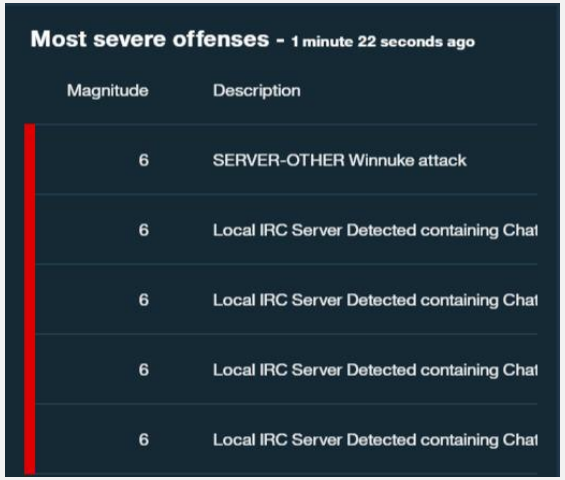
Круговые диаграммы



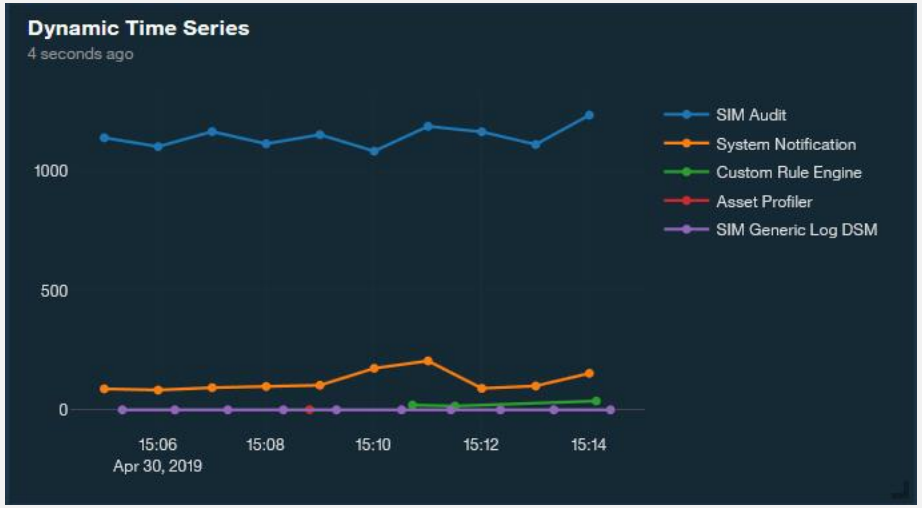
Точечные диаграммы



