الدورة التدريبية: الأمن السيبراني للمنظمات الحكومية (حماية البيانات الوطنية)

يونيو - ٠٣ يوليو ٢٠٢٦ ٢٩

كوالالمبور

(للشخص الواحد) € ٥٢٠٠

Ref: #CYB5716_268226

مقدمة الدورة التدريبية / لمحة عامة:

الاعتماد على البنية التحتية أساسية لحماية الأمن القومي وسلامة البيانات يمثل الأمن السيبراني للمنظمات الحكومية ركيزة السيبرانية التي تستهدف البيانات الحساسة والأنظمة الرقمية في القطاع الحكومي، تتصاعد التهديدات الوطنية. فمع تزايد السيادية، بهدف تزويدهم مصممة خصيصًا للموظفين الحكوميين والمهنيين الحيوية للدولة. هذه الدورة التدريبية المتخصصة هذه الدورة الحكومية، حماية البيانات الوطنية، والامتثال بالمعرفة والمهارات المتقدمة لتأمين الأنظمة العاملين في الجهات الوطني، وتطبيق أطر العمل مفاهيم الأمن السيبراني الحكومي، إدارة المخاطر للسياسات الأمنية الوطنية. سنتناول في نقاط الضعف، تصميم دفاعات قوية، والاستجابة الأمنية المعتمدة. سيكتسب المشاركون القدرة على السيبرانية على المستوى المحتوى إلى القومي. تهدف الدورة إلى بناء كوادر وطنية مؤهلة في الفعالة للحوادث السيبرانية التي قد تهدد الأمن تحديد إلى مساهمات خبراء أكاديميين أحدث المعايير الدولية والوطنية لـأمن المعلومات مجال الأمن السيبراني الحكومي. يستند ، الذي كان مستشارًا للأمن السيبراني(Schmidt بارزين مثل البروفيسور هوارد شميدت (Howard الحكومية، مع الإشارة BIG BEN Training Center السيبرانية وإدارة المخاطر الحكومية. يقدم للرؤساء الأمريكيين، ومعروفًا بأعماله في السياسة للدولة. السيبرانية الحكومية وحماية الأصول الرقمية هذه الدورة لتعزيز القدرات

لـ الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مسؤولون رفيعو المستوى في القطاع الحكومي.
- متخصصو الأمن السيبراني في الهيئات الحكومية.
- الحكومية. مسؤولو حماية البيانات والخصوصية في الجهات
- مديرو تكنولوجيا المعلومات في القطاع العام.
- المختصون في الأمن القومي والاستخبارات الرقمية.
- مدققو الأنظمة الحكومية.

القطاعات والصناعات المستهدفة:

- الهيئات الحكومية والوزارات.
- الجهات الأمنية والدفاعية وما في حكمها.
- البنوك المركزية والمؤسسات المالية الحكومية.
- اتصالات). شركات البنية التحتية الحيوية (طاقة، مياه،
- المؤسسات التعليمية والبحثية الحكومية.
- شركات التكنولوجيا التي تتعامل مع القطاع الحكومي.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني الوطني.
- إدارة تقنية المعلومات الحكومية.
- والبيانات السرية. الأقسام المعنية بحماية البيانات الحساسة
- إدارة المخاطر والامتثال الحكومي.
- فرق الاستجابة للحوادث الحكومية (Gov-CSIRT).

أهداف الدورة التدريبية:

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

- الحكومي. فهم شامل لـتحديات الأمن السيبراني في القطاع
- والدولية. القدرة على تطبيق أطر عمل الأمن السيبراني الوطنية
- الحرجة. حماية البيانات الحكومية الحساسة والبنية التحتية
- تطوير سياسات وإجراءات أمنية حكومية فعالة.
- الحكومية. التعامل مع الهجمات السيبرانية الموجهة ضد الكيانات
- الحكومية. إدارة المخاطر السيبرانية على مستوى المؤسسات
- الجهات الحكومية. تعزيز التعاون المشترك في الأمن السيبراني بين

منهجية الدورة التدريبية:

لحماية البيانات الوطنية للقطاع الحكومي، تركز على تزويد المشاركين تعتمد هذه الدورة التدريبية منهجية متقدمة وموجهة من خلال دراسات الحالة الواقعية لهجمات سيبرانية وتعزيز الأمن السيبراني الحكومي. سيتمكن المتدربون بالمهارات اللازمة مناقشات معمقة حول إجراءات الأمن السيبراني في البيئات الحكومية حكومية، وورش العمل التفاعلية، من فهم كيفية تطبيق البنية التحتية الحرجة للدولة. سيتم التركيز على الامتثال للوائح والسياسات الأمنية الوطنية، وأمن المعقدة. تتضمن المنهجية BIG BEN Training هذه المعقدة، والتعاون الدولي في مكافحة الجرائم الاستخبارات السيبرانية، التحقيق في الهجمات لحماية الأمن السيبراني الوطني. الدورة لتمكين الكوادر الحكومية من أن تصبح درعًا السيبرانية. يقدم Center

