

دورة تصميم برنامج التوعية بالأمن السيبراني: مخاطر الأدوار ومحاكاة التصيد وقياس السلوك

2027 – 15 يناير

جنييف





دورة تصميم برنامج التوعية بالأمن السيبراني: مخاطر الأدوار ومحاكاة التصيد وقياس السلوك

المرجع: 311_21063 التاريخ: 11 - 15 يناير 2027 المكان: جنيف الرسوم: GBP 5500

ملخص البرنامج

تصميم برنامج التوعية بالأمن السيبراني محور دورة تدريبية تمتد 5 أيام بمستوى إداري للمديرين ورؤساء الأقسام المسؤولين عن سلوك العاملين الأمني، ويخرج منها كل مشارك بخطة برنامج للتوعية السيبرانية لمؤسسة أو إدارة واحدة. فتصرفات العاملين ما زالت من أبرز مسارات الحوادث، بينما يأتي جهد التوعية في الغالب عاما وغير مقيس. ويتدرج البرنامج من الغاية والفئات المستهدفة، مروراً بمخاطر الأدوار وتشخيص السلوك، إلى تصميم المحتوى والمحاكاة، ثم إلى القياس وخطة عملية. تقدم مارس للتدريب المملكة المتحدة هذا البرنامج في تصميم برنامج التوعية بالأمن السيبراني.

المبررات المؤسسية

جلسات التوعية التي تتجاهل مخاطر الأدوار تنسى سريعا، والنتائج التي تعرض في صورة حضور لا تكشف شيئا عن السلوك. أما المديرون الذين يستهدفون الأدوار والعادات المسببة للتعرض، ويجرون محاكاة واقعية، ويتبعون ما يفعله العاملون فعلا، فيستطيعون إثبات الأنشطة التي تغير السلوك وإيقاف ما لا يفيد منها.

- القابلية للتصيد: تنخفض حين تركز المحاكاة والتغذية الراجعة على الأدوار والرسائل التي تخفق أكثر من غيرها.
- سرعة الإبلاغ عن الحوادث: تتحسن حين يشجع مسار إبلاغ واضح وتغذية راجعة إيجابية العاملين على رفع الشكوك مبكرا.
- فاعلية الإنفاق على التوعية: تتحسن حين تحل مقاييس السلوك محل مقاييس الحضور.

المبادئ والأساس المعرفي

- NIST SP 800-50 Rev. 1 إرشادات بناء برنامج تعلم في الأمن السيبراني والخصوصية: تنظم إرشاداته عمل دورة حياة البرنامج في الجلستين 1 و4.
- Fogg Behavior Model نموذج فوغ للسلوك: يوجه ربطه بين الدافع والقدرة والمحفز تحليل العوائق في الجلسة 2 وخيارات التصميم في الجلسة 3.
- Kirkpatrick Model نموذج كيركباتريك للتقييم: تقوم عليه مستوياته من رد الفعل والتعلم والسلوك والنتائج أعمال التقييم في الجلسة 4.



المشاركون المستهدفون

- مدبرون مسؤولون عن طريقة تعامل فرقهم مع المعلومات واستجابتها للرسائل المشبوهة.
- رؤساء أقسام يرفعون أنشطة التوعية ويتيحون وقت العاملين لها.
- قيادات التوعية والتعلم التي تخطط المحتوى والقنوات والجدول.
- جهات الاتصال في الأمن والمخاطر التي توفر بيانات الحوادث وتحدد رسائل السياسات.

يخدم البرنامج المصارف والرعاية الصحية والخدمات الحكومية والصناعات التحويلية.

مخرجات التعلم

1. سيكون المشاركون قادرين على تقسيم الفئات المستهدفة وترتيب الموضوعات بحسب مخاطر الأدوار باستخدام مصفوفة تحليل.
2. سيكون المشاركون قادرين على تشخيص عوائق السلوك من بيانات الحوادث والحوادث الوشيكة وخط أساس للتصيد.
3. سيكون المشاركون قادرين على بناء موجز لمحاكاة التصيد يتضمن مسارات التغذية الراجعة والإبلاغ.
4. سيكون المشاركون قادرين على تقييم أنشطة التوعية بمقاييس السلوك لا بمقاييس الحضور.
5. سيكون المشاركون قادرين على تبرير قواعد التعزيز وإرشادات التصعيد أمام مسؤول الأمن.
6. سيكون المشاركون قادرين على ترتيب أولويات خطة القنوات والجدول ضمن ميزانية محدودة.

