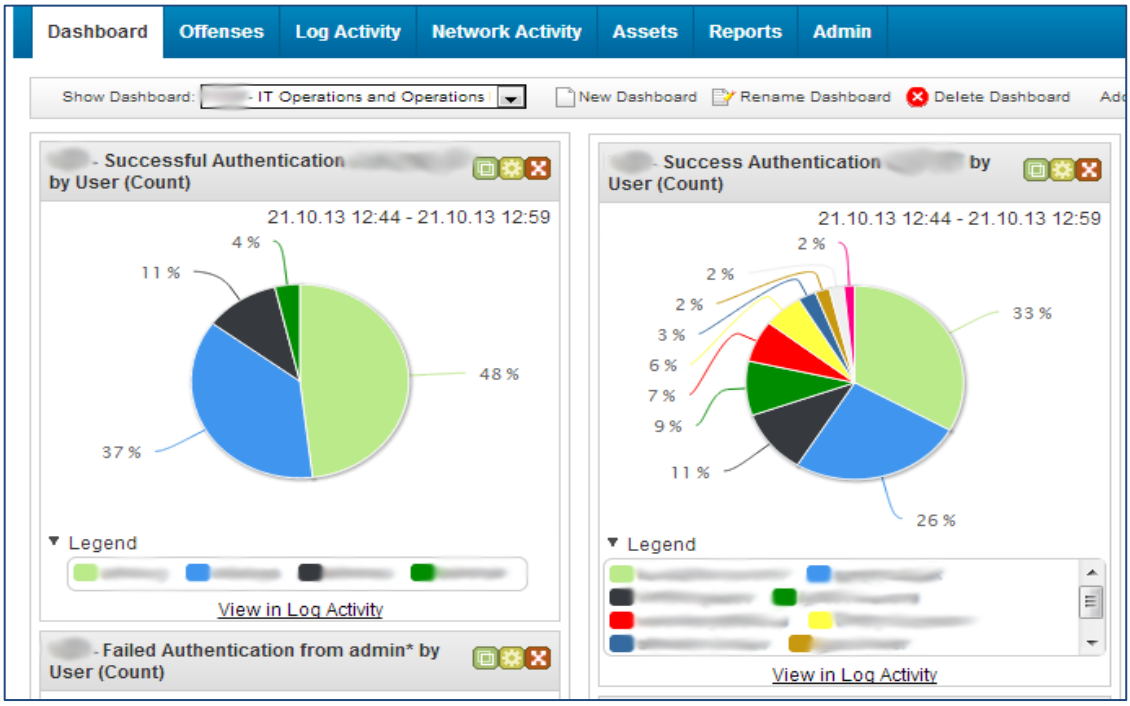
105318 г. Москва, ул. Ибрагимова, д.31
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

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

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

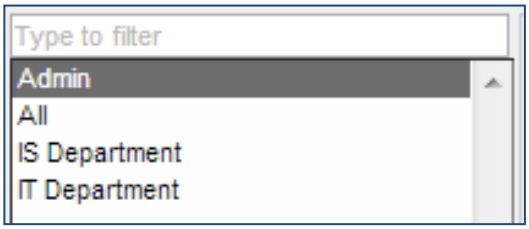
Способы и методы сбора событий:

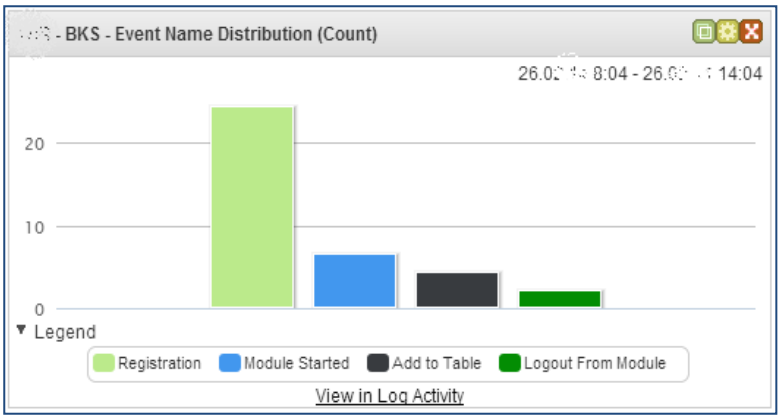
- WinCollect и ALE агенты
- протокол Syslog
- протокол JDBC
- Log File (протокол FTP)

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*