SOC AS A SERVICE

HACIENDO LA SEGURIDAD
MÁS SIMPLE

TECNOLOGIA AVANZADA
TECNOAV

GET SHARP.

Las prácticas de seguridad de una organización resultan igual de importantes que sus productos y servicios en el panorama actual de amenazas en constante evolución. En un intento por proteger sus activos, las organizaciones recurren a una multitud de soluciones de seguridad para anticiparse a posibles amenazas y vulnerabilidades antes de que sucedan.

Al mismo tiempo, el éxito y la eficiencia de la seguridad cibernética de una organización dependen de factores como presupuesto y priorización de necesidades.Las organizaciones luchan por mantener laseguridad de sus activos a medida que aparecen nuevas amenazas y sus prioridades de financiación van cambiando.Sea cual sea el motivo, los recortes frecuentemente acaban afectando a la compra de soluciones, la mano de obra y otros recursos de TI y seguridad.

En estas circunstancias, mientras las organizaciones se esfuerzan por tener un entorno cibernético seguro, sus equipos de seguridad TI a menudo tienen que recurrir a una gran variedad de diferentes soluciones para poder satisfacer sus necesidades de detección, protección y respuesta. Los analistas de seguridad pasan horas integrando la masa de información que reciben procedente de numerosas soluciones de seguridad distintas y que “no hablan el mismo idioma.”

PRINCIPALES VENTAJAS

RECORTA COSTES
Proporciona múltiples capacidades y visibilidad en sistemas para conseguir más efectividad en la protección, detección y respuesta con menos gasto.

REDUCE RIESGOS
Da una visión eyes-on-glass del mapa de seguridad de la organización y permite una capacidad de respuesta rápida y de alta precisión.

AUMENTA LA EFICIENCIA
Asegura que los equipos de seguridad IT dispongan de un completo conjunto de herramientas y capacidades para detectar rápidamente las amenazas y mitigarlas de forma precisa.

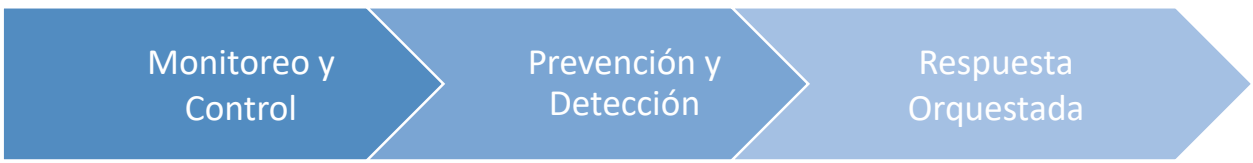
PROTEGE EN MINUTOS
Implementa, detecta y analiza decenas de miles de terminales en tal solo 2 horas, sin tiempo de inactividad IT.

Resulta fácil ver cómo se pierde visibilidad mientras las amenazas reales quedan ocultas bajo una montaña de falsos positivos.

Plataforma SOCaaS

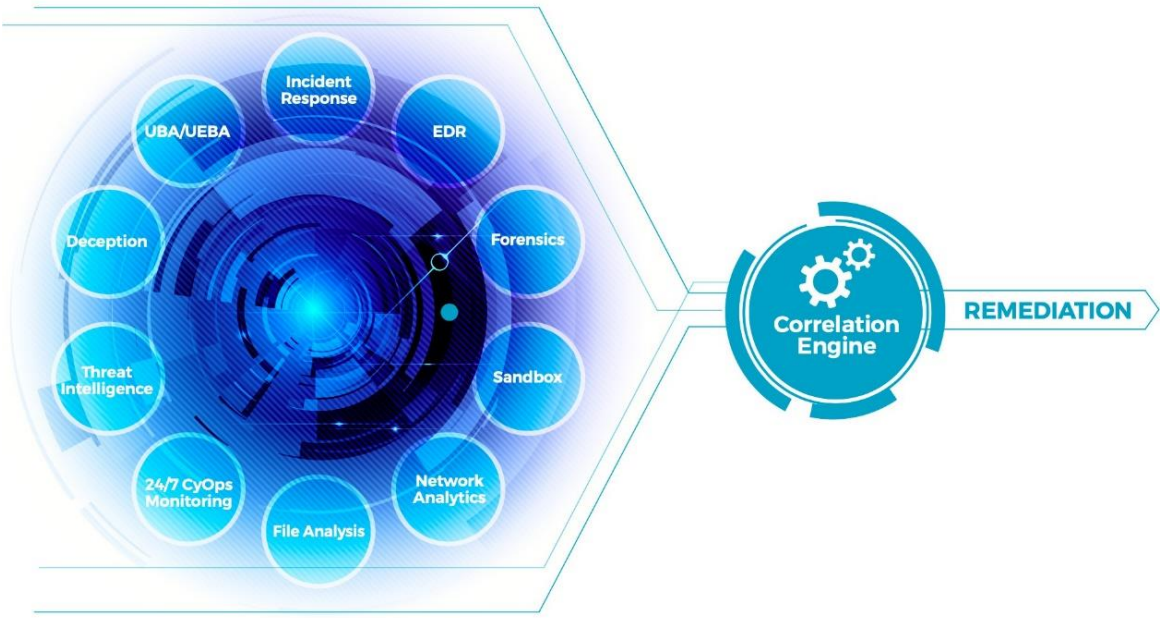
SOCaaS (usando tecnología Cynet) advanced threat detection and response platformsimplifica la seguridad empresarial proporcionando una respuesta holística a todas lasnecesidades de protección de una organización.

