RESPUESTA Y DETECCIÓN ADMINISTRADAS CON ACTIVEEYE

RESUMEN TÉCNICO

RESPUESTA Y DETECCIÓN ADMINISTRADAS CON ACTIVEEYE

La Respuesta y Detección Administradas (MDR, por sus siglas en inglés) de ActiveEye aprovecha nuestra plataforma de seguridad y analistas expertos para detectar y responder a las ciberamenazas en su ambiente de TI, así como en sus sistemas VESTA® 9-1-1 de Despacho Asistido por Cómputo (CAD, por sus siglas en inglés) y sistemas ASTRO® 25.

COMPONENTES DE LA MDR DE ACTIVEEYE

Plataforma de Administración de Seguridad de ActiveEye

ActiveEye es una plataforma de Organización, Automatización y Respuesta de Seguridad (SOAR, por sus siglas en inglés) que funciona como el corazón de las operaciones de seguridad. La plataforma de ActiveEye ingiere datos de los elementos de red conectados, los analiza y envía datos y perspectivas relevantes al personal de ciberseguridad. La analítica y el filtrado ayudan a diferenciar entre el tráfico rutinario y el malintencionado, simplificando el enfoque en las amenazas reales. Los siguientes módulos de detección de amenazas están disponibles en la plataforma de ActiveEye:

- Analítica de bitácoras
- Detección de redes
- Respuesta y Detección de Terminales (EDR)
- Detección de DNS
- Detección de vulnerabilidades

La plataforma de ActiveEye recolecta y administra los datos de seguridad, optimizando la detección de amenazas e incrementando el enfoque de las alertas más críticas que requieren respuestas. Las capacidades de analítica integrada examinan varias fuentes de inteligencia contra amenazas en tiempo real, referenciando eventos pasados y siguiendo tácticas establecidas para automatizar la mayoría de las acciones del analista. La analítica también clasifica las investigaciones manuales, priorizando aquellas que tengan más posibilidad de requerir correcciones.

Sensor de Seguridad Remota de ActiveEye (AERSS)

El AERSS es un componente que se despliega opcionalmente y proporciona recopilación remota de bitácoras, detección de intrusión a redes y escaneo de vulnerabilidades.

Centro de Operaciones de Seguridad (SOC)

Los analistas de ciberseguridad expertos de Motorola Solutions realizan un monitoreo de 24/7 en busca de señales de amenazas potenciales. Los analistas alertan a los contactos clave de su organización para movilizar una respuesta y hacen recomendaciones con base en un plan de acción predefinido en caso de que detecten una amenaza. Los servicios estándar del SOC pueden ampliarse con nuestro servicio de perspectivas avanzadas sobre las amenazas que proporciona un personal de cuenta dedicada y una búsqueda proactiva de amenazas.

PLATAFORMA DE ADMINISTRACIÓN DE SEGURIDAD DE ACTIVEEYE

ActiveEye es rápido y simple de desplegar, lo que elimina la carga de instalar, mantener y administrar un componente de seguridad informática y administración de eventos (SIEM) en las instalaciones. Dependiendo de las fuentes de las bitácoras que deban monitorearse, ActiveEye puede reemplazar la necesidad de un SIEM por separado. Las poderosas funciones de seguridad protegen el contenido y acceso a ActiveEye. Los usuarios acceden a la plataforma a través de un buscador web seguro, utilizando una autenticación multifactorial (MFA). Las funciones administrativas permiten administrar el acceso de los usuarios conforme se requiera.

La plataforma se somete a auditorías de seguridad frecuentes y tiene una certificación de auditoría SOC 2 Tipo 2 activa. Utilizamos las mejores prácticas de seguridad en datos para cifrar los datos en tránsito hacia/desde la plataforma y mientras están estáticos. Los datos sin procesar de los eventos y las alertas se almacenan durante 13 meses por defecto y pueden almacenarse por más tiempo en caso de que así se requiera.

ENRIQUECIMIENTO DE DATOS E INTELIGENCIA CONTRA AMENAZAS

ActiveEye utiliza la inteligencia contra amenazas tanto para su detección como para el enriquecimiento de las alertas. Los expertos en el dominio de la seguridad seleccionan cuidadosamente las fuentes de inteligencia contra amenazas y son ellos mismos quienes monitorean el panorama de la ciberseguridad con respecto a las amenazas emergentes, los nuevos actores de estas, la infraestructura de control y dominio y otras entidades relevantes. Esta selección garantiza que las amenazas nuevas se detecten y traten tan pronto como sea posible después de que se anuncia una vulnerabilidad o amenaza. En conjunto, la inteligencia contra amenazas en ActiveEye se deriva de fuentes múltiples, incluyendo:

- Inteligencia expansiva de código abierto (OSINT) que incorpora diversas fuentes más pequeñas
- Fuentes comerciales de pago que permiten tener tanto datos agregados como información bajo demanda sobre las entidades tales como los archivos o las IP
- Datos derivados de los expertos del SOC de ActiveEye conforme navegan entre decenas de miles de alertas cada día

Adicionalmente, Motorola Solutions desarrolla y mantiene una inteligencia contra amenazas amplia y específica de la industria para los gobiernos estatales y locales, así como para la seguridad pública y las grandes empresas.

