Система безопасности

О компании Tenable

- Основана в 2002 году
- Создана система мониторинга масштаба крупных предприятий
- Создан сетевой сканер уязвимостей Nessus scanner
- Частная компания без государственных инвестиций
- Входит в число крупных компаний которые обеспечивают поставку решений по ИБ для Nasa, Министерства обороны США, ряда Европейских Банков, федеральных органов власти Европы
- Компания успешно развивает свой бизнес

Состав команды разработчиков и топ-менеджмента

Ron Gula, CEO/CTO

- Совладелец компании
- Автор системы обнаружения атак Dragon IDS

Jack Huffard, President/COO

- Совладелец компании

Renaud Deraison, CRO

- Совладелец компании
- Автор сетевого сканера Nessus

Marcus J. Ranum, CSO

- Совладелец компании
- Разработчик решений для МЭ, VPN и систем обнаружения атак

TENABLE Network Security®

Решения уровня масштаба предприятий

Сканер уязвимостей (Nessus Vulnerability Scanner)

- Конфигурация по профилям
- Более 40,000 проверок систем

Система сканирования трафика (PVS)

- Незаметный контроль трафика
- Мониторинг 24x7
- Вытаскивает данные на «лету»

Система сбора и корреляции логов (LCE)

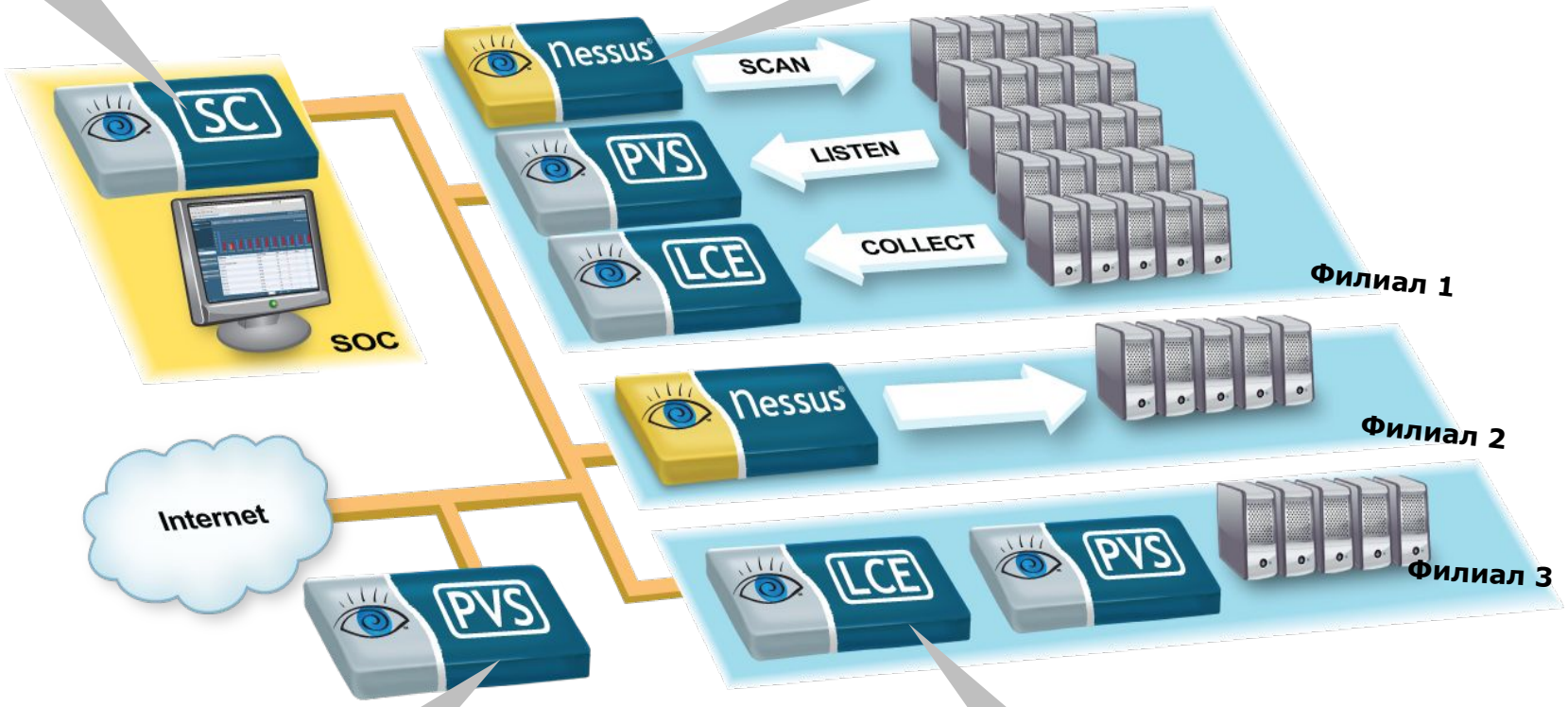
- Корреляция и сбор логов
- Автоматическая архивация логов
- Настраиваемые отчеты
- Корреляция событий от IDS

