الفصل السادس: قياس أمن المعلومات

6

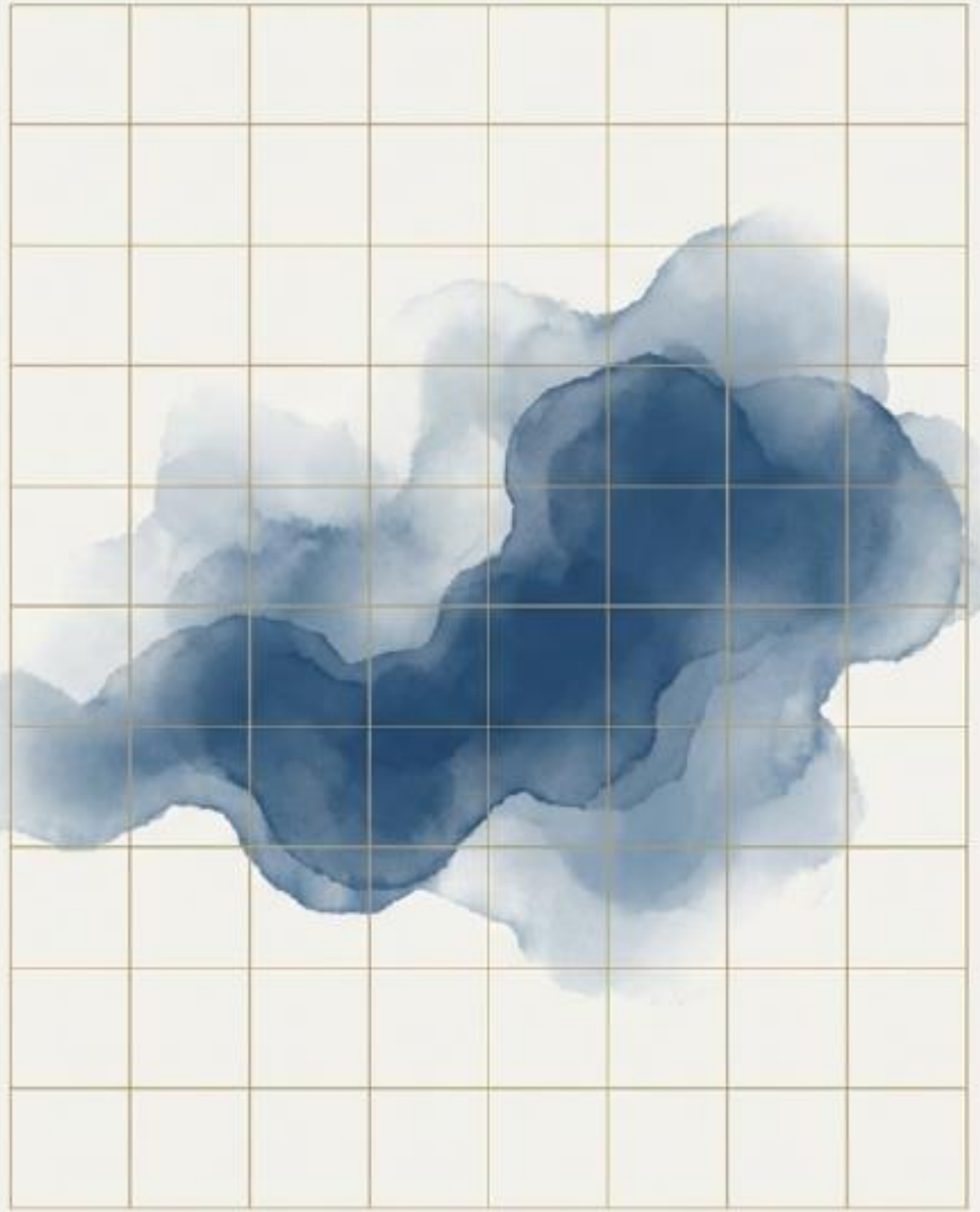
إعداد: ا. د. محمد الزعبي

معضلة القياس: «ليس كل ما هو مهم يمكن عده عده»

«ليس كل ما يمكن عده يكون مهماً، وليس كل ما هو مهم يمكن عده.»

- ألبرت أينشتاين

- إن قياس أمن المعلومات يمثل تحدياً فريداً. كيف نضع أرقاماً على مفاهيم معقدة مثل «مستوى الأمان»؟
- غالباً ما يبدو الأمر أشبه بمحاولة قياس أشياء مجردة مثل «الألم» أو «الحب».
- هذا العرض سيستكشف كيفية الانتقال من الغموض إلى الوضوح، ومن التقديرات إلى المقاييس الدقيقة.



