SCM, Security Configuration Management, gestión segura de contenidos

Security Configuration Management (SCM). Vamos a seguir abarcando el campo de la seguridad informática, completando el cuadro general para tener las cosas más claras y tomar mejores decisiones. El tema a desarrollar es la gestión segura de contenidos.

Introducción

La configuración de un sistema de información y sus componentes tiene un impacto directo en la postura de seguridad del sistema. La forma en que se establecen y mantienen esas configuraciones requiere un enfoque disciplinado para proporcionar la seguridad adecuada. Los cambios en la configuración de un sistema de información a menudo son necesarios para mantenerse al día con las funciones y servicios comerciales cambiantes y las necesidades de seguridad de la información.

Atrás quedaron los días en que los equipos de seguridad podían concentrar todos sus esfuerzos en mantener a los atacantes fuera de la red. Ya no hay ni adentro ni afuera. La red moderna es porosa; permite que un mayor número y tipos de dispositivos se conecten a él desde todo el mundo.

¿Qué es es?

SCM es un control de seguridad crítico que permite a los equipos de seguridad monitorear el estado deseado de los

activos de la organización. Este estado suele estar en desacuerdo con las configuraciones predeterminadas disponibles para terminales POS, computadoras portátiles, tabletas, aplicaciones y otros dispositivos de red. De hecho, esas configuraciones tienden a favorecer la facilidad de instalación en lugar de la seguridad.

Implicaciones y características

SCM es una práctica de seguridad que combina elementos de evaluación de vulnerabilidades, corrección automatizada y evaluación de la configuración.

Reduce los riesgos de seguridad al garantizar que los sistemas estén configurados correctamente (reforzados) para cumplir con los estándares de cumplimiento y seguridad internos y / o reglamentarios.

El Instituto Nacional de Estándares y Tecnología (NIST) define la gestión de la configuración de seguridad como «La gestión y el control de las configuraciones de un sistema de información con el objetivo de habilitar la seguridad y gestionar el riesgo».

Los atacantes buscan sistemas que tengan configuraciones predeterminadas que sean inmediatamente vulnerables. Una vez que un atacante explota un sistema, comienza a realizar cambios. Estas dos razones explican por qué las herramientas de gestión de la configuración de seguridad son tan importantes. S

CM no solo puede identificar configuraciones incorrectas que hacen que sus sistemas sean vulnerables, sino que también puede identificar cambios «inusuales» en archivos críticos o claves de registro.

Con una nueva amenaza de día cero revelada casi a diario, las defensas basadas en firmas no son suficientes para detectar amenazas avanzadas. Para detectar una infracción de forma temprana, las organizaciones deben comprender no solo qué está cambiando en los dispositivos críticos, sino también ser capaces de identificar los cambios «malos».

Las herramientas SCM permiten a las organizaciones comprender exactamente qué está cambiando en sus activos clave. Al establecer una configuración estándar de oro para sus sistemas y monitorear continuamente los indicadores de compromiso, las organizaciones pueden identificar rápidamente una infracción. La detección temprana de una infracción ayudará a mitigar el daño de un ataque. El uso de SCM para hacer cumplir un estándar de fortalecimiento corporativo como CIS, NIST e ISO 27001 o un estándar de cumplimiento como PCI , SOX o HIPAA proporciona la capacidad de fortalecer continuamente los sistemas para reducir la superficie de ataque. Los sistemas reforzados brindan menos oportunidades para que los malos lancen un ataque exitoso.

Leer también: UTM, Unified Threat Management, gestión unificada de amenazas ; ¿Qué es un sistema de prevención de intrusiones, IPS? ; ¿Qué es un sistema de detección de intrusiones, IDS?