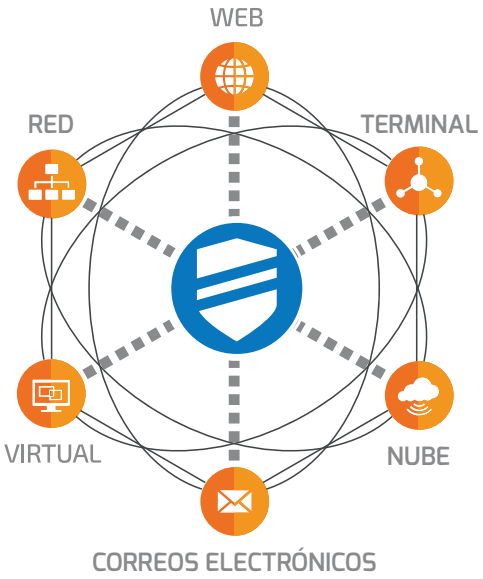
TALOS INTELLIGENCE

RED DE INTELIGENCIA SOBRE AMENAZAS DE CISCO

El mundo digital se expande a un ritmo sin precedentes y las oportunidades de ataque crecen con la misma rapidez.

El mundo digital se expande a un ritmo sin precedentes y las oportunidades de ataque crecen con la misma rapidez. Los atacantes cuentan con intentos y recursos ilimitados para lograr su objetivo, por lo que los defensores tienen que luchar y ganar cada batalla sin descanso. Para combatir estas amenazas, la seguridad necesita ir más allá del rastreo y la detección, traspasando los límites de las tecnologías de seguridad actuales para enfrentarse a los exploits del futuro.

Talos se adelanta a este escenario ofreciendo soluciones integrales de inteligencia y seguridad contra las amenazas de la industria. Talos ofrece inteligencia armada y tecnologías de detección para informar y defender a nuestros clientes con la máxima celeridad. Nuestros ingenieros y analistas trabajan en todo el mundo para mantener informados a todos los clientes de Cisco Security, así como a los miembros que integran la seguridad, sobre el escenario actual de amenazas.

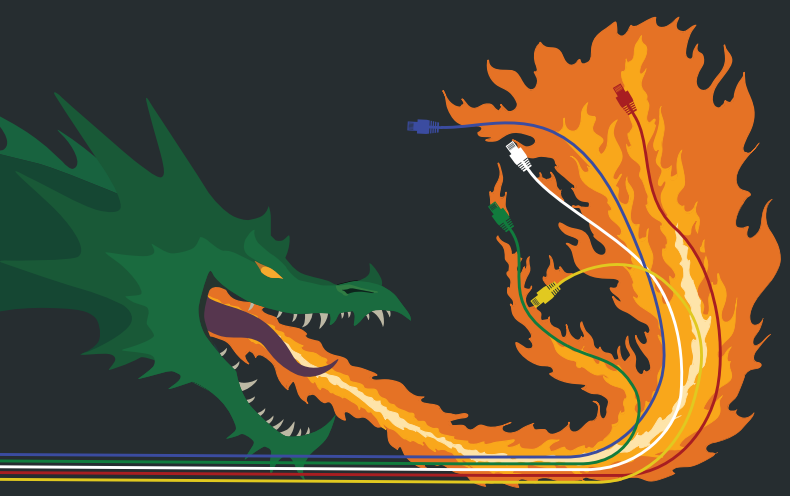


TALOS VISIBILITY

El ecosistema de Cisco Security abarca correos electrónicos, redes, la nube, la web, los terminales y todo lo que tenga que ver con esto. Cisco Talos cuenta con más visibilidad que cualquier otro proveedor de seguridad en el mundo, gracias al tamaño y amplitud de la cartera de Cisco Security y a la telemetría entrante de los clientes y productos de Cisco.

Esta visibilidad única nos ofrece un mayor contexto desde muchos puntos de datos mientras tiene lugar un incidente o campaña. Esto, junto con otros recursos como las comunidades de código abierto y el descubrimiento de vulnerabilidades internas, permite a Talos responder con mayor rapidez y crear evaluaciones más completas de las amenazas actuales.

