↑ 목록으로 ← 이전 단원

5단원. 보안 관제 실무

> 대상: 전공자 · 정보처리기사 취득자 | 목적: 인프라 직무(네트워크·클라우드·시스템·보안) 기술 면접 대비 중요도: ★★★ 최빈출 · ★★ 자주 출제 · ★ 기본 개념

Q1. **SOC(Security Operations Center)**의 주요 업무를 설명하세요. ★★★

답안 **SOC**는 조직의 보안 위협을 상시로 모니터링하고 대응하는 전담 조직으로, 핵심 업무는 24시간 실시간 로그·이벤트 모니터링을 통해 침해 징후를 탐지하는 것입니다. 탐지된 이벤트는 정상·오탐·실제 위협 여부를 분석(트리아지, **Triage**)하여 심각도를 판단하고, 실제 위협으로 확인되면 침해사고 대응 절차에 따라 격리·차단 등의 조치를 취합니다. 이 외에도 보안 장비(방화벽, IPS, EDR 등)의 정책 관리와 튜닝, 신규 위협 인텔리전스 반영, 정기적인 취약점 점검 및 패치 관리 조율, 경영진 보고를 위한 보안 현황 리포팅 등이 SOC의 주요 업무에 포함됩니다.

관련 개념 실시간 모니터링, 트리아지, 위협 인텔리전스, EDR, 보안 리포팅

Q2. **SIEM(Security Information and Event Management)**의 개념과 필요성을 설명하세요. ★★★

답안 **SIEM**은 방화벽, IPS, 서버, 애플리케이션 등 조직 내 다양한 장비와 시스템에서 발생하는 로그와 이벤트를 한곳에 수집·정규화·저장하고, 이를 상관분석(Correlation)해 의미 있는 보안 이벤트로 만들어주는 플랫폼입니다. 개별 장비의 로그만 봐서는 발견하기 어려운 복합적인 공격 패턴(예: 여러 시스템에 걸친 로그인

실패 후 특정 서버에서의 이상 행위)을, 여러 소스의 로그를 시간 순으로 연관지어 탐지할 수 있다는 점이 핵심 가치입니다. 실무에서는 사전에 정의된 상관 분석 규칙 **(Correlation Rule)**에 따라 의심스러운 이벤트가 발생하면 자동으로 경보를 생성해 관제 담당자에게 전달하며, 사고 발생 시 과거 로그를 신속히 검색해 조사(포렌식)하는 용도로도 활용됩니다.

관련 개념 로그 수집·정규화, 상관분석(Correlation Rule), 알람(Alert), 로그 보존 기간, SOAR 연계

> **Q3.** 로그 분석 시 정상 트래픽과 이상 트래픽을 구분하는 일반적인 접근 방법을 설명하세요. ★★★

답안 로그 분석의 기본 접근은 베이스라인(평상시 정상 패턴)을 파악한 뒤 이로부터의 이탈을 탐지하는 것입니다. 예를 들어 특정 계정의 평소 로그인 시간대·위치·빈도를 기준으로 삼아, 심야 시간대 해외 IP에서의 접속이나 짧은 시간 내 다수의 로그인 실패 후 성공(**Brute Force** 의심) 같은 패턴을 이상 징후로 판단합니다. 또한 알려진 공격 시그니처와의 매칭(시그니처 기반)과 정상 범위를 벗어난 통계적 변화 탐지(이상탐지 기반)를 함께 활용하며, 단일 로그만으로 판단하기보다 여러 로그 소스(방화벽, 서버, 인증 시스템 등)를 상관 분석해 오탐을 줄이고 실제 위협 여부를 검증합니다. 최종적으로는 담당자가 이벤트의 맥락(어떤 시스템인지, 얼마나 민감한 자산인지)을 고려해 실제 대응 여부를 결정합니다.

