NOVENTIQ
Global expertise, local outcomes

Análisis de Dominio

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

Análisis de Dominio

Análisis de Dominio

El análisis comprende una serie de pruebas unitarias en el dominio público de la compañía con el fin de buscar vulnerabilidades, bugs o malas prácticas de seguridad e informar al cliente debidamente como pueda mitigar las amenazas encontradas.

Actividades

- Identificación de Subdominios
- Identificación de Direcciones IP
- Análisis de Puertos Abiertos
- Análisis de tecnologías utilizadas y debilidades vinculadas
- Estructura de sitios web
- Análisis de Seguridad TLS/SSL
- Ficheros accesibles y metadatos
- Directorios sensibles
- Archivos de respaldo (backup)
- Archivos de configuración (.htacces,gitignore,etc)
- Direcciones de correo con contraseñas comprometidas
- Dirección manual de las principales vulnerabilidades web

Noventiq is a leading Microsoft partner

Noventiq is a leading global solutions and services provider in digital transformation (DX) and cybersecurity. We specialize in multi-cloud environments with a focus on Microsoft technology, coupled with expertise in software, proprietary services and solutions. We offer customers a comprehensive portfolio of Microsoft cloud services alongside our own services for transformation, management, security and modernization.

25+
Years of collaboration

700+
Microsoft Certified Professionals

One of 10
Microsoft globally managed partners worldwide

Best licensing practices
LSP authorization in 34 countries
CSP authorization in 50+ countries
SPLA reseller for 8 years

Microsoft Partner of the Year


Bulgaria


Cambodia x2


Malaysia


Vietnam x2

2020
2021
2022

Noventiq is a trusted partner in Microsoft Cloud Partner Program with all 6 Solution Designations, deep solutions expertise supported by Azure Expert MSP status, 12 Advanced Specialization in Azure, Security, Modern Work and Business Applications. An active member of Microsoft Intelligent Security Association.

Microsoft Solutions Partner

Microsoft Partner
Azure Expert MSP
Microsoft

Member of
Microsoft Intelligent Security Association
Microsoft

Azure

Solution Partner Designation

Infrastructure, Data & AI

Digital App and Innovation

Advanced Specializations

- Windows Server and SQL Server Migration to Microsoft Azure
- Linux and Open-Source Databases Migration to Microsoft Azure
- Microsoft Azure Virtual Desktop
- Kubernetes on Microsoft Azure

Security

Solution Partner Designation

Security

Advanced Specializations

- Cloud Security
- Identity and Access Management
- Threat Protection
- Information Protection and Governance

Modern Work & Business Applications

Solution Partner Designation

Modern Work

Business Applications

Advanced Specializations

- Adoption and Change Management
- Calling for Microsoft Teams
- Teamwork Deployment
- Microsoft Low Code Application Development

NOVENTIQ

Global expertise, local outcomes

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.

NOVENTIQ

Global expertise, local outcomes