Сетевой аудит

- Как начать?
- Что искать?
- Какие инструменты использовать?
- Примеры

Цикл ВА


Оценка рисков и разработка плана аудита
Сбор информации и планирование
Разработка программы аудита
Исполнение программы аудита и документирование
Подготовка аудиторского отчета
Процедуры последующего контроля
Отчетность аудиторского комитета перед Советом

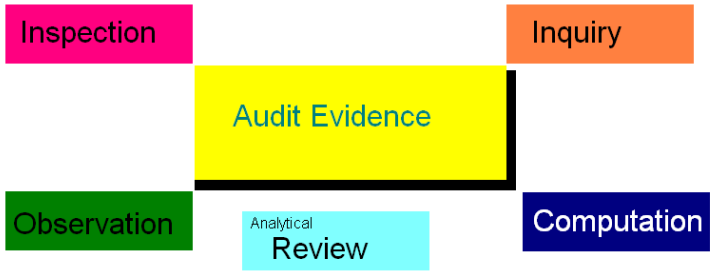
Суть аудиторской проверки

Планирование аудита

- ✓ Установить объём и цели
- ✓ Организовать аудиторскую группу
- ✓ Ознакомиться с особенностями ведения бизнеса
- ✓ Рассмотреть результаты предыдущих аудиторских проверок
- ✓ Выявить факторы риска
- ✓ Подготовить программу аудита

Сбор аудиторских доказательств

- ✓ Наблюдение за операционной деятельностью
- ✓ Рассмотрение документации
- ✓ Обсуждения с сотрудниками
- ✓ Физический осмотр имущества
- ✓ Подтверждение через третьих лиц
- ✓ Воспроизведение процедур
- ✓ Аналитический обзор
- ✓ Аудиторская выборка



Планирование, 1

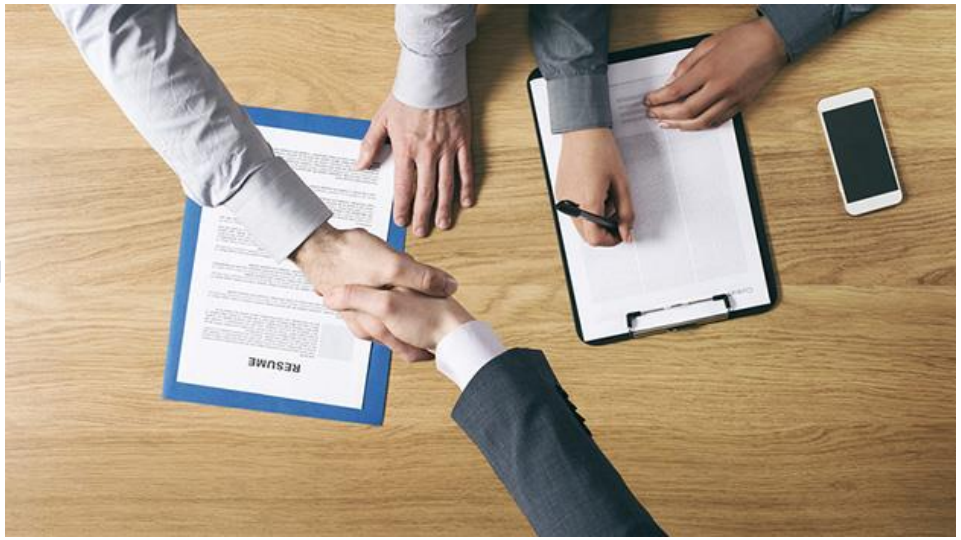
1. Понимание сети на уровне политики

- Сетевая схематика (физическая и логическая)
- Политика сетевой безопасности
- Политика удаленного доступа
- Политика управления конфигурацией
- Политика управления изменениями
- Политика управления пользователями
- Политика доступа в Интернет
- Политика в области электронной почты и коммуникаций
- Политика в отношении использования сотрудниками собственных устройств (BYOD)
- Политика резервного копирования и восстановления

