CONCEPT

الأمن السيبراني للطيران وأنظمة النقل الذكية: رصد مراكز العمليات الأمنية والاستجابة للحوادث

31 مايو – 4 يونيو 2027

لندن - فندق أربع نجوم في وسط لندن



الأمن السيبراني للطيران وأنظمة النقل الذكية: رصد مراكز العمليات الأمنية والاستجابة للحوادث

المرجع: 20979_885 **التاريخ:** 31 مايو – 4 يونيو 2027 **المكان:** لندن - فندق أربع نجوم في وسط لندن **الرسوم:** SAR 25300

مقدمة:

لا تبقى حوادث الأمن السيبراني للطيران وأنظمة النقل الذكية داخل حدود تقنية المعلومات، فهجوم فدية على منصات تسجيل الركاب المشتركة أو تلاعب في تغذية بيانات الرحلات أو اختراق متعاقد يدير وحدات التحكم في الإشارات قد يؤخر الإقلاع ويشل الممرات المرورية خلال دقائق. وما زالت مطارات وشركات طيران وهيئات نقل كثيرة تراقب هذه البيئات بقواعد صممت لشبكات المكاتب، دون دليل تشغيل يربط محللي الأمن بمديري المناوبة ومشغلي المرور. تبني هذه الدورة من كور كونسبت قدرات الكشف وتبادل المعلومات والاستجابة الخاصة بأنظمة المطارات والملاحة الجوية والطرق، ويعد المشاركون نموذج تهديدات قطاعيا ودليل استجابة للحوادث لمطار أو مركز إدارة مرور في دراسة حالة.

أهداف الدورة:

- رسم خريطة سطح الهجوم السيبراني لأنظمة تشغيل المطارات ومعالجة الركاب وتقنية معلومات شركات الطيران والروابط المتصلة بإدارة الحركة الجوية والبنية التحتية على جوانب الطرق
- بناء نموذج تهديدات خاص بكل نمط نقل يربط أهداف الخصوم بعواقبها على الرحلات والركاب وحركة الطرق
- تبادل معلومات التهديدات عبر مجتمعات المشاركة في قطاعي الطيران والنقل وتحويل التنبيهات إلى إجراءات رصد
- تصميم حالات استخدام للكشف في مركز العمليات الأمنية ومعايير فرز التنبيهات لتقنيات المطارات والتحكم المروري
- قيادة الاستجابة للحوادث بما يراعي التقاطع بين السلامة والأمن، بما في ذلك التحول إلى التشغيل اليدوي وقرارات تقييد العمليات
- إعداد نموذج تهديدات قطاعي ودليل استجابة للحوادث يغطيان الموردين وتسلسل استعادة الخدمات واختبار التمارين

الفئة المستهدفة:

- محللو مراكز العمليات الأمنية ومعالجو الحوادث الذين يراقبون شبكات المطارات أو شركات الطيران أو هيئات النقل
- مهندسو تقنية المعلومات والتقنيات التشغيلية المسؤولون عن أنظمة مناولة الأمتعة وساحات الطيران والإشارات والمعدات على جوانب الطرق
- كوادر مراكز التحكم التشغيلي في المطارات وشركات الطيران الذين ينسقون استمرارية الخدمة أثناء الاضطرابات
- مشغلو مراكز إدارة المرور ومهندسو أنظمة النقل الذكية الذين يديرون الإشارات ولوحات الرسائل والتحصيل الإلكتروني للرسوم
- مختصو أمن المعلومات لدى مقدمي خدمات الملاحة الجوية الذين يحمون تبادل البيانات مع المطارات وشركات الطيران

محاور الدورة:

اليوم 1: سطح الهجوم في الطيران والطرق وخصوم القطاع

- خريطة أنظمة تشغيل المطار: قاعدة البيانات التشغيلية AODB وشاشات معلومات الرحلات FIDS ومناولة الأمتعة وواجهات إنارة ساحة الطيران
- تعرض معالجة الركاب: منصات تسجيل الوصول المشتركة والتسليم الذاتي للأمتعة وبوابات الصعود والبوابات الإلكترونية الحيوية
- تقنية معلومات شركات الطيران والروابط المتصلة بإدارة الحركة الجوية: الحجوزات وتطبيقات الطواقم وتخطيط الرحلات وتغذيات بيانات المراقبة
- تعرض مراكز التحكم المروري ووحدات جوانب الطرق ووحدات التحكم في الإشارات ورسائل المركبات المتصلة
- مراجعة خصوم القطاع وحوادثه: فدية المطارات والتشويش على إشارات الملاحة وتشويه اللوحات وتعطل بوابات الرسوم