DETECCIÓN DE AMENAZAS

La plataforma de ActiveEye maximiza el valor de las detecciones que proporcionan los servicios de seguridad integrados, tales como los proveedores de detección y respuesta de terminales (EDR) de última generación. También ofrece detecciones personalizadas contra los servicios que solo proporcionan bitácoras, como muchas plataformas en la nube o SaaS. En ambos casos, los datos sin procesar de los eventos se suministran a ActiveEye y se analizan mediante cientos de reglas que filtran los datos para descubrir anomalías, familias de malware conocidas y otros riesgos.

Para los proveedores que proporcionan detecciones, las reglas de ActiveEye enriquecen las alertas que se reciben con taxonomía de alertas, gravedades derivadas del aprendizaje automatizado (ML) y otros metadatos. Las alertas también pueden correlacionarse con otros datos relevantes para exponer relaciones ocultas, enriquecerse con inteligencia contra amenazas y modificarse con base en su comportamiento histórico.

El mismo proceso aplica para las integraciones de las bitácoras sin alertas integradas. Sin embargo, las reglas operan en los datos sin procesar para descubrir si se violan los umbrales, los patrones de riesgo conocidos y otras condiciones que requieren investigación. Así como con las alertas derivadas de los proveedores, los datos resultantes se enriquecen y correlacionan antes de clasificarse.

Todas las políticas se ejecutan como procesos de transmisión, tan pronto llegan los datos, y como escaneo histórico para identificar los agregados que podrían faltar en el proceso de transmisión sin estado. La lista completa de reglas aplicables puede revisarse en la interfaz de ActiveEye.

AUTOMATIZACIÓN Y ORGANIZACIÓN DE LA SEGURIDAD

Ya que es una plataforma SOAR, ActiveEye organiza el flujo de datos y las acciones, acelerando la remediación al realizar la investigación y las tareas de respuesta automáticamente. Utilizando tácticas personalizadas o predefinidas, ActiveEye maneja las tareas precisas y repetitivas en vez de los analistas humanos de un SOC. ActiveEye es compatible con dos tipos de automatización:

- Automatización de investigación y enriquecimiento — ActiveEye puede buscar información sobre las amenazas, consultar datos anteriores y mostrar los detalles en la pantalla de la investigación principal. Estos datos mejoran la calidad y la velocidad de la investigación manual y proporcionan una base sobre la cual pueden tomarse decisiones automatizadas.

- Automatización de la respuesta — ActiveEye puede tomar las acciones de respuesta que se definen en las tácticas. Las acciones pueden incluir el hacer recomendaciones a los analistas, cambiar la prioridad de las alertas, cerrar una alerta, agregar archivos al listado de bloqueados, eliminar archivos de los sistemas o aislar a un host de la red.

PORTAL DE SEGURIDAD COADMINISTRADO DE ACTIVEEYE

Como una plataforma coadministrada, ActiveEye sincroniza los esfuerzos de seguridad entre su equipo de seguridad y los analistas de nuestro SOC. El portal basado en web proporciona visibilidad a las perspectivas de las amenazas, investigaciones de eventos, reportes de seguridad, asesorías sobre las amenazas y el estado de cualquier caso de seguridad.

Tablero

La información clave en el portal de ActiveEye se resume en el tablero. Este tablero incluye alertas abiertas, un resumen de categorías de estas, Indicadores Clave del Desempeño (KPI) del procesamiento de las alertas, casos de seguridad abiertos y asesorías sobre amenazas recientes. Desde este punto, los usuarios pueden acceder a información más profunda, como los casos de seguridad, los detalles de las alertas, las tendencias de las alertas, los reportes y las comunicaciones grupales.

Casos de seguridad

Cuando Motorola Solutions identifica una amenaza, el SOC crea un caso de seguridad. Los casos de seguridad se pueden ver en el portal de ActiveEye y pueden consolidarse en un resumen de seguridad diario que se envía por correo electrónico.

Detalles y tendencias de las alertas

Las alertas son notificaciones del sistema sobre la actividad inusual. Estas alertas pueden ser evidencia de una amenaza pasada, activa o en desarrollo. Si los analistas creen que las alertas indican una amenaza, pueden abrir los casos de seguridad con base en ellas.

ActiveEye registra los datos relevantes para cada alerta, habilitando a los usuarios para que puedan ver rápidamente sus detonadores, los sistemas a los que impacta y cualquier acción que se toma para tratarlos. Cada registro de alerta también incluye un resumen de atributos clave. Desde ese resumen de alerta, los usuarios pueden acceder a los registros relacionados para obtener más detalles. Estos registros incluyen información sobre las amenazas, datos de eventos pasados, eventos relacionados y bitácoras de actividad.