TENABLE Network Security®

Взаимодействие данных в Системе

Центр безопасности на базе Security Center.

Сканеры Nessus в объектах предприятия (сканирование)

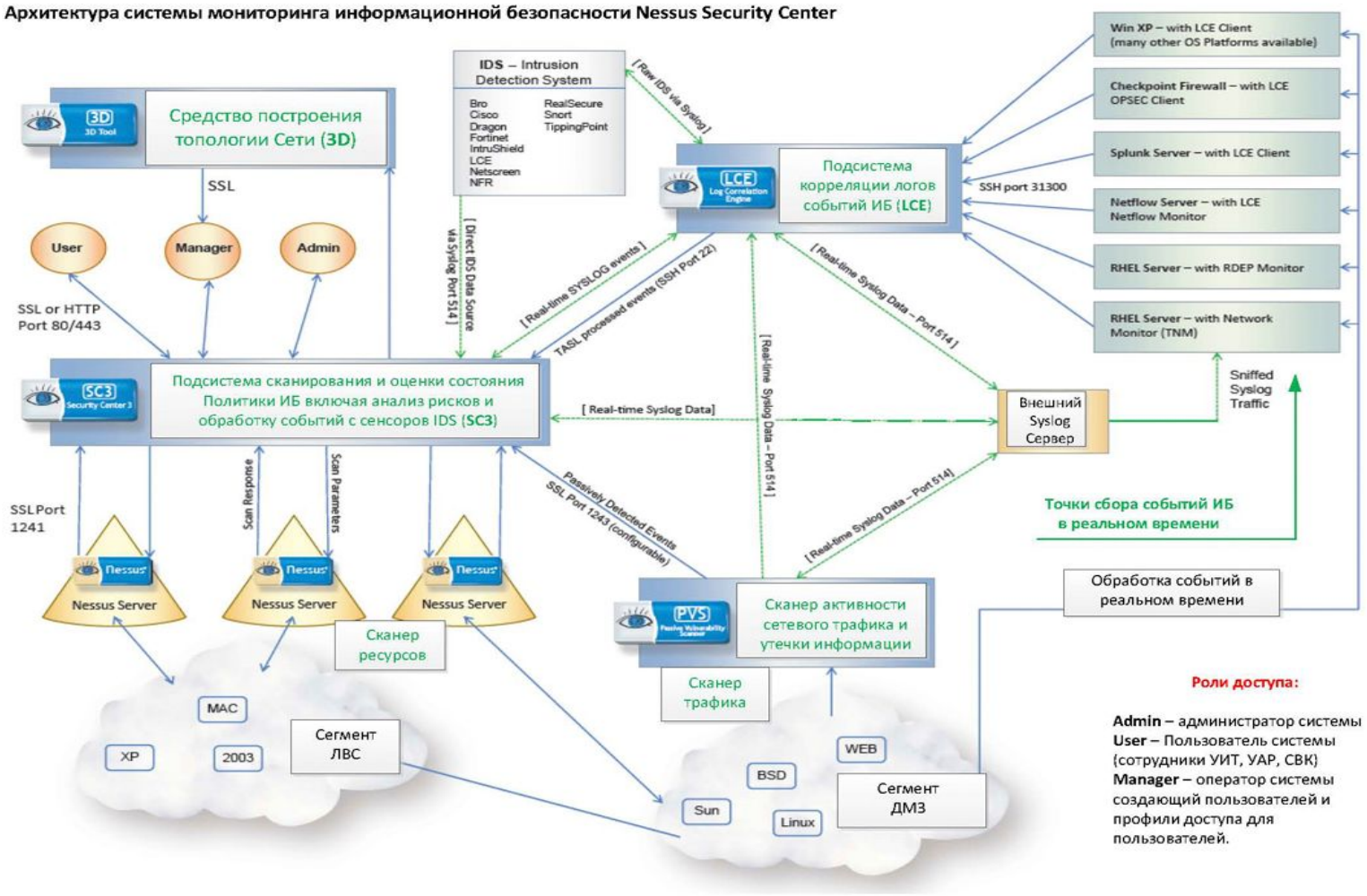


Пассивный сканер (PVS) – обнаружение аномалий в трафике

Система корреляции логов событий и их агрегации (LCE)