Cynet 360 disminuye el gasto en seguridad facilitando múltiples capacidades en una única solución y reduciendo fugas de los recursos organizativos, la mano de obra y el presupuesto. Además, la plataforma 360 proporciona el más alto nivel de seguridad empresarial al correlacionar indicadores en los sistemas, aumentando así la visibilidady precisión de detección en toda la organización, sin que hagan falta múltiples soluciones de seguridad cibernética.



¿CÓMO LO HACEMOS?

Monitoreamos los endpoints mediante un agente liviano. Cuando está operativa, la plataforma comienza a analizar y correlacionar indicadores en la red, archivos, usuarios y terminales, emitiendo clasificaciones de riesgos para comportamientos potencialmente anómalos, asegurando el menor número de falsos positivos y consiguiendo una imagen clara de las operaciones de ataque a lo largo del tiempo. Las capacidades SOCaaS de aprendizaje automático y remediación automatizada consiguen simplificar los procesos,aliviando la presión sobre el personal de seguridad IT.



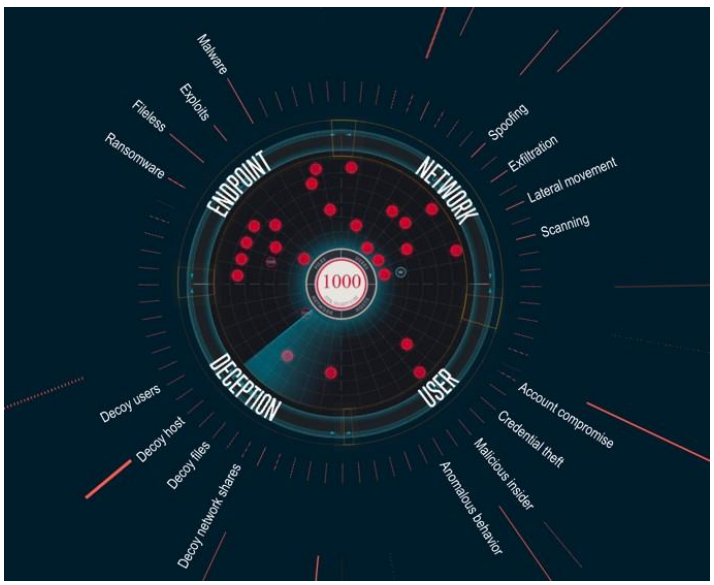
CASOS DE USO PRINCIPALES

Endpoint Detection & Response –

SOCaaS se despliega y detecta rápidamente amenazas en miles de terminales en menos de 2 horas. Como parte de una solución integral SOCaaS correlaciona indicadores y proporciona visibilidad completa en toda la empresa.

User & Entity Behavior Analytics –

Las capacidades UEBA de SOCaaS ayudan a losequipos de seguridad IT a identificar amenazas internas, cuentas comprometidas y ataques dirigidos antes de que se haya producido el daño.



FUNCIONALIDADES

Network Analytics – SOCaaS proporciona visibilidad completa además de análisis del tráfico de red y de la actividad en toda la organización.

UBA Verification – Basada en la capacidad User & Entity Behavior Analytics de SOCaaS, UBA Verification proporciona a los equipos de seguridad empresarial una herramienta para analizar la actividad de los usuarios y asegurar que aquellos que acceden a los activos de la organización son quienes dicen ser.

Incident Response – SOCaaS proporciona a las organizaciones objeto de ataques laherramienta global Incident Response 24/7, liderada por un equipo de expertos en seguridad altamente experimentados.

24/7 Monitoring – El equipo de monitoreo 24/7 plenamente operativo observa eyes-on-glass los acontecimientos que están sucediendo en tiempo real, marcando la actividad sospechosa y asegurando el perímetro de la organización.

Threat Intelligence – SOCaaS utiliza 20 bases de datos internas y externas que contienen la última información en Threat Intelligence, además de integrar el input de las CPIs. Esto proporciona a las organizaciones una capa adicional de protecciónc ontra las actividades sospechosas y maliciosas.

Forensics – SOCaaS ofrece un fácil seguimiento de alertas, amenazas y procesos asociados en una sencilla herramienta GUI. Los equipos de seguridad IT gestionan fácilmente investigaciones forenses profundas, permitiéndoles identificar e investigar rápidamente incidentes sospechosos.

DIFERENCIADORES CLAVE DE CYNET

- Da cobertura a decenas de miles de terminales en tan solo 2 horas.
- Heuristic analysis engine identifica comportamientos anómalos y protege contra las amenazas internas.
- La correlación cruzada en redes, usuarios, archivos y terminales significa completa visibilidad en toda la red.
- Permite la creación de reglas para las herramientas automatizadas de Remediation e Incident Response.
- Ofrece una solución completa para la ciberseguridad de una organización con capacidades de anti-malware, anti-ransomware, anti-APT y anti-exploit.
- Un equipo eyes-on-glass Incident Response a su disposición, 24 horas al día/7 días a la semana.

Deception – SOCaaS despliega estratégicamente señuelos en archivos, carpetas, servidores y recursos compartidos para atraer a posibles atacantes hasta trampas previamente desplegadas. Después los mecanismos de seguimiento monitorizan y proporcionan una imagen clara de la actividad del atacante.

Sandbox – SOCaaS proporciona un sandbox tanto para análisis estáticos de archivos como para análisis dinámicos de procesos permitiendo una investigación segura de los elementos sospechosos.

GUAYAQUIL
Calle 3ra. Este 112 y Calle E,
Nueva Kennedy
090112

PBX: +(593-4) 228-6799

QUITO
Av. República 770 y Eloy Alfaro
Edificio EPZA Piso 6to, Of. 602
170516

Tel. (02) 290-3079 / 290-3708

Más de 33 años Innovando Soluciones Tecnológicas