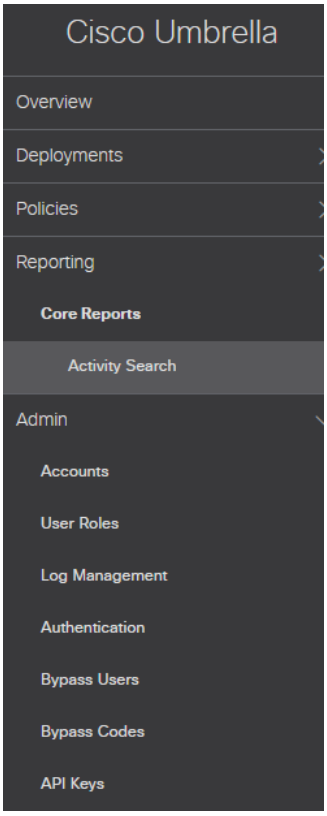
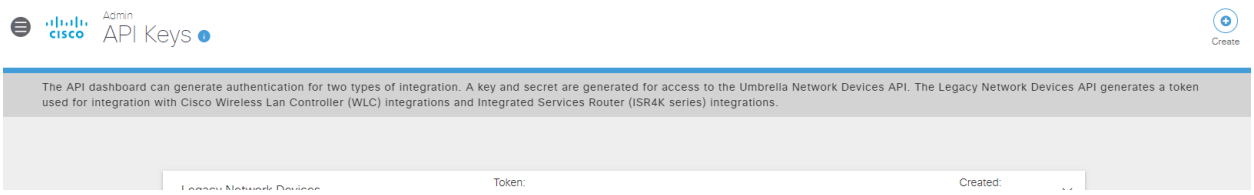
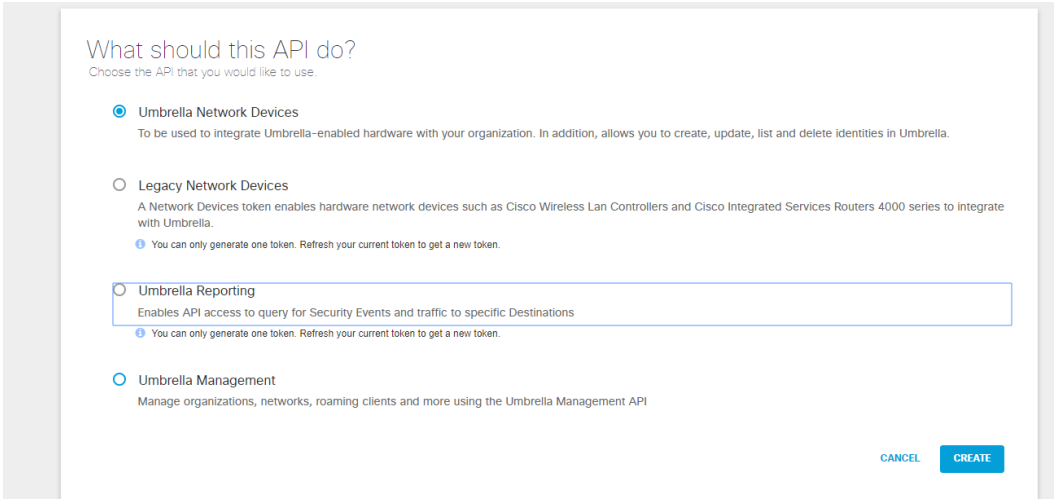
CISCO UMBRELLA INTEGRATION THREAT RESPONSE

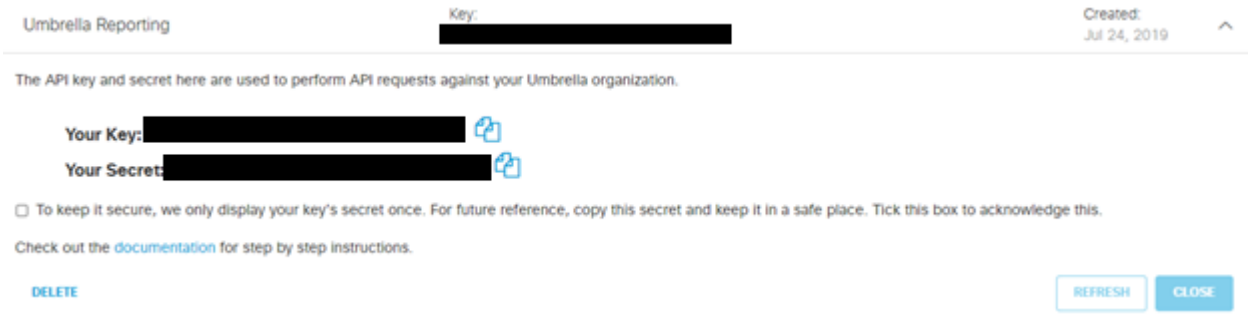
1- Inicia sesion en la consola de Umbrella , seleccionar Admin > API Keys