هيكل البرنامج

اليوم 1: تصميم برنامج التوعية بالأمن السبراني: الغاية والفئات

ما الذي يجب أن يغيره البرنامج، ولدى من؟

- ميثاق برنامج التوعية
- دورة حياة البرنامج وفق NIST SP 800-50 Rev. 1
- خريطة تقسيم الفئات المستهدفة
- بيان احتياجات التعلم
- مراجعة حالتين لحوادث في قطاعين سببها تصرف العاملين

اليوم 2: مخاطر الأدوار وتشخيص السلوك

أي الأدوار والعادات تسبب التعرض، وما الذي يمنع العاملين من التصرف بأمان؟



- مصفوفة مخاطر الأدوار
- مراجعة الحوادث والحوادث الوشيكة
- خط أساس القابلية للتصيد
- تحليل العوائق وفق Fogg Behavior Model
- مراجعة فجوات فهم السياسات

اليوم 3: المحتوى والقنوات والمحاكاة

ما الذي يجب أن تراه كل فئة، وبأي وسيلة، ومتى؟

- خطة موضوعات بحسب الأدوار
- موجز تصميم محاكاة التصيد
- مسار الإبلاغ وحلقة التغذية الراجعة
- خطة القنوات والجدول
- حزمة إحاطة المديرين

اليوم 4: المقاييس والتعزيز ورفع التقارير

كيف يثبت تغير السلوك ويستدام؟

- مجموعة مؤشرات السلوك
- مستويات التقييم وفق Kirkpatrick Model
- قواعد تفسير نتائج المحاكاة
- إرشادات التعزيز والتصعيد
- نموذج تقرير القيادة

اليوم 5: تطبيق تصميم برنامج التوعية بالأمن السيبراني على مؤسسة واحدة

هل خطة البرنامج جاهزة ليعتمدها الراعي ومسؤول الأمن؟

- تطبيق خريطة التقسيم من الجلسة 1 على المؤسسة المختارة
- اختبار مصفوفة المخاطر من الجلسة 2 على بيانات حوادث نموذجية
- فحص موجز المحاكاة من الجلسة 3 مقابل خطة الموضوعات
- تطبيق مجموعة المؤشرات من الجلسة 4 على القضايا المفتوحة
- إنجاز خطة برنامج التوعية السيبرانية



المنهجية

يقوم البرنامج على تمارين منظمة تعتمد مؤسسة مجهولة المصدر وبيانات نموذجية للحوادث والمحاكاة. يحدد المشاركون مخاطر الأدوار ويشخصون العوائق ويصوغون موجزات المحاكاة ويختارون المقاييس في فرق صغيرة، ثم يدافعون عن خطتهم أمام لجنة قيادية محاكاة. ولا يتطلب البرنامج خلفية تقنية في الأمن.

- نشاط مقترح: ترتيب ستة أدوار بحسب التعرض باستخدام بيانات حوادث وتصيد نموذجية.
- نشاط مقترح: صياغة موجز محاكاة ورسالة تغذية راجعة لفريق مالي.
- نشاط مقترح: استبدال خمسة مقاييس حضور بمؤشرات للسلوك.

المخرج الختامي

يعد كل مشارك خطة برنامج للتوعية السيبرانية لمؤسسة أو إدارة واحدة. وتتضمن ميثاقا للبرنامج، ومصفوفة لمخاطر الأدوار، وجدولا للموضوعات والقنوات، وموجزا للمحاكاة، ومجموعة مؤشرات للسلوك، ونموذجا للتقارير. وتستخدم لإحاطة الراعي ومسؤول الأمن وإطلاق الدورة الأولى من التوعية.

الأسئلة الشائعة

هل يناسب تصميم برنامج التوعية بالأمن السيبراني المديرين من غير ذوي الخبرة الأمنية؟

نعم، فتصميم برنامج التوعية بالأمن السيبراني بمستوى إداري، ويفترض مسؤولية عن سلوك العاملين أو أنشطة التوعية، لا مهارات في الأمن التقني أو البرمجة.

ما النماذج التي يقوم عليها تصميم برنامج التوعية بالأمن السيبراني؟

يقوم تصميم برنامج التوعية بالأمن السيبراني على 1. NIST SP 800-50 Rev. 1 لدورة حياة البرنامج، وFogg Behavior Model للعوائق، Kirkpatrick Modelg للتقييم.

كيف تستخدم الخطة الناتجة عن تصميم برنامج التوعية بالأمن السيبراني في العمل؟

تستخدم الخطة الناتجة عن تصميم برنامج التوعية بالأمن السيبراني لإحاطة الراعي ومسؤول الأمن، وإطلاق الدورة الأولى من التوعية، ورفع نتائج السلوك.



بماذا يختلف تصميم برنامج التوعية بالأمن السيبراني عن التدريب الأمني للمتخصصين؟

يركز تصميم برنامج التوعية بالأمن السيبراني على سلوك العاملين ومخاطر الأدوار والقياس، بينما يركز التدريب الأمني للمتخصصين على الدفاع التقني والأدوات.