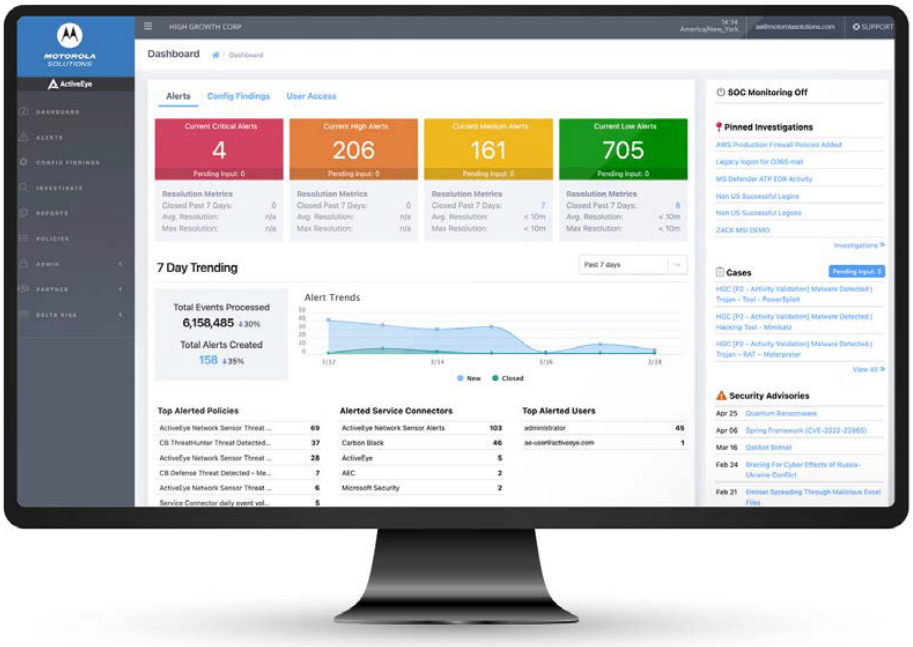


Figura 1-1: Interfaz de ActiveEye

Para poner las alertas en contexto, ActiveEye proporciona herramientas para revisar grupos de alertas según atributos clave o períodos de tiempo. Los filtros de atributos permiten a los usuarios alternar qué grupos de alertas muestra ActiveEye, lo que ayuda a detectar tendencias o actividad de amenazas. Los usuarios también pueden comparar registros de alertas por períodos de tiempo para determinar si las tendencias están asociadas con una amenaza o si son falsos positivos.

Investigaciones y reportes

La robusta capacidad ad hoc de ActiveEye permite a los usuarios investigar y perseguir a las amenazas activas, así como ver los conjuntos de datos históricos. Los reportes proporcionan una vista consistente y simple de los datos de eventos recolectados. Las plantillas predefinidas organizan los datos y muestran los atributos más importantes de los tipos de eventos. Los usuarios pueden personalizar estos reportes estándar para mostrar y resumir los diversos atributos cuando se requiera. Para compartir la información fuera de ActiveEye, los usuarios pueden descargar reportes de hasta 50,000 filas en formato .csv o .json.

Adicionalmente a los reportes y consultas ad hoc, ActiveEye puede proporcionar reportes mensuales opcionales y resúmenes diarios por correo electrónico. El reporte mensual resume los elementos de seguridad importantes y está disponible en un PDF descargable. El resumen de seguridad diario proporciona un conjunto de estadísticas personalizadas del día anterior a una lista de usuarios predeterminada. Este resumen puede incluir conteos de alertas, casos de seguridad abiertos/cerrados, consultas guardadas que tengan datos nuevos y estadísticas de seguridad detalladas sobre las terminales. ActiveEye puede enviar uno o más correos electrónicos de seguridad con contenido diferente para los diferentes grupos.

Asesorías de seguridad

Las asesorías de seguridad son mensajes del SOC que contienen información sobre las amenazas activas para la población general o para su industria específica. Estas asesorías guían a los equipos de seguridad sobre la mejor forma de actuar en contra de una amenaza y les indica en dónde pueden encontrar más información.

Compartir información

Para apoyar la administración de seguridad efectiva, ActiveEye tiene varias funciones para compartir la información. Las alertas de seguridad automáticas notifican a los contactos clave sobre los incidentes con base en su prioridad. Adicionalmente a las alertas de seguridad automáticas, ActiveEye presenta otras funciones para compartir información a las cuales pueden acceder tanto usted como el equipo del SOC de Motorola Solutions, las cuales incluyen:

- **Boletines del SOC** — Instrucciones de su equipo de seguridad o del SOC que los analistas del SOC pueden referenciar cuando creen casos de seguridad. Estas pueden comunicar situaciones a corto plazo en donde podría no necesitarse un caso de seguridad, tal como durante las pruebas o las ventanas de mantenimiento.
- **Libreta de clientes** — EL SOC puede utilizar la libreta de clientes para documentar los detalles sobre su ambiente e información de implementación de redes específicos para ayudar a que nuestros analistas investiguen los casos de seguridad.
- **Procedimientos de contacto** — También están listos y disponibles los procedimientos de escalamiento y las instrucciones sobre a quién contactar si ocurre un incidente. Los procedimientos de contacto incluyen las instrucciones y protocolos para los diversos niveles de incidentes de seguridad específicos. Tanto el SOC como el cliente administrarán los procedimientos de contacto conjuntamente.