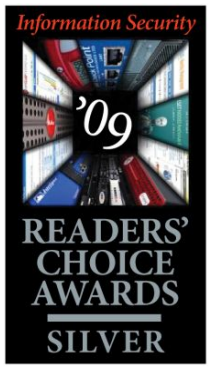
TENABLE Network Security®

Архитектура системы



TENABLE Network Security®

Признаный в мире продукт в области ИБ

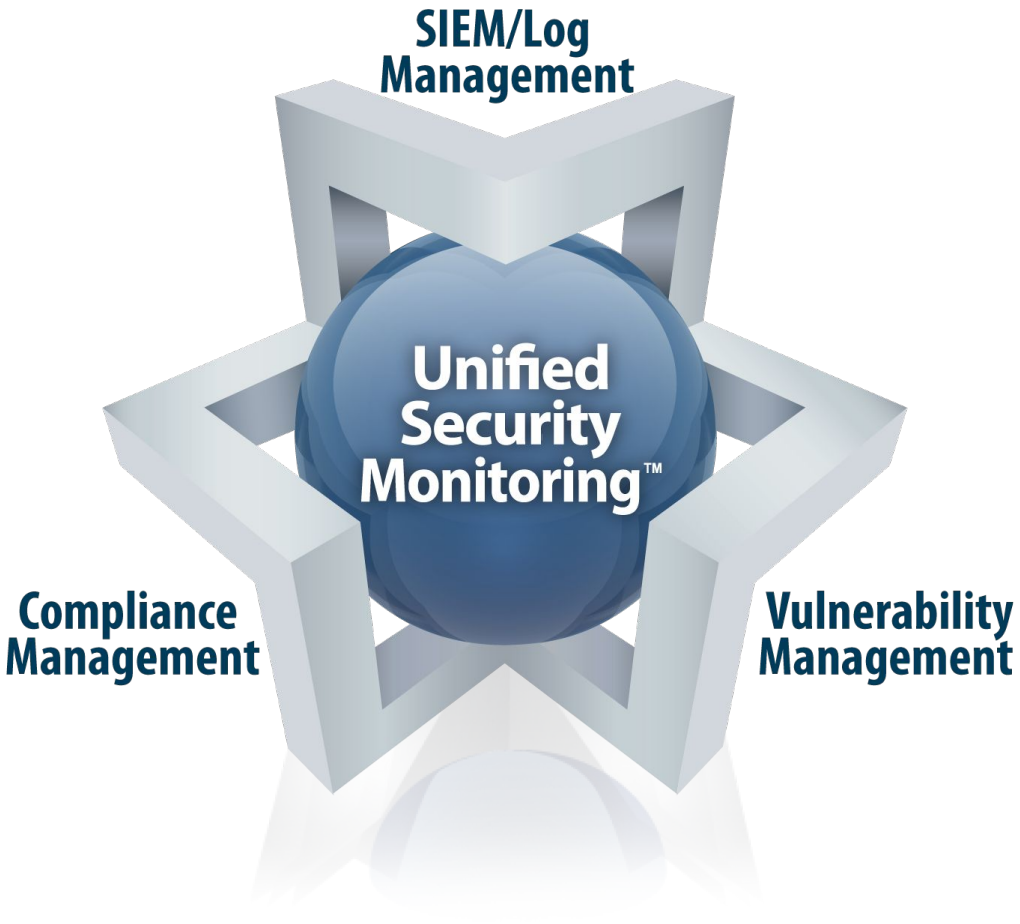


TENABLE Network Security®

Концепция единой системы безопасности

Компания Tenable впервые предложила концепцию системы безопасности состоящей из трех составляющих

- **Мониторинг уязвимости в режиме реального времени** используется комбинация данных полученных в результате активного и пассивного сканирования
- **Критические событиям** использован механизм корреляции логов и событий
- **Мониторинг соответствия стандартам** использован механизм аудита конфигураций и профилей настроек систем

