ALJHOOD®
مجموعة الجهود المشتركة

ممارسات في تدقيق الأمن السيبراني والإمتثال للضوابط

لتعزيز إستراتيجية مؤسستك في
التعامل مع الأمن السيبرانية

لا يقتصر الأمر على التكلفة العالية التي تتحملها المؤسسة في حالة حدوث خرق، ولكن حتمية الهجوم هي التي تجعل الأمن السيبراني أمراً بالغ الأهمية، ومع تزايد عدد التهديدات السيبرانية أصبح من الضروري أن تتضمن خطة التدقيق على الأمن السيبراني في كل مؤسسة

نتيجة لذلك،

يُطلب من المدققين بشكل متزايد تدقيق عمليات وسياسات وأدوات الأمن السيبراني لتوفير ضمان بأن مؤسستهم لديها ضوابط مناسبة مطبقة، حيث تشكل نقاط الضعف في الأمن السيبراني مخاطر جسيمة على المؤسسة بأكملها – مما يجعل الحاجة إلى مدققي تكنولوجيا المعلومات على دراية جيدة في تدقيق الأمن السيبراني أكبر من أي وقت مضى

ملخص ورشة العمل والهدف منها؟

من خلال ورشة عمل تدقيق الأمن السيبراني سيتم إستعراض مفاهيم وجوانب حوكمة الأمن السيبراني وتدقيق الأمن السيبراني وإستعراض إستراتيجيات التكيف مع مخاطر الأمن السيبراني، ومناقشة أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات، وأطر العمل الأمنية لتحديد أفضل الممارسات، لمساعدة المشاركين في تحديد التهديدات ونقاط الضعف.

تقييم التهديدات بمساعدة أدوات إدارة الثغرات الأمنية، ورفع قدراتهم في التمييز بين جدار الحماية وتقنيات أمان الشبكة بغرض تحسين ممارسات إدارة الأصول والتكوين والتغيير والتصحيح، وصولاً الى مساعدة المشاركين في وضع الإطار العام لإدارة الوصول إلى المعلومات والهوية المؤسسية والمتطلبات التنظيمية السيبرانية والقانونية للمساعدة في تقييمات الإمتثال.

حوكمة الأمن السيبراني؟

توضح حوكمة الأمن السيبراني بأنّه يجب أن يكون لكل جزء من النظام المسؤول عن مخاطر أمن المعلومات مالك، أو فريق يتحمل مسؤولية ضمان أهداف هذا الجزء، حيث تُساعد حوكمة الأمن السيبراني على حماية الشركات والمؤسسات من هجمات الجهات الخارجية، أو الجهات الداخلية التي تشمل الموظفين الحاليين والسابقين من خلال تركيزها على إدارة المخاطر، وزيادة الوعي في المؤسسات، وخاصةً المؤسسات ذات النظام المعقد.

تدقيق الأمن السيبراني؟

تدقيق الأمن السيبراني هو عملية فحص أنظمة الرقابة الأمنية المطبقة في كيانات الأعمال للتأكد من توفر المعلومات وسلامتها وحماية سريتها، حيث يُغطي كافة أنظمة الرقابة وممارسات الإدارة والحوكمة والمخاطر والالتزام الرقابي المطبقة على مستوى كيان الأعمال، ويُعتبر تدقيق الأمن السيبراني من الاشياء المهمة لرواد الاعمال، وتتسأل المؤسسات عن أهمية إجراء الأمن الإلكتروني الداخلي ومدى جدوته، وكثيراً ما يُطرح السؤال التالي: "ألا تكون تقييمات المخاطر القياسية كافية لصياغة إستراتيجية أمنية لحماية الأصول الرقمية لأي مؤسسة؟"، ولكن في الواقع لا تكون تقييمات المخاطر القياسية مفيدة بشكل خاص عندما يتعلق الأمر بوضع خطة أمن واسعة النطاق ومتعمقة لمؤسستك.

ما أهمية اجراء تدقيق الأمن السيبراني؟

تعد المراجعات الذاتية السيبرانية أمراً بالغ الأهمية للمؤسسة، حيث تتيح الفرصة للقيام بما يلي:

وضع مجموعة من معايير الأمان: ستوفر نتائج المراجعة الذاتية فرصة لتحديد معايير الأمان الخاصة بك في الأمن الإلكتروني وكيفية إظهارها في المؤسسة.

للمساعدة في فرض اللوائح وأفضل الممارسات: تضمن عمليات التدقيق إتباع كل اللوائح والممارسات، وكل من معايير الأمان الداخلية وأي تشريع خارجي إلزامي.

تحديد حالة الأمن لديك: ستوضح لك المراجعة الشاملة كيفية عمل بروتوكولات الأمن الإلكتروني الحالية بطريقة لا يمكن لتقييم المخاطر القيام بها. وإلى جانب ما هو مفقود، فإن هذا من شأنه أيضاً أن يضع في الحسبان الكيفية التي تتم بها العمليات الحالية، إلى جانب الأسباب والكيفية التي يمكن بها تحسين هذه العمليات.

أهم مواضيع الورشة

- حوكمة الأمن السيبراني وأدوار ومسؤوليات الأمن السيبراني.
- الرقمنة والأمن السيبراني تحديات تواجه "التدقيق الداخلي".
- طبيعة تدقيق الأمن السيبراني (مفهوم، أهداف، نطاق التدقيق).
- إطار خطط وإجراءات تدقيق الأمن السيبراني، وسيناريوهات العمل.
- حماية الأصول الرقمية وهوية المؤسسة والتكيف والمخاطر السيبرانية.
- أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات في المؤسسة.
- إعداد تقارير تدقيق الأمن السيبراني وحفظ سجلات بأدلة نتائج التدقيق.
- مراجعة تدقيقات البرامج والمشاريع السيبرانية، وتنفيذها، والمشاركة فيها.
- أفضل الممارسات تنفيذ عمليات تدقيق الأمن السيبراني باستخدام أدوات التدقيق.
- التواصل الفعّال مع الإدارة العليا والإدارات ذات العلاقة بشأن تدقيق الأمن السيبراني.