Juntas, estas instrucciones diseminarán rápidamente la información importante a los equipos y analistas de seguridad.

Acceso del usuario a ActiveEye

Los ajustes de acceso de usuario simplifican la adición, actualización y eliminación del acceso a ActiveEye. Cada usuario de ActiveEye puede guardar consultas, personalizar reportes y configurar resúmenes diarios por correo electrónico. Se puede otorgar acceso administrativo a los usuarios, lo cual les permitirá realizar tareas administrativas, tales como configurar conectores de servicio nuevos, restablecer contraseñas y configurar la autenticación multifactorial de otros usuarios.

MÓDULOS DE DETECCIÓN DE AMENAZAS DE ACTIVEEYE

Analítica de bitácoras

La función de analítica de bitácoras recopila los datos de las bitácoras de los sistemas, aplicaciones componentes de red, sistemas de seguridad e incluso de otras soluciones SIEM. Muchas políticas de seguridad y componentes de analítica procesan datos de bitácoras para identificar violaciones a la política y actividad sospechosa. Si ActiveEye detecta un evento de interés que podría representar una amenaza, este alertará al analista con base en los ajustes establecidos por usted.

Con el tiempo, los eventos registrados anteriormente pueden proporcionar un contexto crítico para rastrear el origen de una amenaza e identificar las nuevas amenazas utilizando patrones de ataque anteriores. ActiveEye almacena los eventos para que los analistas puedan buscar en ellos y utilizarlos para buscar amenazas. Los eventos permanecen almacenados durante un periodo definido con base en una suscripción. Si bien el periodo predeterminado es de un año, diferentes extensiones están disponibles mediante suscripción.

"ActiveEye puede incorporar diversas bitácoras de varias fuentes, incluyendo los sistemas de autorización y autenticación, almacenamiento de objetos, redes virtuales en la nube, servidores virtuales, servicios de seguridad de la nube, aplicaciones de software e infraestructura física a través de AERRS.

Detección de redes

El módulo de servicio de detección de redes utiliza un enfoque sin agentes para monitorear toda la actividad a través de la red, proporcionando visibilidad sobre qué dispositivos se conectan y qué aplicaciones se están comunicando desde cada dispositivo. Con la integración de ActiveEye, los equipos de seguridad pueden automatizar la investigación de las alertas de tráfico de red y luego verlas en el contexto de la actividad de otro usuario. Además de proporcionar alertas sobre los indicadores de reconocimiento o compromiso activo, las pantallas de investigación de ActiveEye identifican fácilmente a las aplicaciones indeseadas en uso, los dispositivos desconocidos en la red y los patrones de comunicación que crean riesgos.

Para apoyar esto, Motorola Solutions despliega un Sistema de Detección de Intrusiones (IDS) conectado a uno o más puertos SPAN del switch para monitorear las firmas y anomalías de tráfico en tiempo real en busca de señales de actividad malintencionada. El IDS también modela las comunicaciones de red utilizando análisis de paquetes y de niveles de flujo. Esto permite que la analítica identifique el comportamiento anómalo que no capturan las firmas de tráfico predefinidas, incluyendo la actividad sobre las conexiones cifradas.

El conjunto de firmas para el módulo de detección de redes se actualiza cada hora, garantizando que las amenazas emergentes se traten tan pronto como la comunidad de ciberseguridad sepa de ellas.

Respuesta y Detección de Terminales

Si un atacante intenta violar la seguridad, es esencial poder responder más rápido. La integración de herramientas de Respuesta y Detección de Terminales (EDR) con la plataforma de ActiveEye, permite que los analistas de seguridad respondan a los ataques y vean la información de las amenazas en una sola interfaz. Esto les permite reaccionar rápidamente a una emergencia en vez de tener que cambiar de herramienta para investigar y contraatacar.

Los analistas pueden acceder a diversas acciones de respuesta dentro de ActiveEye, tales como aislar hosts, bloquear, permitir y eliminar archivos. Las políticas de seguridad y herramienta de EDR determinan las respuestas disponibles. Si el cliente no tiene una solución de EDR, Motorola Solutions podría recomendar o proporcionar una como parte de este servicio por un costo adicional.