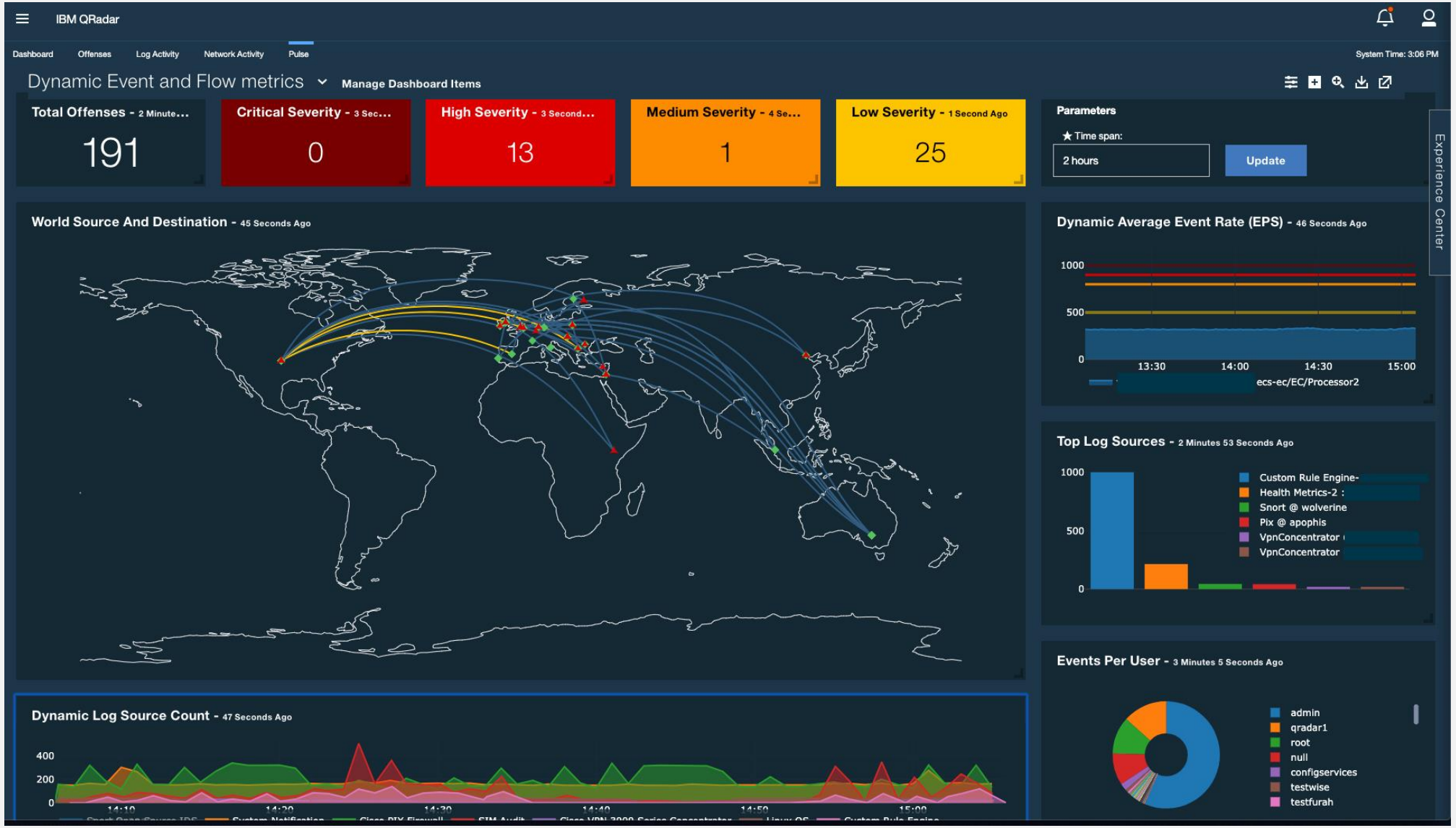
Таблицы



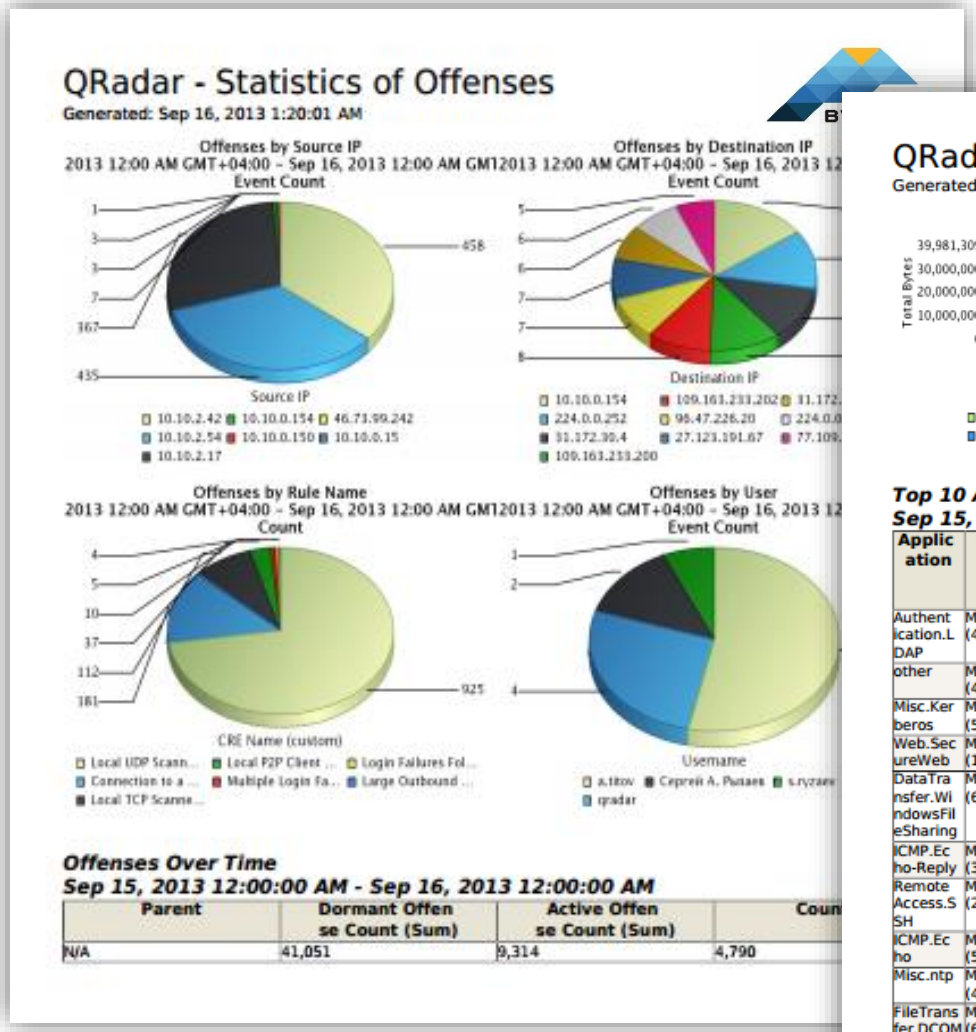
Временные графики