اليوم 2: أطر القطاع ونمذجة التهديدات وتبادل المعلومات

- أحكام الأمن السيبراني في ICAO Annex 17 الملحق 17 لمنظمة الطيران المدني الدولي ومبدأ التقاطع بين الأمن السيبراني والسلامة
- وظائف NIST Cybersecurity Framework إطار الأمن السيبراني مطبقة على ملاك منشآت النقل ومشغليها
- أساليب MITRE ATT&CK for ICS قاعدة معرفة أساليب الخصوم في أنظمة التحكم الصناعي ومطابقتها مع وحدات تحكم الأمتعة وساحات الطيران وجوانب الطرق
- Aviation ISAC مركز تبادل وتحليل المعلومات للطيران ومجتمعات المشاركة في النقل: العضوية ومعالجة التنبيهات والإبلاغ المتبادل
- ورقة عمل نمذجة التهديدات لكل نمط نقل: الأصول ونقاط الدخول وأهداف الخصوم والعواقب التشغيلية

اليوم 3: رصد مركز العمليات الأمنية لأنظمة النقل وحالات استخدام الكشف

- مصادر بيانات الرصد: سجلات تدقيق AODB وسجلات المنصات المشتركة وبوابات واجهات المراقبة الجوية وأحداث وحدات التحكم في الإشارات
- الرصد السلبي لحركة الشبكات في أنظمة مناولة الأمتعة وشبكات الإشارات المرورية
- دليل حالات استخدام الكشف: جلسات الموردين غير المصرح بها والعبث بتغذية بيانات الرحلات وتغيير خطط الإشارات
- فرز التنبيهات في سياقها التشغيلي: معايير التصعيد إلى مدير المناوبة وبرج المراقبة ومشغل المرور
- دليل تشغيل مركز العمليات الأمنية لربط أعطال الخدمات الموجهة للركاب بالأحداث الأمنية

اليوم 4: الاستجابة للحوادث وتعرض الموردين واستعادة خدمات النقل

- دليل الاستجابة لحادث سيبراني في مطار: فدية منصات تسجيل الوصول والمعالجة اليدوية البديلة
- دليل مركز إدارة المرور: الاستيلاء على لوحات الرسائل المتغيرة والتلاعب بتوقيت الإشارات
- قواعد القرار بين السلامة والأمن: متى يستدعي الحدث السيبراني تقييد العمليات أو إيقاف الإقلاع
- مخاطر وصول الأطراف الثالثة: شركات الخدمات الأرضية ومكاملو أنظمة الأمتعة ومشغلو الرسوم ومزودو الحوسبة السحابية
- تسلسل استعادة الخدمات الحرجة للرحلات والركاب والطرق

اليوم 5: تمرين سيبراني متعدد الجهات وإعداد نموذج التهديدات ودليل الاستجابة

- موجز الحالة: مطار محوري ومركز إدارة مرور حضري مجاور يتعرضان لهجوم منسق
- محاكاة بمدخلات زمنية: العمليات الأمنية ومركز عمليات المطار ومشغلو المرور
- بناء نموذج التهديدات القطاعي للمطار أو مركز إدارة المرور في الحالة
- صياغة دليل الاستجابة للحوادث: الأدوار ونقاط القرار والاتصالات ومعايير الاستعادة
- مراجعة ما بعد التمرين والدفاع عن الدليل أمام مجلس أزمات تجريبي

المهارات التي ستكتسبها:

- رسم سطح الهجوم في قطاع النقل
- نمذجة التهديدات القطاعية
- تبادل معلومات تهديدات الطيران
- هندسة الكشف في التقنيات التشغيلية للنقل
- فرز التنبيهات وفق السياق التشغيلي
- اتخاذ القرار عند تقاطع الأمن السيبراني والسلامة
- ضبط وصول موردي النقل
- تخطيط استعادة الخدمات الحرجة

لماذا تحضر هذه الدورة:

- العودة بنموذج تهديدات قطاعي ودليل استجابة للحوادث لمطار أو مركز إدارة مرور، جرى اختبارهما في تمرين محدد بزمن
- تزويد مديري المناوبة ومشغلي المرور بمحفزات واضحة للتحول إلى التشغيل اليدوي عند اختراق الأنظمة
- تحويل تنبيهات مجتمعات المشاركة إلى قواعد كشف يشغلها مركز العمليات الأمنية على بيانات المطارات وجوانب الطرق
- مقارنة ممارسات الاستجابة مع زملاء من المطارات وشركات الطيران ومقدمي خدمات الملاحة الجوية وهيئات الطرق والنقل العام

الخاتمة:

لا تستمر حركة المطارات وشبكات الطرق إلا حين تدرك فرق الأمن ما يعنيه كل نظام مخترق للرحلات والركاب والمرور. تنتقل الدورة من سطح الهجوم في الطيران والطرق وخصوم القطاع، إلى أحكام ICAO Annex 17 for ICSg NIST Cybersecurity Frameworkg ومجتمعات المشاركة، ثم إلى بيانات الرصد وحالات استخدام الكشف والفرز المرتبط بالعمليات، وصولا إلى أدلة الاستجابة وقرارات السلامة والأمن ووصول الموردين واستعادة الخدمات. ويخرج المشاركون من تمرين اليوم الأخير بنموذج تهديدات قطاعي ودليل استجابة للحوادث جاهز للاعتماد الداخلي.