Detección de DNS

Las redes de cómputo utilizan el Sistema de Nombres de Dominio (o DNS) para traducir los nombres de los dominios a direcciones IP, las cuales utilizan los equipos de cómputo para comunicarse entre ellos. Nuestra característica de detección de DNS emplea un servicio de resolución de DNS consciente de la seguridad para prevenir que los ataques de malware, botnets y phishing pongan en riesgo los sistemas y eliminen los datos. Para prevenir la pérdida de datos, el servicio puede bloquear la eliminación o la transferencia de datos a través de puertos o protocolos de red específicos. Esto puede prevenir que un atacante o usuario no autorizado elimine los datos, ya sea que inicien el ataque con una solicitud de DNS o intenten evitar el DNS con una conexión directa de IP. También puede bloquear la transferencia de datos que se inició en o desde su red para prevenir la resolución del DNS hacia destinos malintencionados potenciales. Una vez que se integra con la plataforma de ActiveEye, la detección de DNS proporcionará alertas de los sistemas que intenten acceder a destinos malintencionados conocidos o a aquellos que bloquearon las políticas de seguridad de su organización. El servicio también le permite ver y descargar los reportes de tendencias de uso por categoría o por sistemas individuales.

Puede ser necesario que algunos ajustes de DNS varíen con base en la ubicación del dispositivo. La detección de DNS puede personalizarse con reglas conscientes de la ubicación (en qué red está el sistema) que bloqueen o permitan el tráfico con base en las listas predefinidas.
La detección de DNS se integra habitualmente al perímetro de red, protegiendo los dispositivos dentro de la red. Al instalar un agente de software en los dispositivos móviles aplicables, puede extender la protección de DNS en estos hacia afuera del perímetro de la red. La Detección de DNS puede requerir protecciones únicas en estos dispositivos, con configuraciones variables de restricciones de acceso a internet y de registro si están fuera de su red.

Detección de vulnerabilidades

Durante las actualizaciones o los ajustes del sistema, algunas configuraciones, software o actualizaciones pueden crear inadvertidamente una apertura en la seguridad. El módulo de servicio de detección de vulnerabilidades conecta las herramientas de terceros con ActiveEye para que puedan resaltar estas vulnerabilidades para los equipos de seguridad. Los equipos de seguridad pueden entonces tratar estas vulnerabilidades para brindar protección contra las ciberamenazas como el ransomware o la pérdida y brechas de disponibilidad.
La función de detección de vulnerabilidades escaneará frecuentemente los sistemas y redes configurados en busca de vulnerabilidades en los nuevos componentes de software y sistemas o ajustes de red inseguros. Un motor de escaneo basado en la nube verificará si hay terminales vulnerables accesibles a través de internet, mientras que el AERRS escaneará la infraestructura en las instalaciones. Motorola Solutions trabajará con su equipo para determinar el itinerario de escaneo óptimo y el alcance del sistema. Los escaneos completados resumirán cualquier vulnerabilidad detectada, junto con las acciones recomendadas para cerrarlas. Los escaneos puntuarán las vulnerabilidades detectadas utilizando el Sistema de Puntuación Común de Vulnerabilidades, identificarán si están en una Lista de Exposiciones y Vulnerabilidades Comunes y listarán cualquier host que se vea afectado.

SENSOR DE SEGURIDAD REMOTA DE ACTIVEEYE

El Sensor de Seguridad Remota de ActiveEye (AERSS) es un servidor montado en bastidor y desplegado en su ambiente. El AERSS recopila y monitorea las bitácoras relevantes para la seguridad y el tráfico de red y lo reporta a la plataforma de ActiveEye. Para la configuración de administración inicial, el AERSS se configurará utilizando herramientas de línea de comandos.

Después de la configuración inicial, el AERSS es una caja autogestionada; todas las actualizaciones de los componentes y el sistema operativo se llevan a cabo automáticamente en segundo plano. En algunos casos, se necesita acceso remoto para darle mantenimiento integral al sistema. Habitualmente, no se requiere ninguna acción del personal local.

COLOCACIÓN DEL AERSS EN LA RED

EL monitoreo de red es una de las funciones principales del AERSS. Un dispositivo de AERSS observa el tráfico a través de varios puntos en la red para verificar si hay actividad malintencionada. Las consideraciones para saber dónde conectar el puerto de monitoreo serían:

- Interfaces internas de firewalls perimetrales para permitirles bloquear el "ruido" excesivo del internet y que así se pueda monitorear solo el tráfico que pasa

