AL KHABEER
معهد الخبير العالي للتدريب

دليل تعريف الأقسام الأساسية للمقررات الإلكترونية

لدورة الأمن السيبراني والجرائم الإلكترونية

الفئة المستهدفة من الدليل:

- المدرب.
- المتدرب.
- الدعم الفني.

تفاصيل الدليل:

يتضمن دليل الأقسام الأساسية لمقرر دورة الأمن السيبراني والجرائم الإلكترونية طبقا لمعايير ما يلي:

- التعريف بالبرنامج
- الهدف العام من البرنامج
- الأهداف التفصيلية للبرنامج
- محاور البرنامج
- التقييم الذاتي للبرنامج

فيما يلي توضيح الأقسام الأساسية

التعريف بالبرنامج

يُعد الأمن السيبراني أحد أهم التحديات التي تُواجه الشركات والمؤسسات في عصرنا الحالي، حيث تتعرض البيانات والمعلومات لمخاطر كبيرة نتيجة التهديدات والهجمات الإلكترونية المتزايدة، وتكمن أهمية الأمن السيبراني في الحفاظ على سرية وسلامة وتوافر البيانات، وحمايتها من الاختراق أو التلف أو سوء الاستخدام. كما يتطلب ضمان أمن البيانات اتباع أفضل الممارسات والضوابط الأمنية على جميع المستويات، بالإضافة إلى تدريب وتوعية الموظفين حول كيفية التعامل مع البيانات وحمايتها، فالعنصر البشري هو أحد أهم حلقات الأمن السيبراني، لذا ينبغي تزويده بالمعرفة والمهارات اللازمة للتصدي للتهديدات الإلكترونية والحد منها.

الهدف العام من البرنامج

يحتاج جميع موظفي المؤسسات بشكل عام إلى التدريب على الأمن السيبراني، وذلك للحد من خطورة الاختراقات والهجمات الإلكترونية

الأهداف التفصيلية للبرنامج

سيتمكن المتدرب في نهاية الدورة من أن:

1. يحصل المتدرب على المعارف والكفايات النظرية والمهارات العملية التطبيقية اللازمة في مجال أمن المعلومات والفضاء السيبراني.
2. يتمكن المتدرب من التكيف مع التطورات المستقبلية المتسارعة في مجال أمن المعلومات
3. يتمكن المتدرب من تطوير مهارات البحث.

4. يحدد المتدرب المخاطر والتهديدات الشائعة للأمن السيبراني.
5. يتمكن المتدرب من معرفة تقنيات الأمن السيبراني الحديثة.
6. يقارن المتدرب بين red team and blue team
7. يتمكن المتدرب من تحديد عوامل زيادة مخاطر الأمن السيبراني
8. يتمكن المتدرب من تحديد مراحل عملية إدارة مخاطر الأمن السيبراني بعد حدوث مخاطر سيبرانية
9. يتمكن المتدرب من معرفة مراحل اختبار الاختراق
10. يتمكن المتدرب من معرفة كيفية الاستجابة للحوادث السيبرانية.
11. يتمكن المتدرب من معرفة البنية التحتية لأمن الشبكات
12. يتمكن المتدرب من معرفة كيفية حماية البيانات.
13. يتمكن المتدرب من التعرف على التشفير وكيف يعمل وأنواعه.
14. يتمكن المتدرب من معرفة التجزئة في الأمن السيبراني.
15. يتمكن المتدرب من فهم ما هو الترميز
16. يفهم المتدرب ما هو الوعي بالأمن السيبراني
17. يتمكن المتدرب من معرفة دورة حياة البيانات كاملة
18. يتمكن المتدرب من فهم الجرائم الالكترونية وكيفية التصدي لها
19. يتمكن المتدرب من التعرف على أمن الشبكات والمعلومات.
20. يتمكن المتدرب من التعرف على الفيروسات الحاسوبية وأنواعها
21. يتمكن المتدرب من التعرف على وظيفة جدار الحماية fire wall