La principal misión de Talos consiste en proporcionar tecnologías y técnicas defensivas verificables y personalizables, que ayuden a los clientes a proteger rápidamente sus activos desde la nube hasta el núcleo. Nuestro trabajo es proteger su red.



Talos a la vanguardia: Nyetya y la Conexión MeDoc

El Nyetya Ransomware atacó y comprometió sistemas en todo el mundo en junio de 2017, y Talos ofreció cobertura desde la primera línea de fuego, utilizando inteligencia verificada de Cisco Incident Response. Talos detectó el vector de amenaza inicial que apuntaba a un ataque destructivo y motivado geopolíticamente para infectar la cadena de suministro de MeDoc, un software de impuestos. A su vez, el ataque iba dirigido contra empresas que hacían negocios en y con Ucrania. Esta información ahorró a nuestros clientes y al público en general un tiempo muy valioso de búsqueda de malware inexistente o de un email fantasma. Para ver la historia completa, visite http://cs.co/nyetya.

¿QUÉ ES TALOS?

El nombre de Talos, el centro de investigación de ciberseguridad de Cisco, deriva del gigante griego cuyo único propósito era proteger a Europa de invasores y piratas. Al igual que nuestro homónimo, somos un grupo de élite de expertos en seguridad dedicados a ofrecer una protección superior a los clientes con nuestros productos y servicios.

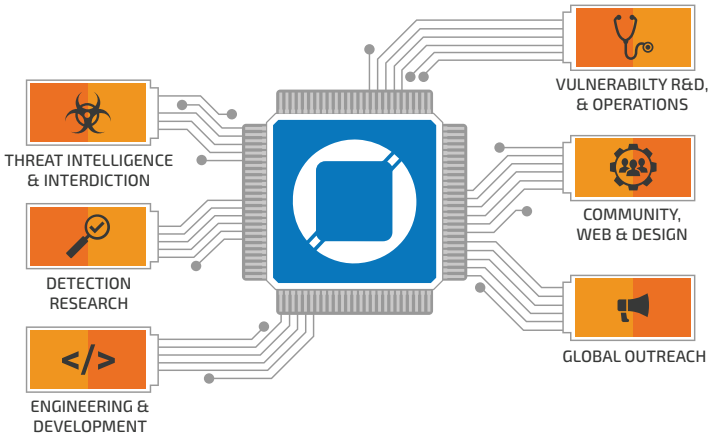
En Talos, y gracias a Cisco Incident Response (IR), Cisco Penetration Testing y Cisco Advanced Services, somos capaces de aumentar la eficiencia y eficacia de nuestra inteligencia. Esta colaboración permite introducir datos de diferente índole al flujo de inteligencia general que Talos utiliza para crear y ofrecer protección a los clientes. Esta telemetría da visibilidad y contexto a los datos, lo que nos proporciona una visión única de los ataques dirigidos y de la actividad de prueba de penetración de aplicaciones (tipo APT).

Talos abarca seis áreas clave: Inteligencia e Interceptación de Amenazas; Investigación de la Detección; Ingeniería y Desarrollo; Investigación, Descubrimiento de Vulnerabilidades y Operaciones; Comunidad, Web y Diseño; y Alcance Global.

Inteligencia e Interceptación de Amenazas se encarga de la correlación y el seguimiento de las amenazas para que Talos pueda convertir la información imputable en información de amenazas procesable. Al identificar rápidamente las amenazas y los actores de las amenazas, somos capaces de proteger a nuestros clientes de forma rápida y eficaz.

Investigación de la Detección consiste en el análisis de vulnerabilidades y malware que lleva al desarrollo de contenidos de detección para todos los productos de Cisco Security. Esto incluye la descompresión, la ingeniería inversa y el desarrollo de código de prueba de concepto. Así nos aseguramos de que abordamos cada amenaza de la manera más eficiente y efectiva posible según cada plataforma.

