CONCEPT

دورة تدقيق الأمن السيبراني: اختبار الضوابط السيبرانية وتقييم نضج البرنامج



دورة تدقيق الأمن السيبراني: اختبار الضوابط السيبرانية وتقييم نضج البرنامج

مقدمة:

دورة تدقيق الأمن السيبراني دورة تدريبية مدتها أسبوع للمدققين الداخليين ومدققي تقنية المعلومات ومراجعي التوكيد، وتنتهي بإعداد برنامج تدقيق للأمن السيبراني ومسودة تقرير موجه إلى لجنة المراجعة لمنظمة محل الدراسة. تكتفي كثير من وظائف التدقيق بمراجعة السياسات وإفادات الإدارة عند إبداء الرأي في المخاطر السيبرانية، فتبقى ثغرات الصلاحيات المميزة والخوادم غير المحدثة وعمليات الاستعادة غير المختبرة خارج نطاق الرأي. يمارس المرشحون مهام التدقيق فعلا، وتعتمد الدورة على دراسات حالة مبنية على مخرجات فحص الثغرات وقوائم الصلاحيات وعينات السجلات ودرجات النضج. وتقدم كور كونسبت هذه الدورة لتعزيز قدرة فرق التدقيق على اختبار الضوابط السيبرانية.

أهداف الدورة:

- تحديد نطاق مهمة تدقيق الأمن السيبراني انطلاقا من حصر الأصول السيبرانية وترتيبها حسب المخاطر ومذكرة نطاق مكتوبة
- تحويل نتائج إطار NIST CSF لإدارة مخاطر الأمن السيبراني وضوابط الملحق A في ISO/IEC 27001 وإجراءات CIS Controls إلى معايير تدقيق قابلة للاختبار
- اختبار ضوابط الهوية والثغرات والرصد والاستجابة للحوادث والنسخ الاحتياطي بالفحص المستندي وإعادة الأداء وعينات البيانات
- تقييم ترتيبات أمن الأطراف الثالثة والحوسبة السحابية وتحديد مدى الاعتماد على تقارير التوكيد الصادرة عن الموردين
- قياس نضج البرنامج السيبراني وفق حدود أدلة محددة وإظهار الفجوة بين الوضع الحالي والوضع المستهدف
- صياغة ملاحظات التدقيق السيبراني وتقرير تستطيع لجنة المراجعة اتخاذ قرارات بناء عليه

الفئة المستهدفة:

- المدققون الداخليون المسؤولون عن إدراج المخاطر السيبرانية في مهام التوكيد
- مدققو تقنية المعلومات المسؤولون عن اختبار الضوابط الأمنية التقنية وأدلتها
- مراجعو التوكيد وخط الدفاع الثاني المسؤولون عن التحقق من ادعاءات البرنامج السيبراني
- موظفو التدقيق المسؤولون عن إعداد أوراق عمل التدقيق السيبراني وملفات الأدلة
- محللو المخاطر والرقابة المسؤولون عن متابعة إجراءات المعالجة السيبرانية حتى إقفالها

محاور الدورة:

اليوم 1: المخاطر السيبرانية ودور المدقق وتحديد نطاق المهمة

- خريطة مشهد التهديدات السيبرانية وربطها بأولويات التوكيد للمدققين
- خريطة التوكيد لوظائف الأمن والمخاطر والتدقيق
- حصر الأصول السيبرانية وتدفقات البيانات لتحديد نطاق التدقيق
- عالم تدقيق الأمن السيبراني واختيار المهام حسب ترتيب المخاطر
- مذكرة نطاق المهمة بأهدافها وحدودها واستثناءاتها

اليوم 2: الأطر الرقابية معايير لتدقيق الأمن السيبراني

- تحويل وظائف NIST CSF إلى أهداف اختبار للتدقيق
- الملف الحالي والملف المستهدف في NIST CSF لمقارنة الفجوات
- ضوابط الملحق A في ISO/IEC 27001 معايير قابلة للاختبار
- إجراءات CIS Controls ومجموعات التطبيق خطوط أساس للتدقيق
- مصفوفة معايير موحدة عبر الأطر لبرنامج تدقيق واحد

اليوم 3: اختبار الضوابط السيبرانية الأساسية

- مراجعة منظومة السياسات السيبرانية وميثاق الأدوار الأمنية
- خطوات اختبار الهوية والوصول للحسابات المميزة وحسابات الوصول عن بعد
- تحليل مخرجات فحص الثغرات وتقرير تقادم التحديثات الأمنية
- اختبار قواعد تنبيهات SIEM لإدارة الأحداث الأمنية وتغطية الاحتفاظ بالسجلات
- مراجعة خطة الاستجابة للحوادث وأدلة التشغيل وسجلات التمارين

