SOC en seguridad informática

El SOC es una instalación dedicada que alberga un equipo de analistas de seguridad que utilizan una variedad de tecnologías, incluidos firewalls, sistemas de prevención de intrusos (IPS) y sistemas de gestión de eventos e información de seguridad (SIEM) para mantener una sólida postura de seguridad y detectar y responder rápidamente a las amenazas que se presentan

El sistema SIEM recopila datos de varias fuentes, como flujos de datos, registros, capturas de paquetes, syslogs y otros métodos, y correlaciona y analiza los datos en busca de signos de actividad maliciosa o comportamiento anormal. El equipo SOC también utiliza fuentes de inteligencia de amenazas, informes externos y actualizaciones de productos para mantenerse actualizado sobre las últimas advertencias y vulnerabilidades.

El equipo SOC está formado por analista

s
e
in
ge
ni
er
os
qu
e
su
pe
rv
is
an
la
re
d,
lo
s
en
dp
oi
nt
s,
lo
s
se
rv
id
or
es
,
la
s
ba
se
s

de
da
to
s,
la
s
ap
li
ca
ci
on
es
,
lo
s
si
ti
os
we
b
y
ot
ro
s
si
st
em
as
en
bu
sc
a
de
po
si
bl
es

in
ci
de
nt
es
o
co
mp
ro
mi
so
s
de
se
gu
ri
da
d.
Ta
mb
ié
n
re
al
iz
an
ta
re
as
de
bl
in
da
je
pr
oa
ct

iv
as
,
co
mo
pa
rc
he
ar
so
ft
wa
re
y
fi
re
wa
ll
s,
id
en
ti
fi
ca
r
co
nf
ig
ur
ac
io
ne
s
in
co
rr
ec

ta
s
y
ag
re
ga
r
nu
ev
os
ac
ti
vo
s
a
me
di
da
qu
e
se
co
ne
ct
an
.

La colaboración entre el SOC y los equipos de respuesta a incidentes es fundamental para el éxito de cualquier programa de cyber-protección, ya que garantiza que los incidentes de seguridad sean detectados rápidamente y abordados con eficacia.

Ventajas y beneficios

Las ventajas de tener un SOC incluyen:

– Visibilidad mejorada de la postura de seguridad de la organización y el panorama de riesgos

– Capacidades mejoradas de detección y respuesta para incidentes de ciberseguridad

– Riesgo reducido de filtraciones de datos y violaciones de cumplimiento

– La implementación de un SOC puede mejorar el rendimiento de las operaciones de blindaje al optimizar los procesos, permitir una mejor colaboración entre los equipos de control de amenazas y proporcionar una mayor visibilidad de las posibles peligros a la seguridad.

– Mayor seguridad y confianza de los clientes y partes interesadas

-Al final del ejercicio y, dada la necesidad de participar en licitaciones y ser evaluado por variables de competencia, esto otorga una mejor puntuación.

Framework-Estructura

Un Centro de Operaciones de Seguridad (SOC) es un departamento central responsable de gestionar los problemas de seguridad tanto a nivel organizativo como técnico. Un SOC físico dentro de un edificio o instalación sirve como Hub central para monitorear y responder a incidentes de seguridad utilizando tecnología de procesamiento de datos.

Por lo general, un SOC está equipado con una variedad de herramientas de protección, como firewalls, sistemas de detección de intrusos, software antivirus y más. Como parte de su misión de mantener una sólida postura de blindaje, un SOC monitorea y analiza de forma rutinaria la actividad en redes, servidores, terminales y otros sistemas, empleando una gama de herramientas y técnicas avanzadas para detectar comportamientos anómalos que podrían indicar una amenaza a la

estabilidad de los sistemas.

Un marco de un Centro de operaciones de seguridad, es un conjunto de pautas y mejores prácticas que ayudan a una organización a establecer y mantener este tipo de aseguramiento. Un marco SOC cubre varios aspectos de las operaciones, tales como:

– Los objetivos y alcance

– Las funciones y responsabilidades del personal

– Los procesos y procedimientos de respuesta a incidentes, inteligencia de amenazas, gestión de vulnerabilidades, etc.

– Las herramientas y tecnologías utilizadas

– Las métricas e indicadores para medir el desempeño y la efectividad

– Los requisitos de gobernanza y cumplimiento.