Ingeniería y Desarrollo su labor es la de asegurar que nuestros diversos motores de inspección permanecen actualizados y



mantienen su capacidad para detectar y abordar amenazas emergentes. Este equipo es responsable de todo el contenido de detección impulsado por Cisco Anti-Spam, Cisco Outbreak Filters, Talos E-mail y Web Reputation, así como de muchos otros productos. La categorización web y @@ SpamCop también son impulsadas por el equipo de Ingeniería y Desarrollo. Compuesto por desarrolladores, ingenieros de control de calidad, investigadores de seguridad, ingenieros de operaciones y analistas de datos, el departamento de Ingeniería y Desarrollo trabaja conjuntamente para desarrollar sistemas y herramientas que produzcan contenido de detección que utilizarán los productos de Cisco.

Investigación, Descubrimiento de Vulnerabilidades y Operaciones consiste en el desarrollo programático y repetitivo para identificar problemas de seguridad de Día Cero en las plataformas y sistemas operativos de las que dependen los clientes, y así encontrar y defenderse contra los problemas de seguridad. Nuestro equipo trabaja con los proveedores para descubrir y parchear de forma responsable más de 200 vulnerabilidades al año. De esta manera, se reducen los vectores de ataque potenciales antes de que los que se esconden detrás de la amenaza puedan hacer uso de ellos.

Comunidad, Web y Diseño lidera los esfuerzos de Cisco Security para ofrecer a la comunidad de código abierto nuevas herramientas para los clientes y los profesionales de la seguridad a la hora de combatir a los malos. Este equipo también está formado por los equipos de diseño y web de Talos, que crean los gráficos, sitios web, libros blancos y mucho más para la organización Talos y los productos de código abierto. El equipo web gestiona el diseño y las características de TalosIntelligence.com, así como las de los sitios web de nuestras otras comunidades de código abierto y herramientas internas. El equipo de diseño está a cargo de todo el branding de Talos. Además, el departamento de diseño ayuda en la creación de todos los documentos públicos de Talos, como diagramas, gráficos y newsletters.

Alcance Global difunde toda la inteligencia de Talos a los clientes y a la comunidad de seguridad global. Colaboran en la investigación sobre seguridad con todos los demás equipos de investigación de Talos, permaneciendo alerta al panorama de amenazas para identificar nuevas tendencias y realizar un seguimiento tanto de las nuevas como de las existentes. El equipo está presente en todo el mundo y comunica los resultados a través de reuniones con clientes, presentaciones en conferencias, el blog de Talos, seminarios web, entrevistas en prensa, podcasts y recursos en idiomas locales.

PROTECCIÓN SUPERIOR

AMPLITUD Y PROFUNDIDAD DE LA COBERTURA DE SEGURIDAD

La protección de su red requiere una cobertura amplia y profunda. Mientras que algunos equipos de investigación limitan su enfoque a unas pocas áreas, Talos ofrece protección contra una amplia gama de amenazas. La información sobre amenazas de Talos es compatible con una amplia gama de soluciones de seguridad, entre las que se incluyen el Sistema de Prevención de Intrusiones de Última generación (NGIPS), los Firewalls de nueva generación (NGFW), la Protección frente a malware avanzado (AMP), el Email Security Appliance (ESA), la seguridad del correo electrónico en la nube (CES), la Seguridad del correo electrónico de la nube (CWS), el dispositivo de seguridad de la Red (WSA), Umbrella y ThreatGrid, así como numerosos sistemas de protección contra amenazas comerciales y de código abierto.

Los clientes de Cisco se benefician de manera exclusiva de los productos de seguridad de Cisco. Estos productos contribuyen directamente a la telemetría de Talos, que a su vez se utiliza para ofrecer contenido de detección que puede implementarse en cualquier entorno para proteger todo tipo de activos.

