SOC169 - Possible IDOR Attack Detected

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:

Foi identificado um possível ataque do tipo IDOR (Insecure Direct Object Reference) no host WebServer1005, a partir de uma requisição não autorizada que tentava acessar dados sensíveis de usuários por meio de manipulação direta de parâmetros na URL.

Análise:

Em 28 de fevereiro de 2022, às 22h48, o alerta SOC169 foi gerado pelo SIEM, indicando requisições consecutivas à mesma página no host WebServer1005 (IP: 172.16.17.15). O atacante tentou explorar uma vulnerabilidade IDOR acessando a URL: hxxps://172.16.17.15[.]/get_user_info/

Ferramentas utilizadas:
- Logs HTTP brutos para verificar os parâmetros manipulados (user_id=3) e o método POST utilizado.
- Reputação do IP no VirusTotal e AbuseIPDB, que indicaram o IP 134.209.118[.]137 como malicioso.
- Consulta de domínio digitalocean[.]com para associar o tráfego com infraestrutura do atacante.

Evidências:
- Origem do ataque: IP 134.209.118[.]137 (EUA), classificado como malicioso.
- Método: Manipulação direta de parâmetro POST.
- Resposta HTTP: Código 200 OK, com tamanho da resposta 351 bytes → o recurso foi acessado com sucesso, o que evidencia a falha de autorização.
- Domínio relacionado ao atacante: digitalocean[.]com

Ação tomada:

- O host foi contido para análise detalhada e o incidente foi escalado para o time N2.
- As evidências foram coletadas conforme o playbook da LetsDefend.

Escalonamento:

- O caso foi escalado ao time N2 após confirmação do ataque.

Evidências / IOCs:

Tipo	Valor	Descrição
IP Address	134.209.118[.]137	IP do atacante (EUA)

URL Address	hxxps://172.16.17.15/get_user_info/	Requisição IDOR
IP Address	172.16.17[.]15	Servidor vítima
Domain	digitalocean[.]com	Domínio relacionado ao atacante