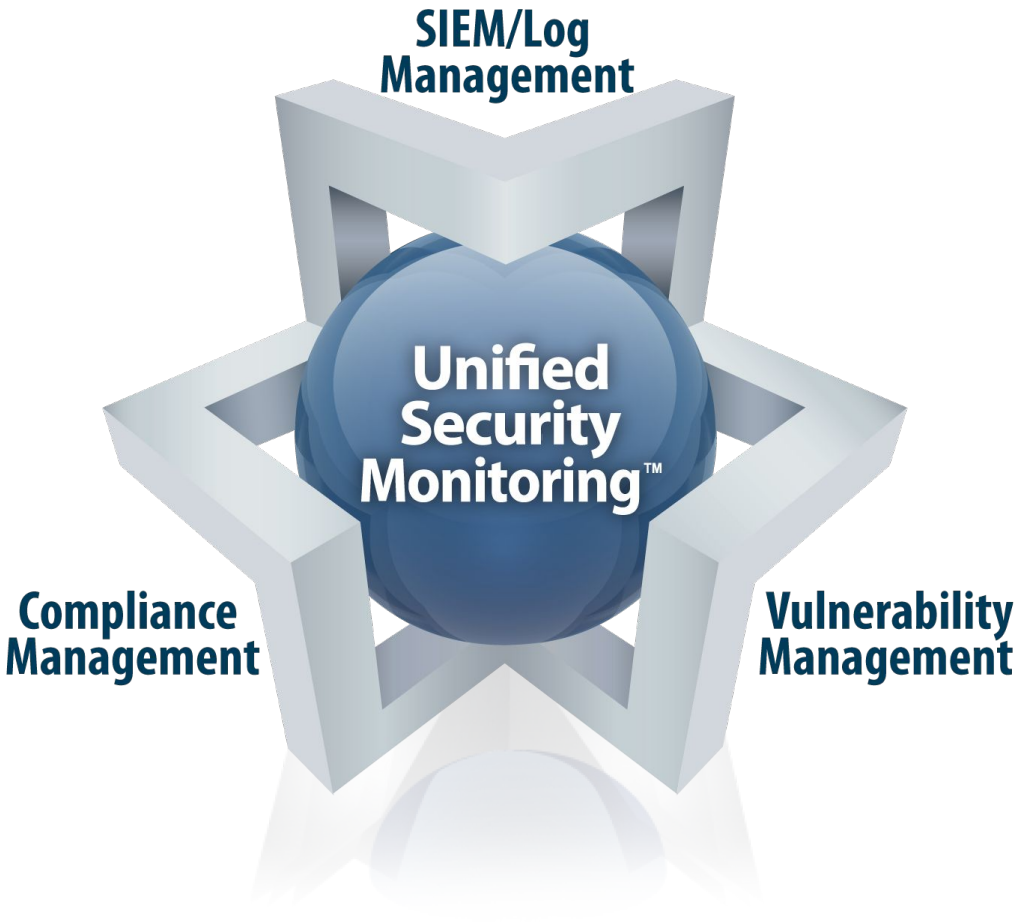


TENABLE Network Security®

В чем уникальность решения от Tenable

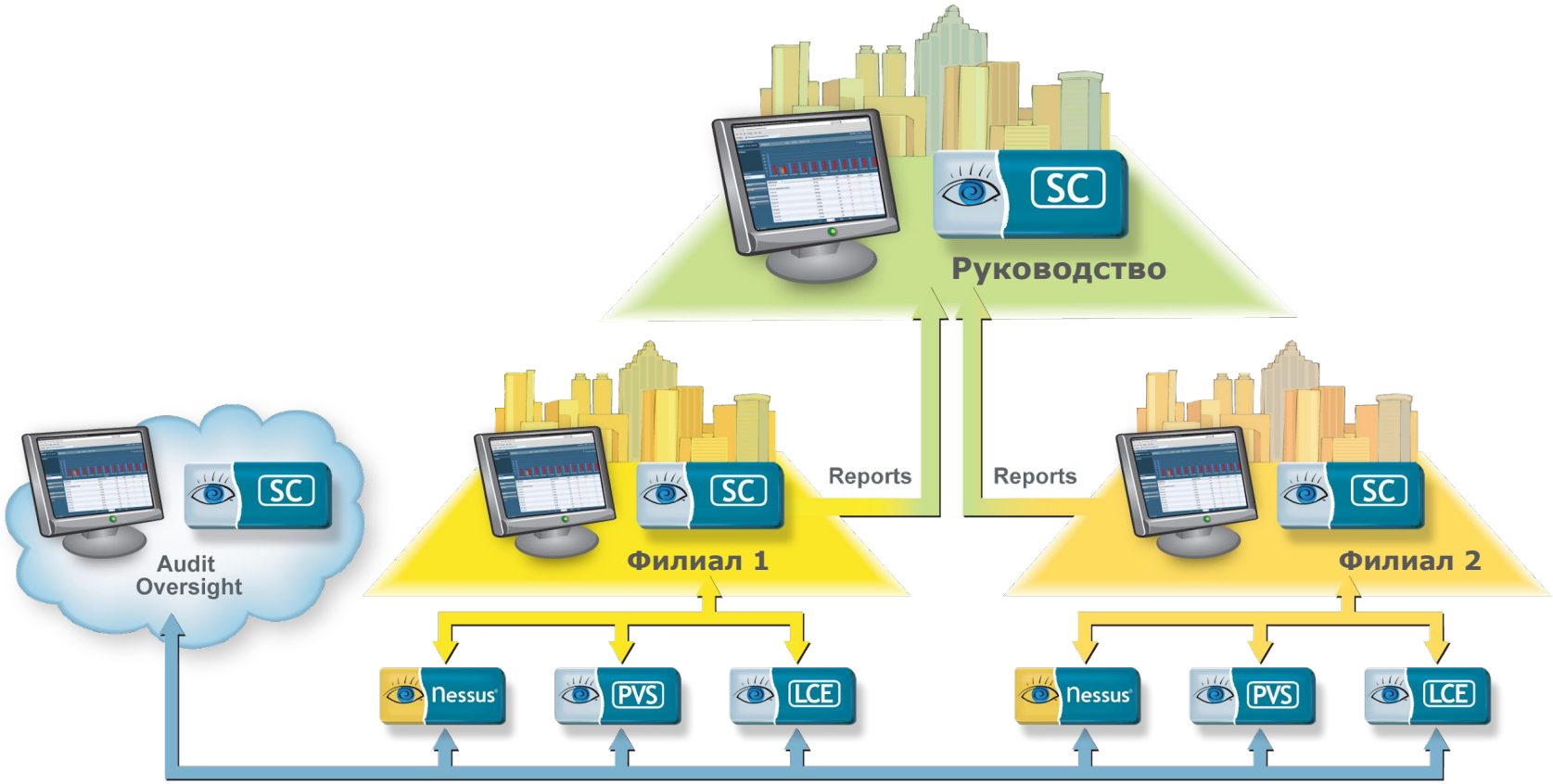
Концепция объединенной безопасности от Tenable отличается от других продуктов на рынке именно возможностью комбинацией любого решения по наличию модулей или использовать одно единое решение для всех задач.