관련 개념 베이스라인, Brute Force 탐지, 시그니처/이상탐지, 로그 상관분석, 오탐 최소화

> **Q4.** 침해사고 대응 절차를 단계별(탐지-분석-격리-복구 등)로 설명하세요. ★★★

답안 일반적인 침해사고 대응은 탐지(**Detection**) → 분석(**Analysis**) → 격리/차단(**Containment**) → 제거(**Eradication**) → 복구(**Recovery**) → 사후 분석 **(Lessons Learned)**의 순서로 진행됩니다. 탐지 단계에서는 SIEM 알람, 관제 요

원의 이상 징후 발견, 사용자 신고 등을 통해 사고를 인지하고, 분석 단계에서는 로그와 시스템을 조사해 침해 경로와 피해 범위를 파악합니다. 격리 단계에서는 감염된 시스템을 네트워크에서 분리하거나 관련 계정을 차단해 피해 확산을 막는 것이 최우선이며, 제거 단계에서는 악성코드나 백도어 등 원인을 완전히 제거하고, 복구 단계에서 정상 서비스를 재개합니다. 마지막 사후 분석 단계에서는 사고 원인과 대응 과정을 정리해 재발 방지 대책과 프로세스 개선에 반영합니다.

관련 개념 Containment(격리), Eradication(제거), Recovery(복구), Lessons Learned, 사고 대응 계획(IRP)

> **Q5.** 침해사고 발생 시 초기 대응에서 격리(**Containment**)가 가장 중요한 이유와 주의할 점을 설명하세요. ★★★

답안 격리는 피해가 다른 시스템으로 확산되는 것을 막는 가장 시급한 조치이기 때문에 사고 대응 초기 단계에서 최우선으로 다뤄집니다. 감염된 서버를 즉시 네트워크에서 분리하거나 방화벽에서 관련 IP·포트를 차단해 랜섬웨어의 추가 확산이나 공격자의 지속적인 접근을 차단하는 것이 목적입니다. 다만 주의할 점은, 시스템을 무조건 종료하거나 재부팅하면 메모리에 남아 있는 휘발성 증거(실행 중인 프로세스, 네트워크 연결 정보 등)가 사라져 이후 포렌식 분석에 어려움이 생길 수 있다는 것입니다. 따라서 실무에서는 가능하다면 네트워크 연결만 차단하고 시스템 전원은 유지한 채로 증거를 수집한 뒤 격리 조치를 이어가는 것을 원칙으로 합니다.

관련 개념 네트워크 격리, 휘발성 증거 보존, 디지털 포렌식, 증거 보전의 원칙, 사고 대응 우선순위

> **Q6.** 취약점 관리 프로세스(**Vulnerability Management**)의 전반적인 흐름을 설명하세요. ★★★

답안 취약점 관리는 자산 식별 → 취약점 스캐닝 → 위험도 평가 및 우선순위화 → 조치(패치/완화) → 재검증의 순환 구조로 이루어집니다. 먼저 조직 내 어떤 시스템과 자산이 존재하는지 자산 목록(인벤토리)을 파악하고, 정기적인 취약점 스캔을 통해

각 자산의 보안 취약점을 식별합니다. 발견된 취약점은 **CVSS** 점수와 자산의 중요도를 함께 고려해 우선순위를 매기고, 우선순위가 높은 것부터 패치 적용이나 설정 변경 등의 완화 조치를 수행합니다. 조치 후에는 반드시 재스캔을 통해 실제로 취약점이 해소되었는지 검증하며, 이 전체 과정을 정기적으로 반복해 지속적으로 보안 수준을 관리하는 것이 핵심입니다.

관련 개념 자산 인벤토리, 취약점 스캐닝, CVSS 우선순위화, 패치 관리, 재검증(재스캔)

> **Q7. EDR(Endpoint Detection and Response)**의 개념과 기존 백신(안티바이러스)과의 차이를 설명하세요. ★★

답안 전통적인 백신(안티바이러스)은 주로 알려진 악성코드의 시그니처(패턴)와 파일을 비교해 탐지·차단하는 방식으로, 새로운 변종이나 알려지지 않은(제로데이) 공격에는 취약합니다. **EDR**은 엔드포인트(PC, 서버 등)에서 발생하는 프로세스 실행, 파일 접근, 네트워크 연결 등 행위 정보를 지속적으로 수집·기록해, 시그니처에 의존하지 않고 비정상적인 행위 패턴을 탐지할 수 있으며, 사고 발생 시 해당 엔드포인트의 상세한 활동 이력을 조사(포렌식)하고 원격으로 격리·프로세스 종료 같은 대응 조치까지 수행할 수 있다는 점에서 차이가 있습니다. 실무 SOC에서는 EDR에서 발생하는 알람도 SIEM과 연계해 통합 모니터링하는 경우가 많습니다.