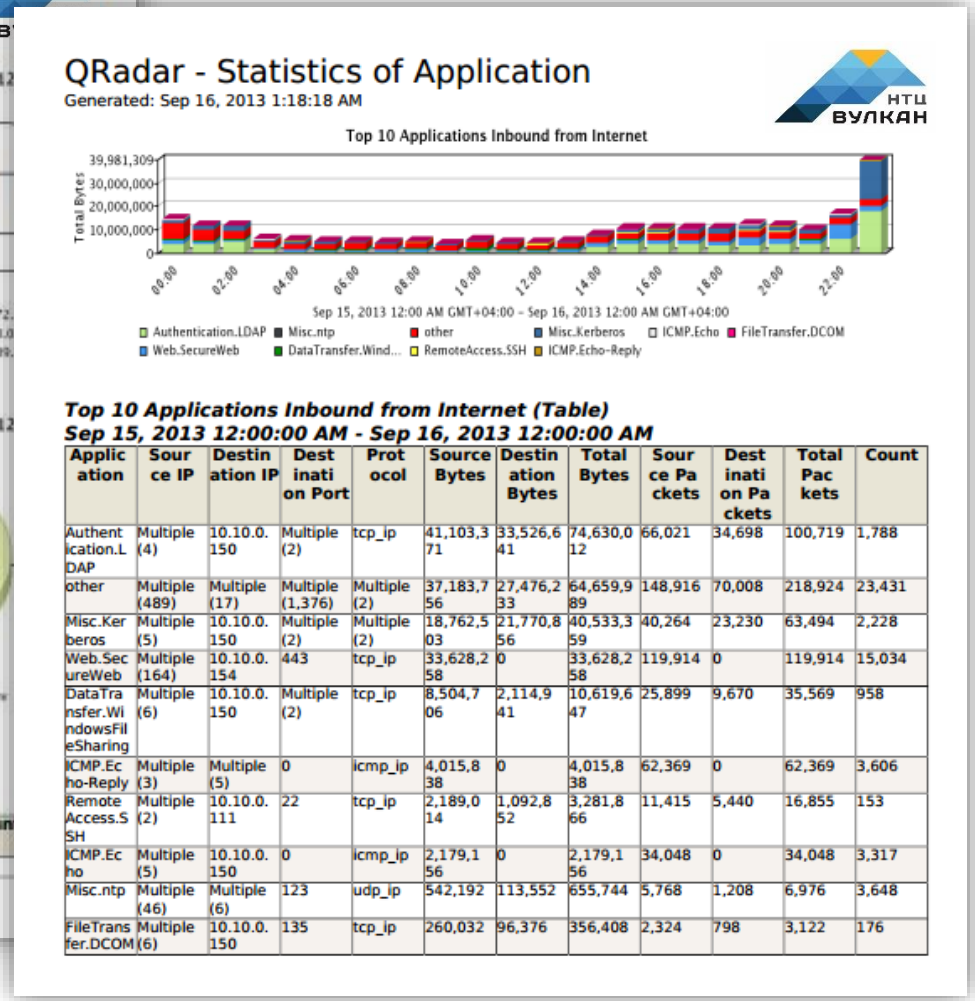


QRadar SIP: современный вид пользовательских панелей (Pulse App)



