BLACKBIRD FOR TRAINING

هندسة أمن الشبكات القائمة على مبدأ انعدام الثقة



هندسة أمن الشبكات القائمة على مبدأ انعدام الثقة

مقدمة

في ظل ازدياد التهديدات السيبرانية وتطور أساليب الهجمات الرقمية، لم تعد الأنظمة الأمنية التقليدية القائمة على الثقة داخل الشبكات كافية لحماية البنى التحتية للمؤسسات. هنا يظهر مفهوم هندسة أمن الشبكات المعمارية القائمة على مبدأ انعدام الثقة كأحد أكثر النماذج تطوراً وفعالية في إدارة الأمن السيبراني.

يرتكز هذا النموذج على مبدأ أساسي هو "عدم الثقة بأي كيان سواء داخل الشبكة أو خارجها"، حيث تُمنح الصلاحيات فقط بناءً على تحقق الهوية والتحكم الدقيق في الوصول. تسعى هذه الدورة إلى تزويد المشاركين بفهم شامل لمفاهيم هندسة انعدام الثقة، وآليات تنفيذها، وأفضل الممارسات لتطبيقها في بيئات العمل الحديثة.

تهدف الدورة إلى تطوير القدرات التحليلية والعملية لدى المهنيين في مجال الأمن السيبراني، من خلال منهج تطبيقي يربط بين المفاهيم النظرية وحلول الحماية الفعلية في المؤسسات.

أهداف الدورة

بنهاية هذه الدورة، سيتمكن المشاركون من:

- فهم الأسس النظرية لمبدأ انعدام الثقة في الأمن السيبراني.
- تحليل نقاط الضعف في الأنظمة التقليدية ومقارنتها بهندسة انعدام الثقة.
- تصميم بنية أمنية متكاملة تعتمد على التحقق المستمر والحد الأدنى من الصلاحيات.
- تطبيق تقنيات المصادقة متعددة العوامل وإدارة الهوية والوصول.
- تنفيذ سياسات التحكم في حركة البيانات داخل الشبكات السحابية والهجينة.
- استخدام أدوات المراقبة والتحليل للكشف عن التهديدات في الوقت الفعلي.
- تطوير خطة انتقال تدريجية لتبني نموذج انعدام الثقة ضمن المؤسسة.



محاور الدورة

اليوم الأول: مدخل إلى هندسة انعدام الثقة

- المفهوم العام لانعدام الثقة وأسباب ظهوره في الأمن السيبراني.
- مقارنة بين أمن الشبكات التقليدي ونموذج انعدام الثقة.
- المبادئ الأساسية: التحقق المستمر، التحكم في الوصول، التقسيم الدقيق للشبكة.
- البنية التحتية التقنية الداعمة للنموذج.
- تحديات التطبيق في المؤسسات ذات الأنظمة القديمة.

اليوم الثاني: إدارة الهوية والتحقق من المستخدمين

- دور الهوية الرقمية في تطبيق انعدام الثقة.
- المصادقة متعددة العوامل وأهميتها في الحماية.
- إدارة الوصول القائمة على الدور والسياسات الديناميكية.
- التحكم في الأجهزة المصرح لها بالدخول إلى الشبكة.
- بناء بيئة مصادقة موحدة في الأنظمة السحابية والهجينة.

اليوم الثالث: التقسيم الشبكي والتحكم في حركة البيانات

- تصميم الشبكات الدقيقة Micro-Segmentation وتقليل مخاطر الاختراق.
- مراقبة حركة البيانات والتحقق من الأنشطة المشبوهة.
- تطبيق سياسات "الأقل صلاحية" في بيئة العمل.
- حماية البيانات أثناء النقل والتخزين باستخدام التشفير.
- آليات الاستجابة الفورية عند اكتشاف محاولات غير مصرح بها.

اليوم الرابع: الرؤية والتحليل الأمني المتقدم

- استخدام أدوات التحليل للكشف المبكر عن التهديدات.
- دور الذكاء الاصطناعي في دعم قرارات الأمان السيبراني.
- دمج أنظمة المراقبة والسياسات الأمنية في منصة واحدة.
- إدارة التنبيهات وتحديد أولويات الاستجابة.
- التحليل الجنائي للحوادث وتوثيقها لتحسين البنية الأمنية.



اليوم الخامس: التنفيذ العملي والاستراتيجية المؤسسية

- تطوير خارطة طريق لتطبيق نموذج انعدام الثقة.
- مراحل الانتقال من الأنظمة التقليدية إلى الأنظمة الحديثة.
- دمج النموذج مع سياسات الحوكمة المؤسسية وإدارة المخاطر.
- اختبار الأداء الأمني وتقييم كفاءة النظام الجديد.
- إعداد خطط استمرارية الأعمال واستعادة الأنظمة بعد الهجمات.

لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- اكتساب معرفة معمقة بمفهوم انعدام الثقة وأحدث تقنيات الأمان السيبراني.
- تطوير القدرة على تصميم وتنفيذ بنى أمنية متقدمة للمؤسسات.
- تعلم كيفية اكتشاف التهديدات مبكراً وتقليل فرص الاختراق.
- تعزيز مهارات إدارة الهوية والتحكم في الصلاحيات الرقمية.
- فهم كيفية حماية البيانات في البيئات السحابية والهجينة.
- تطبيق أدوات التحليل الأمني والاستجابة الفورية للحوادث.
- تحسين كفاءة أنظمة الأمن وتقليل التكاليف التشغيلية طويلة الأمد.
- بناء ثقافة مؤسسية قائمة على الثقة الصفرية لحماية الأصول الرقمية.

الخاتمة

تعد هندسة أمن الشبكات القائمة على مبدأ انعدام الثقة تحولاً جذرياً في منهجية إدارة الأمن السيبراني، فهي لا تركز فقط على الحماية من الخارج، بل تعيد تعريف مفهوم الأمان داخل المؤسسات ذاتها. من خلال تطبيق هذا النموذج، يمكن بناء بيئة رقمية آمنة ومرنة قادرة على التصدي للتحديات المعقدة التي تفرضها الهجمات الإلكترونية الحديثة.

تزود هذه الدورة المشاركين بفهم متكامل لكيفية تصميم وتطبيق هذا النموذج بفعالية، مما يضمن للمؤسسات تحقيق توازن بين الأمان، الأداء، والمرونة التشغيلية. ومع تزايد الاعتماد على الأنظمة الرقمية والسحابة، يصبح تبني مبدأ انعدام الثقة ضرورة استراتيجية وليست خياراً تقنياً فقط.

