تحليل بيانات الأمنية في القطاع العام

سوريا - دمشق

01 – 05/ 11 / 2026

مقدمة:

في ظل التحديات المتزايدة والمتسارعة، أصبح تحليل البيانات الأمنية أداة استراتيجية لا غنى عنها لأي مؤسسة في القطاع العام تسعى للنمو وتحقيق النجاح المستدام. يهدف هذا البرنامج إلى تمكين الكوادر الأمنية والإدارية من مهارات استخلاص الأنماط والعلاقات الحيوية من البيانات، سواء كانت كمية أو نوعية، وتحويلها إلى معلومات استخباراتية تدعم اتخاذ القرار. من خلال دمج التقنيات الإحصائية المتقدمة والبرمجيات المتخصصة، يوفر البرنامج منهجية متكاملة لجمع وتدقيق ونمذجة البيانات الأمنية، مما يعزز القدرة الاستباقية للمؤسسات الحكومية في مواجهة المخاطر وتحقيق التميز الأمني الرقمي.

أهداف الدورة:

- إكساب المشاركين مهارة تحديد الأنماط والعلاقات والمعلومات الأساسية من البيانات الأمنية (الكمية والنوعية).
- التمكن من استخدام التقنيات الإحصائية وأدوات التحليل والبرمجيات المتخصصة في القطاع العام.
- فهم الأهمية الاستراتيجية لتحليل البيانات في تحقيق النمو والنجاح المستدام للمؤسسات الأمنية.
- إتقان مراحل التعامل مع البيانات بدءاً من الجمع والتنظيف وصولاً إلى التنظيم والنمذجة.
- القدرة على بناء نماذج تنبؤية واستخدام أشجار القرار في تحليل السيناريوهات الأمنية.

محتويات الورشة:

اليوم الأول:

مقدمة في تحليل البيانات الأمنية

- تعريف تحليل البيانات الأمنية وأهميتها الاستراتيجية.
- مقدمة إلى أدوات تحليل البيانات الأمنية وأنواع البيانات.
- جمع البيانات الأمنية، تنظيفها، وتنظيمها.

اليوم الثاني:

استكشاف البيانات الأمنية وتصورها

- التحليل الوصفي والتصور البياني للبيانات الأمنية.
- التحليل التكراري والتحليل المتعدد المتغيرات.
- الكشف عن القيم الشاذة وتقنيات أخذ العينات.

اليوم الثالث:

التحليل الإحصائي واختبار الفرضيات الأمنية

- المفاهيم الأساسية في الإحصاءات الأمنية وتوزيع البيانات.
- اختبار الفرضيات وتحليل التباين.(ANOVA)
- التحليل الارتباطي، الانحدار الخطي، والاختبارات غير المعلمية.

اليوم الرابع:

النمذجة والتحليل التنبؤي

- مقدمة إلى النماذج التنبؤية وكيفية بنائها.
- التحليل التنبؤي باستخدام الانحدار وأشجار القرار.
- النماذج العشوائية والاختبارات الإحصائية المتقدمة.

اليوم الخامس:

التطبيقات الإلكترونية والمختبر العملي

- تطبيقات إلكترونية متخصصة في تحليل البيانات الأمنية.
- تمارين وأمثلة بيانات عملية مكثفة على الحاسب الآلي.

المخرجات الرئيسية للدورة:

- القدرة على تحويل البيانات الأمنية الخام إلى تقارير تحليلية تدعم صناعة القرار.
- إتقان مهارات الكشف عن الأنماط الإجرامية أو المخاطر الأمنية باستخدام التحليل الإحصائي.
- التمكن من بناء نماذج تنبؤية دقيقة تساعد في استباق التحديات الأمنية المستقبلية.
- امتلاك الكفاءة التقنية في استخدام البرمجيات الحديثة لتنظيف ومعالجة البيانات الأمنية.
- القدرة على عرض البيانات الأمنية بصرياً (Data Visualization) لتسهيل قراءتها من قبل القيادات.

الفئة المستهدفة:

- المحللون الأمنيون والباحثون في المؤسسات الشرطية والجهات السيادية.
- الكوادر الإدارية والتقنية العاملة في قطاعات تحليل البيانات ودعم القرار بالقطاع العام.
- مسؤولو التخطيط الاستراتيجي وإدارة المخاطر في الهيئات الحكومية.
- العاملون في وحدات مكافحة الجرائم الإلكترونية وتحليل المعلومات الاستخباراتية.

أساليب التدريب:

يتم استخدام بعض من الأساليب التالية أو الكل حسب المتطلبات لكل تخصص :

- دراسة الحالة المعقدة (Complex Case Studies)
- المحاكاة والألعاب الاستراتيجية (Simulation and War Gaming)
- ورش العمل القائمة على التفكير التصميمي (Design Thinking Workshops)
- حلقات النقاش مع خبير من القطاعين العام أوالخاص.(Expert Panels)
- المختبرات التقنية التفاعلية (Interactive Technology Labs)
- التعلم من الأقران عبر الجهات الحكومية (Inter-Agency Peer Learning)
- نهج التعلم المدمج والمستمر (Blended & Continuous Learning Approach)