LA ENCUESTA DE FORTINET REVELA IDEAS CRÍTICAS PARA ABORDAR LA CRECIENTE BRECHA DE HABILIDADES

Por Sandra Wheatley | 27 de Mayo de 2020

La brecha de habilidades en Ciberseguridad continúa planteando desafíos para organizaciones de todos los tamaños y en todas las industrias, además los cambios en la economía, como resultado de la pandemia de COVID-19, están agravando la brecha de habilidades. A medida que el concepto de trabajo remoto se convierta en norma y las infraestructuras se distribuyan aún más, la necesidad de profesionales de TI que tengan habilidades y conocimientos de seguridad oportunas solo crecerá.

Además de las estrategias de teletrabajo a tiempo completo que cambian la forma en que las organizaciones administran la seguridad, hay otro factor que ha sido un motor significativo detrás de la brecha de habilidades: la innovación digital. A medida que las organizaciones adoptan nuevas tecnologías para mantenerse competitivas y garantizar la continuidad del negocio, su superficie de ataque se expande, abriendo la puerta para que los cibercriminales exploten los entornos de red. Este potencial de ataque resulta en una necesidad sustancial de talento especializado en seguridad cibernética. Pero a medida que el número de profesionales sigue estancado, la demanda de su experiencia para abordar nuevos segmentos de la red distribuida continúa creciendo.

Comprendiendo el impacto generalizado de la brecha de habilidades en Ciberseguridad

Fortinet comisionó recientemente un informe que destaca los resultados de una encuesta realizada por MaritzCX a personas responsables de la ciberseguridad en sus organizaciones. El objetivo fue comprender el verdadero alcance e impacto de la brecha de habilidades. Este informe de Fortinet arroja luz no solo sobre los desafíos que enfrentan los trabajadores directamente afectados por este problema, sino también sobre lo que se puede y se debe hacer para abordar la brecha de habilidades.

El informe destaca las siguientes tres tendencias.

Todos los tipos de organizaciones se ven afectadas

Los participantes que respondieron a esta encuesta reiteraron una verdad ampliamente conocida sobre la brecha de habilidades en seguridad cibernética: este problema afecta a las organizaciones en todas las partes del mundo. El 68% de los encuestados informaron que sus empresas luchan por reclutar, contratar y retener talentos en seguridad cibernética. El tema es aún más grave en Canadá, donde el 78% dijo que sus organizaciones enfrentaban estos desafíos. Cuando se considera que el 76% de los encuestados señaló que la falta de profesionales de seguridad calificados está creando nuevos riesgos en sus organizaciones, queda claro que la brecha de habilidades es más que un problema teórico.

Aproximadamente el 73% de los encuestados informó haber tenido al menos una intrusión o alerta en su organización durante el año pasado como resultado directo de la escasez de profesionales de seguridad calificados, y el 47% señaló haber tenido hasta tres en los últimos 12 meses. Sin un equipo de seguridad completamente integrado, las organizaciones corren el riesgo de perder datos de clientes, información de empresas privadas o secretos comerciales.

Según los encuestados, los trabajadores en arquitectura de seguridad y arquitectura de seguridad en la nube se encuentran entre los roles de trabajo más difíciles de completar. Esto probablemente se deba a la gran demanda de individuos y a que las redes de la mayoría de las organizaciones se están volviendo cada vez más complejas debido a labores como operar nubes dinámicas y la priorización de la seguridad en estos entornos. Sin embargo, los administradores de seguridad, una posición de nivel básico, también se encuentran dentro de los tres roles más difíciles de completar. Para combatir este desafío, las organizaciones promueven en gran medida roles como éste en los sitios de trabajo y se centran en la retención al ofrecer salarios altos, maximizar las oportunidades de avance y proporcionar una cultura laboral saludable.

