1.Apa itu *CIA Triad* dalam keamanan informasi, dan bagaimana prinsip ini diterapkan dalam lingkungan SOC?
2.Bagaimana langkah-langkah yang Anda ambil jika mendeteksi adanya aktivitas *malware* dalam jaringan perusahaan?
3.Jelaskan bagaimana Anda menggunakan alat SIEM untuk mendeteksi anomali dalam log jaringan. Apa metrik yang Anda pantau?
4.Bagaimana cara Anda mengidentifikasi serangan *phishing*? Apa langkah-langkah mitigasi yang Anda rekomendasikan?
5.Bagaimana Anda menilai risiko dari kerentanan yang ditemukan dalam sistem perusahaan?
6.Jika perusahaan mengalami serangan DDoS, langkah apa yang Anda ambil untuk memitigasi dampaknya?
7.Bagaimana Anda melakukan analisis forensik pada endpoint yang dicurigai telah diretas? Apa alat yang biasa Anda gunakan?
8. Jika Anda menemukan adanya backdoor yang aktif di server produksi, apa prioritas pertama Anda?
9. Analisa file pada url berikut: https://github.com/adriyansyah-mf/sample
10. Lakukan analisa pada log pada repo: https://github.com/adriyansyah-mf/sample