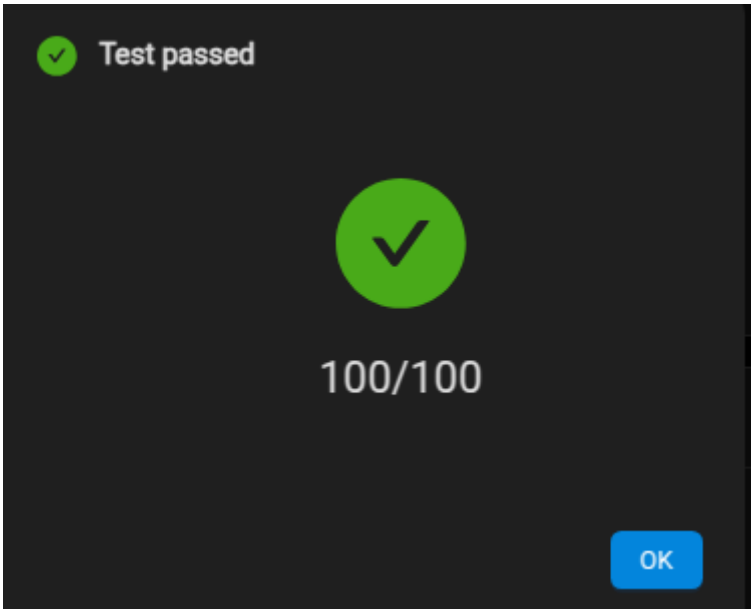

1. Какой метод наиболее эффективен для предотвращения утечек данных через USB

○ Записать все данные на CD-диски
○ Ghi toàn bộ dữ liệu vào đĩa CD

○ Удалить драйверы USB из системы
○ Gỡ trình điều khiển USB khỏi hệ thống

○ Разрешить USB, но периодически проверять их антивирусом
○ Cho phép sử dụng USB, nhưng kiểm tra định kỳ bằng phần mềm diệt virus

✅ **Запретить использование USB-устройств через DLP-политики**
✅ **Cấm sử dụng thiết bị USB thông qua chính sách DLP**

---

2. Какая функция SIEM критична для анализа угроз

✅ **Корреляция событий из разных источников в реальном времени**
✅ **Tương quan sự kiện từ nhiều nguồn khác nhau theo thời gian thực**

○ Удаление старых событий через 1 день
○ Xóa sự kiện cũ sau 1 ngày

○ Отключение логов для экономии места на диске
○ Tắt ghi log để tiết kiệm dung lượng

○ Ручной просмотр логов раз в месяц
○ Xem log thủ công mỗi tháng một lần

---

3. Как настроить резервное копирование для защиты от ransomware
○ Копировать данные в ту же папку на основном диске
○ Sao chép dữ liệu vào cùng thư mục trên ổ chính

○ Использовать только облачное хранилище без шифрования
○ Chỉ sử dụng lưu trữ đám mây mà không mã hóa

○ Не делать бэкапы, чтобы не привлекать злоумышленников
○ Không sao lưu để tránh bị kẻ xấu chú ý

✅ **Хранить бэкапы на изолированном носителе с историей версий**
✅ **Lưu trữ bản sao lưu trên thiết bị cách ly có lưu lịch sử phiên bản**

---

4. Как DLP-система обнаруживает утечку конфиденциальных данных
○ Блокирует доступ в интернет для всех сотрудников
○ Chặn quyền truy cập Internet cho toàn bộ nhân viên

✅ **Анализ ключевых слов, шаблонов (например, номеров карт) и меток**
✅ **Phân tích từ khóa, mẫu (ví dụ: số thẻ) và nhãn**

○ Удаляет все вложения из электронной почты
○ Xóa tất cả tệp đính kèm trong email

○ Отключает клавиатуру при вводе слова "секретно"
○ Vô hiệu hóa bàn phím khi nhập từ “bí mật”

---

5. Что включает в себя настройка SIEM для мониторинга атак
○ Отправка всех логов в корзину
○ Gửi tất cả log vào thùng rác

○ Удаление событий, связанных с администраторами
○ Xóa sự kiện liên quan đến quản trị viên

✅ **Интеграция с Active Directory, фаерволом и антивирусом**
✅ **Tích hợp với Active Directory, tường lửa và phần mềm diệt virus**

○ Запись только успешных входов в систему
○ Ghi lại chỉ những lần đăng nhập thành công vào hệ thống

---

6. Какой метод резервного копирования обеспечит минимальное время восстановления
○ Хранить бэкапы на том же сервере, что и исходные данные
○ Lưu bản sao lưu trên cùng máy chủ với dữ liệu gốc

○ Не проверять целостность бэкапов
○ Không kiểm tra tính toàn vẹn của các bản sao lưu

✅ **Полное + инкрементальные бэкапы с ежедневным выполнением**
✅ **Sao lưu đầy đủ + gia tăng, thực hiện hàng ngày**

○ Только полные бэкапы раз в месяц
○ Chỉ sao lưu đầy đủ mỗi tháng một lần

---

7. Какое правило DLP поможет предотвратить утечку через почту
○ Удалить все вложения из исходящих писем
○ Xóa tất cả tệp đính kèm khỏi thư gửi đi

○ Разрешить пересылку данных на личные email-адреса сотрудников
○ Cho phép chuyển tiếp dữ liệu đến email cá nhân của nhân viên

○ Шифровать только заголовки писем
○ Chỉ mã hóa tiêu đề email

✅ **Блокировка отправки писем с вложениями, содержащими ключевые слова**
✅ **Chặn gửi email có tệp đính kèm chứa từ khóa nhạy cảm**

---

8. Как SIEM помогает в расследовании инцидентов
○ Отключение уведомлений при обнаружении подозрительных событий
○ Tắt thông báo khi phát hiện sự kiện đáng ngờ

✅ **Сбор и визуализация логов с возможностью поиска по временным меткам**
✅ **Thu thập và trực quan hóa log với khả năng tìm kiếm theo dấu thời gian**

○ Хранение логов в незащифрованном виде
○ Lưu log dưới dạng không mã hóa

○ Автоматическое удаление логов через 1 час после записи
○ Tự động xóa log sau 1 giờ ghi

---

9. Как защитить резервные копии от несанкционированного доступа
○ Отказаться от бэкапов, чтобы не рисковать
○ Không sao lưu để tránh rủi ro

○ Хранить пароли от бэкапов в открытом файле на рабочем столе
○ Lưu mật khẩu của bản sao lưu trong file văn bản trên desktop

○ Использовать один пароль для всех архивов
○ Dùng chung một mật khẩu cho mọi bản lưu trữ

✅ **Шифрование бэкапов + многофакторная аутентификация для доступа**
✅ **Mã hóa bản sao lưu + xác thực đa yếu tố khi truy cập**

---

10. Что исключить из политики DLP
○ Мониторить трафик на наличие ключевых слов
○ Giám sát lưu lượng để phát hiện từ khóa

○ Шифровать данные при передаче в облако
○ Mã hóa dữ liệu khi truyền lên đám mây

○ Классифицировать данные по уровню конфиденциальности
○ Phân loại dữ liệu theo mức độ nhạy cảm

✅ **Разрешить сотрудникам копировать базы данных на личные флешки**
✅ **Cho phép nhân viên sao chép cơ sở dữ liệu vào USB cá nhân**
