

# ¿Cómo Proteger El Entorno Digital En Tor?



La navegación por Internet no relacionada con el trabajo es inofensivo, hay algunos casos en los que podría ser participe sin saberlo de alguna actividad criminal. Y todo esto se esconde detrás de la

popular red de anonimato, Tor.

[The Onion Router](#), más conocido como «Tor», un **proyecto de código abierto**, iniciado en 2002, está diseñado para permitir a un usuario navegar por Internet de **forma anónima a través de una red** de servidores de más de 5.000 relés. No comparte su información de identificación como su dirección IP y la ubicación física con sitios web o proveedores de servicios.

Un usuario que navegue en Internet **utilizando Tor**, es bastante difícil de rastrear sus actividades, lo que garantiza su privacidad en línea. Tor ha sido un blanco favorito de las agencias de inteligencia. El FBI es capaz de rastrear el propietario de 'Freedom Hosting', el mayor proveedor de servicios para los sitios de la red cifrada Tor, la cual hospedo una gran cantidad de sitios de pornografía infantil.

Una gran cantidad de atacantes informáticos aprovechan la **red Tor para ocultar** la ubicación de los servidores de comando y control, máquinas de **infección con ransomware**, etc. Esto hace que la identificación de estos ellos y su malware mucho más difícil.



En otras palabras, un usuario que solo entre por curiosidad en al red Tor, puede ser infectado, ya sea por un malware, o por algún código que use su computadora ya sea para robar información o para usarla como un bot.

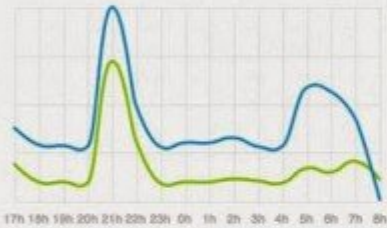
## ¿Qué Medidas Tomar?

[AlienVault Unified Security Management™ \(USM\)](#) puede ayudar a revisar los riesgos que puedes encontrar en Tor. **USM** ofrece el descubrimiento de peligros potenciales, evaluación de vulnerabilidades, detección de amenazas (IDS), el seguimiento del comportamiento y SIEM en una única consola, además de actualizaciones semanales de análisis de riesgos desarrollados por el equipo de investigación de amenazas de **AlienVault Labs**.

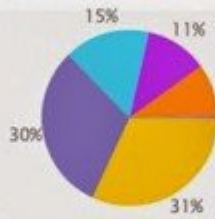
OVERVIEW

EXECUTIVE TICKETS SECURITY TAXONOMY VULNERABILITIES COMPLIANCE

LATEST SIEM VS LOGGER EVENTS



SIEM: TOP 10 EVENTS BY PRODUCT TYPE



THREAT LEVEL

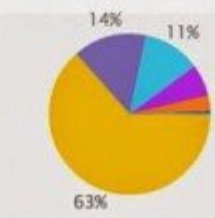


UNRESOLVED ALARMS VS OPENED TICKETS



- Authentication and DHCP
- Operating System
- Intrusion Detection
- Anomaly Detection
- Server
- Web Server
- Alarm
- Application

SIEM: TOP 10 EVENT CATEGORIES



SIEM: EVENTS BY SENSOR/DATA SOURCE

