Enfoque Pragmático para la Seguridad de Datos

Cesar Mahecha
STEALTHbits Technologies

Identify Threats. Secure Data. Reduce Risk.

Acerca STEALTHbits

STEALTHbits es una empresa de software de seguridad de datos.

Aseguramos la información de una organización al defenderla frente al abuso de credenciales y controlando el acceso a los datos.

El estado de Detección de Amenazas Avanzadas Hoy

Su riesgo no esta donde usted cree que esta…

Cada Brecha Mayor Involucra el Abuso de Credenciales

$400M – El estimado de perdida financiera de 700 millones de archivos comprometidos.
Verizon 2015 Data Breach Investigations Report

El promedio en numero de días que se necesita para detectar una brecha es de 200 a 230.
"Sony Hacking Fallout Puts All Companies on Alert", Associated Press, Dec 18, 2014

55% de las brechas involucran empleados maliciosos internos abusando su acceso de forma maliciosa.
Verizon 2015 Data Breach Investigations Report

57% de las brechas involucran el robo de datos no estructurados.
"Survey on the Governance of Unstructured Data", Ponemon Institute

Acceso Es La Clave De Seguridad de la Data

La clave para asegurar datos no estructurados es entender y controlar quien tiene acceso a esta.

- Directorio Activo (AD) es el eje que controla el acceso a virtualmente cada Sistema, aplicación y recurso de datos en la organización.
- 95% de todas las organizaciones utilizan AD, y la mayoría de estas admiten que AD es un enredo, lo cual hace imposible asegurar el acceso.

Mírelo como esto…

- Cerrar sus puertas
- Instalar cámaras
- Poner sensores en sus Ventanas
- Saber donde sus pertenencias de ‘valor’ están

Mírelo como esto…

- Cierre el Acceso Abierto
- Monitoree actividad
- Detecte actividad de autenticación anormal
- Localice sus datos sensibles

El Enfoque Pragmático para la Detección de Amenazas Avanzadas y Seguridad de Datos

4 Mejores Practicas

Mejor Practica #1

Cierre el Acceso Abierto

Cierre el Acceso Abierto

- **Paso 1** – Identifique donde el Acceso Abierto Existe
- **Paso 2** – Evalúe Quien Necesita Acceso
- **Paso 3** – Cree Grupos de Lectura y Escritura
- **Paso 4** – Remueva el Acceso Abierto
- **Paso 5** – Designe Propietarios del Negocio

Mejor Practica #2

Monitoree Actividad

Monitoree Actividad

- **Paso 1** – Monitoree objetos críticos de Active Directory
- **Paso 2** – Monitoree cuentas privilegiadas de AD
- **Paso 3** – Monitoree todos los Objetos de Group Policy
- **Paso 4** – Monitoree las rutas conocidas de datos sensibles

Mejor Practica #3

Detecte Actividad Anormal de Autenticación

Detecte Actividad Anormal de Autenticación

1. X logins fallidos contra cualquier host único en Y minutos
2. Autenticaciones exitosas o fallidas de una cuenta dada a través de X numero de recursos en Y minutos
3. X numero de intentos de logins fallidos de una cuanta de usuario individual en Y minutos
4. Autenticación exitosa después de repetidos fallidos
5. X numero de logins desde múltiples sistemas dentro de Y minutos

Mejor Practica #4

Localice Sus Datos Críticos

Localice Sus Datos Críticos

- **Paso 1** – Determine el criterio
- **Paso 2** – Identifique todos los sistemas dentro del alcance
- **Paso 3** – Escanee por datos sensibles SDD
- **Paso 4** – Remedie
- **Paso 5** – Manténgase haciéndolo

Preguntas?

Gracias por asistir!

STEALTHbits

TECHNOLOGIES

Agenda

- El estado de Detección de Amenazas Avanzadas Hoy
- El Enfoque Pragmático - 4 Mejores Practicas
- Próximos Pasos

Próximos Pasos

- Asista a una Demostración del Producto
  - www.stealthbits.com/events
- Solicite una Prueba
  - www.stealthbits.com/trial
- Conozca Mas
  - www.stealthbits.com
- Háganos Preguntas
  - www.stealthbits.com/company/contact-us

Identify threats. Secure data. Reduce risk.

STEALTHbits TECHNOLOGIES