Diseñar un Protocolo de Priorización de Alertas

Investiga cómo diferentes organizaciones priorizan alertas en sus SIEM.

- La gravedad del evento

Descripción: Se refiere al nivel de severidad asociado a una alerta específica. Las alertas pueden clasificarse en niveles como bajo, medio o alto, dependiendo de la amenaza que representan.

Ejemplo: Un intento fallido de inicio de sesión puede considerarse de baja gravedad, mientras que la detección de malware activo sería de alta gravedad.

- El potencial impacto en la seguridad de la red y los sistemas

Descripción: Evalúa las posibles consecuencias que una alerta podría tener sobre la integridad, confidencialidad y disponibilidad de los sistemas y datos de la organización.

Ejemplo: Una alerta que indique un posible acceso no autorizado a datos sensibles tendría un alto impacto potencial en la seguridad.

- La criticidad de los activos afectados

Descripción: Considera la importancia de los sistemas o datos involucrados en la alerta. Los activos críticos son aquellos cuya alteración o pérdida podría afectar significativamente las operaciones de la organización.

Ejemplo: Una alerta relacionada con un servidor que alberga información financiera esencial sería priorizada más alto que una que afecte a un sistema menos crítico.

- La relevancia del evento en relación con amenazas conocidas

Descripción: Determina si la alerta está asociada con patrones de ataque previamente identificados o amenazas reconocidas en el panorama de seguridad actual.

Ejemplo: Si una alerta coincide con indicadores de compromiso de una campaña de ataque conocida, se le asignará una prioridad más alta.

- El historial de actividades del usuario o entidad involucrada.

Descripción: Analiza el comportamiento previo del usuario o sistema implicado en la alerta para identificar anomalías o patrones sospechosos.

Ejemplo: Si un usuario que normalmente accede desde una ubicación específica intenta conectarse desde una ubicación inusual, podría ser indicativo de una posible amenaza.

Diseña un flujo de trabajo que detalle cómo clasificar y priorizar alertas, incluyendo roles y responsabilidades.