الدورة التدريبية: أمن الشبكات والوقاية من الاختراقات للشركات

Ref: #CYB6531

مقدمة الدورة التدريبية / لمحة عامة:

الشاملة للمحترفين أمن الشبكات ضرورة حتمية للشركات بجميع أحجامها. في ظل التزايد المستمر للتهديدات السيبرانية، أصبح والوقاية من الاختراقات بفعالية. سنتناول في هذه الأدوات والمعرفة اللازمة لبناء شبكات آمنة تقدم هذه الدورة التدريبية عملية في تكوين تصميم الشبكات الآمنة، وتطبيق الدفاعات ضد الهجمات الدورة مفاهيم أمن الشبكات الأساسية والمتقدمة، إلى .VPN ، وشبكات(IDS/IPS) جدران الحماية (Firewalls)، أنظمة كشف التسلل المتطورة. سيكتسب المشاركون مهارات إلى الشركات، وضمان استمرارية الأعمال في مواجهة المهنيين من حماية البنية التحتية للشبكة، بيانات تمكين تهدف الدورة خبراء أكاديميين بارزين مثل أحدث المعايير الصناعية وأفضل الممارسات، مع التهديدات السيبرانية المتغيرة. يستند المحتوى BIG BEN ، مؤلف العديد من الكتب المرجعية في أمن(William Stallings البروفيسور ويليام ستالينغز (الاستفادة من خبرات وتقليل مخاطر الهجمات هذه الدورة لمساعدة الشركات على تعزيز Center الشبكات والأنظمة الموزعة. يقدمTraining الإلكترونية. قدراتها الدفاعية السيبرانية

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مهندسو الشبكات ومسؤولون الشبكات.
- متخصصو الأمن السيبراني.
- مديرو تكنولوجيا المعلومات ومديرو أمن المعلومات.
- مدققو الأنظمة الأمنية.
- مؤسسته. أي مهني مسؤول عن أمن البنية التحتية للشبكة في

القطاعات والصناعات المستهدفة:

- شركات تكنولوجيا المعلومات والاتصالات.
- القطاع المالي والمصرفي لـأمن الشبكات المصرفية.
- لـحماية الشبكات الحكومية. القطاع الحكومي والهيئات العامة وما في حكمها
- قطاع الطاقة والمرافق الحيوية.
- شركات التصنيع.
- قطاع التجزئة والتجارة الإلكترونية.

الأقسام المؤسسية المستهدفة:

- إدارة تقنية المعلومات.
- إدارة أمن المعلومات.
- إدارة الشبكات.
- إدارة العمليات.
- إدارة المخاطر.

أهداف الدورة التدريبية:

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

- فهم مبادئ أمن الشبكات وآليات الهجوم الشائعة.
- القدرة على تصميم وتنفيذ شبكات آمنة.
- التسلل (IDS/IPS) وأنظمة كشف ومنع (Firewalls) تكوين جدران الحماية
- الاختراقات. إدارة الثغرات الأمنية في الشبكات والوقاية من
- الخاصة (VPNs) تأمين الشبكات اللاسلكية والشبكات الافتراضية
- مراقبة أمن الشبكات والاستجابة للحوادث الأمنية.
- وضع سياسات وإجراءات أمن الشبكات الفعالة.

منهجية الدورة التدريبية:

من الاختراقات. سيتمكن تركز على تزويد المشاركين بالخبرة المباشرة في تعتمد هذه الدورة التدريبية منهجية عملية وشاملة، من تطبيق أدوات وتقنيات أمن الشبكات بشكل المتدربون من خلال ورش العمل المكثفة والمحاكاة تأمين الشبكات والوقاية على التكوينات لـاختراقات شبكية حقيقية، مع تحليل كيفية حدوثها عملي. تتضمن المنهجية دراسات حالة مفصلة الواقعية الأنشطة المشبوهة. يقدم BIG الأمنية الصحيحة للأجهزة والبرمجيات، وكيفية تحليل وكيفية الوقاية منها. سيتم التركيز بناء دفاعات شبكية قوية وفعالة في بيئاتهم هذه الدورة لتمكين المهنيين BEN Training Center سجلات الشبكة لاكتشاف الممارسات والخبرات بين المشاركين. التنظيمية. يتم تشجيع التفاعل والنقاش لتبادل أفضل من

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات أمن الشبكات ومفاهيم الهجوم

- مقدمة إلى مبادئ أمن الشبكات.
- نماذج التهديدات الشبكية وأنواع الهجمات.
- نقاط الضعف الشائعة في الشبكات.
- أمن الطبقات المختلفة في نموذج OSI/TCP-IP.
- المهارات الأساسية لمحلل أمن الشبكات.
- هجمات حجب الخدمة (DoS/DDoS).
- الهندسة الاجتماعية وأثرها على أمن الشبكات.