Гибкая ценовая политика на рынке позволяет строить систему существенно дешевле по стоимости чем у конкурентов



TENABLE Network Security®

Гибкое управление предприятием



TENABLE Network Security®

Аудит систем

UNIX, Windows & Cisco

- ИспользованиеWindows Domain Credentials
- Cisco SNMP
- Unix Secure Shell/Elevated Su/Sudo

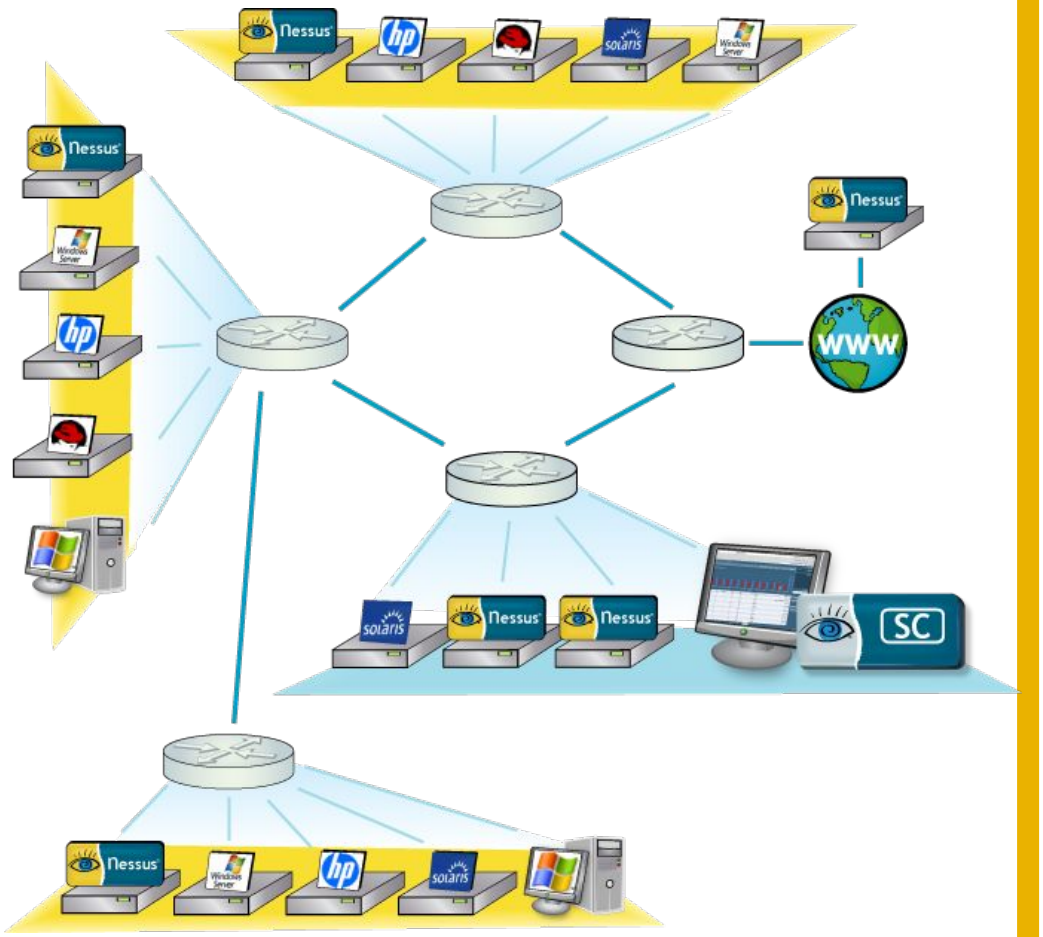
Проверка обновлений

- Обнаружение неактуальных патчей
- Аккуратное сканирование
- Отражение результата
- Работа с .dll, .exe & MD5 файлами

Опрос по WMI

Механизм WMI позволяет:

- Получать информацию о системе
- Сохранять данные по NIC
- Сохранять историю использования USB устройств
- Проверять лицензионное ли ПО
- Производить проверки ОС по WMI



TENABLE Network Security®

SecurityCenter и аудита соответствия систем.

Аудит UNIX & Windows

- Nessus через консоль SecurityCenter использует файлы проверки конфигураций
- Файлы ".audit" проверяют политику настройки систем на соответствие локальной или глобальной политикам ИБ
- Результаты проверки отображаются в консоли SecurityCenter как «успешно»", "неуспешнol" or "недоступно"
- Аутентификация типа AGENT-LESS
- 26 сертифицированных шаблонов от CIS

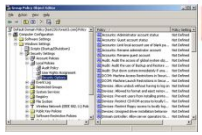
От класса C до класса A

- Средства поддержки файлов *nix
- Создание своих файлов аудита для анализа конфигурационных файлов *nix
- Проверка контрольных сумм файлов MD5
- Проверка текстовых файлов логов и журналов по содержимому из таких систем как Snort, Apache, межсетевые экраны и других

