SOC170 – Passwd Found in Requested URL — Possible LFI Attack

Caso conduzido individualmente no simulador SOC da plataforma LetsDefend. Atuei como analista SOC N1, realizando todas as etapas de triagem, investigação, contenção e relatório.

📝 Descrição:

Recebido alerta SOC170 destacando uma tentativa suspeita de acesso ao arquivo sensível 'passwd' via LFI, a partir do endpoint WebServer1006 (172.16.17.13). A requisição HTTP incluía o parâmetro 'file=../../../../etc/passwd' — típico de exploração de Local File Inclusion (LFI).

🧠 Análise:

- Data/hora do evento: 1 de março de 2022, às 10h10 (UTC).
- Detalhes da requisição:
  - Fonte: IP 106.55.45.162, de origem externa (Internet).
  - Resposta HTTP: 500 Internal Server Error, com tamanho de resposta zero bytes, indicando que o ataque não teve sucesso, com base nos logs do firewall.
- Verificação de reputação:
  - Usei VirusTotal e Cisco Talos para analisar o IP de origem, confirmando atividade maliciosa e proveniência da China.

Apesar da tentativa de ataque, o sistema não retornou dados ao atacante, confirmando que a tentativa falhou.

🛠️ Ação tomada:

- Alerta classificado como True Positive, com base na tentativa explícita de acesso a 'passwd'.
- Não foi necessário isolar o servidor WebServer1006, já que o ataque falhou sem impactar o sistema.
- Sem movimentação lateral detectada ou execução remota bem-sucedida.

📤 Escalonamento:

Não houve necessidade de escalonar para o N2, visto que o ataque foi impedido com falha técnica sem causar impacto.

🖼️ Evidências / IOCs:

Tipo	Valor	Descrição
IP externo	106.55.45[.]162	Origem da requisição — associado a LFI
URL	/etc/passwd via LFI	Tentativa de incluir arquivo sensível
Host alvo	172.16.17[.]13	WebServer1006 — alvo da LFI

Resposta	HTTP 500	Indica falha na execução