Resumen Ejecutivo Operacional – RBVM basado en EPSS

Este documento describe un modelo práctico de Gestión de Vulnerabilidades Basada en Riesgo (Risk-Based Vulnerability Management, RBVM) diseñado para organizaciones medianas con un número elevado de activos y equipos de seguridad reducidos. El enfoque prioriza la reducción de riesgo real utilizando criterios defendibles y alineados con estándares reconocidos.

Objetivo del Framework

Optimizar el esfuerzo de remediación enfocándolo en las vulnerabilidades que presentan mayor probabilidad de explotación y mayor impacto organizacional, evitando la priorización basada exclusivamente en severidad técnica (CVSS).

Principios Clave

1. El riesgo está determinado por probabilidad de explotación y impacto, no por el número de vulnerabilidades.
2. Una sola vulnerabilidad explotable es suficiente para comprometer un activo.
3. La priorización debe ser operable, automatizable y sostenible con recursos humanos limitados.

Componentes del Modelo de Riesgo

1. **EPSS:** Probabilidad empírica de explotación de una vulnerabilidad específica (CVE).
2. **Exposición:** Nivel de accesibilidad del activo (Internet, DMZ, red interna, segmentado).
3. **Criticidad del activo:** Impacto del compromiso del activo en la organización (Alta, Media, Baja).

Modelo de Cálculo

Cada vulnerabilidad se evalúa de forma individual utilizando la siguiente expresión:

Riesgo_CVE = EPSS × Exposición × Criticidad del activo

En activos con múltiples vulnerabilidades, el riesgo del activo se determina por la vulnerabilidad con mayor valor de riesgo (escenario de compromiso más probable). No se agregan ni promedian valores EPSS.

Criterios de Priorización Operacional

1. Riesgo Alto: remediación inmediata.
2. Riesgo Medio: planificar corrección o mitigar mediante controles compensatorios.
3. Riesgo Bajo: aceptar riesgo o mantener en backlog.

Beneficios Operativos

1. Reducción significativa del ruido generado por CVSS alto sin explotación real.
2. Priorización efectiva en entornos con gran volumen de IoT.
3. Alineación con NIST, ISO/IEC 27005, CIS Controls y CISA.
4. Modelo defendible ante auditorías y fácil de comunicar a dirección.

Este enfoque permite a equipos pequeños maximizar la reducción de riesgo real, enfocando los esfuerzos en lo que es más probable que sea explotado y cause impacto, en lugar de intentar corregir todas las vulnerabilidades con la misma prioridad.