2. Беседа с директором по информации и директором по информационной безопасности

2.1. Беседа со старшим администратором сети

2.2. Беседа со старшим администратором по сетевой безопасности



Мероприятия по подготовке задания

Определить требования к составу группы для выполнения аудиторского задания

Оценить достаточность компетенции в группе

Планирование, 2

3. Изучить последний отчет об оценке и анализе рисков

3. Изучить последний отчет о проверке сети

Report Summary			
Scanner Name	Retina	Machines Scanned	1
Scanner Version	5.11.3.2135	Vulnerabilities Total	132
Scan Start Date	4/22/2010	High Risk Vulnerabilities	75
Scan Start Time	4:15:36 PM	Medium Risk Vulnerabilities	20
Scan Duration	0h 0m 57s	Low Risk Vulnerabilities	37
Scan Name	Untitled	Information Only Audits	18
Scan Status	Completed	Credential Used	56563119E37464C1B98CF5EB34680809
Vulnerable Machines	1		

Цели и риски контроля

Созданы механизмы выявления как внутренних, так и внешних рисков и реагирования на них.

Для защиты ИТ-ресурсов и данных компании внедрены средства контроля сетевой безопасности. Управление устройствами сетевой безопасности осуществляется надлежащим образом

ИТ-активы в сети защищены надлежащим образом

Внедрено надлежащее управление изменениями

Обязанности в области ИТ надлежащим образом определены и доведены до сведения соответствующих лиц

Сеть по своим параметрам инфраструктуры, мощности и безопасности отвечает стратегическим планам в области ИТ, которые тесно согласованы с бизнес-целями.

Привилегии доступа пользовательских учетных записей должным образом санкционированы

Разработаны и внедрены резервные мощности на случай непредвиденных событий.

Существуют средства контроля аутентификации и авторизации для доступа к операционным и значимым прикладным системам.

Не определены функциональные обязанности по авторизации и администраторскому доступу.

Слабый план послеаварийного восстановления

Отсутствуют средства контроля для настройки нового пользователя и закрытия учетной записи

Стратегический план по ИТ устарел или отсутствует

Отсутствуют методологии администрирования ИТ, процедуры и стандарты конфигурирования паролей

