



Forcepoint crea una unidad de negocio basada en las infraestructuras críticas

La formación de la nueva unidad de negocio de Infraestructuras Críticas abordará el desafío de equilibrar la detección de amenazas internas y la seguridad de datos con la disponibilidad de sistemas de control industrial y de dispositivos IoT conectados.

Forcepoint, líder mundial en ciberseguridad, ha anunciado la creación de una nueva unidad de negocio para hacer frente a los desafíos de seguridad que tienen los proveedores de infraestructura crítica debido a las amenazas tan sofisticadas que existen actualmente. El negocio de Infraestructura Crítica de Forcepoint aprovechará el conjunto de capacidades de las agencias gubernamentales globales y de la seguridad empresarial para ofrecer ciberseguridad en grado de defensa, dirigido a la protección de amenazas internas y externas, la seguridad de datos y la defensa avanzada contra amenazas a la infraestructura crítica. En un principio, la compañía tiene previsto focalizarse en las organizaciones que utilicen Sistemas de Control Industrial (ICS) tales como energía, petróleo y gas, y fabricación crítica.

Con 20 años de experiencia protegiendo entornos de alta seguridad, Forcepoint es la única compañía que puede abordar las amenazas de infraestructura crítica donde existen más vulnerabilidades –el punto humano de interacción con los sistemas y los datos–. La compañía ofrecerá un portfolio de ciberseguridad integrada con contenido relevante para el espacio industrial, que se centrará inicialmente en soluciones de seguridad de red diseñadas para entregar una mayor visibilidad de las amenazas más sofisticadas, las cuales pueden afectar a los sistemas de control industrial.

La conexión de Tecnología Operacional (OT) como los ICS o los Sistemas de Control, Supervisión y Adquisición de Datos (SCADA, por sus siglas en inglés) pueden ofrecer a la red de TI nuevos niveles de funcionalidad, ahorro de costes y transparencia para aprovechar el big data y la información analítica. Esta dependencia de los dispositivos conectados también amplía exponencialmente la superficie de ataque del entorno OT dentro de la infraestructura crítica. La combinación de atacantes

sofisticados que conocen cómo interrumpir un proceso físico a través de la frecuencia de ataques dirigidos a usuarios con acceso de confianza a información confidencial aumentan los desafíos que enfrentan a CISOs con operadores de plantas industriales para definir quién es el encargado de cada área. Según el informe de Gartner '2018 Strategic for Integrated IT and OT Security', publicado el 3 de mayo, "para 2021, el 70% de la seguridad OT será dirigida directamente por el CIO, el CISO o el CSO. Actualmente, esta cifra tan sólo alcanza el 35%".

"La relativa facilidad y bajo coste actual de los ciberataques a través de las fronteras está derivando en una crisis en la infraestructura crítica, donde tanto la tecnología de la información como la de operación tienen que unirse rápidamente", afirma Sean Berg, Vicepresidente y Director General de Agencias Gubernamentales Globales e Infraestructura Crítica de Forcepoint. "Estas industrias proporcionan servicios esenciales que sustentan a la sociedad. Por ello, necesitan tener el control de acceso a la planta o a la red eléctrica para proteger a sus usuarios y a los datos críticos. El enfoque más efectivo y holístico requiere una visión de comportamiento para proporcionar automáticamente contramedidas de seguridad sin afectar a la disponibilidad y evitar así la intrusión en sistemas críticos".

Segmentación de red para proteger los entornos industriales

[La oferta de Infraestructura Crítica](#) de Forcepoint se basa en décadas de experiencia proporcionando soluciones de seguridad para proteger las redes gubernamentales sensibles y la conectividad segura a Internet. Estas soluciones se adaptarán para cumplir con los requisitos de los entornos industriales, proporcionando una segmentación segura con el fin de satisfacer las necesidades operativas. Por ejemplo, partners que requieran acceso remoto para monitorear amenazas dentro de los entornos industriales. La solución de Forcepoint permite a los operadores de infraestructura crítica tener la seguridad de un firewall y una transferencia de datos segura y unidireccional en las áreas más sensibles, al mismo tiempo que garantiza el cumplimiento de los estándares [NERC-CIP](#), [NEI-08-09](#) e [ISA/IEC 62443](#).

[Forcepoint NGFW](#) proporciona seguridad, rendimiento y operaciones consistentes en los sistemas físicos, virtuales y cloud. Dispone de tres fases de defensa de red: derrotar las evasiones, detectar las vulnerabilidades y detener el malware. Esto proporciona un rápido descifrado del tráfico cifrado, incluyendo conexiones web HTTPS, junto con controles de privacidad granular que mantienen a las organizaciones y a los usuarios seguros en un mundo que cambia rápidamente.

[Forcepoint Data Guard](#) puede validar todas las transferencias de datos en las aplicaciones y las capas de datos, permitiendo sólo comandos válidos y conjuntos de datos necesarios para las operaciones.

El flujo de datos entre las operaciones y las redes de información puede ser auditado y controlado a través de una conexión unidireccional, proporcionando un alto nivel de seguridad y confiabilidad a las industrias altamente reguladas, por ejemplo, las plantas de energía nuclear.

Estos productos de seguridad de red forman parte del portfolio de Human Point System de Forcepoint que permite a los ICS, a las agencias gubernamentales y a las organizaciones empresariales 'empezar en cualquier lugar' para satisfacer las necesidades de seguridad de datos y de usuarios a través de [amenazas internas](#), [analíticas de comportamiento centradas en los seres humanos](#), [prevención de pérdida de datos](#), [tecnologías de seguridad cloud \(CASB\)](#) y seguridad [web/email](#). Las innovaciones de ciberseguridad de Forcepoint se integran sin problema en un sistema de gestión unificada de políticas o en entornos cloud o locales ya existentes.

El ex ejecutivo de Intel/McAfee y Belden liderará la división de Infraestructura Crítica de Forcepoint

David Hatchell liderará esta nueva línea de negocio de Forcepoint como vicepresidente de Infraestructura Crítica y reportará a Sean Berg. Veterano de las industrias de tecnología y seguridad, Hatchell dirigió el área de infraestructura crítica de Intel/McAfee y de Belden. La línea se focalizará en adaptar las soluciones de Forcepoint a los requisitos, desafíos y mercados de infraestructura crítica.



Contacto de prensa:

JAVIER MODUBAR ALVAREZ

info@ingecom.net

944395678

<http://www.ingecom.net>