



دورة CCSS في عمليات أخطائي الأمن السيبراني



دورة CCSS في عمليات أخصائي الأمن السيبراني

المرجع: 157135_750 التاريخ: 3 - 7 مايو 2027 المكان: تبليسي الرسوم: Euro 5700

نظرة عامة

دورة CCSS في عمليات أخصائي الأمن السيبراني دورة متوسطة لمدة 5 أيام للمحليين وفرق العمليات الأمنية ومديري تقنية المعلومات ووظائف المخاطر والامتثال والتدقيق والمهنيين التقنيين، ويعود المشاركون منها بدليل عمليات أخصائي الأمن السيبراني. تنظم الدورة الحوكمة وتقييم المخاطر وحماية الأصول والهوية ودفاع الشبكات والأجهزة الطرفية وإدارة الثغرات والمراقبة والاستجابة والتعافي والتقارير عبر وظائف NIST CSF 2.0. تطور أجايل للتدريب عمليات أخصائي الأمن السيبراني CCSS.

الفئة المستهدفة

- وظائف تحليل الأمن السيبراني المسؤولة عن تقييم التهديدات والثغرات والأدلة الدفاعية
- وظائف العمليات الأمنية المسؤولة عن المراقبة والفرز وتنسيق الحوادث
- وظائف إدارة تقنية المعلومات المسؤولة عن الهويات والأجهزة والشبكات والعمليات الآمنة
- وظائف المخاطر والامتثال المسؤولة عن الحوكمة والمعالجة وأدلة الضوابط
- وظائف التدقيق والضمان التقني المسؤولة عن تقييم ممارسات الأمن السيبراني

تفترض الدورة أن المشاركين يعملون مع أنظمة تقنية أو ضوابط أمنية أو سجلات مراقبة أو سجلات مخاطر، وتستبعد استغلال اختبار الاختراق وتطوير البرمجيات الضارة والاختساب الجنائي وأي ادعاء بأن الحضور يمنح شهادة.

الإدارات والقطاعات المستهدفة

تدعم الدورة الإدارات والقطاعات التي تحتاج إلى تنسيق مخاطر الأمن السيبراني والعمليات الدفاعية.

- الأمن السيبراني والعمليات الأمنية
- البنية التحتية لتقنية المعلومات وإدارة الخدمات
- المخاطر والامتثال والتدقيق الداخلي
- الخدمات المالية والرعاية الصحية والاتصالات
- العمليات الصناعية والخدمات اللوجستية والرقمية



أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق وظائف NIST CSF 2.0 على عمليات الأمن السيبراني
- تقييم المخاطر والأصول والهويات وأولويات الضوابط
- بناء مسارات دفاع الشبكات والأجهزة وإدارة الثغرات
- تحليل أدلة المراقبة الأمنية والكشف
- ترتيب إجراءات الاستجابة للحوادث والتعافي
- بناء دليل عمليات أخصائي الأمن السيبراني

جدول الدورة

اليوم 1: حوكمة المخاطر السيبرانية وتحديدها

- خريطة وظائف ونتائج NIST CSF 2.0
- مصفوفة أدوار حوكمة الأمن السيبراني
- سجل تبعيات الأصول والخدمات والبيانات
- ورقة التهديد والثغرة والأثر والاحتمالية
- لوحة معالجة المخاطر السيبرانية وتقاريرها

اليوم 2: حماية الأصول والهويات

- مصفوفة التحكم في الهوية والوصول ذي الصلاحيات
- مخطط تجزئة الشبكة وحدود الثقة
- خط أساس تهيئة أمن الأجهزة الطرفية
- خريطة ضوابط حماية البيانات ومعالجتها
- خطة التوعية الأمنية ومخاطر العنصر البشري



اليوم 3: إدارة الثغرات وكشف الأحداث

- مسار استقبال الثغرات والتحقق منها
- مصفوفة أولوية المعالجة المبنية على المخاطر
- خريطة تغطية التسجيل والقياس الأمني
- سجل حالات استخدام الكشف وفرز التنبيهات
- قائمة فحص فجوات المراقبة والتصعيد

