NOVENTIQ
Global expertise, local outcomes

Cerberus

Dicembre 2022

CERBERUS by Noventiq

EN UN AMBIENTE CAMBIANTE DONDE LAS CIBERAMENAZAS EVOLUCIONAN TODOS LOS DÍAS.

CERBERUS NACIÓ PARA RETAR UNA CATEGORÍA QUE TIENDE A OLVIDARSE DE LO IMPORTANTE DEL ACOMPAÑAMIENTO AL CLIENTE.

CERBERUS

Cerberus, detecta, previene, acompaña.

Cerberus es un servicio de seguridad enfocado en el acompañamiento continuo a nuestros clientes, ayudándolos a identificar la estrategia de seguridad más conveniente para su compañía.

CERBERUS

Implementación Básica de Sentinel (SIEM)

Implementación Básica de Sentinel (SIEM)

Mediante el servicio de implementación Análisis de Seguridad SIEM de Noventiq podrá Compilar operaciones de seguridad de última generación con la nube y la IA de Microsoft Azure.

Vea y detenga las amenazas antes de que causen daños, con SIEM reinventado para un mundo moderno. Microsoft Sentinel es su visión general de toda la empresa. Ponga en funcionamiento la inteligencia en la nube y a gran escala de décadas de experiencia en seguridad de Microsoft. Haga que la detección de amenazas y la respuesta sean más inteligentes y rápidas con inteligencia artificial (IA). Elimine la configuración y el mantenimiento de la infraestructura de seguridad y escale elásticamente para satisfacer sus necesidades de seguridad a la vez que reduce los costos hasta un 48 % en comparación con los SIEM tradicionales.

CERBERUS

Servicios Adicionales

Ethical Hacking

Las pruebas de vulnerabilidad sobre este escenario buscan encontrar vulnerabilidades no catalogadas (0 day) sobre aplicaciones propietarias o fallos de seguridad en el despliegue, configuración o diseño de aplicaciones comerciales o libres.

- Identificar y enumerar los servicios y aplicaciones que soportan o están involucrado en las aplicaciones.
- Realizar un proceso de decodificación e ingeniería inversa sobre los protocolos que usen los servicios propietarios con el fin de analizar el protocolo en busca de malas prácticas de desarrollo.
- Hacer uso de herramientas automatizadas que permitan la realización de diferentes tipos de pruebas sobre el servicio.
- Identificar malas prácticas en cuanto a la configuración y despliegue del servicio.
- Estas pruebas están conformadas por un conjunto de ataques simulados que permitan identificar cualquier tipo de falla o vulnerabilidad en cuanto a la configuración y el despliegue de las aplicaciones web (Fuerza bruta, uso de servicios sin autenticación, descubrimiento de parámetros y servicios, permisos de archivos, canales de comunicación, etc).
- Verificar los mecanismos de seguridad horizontales y verticales (suplantación de identidad y elevación de privilegios)
- Clasificar los riesgos según el impacto de las vulnerabilidades o fallas sobre los parámetros del CVE.

Análisis de Vulnerabilidades

Mediante un análisis de riesgos, se determina el estado actual de seguridad de la información y un roadmap para la implementación de controles que apoyen en la gestión de seguridad de la información de la compañía.

- Identificar y enumerar los servicios y aplicaciones que soportan o están involucrado en las aplicaciones.
- Realizar un proceso de decodificación e ingeniería inversa sobre los protocolos que usen los servicios propietarios con el fin de analizar el protocolo en busca de malas prácticas de desarrollo.
- Hacer uso de herramientas automatizadas que permitan la realización de diferentes tipos de pruebas sobre el servicio.
- Identificar malas prácticas en cuanto a la configuración y despliegue del servicio.
- Clasificar los riesgos según el impacto de las vulnerabilidades o fallas sobre los parámetros del CVE.

Hardening de Infraestructura

Por medio de la definición de controles y configuraciones específicas, tomando las mejores prácticas del mercado y los diferentes estándares, definiremos listas de controles específicas para los diferentes sistemas de información de la organización.

