النشرة الفنية لبرنامج

تحليل وتقييم مخاطر الأمن السيبر اني

ANALYSIS AND EVALUATION OF CYBER SECURITY RISKS

4 أيام، 20 ساعة

يبدأ بتاريخ 19/ 3/2023م

القاهرة، مصر

06 - 5522807
info@aljhood.com
www.aljhood.com
jordan amman queen rania st building.155

بطاقة معلومات البرنامج:

مدة التدريب	:	(4) أيام، (20) ساعة
مكان التدريب	:	القاهرة – مصر
تاريخ الانعقاد	:	19 – 22 /2023/03م
شهادة التدريب	:	شهادة صادرة من مجموعة الجهود المشتركة
لغة التدريب	:	اللغة العربية مع بعض المصطلحات الفنية باللغة الإنجليزية
أساليب التدريب	:	– إسلوب السيناريوهات. – إسلوب العصف الذهني. – إسلوب تمارين وأنشطة الفريق. – إسلوب تقديم الحلول والممارسات. – حالات من واقع عمل المشاركين.
الفئة المستهدفة	:	– العاملين في إدارة الإمتثال . – العاملين في إدارة المخاطر . – مدراء إدارة تدقيق أمن المعلومات . – المتخصصين في تكنولوجيا المعلومات الذين يرغبون في تطوير مهاراتهم بالأمن السيبراني.

ملخص البرنامج التدريبي:

تعتبر التهديدات الإلكترونية السيبرانية أكبر المخاطر المهددة لقطاع الأعمال والبيئة الاستثمارية على وجه العموم، مما يتطلب من المؤسسات بمختلف أنواعها في القطاعين العام والخاص اتخاذ عدد من التدابير الوقائية للتصدي لأي تهديدات تتعرض لها أنظمة المعلومات الخاصة بها أو تسريب بياناتها، ولا بد من القيام بعدد من الإجراءات اللتي على المؤسسات أن تأخذها بعين الإعتبار لحماية تقنياتها، مثل تقييم المخاطر اللتي قد تتعرض لها و جعل أمن المعلومات من أولويات أعمالها، والمراجعه المستمرة للممارسات الأمنية و إدارة الدخول إلى النقاط المؤدية لأنظمة الشبكات والتطبيقات والأمن الإستباقي أو الحماية الإستباقية مثل الجدران النارية، وإدارة أمن المعلومات، وتقييم نقاط الضعف واختبار الإختراق .

لذا إرتأت مجموعة الجهود المشتركة على تنفيذ البرنامج التدريبي الذي يهدف إلى رفع سوية المشاركين في إدارة عملية تقييم مخاطر الأمن السيبراني وزيادة وعيهم الفني في تنفيذ خطط التقييم الأمني لتلك المخاطر والتعامل مع التهديدات والهجمات السيبرانية، كما يستهدف البرنامج التدريبي كامل المعنيين المسؤولين عن أمن و إدارة شبكات نظم المعلومات، وطرق تقييم مخاطر أمن نظم المعلومات، وتطبيق قواعد أمن المعلومات السيبرانية بهدف إذكاء الوعي بهذا الموضوع من خلال إجراء دراسات تقييم جماعي للمخاطر مع الأساليب الدولية من خلال العمل الجماعي الذي يتعين القيام به .

الأردن / عمان – شارع الملكة رانيا العبدالله – بناية رقم 155 – الموقع الالكتروني : www.aljhood.com

الجدارات المستهدفة في التطوير:

- جدارة إكتشاف الإحتيال وطرق مكافحته .
- جدارة فهم مخاوف الأمن السيبراني للمؤسسات .
- جدارة تحديد الاحتياجات الأمنية الفورية بخطوات قابلة للتنفيذ .
- جدارة تعرف على كيفية تمكين تقليل التهديدات الأمنية بشكل أفضل .
- جدارة دراية بالنهج والأطر الخاصة بممارسات الأمن السيبراني الفعالة .

