Security+ وSSCP: الجمع بين المعرفة الأساسية والجاهزية التشغيلية



يقارن مقال في Help Net Security بين شهادة Security+ التأسيسية وشهادة SSCP من ISC2 التي تقيس المهارة التشغيلية العملية، ويرى أن الجمع بينهما يخدم فرق الأمن.

- يُقدَّم Security+ بوصفه أساسًا واسعًا محايدًا للموردين يشمل المصطلحات والتهديدات والتحكم بالوصول وإدارة المخاطر وأساسيات الاستجابة للحوادث.
- تستهدف SSCP التنفيذ والإدارة العملية للبنية التقنية، وتشترط سنة من الخبرة التشغيلية التراكمية.
- يمكن لمن لا يملك الخبرة اجتياز الاختبار أولاً وأن يصبح Associate من ISC2، ثم استكمال الخبرة خلال سنتين.
- تغطي SSCP سبعة مجالات، من التحكم بالوصول ومراقبة SIEM إلى الاستجابة للحوادث والتشفير وأمن السحابة ونقاط النهاية.

- يعرض المقال الشهادتين كمرحلتين متكاملتين لا خيارين متنافسين.

يفرّق مقال نشره موقع Help Net Security، ويتضمن مادة ترويجية من ISC2 لشهادة SSCP، بين معرفة المفاهيم الأمنية والقدرة على تطبيقها تحت الضغط. ويتعامل مع شهادتي CompTIA Security+ وISC2 Systems Security Certified Practitioner (SSCP) باعتبارهما مرحلتين في مسار مهني واحد.

ما تقيسه كل شهادة بحسب المقال

يوصف Security+ بأنه أساس واسع محايد للموردين: مصطلحات مشتركة، ومثلث CIA، والتهديدات والثغرات، والتحكم بالوصول، وإدارة المخاطر، وأساسيات الاستجابة للحوادث، وأساسيات أمن الشبكات. ويشير المقال إلى أنه لا يتحقق من الخبرة العملية في بيئات العمل.

أما SSCP فتُقدَّم كخطوة تشغيلية. فهي تشترط سنة من الخبرة العملية التراكمية، أو الحصول على صفة Associate من ISC2 باجتياز الاختبار ثم استكمال الخبرة خلال سنتين. وتشمل مجالاتها السبعة التحكم بالوصول، وتحديد المخاطر ومراقبتها، والاستجابة للحوادث والتعافي، والتشفير، وأمن الشبكات، وأمن الأنظمة والتطبيقات.

الدلالة لقادة الأمن

المقال وجهة نظر متوافقة مع مصلحة الجهة المانحة، لذا ينبغي قراءة ما يقوله عن تفضيلات أصحاب العمل بهذا الاعتبار. ومع ذلك يبقى التمييز مفيدًا عند بناء فرق العمليات الأمنية أو تقييمها: فالشهادة التي تثبت المعرفة النظرية لا تثبت وحدها القدرة على احتواء حادثة أو ضبط المراقبة أو تجزئة الشبكة في بيئة الإنتاج.

ويذكر المقال أيضًا تأهيل DoD 8140 الخاص بالقوى العاملة الدفاعية الأمريكية، وهو لا يرتبط مباشرة بالمتطلبات التنظيمية في المملكة.

والخلاصة العملية للجهات المنظَّمة مواءمة الشهادات والخبرات مع متطلبات الدور الوظيفي، واختبار الحكم التشغيلي عبر التمارين لا الاكتفاء بالشهادات.

ما يجب فعله الآن

1. ربط أدوار عمليات الأمن بالمعرفة والشهادات وسنوات الخبرة العملية المطلوبة، وتوثيق هذه المعايير.
2. اعتبار الشهادات مدخلاً واحدًا، والتحقق من المهارة التشغيلية عبر تمارين الطاولة ومحاكاة الحوادث.
3. التأكد من أن العاملين في المراقبة والتحكم بالوصول والاستجابة للحوادث لديهم مسار تطوير محدد من المؤهلات الأساسية إلى التشغيلية.
4. مراجعة مواءمة متطلبات الكوادر مع توقعات ضوابط الأمن السيبراني الأساسية (NCA ECC) وإطار الأمن السيبراني للقطاع المالي (SAMA CSF) بشأن الكوادر المؤهلة.
5. تقييم ما ترد في المواد التي ترعاها الجهات المانحة للشهادات بعين ناقدة قبل اعتمادها في التوظيف أو ميزانيات التدريب.