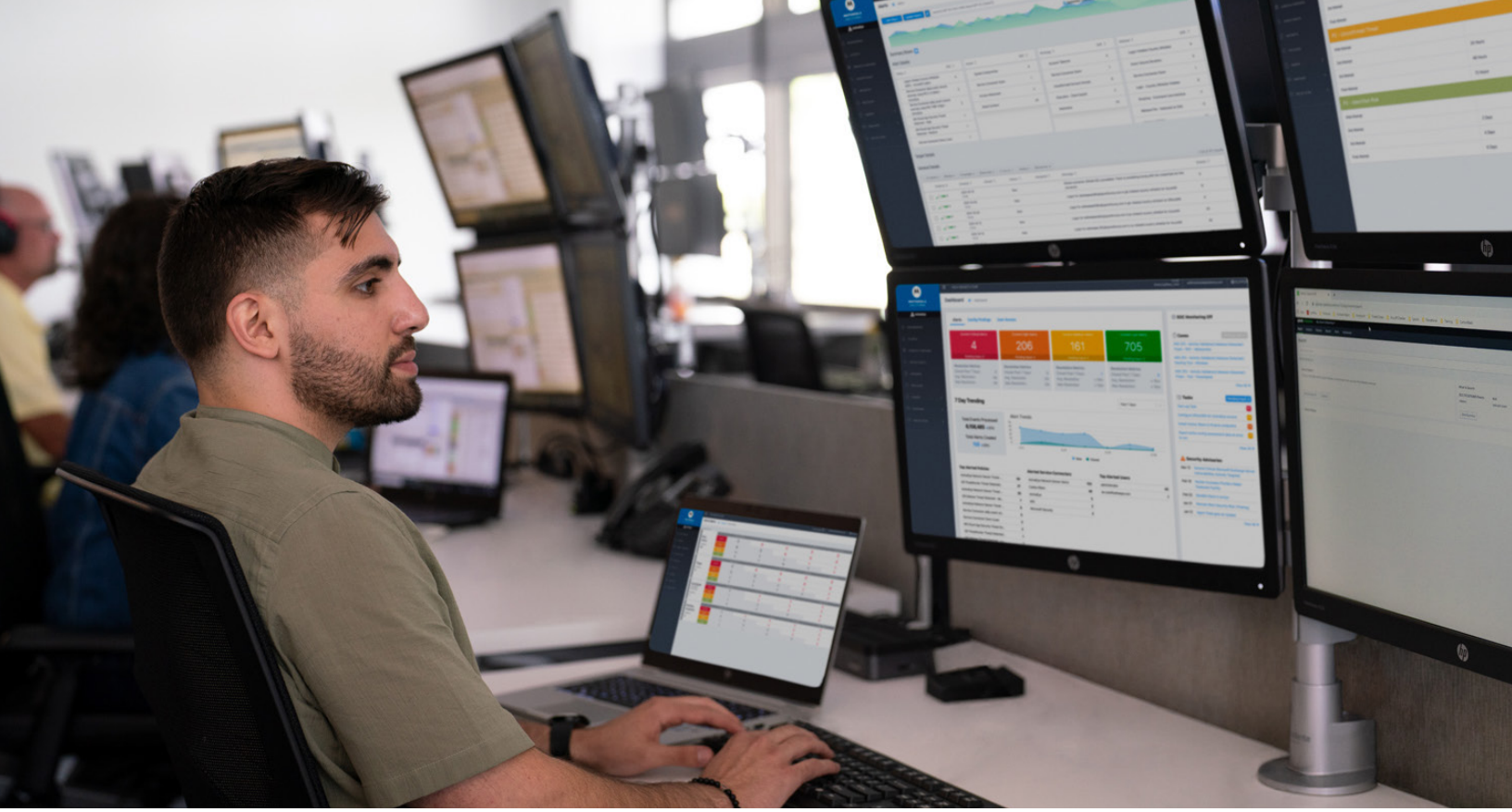
- Las redes y servidores internos que contengan datos sensibles para garantizar que se monitoreen las comunicaciones entre dichos sistemas u otros cuellos de botella internos en la red, incluyendo las conexiones de las oficinas o socios/proveedores remotos.

Otra consideración sería recolectar las bitácoras de los dispositivos dentro de la red. Los sistemas o dispositivos de red habitualmente reenvían bitácoras a través de syslog hacia el dispositivo de AERSS para su recopilación y reenvío a ActiveEye.

La última consideración sería escanear la red en los ambientes aplicables. Esto requiere que el dispositivo de AERSS escanee la red en busca de vulnerabilidades. Las consideraciones para saber dónde conectar el puerto de administración serían:

- Una ubicación dentro de la red, para facilitar el escaneo sin cambiar los controles de red que se podrían requerir cuando se escaneen los firewalls u otros controles de seguridad que podrían afectar el escaneo.

- Para agregar seguridad, el puerto de administración puede estar más aislado. De ser el caso, para su configuración, se requiere una configuración precisa de tráfico saliente para escanear las redes deseadas. Esto es necesario para que el descubrimiento de los escaneos y otras verificaciones identifiquen los sistemas en vivo correctamente en la red en vez de dar falsos positivos.



USO DE ANCHO DE BANDA DEL AERSS

El dispositivo de AERSS utiliza ancho de banda para diversos propósitos. Podría afectar la red en los ambientes con ancho de banda limitado. La consideración principal del ancho de banda es para el internet, el cual se utiliza para la instalación, administración y recopilación de bitácoras del dispositivo de AERSS. Como mínimo, el dispositivo debe tener disponible una conexión de 10Mbps al internet.

