التدريبية: تحليل البيانات لتقييم المخاطر السيبرانية وحماية الأنظمة الدورة

يوليو ٢٠٢٦ ١٠ - ٠٦

فيينا

(للشخص الواحد) ٥٧٠٠ €

Ref: #DM6951_367364

مقدمة الدورة التدريبية / لمحة عامة:

الأصول الرقمية أمراً أصبحت القدرة على تحليل البيانات بفعالية لتقييم في ظل التهديدات السيبرانية المتزايدة والمتطورة، السيبراني مجرد مسألة دفاعية، بل هو جانب حيوياً للمؤسسات من جميع الأحجام والقطاعات. لم يعد المخاطر السيبرانية وحماية المؤسسات عرضة اكتشاف الاختراقات، والاستجابة للحوادث بفعالية. استراتيجي يعتمد على البيانات للتنبؤ بالتهديدات، الأمن مالية فادحة، الإضرار بالسمعة، وتسرب للهجمات السيبرانية المدمرة التي يمكن أن تؤدي إلى بدون تحليل بيانات قوي، قد تظل لتسخير قوة تحليل إلى تزويد المهنيين BIG BEN Training Center البيانات الحساسة. تهدف هذه الدورة التدريبية من خسائر وتحسين الدفاعات الأمنية. ستتناول الدورة البيانات لتقييم المخاطر السيبرانية، وتحديد نقاط بالمعرفة والمهارات اللازمة التحليلات الإحصائية الأمنية، أدوات وتقنيات جمع البيانات الأمنية المفاهيم الأساسية لأمن المعلومات، أنواع البيانات الضعف، خبراء وإدارة الاستجابة للحوادث بناءً على البيانات. والتعلم الآلي لاكتشاف الشذوذ والتنبؤ بالهجمات، وتحليلها، كيفية استخدام وهو خبير Bruce Schneier مرموقين في الأمن السيبراني وتحليل البيانات، مثل تستند الدورة إلى رؤى أكاديمية وعملية من البيانات لفهم المخاطر الأمنية واتخاذ قرارات مشهور في الأمن السيبراني والتشفير يركز على أهمية عالمي (بروس شناير، قوية ومرنة. النظرية والتطبيقية. ستمكن هذه الدورة المتدربين من استراتيجية، مما يضمن محتوى غنياً بالمعرفة تحليل دفاعات سيبرانية

بناء

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- محللو الأمن السيبراني.
- مهندسو الأمن السيبراني.
- محللو المخاطر الأمنية.
- مديرو أمن المعلومات (CISO).
- مديرو تكنولوجيا المعلومات.
- مدققو الأمن.
- محللو العمليات الأمنية (SOC Analysts).
- أي مهني يعمل في مجال أمن المعلومات.

القطاعات والصناعات المستهدفة:

- الخدمات المالية.
- التكنولوجيا والبرمجيات.
- الحكومة والدفاع.
- الرعاية الصحية.
- الاتصالات.
- التصنيع.
- الطاقة والمرافق.
- القطاع الحكومي وما في حكمه.

الأقسام المؤسسية المستهدفة:

- الأمن السيبراني.
- تكنولوجيا المعلومات.
- إدارة المخاطر.
- الامتثال.
- العمليات الأمنية.
- التحقيقات الرقمية.
- حوكمة تكنولوجيا المعلومات.
- الاستجابة للحوادث.

أهداف الدورة التدريبية:

أتقن المهارات التالية: بنهاية هذه الدورة التدريبية، سيكون المتدرب قد

- السيبرانية. فهم العلاقة بين تحليل البيانات وتقييم المخاطر
- تحديد أنواع البيانات الأمنية ومصادرها.
- جمع وتنظيف وإعداد البيانات الأمنية للتحليل.
- تطبيق تقنيات التحليل الإحصائي لكشف الشذوذ.
- الأمنية. استخدام أدوات تحليل البيانات لتحليل السجلات
- بناء نماذج تنبؤية للهجمات السيبرانية.
- تطبيق التعلم الآلي لاكتشاف التهديدات.
- البيانات. تقييم نقاط الضعف والثغرات الأمنية بناءً على
- تطوير تقارير المخاطر السيبرانية ولوحات المعلومات.
- اتخاذ قرارات مستنيرة لتعزيز الأمن السيبراني.

منهجية الدورة التدريبية:

المحتوى من مصممة لتمكين المشاركين من تحليل البيانات بفعالية تتبنى هذه الدورة التدريبية منهجية عملية وتطبيقية، الأساسية لأمن البيانات، المخاطر خلال مزيج من المحاضرات التفاعلية، التي تشرح لتقييم المخاطر السيبرانية. يتم تقديم أمنية حقيقية. سيقوم التطبيقية المكثفة التي تتيح للمشاركين العمل السيبرانية، والتحليلات الأمنية، وورش العمل المفاهيم وتحليلها باستخدام أدوات شائعة، وتحديد المتدربون بجمع السجلات الأمنية من أنظمة مختلفة، مباشرة على سيناريوهات بيانات في لكشف الاختراقات، وإنشاء تقارير مخاطر واضحة. يعزز الأنماط المشبوهة، وتطبيق خوارزميات التعلم الآلي وتنظيفها، فرصة لطرح الأسئلة وتلقي معالجة تحديات المخاطر السيبرانية الواقعية، بينما العمل الجماعي مهارات التعاون وتبادل الخبرات على توفير بيئة تعليمية غنية BIG BEN Training Center تغذية راجعة من المدربين الخبراء. يحرص تتيح الجلسات التفاعلية لمؤسساتهم. لضمان اكتساب المتدربين خبرة عملية مباشرة في تسخير بالأمثلة ودراسات الحالة من حوادث أمنية حقيقية، البيانات لتعزيز الدفاعات السيبرانية

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات المخاطر السيبرانية والبيانات الأمنية.