- Diseño de plantillas de aseguramiento para diferentes sistemas operativos, incluyendo:
- Sistema operativo base Windows.
- Sistema operativo base Linux.
- Bases de datos convencionales.
- Servidores de aplicaciones.
- Sistemas de administración y virtualización.
- Servicios Cloud.
- Tiempo de ejecución: 1.5 días por plantilla.
- En caso de ser más de 40 plantillas, el tiempo podría disminuir considerablemente

Servicio Administrado de Seguridad (MSSP Managed Security Service Provider)

A través de un servicio administrado de seguridad de la información y ciberseguridad, basado en un plan de tratamiento que evalúa periódicamente el desempeño de los procesos que se desean proteger:

Antes de iniciar el servicio se crea un análisis de riesgos de la mano del dueño del proceso, en este se valoran:

- Los riesgos mediante la probabilidad y el impacto de una amenaza sobre las vulnerabilidades del proceso.
- Se implementan los controles pactados y mensualmente se acompaña al dueño del proceso mediante informes que deben retroalimentar dicho proceso, para la mejora continua de la seguridad de la información y de la ciberseguridad.
- Implementación de los controles tecnológicos que disminuyen las amenazas o las vulnerabilidades que originan el riesgo de seguridad de la información y ciberseguridad, tales como:
    - SIEM: Security Information and Event Management.
    - EDR: Endpoint Detection & Response.

Servicios de Seguridad Microsoft 365

Evaluación general del estado del tenant, obteniendo como resultado recomendaciones asociadas a políticas y configuraciones en funcionalidades como:

- **Clasificación de información confidencial**
- **DLP**
- **Filtrado de Conexión**
- **Filtro Antimalware**
- **Filtrado de Correo No Deseado**
- **Etiquetas de Confidencialidad**
- **Servicios de Auditoria**

- Phase I Auditoria **– 2 políticas por funcionalidad.**
  - Alert Policies
  - Audit Logs
  - Data Loss Prevention
  - eDiscovery
  - EOP

- Phase II Threats **– 2 políticas por funcionalidad.**
  - Retention Policy
  - Antyphising
  - Safe Attachement
  - Safe Links
  - Attack Simulator
  - Automated Investigation & Response
  - Campaign View
  - Compromised user Detection
  - Threat Explorer
  - Threat Tracker

- Phase III Rules & Encryption **– 2 políticas por funcionalidad.**
  - Advance Message Encryption
  - Customer Key
  - Double Key Encryption
  - Information Governance
  - Records Management
  - Rules – Based on O365 clasification
  - Teams DLP

Entre otras.

Implementación Básica de Sentinel (SIEM)

Mediante el servicio de implementación Análisis de Seguridad SIEM de Noventiq podrá Compilar operaciones de seguridad de última generación con la nube y la IA de Microsoft Azure.

- **Fase de Inicio y planeación Fase de ajuste de ingesta de datos**
  - Ajuste de datos y eventos de Microsoft 365
  - Ajuste de datos y eventos de Plataforma de Antivirus
  - Ajuste de datos y eventos de Azure Active Directory
- **Fase de Estabilización y Cierre**
  - Monitoreo de los servicios
  - Resolución y ajustes a problemas
  - Optimización o configuración de servicios
- **Fase de cierre**
  - Documentación de servicio y configuraciones
  - Transferencia de conocimiento
  - Reunión de cierre
  - Definición de Arquitectura, configuraciones de políticas y Relevamiento físico.
- **Fase de Despliegue**
  - Creación de servicio Log Analitics workspace
  - Creación de servicio Microsoft Sentinel
  - Alistamiento de escenarios a monitorear
  - Configuración de conector de Microsoft 365
  - Configuración de conector de Plataforma Antivirus
  - Configuración de conector de Azure Active Directory
  - Validación funcionamiento conectores
  - Validación funcionamiento eventos de los conectores

En caso de necesitar más conectores podrán realizar la solicitud a el área de servicios para su estimación de tiempos y precios.

Cerberus Packages (Every customer count)

Cerberus
ACR over 1,500 USD monthly
Service:
6 hours consultation per month/ 12 months

Cerberus Lite
ACR from 500 to 1,500 USD monthly
Service:
6 hours consultation per month/ 6 months

Cerberus Baseline
ACR from 1 to 500 USD monthly
Service:
Massive webinar with all customers about security features

NOVENTIQ

Global expertise, local outcomes