Exemplo de um Relatório de incidentes de segurança cibernética

Este exemplo de relatório é para um evento de segurança diferente do cenário apresentado na atividade. Este exemplo só deve ser usado para se familiarizar com o formato de relatório esperado.

|  |
| --- |
| **Parte 1: Fornecer um resumo do problema encontrado no log de tráfego DNS e ICMP** |
| Os logs do analisador de protocolo de rede indicam que a porta 443 está inacessível ao tentar acessar o site seguro de verificação de antecedentes do funcionário. A porta 443 é normalmente usada para tráfego HTTPS. Isso pode indicar um problema com o servidor Web ou a configuração do firewall. É possível que isso seja um indício de um ataque malicioso ao servidor web. |
|

|  |
| --- |
| **Parte 2: Explique sua análise dos dados e forneça pelo menos uma causa do incidente** |
| O incidente ocorreu no início desta manhã, quando a equipe de recursos humanos (RH) informou que não conseguiu acessar o portal de verificação de antecedentes. A equipe de segurança de rede respondeu e começou a executar testes com a ferramenta de análise de protocolo de rede tcpdump. Os logs resultantes revelaram que a porta 443, que é usada para tráfego HTTPS, não está acessível. Continuamos a investigar a causa raiz do problema para determinar como podemos restaurar o acesso ao portal da Web seguro. Nossos próximos passos incluem verificar a configuração do firewall para ver se a porta 443 está bloqueada e entrar em contato com o administrador do sistema para que o servidor web verifique se há sinais de um ataque no sistema. A equipe de RH acredita que é possível que um determinado novo contratado queira impedi-los de realizar a verificação de antecedentes. A equipe de segurança da rede suspeita que essa pessoa pode ter lançado um ataque para travar o site de verificação de antecedentes. |