proofpoint

CASO DE CLIENTE

Una empresa energética refuerza sus defensas con Proofpoint

El desafío

- Aumentar la visibilidad de las amenazas para la seguridad en la infraestructura y activos críticos.
- Acelerar la identificación de amenazas y mejorar la respuesta a incidentes.
- Mejorar la capacidad de recopilar datos forenses.

La solución

Proofpoint Identity Threat Defense

- Proofpoint Shadow

Los resultados

- Recepción exclusiva de alertas positivas de la actividad de ataque.
- Visibilidad de la actividad del atacante en tiempo real.
- Reducción del tiempo de investigación en dos tercios.
- Obtención de datos forenses detallados de manera instantánea, facilitando las acciones con pruebas irrefutables.
- Desarrollo de una verdadera alianza con Proofpoint a través del ciclo de vida de desarrollo.

La organización

Esta organización proporciona servicios energéticos y relacionados a millones de consumidores y partners en todo el mundo. Se trata de una empresa multinacional que además lleva a cabo actividades de exploración y producción de energía. Dado que la energía es esencial para la vida y la seguridad nacional, la empresa recurre a la innovación tecnológica, creando productos, aplicaciones y servicios avanzados. Con la seguridad como prioridad principal, la empresa se puso en contacto con Proofpoint para incorporar funciones exclusivas de detección de actividad maliciosa y ofrecer información forense instantánea.

El desafío

Para una empresa energética, uno de los mayores desafíos de seguridad es sin duda proteger su compleja superficie de ataque. Esta empresa cuenta con infraestructura en cliente y en la nube, así como una red y dispositivos críticos SCADA (control de supervisión y adquisición de datos). Tener varios partners externos requiere numerosas conexiones de entrada y salida de red. El enfoque en DevOps también requiere proteger los endpoints para una gran comunidad de desarrolladores, así como el código de las aplicaciones y los sistemas de prueba. Como proveedor de energía, el cumplimiento con las normativas del sector, el Reglamento General de Protección de Datos (RGPD), y otros requisitos de seguridad precisa una visibilidad clara de la infraestructura de seguridad y la capacidad de capturar telemetría en caso de que se detecte una amenaza.

Este empresa ya contaba con un enfoque de defensa en profundidad de la seguridad y trabaja permanentemente en implementar y mejorar las mejores prácticas. Antes de Proofpoint habían sido muchas las ocasiones en las que usuarios internos habían activado alertas desde sistemas de seguridad de la empresa. Cuando el equipo del SOC recibía una alerta, tenían que obtener el portátil del usuario e investigar manualmente, revisando los registros del sistema y reconstruyendo minuciosamente los datos forenses necesarios para conocer lo sucedido. Asumiendo que el SOC pudiera acceder rápidamente al portátil, la investigación podía llevar horas. Para mejorar la capacidad de respuesta, le empresa lanzó una iniciativa de seguridad centrada en la protección de los equipos portátiles y las estaciones de trabajo.

La solución

La empresa exploró inicialmente tecnologías honeypot tradicionales, pero descubrió la tecnología de engaño basada en endpoints de Proofpoint Identity Threat Defense durante el proceso de búsqueda de soluciones. Proofpoint Shadow fue la solución elegida.

"En un primer momento, pensé que Proofpoint Shadow era como un honeypot", afirma el responsable de seguridad de la información. "No tardé en darme cuenta de que el enfoque de Proofpoint era mucho más sofisticado".

Los engaños sin agente y basados en inteligencia en cada endpoint de Proofpoint Shadow están diseñados para imitar datos, credenciales y conexiones reales. Ahora, cuando un ciberdelincuente (o usuario interno con acceso de red legítimo) intenta infiltrarse en los sistemas, se enfrenta a una gran cantidad recursos falsos con apariencia real. Elegir un camino seguro e indetectable se hace casi imposible, y un paso en falso alerta al SOC de su presencia. Una vez se activa el engaño, el sistema empieza a recopilar datos forenses detallados de los sistemas en los que el ciberdelincuente actúa, a fin de ofrecer datos precisos y en tiempo real para ofrecer una respuesta rápida e informada.