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: المشهد السيبراني الحكومي والتحديات

- مقدمة إلى الأمن السيبراني في القطاع الحكومي.
- والحكومات. أنواع التهديدات السيبرانية التي تواجه الدول
- الحرجة. أهمية حماية البيانات الوطنية والبنية التحتية
- التحديات الفريدة للأمن السيبراني الحكومي.
- أمن الفضاء السيبراني كجزء من الأمن القومي.
- الحكومي. دور السياسات والتشريعات في الأمن السيبراني
- إدارة المخاطر السيبرانية الاستراتيجية.

الحكومية الوحدة الثانية: أطر العمل والسياسات الأمنية

- الحكومة: إطار عمل NIST للأمن السيبراني وتطبيقه في
- معايير ISO ٢٧٠٠٠ في القطاع العام.
- الحكومية: السياسات الأمنية الوطنية لحماية البيانات
- إدارة الثغرات الأمنية في الأنظمة الحكومية.
- وضع خطط أمنية شاملة للوزارات والهيئات.
- الامتثال للوائح حماية البيانات الوطنية.
- تقييم النضج الأمني للمنظمات الحكومية.

الحكومية الوحدة الثالثة: حماية البنية التحتية والأنظمة

- أمن الشبكات الحكومية وأنظمة الاتصالات.
- تأمين الخوادم وقواعد البيانات الحكومية.
- حماية السحابة الحكومية (Government Cloud Security).
- أمن أنظمة التحكم الصناعي (ICS/SCADA) في القطاع الحيوي.
- أمن الأجهزة المحمولة المستخدمة في العمل الحكومي.
- التحكم بالوصول وإدارة الهوية في الأنظمة الحكومية.
- أمن تطبيقات الويب الحكومية.

والتحقيق الحكومي الوحدة الرابعة: الاستجابة للحوادث السيبرانية

- إنشاء فرق الاستجابة للحوادث الحكومية (Gov-CSIRT).
- مراحل الاستجابة للحوادث السيبرانية الوطنية.
- التحقيق الجنائي الرقمي في الهجمات الحكومية.
- جمع الأدلة الرقمية وتوثيقها للأغراض القانونية.
- التواصل أثناء الأزمات الأمنية على المستوى الوطني.
- التعافي من الهجمات السيبرانية الكبرى.
- التعاون الدولي في التحقيقات السيبرانية.

الوطنية الوحدة الخامسة: الوعي السيبراني والثقافة الأمنية

- بناء ثقافة أمنية قوية داخل المؤسسات الحكومية.
- برامج تدريب الوعي السيبراني للموظفين الحكوميين.
- الحكومية. مكافحة الهندسة الاجتماعية التي تستهدف الجهات
- القطاع العام. أمن سلسلة التوريد (Supply Chain Security) في
- مبادرات الأمن السيبراني الوطنية وحملات التوعية.
- التصدي لحملات التضليل السيبراني.
- مستقبل الأمن السيبراني الحكومي.

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:

دفاعية لا والتطور السريع في تقنيات التجسس الرقمي، كيف يمكن في ظل تصاعد الهجمات السيبرانية المدعومة من الدول وتُنشئ درعًا سيبرانيًا وطنيًا قادرًا تكتفي بصد التهديدات الحالية، بل تتوقع التحديات للمنظمات الحكومية أن تبتكر استراتيجيات على حماية سيادة الدولة في الفضاء الرقمي؟ المستقبلية

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

الفريدة التي الأمن السيبراني للمنظمات الحكومية، مما يوفر محتوى تتميز هذه الدورة بتركيزها المتخصص والعميق على المفاهيم العامة، نغوص في أطر العمل تواجه البيانات الوطنية والبنية التحتية الحكومية. مصممًا خصيصًا لمواجهة التحديات لنتائجها وكيفية بفعالية. تقدم الدورة دراسات حالة واقعية لـهجمات والسياسات الأمنية الوطنية وكيفية تطبيقها بدلاً من وأمن البنية التحتية الحرجة، وهي بناء دفاعات قوية. نركز على التعاون المشترك بين سيبرانية حكومية، مع تحليل مفصل الأساسيات، بل هي برنامج تدريبي شامل يهدف جوانب حاسمة في الأمن القومي. إنها ليست مجرد دورة الجهات الحكومية الرقمية للدولة وضمان الأمن السيبراني الوطني. إلى بناء كوادر حكومية مؤهلة لحماية الأصول لتعلم