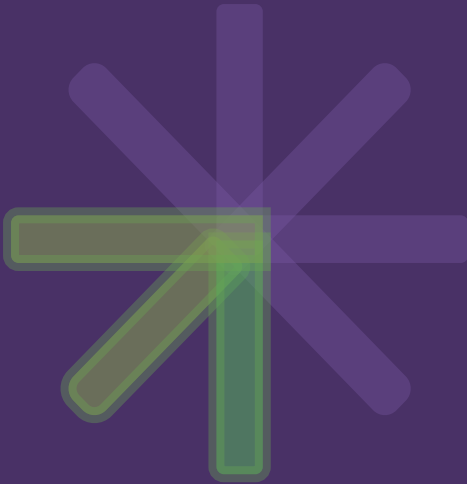


دورة قيادة الأمن المؤسسي وتقييم التهديدات وحماية المنشآت والاستجابة للحوادث





دورة قيادة الأمن المؤسسي وتقييم التهديدات وحماية المنشآت والاستجابة للحوادث

ملخص البرنامج

قيادة الأمن المؤسسي وتقييم التهديدات وحماية المنشآت والاستجابة للحوادث دورة تدريبية تمتد 5 أيام بمستوى متقدم، موجهة إلى رؤساء الأمن المؤسسي وأمن المنشآت، ويخرج منها كل مشارك باستراتيجية أمنية وخطة تشغيل لموقع يختاره. فكريا ما تقاس إدارات الأمن بعدد ساعات الحراسة وكاميرات المراقبة، لا بقدرتها على خفض التهديدات الفعلية للأفراد والأصول والعمليات. ويتدرج البرنامج من تقييم التهديدات والمخاطر إلى تصميم الحماية، ثم إدارة العمليات الأمنية والاستجابة للحوادث وقياس الأداء. تقدم هذا البرنامج في قيادة الأمن المؤسسي وتقييم التهديدات مارس للتدريب المملكة المتحدة.

المبررات المؤسسية

حين تشتري إجراءات الحماية دون تقييم للتهديدات، تنفق المنشأة على ضوابط ظاهرة وتترك ثغرات حقيقية مفتوحة، ويصعب عليها تبرير ميزانية الأمن. كما تتحول الحوادث الصغيرة إلى خسائر وأضرار بالسمعة حين لا تختبر خطط الاستجابة. ويتيح برنامج أمني قائم على المخاطر للقيادات أن تبين لمجلس الإدارة ما يحمله كل إجراء ولماذا.

- التعرض للمخاطر الأمنية: ينخفض حين تقيم التهديدات المعقولة وتقابل بضوابط متعددة الطبقات ومختبرة.
- كفاءة الإنفاق الأمني: تتحسن حين يتبع الإنفاق على الحراسة والتقنية أولويات المخاطر.
- أثر الحوادث: يتراجع حين يتدرب الفريق على الاكتشاف والتصعيد والاستجابة وتقاس نتائجها.

المبادئ والأساس المعرفي

- معيار ISO 18788 لنظام إدارة العمليات الأمنية: ينظم تخطيط العمليات الأمنية وضبطها وتقييمها في الجلسة 3 والجلسة 5.
- معيار ISO 31000 لإدارة المخاطر: يوفر منطق تقييم المخاطر ومعالجتها المطبق على التهديدات الأمنية في الجلسة 1.
- نموذج الردع والاكتشاف والإعاقة والاستجابة: يشكل تصميم الحماية متعددة الطبقات الذي تقيمه الجلسة 2.
- منهج CPTED لمنع الجريمة من خلال التصميم البيئي: يوجه المخطط العام والإنارة والمراقبة الطبيعية وتحديد الحيز في الجلسة 2.



المشاركون المستهدفون

- القيادات المسؤولة عن حماية الأفراد والمواقع والأصول على مستوى المؤسسة.
- المدبرون الذين يوجهون قوات الحراسة والمقاولين وغرف العمليات الأمنية.
- رؤساء المرافق الذين يحددون مواصفات أنظمة التحكم في الدخول والأنظمة الأمنية الإلكترونية.
- القيادات التي تنسق الاستجابة للحوادث الأمنية مع فرق الطوارئ والأزمات.

يخدم البرنامج قطاعات الطاقة والمرافق والمنشآت الحكومية والمصارف والضيافة.

مخرجات التعلم

1. سيكون المشاركون قادرين على بناء تقييم للتهديدات ونقاط الضعف الأمنية في موقع محدد.
2. سيكون المشاركون قادرين على تقييم تصاميم الحماية وفق مبادئ الردع والاكتشاف والإعاقة والاستجابة متعددة الطبقات.
3. سيكون المشاركون قادرين على تحديد متطلبات التحكم في الدخول والأنظمة الأمنية الإلكترونية بما يتناسب مع المخاطر المقيمة.
4. سيكون المشاركون قادرين على تصميم إجراءات قوة الحراسة وغرفة العمليات الأمنية مع مسارات تصعيد واضحة.
5. سيكون المشاركون قادرين على تشخيص مواطن الضعف في الاستجابة للحوادث الأمنية وممارسات التحقيق.
6. سيكون المشاركون قادرين على تبرير خطة التشغيل الأمني ومؤشرات أدائها أمام الإدارة العليا.

