DETECCIÓN DE AMENAZAS AVANZADAS

Prevenga, detecte y **actúe** oportunamente ante las ciberamenazas provenientes de usuarios y dispositivos teniendo visibilidad de comportamientos anómalos.

BENEFICIOS

Aumente la visibilidad de usuarios y **entidades** que comprometan la seguridad de la organización mediante herramientas de analítica avanzada.

Detecte desviaciones en el comportamiento de los usuarios y de los dispositivos en la red, y que las plataformas de seguridad tradicional no lo pueden llevar a cabo.

Tome decisiones oportunas orientadas a la contención de ataques o a la prevención de brechas de seguridad relacionadas con los usuarios y dispositivos conectados a la red.

Cuente con una investigación profunda de las **brechas de seguridad** por parte de expertos en Ciberseguridad de Scitum.

Reforzar el nivel de seguridad de su organización y obtenga asesoría especializada

DS / Detección_de_Amenazas / MAR20 / V1

¿CÓMO FUNCIONA?

Nuestros Ciberanalistas monitorean el comportamiento de los usuarios y le notifican ante un posible incidente o brecha de seguridad, analizan la información y envían recomendaciones basadas en las mejores prácticas de seguridad.

Más información en telmex.com/ti, consulte a su **Ejecutivo de Cuenta** o llame al **800 123 1212.**

Síganos en:

Scitum MR | TELMEX® está contigo

MODALIDADES

Servicio Básico

Componente Tecnológico

- Módulo de ingesta y retención de datos
- Módulo de analítica avanzada de comportamiento de usuarios y entidades

Actividades

- Perfilamiento de Usuarios
- Administración de logs
- Almacenamiento de actividad
- Aprendizaje de comportamiento
- Detección de comportamiento anómalo
- Calificación de nivel de riesgo
- Alertamiento

Servicio Avanzado

Componente Tecnológico

- Módulo de ingesta y retención de datos
- Módulo de analítica avanzada de comportamiento de usuarios y entidades
- Módulo de Respuesta a Incidentes

Actividades

- Correlación de eventos de distintas plataformas de Inteligencia
- Investigación de Indicadores de Compromiso
- Análisis Avanzado de eventos
- Notificación de Amenazas Criticas

CASOS DE USO

Monitoreo de cuentas Privilegiadas.

- Abuso en uso de cuentas de servicio / privilegiadas.
- Creación o elevación de cuentas y privilegios no autorizados.
- Cuentas no administradoras haciendo tareas de administrador.
- Consultas a bases de datos sensibles sin autorización.

Inteligencia en los accesos

- Privilegios de acceso anómalo comparado con sus semejantes.
- Cuentas activas de usuarios que ya no pertenecen a la organización.
- Cuentas de dominio que no has sido usadas en más de 90 días.
- Cuentas huérfanas.
- Certificados de acceso.

Inteligencia en aplicaciones

- Acceso sospechoso a información confidencial.
- Mal uso de cuentas privilegiadas.
- Actividad fraudulenta.
- Robo de identidad.

Filtración de datos

- Usuarios fuera de la oficina potencialmente riesgosos.
- Envió de mail a cuentas personales, competidores o dominios no empresariales.
- Envió anómalo de gran cantidad de datos.
- Acceso sospechoso a datos confidenciales.
- Archivos compartidos en almacenamientos personales.

Ciberseguridad

- Descargas de malware de sitios infectados.
- Movimiento lateral.
- Procesos sospechosos disparados en equipos de sistemas.
- Gran cantidad de datos transferidos desde equipos de sistemas.
- Equipos infectados y con cierto nivel de compromiso.

Actividad en la red

- Patrón de tráfico robótico a sitios web maliciosos / no categorizados / sospechosos.
- Conexiones a dominios generados digitalmente.
- Solicitudes DNS inusuales.
- Duración inusual de sesiones de red.
- Conexiones a IP / Dominios en black list.
- Actividad de escaneo de puerto / Ataque DDoS.
- Redirección de peticiones de sesión anormal.

¿POR QUÉ TELMEX-SCITUM?

- Más de 22 años de experiencia
- Personal especializado. Más de 650 colaboradores que acreditan más de 1,500 certificaciones en mejores prácticas y tecnologías de fabricantes líderes en ciberseguridad.
- Operación de clase mundial, alineada a estándares internacionales metodologías propias, marcos de referencia y mejores prácticas.
- Mayor visibilidad de amenazas cibernéticas en México. Nuestro centro de ciberseguridad forma parte de una red internacional de colaboración en inteligencia de amenazas integrada por equipos de respuesta nacionales e internacionales, organizaciones de cumplimiento de la ley y centros de inteligencia de amenazas de fabricantes líderes.

Más información en telmex.com/ti, consulte a su **Ejecutivo de Cuenta** o llame al **800 123 1212.**

Síganos en:

Scitum MR | TELMEX® está contigo