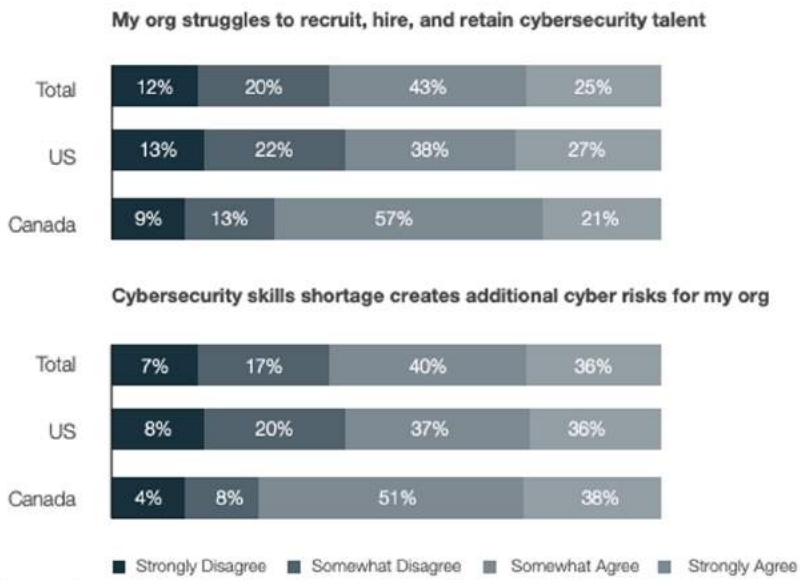

Figura 1: Dificultades de reclutamiento y riesgos cibernéticos relacionados para las organizaciones.

Las organizaciones reconocen el valor de las Certificaciones de Seguridad

Los datos resaltados en este informe ilustran la necesidad de que las organizaciones vayan más allá de los medios tradicionales de reclutamiento de talentos para cumplir roles de seguridad. Estos incluyen a los empleadores que consideran altamente a las personas con certificaciones orientadas en la tecnología, ya que reconocen que tales certificaciones demuestran conocimiento y experiencia en varios conceptos de seguridad cibernética.

Estas certificaciones también proporcionan valor a aquellos que ya están dentro de los roles de seguridad, el 81% de los encuestados que han obtenido certificaciones ellos mismos, y el 85% reportó tener colegas en sus equipos que están certificados. Este valor se ejemplifica aún más por el hecho de que el 94% declaró que sus certificaciones ayudaron a prepararlos mejor para sus roles actuales. Teniendo en cuenta estas respuestas, no sorprende que la mayoría de las organizaciones (82% de los encuestados) prefieran contratar candidatos que tengan certificaciones que validen su entendimiento y conocimiento de la ciberseguridad.

El campo de la seguridad cibernética está cambiando constantemente, y las certificaciones son una forma valiosa de mantenerse al día frente al panorama de amenazas en evolución, así como permitir a quienes se encuentran sin antecedentes técnicos obtener capacitación para pasar a una carrera en seguridad cibernética. Las certificaciones también pueden basarse en el valor de los estudios universitarios al ayudar a los profesionales a actualizar sus conocimientos de seguridad cibernética cada vez que los decidan renovar. También pueden ayudar a los candidatos no tradicionales a pasar a una carrera de seguridad cibernética al proporcionarles el conocimiento que necesitan para tener éxito en una variedad de roles de nivel fundamental. Al enfatizar el valor de las certificaciones, las organizaciones pueden ampliar su grupo de talentos para cubrir candidatos no tradicionales, profesionales graduados de otros campos y otros grupos que pueden no haber sido considerados en el pasado.

