



تحليل البيانات الأمنية



سوريا - دمشق

2026 / 11 / 26 – 22



مقدمة:

في ظل التسارع الرقمي، أصبح تحليل البيانات الأمنية أداة استراتيجية لا غنى عنها لأي مؤسسة تسعى للنمو وتحقيق النجاح المستدام. يهدف هذا البرنامج إلى إكساب المشاركين مهارات تحديد الأنماط والعلاقات والمعلومات الأساسية من البيانات الأمنية، سواء كانت أرقاماً كمية أو نوعية. من خلال استخدام التقنيات الإحصائية المتقدمة والبرمجيات المتخصصة، يسعى البرنامج إلى تمكين الكوادر من تحويل البيانات الخام إلى رؤى أمنية دقيقة تدعم اتخاذ القرار وتساهم في بناء منظومة أمنية استباقية وفعالة.

أهداف الدورة:

- إكساب المشاركين مهارة تحديد الأنماط والعلاقات والمعلومات الأساسية من البيانات الأمنية (الكمية والنوعية).
- استخدام التقنيات الإحصائية وأدوات التحليل والبرمجيات المتخصصة بمهارة واحترافية.
- فهم الأهمية الاستراتيجية لتحليل البيانات في تحقيق النمو والنجاح المستدام للمؤسسات.
- التمكن من مراحل التعامل مع البيانات بدءاً من الجمع والتنظيف وصولاً إلى التنظيم والنمذجة.
- إتقان مهارات التنبؤ والنمذجة الأمنية باستخدام الأدوات الإحصائية والرياضية الحديثة.



محتويات الورشة:

اليوم الأول:

مقدمة في تحليل البيانات الأمنية والتعامل الأولي

- تعريف تحليل البيانات الأمنية وأهميتها.
- مقدمة إلى أدوات تحليل البيانات الأمنية وأنواع البيانات الأمنية.
- جمع البيانات، تنظيف البيانات، وتنظيم البيانات.

اليوم الثاني:

استكشاف البيانات الأمنية والتصور البياني

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

اليوم الثالث:

تحليل البيانات الأمنية واختبار الفرضيات

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

اليوم الرابع:

النمذجة والتحليل التنبؤي

- مقدمة إلى النماذج التنبؤية وكيفية توظيفها.
- 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 شاملة على الحاسب الآلي.

المخرجات الرئيسية للدورة:

- القدرة على استخلاص الأنماط والعلاقات الأساسية من البيانات الأمنية المعقدة.
- إتقان استخدام البرمجيات والأدوات الإحصائية في تحليل البيانات النوعية والكمية.
- التمكن من بناء نماذج تنبؤية أمنية دقيقة تساعد في استباق التحديات.
- اكتساب مهارة تنظيف وتنظيم البيانات لضمان دقة النتائج التحليلية.
- الجاهزية لإعداد تقارير أمنية احترافية مدعومة بالتصورات البيانية والإحصائية.

الفئة المستهدفة:

- المحللون الأمنيون والباحثون في المؤسسات الشرطية والجهات السيادية.
- الكوادر العاملة في وحدات دعم القرار وتحليل المعلومات.
- مسؤولو إدارة المخاطر والتخطيط الاستراتيجي في القطاعات الأمنية والحكومية.
- المتخصصون في تقنية المعلومات والبيانات الضخمة المعنيون بالجانب الأمني.

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 أو الخاص. (Expert Panels)
- المختبرات التكنولوجية التفاعلية (Interactive Technology Labs)
- التعلم من الأقران عبر الجهات الحكومية (Inter-Agency Peer Learning)
- نهج التعلم المدمج والمستمر (Blended & Continuous Learning Approach)