Título: Protocolo de Respuesta y Mitigación - Cortex XDR SI360

Contenido:

1. Definición de la Alerta: Cortex XDR detecta anomalías basadas en comportamiento. Si el tráfico en el **NOC** supera el 85%, se considera un incidente crítico de disponibilidad.

2. Procedimiento de Aislamiento:

- **Paso A:** Identificar la IP de origen (generada aleatoriamente por el SI360).
- **Paso B:** Evaluar el impacto en el Nodo (Cúcuta o Catatumbo).
- **Paso C:** Ejecutar "Bloqueo de IP" en el panel de control para cortar la sesión maliciosa.

3. Post-Aislamiento: Verificar en el comando status que la IP ha sido enviada a la **Blacklist** del Firewall perimetral.