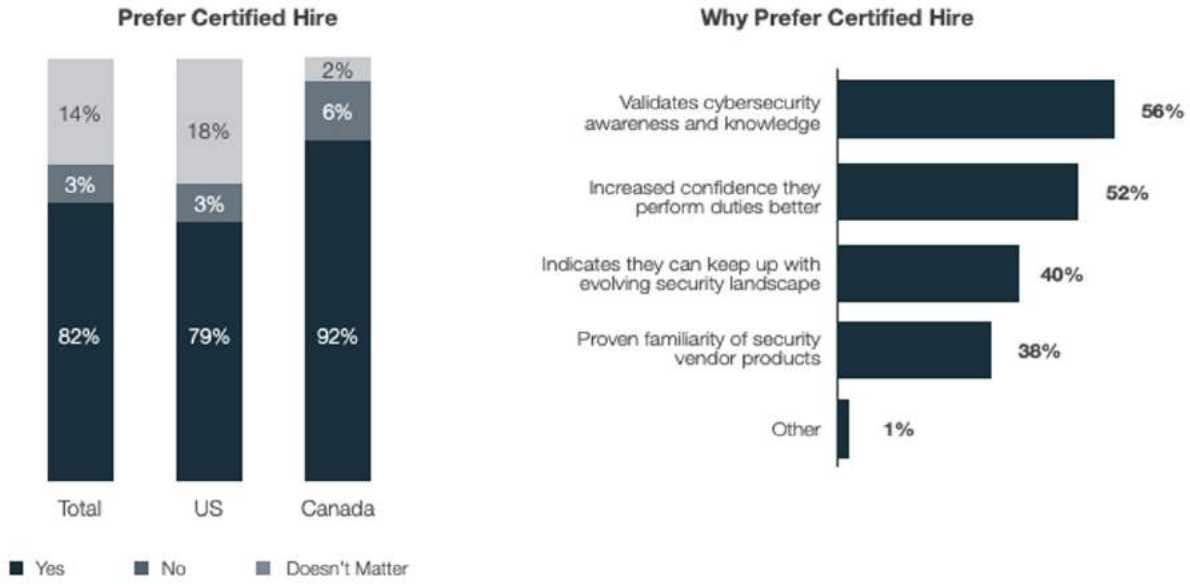

Figura 2: Importancia de las certificaciones en la contratación..

Figura 3: Beneficios percibidos de la certificación.

Los veteranos juegan un papel crítico para cerrar la brecha de habilidades

Al abandonar el servicio activo, los miembros del servicio militar pueden proporcionar un valor significativo al campo de la seguridad cibernética con las habilidades y rasgos que desarrollaron durante sus años de servicio que complementan la industria. El informe de Fortinet encontró que la mayoría de las organizaciones reconocen este valor, y el 57% de los encuestados de los Estados Unidos señalaron que su equipo de ciberseguridad había contratado al menos a un veterano. Si bien los roles de los veteranos varían, casi la mitad (45%) hizo la transición a sus carreras civiles al comenzar como administradores de seguridad o especialistas en SOC (System-on-Chip).

Fuera del ámbito de las posiciones de nivel básico, el 43% de los encuestados estadounidenses declararon que al menos un ejecutivo de la C-suite (grupo de CEOs) en su organización es veterano o está casado con uno, la mayoría (80%) que cae dentro de esta categoría trabajó o ha trabajado para su empresa durante al menos cinco años.

Por lo general, estos trabajadores demuestran una fuerte ética de trabajo, atención al detalle y tienen éxito en entornos acelerados y de alto estrés, como lo señalan sus colegas (40%).

A pesar de la presencia de veteranos en roles de seguridad cibernética y puestos de dirección ejecutiva, solo el 49% de los encuestados de EE. UU. informó que sus organizaciones tienen un programa de contratación específico para veteranos, y solo el 22% tiene uno específico para cónyuges militares. Debido a que los veteranos y sus cónyuges pueden desempeñar un papel vital en cerrar la brecha de habilidades de seguridad cibernética, las organizaciones tienen la oportunidad de hacer más para reclutarlos para cumplir roles críticos. Para aprovechar al máximo lo que estos individuos tienen para ofrecer, las organizaciones deben invertir en los recursos apropiados para aprovechar al máximo sus conjuntos de habilidades especializadas, esto incluye programas de capacitación y procesos de contratación específicos.