"Proofpoint redujo el tiempo de investigación en dos tercios. El panel gráfico nos muestra dónde se encuentra el atacante respecto a los activos críticos. Podemos examinar rápidamente los detalles específicos, y el sistema proporciona automáticamente una cronología de lo que ha ocurrido en el endpoint. Tiene un valor incalculable".

Responsable de seguridad de la información, empresa energética

La empresa energética desplegó Proofpoint Identity Threat Defense en todo su entorno con la ayuda de su proveedor de servicios gestionados y los servicios profesionales de Proofpoint. Inmediatamente, la solución identificó rutas clave a los activos críticos y varios errores de configuración de sistemas heredados que representaban vulnerabilidades.

"Proofpoint Identity Threat Defense es enormemente útil", afirma el responsable de seguridad de la información. "Recopila inteligencia de los endpoints y sugiere una lista de los engaños más adecuados, lo que ahorra tiempo y mejora de manera importante nuestras defensas. También estamos impresionados con el equipo de Proofpoint. Escuchan nuestras necesidades con paciencia, nos ayudan a adaptar las defensas a nuestro entorno y son muy receptivos".

Los resultados

Una vez desplegada la solución de Proofpoint, detectamos inmediatamente instancias en las que un adversario intentaba infiltrarse en los sistemas y activaba un engaño. Ahora el equipo del SOC puede ver y vigilar la actividad de los atacantes en tiempo real. Al mismo tiempo, el análisis forense en tiempo real pone a disposición del equipo del SOC inteligencia sobre los ataques, lo que les permite examinar rápidamente detalles específicos, sin que el atacante sepa que está siendo investigado. El equipo de respuesta a incidentes puede determinar rápidamente dónde centrar su investigación, gracias al conocimiento de las herramientas que utiliza el atacante. Las alertas de Proofpoint se envían simultáneamente al sistema ServiceNow de la empresa, lo que permite optimizar las asignaciones de los analistas, la priorización de respuestas y la gestión de incidentes.

"Antes, no habríamos tenido conocimiento de esta actividad", afirma el responsable de seguridad de la información. "Habríamos necesitado alertas de varias capas de seguridad y tiempo para comprobar que la alertas eran positivas. A partir de ahí, habríamos tenido que poner en cuarentena y confiscar el portátil antes de poder investigar y recopilar pruebas".

Un verdadero punto de inflexión

"La telemetría ha supuesto un punto de inflexión", continuó. "Proofpoint Identity Threat Defense redujo el tiempo de investigación en dos tercios. El panel gráfico nos muestra dónde se encuentra el atacante respecto a los activos críticos. Podemos examinar rápidamente los detalles, y el producto automáticamente nos proporciona una cronología de lo que ha ocurrido en el endpoint. Tiene un valor incalculable".

La telemetría del producto también proporciona pruebas irrefutables. Si el atacante es un usuario malicioso, la empresa puede determinar inequívocamente lo que ocurrió y adoptar las medidas necesarias. Con un mayor número de intentos de ataque externos más habituales, la empresa dispone ahora de datos detallados sobre los objetivos y las técnicas del atacante, de manera que puede reforzar las defensas donde sea necesario.

Fundamental para el futuro

La necesidad de proteger plantas remotas, un entorno SCADA y dispositivos IoT, hace que la empresa energética tenga previsto utilizar Proofpoint Identity Threat Defense para ampliar su enfoque de seguridad de defensa en profundidad para estos activos.

"Proofpoint Identity Threat Defense es una herramienta fundamental", asevera el responsable de seguridad de la información. "Ha sido muy eficaz para nuestra empresa. Si, por alguna razón, tuviéramos que racionalizar nuestras herramientas de seguridad, sería la última de la que nos desharíamos".

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.