التسلل الوحدة الثانية: جدران الحماية وأنظمة كشف ومنع

- مفاهيم جدران الحماية (Firewalls) وأنواعها.
- تكوين قواعد جدران الحماية وتطبيقها.
- أنظمة كشف التسلل (IDS) وأنظمة منع التسلل (IPS).
- تصميم وتنفيذ IDS/IPS.
- تجاوز جدران الحماية وأنظمة IDS/IPS.
- أمن الشبكات في البيئات الافتراضية.
- إدارة السجلات والإنذارات الأمنية.

الافتراضية الخاصة الوحدة الثالثة: تأمين الشبكات اللاسلكية والشبكات

- تحديات أمن الشبكات اللاسلكية (Wi-Fi Security).
- معايير أمن الشبكات اللاسلكية (WEP, WPA, WPA٢, WPA٣).
- تكوين نقاط الوصول الآمنة.
- مقدمة إلى الشبكات الافتراضية الخاصة (VPNs).
- أنواع VPNs وتكوينها.
- تشفير الاتصالات في VPNs.
- أمن الشبكات اللاسلكية للمؤسسات.

الشبكية الوحدة الرابعة: تقييم الثغرات وإدارة المخاطر

- عملية تقييم الثغرات الأمنية في الشبكات.
- أدوات فحص الثغرات (مثل: Nessus, OpenVAS).
- إدارة المخاطر الأمنية للشبكات.
- التعامل مع الثغرات المكتشفة.
- اختبار الاختراق للشبكات الداخلية والخارجية.
- تحليل سجلات الشبكة (Network Log Analysis).
- الاستجابة للحوادث الأمنية في الشبكة.

المستقبلية الوحدة الخامسة: أمن الشبكات المتقدم والاتجاهات

- أمن الشبكات في البيئات السحابية.
- أمن الشبكات المعرفة بالبرمجيات (SDN Security).
- أمن الإنترنت من الأشياء (IoT Security) في الشبكات.
- أمن شبكات التشغيل الصناعية (OT Security).
- الذكاء الاصطناعي في أمن الشبكات.
- الاتجاهات المستقبلية لـأمن الشبكات.
- بناء إطار عمل أمني شامل للشبكة.

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:

استباقيًا لـأمن الشبكات وتنوع الشبكات (تقليدية، سحابية، IoT)، كيف يمكن في عصر تتزايد فيه تعقيدات الهجمات السيبرانية ليشمل بناء بنية تحتية شبكية مرنة قادرة على لا يقتصر على الدفاع ضد التهديدات المعروفة، بل للمؤسسات أن تتبنى نهجًا التكيف مع التحديات المستقبلية غير المتوقعة؟ يمتد

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

في التكوينات الشبكات والوقاية من الاختراقات، وتقديم رؤى عملية تتميز هذه الدورة بتركيزها الشامل والعميق على أمن عن الدورات التي تقدم نظرة عامة فقط. الأمنية المتقدمة لجدران الحماية وأنظمةIDS/IPS ، تتجاوز المفاهيم النظرية. نغوص في تأمين وكيفية بناء دفاعات قوية ضدها. تركز الدورة على نقدم أمثلة عملية واقعية لسيناريوهات الاختراق مما يميزها الثغرات. إنها ليست مجرد دورة(VPNs) الشبكات اللاسلكية، والشبكات الافتراضية الخاصة تزويد المشاركين بالمهارات العملية وكفاءة. بناء مهندسي شبكات أمنيين قادرين على حماية البنية لتعلم أدوات محددة، بل هي تدريب مكثف يهدف إلى ، وإدارة التحتية الحيوية للشركات بفعالية