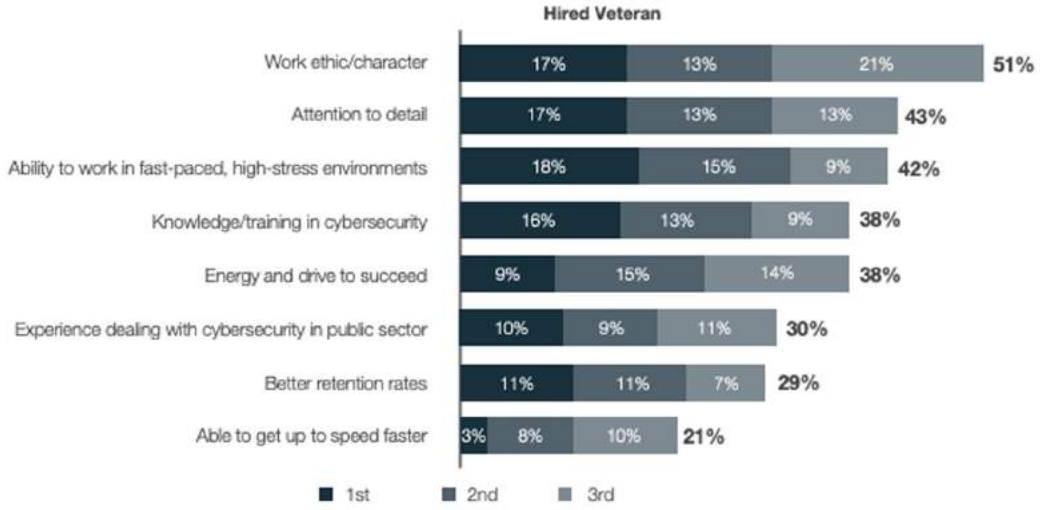

Figura 4: Atributos sobresalientes de los veteranos en las organizaciones de los participantes encuestados.

Abordar la escasez de talentos necesita de la intervención de todos

La brecha de habilidades de seguridad cibernética es efectivamente real, impacta a las organizaciones incrementando el potencial de violaciones de datos e intrusiones en la red. Este informe de Fortinet no solo demuestra la realidad de la escasez de talento, sino que también revela lo que las organizaciones pueden hacer para construir y fortalecer a sus equipos, al enfatizar la importancia de las certificaciones tanto para los nuevos empleados como para los miembros actuales del equipo, incluida la contratación de veteranos para desempeñar funciones críticas. Las empresas en todas las industrias deben reforzar sus estrategias de seguridad y al mismo tiempo ayudar a cerrar la brecha de habilidades. El Instituto de expertos en Seguridad de Redes (Network Security Expert) de Fortinet imparte el programa de certificación y capacitación NSE y el programa de Veteranos de Fortinet (FortiVet) para hacer precisamente eso.

Además, las alianzas entre empresas, gobiernos, academias y ONG son críticas para cerrar la brecha de habilidades. Reconociendo el importante papel que desempeñan tanto el sector público como el privado, en Fortinet nos hemos centrado en construir alianzas estratégicas con organizaciones como el Foro Económico Mundial (World Economic Forum) socio fundador de su Centro de Seguridad Cibernética, así como con la Alianza Global de Amenazas, CompTIA (Global Threat Alliance) y múltiples programas de investigación universitaria para abordar la escasez de talento. Como empresa de tecnología y una organización de aprendizaje, Fortinet se compromete a resolver la escasez de habilidades que afecta a nuestra industria a través de nuestros programas y asociaciones del Instituto NSE (Network Security Expert Institute).

Más información sobre los programas del Instituto NSE de Fortinet, incluido el programa Network Security Expert , el programa Network Security Academy y el programa FortiVet, que brindan capacitación y educación sobre seguridad cibernética crítica para ayudar a resolver la brecha de habilidades cibernéticas y preparar la fuerza laboral de seguridad cibernética del mañana.