Потребность в официальной системе управления изменениями

Недостаточность средств контроля для серверного помещения

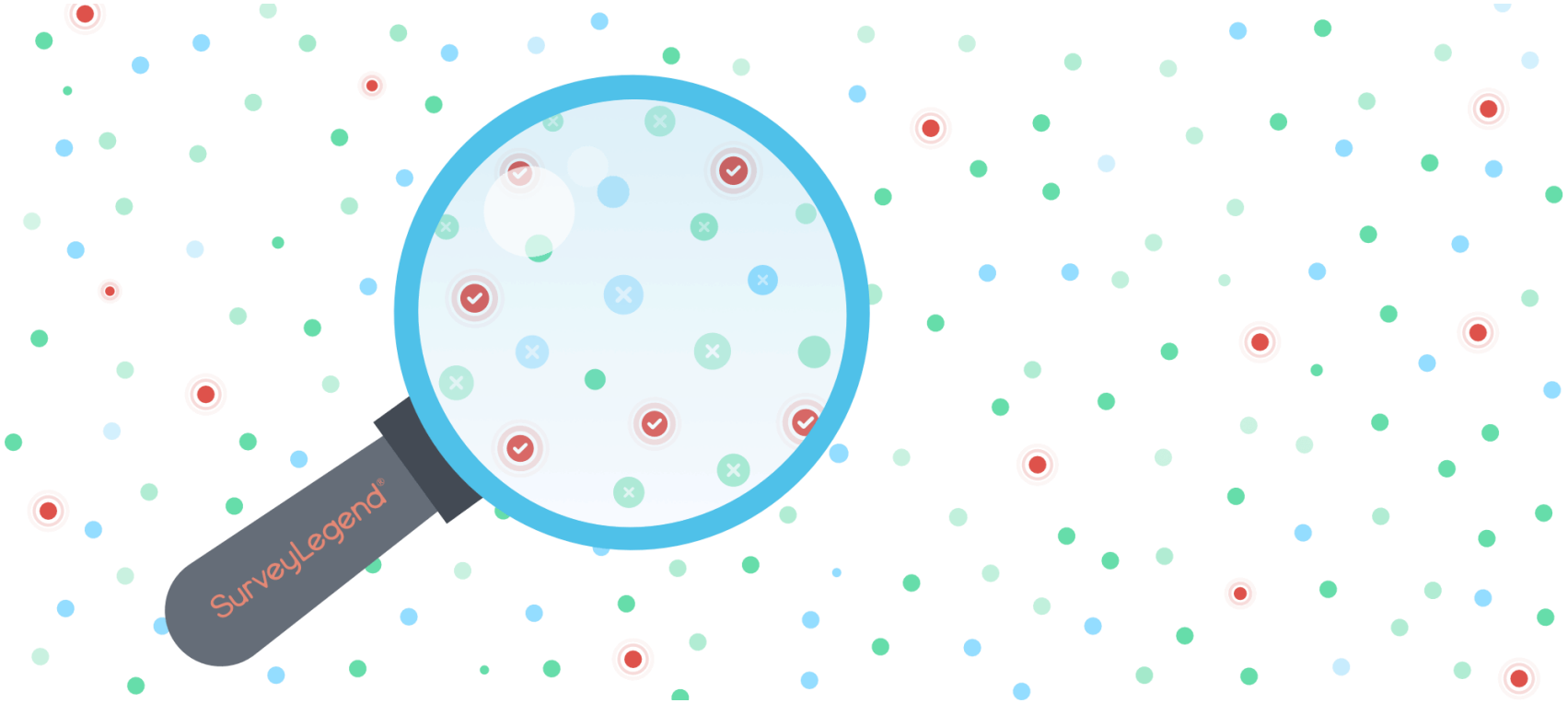
Недостаточный мониторинг сети

Отсутствие оценки ИТ-рисков

Создание матрицы контроля рисков

Риск	Средство контроля	Процедура проверки
Отсутствие или недостаточность оценки ИТ-рисков	Выявление рисков *(как внутренних, так и внешних)* задокументировано в руководстве по управлению рисками	Убедиться в том, что были созданы механизмы выявления как внутренних, так и внешних рисков и реагирования на них и найти подтверждение их наличия. ✓ Беседа с директорами по информации и информационной безопасности ✓ Изучить руководство по управлению рисками ✓ Изучить выявленный высокий риск ✓ Изучить внедренные средства контроля
Недостаточность средств контроля настройки нового пользователя и закрытия учетной записи	Имеется руководство по работе с пользователями	✓ Беседа с кадровой службой ✓ Выбрать ключевых сотрудников и проверить настройки их учетных записей и закрытие учетных записей
Отсутствуют методологии администрирования ИТ, процедуры и стандарты конфигурирования паролей	Имеется политика по работе с паролями	✓ Беседа с сетевым администратором ✓ Проверить и подтвердить, было ли внедрено и соблюдается ли требование относительно сложности пароля для всех сетевых устройств.
Недостаточно проработанный процесс управления изменениями	Действует процесс управления изменениями, имеются соответствующие процедуры	✓ Беседа с директором по сетевой безопасности и администратором сети ✓ Убедиться и получить подтверждение того, что требования по управлению изменениями соблюдаются при любых изменениях в сети, конфигурации устройств, правилах использования межсетевого экрана и т.д..
✓ Несанкционированный доступ в	✓ Доступ в серверную предоставлен	✓ Изучить записи на предмет наличия случаев

Формирование выборки



Пример

Описание средства контроля: Доступ к корневым каталогам сетевых устройств имеют только старшие администраторы

В отношении описанного выше средства контроля ответьте на следующие вопросы:

1. Какие доказательства необходимо получить?
2. Как определить размер выборки?
3. Какие проверочные шаги необходимо предпринять для проверки данного средства контроля?