اليوم 4: الاستجابة والتعافي والتقارير

- مصفوفة تصنيف الحوادث ودرجة شدتها
- خطة احتواء الحوادث وحفظ الأدلة
- مسار أدوار الاستجابة والاتصال
- خريطة تبعيات التعافي وأولوية الاستعادة
- تقرير الأمن التشغيلي والإداري

اليوم 5: ممارسة أخصائي الأمن السيبراني

- تمرين: توصيف المخاطر السيبرانية والأصول الحرجة
- تمرين: تصميم ضوابط الهوية والشبكة والأجهزة الطرفية
- تمرين: ترتيب الثغرات وفجوات الكشف
- تمرين: تنسيق الاستجابة للحوادث والتعافي
- المشروع الختامي: دليل عمليات أخصائي الأمن السيبراني

التمارين التطبيقية

تستخدم الدورة أنشطة مقترحة من الخدمات المالية والرعاية الصحية والاتصالات والعمليات الصناعية والخدمات اللوجستية والرقمية.

- نشاط مقترح: ربط الأصول الحرجة والتبعيات والتهديدات والثغرات وقرارات المعالجة.
- نشاط مقترح: تصميم ضوابط الهوية والتجزئة والأجهزة الطرفية وحماية البيانات لخدمة محددة.
- نشاط مقترح: ترتيب نتائج الثغرات وبناء أولويات الكشف والتصعيد.
- نشاط مقترح: تنسيق الاحتواء وحفظ الأدلة والاتصال والتعافي والتقارير لحادث أمني.



الأسئلة الشائعة

لمن تناسب دورة CCSS في عمليات أخصائي الأمن السيبراني، وماذا تفترض؟

تناسب وظائف الأمن وتقنية المعلومات والمخاطر والامتثال والتدقيق والوظائف التقنية، وتفترض العمل مع أنظمة أو ضوابط أو سجلات مراقبة أو سجلات مخاطر.

كيف تختلف دورة CCSS لأخصائي الأمن السيبراني عن تدريب اختبار الاختراق؟

تنظم دورة CCSS الحوكمة والمخاطر والحماية والمراقبة والثغرات والحوادث والتعافي والتقارير، بدلا من تعليم تقنيات الاستغلال أو الاختبار الهجومي.

كيف ينظم NIST CSF 2.0 عمليات أخصائي الأمن السيبراني؟

ينظم NIST CSF 2.0 العمليات عبر نتائج الحوكمة والتحديد والحماية والكشف والاستجابة والتعافي التي تربط قرارات المخاطر بالعمل الدفاعي والتحسين.

كيف يرتب أخصائيو الأمن السيبراني الثغرات والتنبيهات؟

يرتب الأخصائيون الثغرات والتنبيهات وفق أهمية الأصل والتعرض وقابلية الاستغلال والنشاط الملحوظ وتغطية الضوابط وأثر الأعمال والثقة وإلحاح الاستجابة.

ماذا يتضمن دليل عمليات أخصائي الأمن السيبراني؟

يتضمن الدليل أدوار الحوكمة وتبعيات الأصول وقرارات المخاطر وخطوط الحماية ومسارات الثغرات وتغطية القياس وحالات الكشف وإجراءات الحوادث وأولويات التعافي والتقارير ومالكي التحسين.

الخاتمة

يعود المشاركون بدليل عمليات أخصائي الأمن السيبراني مدعوم بلوحات المخاطر وخرائط الضوابط وخطوط الدفاع ومسارات الثغرات وسجلات الكشف وخطط الحوادث وخرائط التعافي والتقارير. يحول الدليل المهام الأمنية المنفصلة إلى قرارات تشغيلية منسقة. ويوفر أساسا قابلا للتكرار لترتيب الأولويات والتصعيد والاستجابة والتعافي والتحسين.