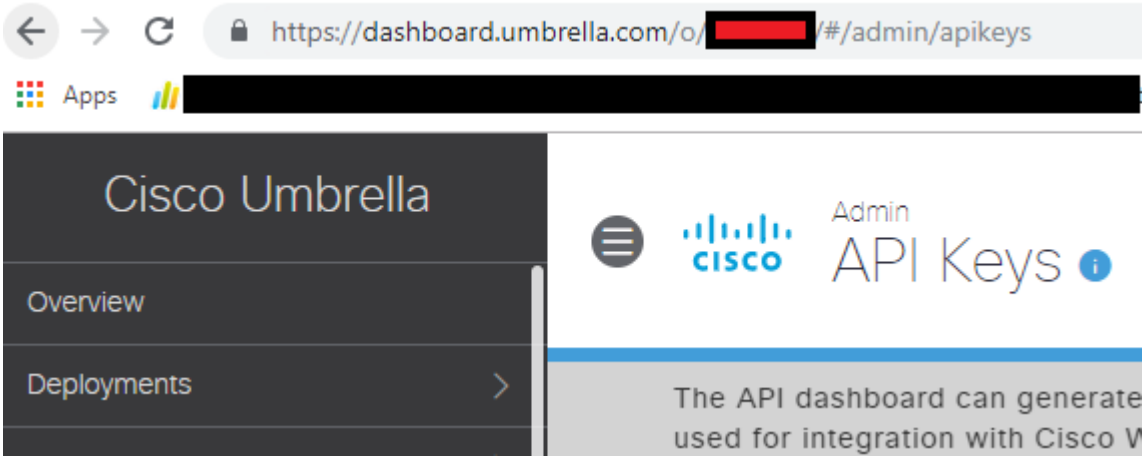
2- Hacer clic en el boton Crear , se abrira un formulario ,
   a. Seleccionar Umbrella Reporting y dar clic en Crear



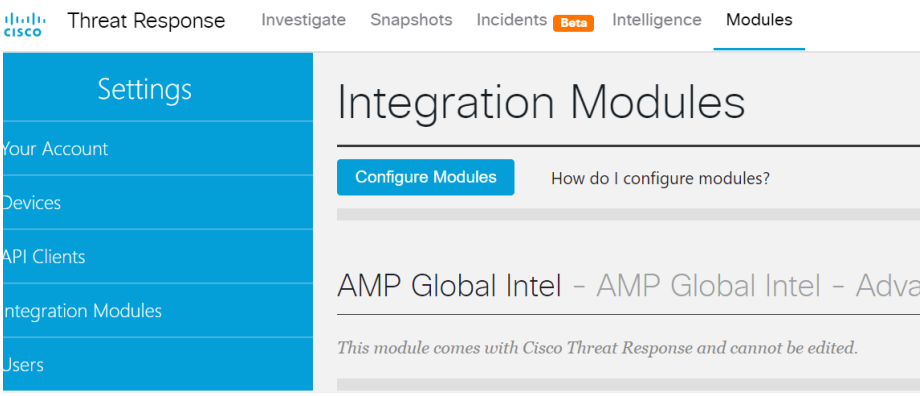


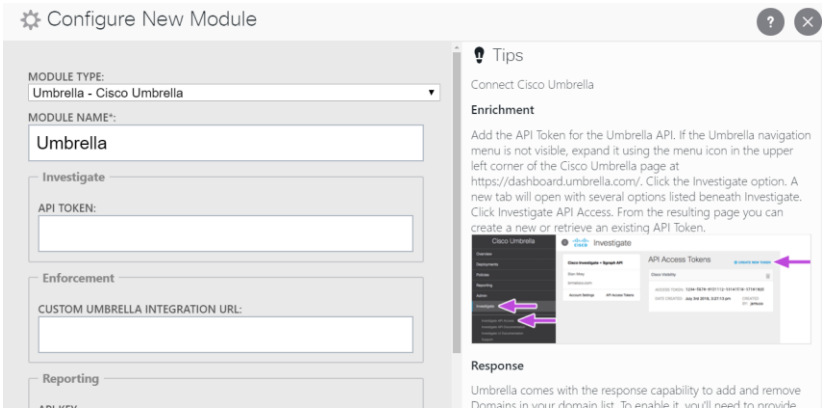


3- Copiar Key y Secret para poder agregar al modulo de Threat Response
4- Guarda tu ID de Umbrella que encontraras en la barra de URL , tu ID es el numero que se encuentra entre /o/ y /#/ en la barra de URL.

