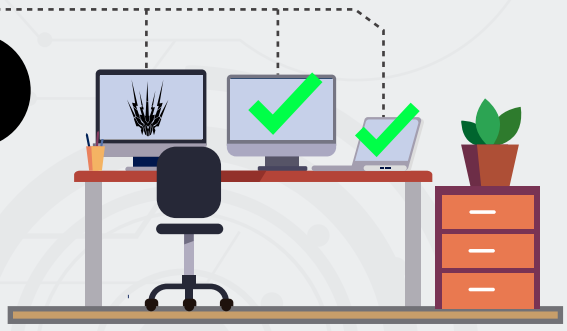
TRATAMIENTO DE EVENTOS DE SEGURIDAD

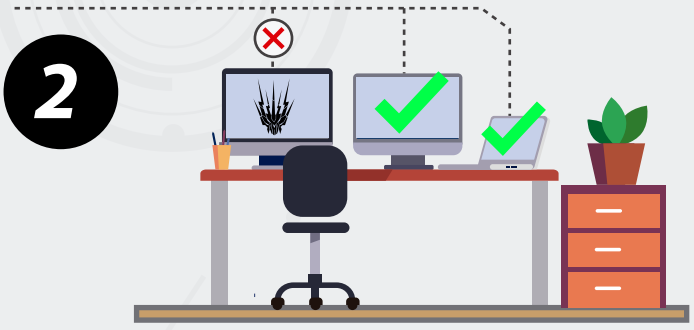
El siguiente instructivo da a conocer los pasos para el tratamiento de eventos de seguridad conocidos y desconocidos que se encuentre sobre la red.

1



Identificación del equipo o equipos afectados en la red.

2



Aislar la maquina de la red durante el proceso de tratamiento adicional.

3

Verificar la instalación y el correcto funcionamiento del agente Traps Palo Alto.

4

Verificar la instalación del certificado de Traps sobre el equipo.

5

A ***Autoruns para visualizar las aplicaciones y llaves de registro que se activan al iniciar el equipo.***

Autoruns
v13.90 (July 5, 2018)
See what programs are configured to startup automatically when your system boots and you login. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns

B ***Process Explorer se usa para evidenciar los procesos activos sobre el equipo.***

Process Explorer
v16.21 (May 16, 2017)
Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

https://docs.microsoft.com/en-us/sysinternals/downloads/procmon

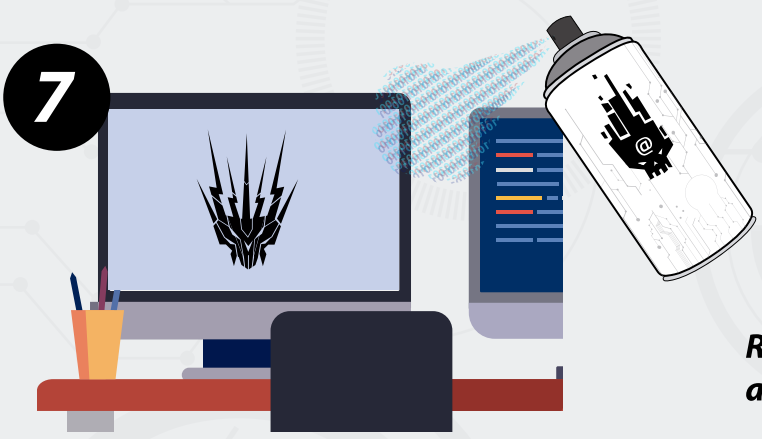
Verificación de registro y procesos del equipo con la herramienta systeminternals.

6

En caso de contar con la muestra de malware, se debe comprimir en un archivo RAR o ZIP con la contraseña "virus" sin comillas adicionalmente enviar las evidencia fotográfica, nombre de equipo e IP y enviarla al siguiente correo:

mesadeayuda@bhamesadeayuda.net.

7



Realizar la limpieza al equipo afectado.