Un marco SOC ayuda a una organización a diseñar e implementar un SOC que satisfaga sus necesidades y objetivos específicos.Este tipo de referentes, también ayuda a garantizar que este Centro opere de manera consistente y eficiente, siguiendo los estándares de la industria y las mejores prácticas.

Del mismo modo, se puede personalizar y adaptar a diferentes tipos de organizaciones, como empresas, agencias gubernamentales, proveedores de servicios gestionados, etc.

Servicios

Los servicios del Centro de operaciones de seguridad son esenciales para proteg

er
lo
s
ac
ti
vo
s
di
gi
ta
le
s
de
un
a
or
ga
ni
za
ci
ón
de
la
s
am
en
az
as
ci
be
rn
ét
ic
as
.
Un
SO

C
es
un
a
un
id
ad
ce
nt
ra
li
za
da
qu
e
de
se
mp
eñ
a
un
pa
pe
l
fu
nd
am
en
ta
l
en
la
pr
ot
ec
ci
ón

de
la
s
or
ga
ni
za
ci
on
es
de
la
s
am
en
az
as
de
se
gu
ri
da
d,
al
mo
ni
to
re
ar
,
de
te
ct
ar
,
an
al

iz
ar
y
re
sp
on
de
r
a
in
ci
de
nt
es
de
ma
ne
ra
op
or
tu
na
y
ef
ec
ti
va
,
al
mi
sm
o
ti
em
po
qu
e

ta
mb
ié
n
pr
op
or
ci
on
a
in
fo
rm
es
y
an
ál
is
is
va
li
os
os
pa
ra
ap
oy
ar
la
s
op
er
ac
io
ne
s
de

se
gu
ri
da
d
en
cu
rs
o.

Un SOC consta de un equipo de expertos en seguridad que utilizan diversas herramientas y técnicas para proteger la red, los servidores, las aplicaciones, las bases de datos, los sitios web y los puntos finales de la organización. Este tipo de ente, también garantiza el cumplimiento de las normas y mejores prácticas de la industria y del gobierno.

Algunas de las funciones clave de los servicios de un Centro de Operaciones de Seguridad incluyen:

– Supervisión de la red:Proporciona una visibilidad completa de la actividad digital de la organización y detecta cualquier anomalía o comportamiento sospechoso que pueda indicar un compromiso.

– Técnicas de prevención: Implementa medidas proactivas para disuadir y desviar riesgos conocidos y desconocidos, como firewalls, software antivirus, cifrado, autenticación, etc.

– Detección e inteligencia de amenazas: Aprovecha las tecnologías avanzadas y la experiencia humana para evaluar el origen, el impacto y la gravedad de cada incidente de ciberseguridad y priorizar la respuesta en consecuencia.

– Respuesta y remediación de incidentes: Coordina y ejecuta acciones rápidas y efectivas para contener y neutralizar amenazas, utilizando una combinación de intervenciones automáticas y manuales.

– Informes: Documenta y comunica todos los incidentes y amenazas a las partes interesadas relevantes y los alimenta a un depósito central de datos para futuros análisis y mejoras.

– Riesgo y cumplimiento: Garantiza que la organización se adhiere a los estándares y regulaciones aplicables para la seguridad de la información, como ISO 27001, PCI DSS, HIPAA, GDPR, etc.

Al subcontratar los servicios del Centro de operaciones de seguridad a un proveedor confiable, una organización puede beneficiarse de:

– Monitoreo y protección 24/7 de sus activos digitales por parte de un equipo de profesionales de seguridad experimentados y certificados

– Acceso a herramientas y tecnologías de última generación que pueden mejorar las capacidades de detección y respuesta del SOC

– Reducción de costos y complejidad de administrar y mantener un SOC interno

– Postura de seguridad mejorada y resiliencia contra ataques cibernéticos.

– Aumento de la confianza y satisfacción del cliente.

Mejores prácticas

Un Centro de Operaciones de Seguridad (SOC) es una unidad centralizada que monitorea, detecta, responde y previene ataques cibernéticos. Está compuesto por un equipo de analistas de seguridad, ingenieros y gerentes que utilizan varias herramientas y procesos para proteger los activos y datos de la organización.