Управление в SecurityCenter

- Scan management for applying the right audit to the correct asset group
- Reporting on compliant or non-compliant devices by asset group
- Management of credentials required to perform the audit testing
- Required use of Nessus 3.x or above

Разные источники для аудита



MS .inf файл Политик от Microsoft

Своя Политика

TENABLE Network Security®

Политки Tenable

C to A Tool

*nix Config. И Audit файлы

TENABLE Network Security®

Ролевая модель доступа

Пользователь SecurityCenter ограничен в рамках организации по анализу состояния ИБ, событий IDS и логов при авторизации.

	Nessus	PVS	SC	LCE
Поддерживаемая ОС	Различные версии UNIX и Windows платформ, Mac OS X VMWARE	RedHat ES3, ES4, ES5 CentOS 5	RedHat ES5 CentOS 5 VMWARE	RedHat ES3, ES4, ES5 CentOS 5
Требует APPS	Нет	Нет	Нет	Нет
Поддержка платформ 32- И 64-bit	нет	нет	RedHat ES5, CentOS 5 (64-bit)	нет
Обнаружение уязвимостей	Аудит на наличие патчей и сетевое сканирование систем	Прослушивание трафика	Система сбора результатов	нет
Обнаружение атак и закладок	Обнаружение Backdoor	Система IDS	нет	В наличии 4000+ отдельные сигнатуры + 50 правил корреляции логов
Управление	CLI	W2K: GUI Unix: CLI	WEB интерфейс 100 пользователей	CLI
Поставка	RPM пакет	W2K: exe Unix: RPM	RPM пакет	RPM пакет
Агрегация	N/A	N/A	N/A	100 уникальных устройств и ОС
Корреляция	Обнаружение потенциальных уязвимостей	Обнаружение фактов компрометации в трафике приложений	Корреляция событий ИБ и в разрезе активов организации	Статистическая и событийная корреляция