SEGURIDAD DEL CORREO ELECTRÓNICO

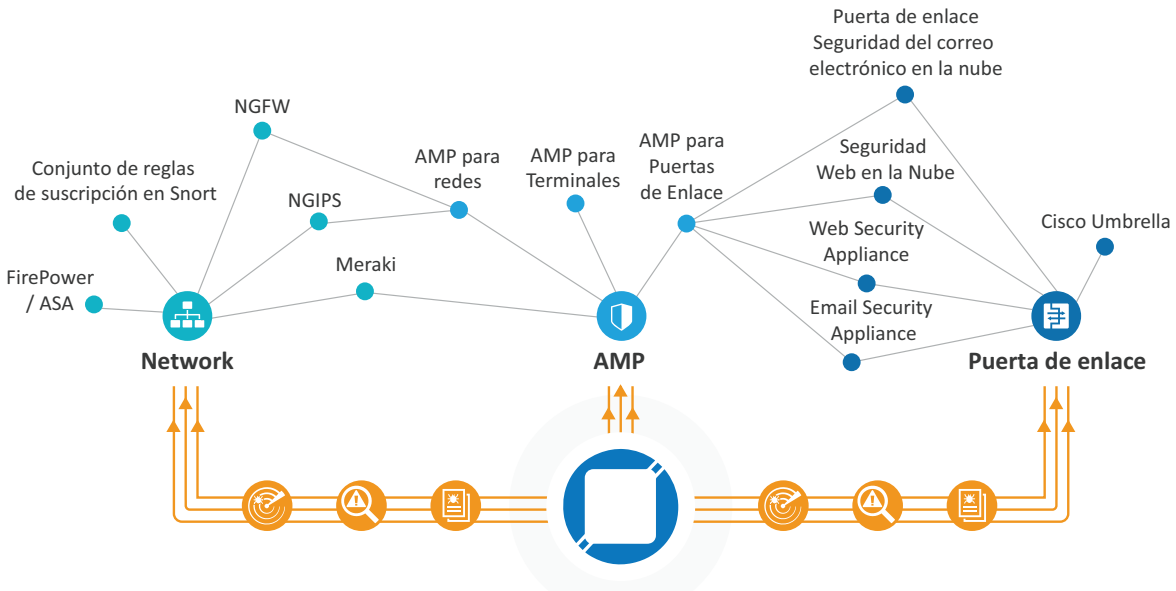
Cada día, Talos inspecciona más de 300.000 millones de correos electrónicos, utilizando tecnologías de detección por capas, como filtros de brotes y filtros de reputación basados en el aprendizaje automático, junto con la Protección frente a malware avanzado (AMP) de Cisco. Con todas las características combinadas, Talos bloquea aproximadamente 200 mil millones de correos electrónicos maliciosos al día, lo que equivale a aproximadamente 2,3 millones de bloqueos por segundo.

VISIBILIDAD WEB INIGUALABLE

La tecnología de Cisco Web Security es conocida por detectar e identificar nuevas y emergentes técnicas de explotación web. Talos inspecciona casi 17 mil millones de solicitudes web cada día, utilizando múltiples métodos de protección, incluyendo nuestra tecnología AMP para la protección de usuarios.

VULNERABILIDAD DEMOSTRADA BASADA EN LA PROTECCIÓN

Talos es bien conocido en la industria por su excelencia en la detección de vulnerabilidades, exploits y malware que surgen diariamente. Mediante versiones rápidas y de alta calidad,



La inteligencia de amenazas de Talos es compatible con una amplia gama de soluciones de seguridad, entre las que se incluyen NGIPS, NGFW, AMP, ESA, CES, CWS, WSA, Umbrella y ThreatGrid, así como numerosos sistemas de protección contra amenazas comerciales y de código abierto.

Talos recopila datos de múltiples fuentes para crear una de las plataformas de recopilación y análisis de inteligencia más completas de la industria.

mantenemos a nuestros clientes al día ofreciendo protección basada en vulnerabilidades contra las últimas amenazas. Talos así lo ha demostrado de manera constante y habiendo sido validado por terceros (NSS labs Inc, una agencia independiente líder en investigación de seguridad). Hemos liderado las pruebas NGIPS y NGFW de la Red en cuando a tasas de detección durante los últimos siete años.