Como segundo punto, existen consideraciones de ancho de banda dentro de la red, las cuales podrían afectar la cantidad o la colocación de los dispositivos de AERSS. Las siguientes funciones pueden afectar los requisitos del ancho de banda internos al ambiente:

- Recopilación de bitácoras de los dispositivos — La entrega de las bitácoras de los dispositivos en el otro lado de una conexión de red con ancho de banda bajo podría resultar afectada.
- Escaneo de red — El escaneo de una red con una conexión de ancho de banda baja podría incrementar los tiempos de escaneo o afectar otro tipo de tráfico que utilice esa conexión.
- Monitoreo de red — Si el tráfico de red que se está replicando para el monitoreo no utiliza una conexión dedicada, entonces podría afectar otros tipos de tráfico. Recomendamos utilizar siempre una conexión directa y dedicada desde el switch que replique el tráfico al dispositivo de AERSS.

ASPECTOS DESTACADOS DE LA SEGURIDAD DE AERSS

El dispositivo del AERSS también cuenta con características de seguridad integradas, que incluyen:

- Actualizaciones — Todo el software del AERSS se administra en la nube y se actualiza frecuentemente para garantizar que se mantenga actualizado y seguro. Esto incluye al firmware, los sistemas operativos, las aplicaciones y los parches.
- Certificados — El dispositivo de AERSS utiliza certificados para asegurar las configuraciones que se aplican a la plataforma.
- Claves de API — Los datos de las bitácoras que se procesan mediante la plataforma se autentican en ActiveEye utilizando claves de API dedicadas que se cambian frecuentemente para agregar seguridad.
- Fortalecimiento de plataforma — La plataforma base del dispositivo de AERSS ejecuta un sistema operativo fortalecido.
- Monitoreo de plataforma — Las bitácoras del dispositivo de AERSS se incluyen en el monitoreo del ambiente.
- Comunicación — El AERSS utiliza cifrado para todos los datos en tránsito. Todas las comunicaciones del dispositivo de AERSS emplean cifrado para garantizar que los datos sensibles se protejan contra el espionaje potencial.

CENTRO DE OPERACIONES DE SEGURIDAD

El Centro de Operaciones de Seguridad (SOC) de Motorola Solutions puede monitorear redes, aplicaciones y dispositivos contra amenazas de seguridad por 24/7 a través de ActiveEye. Nuestros analistas del SOC tienen habilidades técnicas superiores tanto de lado defensivo como en el ofensivo de la seguridad. Con base en su amplia experiencia de seguridad, nuestros analistas del SOC recomiendan configuraciones de seguridad de dispositivos que optimizan la detección de amenazas e implementan tácticas para sobrepasar el ruido y tratar las amenazas más críticas rápidamente. Esto coloca nuestro enfoque en la identificación de las actividades que podrían ser un riesgo o incidente de seguridad potencial.

El SOC utiliza la capacidad de ActiveEye para priorizar las alertas en cola y se enfoca en aquellas con mayor probabilidad de dar como resultado un incidente o riesgo de seguridad. El equipo administrativo del SOC monitorea regularmente los SLA internos y ha establecido KPI internos para garantizar que las alertas se investiguen a tiempo.

Nuestro SOC trabaja frecuentemente con clientes nuevos que están en proceso de mitigar y recuperarse de cualquier riesgo. Utilizando las herramientas de EDR, el equipo detecta, investiga y detiene activamente a quienes realizan las amenazas y a sus ataques. Cuando se identifica actividad sospechosa, el equipo tiene experiencia para mitigar e interceptar las amenazas rápidamente antes de que se aprovechen activamente.

Si la investigación de una amenaza requiere la acción de su equipo de seguridad, el SOC creará un caso de seguridad y seguirá los procedimientos de escalamiento predeterminado para cada nivel de prioridad. Si el SOC no puede ponerse en contacto con el primer nivel, este escalará de acuerdo con los procedimientos definidos por el cliente. ActiveEye le permite ver los casos de seguridad y el historial de investigación de eventos en cualquier momento. El SOC siempre está disponible para proporcionar asesoría adicional sobre cualquier caso de seguridad, revisar los detalles de estos a profundidad o proporcionar asistencia adicional con las investigaciones conforme se requiera.

En caso de que exista un incidente potencial, el SOC utilizará los datos disponibles en ActiveEye y accederá a su sistema para determinar la magnitud de la actividad malintencionada. De ser necesario, el SOC agregará más políticas de detección a los módulos de su servicio. Con el módulo de servicio de EDR, el SOC puede tomar acciones de mitigación en los sistemas de hosts remotos con base en un plan de respuesta preaprobado o, si lo consideran necesario, para un caso en específico. Conforme se necesite, el SOC recomendará acciones de mitigación que usted puede realizar para atender a una amenaza.

El tiempo es esencial cuando se trata de las investigaciones y respuestas de seguridad. La mayoría de los riesgos iniciales darán como resultado un movimiento lateral si no se detectan y mitigan dentro de los primeros 60 minutos. El SOC monitorea el tiempo de resolución de sus alertas de seguridad minuciosamente como medida conjunta de nuestra capacidad de interactuar y responder a las actividades de su ambiente. Estas métricas y tendencias en los tiempos de respuesta están disponibles en su tablero de ActiveEye y en su reporte mensual.