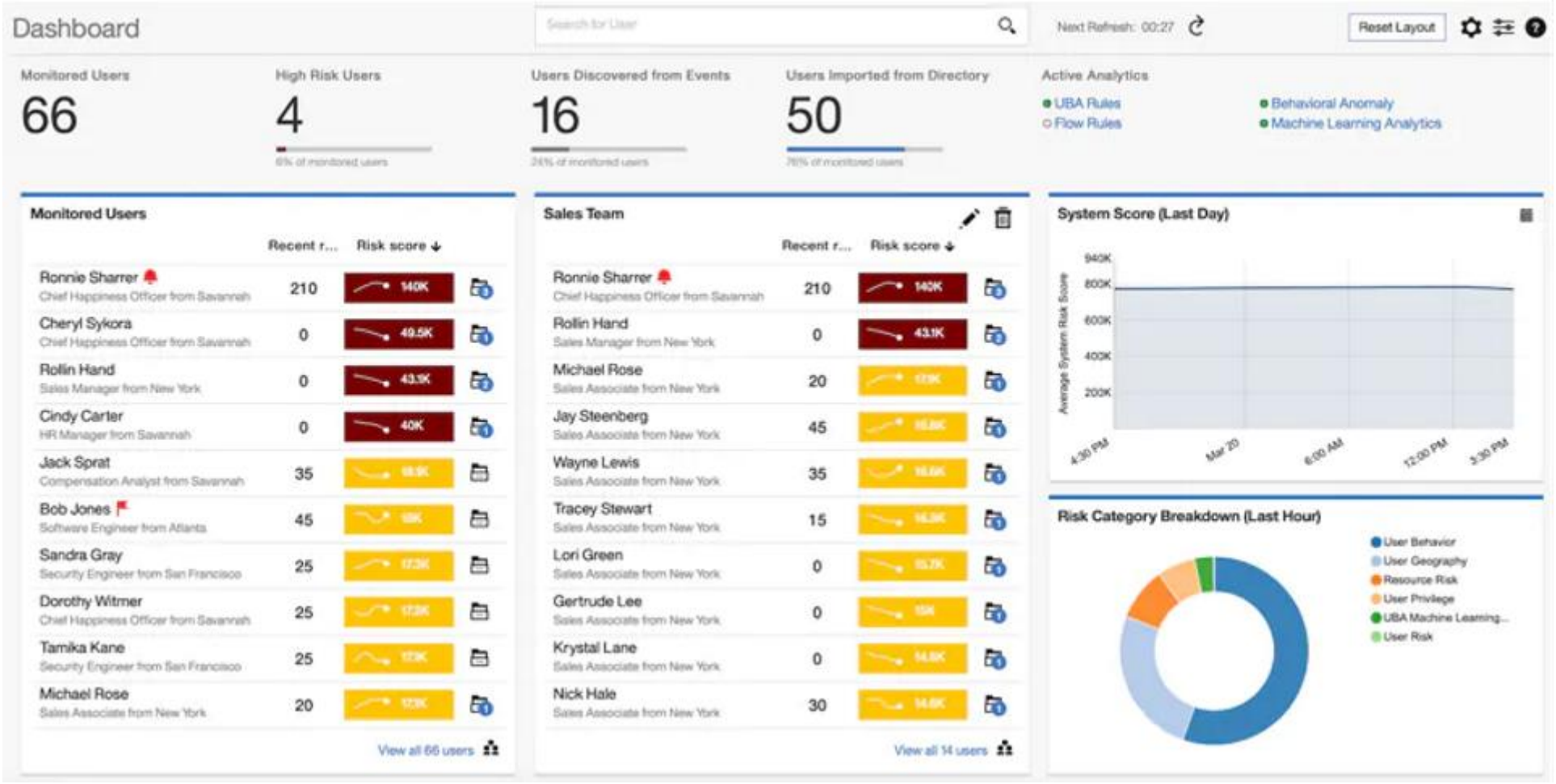
QRadar SIP обеспечивает возможность гибкой настройки шаблонов отчетности