هيكل البرنامج

اليوم 1: تقييم التهديدات في الأمن المؤسسي

ما التهديدات الأهم للمؤسسة، وما مدى انكشاف كل موقع لها؟

- تفويض الأمن المؤسسي وهيكل حوكمته
- تحديد التهديدات وتوصيف الجهات المعادية
- حرجية الأصول وترتيب العواقب
- أساليب مسح نقاط الضعف والجولات الميدانية في المواقع
- سجل المخاطر الأمنية وخيارات المعالجة وفق ISO 31000

اليوم 2: تصميم الحماية والأمن المادي

كيف تصمم إجراءات الحماية المادية متعددة الطبقات بحيث يكتشف المتسلل ويعاقب قبل وقوع الضرر؟



- الردع والاكتشاف والإعاقة والاستجابة ومبدأ الدفاع المتعمق
- مبادئ CPTED في المخطط العام والإنارة والمراقبة الطبيعية
- إجراءات المحيط والحواجز والحد من خطر المركبات
- التحكم في الدخول وإدارة الهوية وإجراءات الزوار
- متطلبات كاميرات المراقبة وأنظمة كشف التسلل وتكامل الأنظمة

اليوم 3: إدارة العمليات الأمنية

كيف تنظم الكوادر والإجراءات وغرفة العمليات لتحقيق الحماية في كل مناوبة؟

- التخطيط التشغيلي والضبط وفق ISO 18788
- توزيع قوة الحراسة وتعليمات المواقع وتصميم الدوريات
- أدوار غرفة العمليات الأمنية والإنذارات والتصعيد
- اختيار مزودي خدمات الحراسة المتعاقدين والإشراف عليهم
- أمن الأفراد وضوابط التهديد الداخلي

اليوم 4: الاستجابة للحوادث الأمنية والتحقيقات

كيف تستجيب إدارة الأمن للحوادث وتحقق فيها وتستخلص منها الدروس؟

- تصنيف الحوادث الأمنية وخطط الاستجابة لها
- إجراءات التهديد بالمتفجرات والتسلل والعنف في مكان العمل
- التنسيق مع فرق الطوارئ والأزمات واستمرارية الأعمال
- إجراءات التحقيق الداخلي والتعامل مع الأدلة
- مراجعة ما بعد الحادث والدروس المستفادة

اليوم 5: الأداء الأمني وخطة التشغيل

كيف تجتمع التهديدات والضوابط والعمليات في خطة واحدة تعتمدها الإدارة؟

- مؤشرات الأداء الأمني وتقارير التأكيد
- تطبيق تقييم التهديدات على موقع أحد المشاركين
- تطبيق مراجعة طبقات الحماية مقابل التهديدات المقيمة
- تطبيق اختبار إجراءات غرفة العمليات والاستجابة
- إنجاز الاستراتيجية الأمنية وخطة التشغيل للموقع



المنهجية

يعتمد البرنامج على تحليل حالات لحوادث أمنية في مواقع الطاقة والمنشآت الحكومية والمنشآت التجارية، مع تمارين منظمة ومحاكاة على الطاولة. فيقيم المشاركون التهديدات، وينقدون مخططات الحماية، ويختبرون التصعيد في غرفة العمليات، وينفذون سيناريو للاستجابة لحدث.

- نشاط مقترح: إجراء جولة لمسح نقاط الضعف على مخطط منشأة نموذجية.
- نشاط مقترح: إعادة تصميم المحيط ومسارات الدخول وفق مبادئ CPTED.
- نشاط مقترح: تنفيذ تمرين محاكاة على الطاولة لحدث تسلل في مناوبة ليلية.

المخرج الختامي

يعد كل مشارك استراتيجية أمنية وخطة تشغيل لموقعه، تتضمن تقييم التهديدات، والمخاطر مرتبة حسب الأولوية، وطبقات الحماية، ومتطلبات التقنية والحراسة، وإجراءات غرفة العمليات، وترتيبات الاستجابة للحوادث، ومؤشرات الأداء، في صيغة جاهزة لاعتماد الإدارة العليا.

الأسئلة الشائعة

هل يناسب تدريب قيادة الأمن المؤسسي المديرين الجدد في منصب رئيس الأمن؟

نعم، إذا كنت تدير فرق الأمن أو المرافق بالفعل، فهو يفترض خبرة في العمليات الأمنية دون اشتراط تدريب سابق في تقييم التهديدات أو أنظمة إدارة الأمن.

ما المعايير التي تستند إليها قيادة الأمن المؤسسي وتقييم التهديدات؟

تستند إلى معيار ISO 18788 لإدارة العمليات الأمنية، ومعيار ISO 31000 لإدارة المخاطر، ونموذج الردع والاكتشاف والإعاقة والاستجابة، ومنهج CPTED لمنع الجريمة من خلال التصميم البيئي.

كيف تستخدم خطة التشغيل في الأمن المؤسسي في العمل؟

تستخدمها لتبرير أولويات الأمن وميزانيته أمام الإدارة العليا، وتوجيه مزودي الحراسة، ومتابعة الأداء عبر مؤشرات متفق عليها.

بم تختلف قيادة الأمن المؤسسي عن برامج إدارة الأمن السيبراني؟

تناول الأمن المادي وأمن الأفراد والعمليات لحماية الناس والمواقع والأصول، بدلا من حماية الشبكات والأنظمة والبيانات.