الدورة التدريبية: الاحتراف في إدارة الهوية والوصول (IAM) وأمن الأنظمة



27 - 31 ديسمبر 2026
المنامة
4400 € (للشخص الواحد)
Ref: #IT4330_411049

مقدمة الدورة التدريبية / لمحة عامة:

في المشهد الرقمي المعاصر، حيث تتزايد التهديدات السيبرانية وتتنوع أساليب الهجمات، أصبحت إدارة الهوية والوصول (IAM) وأمن الأنظمة حجر الزاوية في استراتيجيات الأمن السيبراني للمؤسسات. تُعد القدرة على التحكم الدقيق فيمن يمكنه الوصول إلى الموارد الرقمية وما يمكنه فعله بها أمرًا بالغ الأهمية لحماية البيانات الحساسة وضمان استمرارية الأعمال. تقدم هذه الدورة التدريبية المتقدمة من BIG BEN Training Center فهمًا شاملًا لمفاهيم إدارة الهوية والوصول، بدءًا من أساسيات المصادقة والتفويض، وصولًا إلى استراتيجيات التحكم في الوصول القائم على الدور والسمات، وإدارة الوصول المميز. سيتعلم المشاركون كيفية تصميم وتطبيق أنظمة IAM قوية، وكيفية دمجها مع البنى التحتية الأمنية الحالية، بالإضافة إلى فهم أحدث التهديدات والحلول في مجال أمن الأنظمة. تركز الدورة على الجوانب النظرية والتطبيقية، مستلهمة من أفكار رواد الأمن السيبراني مثل البروفيسور روس أندرسون (Ross Anderson) من جامعة كامبريدج، المعروف بأبحاثه الرائدة في أمن الكمبيوتر والتشفير، مما يضمن تزويد المتدربين بمعرفة عميقة ومحدثة. يهدف BIG BEN Training Center إلى تمكين المتدربين من حماية الأنظمة الرقمية بفعالية، والامتثال للمتطلبات التنظيمية، وبناء بيئة آمنة للمعلومات.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو الأمن السيبراني.
- مديرو أمن المعلومات.
- متخصصو إدارة الهوية والوصول.
- مدققو الأنظمة الأمنية.
- مهندسو الشبكات والبنية التحتية.
- المطورون المسؤولون عن أمن التطبيقات.
- مسؤولو الامتثال والمخاطر.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- قطاع التكنولوجيا والاتصالات.
- القطاع الحكومي والدفاع.
- قطاع الرعاية الصحية.
- شركات التجارة الإلكترونية.
- مزودو الخدمات السحابية.
- الشركات التي تتعامل مع بيانات حساسة.

الأقسام المؤسسية المستهدفة:

- إدارات الأمن السيبراني.
- أقسام تكنولوجيا المعلومات.
- إدارات الامتثال والمخاطر.
- أقسام التدقيق الداخلي.
- أقسام تطوير البرمجيات.
- أقسام إدارة الأنظمة.

أهداف الدورة التدريبية:

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

- تصميم وتنفيذ أنظمة إدارة الهوية والوصول (IAM) شاملة.
- تطبيق مبادئ المصادقة والتفويض المتقدمة.
- إدارة الوصول المميز (PAM) وتقليل المخاطر المرتبطة به.
- فهم آليات (Single Sign-On (SSO Federationg.
- تأمين الأنظمة ضد الهجمات المستندة إلى الهوية.
- إجراء تقييمات للثغرات الأمنية المتعلقة بالهوية والوصول.
- الامتثال للمتطلبات التنظيمية ومعايير الأمن ذات الصلة.
- تطوير استراتيجيات الأمن السيبراني القائمة على الهوية.
- بناء بيئة عمل آمنة وموثوقة من خلال إدارة الوصول الفعالة.

منهجية الدورة التدريبية:

يقدم BIG BEN Training Center هذه الدورة التدريبية بمنهجية شاملة تركز على التعلم التفاعلي والتطبيقي، لضمان اكتساب المتدربين مهارات عملية قابلة للتنفيذ في مجال إدارة الهوية والوصول وأمن الأنظمة. تجمع المنهجية بين الشرح النظري المتعمق لأحدث المفاهيم والتقنيات، مع التركيز على دراسات الحالة الواقعية التي تُحلل التحديات الأمنية المعقدة وتُقدم حلولًا فعالة. تُشجع ورش العمل الجماعية المتدربين على التعاون في تصميم وتنفيذ حلول IAM، ومحاكاة سيناريوهات الاختراق، وتطبيق أفضل الممارسات الأمنية. تُعد الجلسات التفاعلية جزءًا لا يتجزأ من الدورة، حيث تتيح الفرصة لطرح الأسئلة، والمناقشات المفتوحة، وتبادل الخبرات بين المشاركين والمدربين الخبراء. يتم استخدام أدوات ومنصات تدريب متخصصة لمحاكاة بيئات العمل الحقيقية، مما يُمكّن المتدربين من تطبيق المعرفة المكتسبة وتطوير قدراتهم في بيئة آمنة ومُتحكم بها. يهدف هذا النهج إلى تزويد المتدربين بالمعرفة النظرية القوية والخبرة العملية اللازمة لمواجهة تحديات الأمن السيبراني الحديثة بثقة وكفاءة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات إدارة الهوية والوصول (IAM).