اليوم 4: الصمود والأطراف الثالثة وقياس النضج وإشكالات الأدلة

- سجلات اختبار استعادة النسخ الاحتياطية والتحقق من النسخ غير القابلة للتعديل
- استبيانات أمن الأطراف الثالثة والاعتماد على تقارير التوكيد
- مصفوفة المسؤولية المشتركة في الحوسبة السحابية وأدلة مراجعة الإعدادات
- مقياس درجات النضج السيبراني بحدود أدلة لكل مستوى
- اختبارات كفاية الأدلة بالاستفسار والفحص وإعادة الأداء

اليوم 5: دراسة حالة لإعداد برنامج تدقيق الأمن السيبراني ومسودة التقرير

- إعداد مذكرة النطاق ومصفوفة المعايير للمنظمة محل الدراسة
- أوراق اختبار الضوابط لمجالي الوصول والثغرات في الحالة
- خريطة حرارية لنضج الحالة عبر وظائف NIST CSF
- صياغة ملاحظات التدقيق السيبراني بعناصر الواقع والمعيار والسبب والأثر
- استكمال برنامج تدقيق الأمن السيبراني ومسودة تقرير لجنة المراجعة

المهارات التي ستكتسبها:

- تحديد نطاق التدقيق السيبراني
- ربط المعايير الرقابية
- اختبار الصلاحيات المميزة
- تحليل تقادم التحديثات
- تقييم تغطية السجلات
- الاعتماد على توكيد الموردين
- قياس النضج السيبراني
- إعداد تقارير لجنة المراجعة

لماذا تحضر هذه الدورة:

- تسليم برنامج تدقيق للأمن السيبراني ومسودة تقرير لمنظمة محل الدراسة إلى رئيس التدقيق الداخلي لتكييفهما مع خطة التدقيق القادمة
- الحكم على كفاية نتائج فحص الثغرات وقوائم الصلاحيات وسجلات الاستعادة دليلا يدعم رأي التدقيق السيبراني
- تفادي إصدار توكيد سيبراني يقوم على قراءة السياسات وحدها ويترك فجوات رقابية قابلة للاستغلال خارج رأي التدقيق
- نقل مصفوفة المعايير وأوراق اختبار الضوابط إلى فريق التدقيق لتسير مهام التدقيق السيبراني على منهج واحد

الخاتمة:

بعد العودة إلى العمل يسلم المشارك رئيس التدقيق الداخلي برنامج تدقيق للأمن السيبراني ومسودة تقرير قابلين للتكييف مع أنظمة المنظمة وخطة التدقيق لديها. وتستخدم وظيفة التدقيق مصفوفة المعايير للاتفاق على النطاق مع إدارة الأمن، وتتلقى لجنة المراجعة درجات نضج وملاحظات مستندة إلى أدلة لا إلى إفادات. وبعد أول استخدام تراجع الوظيفة الاختبارات التي أنتجت أدلة موثوقة، ومواضع الخلاف على درجات النضج، وسرعة إقفال الإدارة للإجراءات المتفق عليها.

الأسئلة الشائعة:

ما الذي يحتاج المشارك إلى معرفته قبل دورة تدقيق الأمن السيبراني؟

يكفي أن يمارس المشارك مهام التدقيق أو التوكيد وأن يفهم أساسيات اختبار الضوابط. وتفيد معرفة الحسابات والشبكات والأدوات الأمنية بمستوى المستخدم دون حاجة إلى خلفية هندسية، ويساعد إحضار تقرير فحص أو قائمة صلاحيات بعد إخفاء بياناتها على تطبيق دراسات الحالة.

بم تختلف دورة تدقيق الأمن السيبراني عن دورات تدقيق تقنية المعلومات العامة؟

تركز الدورة على البرنامج السيبراني ذاته: معايير الأطر والوصول والثغرات والرصد والاستجابة للحوادث والنسخ الاحتياطي وضوابط الأطراف الثالثة والسحابة وقياس النضج. أما دورات تدقيق تقنية المعلومات العامة فتوزع وقتها على الضوابط العامة وضوابط التطبيقات وتتناول الجانب السيبراني باختصار.

لماذا يجمع تدقيق الأمن السيبراني بين قياس النضج واختبار الضوابط؟

يبين اختبار الضوابط ما إذا كانت كل ضابطة تعمل فعلا، بينما يبين قياس النضج مدى اتساق إدارة البرنامج بأكمله وتطويره. ويتيح الجمع بينهما للجنة المراجعة رؤية الإخفاقات المحددة والمسافة بين الوضع الحالي والوضع المستهدف للبرنامج.

ماذا يعود به المشارك من دورة تدقيق الأمن السيبراني؟

يعود المشارك ببرنامج تدقيق للأمن السيبراني يضم مذكرة نطاق ومصفوفة معايير وأوراق اختبار للضوابط وخريطة حرارية للنضج، إضافة إلى مسودة تقرير لمنظمة محل الدراسة. ويمكن تكييف كل جزء منها مع خطة التدقيق وأنظمة جهته.