Este tipo de instrumentos puede proporcionar varios

beneficios, como visibilidad mejorada, respuesta más rápida a incidentes, costos reducidos y cumplimiento mejorado. Sin embargo, para lograr estos beneficios, este centro necesita seguir algunas mejores prácticas que aseguren su eficacia y eficiencia. Estas son algunas de las mejores prácticas, de acuerdo con los expertos:

– Definir el alcance y los objetivos: Debe tener una visión y una misión claras que se alineen con las metas y prioridades de la organización. El alcance debe definir qué activos y datos cubre, qué amenazas enfrenta, qué servicios brinda y a qué partes interesadas apoya. Los objetivos deben ser específicos, medibles, alcanzables, relevantes y de duración determinada (SMART) y deben comunicarse a todos los miembros del equipo y otras partes relevantes.

– Establecer un marco de gobierno: Debe tener un marco de gobierno que defina las funciones y responsabilidades de los miembros del grupo de trabajo, la estructura de informes, los procedimientos de escalamiento, las políticas y procedimientos, las métricas de desempeño y los mecanismos de auditoría. El marco de gobernanza también debe garantizar que cumpla con las leyes, regulaciones y estándares aplicables y que siga las mejores prácticas para las operaciones de seguridad.

– Implementar un sistema de gestión de eventos e información de seguridad (SIEM): un sistema SIEM es un componente central de un SOC que recopila, correlaciona, analiza y alerta sobre eventos de seguridad de diversas fuentes, como dispositivos de red, servidores, aplicaciones y puntos finales.Este sistema puede ayudar a detectar anomalías, identificar patrones, priorizar incidentes, automatizar respuestas y generar informes. Es por eso que este mecanismo debe configurarse correctamente para adaptarse a las necesidades y el entorno de la organización y debe integrarse con otras herramientas y sistemas que utiliza el SOC.

– Desarrollar un programa de inteligencia de amenazas:se trata de un proceso de recopilación, análisis y uso compartido de información sobre amenazas actuales y emergentes que pueden afectar a la organización. Este tipo de implementaciones puede ayudar al SOC a comprender el panorama de amenazas, anticipar ataques, mejorar las capacidades de detección, mejorar las estrategias de respuesta y reducir los riesgos. Este, debe aprovechar las fuentes de inteligencia tanto internas como externas, como registros, alertas, fuentes, informes y plataformas, y debe difundir la inteligencia a las partes relevantes de manera oportuna y procesable.

– Capacitar y retener al personal del SOC: el personal es el activo más valioso, que requiere capacitación y desarrollo constantes para mantenerse al día con las amenazas y tecnologías en evolución.

El personal de estos equipos debe tener un conjunto diverso de habilidades y competencias, como conocimientos técnicos, pensamiento analítico, habilidades de comunicación, habilidades de trabajo en equipo y habilidades para resolver problemas. El personal de un SOC también debe tener una trayectoria profesional clara y oportunidades de crecimiento que los motiven a desempeñarse bien y permanecer leales a la organización.

Herramientas-Tools

Las herramientas del Centro de operaciones de seguridad son aplicaciones de software que ayudan a los analistas de seguridad a monitorear, detectar, responder y prevenir ataques cibernéticos. Algunas de las herramientas comunes utilizadas por los equipos SOC son:

– Administración de eventos e información de seguridad (SIEM): Estas herramientas recopilan y analizan datos de varias fuentes, como dispositivos de red, servidores, aplicaciones y dispositivos de seguridad, y brindan una vista centralizada de

la postura de seguridad de una organización. Del mismo modo este instrumental, también puede generar alertas basadas en reglas o anomalías predefinidas, y facilitar la respuesta a incidentes y el análisis forense.

– Detección y respuesta de endpoints (EDR): las herramientas EDR brindan visibilidad y control sobre los puntos finales de una organización, como computadoras portátiles, de escritorio y dispositivos móviles.También,pueden detectar actividades maliciosas, como infecciones de malware, acceso no autorizado o exfiltración de datos, y permiten a los analistas aislar, remediar o borrar puntos finales comprometidos de forma remota.