- مقدمة إلى مفاهيم IAM وأهميتها في الأمن السيبراني.
- المصادقة (Authentication) وأنواعها (MFA, SSO).
- التفويض (Authorization) ونماذج التحكم في الوصول (RBAC, ABAC).
- دورة حياة الهوية وإدارة المستخدمين.
- مفاهيم إدارة الجلسات والأمن.
- مراجعة الهوية والوصول والتدقيق.
- التحديات الأمنية الشائعة في IAM.

الوحدة الثانية: تقنيات المصادقة المتقدمة والهوية الموحدة.

- المصادقة متعددة العوامل (MFA) وتطبيقها.
- تسجيل الدخول الموحد (SSO) وبروتوكولاته (SAML, OAuth, OpenID Connect).
- إدارة الهوية الموحدة (Federated Identity Management).
- المصادقة بدون كلمة مرور (Password less Authentication).
- التحكم في الوصول التكيفي والقائم على السياق.
- أمن الهوية في بيئات الحوسبة السحابية.
- أمن الهوية للخدمات المصغرة (Microservices).

الوحدة الثالثة: إدارة الوصول المميز (PAM) وأمن الأنظمة.

- مقدمة إلى PAM وأهميتها في حماية الأصول الحساسة.
- إدارة الحسابات المميزة (Privileged Accounts).
- مراقبة الجلسات المميزة وتسجيلها.
- إدارة كلمات المرور المميزة (Privileged Password Management).
- التحكم في وصول المستخدمين المميزين (Just-in-Time Access).
- عزل الجلسات المميزة.
- دمج PAM مع أنظمة IAM الأخرى.

الوحدة الرابعة: حوكمة الهوية (IGA) والامتثال الأمني.

- مفاهيم حوكمة الهوية والإدارة (IGA).
- مراجعات الوصول (Access Reviews) وإصدار الشهادات.
- فصل الواجبات (Segregation of Duties - SoD).
- إدارة دورة حياة الوصول.
- الامتثال للمعايير واللوائح (GDPR, HIPAA, SOC 2).
- إعداد التقارير والتدقيق لأغراض الامتثال.
- بناء سياسات وإجراءات حوكمة الهوية.

الوحدة الخامسة: أمن الأنظمة المتقدم والاتجاهات المستقبلية.

- تأمين الخوادم وأنظمة التشغيل.
- أمن قواعد البيانات وتأمين البيانات في حالة السكون والحركة.
- أمن الشبكات وحماية نقاط النهاية.
- الاستجابة للحوادث الأمنية المتعلقة بالهوية.
- الذكاء الاصطناعي وتعلم الآلة في أمن الهوية.
- الهوية اللامركزية والبلوك تشين.
- التحديات المستقبلية في أمن الهوية والوصول.

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:

كيف يمكن للمؤسسات تحقيق التوازن بين توفير وصول سهل ومرن للمستخدمين إلى الأنظمة والموارد، وبين تطبيق أقصى مستويات الأمان الصارمة لمنع الاختراقات والوصول غير المصرح به؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية بتقديمها لنهج شامل وعميق في مجال إدارة الهوية والوصول وأمن الأنظمة، مما يجعلها مختلفة عن الدورات التي قد تركز على جانب واحد فقط. يلتزم BIG BEN Training Center بتزويد المتدربين بأكثر من مجرد معلومات نظرية؛ حيث يتم التركيز على الرؤى العملية والأمثلة التطبيقية المستقاة من تحديات الأمن السيبراني الفعلية. بدلًا من مجرد استعراض الأدوات والتقنيات، تُقدم الدورة فهمًا معمقًا للمبادئ الأمنية الكامنة وراء هذه الحلول، مما يُمكّن المتدربين من تصميم وتنفيذ استراتيجيات IAM وأمن أنظمة قوية وفعالة. كما تتميز الدورة بتغطيتها للاتجاهات المستقبلية في هذا المجال، مثل الذكاء الاصطناعي والهوية اللامركزية، مما يُعد المشاركين للتحديات القادمة. هذا المزيج الفريد من العمق النظري، والتطبيق العملي، والرؤية المستقبلية، يُمكّن خريجي هذه الدورة من أن يصبحوا قادة في مجال الأمن السيبراني، قادرين على حماية الأصول الرقمية لمؤسساتهم بفعالية وثقة.