AlienVault Open Threat Exchange

La primera comunidad de conocimiento de amenazas verdaderamente abierta del mundo que permite la defensa colaborativa con datos de amenazas utilizables proporcionados por la comunidad.

Compartir amenazas en el sector de la seguridad continúa siendo principalmente un proceso ad-hoc e informal, repleto de puntos ciegos, frustración y escollos. Nuestra visión es que las empresas y los organismos gubernamentales reúnan y compartan, lo más rápidamente posible, información relevante, oportuna y precisa sobre amenazas y ciberataques nuevos o en curso. Armados con esta información, las organizaciones de todos los tamaños pueden evitar las grandes brechas de seguridad o minimizar el daño debido a un ataque. AlienVault Open Threat Exchange (OTX) proporciona la primera comunidad de conocimiento de amenazas verdaderamente abierta que hace realidad esta visión.

AlienVault OTX ofrece acceso abierto a una comunidad global de investigadores de amenazas y profesionales de la seguridad. Proporciona datos sobre amenazas generados por la comunidad, permite la investigación colaborativa y automatiza el proceso de actualización de su infraestructura de seguridad con datos de amenazas procedentes de cualquier fuente. OTX permite que cualquiera de la comunidad de la seguridad contraste activamente, investigue y comparta los últimos datos de amenazas, tendencias y técnicas, fortaleciendo sus defensas a la vez que ayuda a otros a hacer lo mismo.

Pulsos

Los pulsos son el formato en el que la comunidad OTX comparte información sobre amenazas. Los pulsos le proporcionan un resumen de la amenaza, una visión del software amenazado y los respectivos indicadores de compromiso (IoC, Indicators of Compromise) que pueden usarse para detectar la amenaza.

Los IoC incluyen direcciones IP, nombres de dominios, funciones hash de archivos (MD5, SHA1, SHA256, PEHASH etc.), números CVE y mucho más. Los pulsos y sus IoC incluidos ayudan a dar respuesta a preguntas como:

- ¿Está mi entorno expuesto a esta amenaza?
- ¿Es esto relevante para mi organización?
- ¿Quién está detrás de esto, y cuáles son sus motivaciones?
- ¿Cuál es su diana dentro de mi organización?

Acceso abierto

La investigación en seguridad tiende a ser un proceso insular, y pocas veces los individuos o los grupos comparten datos sobre amenazas entre ellos. Esto se debe a una falta de confianza, a políticas internas, o simplemente a la incapacidad de hacer llegar la información a las masas. OTX ayuda a solucionar este problema con la capacidad de suscribirse o seguir los pulsos de más confianza de la comunidad.

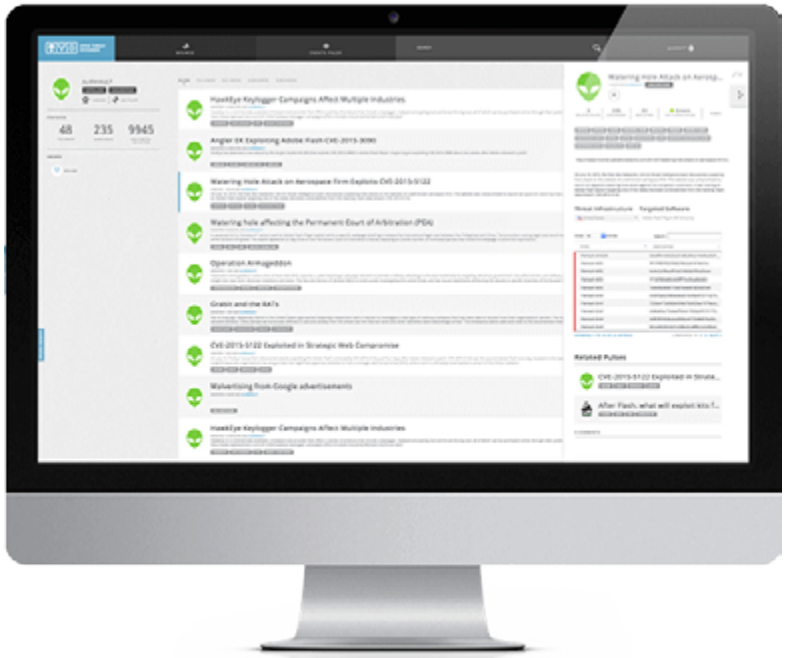
- Suscríbase a los pulsos y use la función DirectConnect para actualizar automáticamente sus productos de seguridad.
- Siga a los contribuidores de OTX y obtenga una visión desde dentro de las amenazas que han investigado recientemente.

Investigación y colaboración abierta sobre amenazas emergentes

El modelo tradicional utilizado para compartir amenazas se basa en la comunicación en un solo sentido entre investigadores/vendedores y suscriptores. No hay forma de que los suscriptores interaccionen con sus iguales o con los investigadores de amenazas para tratar de amenazas emergentes, ya que cada receptor está aislado de los demás. Por esa razón construimos OTX: para cambiar la forma en la que todos creamos, colaboramos y consumimos los datos de amenazas.

Integre IoC con USM de AlienVault y expórtelo a cualquier producto de seguridad

La mayoría de los productos o servicios para compartir datos de amenazas son caros y complejos. A menudo, los usuarios se encuentran con que compran varios servicios, ya que el abordaje tradicional aislado de los datos de amenazas limita su capacidad para exportar datos de amenazas de una herramienta a otra. OTX ofrece varios sistemas para que sus herramientas de seguridad ingieran los datos de pulsos, permitiéndole reaccionar rápidamente y más eficientemente ante las amenazas.



Integración directa con USM
Despliegue automáticamente su capacidad IDS integrada en las implementaciones de USM, así como las herramientas de seguridad de terceros, con los datos utilizables de amenazas más recientes provenientes de pulsos generados por la comunidad. La detección automática de amenazas permite el conocimiento continuo sobre amenazas emergentes sin intervención manual.

API DirectConnect de OTX
Exporte los IoC automáticamente a sus herramientas de seguridad existentes, eliminando la necesidad de añadir manualmente direcciones IP, funciones hash MD5 de archivos de malware, nombres de dominio, etc.

Exporte a herramientas de seguridad de terceros
Importe los IoC de los pulsos a herramientas de seguridad de terceros a través de varios formatos: OpenIoC (1.0 y 1.1), STIX y CSV.

CONTÁCTENOS PARA SABER MÁS

WWW.ALIENVAULT.COM