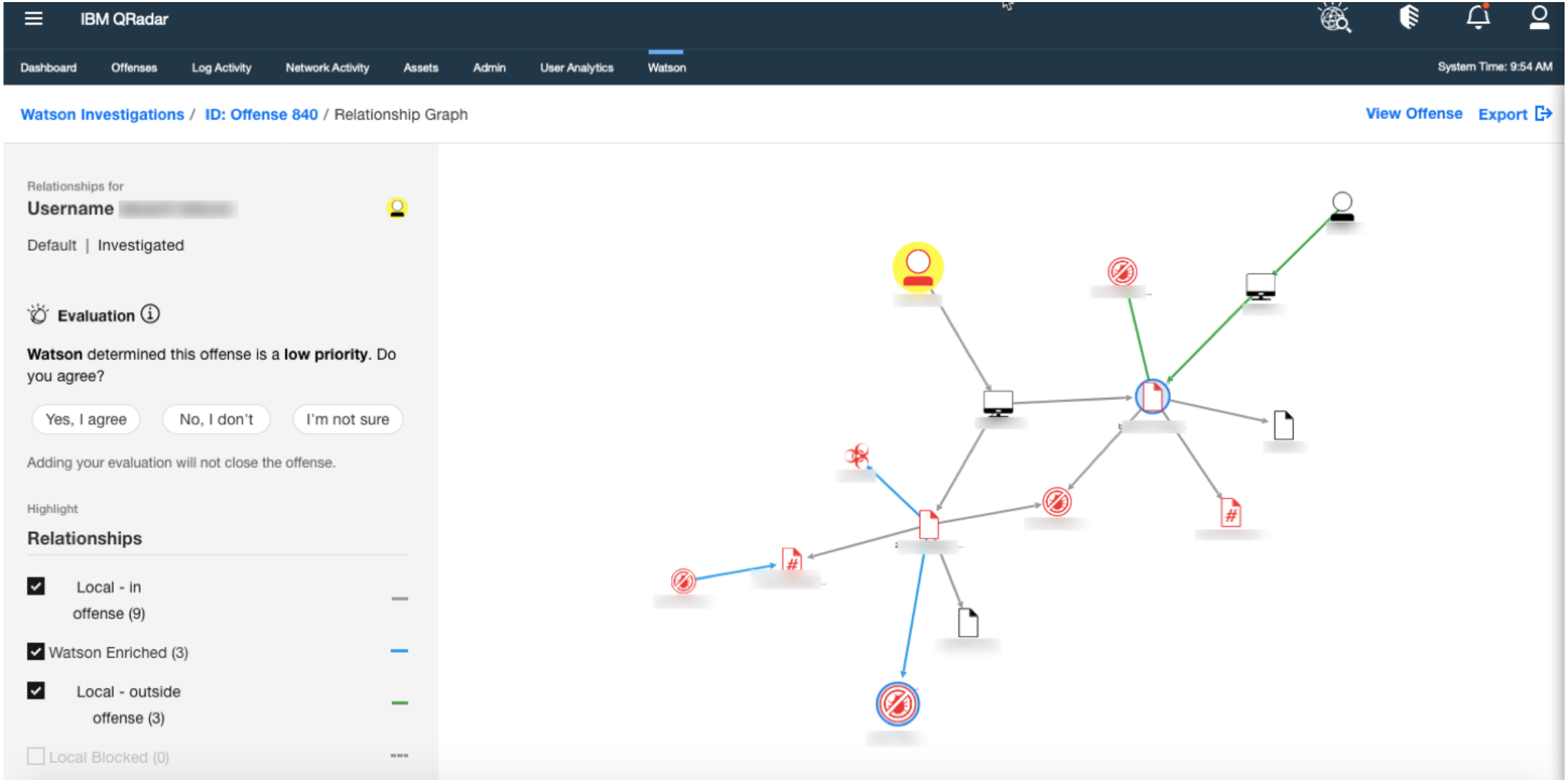


Application	Source IP	Destination IP	Destination Port	Protocol	Source Bytes	Destination Bytes	Total Bytes	Source Packets	Destination Packets	Total Packets	Count
Authentication.LDAP	Multiple (4)	10.10.0.150	Multiple (2)	tcp_ip	41,103,371	33,526,641	74,630,012	66,021	34,698	100,719	1,788
other	Multiple (489)	Multiple (17)	Multiple (1,376)	Multiple (2)	37,183,756	27,476,233	64,659,989	148,916	70,008	218,924	23,431
Misc.Kerberos	Multiple (5)	10.10.0.150	Multiple (2)	Multiple (2)	18,762,503	21,770,856	40,533,359	40,264	23,230	63,494	2,228
Web.SecureWeb	Multiple (164)	10.10.0.154	443	tcp_ip	33,628,258	0	33,628,258	119,914	0	119,914	15,034
DataTransfer.WindowsFileSharing	Multiple (6)	10.10.0.150	Multiple (2)	tcp_ip	8,504,706	2,114,941	10,619,647	25,899	9,670	35,569	958
ICMP.Echo-Reply	Multiple (3)	Multiple (5)	0	icmp_ip	4,015,838	0	4,015,838	62,369	0	62,369	3,606
RemoteAccess.SSH	Multiple (2)	10.10.0.111	22	tcp_ip	2,189,014	1,092,852	3,281,866	11,415	5,440	16,855	153
ICMP.Echo	Multiple (5)	10.10.0.150	0	icmp_ip	2,179,156	0	2,179,156	34,048	0	34,048	3,317
Misc.ntp	Multiple (46)	Multiple (6)	123	udp_ip	542,192	113,552	655,744	5,768	1,208	6,976	3,648
FileTransfer.DCOM	Multiple (6)	10.10.0.150	135	tcp_ip	260,032	96,376	356,408	2,324	798	3,122	176

QRadar SIP: User Behavior Analytics App



QRadar SIP: Advisor With Watson App



Преимущества QRadar SIP как платформы создания и внедрения SIEM-решения