PROTECCIÓN AVANZADA CONTRA MALWARE

La protección contra el ataque de malware requiere tecnologías de detección innovadoras y avanzadas, recopilar grandes cantidades de información, ingeniería inversa y análisis. Talos utiliza todo esto para desarrollar sistemas de protección contra el malware y post-compromiso, servicios de reputación y herramientas de análisis para localizar las amenazas a medida que estas van apareciendo. Estas capacidades se incluyen en todos los productos de Cisco para proteger hosts, puertas de enlace de correo y activos de red, protegiendo realmente a los clientes antes, durante y después de la amenaza.

INTELIGENCIA INTEGRAL

DATOS SOBRE AMENAZAS VIABLES IMPULSADOS POR LA COMUNIDAD

El componente central de cualquier estrategia de seguridad holística es una inteligencia sólida y viable. Talos ha construido una de las plataformas de recopilación y análisis de inteligencia más completas de la industria. A través de ClamAV®, Snort®, Immunet®, SpamCop©, Talos Reputation Center, Threat Grid® y otras comunidades de usuarios de Talos, recibimos información valiosa que ningún otro equipo de investigación de seguridad puede igualar. Mediante la colaboración con usuarios y clientes de todo el mundo que utilizan nuestro programa de Creta, Talos es capaz de detectar amenazas por regiones a medida que surgen.

ACCESO A LA INFORMACIÓN SOBRE LA VULNERABILIDAD

Talos analiza diariamente numerosas fuentes de inteligencia públicas y privadas, buscando nuevas amenazas y actuando en base a información en tiempo real para desarrollar nuevos contenidos de detección. Asociaciones como el Microsoft Active Protection Program (MAPP) permiten a Talos gestionar de forma rápida y eficaz las nuevas amenazas dirigidas a Microsoft y Adobe, lo que nos permite difundir nuestros sistemas de detección a la vez que los parches de Microsoft.

INTELIGENCIA DE MALWARE EN TIEMPO REAL

Talos recopila más de 1,1 millones de muestras de software malicioso al día gracias a la compilación de datos adquiridos a partir de la telemetría de productos junto con honeypots, sandboxes y asociaciones industriales en la comunidad de malware. Nuestra avanzada infraestructura de análisis analiza automáticamente muestras y genera rápidamente contenido de detección para mitigar las amenazas diarias. Esto nos proporciona una visión significativa del panorama de las amenazas y una perspectiva sin precedentes cuando nuestros adversarios intentan comprometer a los usuarios.

INVESTIGACIÓN DE AMENAZAS

Tanto si se trata de identificar nuevas familias de malware dirigidas a terminales de punto de venta, redes maliciosas generalizadas o incluso amenazas que suponen un riesgo para los servicios centrales de Internet, se puede contar con Talos para identificar, investigar y documentar a nuestros adversarios.

Para cada investigación, Talos identifica múltiples formas en las que los clientes pueden defenderse contra las amenazas. Nos enorgullecemos no sólo de identificar y dar solución al problema en cuestión, sino también identificar todas las facetas de la red criminal del adversario, incluso si están asociadas con campañas de malware totalmente independientes.

Los clientes de Cisco se benefician al incorporar esta investigación y protección de inteligencia de amenazas en todos los productos de seguridad de Cisco. Además, compartimos esta información con el público a través de blogs, reglas en Snort, conferencias y libros blancos para mejorar la seguridad de Internet para todos y ayudar a introducir obstáculos para los adversarios.

TECNOLOGÍAS INNOVADORAS DE DETECCIÓN

TECNOLOGÍAS DEFENSIVAS FLEXIBLES PARA ENTORNOS DINÁMICOS

El panorama de las amenazas evoluciona rápidamente y, a medida que cambian los ataques, también lo hacen las tecnologías defensivas utilizadas para detectarlos. Talos trabaja constantemente en nuevas tecnologías de detección que van más allá de los mecanismos de detección actuales, a la vez que los flexibiliza para adaptarse rápidamente a las amenazas del mañana.