Los analistas se capacitan frecuentemente para entender la privacidad y administración de datos del cliente para así proteger sus datos sensibles.

El equipo del SOC participa rutinariamente en ejercicios de equipo rojo y morado y utiliza plataformas de capacitación sofisticadas para garantizar que sus habilidades estén al día. Nuestros analistas superiores desarrollan y llevan a cabo ejercicios prácticos que simulan la actividad de los atacantes y las violaciones de seguridad modernas para capacitar al resto de los analistas del SOC.

Los números de ActiveEye: Detección y prevención del malware*

2,078
muestras únicas de malware

QUE DAN COMO RESULTADO

6,392
ACCIONES DE RESPUESTA implementadas

QUE EVITAN QUE

658,199
procesos SE EJECUTEN

¿Qué veremos en una alerta del SOC?

- Lo que encontramos
- Notas del analista
- Cuándo lo encontramos
- Dónde lo encontramos
- Lo que hicimos
- La respuesta recomendada
- Detalles técnicos

*Datos del 2021

Planeación de seguridad estratégica e información expandida

Recomendaciones mensuales del programa de seguridad y revisión

Análisis de tendencias y búsqueda de amenazas

Búsqueda en la red profunda y oscura

Analista de seguridad asignado

PERSPECTIVAS AVANZADAS SOBRE LAS AMENAZAS

Las perspectivas avanzadas sobre las amenazas de ActiveEye es un servicio opcional que expande los servicios de monitoreo estándar del SOC que proporciona la MDR de ActiveEye. Este servicio proporciona una función de investigación de seguridad a profundidad más proactiva para enriquecer la concientización de su postura continua de ciberseguridad, optimizar el valor de los controles de seguridad existentes y, finalmente, disminuir el riesgo de ciberseguridad.Recomendaciones mensuales del programa de seguridad y revisión Análisis de tendencias y búsqueda de amenazas.

Con el servicio de perspectivas avanzadas sobre las amenazas, Motorola Solutions asignará a un analista de ciberseguridad para que trabaje proactivamente con usted y con su equipo. El analista llevará un programa avanzado de búsqueda de amenazas para identificar aquellas avanzadas y específicas y resumir los patrones de amenazas en evolución que sean de interés. El analista asignado utilizará el MDR de ActiveEye y las herramientas conectadas para buscar los datos de las bitácoras de seguridad en la nube, redes y terminales en busca de evidencia de los riesgos no detectados para la red. Con base en la información sobre amenazas externas relevantes o de las entidades de alto riesgo (las cuentas de usuario o sistemas) que identifique su equipo o ActiveEye, el analista asignado buscará externamente en la web superficial, profunda y oscura en busca de amenazas de ciberseguridad para su red. Las amenazas potenciales incluyen las cuentas de usuario corporativas puestas en riesgo, las direcciones IP corporativas conectadas a las botnets y los datos a la venta.

Cada mes, el analista asignado se reunirá con su equipo de seguridad para proporcionar un resumen de cualquier amenaza que se detecte en el mes anterior y así debatir sobre la estrategia de seguridad que se adoptará en lo subsecuente. También le compartirá un reporte resumido de los resultados de la búsqueda de amenazas y el descubrimiento y mitigación de las amenazas descubiertas.

Aunque el servicio de perspectivas avanzadas sobre las amenazas ofrece información a profundidad de la red superficial, profunda y oscura, diariamente se crean foros clandestinos nuevos en donde los actores comercian con la información y los datos. Como tal, no podemos garantizar la cobertura de todas y cada una de las amenazas en tiempo real, ya que algunos de estos foros y comunidades clandestinas pueden hacerse notar o los investigadores pueden acceder a ellos dentro de meses. Adicionalmente, el alcance de estos servicios no incluye los servicios de investigación relacionados con los empleados, tales como aquellos que podrían dirigirse a trabajadores específicos (u otros individuos) o que impliquen derechos de privacidad, sospecha o presunción de conducta interna indebida o los derechos que podrían estar protegidos o regulados por la ley.

UN SOLO SOCIO PARA TODAS SUS NECESIDADES DE CIBERSEGURIDAD

EXPERIENCIA Y ESCALA GLOBALES

Con más de 90 años de experiencia administrando las tecnologías esenciales y más de 20 años de desarrollar soluciones de ciberseguridad, Motorola Solutions está bien posicionado para ser el único proveedor de servicios para sus necesidades de ciberseguridad.

Con el mejor personal, procesos y tecnología de su clase, proporcionamos operaciones escalables que pueden ayudar a que las organizaciones administren la concientización de los ciber-riesgos, su detección, respuesta y recuperación. Nuestra plataforma de organización y automatización de seguridad vanguardista, ActiveEye, proporciona información 24/7 sobre las amenazas potenciales a su ambiente, así como un enfoque coadministrado para la gestión de seguridad. Proporcionamos un enfoque integrado y creado según sus propósitos para la ciberresiliencia de extremo a extremo.

Visítenos en motorolasolutions.com

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com