Пример, размер выборки

Размер выборки в отношении средств контроля (администраторского) доступа к корневым каталогам зависит от критичности системы; количества учетных записей пользователей, количества сетевых устройств и т.д.

Проверочные шаги

1. Для получения представления о конфигурации системы безопасности обратитесь в ИТ-службу
2. Попросите, чтобы под вашим наблюдением был сгенерирован системный запрос для получения списка пользователей с правами доступа к корневым каталогам.
3. Сравните список старших администраторов с организационной структурой ИТ или списком работающих сотрудников, чтобы определить, соответствует ли уровень доступа пользователей их должностным обязанностям
4. Выясните у руководства ИТ-службы, насколько лица с правами администратора соответствуют предъявляемым требованиям.
5. Проанализируйте журналы событий на предмет наличия аномалий.

Пример

Описание средства контроля: Для управления резервным копированием и сохранением данных на всех сетевых устройствах внедрены автоматизированные инструменты управления конфигурацией. Журналы резервного копирования проверяются каждый раз после любого изменения конфигурации и документируются в контрольном листе "Журнала резервного копирования конфигурации"..

В отношении описанного выше средства контроля ответьте на следующие вопросы:

1. Какие доказательства необходимо получить?
2. Как определить размер выборки?
3. Какие проверочные шаги необходимо предпринять для проверки данного средства контроля?

