Haga que su Centro de Operaciones de Seguridad (SOC) sea Más Eficiente

El secreto para la preparación contra amenazas avanzadas puede de hecho encontrarse dentro de su organización, en sus personas, procesos y tecnologías actuales.

De 38% a 100% de aumento en la efectividad con la colaboración.

Resultados

A pesar de la escasez de habilidades cibernéticas, existen maneras de mejorar los resultados de las operaciones de seguridad.

Tiempo de detección más rápido
Al obtener conocimiento más temprano, bajo contexto, para más colaboradores.

Mayor confianza
Ya que múltiples fuentes pueden validar decisiones según sea necesario.

Menos errores
Al compartir automáticamente datos críticos de manera precisa.

Tiempo más rápido para corregir
Mediante una orientación clara sobre las acciones adecuadas, entregada a las personas adecuadas para actuar.

Personas

La buena comunicación, la transparencia y la rendición de cuentas permiten el trabajo en equipo entre los diversos participantes en la gestión de incidentes.

CISO
Los ingenieros y arquitectos de la oficina del CISO tienen la responsabilidad principal de principio a fin, desde la prevención hasta el análisis y la corrección.

Operaciones
Los administradores de endpoint y de red, así como las personas con funciones de soporte de aplicaciones son críticas para la contención y corrección.

IR
Los analistas y el personal que responde primero del SOC, incluyendo a terceros, desempeñan un papel muy importante en la prevención, no sólo en la detección y análisis.

Proceso

Los encuestados dijeron que estaban dispuestos a automatizar o semi-automatizar muchas de las tareas que solían realizar manualmente.

Tareas principales semi-automatizadas

58%
Orquestación entre productos para sistemas de cuarentena.

57%
Copiar un archivo a almacenamiento externo. Restaurar un archivo.

55%
Eliminar una cuenta de backdoor. Apagar o reiniciar el sistema.

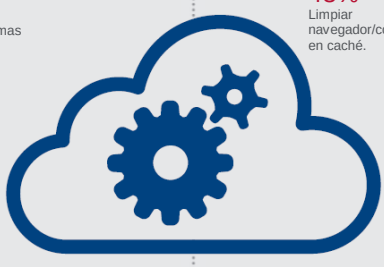
Tareas principales automatizadas

43%
Limpiar navegador/cookies en caché.

37%
Presentación de recinto de seguridad de malware.

36%
Parar/iniciar un servicio de Windows. Aislamiento de la red.

33%
Eliminar el proceso.



Tecnología

Las herramientas de gestión de incidentes pueden colaborar a lo largo de la orquestación entre herramientas, comandos remotos, inteligencia de amenazas compartida, gestión unificada e integración bidireccional.

4 herramientas
El número promedio de herramientas utilizadas fue de 4.

6 a 15 herramientas
20% de las compañías utilizan más de 6, y tantas como 15.

Prioridades de Inversiones en Seguridad

Aunque las mejores herramientas siguen siendo críticas, los encuestados calificaron a la colaboración como su tercera más alta prioridad para el gasto en gestión de amenazas.

40%
Mejores herramientas de detección

33%
Mejores herramientas preventivas

32%
Mejorar la colaboración entre los analistas del SOC, Personas que Responden a Incidentes y Administradores de Endpoint.

La colaboración conecta a personas, procesos y tecnologías, permitiendo a las organizaciones enfrentar más amenazas en menos tiempo y con menos recursos.

Visite www.mcafee.com/collaboration para ver el informe completo.

intel Security

McAfee is now part of Intel Security.