أهداف البرنامج التدريبي:

في نهاية التدريب يجب أن يكون المشاركين قادرين على معرفة:

- المفاهيم الخاصة بالتهديدات والمخاطر السيبرانية ومهارات تقييم ومعالجة مخاطر الأمن السيبراني .
- المهارات العملية والتطبيقية اللازمة لإجراء تقييمات منتظمة لمخاطر الأمن السيبراني لمؤسستك .
- التفاوض بشكل أفضل حول نطاق ودقة التقييمات الأمنية والتفاعل الفعال مع فرق التقييم الأمني.
- تحديد و تنفيذ الضوابط الأمنية اللتي تضمن الإمتثال للقوانين و اللوائح و السياسات و التوجهات المعمول بها .
- مهارات عرض المخاطر لأصحاب الأعمال والمهارات والمعرفة اللازمة لتقييم مخاطر الأمن السيبراني والاستجابة لها ومعالجتها .
- التعرف على كيفية تطبيق منهجيات مجربة و مستندة على المعايير لتقييم و إدارة المخاطر اللتي تهدد البنية التحتية لمعلومات المؤسسة .
- توسيع نطاق الحماية الأمنية لتشمل أنظمة الرقابة الصناعية (ICS) والسحابة، والمهارات اللازمة لإختبار دفاعاتك و إستغلالها بتطبيق تدابير مضادة للحد من المخاطر في مؤسستك .
- التعرف على كيفية إختراق المتسللون أنظمة التشغيل وتهربهم من برامج مكافحة الفيروسات، كيفية اكتشاف نقاط الضعف في شبكتك الخاصة بإستخدام نفس عقلية وطرق المتسللين .
- كيفية جمع المعلومات الإستخبارية من خلال استخدام الاستطلاعات، والبيانات المنشورة، وأدوات المسح الضوئي.
- إختبار و تحسين أمن الشبكة من خلال اختراق شبكتك الخاصة بإستخدام أدوات القرصنة ورفع الحصانة لمنع عملية التسلل .

المحاور الرئيسية للتدريب:

المحور الأول: أساسيات الأمن السيبراني

- مفهوم الأمن السيبراني.
- أهمية الأمن السيبراني.
- مفهوم أمن البيانات.
- الهجمات الالكترونية.
- إطار عمل الأمن السيبراني.

الأردن / عمان – شارع الملكة رانيا العبدالله – بناية رقم 155 – الموقع الالكتروني : www.aljhood.com

- جمع بيانات RIIOT المتقدم وأطر التحكم في الأمن.
- القضايا الحديثة حول جرائم الأمن السيبراني .

المحور الثاني: تحليل و تقييم مخاطر الأمن السيبراني

- أهداف تقييم مخاطر الامن السيبراني.
- أنواع التهديدات والمخاطر السيبرانية.
- نطاق المخاطر السيبرانية وأمن المعلومات.
- نماذج وأدوات إدارة المخاطر السيبرانية.
- طبيعة المخاطر والسياسات للأمن السيبراني.
- جمع وتنظيم معلومات المخاطر الإلكترونية.
- عمليات تقييم مخاطر التهديدات الإلكترونية.
- مراحل وخطط تقييم مخاطر الامن السيبراني.
- النماذج الدولية لإدارة مخاطر الأمن السيبراني.
- متطلبات المخاطر والمواصفة ISO2013: 27001 .
- معاجلة نقاط الضعف في التقييم (الفجوة المتحققة).
- تحديد وتحليل وتحديد أولويات مخاطر أمن المعلومات.

المحور الثالث: إختبار الاختراق (الأدوات و التقنيات)

- طبيعة الاختراق الأخلاقي.
- جمع البيانات عن الهدف.
- بناء خطة الاختراق و تطبيقها .
- تحديد التهديدات ونقاط الضعف .
- أساليب وأدوات تتبع حالات الاختراق .
- ادوات كشف الاختراقات وجمع الأدلة .
- معالجة نقاط الضعف (الفجوة المتحققة) .
- أدوات وتطبيقات لتقييم وإدارة المخاطر على البنية التحتية لمعلومات المؤسسة.

الأردن / عمان – شارع الملكة رانيا العبدالله – بناية رقم 155 – الموقع الالكتروني : www.aljhood.com