



Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**

Protección de DNS de Gobierno

Audiencia Pública



Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**

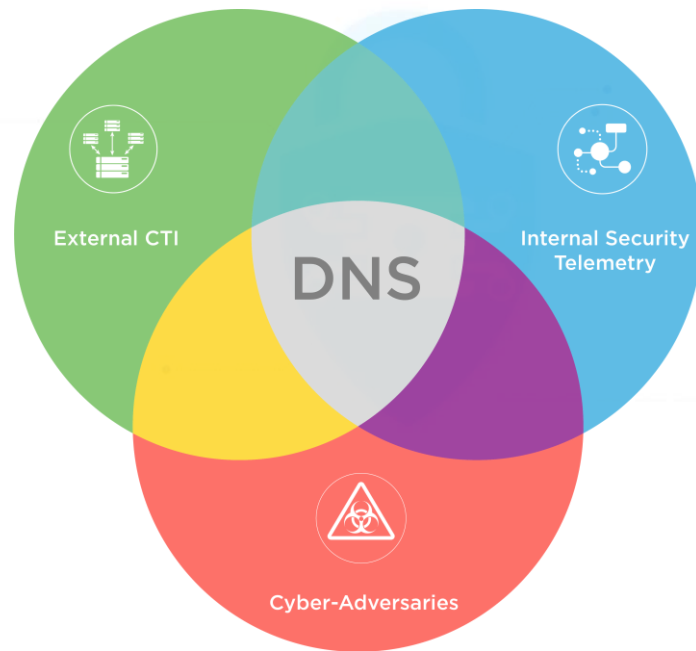




Antecedentes

Hoy en día, el DNS es una fuente de información valiosa para detectar un ciberataque. Los artefactos maliciosos utilizados en un ataque por lo general requieren conectarse a un dominio, ya sea para descargarse o para recibir las instrucciones (C&C).

Detectando una petición DNS a un dominio malicioso e interrumpiendo la respuesta, se podría interrumpiendo un ciberataque en sus etapas tempranas.

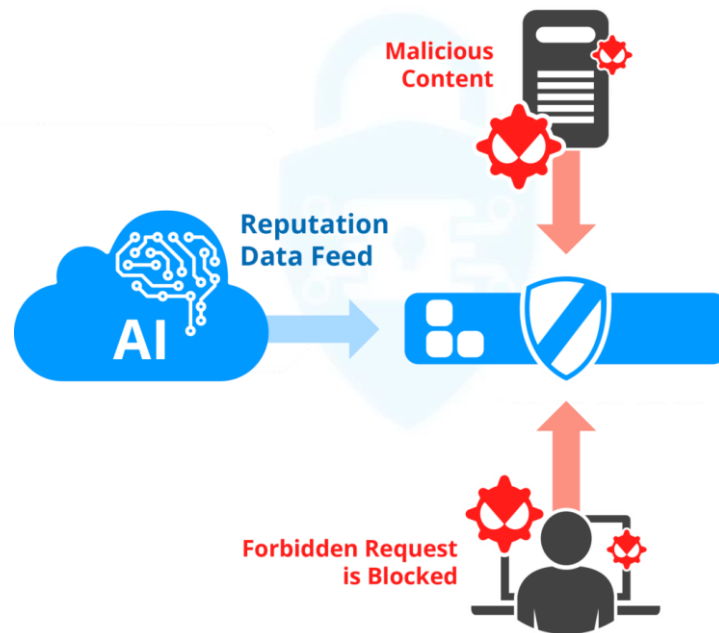




Objetivo del proyecto

Contar con una solución que permita obtener visibilidad sobre las peticiones DNS de otras organizaciones, de tal manera a poder contrastarla contra listas de dominios maliciosos conocidos y poder bloquearlas, así como también poder utilizar dichas detecciones como información accionable para la gestión de incidentes.

De esta manera, la solución permitirá al MITIC ofrecer un **servicio de DNS seguro** a las demás instituciones públicas del Estado Paraguay.





Funcionalidades mínimas esperadas:

- **Monitorear las peticiones DNS** realizadas por las instituciones y detectar aquellas peticiones sospechosas desde el punto de vista de ciberseguridad (peticiones a C&C maliciosos, principalmente)
- **Bloquear las respuestas DNS** a peticiones maliciosas. La lista o base de datos de IPs maliciosas debe poder ser alimentada de manera dinámica a partir de fuentes de información diversas customizadas, incluidas las que el CERT-PY pueda conseguir por otras vías (ej.: Talos, Shadowserver, Microsoft, Kaspersky, ESET, otros CSIRTs, etc.).
- Las **alertas de peticiones DNS** sospechosas que hayan sido detectadas y/o bloqueadas deben poder volcarse a algún sistema de correlación de eventos (SIEM o similar).



