DevelSecurity
PROFESSIONAL SERVICES

Portafolio de SOLUCIONES Y MONITOREO

As-a-service SOLUTIONS

- IPS
- DLP
- SIEM
- Antivirus
- Cloud security
- Vulnerability Mgmt.

Somos el socio de negocios que usted necesita

- Administramos e impedimos amenazas, ataques en aplicaciones y servicios de su empresa.
- Proveemos la experiencia necesaria en seguridad informática para mantenerse al día con las demandas del negocio.
- Lo apoyamos con la carga operacional del día a día como los son las fallas, incidentes y eventos de ciberseguridad.
- Proveemos las herramientas correctas y lo último en tecnología para la resolución de problemas y eventos de seguridad.
- Contamos con ingenieros experimentados y altamente capacitados.

Monitoreo de eventos de ciberseguridad

(Security Operation Center / Dsoc-CERT)

El servicio consiste en llevar a cabo un monitoreo de distintas plataformas de seguridad de su organización, las cuales van a ser las fuentes de información para el servicio y a partir de estas se generan los casos de uso de interés para su negocio.

Beneficios

- Alertas tempranas en incidentes de seguridad.
- Desarrollar una cultura de proactividad en vez de reactividad.
- Reportes alineados al negocio y a procesos críticos.
- Cumplimiento con estándares internacionales y regulaciones.
- Mejora de la postura en ciberseguridad.

Actividades dentro del monitoreo

- Monitoreo en eventos de seguridad **24x7x365.**
- Gestión de incidentes y eventos de seguridad.
- Implementación y adecuación de fuentes de información.
- Generación de conectores para fuentes de información personalizadas.
- Reportes para cumplimiento regulatorio **(PCIDSS, ISO27001, HIPAA, SOX).**
- Dashboards en tiempo real de cada fuente de información monitoreada.
- Asesoría y seguimiento de incidentes de seguridad por personal experto certificado.

Soluciones tecnológicas en ciberseguridad

ArcSight, digicert, TITUS, tenable, CLOUDFLARE, IMPERVA INCAPSULA, paloalto NETWORKS, Check Point SOFTWARE TECHNOLOGIES LTD., ANOMALI, Barracuda, ManageEngine Powering IT ahead, McAfee, CYBERARK, MICRO FOCUS, RAPID7

El servicio de correlación de eventos de seguridad está diseñado para obtener, tanto los eventos como las alertas de seguridad desde múltiples dispositivos con el fin de correlacionar los mismos, mediante un motor que permite identificar posibles amenazas o problemas de seguridad que se puedan estar presentando en los activos que se encuentran siendo monitoreados; esto le permite a la organización identificar riesgos de seguridad en tiempo real.

Este servicio es personalizado por organización sobre el número de fuentes de información que esta desea monitorear. Dentro de algunas de las fuentes de información más solicitadas, tenemos:

Diferentes fuentes de información

- Directorio Activo - Active Directory
- Plataforma de Antivirus
- Equipos Firewall e IPS
- Equipos de Red Core Network
- Equipos Mainframe AS400
- Bases de datos
- Aplicaciones Web
- Correo electrónico

CERT IS A MARK OWNED BY CARNEGIE MELLON UNIVERSITY • CERT AUTHORIZED TO USE CERT