Training Delivery Methods

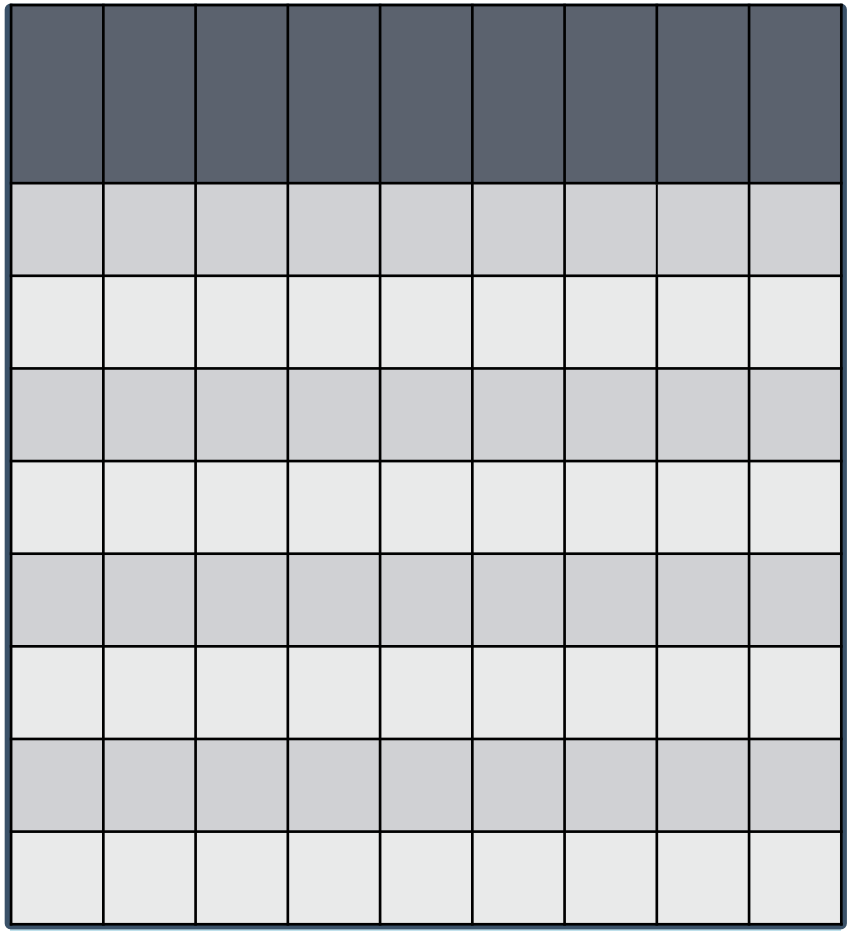
- For more information, please visit: www.tenable.com/training
- All costs are per person, per day

Training Objective	Classroom	Virtual Classroom	Onsite	On Demand
Maximum Interactivity	✓	✓	✓	
Rapid Skill Transfer	✓	✓	✓	✓
Team Building		✓	✓	
Large-scale Deployments		✓	✓	✓
Reduce Travel Costs		✓	✓	✓

Настраиваемый персональный рабочий стол, оповещения и отчетность в Security Center 4.2

Примеры

- Раздел PCI (1-12)
- Стандарт FISMA
- События ИБ
- Мониторинг Web
- Логи для IT службы
- Логи CERT
- Стандарт ISO
- Логи по SCADA



Лицензия на 50 Silo в LCE 3.4.2

- 1 silo до 4GB база - размер 20-35 млн. событий
- Единый формат логов событий
- 3 silo доступны для легальных пользователей:

Размер Silo	Максимальное количество событий (m)
50	1000 – 1750
255	5100 - 8925

Около 9 млрд. событий в минуту