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

#CYB5716

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

مقدمة الدورة التدريبية / لمحة عامة:

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

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مسؤولون رفيعو المستوى في القطاع الحكومي.
- متخصصو الأمن السيبراني في الهيئات الحكومية.
- مسؤولو حماية البيانات والخصوصية في الجهات الحكومية.
- 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.
- شركات البنية التحتية الحيوية (طاقة، مياه، اتصالات).
- المؤسسات التعليمية والبحثية الحكومية.
- شركات التكنولوجيا التي تتعامل مع القطاع الحكومي.

الأقسام المؤسسية المستهدفة:

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

أهداف الدورة التدريبية:

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

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

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: المشهد السيبراني الحكومي والتحديات

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

الوحدة الثانية: أطر العمل والسياسات الأمنية الحكومية

- إطار عمل NIST للأمن السيبراني وتطبيقه في الحكومة.
- معايير ISO 27000 في القطاع العام.
- السياسات الأمنية الوطنية لـحماية البيانات الحكومية.
- إدارة الثغرات الأمنية في الأنظمة الحكومية.
- وضع خطط أمنية شاملة للوزارات والهيئات.
- الامتثال للوائح حماية البيانات الوطنية.
- تقييم النضج الأمني للمنظمات الحكومية.

الوحدة الثالثة: حماية البنية التحتية والأنظمة الحكومية

- 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.

الوحدة الرابعة: الاستجابة للحوادث السيبرانية والتحقيق الحكومي

- 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.

الوحدة الخامسة: الوعي السيبراني والثقافة الأمنية الوطنية

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

الأسئلة المتكررة:

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

لا توجد شروط مسبقة.

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

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20–25 ساعة تدريبية.

سؤال للتأمل:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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