ANTICIPACIÓN DE AMENAZAS

Una cosa es responder a las nuevas amenazas y otra es protegerse contra las que son nuevas y emergentes. Talos está constantemente buscando nuevas vulnerabilidades y amenazas que podrían afectar a nuestros clientes. Cuando se descubren nuevas vulnerabilidades, Talos amplía la cobertura para protegerse contra estas amenazas desde el primer momento, mientras los proveedores afectados desarrollan y prueban sus parches. Esto significa que los clientes de Cisco pueden controlar la amenaza mientras esperan parches de sus proveedores utilizando las protecciones de vulnerabilidad de Día Cero de Talos.

Talos también participa activamente en la localización de nuevos sitios web maliciosos, servidores de comando y control de botnets y otros sitios maliciosos en Internet. Una vez localizada, esta información es catalogada y consolidada en listas negras de IP y feeds de alteración de URL, que se distribuyen a nuestros clientes y se comparten con socios de la industria para hacer de Internet un lugar más seguro.

COMUNIDAD DE CONFIANZA

AMPLIANDO SU EQUIPO

Tener un lugar de confianza al que acudir cuando las cosas se ponen feas resulta esencial para una seguridad eficaz. Si no hay sólidos canales de comunicación entre los equipos de seguridad, los equipos de respuesta y los socios de confianza, es imposible mantenerse al día sobre las amenazas más recientes y resolver sus problemas de seguridad únicos.

Talos cree que deberíamos ser una extensión de su equipo de seguridad. No sólo le enviamos información, queremos tener conversaciones constructivas sobre sus objetivos y cómo podemos ayudarle a alcanzarlos.

INTERCAMBIO DE INFORMACIÓN

El programa Awareness, Education, Guidance, and Intelligence Sharing (Concientización, educación, orientación e inteligencia compartida) se creó específicamente para interactuar con los clientes y socios de Cisco con el fin de ayudarles a resolver los desafíos de detección personalizados en sus entornos especializados. AEGIS© pone a los miembros participantes de la industria de la seguridad en contacto directo con el Talos Threat Intelligence Team. Esto ayuda a crear contenido de detección personalizado, mejorar las prácticas de seguridad, recopilar información sobre nuestros productos y servicios e implementar mejoras en nuestros productos para los clientes. Es otra de las maneras en las que en Talos le ayudamos a proteger su red.

El programa Crete es un intercambio colaborativo entre los clientes de Talos y Cisco FirePower que proporciona a Talos escenarios y tráfico del mundo real. Esto ofrece a los clientes participantes información puntera@@, mientras que los datos recopilados en el programa de Creta nos ayudan a mejorar la detección y prevención de amenazas en todo el mundo.

INFORMACIÓN INTERACTIVA

Talos mantiene un contacto constante con sus clientes a través de numerosos canales interactivos. Los blogs de Talos, ClamAV© y Snort© se actualizan continuamente con información sobre las últimas amenazas, cómo crear contenido de detección personalizado y con un análisis en profundidad de las últimas familias de malware.

CONCLUSIÓN

Para los clientes de Talos, nuestra capacidad e investigación se traduce directamente en productos y servicios de gran prestigio en el sector. Incluso si usted no es cliente de Talos, se beneficiará de los esfuerzos de investigación que Talos ofrece a la comunidad. Talos produce contenidos y herramientas de alto impacto que están disponibles para toda la comunidad, y cumple con nuestro compromiso único y duradero de modelo de código abierto y con un flujo continuo de documentos de investigación, presentaciones y entradas en blogs.

Talos ofrece un enfoque único, integral y proactivo para proteger su red con un historial de liderazgo y éxito en la industria de la seguridad. Los miembros del equipo de Talos se centran en ofrecer información sobre seguridad de alta calidad, orientada al cliente, llegando a los más altos estándares de precisión y relevancia.

TALOS

Content	URL
Talos Website	talosintelligence.com
Talos Blog	blog.talosintelligence.com
Talos Twitter	twitter.com/talossecurity
Talos YouTube Channel	cs.co/talostube
Beers with Talos Podcast	talosintelligence.com/podcasts

Content	URL
ClamAV Website	clamav.net
ClamAV Blog	blog.clamav.net
Snort Website	snort.org
Snort Blog	blog.snort.org
Talos Rule Advisories	snort.org/talos