Funcionalidades mínimas esperadas (cont.):

- Debe poder identificarse **el origen de la petición** sospechosa. Como mínimo, se debe poder identificar la institución que está realizando la petición. Idealmente, quisieramos también considerar una opción en la que se pueda llegar al nivel de detalle de qué máquina interna a dicha institución está realizando la petición.
- **Registro de peticiones de DNS**, aún aquellas que no hayan sido detectadas al momento de la petición, tal que si en un futuro se encuentra un dominio sospechoso, se pueda ver en los registros, qué organizaciones y/o equipos se han conectado a el.
- Preferentemente, quisiéramos tener un **dashboard gráfico** en el que se pueda visualizar las alertas e incluso aplicar acciones que fueran necesarias.



Modelos aceptables

- Solución SaaS (software-as-a-service)
- Appliance / Hardware
- Software
- Híbrido
- Solución comercial
- Solución a medida basada en open source (“from scratch”)
- ...





Características valoradas:

- Mayor **costo-beneficio**: mayor nivel de visibilidad a menor costo (ya sea económico, de esfuerzo o ambos)
- **Sostenibilidad en el tiempo**: una solución cuyo costo de mantenimiento sea el menor posible y cuyo funcionamiento a futuro no estuviera a grandes inversiones monetarias para seguir operando.



Ejemplo: una solución que implique un costo de implementación de 100.000usd y un costo anual de mantenimiento de 5.000usd, por lo general, será preferido a una solución que implique un costo mensual de 5.000usd, ya que en apenas 2 años se estará superando a la primera opción (y ese crecimiento es lineal). Para el análisis de sostenibilidad deberá considerarse por lo menos 5 años.



Características valoradas (cont.):

- **Escalabilidad:** la propuesta debe permitir escalar de una implementación que contemple un número relativamente pequeño de instituciones o cantidad de peticiones, llegando a un volumen mayor, considerando que en un futuro el MITIC pudiera obligar a que todo el Estado utilice este servicio.

La escalación debería requerir el menor costo posible y minimizar la repetición de inversión. Las fases y sus costos deben ser incluidas en las diferentes propuestas que hubiera, de modo a poder tomar la decisión de hasta qué fase puede llegarse, de acuerdo a nuestra disponibilidad financiera.



Obs.: como sería un servicio a demanda que dependerá del interés de los demás OEE, no se puede saber con exactitud la cantidad de usuarios ni el ratio de crecimiento



Características valoradas (cont.):

- **Arquitectura flexible y multi-tenant:** podría haber instituciones que deseen que MITIC detecte qué maquina interna está haciendo la petición sospechosa, pero podría haber otras que no lo desean (les es suficiente que le indiquemos la petición y el timestamp). Podría haber instituciones que desean visualizar también ellos las peticiones DNS que realizan sus usuarios y las alertas asociadas a través de un dashboard.
- **Inversión / esfuerzo por parte de las OEE:** Son igualmente válidas las soluciones en las que la institución "cliente" debe poner **algo de su parte** (una PC en la que instalar algo virtual, una configuración, etc.), siempre y cuando la inversión y/o el esfuerzo requerido como contraparte no sea excesivo. La estimación de esa contraparte (en términos de costo monetario aproximado) debe incluirse igualmente en la propuesta (aunque no vaya a ser financiado por MITIC), para poder tomar la decisión conociendo ese dato.



Estructura de la propuesta

➤ Descripción técnica de la solución:

- Diagramas / Arquitectura
- Explicación de la solución
- Funcionalidades
- ...



Propuestas: audiencias_ciber@mitic.gov.py

Consultas: ciberseguridad@mitic.gov.py

Fecha límite: viernes 30 de julio

➤ Propuesta y/o modelo financiero

- Costo inicial de la solución (hardware/software) – *si lo hubiera*
- Mantenimiento (licenciamientos)
- Implementación, configuración, capacitación, etc.
- Opciones de crecimiento (año 1: X usuario, año 2: Y usuarios, ...)
- ...

➤ Requerimientos o supuestos para la implementación



Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**





Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**

¡MUCHAS GRACIAS!