Адекватное развертывание и поддержка	Solution, а не Framework
	Обновление автоматически или вручную
	Агентный и безагентный сбор событий с ОС Windows
	Использование одного агента для ряда ПО/АРМ Windows
	Работа с «неподдерживаемыми» источниками событий
Глубокий анализ событий и сетевого трафика	Категорирование всех событий (High/Low Level Category)
	Корреляционные правила «из коробки» (Best Practices)
	Корреляция событий и/или сетевого трафика
	Технология DPI - Deep Packet Inspection (QFlow/VFlow/Network Insights)
	Расширенный парсинг событий с помощью регулярных выражений
Дополнительные сервисы	Наличие встроенного сервиса управления инцидентами
	Выявление и управление уязвимостями на активах (Vulnerability Manager)
	Работа с конфигурациями сетевого оборудования (Risk Manager)
	Реконструкция сетевых сессий (Incident Forensics)
	Расширение функциональности за счет установки приложений (UBA, Watson и т.д.)

Состав работ НТЦ «Вулкан» при внедрении SIEM на базе IBM QRadar SIP

1. Анализ и проектирование

Анализ ИТ-инфраструктуры и систем ИБ заказчика, выявление потребностей в их контроле

Идентификация источников событий Системы (средства защиты информации, серверы и рабочие станции, ОС, СУБД, приложения, сетевое и периферийное оборудование и т.п.)

Селекция событий для обработки, определение технологии доступа

Оценка потока событий

Документирование требований к Системе, разработка ТЗ

Разработка процедур управления событиями

2.

