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

Ref: #IT4330

مقدمة الدورة التدريبية / لمحة عامة:

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

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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:

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

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

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات إدارة الهوية والوصول (IAM).

- السيبراني. مقدمة إلى مفاهيم IAM وأهميتها في الأمن
- 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.

الموحدة. الوحدة الثانية: تقنيات المصادقة المتقدمة والهوية

- 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).

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

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

الوحدة الخامسة: أمن الأنظمة المتقدم والاتجاهات المستقبلية

- تأمين الخوادم وأنظمة التشغيل.
- والحركة: أمن قواعد البيانات وتأمين البيانات في حالة السكون
- 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:

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:

الصارمة لمنع سهل ومرن للمستخدمين إلى الأنظمة والموارد، وبين كيف يمكن للمؤسسات تحقيق التوازن بين توفير وصول

الاختراقات والوصول غير المصرح به؟ تطبيق أقصى مستويات الأمان

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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