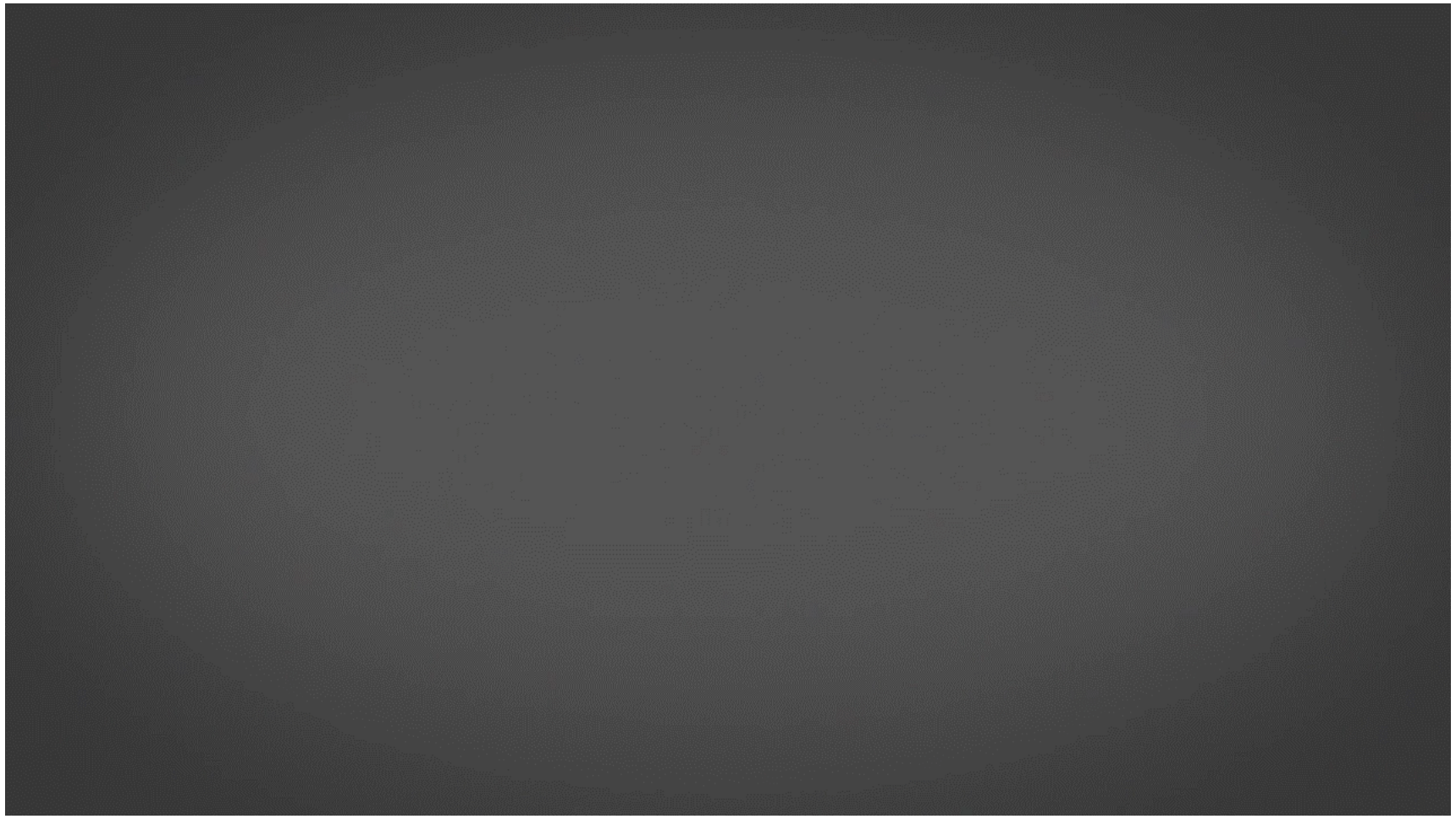
Пример, размер выборки

Размер выборки для контроля управления изменениями конфигурации основан на всей совокупности изменений, критичности сетевых устройств и т.д.

Проверочные шаги:

1. Получить от сетевого администратора расписание резервного копирования (для проверяемых устройств) из автоматизированного инструмента.
2. Произвольно сделайте выборку из нескольких дней
3. Для этой выборки получите файл истории операций и убедитесь в том, что операции выполнялись в соответствии с политикой.
4. Получите проверочный перечень журнала резервного копирования конфигурации и убедитесь в том, что операции выполнялись согласно расписанию резервного копирования.
5. Если операции выполнялись не в соответствии с политикой, определите, было ли проведено соответствующее расследование, и была ли решена проблема.

Инструменты для аудита сети



Инструменты для аудита сети

1. **Spiceworks Inventory -** инструмент инвентаризации сети, который автоматически обнаруживает сетевые устройства.
2. **Nessus -** бесплатный инструмент оценки уязвимости с более чем 450 шаблонами конфигурации и настраиваемыми отчетами.
3. **Network Inventory Advisor -** инструмент инвентаризационного сканирования, совместимый с устройствами Windows, Mac OS и Linux.
4. **ManageEngine Vulnerability Manager** (имеется бесплатная пробная версия) - Этот пакет проверочных программ системной безопасности проверяет вашу сеть и обнаруживает слабые места в системе безопасности. Работает в среде Windows и Windows Server.
5. **Netwrix Auditor -** программное обеспечение для аудита сетевой безопасности с мониторингом конфигурации, автоматическими оповещениями.
6. **Nmap (Zenmap GUI) -** сканер портов с открытым исходным кодом и сетевой картограф, запускаемый через интерфейс командной строки.
7. **OpenVAS -** инструмент оценки уязвимости для пользователей Linux с регулярными обновлениями.
8. **Acunetix -** сканер безопасности веб-приложений, который при условии его интеграции с OpenVAS может обнаруживать более 50 000 сетевых уязвимостей.
9. **Metasploit** - Инструмент для тестирования на проникновение, позволяющий взломать эксплойты в сети.

QA


Thank You