Развертывание п**Ввод в действие**рограммного обеспечения

Подключение к Системе источников событий, в том числе, штатно не поддерживаемых платформой

Настройка правил корреляции

Разработка и кастомизация информационных панелей и шаблонов отчетов

Консультирование по вводу в действие процедур управления событиями

Тестирование Системы и передача в эксплуатацию

3. Поддержка

Инженерно-техническая поддержка и сопровождение

Экспертно-аналитическая поддержка

Дополнительные возможности решения НТЦ «Вулкан»

- Отчеты по ИБ в соответствии с корпоративным стилем Заказчика
- Dashboards с функцией drilldown
- Русифицированные отчеты и dashboards
- Приоритизация данных
- Автоматическая рассылка отчетов по e-mail
- 50+ предустановленных наборов отчетов

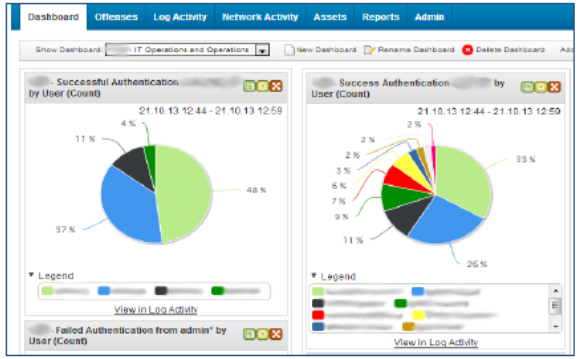
Пример выполненного проекта создания и внедрения SIEM на базе IBM QRadar SIP

НТЦ ВУЛКАН
105318 г. Москва, ул. Ибрагимова, д.31
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

Сбор, хранение и обработка событий информационной безопасности с помощью IBM Security QRadar SIEM

Заказчик: российский банк (ТОП-100), входящий в крупный международный финансовый холдинг.

Назначение проекта: автоматизация процессов централизованного сбора, накопления и аналитической обработки событий от компонентов ИТ-инфраструктуры.



Цели выполнения проекта:

- создание единого центра сбора событий
- обеспечение ретроспективного анализа состояния ИТ-инфраструктуры
- сокращение времени реакции на инциденты
- оптимизация процессов предупреждения и расследования инцидентов ИБ и выявления проблем (в терминологии ITSM)
- обеспечение информационно-аналитической поддержки деятельности по управлению ИБ
- оптимизация функционирования ИТ-инфраструктуры по результатам анализа событий

Scope проекта: компоненты ИТ-инфраструктуры, включенные процесс управления событиями

- активное сетевое оборудование (коммутаторы, маршрутизаторы) – 18 единиц
- межсетевые экраны Cisco Systems, Inc., Microsoft ISA Server – 6 единиц
- системы предотвращение вторжений Palo-Alto IPS – 2 комплекса
- системы удаленного доступа – Citrix Access Gateway – 2 комплекса
- серверы с ОС Microsoft Windows – 130 единиц
- СУБД Microsoft SQL Server – 6 инсталляций
- серверы приложений IBM WebSphere Application Server – 10 единиц
- система виртуализации VMware vSphere
- система антивирусной защиты и управления DLP-агентами McAfee ePolicy Orchestrator
- неподдерживаемые «из коробки» бизнес-системы различных производителей, в том числе российских – 6 типов

IBM

НТЦ ВУЛКАН
105318 г. Москва, ул. Ибрагимова, д.31
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

Неподдерживаемые «из коробки» компоненты ИТ-инфраструктуры:

- связующее программное обеспечение (middleware) xmlBlaster
- связующее программное обеспечение (middleware) Informatica
- программный комплекс Credit Registry
- решение для автоматизации банковской деятельности Диасофт 5NT
- решение фронт-офиса от компании Диасофт
- система дистанционного банковского обслуживания BSS

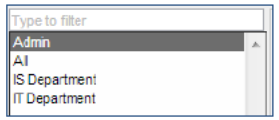
Способы и методы сбора событий:

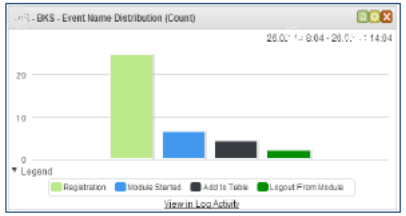
- WinCollect и ALE агенты
- протокол Syslog
- протокол JDBC
- Log File (протокол FTP)

