# التدريبية: أمن الأنظمة السحابية والبيئات الهجينة المتقدمة الدورة

يوليو ٢٠٢٦ ٣١ - ٢٧

روما

(للشخص الواحد) € ٥٧٠٠

Ref: #SM6286_330536

## مقدمة الدورة التدريبية / لمحة عامة:

من أهم التحديات التي والبيئات الهجينة، أصبح أمن الأنظمة السحابية مع التوسع الهائل في الاعتماد على الحوسبة السحابية والتطبيقات في هذه البيئات فهمًا عميقًا تواجه المؤسسات في جميع القطاعات. تتطلب حماية والبيئات الهجينة المتقدمة الأمن السيبراني وأفضل الممارسات لتأمينها. هذه الدورة التدريبية للبنى التحتية السحابية، ونقاط الضعف المحتملة، البيانات لتصميم، وتنفيذ، وإدارة حلول أمنية قوية وتقنية المعلومات بالمعرفة والمهارات المتقدمة الشاملة مصممة لتزويد متخصصي في السحابة. استراتيجيات أمن السحابة، إدارة الهوية والوصول، للأنظمة السحابية والبيئات الهجينة. سنتعمق في اللازمة الحوسبة السحابية، مثل البروفيسور تستند الدورة إلى أعمال خبراء أكاديميين بارزين في تشفير البيانات، ومراقبة التهديدات Training Center البيانات والخصوصية في السحابة. يقدم BIG BEN التي تُعرف بأبحاثها في أمن Indrakshi Ray، مجال أمن الأمنية العالمية. سيركز التدريب من حماية أصولهم في السحابة، وتقليل المخاطر، وضمان المهنيين هذه الدورة بهدف تمكين حالة واقعية وتمارين محاكاة، لمساعدة المشاركين على على الجوانب التطبيقية والعملية، مع تقديم دراسات الامتثال للمعايير بفعالية. وتعزيز قدراتهم على مواجهة التحديات الأمنية تطبيق المفاهيم النظرية في بيئات عملهم المعقدة،

## لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مهندسو الأمن السحابي.
- مهندسو DevOps/SecOps.
- مديرو الأمن السيبراني.
- مسؤولو أمن المعلومات.
- مهندسو الشبكات والسحابة.
- المطورون العاملون على تطبيقات سحابية.
- مدققو الأمن.

## القطاعات والصناعات المستهدفة:

- شركات تقنية المعلومات والبرمجيات.
- مزودو الخدمات السحابية.
- القطاع المالي والمصرفي.
- الحكومة والقطاع العام.
- التجارة الإلكترونية والتجزئة.
- الرعاية الصحية.
- الشركات الكبرى متعددة الجنسيات.

## الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- إدارة تقنية المعلومات.
- إدارة البنية التحتية.
- فرق تطوير البرمجيات.
- إدارة المخاطر والامتثال.
- العمليات السحابية.
- الاستراتيجية الرقمية.

## أهداف الدورة التدريبية:

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

- فهم نماذج النشر السحابي وأنواع الخدمات (IaaS, PaaS, SaaS).
- تطبيق مبادئ الأمن السحابي وإدارة المخاطر.
- تأمين الهوية والوصول في البيئات السحابية.
- حماية البيانات في السحابة (التشفير، DLP).
- مراقبة التهديدات والاستجابة للحوادث في البيئات السحابية.
- تكوين أمن الشبكات السحابية وجدران الحماية.
- إدارة الامتثال والمتطلبات التنظيمية لأمن السحابة.
- تأمين البيئات الهجينة (Hybrid Clouds) بشكل فعال.

## منهجية الدورة التدريبية:

الأنظمة السحابية وعملية مكثفة، تهدف إلى تزويد المشاركين بفهم عميق تعتمد هذه الدورة التدريبية على منهجية تفاعلية خبراء متخصصون في أمن السحابة، والبيئات الهجينة المتقدمة. تبدأ المنهجية بمحاضرات ومهارات تطبيقية في مجال أمن حيث التي يواجهها المشاركون في بيئات عملهم. تركز يليها جلسات نقاش حيوية لتبادل الخبرات والتحديات متعمقة يقدمها بيئات هجينة، وتطوير يقوم المشاركون بتحليل سيناريوهات اختراق سحابي، الدورة بشكل كبير على دراسات الحالة الواقعية، ورش عمل تطبيقية ومختبرات افتراضية، تتيح للمتدربين استراتيجيات للحماية والاستجابة. تتضمن المنهجية وتقييم الثغرات في يشجع BIG BEN Training ، وإدارة الهوية والوصول، (AWS، Azure، GCP) تكوين سياسات أمنية في منصات سحابية رائدة (مثل لتعزيز التفكير النقدي وقدرات حل المشكلات تحت العمل الجماعي والتعاون بين المتدربين Center وتطبيق حلول التشفير. وهم تحقيق أقصى استفادة من الدورة. تهدف هذه المنهجية الضغط. يتم تقديم تغذية راجعة فردية ومستمرة لضمان وضمان أمان ومرونة مسلحون بالمعرفة والأدوات والخبرة العملية اللازمة إلى تمكين المشاركين من العودة إلى مؤسساتهم البيئات الهجينة المعقدة. لحماية أصولهم في السحابة