محاور البرنامج

الأمن السيبراني أنواعه وأهميته

1. ما المقصود بالأمن السيبراني وأهميته؟
2. ما هي أنواع الهجمات التي يحاول الأمن السيبراني الدفاع عنها ؟
3. ما هي أنواع الأمن السيبراني؟
4. ما هي تقنيات الأمن السيبراني الحديثة؟
5. فرق Blue Team && Red Team
6. ما هو مثلث CIA وعلاقته بالأمن السيبراني
7. ما هي مخاطر الأمن السيبراني
8. إدارة المخاطر قبل حدوث مخاطر سيبرانية

مخاطر الأمن السيبراني وطرق ادارتها

1. مراجعة على ما تم مناقشته في اليوم الأول
2. إدارة المخاطر بعد حدوث مخاطر سيبرانية
3. الحوكمة والمخاطر والتدريب
4. Cyber Kill Chain
5. اختبار الاختراق
6. الاستجابة للحوادث
7. التحكم في الوصول

الممارسات العامة للأمن السيبراني

1. مراجعة على ما تم مناقشته في اليوم الأول والثاني
2. البنية التحتيه لأمن الشبكات
3. الأمن السيبراني وحماية المعلومات
4. التشفير
5. التجزئة في الأمن السيبراني
6. الترميز في الأمن السيبراني
7. الوعي بالأمن السيبراني

تطبيقات الأمن السيبراني وامن المعلومات

1. مراجعه ما سبق
2. الأمن السيبراني للتكنولوجيا التشغلية
3. دورة حياة البيانات الكاملة
4. الجرائم الألكترونية والجرائم المعلوماتية
5. امن الشبكات وامن المعلومات
6. الهندسه الأجتماعية
7. طرق تعزيز الأمن السيبراني
8. طرق تفادي اختراقات الأمن السيبراني

الهجمات السيبرانية وأنواعها

1. مراجعه ما سبق
2. انواع الهجمات السيرانية
3. هجوم اليوم الصفري
4. الفيروسات الحاسوبية
5. تخصصات امن المعلومات وكيف تختار تخصصك

AL KHABEER
معهد الخبير العالي للتدريب

التقييم الذاتي للبرنامج

https://eec.edu.sa/cr.php?CR=14

- المحتوى الاثرائي
- دليل المعارف والمهارات
- دليل بدء استخدام المقررات الالكترونية
- دليل سياسة التواصل
- سياسة الإجابة على الاستفسارات
- دليل تعريف الأقسام الأساسية
- الخطة الزمنية للبرنامج
- قياس رضا المستفيدين (المتدرب)
- قياس رضا المستفيدين (المدرب)
- التقييم الذاتي للبرنامج

الأمن السيبراني والجرائم الإلكترونية

Cyber security and cyber crimes

رقم اعتماد الدورة بالمؤسسة العامة للتدريب التقني والمهني 344397632

25 ساعة تدريبية / 5 أيام
عـن بعـــد

تعريف البرنامج

يُعد الأمن السيبراني أحد أهم التحديات التي تُواجه الشركات والمؤسسات في عصرنا الحالي، حيث تتعرض البيانات والمعلومات لمخاطر كبيرة نتيجة التهديدات والهجمات الإلكترونية المتزايدة، وتكمن أهمية الأمن السيبراني في الحفاظ على سرية وسلامة وتوافر البيانات، وحمايتها من الاختراق أو التلف أو سوء الاستخدام. كما يتطلب ضمان أمن البيانات اتباع أفضل الممارسات والضوابط الأمنية على جميع المستويات، بالإضافة إلى تدريب وتوعية الموظفين حول كيفية التعامل مع البيانات وحمايتها، فالعنصر البشري هو أحد أهم حلقات الأمن السيبراني، لذا ينبغي تزويده بالمعرفة والمهارات اللازمة للتصدي للتهديدات الإلكترونية والحد منها.

شارك البرنامج

الهدف العام | الأهداف التفصيلية

يحتاج جميع موظفي المؤسسات بشكل عام إلى التدريب على الأمن السيبـ