LogFileProtocol	Servers, WebSphere	IBM WebSphere Application Server
Syslog	Network	Cisco Adaptive Security Appliance (ASA)
WinCollect	Servers	Microsoft Windows Security Event Log
Syslog	Servers	Citrix NetScaler
EMCVmWareProtocol	Servers	EMC VMWare
Syslog	Network	Palo Alto PA Series
Syslog	Servers, xmlBlaster	Universal DSM
Syslog	Servers	Symantec Endpoint Protection
JDBC	Servers	McAfee ePolicy Orchestrator
Syslog	BSS, Servers	Universal DSM

В рамках проекта проведены следующие работы:

- подключение и тюнинг компонентов ИТ-инфраструктуры
- парсинг и классификация событий от неподдерживаемых компонентов
- интеграция системы с Active Directory и реализация прав разграничения доступа
- формирование выборок событий на основе требований заказчика
- формирование персонифицированных информационных рабочих панелей (Dashboard)
- настройка уведомлений операторов (на информационную панель, по электронной почте)
- настройка управленческой и технической отчетности по расписанию
- подготовка проектной и эксплуатационной документации[1].





В результате внедрения системы заказчик получил:

- сокращение времени реакции на события в ИТ-инфраструктуре
- способность идентифицировать и разрешать часть инцидентов до начала их влияния на работу пользователей
- управление полным жизненным циклом событий ИБ в ИТ-инфраструктуре
- формирование ретроспективных выборок (отчетов) по компонентам ИТ-инфраструктуры
- отслеживание деятельности привилегированных категорий пользователей

[1] *Разработка документации на систему выполнена в соответствии с требованиями ГОСТ «Информационная технология. Комплекс стандартов на автоматизированные системы» и комплекса СТО БР ИББС*

IBM

Возможный подход к внедрению SIEM на базе IBM QRadar SIP

Большинство заказчиков принимают решение о внедрении по результатам пилотного проекта:

- Готовность заказчика (в т.ч. наличие человеческого ресурса)
- Совместное формулирование целей и задач, планирование работы
- Выделение перечня источников событий
- Подготовка ИТ-инфраструктуры (источники, МЭ, учетные записи, SPAN-порты)

Типичная длительность «пилота» - 1 месяц

Результат «пилота» - обоснованное решение о внедрении (и его масштабах)

Результаты внедрения SIEM на базе IBM QRadar SIP для Заказчика

Основные бизнес-результаты внедрения Системы сбора, анализа и обработки событий безопасности (SIEM) на базе IBM QRadar SIP для Заказчика:

- Оптимизация операционных затрат на ИБ
- Существенное повышение эффективности процессов ИБ
- Минимизация рисков ИБ и связанных рисков, включая риски критически важных корпоративных ресурсов организаций в условиях роста количества и разнообразия угроз для ИТ-инфраструктуры
- Обеспечение соответствия требованиям законодательства и нормативных актов в сфере ИБ

НТЦ «Вулкан» - независимый эксперт и интегратор технологий информационной безопасности

На рынке с **2010** года

Комплексные решения в сфере экономической и информационный безопасности

500+ реализованных проектов в ИБ

20+ проектов внедрения SIEM

150+ сотрудников в штате

Сертифицированная система менеджмента качества

Входит в **30** крупнейших компаний РФ в сфере защиты информации

По версии CNews Analytics, 2019

Допуски и лицензии ФСТЭК, ФСБ, Минобороны, Минпромторг

Партнер IBM
по группе продуктов Security
с 2010 года

IBM Gold Business Partner

Развитие партнерских отношений с международными и российскими вендорами и производителями в сфере ИБ

IBM, RSA, INFOWATCH, Эшелон, s•terra, SKYBOX SECURITY, KASPERSKY, Dr.WEB, Check Point, paloalto, CISCO, DELL EMC, FireEye

НТЦ ВУЛКАН

Система сбора, анализа и обработки событий безопасности на базе IBM QRadar Security Intelligence Platform

СПАСИБО ЗА ВНИМАНИЕ!

НТЦ ВУЛКАН

www.ntc-vulkan.ru

marketing@ntc-vulkan.ru