## خريطة المحتوى التدريبي (محاور الدورة التدريبية):

## والبيئات الهجينة الوحدة الأولى: أساسيات أمن الحوسبة السحابية

- مقدمة إلى نماذج الحوسبة السحابية وأنواع الخدمات (IaaS, PaaS, SaaS).
- المشتركة. مفاهيم الأمن في السحابة والنموذج المسؤولية
- والهجينة. التهديدات الأمنية الشائعة في البيئات السحابية
- تصميم بنية أمنية سحابية قوية.
- أهمية أمن البيئات الهجينة (On-Premise + Cloud).
- المعايير وأطر العمل لأمن السحابة (NIST CSA CCM, CSF).
- التقليدي. الفرق بين أمن السحابة وأمن مركز البيانات

## البيانات في السحابة الوحدة الثانية: إدارة الهوية والوصول وحماية

- إدارة الهوية والوصول (IAM) في البيئات السحابية.
- مبادئ الامتياز الأقل (Least Privilege).
- التحقق متعدد العوامل (MFA) وتأمينه في السحابة.
- حماية البيانات في حالة السكون وأثناء النقل (Data at Rest/in Transit).
- تقنيات التشفير المتقدمة في السحابة.
- منع فقدان البيانات (DLP) في البيئات السحابية.
- إدارة المفاتيح وتخزين الأسرار (Key Management).

## التحتية كخدمة (IaaS) الوحدة الثالثة: أمن الشبكات السحابية والبنية

- (VPCs). تأمين الشبكات الافتراضية الخاصة بالسحابة
- (ACLs). جدران الحماية السحابية وقوائم التحكم في الوصول
- أمن الحوسبة عديمة الخادم (Serverless Security).
- (Kubernetes). تأمين حاويات (Containers) وأوركسترا الحاويات
- إدارة الثغرات الأمنية في البنية التحتية السحابية.
- أمن واجهات برمجة التطبيقات (APIs) في السحابة.
- السحابة. أمن التكوين (Configuration Security) في

## والبرمجيات كخدمة (SaaS) الوحدة الرابعة: أمن المنصات كخدمة (PaaS)

- منصات التطوير). تأمين خدمات PaaS (مثل قواعد البيانات المدارة،
- مراجعة أمن التطبيقات المبنية على PaaS
- تقييم الأمن لموردي SaaS
- إدارة المخاطر في تطبيقات SaaS
- Security). أمن البرمجيات كخدمة (Software-as-a-Service
- التكامل الآمن بين الخدمات السحابية المختلفة.
- التعامل مع التهديدات الموجهة لتطبيقات SaaS

## والامتثال السحابي الوحدة الخامسة: مراقبة الأمن، الاستجابة للحوادث،

- في السحابة. مراقبة السجلات (Logging) والتدقيق (Auditing)
- السحابية. أدوات وأنظمة إدارة معلومات وأحداث الأمن (SIEM)
- الاستجابة للحوادث الأمنية في البيئات السحابية.
- خطط التعافي من الكوارث في السحابة.
- (ISO ٢٧٠١٧). HIPAA، الامتثال للمتطلبات التنظيمية في السحابة (GDPR،
- تقييم المخاطر المستمر لأمن السحابة.
- (Automation). أتمتة الأمن السحابي (Cloud Security

## 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 ٢٠-٢٥ 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:

على مرونة والتهديدات السيبرانية، كيف يمكن للمؤسسات أن تضمن في ظل التطور المتسارع لخدمات الحوسبة السحابية

التوسع والابتكار في بيئاتها السحابية والهجينة؟ أقصى درجات الأمان والامتثال مع الحفاظ

### ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تغطي جانبًا واحدًا أمن الأنظمة السحابية والبيئات الهجينة المتقدمة، تتميز هذه الدورة بتركيزها المتقدم والشمولي على في التطبيقات العملية من خلال فقط من أمن السحابة. نحن لا نكتفي بتقديم المفاهيم وهو ما يميزها عن الدورات التي حقيقية، مما يمنح المشاركين خبرة مباشرة لا تقدر ورش عمل مكثفة وتمارين مختبرية على منصات سحابية النظرية، بل نغوص الأمنية في هذا ، أن يكون المشاركون على BIG BEN Training Center بثمن. يضمن المحتوى الأكاديمي المتقدم، المقدم من إلى تزويد المشاركين بالمعلومات، بل إلى المجال الحيوي والمتغير باستمرار. هذه الدورة لا اطلاع بأحدث التهديدات والحلول مرونة المؤسسات وتنفيذ، وإدارة استراتيجيات أمنية قوية للبيئات بناء قدراتهم ليصبحوا خبراء قادرين على تصميم، تهدف فقط استثنائية. وقدرتها على مواجهة التحديات السيبرانية بفعالية السحابية والهجينة، مما يعزز