

Automatización de Respuestas con TDR

Para las pequeñas y medianas empresas con recursos limitados y restringidos, o para las empresas distribuidas con falta de personal técnico en cada sucursal, puede ser difícil tomar medidas sobre cada amenaza que demanda atención. La automatización puede ser clave para detectar y corregir amenazas de manera rápida y efectiva. La automatización de respuestas permite a las organizaciones liberar recursos limitados para enfocarse en otras áreas de seguridad. Además, acorta los tiempos de corrección, lo que puede disminuir el tiempo de permanencia de la infección y hacer que la organización vuelva a funcionar.

La TDR de WatchGuard permite a los usuarios establecer políticas fácilmente, para habilitar la automatización según las necesidades de la organización. A través de la valoración y la priorización de amenazas de ThreatSync, los usuarios pueden establecer políticas para iniciar una corrección según una valoración o una gama de amenazas. Estas políticas pueden incluir destruir procesos, poner un archivo en cuarentena y eliminar el valor de claves del registro. Por ejemplo, las organizaciones con un bajo riesgo de sufrir ataques pueden decidir automatizar la respuesta solo para amenazas de calificación alta, con una valoración de 8 o más. Sin embargo, si se encontraran en un mayor riesgo de ataques, podrían elegir automáticamente corregir las amenazas con valoración de 6 o más.

Una valoración integral de las amenazas permite una respuesta inmediata y segura

A través de políticas, los incidentes se pueden corregir automáticamente según su valoración integral de amenaza. Cualquier amenaza que no esté cubierta por una política también se puede eliminar mediante acciones que requieren un solo clic

Comprenda mejor sus riesgos en general, mediante la recopilación y análisis de datos desde el Firebox y el Sensor de Host

La información adicional brinda más detalles sobre cualquier fuente de firmas de amenazas utilizada

SENSOR	STATUS	HOST/IP	SCORE	SOURCE	INDICATORS	OUTCOMES	MACHINE GUIDED ACTIONS	LAST SEEN	OLDEST INDICATOR
Host Sensor	fx	Host: www.eter.org Path: C:\Users\jminsh\Downloads	8	Host: www.eter.org Path: C:\Users\jminsh\Downloads	19	Multiple Outcomes	Select actions...	01/05/2017 4:46:56 PM	24 days ago
Host Sensor	fx	Host: www.eter.org Path: C:\Users\jminsh\Downloads	6	Host: www.eter.org Path: C:\Users\jminsh\Downloads	2	Multiple Outcomes	Select actions...	01/05/2017 5:37:06 PM	1 month ago
Host Sensor	fx	Host: www.eter.org Path: C:\Users\jminsh\Downloads	6	Host: www.eter.org Path: C:\Users\jminsh\Downloads	1	Externally Remediate	Externally Remediate		
Host Sensor	fx	Host: www.eter.org Path: C:\Users\jminsh\Downloads	8	Host: www.eter.org Path: C:\Users\jminsh\Downloads	1	Externally Remediate	Externally Remediate		
Host Sensor	fx	Host: www.eter.org Path: C:\Users\jminsh\Downloads	8	Host: www.eter.org Path: C:\Users\jminsh\Downloads	1	Externally Remediate	Externally Remediate		

Acerca de WatchGuard

WatchGuard® Technologies, Inc. es un líder mundial en seguridad de red, redes wifi seguras y en productos y servicios de inteligencia de red, con más de 75 000 clientes en todo el mundo. La misión de la empresa es hacer que seguridad de calidad empresarial sea accesible para las compañías de todos los tipos y tamaños a través de la simplicidad. Por ello WatchGuard es una solución ideal para empresas distribuidas, pequeñas y medianas empresas (SMB). WatchGuard tiene sede central en Seattle, Washington, y posee oficinas en Norteamérica, Europa, Asia Pacífico, y América Latina. Para obtener más información, visite WatchGuard.com.

Para obtener información adicional, promociones y actualizaciones, siga a WatchGuard en Twitter @WatchGuard, en Facebook o en la página de nuestra empresa en LinkedIn. Además, visite nuestro blog de seguridad de la información, Secplicity, para obtener información en tiempo real sobre las amenazas más recientes y sobre cómo lidiar con ellas en www.secplicity.org.