- مقدمة إلى المخاطر السيبرانية وأنواعها.
- إطار عمل الأمن السيبراني (NIST, ISO ٢٧٠٠١).
- الشبكة، التطبيقات). مفهوم البيانات الأمنية ومصادرها (سجلات النظام،
- للحوادث. تأثير البيانات على تقييم المخاطر والاستجابة
- نماذج التهديد ونقاط الضعف.
- أهمية جودة البيانات الأمنية.
- بياناتها. أمثلة على الهجمات السيبرانية وكيفية تحليل

الأمني. الوحدة الثانية: جمع وتجهيز البيانات للتحليل

- IDS/IPS). تقنيات جمع البيانات الأمنية (SIEM, EDR,
- تنظيف البيانات الأمنية وتوحيدها.
- إثراء البيانات الأمنية (Threat Intelligence).
- نمذجة البيانات للتحليل الأمني.
- التعامل مع البيانات الضخمة الأمنية.
- أدوات إدارة السجلات (Log Management Tools).
- تحديات خصوصية البيانات وأمنها.

في البيانات الأمنية. الوحدة الثالثة: التحليل الإحصائي واكتشاف الشذوذ

- مقدمة إلى التحليل الإحصائي في الأمن السيبراني.
- مقاييس الاتجاه المركزي والتشتت للبيانات الأمنية.
- الطبيعية. تحديد القيم الشاذة (Anomalies) والأنماط غير
- استخدام الرسوم البيانية لتصور البيانات الأمنية.
- تطبيق الاختبارات الإحصائية لكشف التهديدات.
- تحليل الاتجاهات والتنبؤ بالهجمات.
- ورشة عمل: اكتشاف الشذوذ في سجلات الشبكة.

للأمن السيبراني. الوحدة الرابعة: التعلم الآلي والذكاء الاصطناعي

- الأمن السيبراني. مقدمة إلى التعلم الآلي (Machine Learning) في
- انحدار). أنواع خوارزميات التعلم الآلي (تصنيف، تجميع،
- (Detection). تطبيق التعلم الآلي لكشف البرامج الضارة (Malware)
- الذكاء الاصطناعي. كشف الاختراقات (Intrusion Detection) باستخدام
- التهديدات الداخلية. تحليل السلوك (Behavioral Analytics) لكشف
- بناء نماذج التعلم الآلي للأمن.
- (Positives/Negatives). التعامل مع تحديات النماذج الزائفة (False)

والتوجهات المستقبلية. الوحدة الخامسة: إدارة المخاطر السيبرانية

- بناء تقارير المخاطر السيبرانية ولوحات المعلومات.
- تقييم المخاطر وتصنيفها بناءً على البيانات.
- استراتيجيات التخفيف من المخاطر.
- بالبيانات. الاستجابة للحوادث (Incident Response) المدفوعة
- دور التحقيقات الرقمية (Digital Forensics).
- والتحليلات الأمنية. الاتجاهات المستقبلية في التهديدات السيبرانية
- بناء برنامج أمن سيبراني قائم على البيانات.

الأسئلة المتكررة:

التسجيل في الدورة؟ ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل

لا توجد شروط مسبقة.

الإجمالي لساعات الدورة التدريبية؟ كم تستغرق مدة الجلسة اليومية، وما هو العدد

المدة إلى ٢٥٢٠- بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام، ساعة تدريبية. راحة وأنشطة تفاعلية، ليصل إجمالي

سؤال للتأمل:

مجرد الاستجابة للهجمات إلى وتتزايد فيه أحجام البيانات الأمنية، كيف يمكن في عالم تتسارع فيه وتيرة التهديدات السيبرانية مما يمكنها من التنبؤ بالمخاطر، اكتشاف بناء دفاعات استباقية تستند إلى التحليلات العميقة للمؤسسات أن تتحول من الأكثر قيمة؟ مستوى غير مسبوق من المرونة السيبرانية وحماية الشذوذ، والاستجابة بذكاء للحوادث، وبالتالي تحقيق للبيانات، الأصول

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

مما يوفر للمشاركين فهماً عميقاً والشامل على تحليل البيانات لتقييم المخاطر تتميز هذه الدورة التدريبية بتركيزها العملي السيبراني المدفوع الأمنية. يقدم BIG BEN Training Center محتوى لكيفية تسخير قوة البيانات لتعزيز الدفاعات السيبرانية، التحليلات الإحصائية والتعلم الآلي لاكتشاف بالبيانات، من جمع البيانات الأمنية وإعدادها إلى متقدماً يغطي جميع جوانب الأمن لورش عمل تطبيقية الأمثلة العملية ودراسات الحالة من حوادث أمنية التهديدات والتنبؤ بالهجمات، مع التركيز على تطبيق المشبوهة، وتطبيق خوارزميات التعلم الآلي مكثفة تتيح للمشاركين تحليل سجلات أمنية، وتحديد حقيقية. تبرز الدورة بتوفيرها بل تطبيق المفاهيم النظرية. هذا النهج المتكامل يضمن لكشف الاختراقات، مما يضمن اكتسابهم خبرة مباشرة في الأنماط على بناء دفاعات قوية أيضاً الكفاءات العملية اللازمة ليصبحوا قادة في أن يكتسب المتدربون ليس فقط المعرفة العميقة، ومرنة لمؤسساتهم. الأمن السيبراني، قادرين