Es importante utilizar herramientas como **Security Onion** nos permiten, a través de información del tráfico de la red, comportamiento sospechoso obtener alertas que nos permiten, i.e, **detectar** malwares conocidos y capturar dicho tráfico para posteriormente realizar un análisis con **Wireshark** sobre los incidentes. **Ninda** no es detectado como malware, es un archivo *.cmd*, mientras que **WannaCry** es detectado como malware conocido por su **sha**, que se encuentra oculto bajo el nombre *diskpart.exe*, el cual permite administrar las unidades de equipos y necesita permisos de administrador.

Tenemos buenas prácticas como concientizar a nuestros usuarios de lo riesgoso que es descargar archivos de sitios desconocidos y recomendar utilizar VirusTotal para archivos descargados, siempre y cuando no sean confidenciales. Además de configurar en sus dispositivos tecnológicos un antivirus basado en la detección continua que permita detectar comportamientos sospechosos y amenazas conocidas.