– Supervisión de la seguridad de la red (NSM): las herramientas de NSM capturan y analizan el tráfico y los metadatos de la red para identificar posibles amenazas, como intrusiones, ataques de denegación de servicio o filtraciones de datos. Este conjunto de herramientas también pueden brindar información contextual sobre los activos, protocolos y servicios de la red involucrados en un ataque, y ayudar a los analistas a rastrear el origen y el destino del tráfico malicioso.

– Plataforma de inteligencia de amenazas (TIP): las herramientas TIP agregan y correlacionan datos de varias fuentes externas, como fuentes de código abierto, proveedores comerciales o socios de la industria, y brindan inteligencia procesable sobre las últimas amenazas, vulnerabilidades e indicadores de compromiso. Este grupo de tools TIP también pueden integrarse con otras herramientas SOC para enriquecer las capacidades de análisis y respuesta de los analistas.

– Orquestación, automatización y respuesta de seguridad (SOAR): las herramientas SOAR automatizan y agilizan los flujos de trabajo y los procesos de las operaciones SOC, como la clasificación de alertas, la investigación de incidentes, las acciones de remediación y los informes. Este conjunto de

medidas, también pueden orquestar la colaboración y la comunicación entre diferentes equipos y partes interesadas involucradas en las operaciones de seguridad.

Trabajos

Los trabajos del Centro de operaciones de seguridad tienen una gran demanda a medida que las amenazas y los ataques cibernéticos continúan aumentando.

Un equipo SOC está formado por analistas de seguridad, ingenieros, gerentes y otros especialistas que trabajan juntos para proteger los activos y datos de la organización de las ciberamenazas.

Un trabajo en el Centro de operaciones de seguridad requiere una combinación de habilidades técnicas, habilidades analíticas y habilidades de comunicación. Algunas de las tareas y responsabilidades comunes de un trabajo de SOC incluyen:

– Monitoreo y análisis de alertas

de
se
gu
ri
da
d
de
di
ve
rs
as
fu
en
te
s,
co
mo
di
sp
os
it
iv
os
de
re
d,
fi
re
wa
ll
s,
so
ft
wa
re
an
ti

vi
ru
s,
si
st
em
as
de
de
te
cc
ió
n
de
in
tr
us
os
y
fu
en
te
s
de
in
te
li
ge
nc
ia
de
am
en
az
as
.

– Investigar y evaluar incidentes de seguridad, como infecciones de malware, intentos de phishing, ataques de denegación de servicio y violaciones de datos.

– Escalar y coordinar con otros equipos o partes externas para contener y remediar incidentes de seguridad.

– Documentar e informar sobre incidentes de seguridad, hallazgos y recomendaciones.

– Desarrollar y actualizar políticas, procedimientos y mejores prácticas de seguridad.

– Realización de auditorías, evaluaciones y pruebas de seguridad para identificar vulnerabilidades y brechas en la postura de seguridad de la organización.

– Proporcionar conciencia y capacitación en seguridad a los empleados y partes interesadas.

Para calificar para un trabajo en el Centro de Operaciones de Seguridad, uno debe tener un título o certificación relevante en seguridad cibernética, informática, tecnología de la información o un campo relacionado. Además, es posible que deba tener experiencia en operaciones de seguridad, administración de redes, administración de sistemas u otras funciones de TI. Según el nivel y la función del trabajo de SOC, es posible que también se necesiten certificaciones de seguridad específicas, como CompTIA Security+, CISSP, CEH o GCIH.

Un trabajo en el Centro de operaciones de seguridad puede ser desafiante pero gratificante para aquellos apasionados por la seguridad cibernética y que desean marcar la diferencia en la protección de las organizaciones contra las amenazas cibernéticas. Un trabajo de SOC también puede brindar oportunidades de avance profesional y desarrollo profesional en el campo de rápido crecimiento de la ciberseguridad.

Conclusión

Hemos visto la importancia de un SOC dentro de las compañías internacionales o de franco crecimiento; en HostDime ponemos a tu disposición esta y otros insumos de alto rendimiento para que protejas toda tu información.

Vale la pena considerar que no cualquier infraestructura puede ser catalogada como un SOC, ya que la responsabilidad sobre este tipo de servicios es bastante elevada. Así mismo, contar con un respaldo de marca y de recursos resulta invaluable.
Leer también: Qué es un firewall como servicio; tipos de firewalls o cortafuegos; Cloud HostDime Colombia