관련 개념 시그니처 기반 탐지, 행위 기반 탐지, 엔드포인트 가시성, 원격 격리, 제로데이

> **Q8.** 위협 인텔리전스(**Threat Intelligence**)란 무엇이며 관제 업무에 어떻게 활용되나요? ★★

답안 위협 인텔리전스는 현재 활동 중인 공격자 그룹의 수법, 악성코드의 특징, 알려진 악성 IP·도메인·해시값(IoC, Indicator of Compromise) 등 위협에 대한 정보를 체계적으로 수집·분석한 결과물입니다. SOC에서는 이러한 IoC를 방화벽, IPS, SIEM 등의 탐지 규칙에 반영해 새로운 위협을 선제적으로 차단하거나 탐지 정확도

를 높이는 데 활용합니다. 또한 침해사고 분석 시 발견된 흔적을 위협 인텔리전스와 대조해 어떤 공격 그룹의 수법과 유사한지, 추가로 어떤 시스템이 노려질 가능성이 있는지를 판단하는 데도 사용됩니다. 실무에서는 외부 위협 인텔리전스 피드를 구독하거나 업계·정부 기관 간 정보를 공유하는 체계를 함께 활용합니다.

관련 개념 IoC(침해지표), 공격자 그룹 프로파일링, 위협 피드, 선제적 차단, 정보 공유 체계

> **Q9.** 보안 관제에서 오탐(**False Positive**)이 많이 발생할 때의 문제점과 개선 방법을 설명하세요. ★★

답안 오탐이 지나치게 많으면 관제 담당자가 실제 위협 경보에도 경계심이 무뎌지는 "알람 피로(**Alert Fatigue**)" 현상이 발생해, 정작 중요한 실제 침해 징후를 놓칠 위험이 커집니다. 또한 매번 정상 트래픽을 조사하는 데 인력과 시간을 낭비하게 되어 관제 효율이 크게 떨어집니다. 개선 방법으로는 조직의 실제 환경에 맞게 탐지 규칙(시그니처, 임계치)을 지속적으로 튜닝하고, 알려진 정상 패턴은 화이트리스트(예외 처리)로 등록하며, 여러 로그를 종합해 판단하는 상관분석 규칙을 고도화해 단편적인 이벤트만으로 경보가 발생하지 않도록 개선하는 것이 필요합니다. 최근에는 이러한 반복 업무를 줄이기 위해 **SOAR(**보안 오케스트레이션 자동화**)** 도구로 저위험 이벤트의 초기 분석을 자동화하는 추세입니다.

관련 개념 Alert Fatigue, 탐지 규칙 튜닝, 화이트리스트, 상관분석 고도화, SOAR

> **Q10.** 보안 관제 업무에서 다루는 주요 로그의 종류와 각각에서 확인할 수 있는 정보를 설명하세요. ★★

답안 관제 업무에서는 다양한 소스의 로그를 종합적으로 다룹니다. 방화벽/네트워크 장비 로그에서는 허용·차단된 트래픽의 출발지/목적지 IP, 포트 정보를 확인할 수 있어 비정상 접근이나 스캔 시도를 파악할 수 있습니다. 서버/**OS** 로그(시스템 로그, 인증 로그)에서는 로그인 성공·실패 기록, 권한 변경, 프로세스 실행 이력을 확인해 계정 탈취나 권한 상승 시도를 탐지합니다. 웹 서버/**WAF** 로그에서는 HTTP 요청

패턴을 통해 SQL 인젝션이나 비정상 파라미터 시도를 확인할 수 있으며, 애플리케이션 로그에서는 비즈니스 로직 상의 이상 행위(대량 주문, 비정상 결제 시도 등)를 파악할 수 있습니다. 이러한 서로 다른 계층의 로그를 SIEM으로 통합해 상관분석하는 것이 정확한 침해 탐지의 핵심입니다.

관련 개념 방화벽 로그, 인증 로그, WAF 로그, 애플리케이션 로그, 통합 로그 상관분석
