**Procedimiento para Escaneo de Puertos Desprotegidos en AWS**

**1. Identificación del Caso**

La necesidad de monitorear y escanear puertos desprotegidos en la infraestructura de AWS surge para detectar y notificar la ejecución de herramientas de escaneo bajo la señalización específica de **Recon:EC2/PortProbeUnprotectedPort**.

**2. Inputs de Detección**

* **Ofensa generada en Qradar**
* **Tipo de Amenaza:** Reconocimiento (R\_Reconocimiento)
* **Tipo de Incidente:** TEC-003 - Fingerprinting de Sistemas a través de Escaneo
* **Detección Específica:** Recon:EC2/PortProbeUnprotectedPort

**3. Análisis del Evento**

**a. Identificación Inicial**

* Identificar el recurso desde donde se hizo el escaneo.
* Identificar las IPs (tanto de destino como de origen).
* Identificar los puertos utilizados.
* Identificar posibles conexiones contra IPs sospechosas externas dentro de un periodo cercano a la alerta (geolocalización, categoría implicada, etc).

**b. Verificación de Actividad**

* Verificar si la actividad fue realizada por un usuario de la empresa y si se ejecutó desde un equipo asignado en cumplimiento con las políticas.
* Determinar si la IP origen/host origen ha realizado conexiones previas en un periodo corto. Analizar el comportamiento de esa IP para determinar si es una actividad habitual.
* Analizar la actividad de las IPs/hosts de destino afectadas para identificar comportamientos anómalos adicionales.
* Determinar el alcance del escaneo (cantidad de equipos afectados, criticidad de los equipos, si son SOX, etc) para evaluar la criticidad e impacto.
* Identificar si el escaneo continúa en curso.
* Verificar si la ofensa está asociada a una actividad/tarea programada previamente notificada al CRMC (por ejemplo, Pentest).

**4. Alternativas de Acción**

**a. Ejecución por Usuario "Pentester"**

* Validar la solicitud REQ que respalde la actividad.

**b. Ejecución por Usuario "No Pentester"**

* Solicitar la eliminación de la herramienta y validar si cuenta con REQ.

**5. Validación con el Usuario**

* Validar con el usuario y/o responsable de la cuenta la acción realizada, colocando en copia al Gerente de Monitoreo, Control Preventivo y Respuesta.

**6. Medidas de Contención y Erradicación**

* Si el usuario o responsable desconoce el uso de la herramienta y se sospecha de una actividad malintencionada:
  + Aplicar el Proceso de Cuenta Comprometida.
  + Bloquear la IP sospechosa mediante el automatismo en Resilient (acción “Bloquear host”).