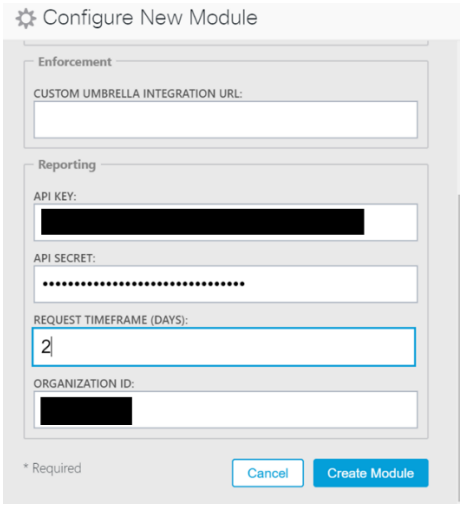


5- Inicia sesion en Cisco Threat Response > Modules > Configure Modules> Umbrella> Cisco Umbrella.



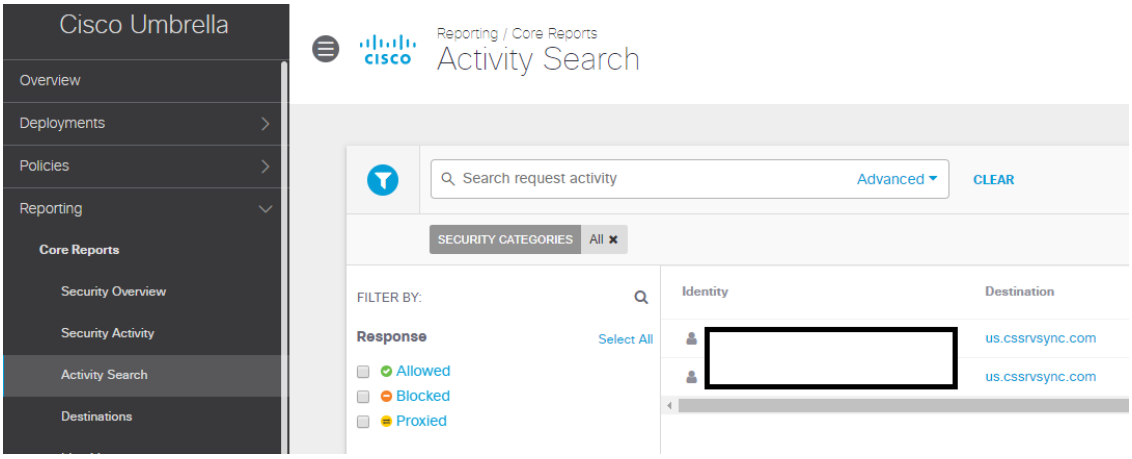


6- En la seccion de Reporting ingresas la llave , el numero secreto y tu ID guardades en los pasos anteriores.
7- El time frame es dias de los mas recientes consultas de DNS.
8- Clic en Create module.

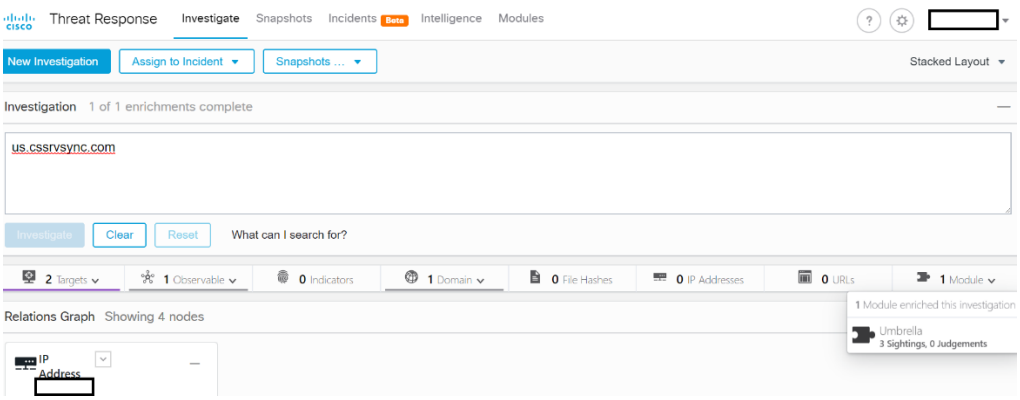


VALIDAR MODULO DE UMBRELLA EN CISCO THREAT RESPONSE

1- Incia sesion en Umbrella > Reporting > Activity Search



2- Selecciona un destino para investigacion, en este caso seleccionare us.cssrvsync.com
3- En Threat response ingreso el dominio para investigar.



Confirmaras que la Fuente de la informacion proviene de Umbrella.