لا يمكنك إدارة ما لا تستطيع قياسه

«إذا كنت لا تستطيع قياسه، فإن معرفتك ضعيفة وغير مرضية.»
– اللورد كلفن، 1893

المقاييس الموضوعية تحول أمن المعلومات من مركز **تكلفة غامض إلى وظيفة عمـل يمكن** إدارتها وتحسينها.

في غياب المقاييس، تعتمد الإدارة على ما يعرف بـ (FUD): الخوف وعدم اليقين والشك.

إنها الأداة الأساسية للإجابة على سؤال جوهري: «هل كان مستوى أمننا أفضل مما كان عليه في الماضي؟»

إطار للوضوح: مجالات قياس أمن المعلومات الأربعة

تشكل هذه المجالات الأربعة معاً رؤية شاملة لأداء أمن المعلومات، مما يضمن أن المقاييس ليست تقنية فحسب، بل ذات صلة استراتيجية بالعمل.

تفصيل المجالات: من الامتثال القانوني إلى الأثر المالي

الفاعلية التنظيمية

تستخدم المقاييس لإثبات قيمة برنامج أمن المعلومات لأصحاب المصلحة وتبرير وجوده.

الامتثال التنظيمي

يركز على تلبية الشروط والمتطلبات التي تضعها التشريعات. الهدف هو تجنب التهديدات القانونية والمالية والمالية للسمعة.

الإدارة المالية

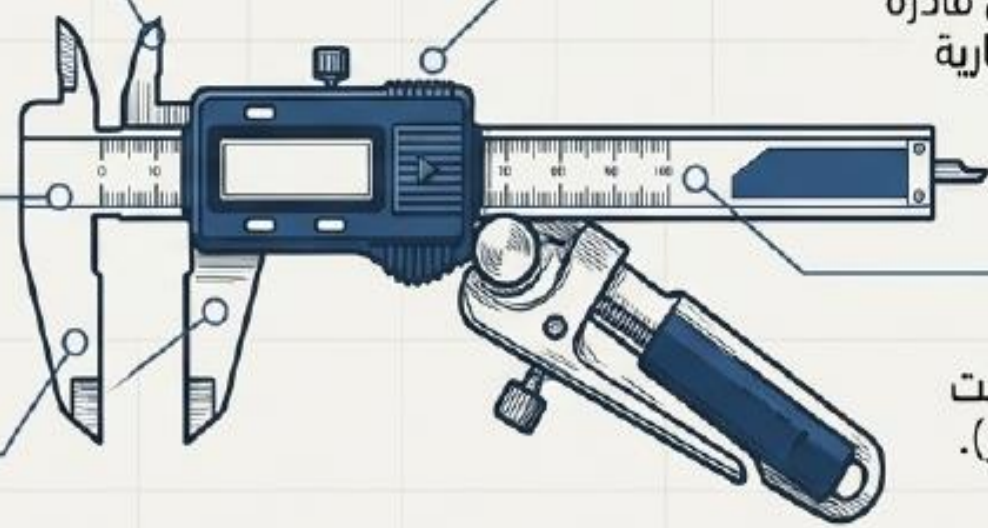
هناك حاجة للاستثمار بانتظام في مختلف جوانب أمن المعلومات. تقيس هذه الفئة أين وكيف يتم إنفاق الميزانية.

التشغيلية

الاهتمام الرئيسي لمدير دائرة أمن المعلومات ومسؤولي توفر هذه الفئة مقاييس قيمة حول الأداء اليومي للأنظمة. للأنظمة.

تشريح المقياس المفيد: خصائص تحويل البيانات إلى رؤى

المقياس المفيد هو «مؤشر رئيسي» (Leading Indicator) يوفر إنذاراً مبكراً، وليس مجرد تقرير عن أحداث وقعت بالفعل.



1. ترتكز على الأعمال

يجب أن تدعم المقاييس أهدافاً تجارية محددة.

2. قابلة للقياس الكمي

يجب أن تكون الأرقام موضوعية وصحيحة.

3. يمكن الحصول عليها

لا تتطلب عمليات جمع بيانات معقدة أو مستحيلة.

4. قابلة للتكرار

يجب أن تكون المقاييس قادرة على التكرار بطريقة معيارية للمقارنة عبر الزمن.

5. متجهة

يجب أن تُظهر بوضوح الاتجاهات مع مرور الوقت (تحسن، تدهور، استقرار).

تحدي إعداد التقارير: تجنب فخ «فيضان المعلومات»

معظم التقارير الأمنية لا **تلبي احتياجات الإدارة العليا.**

غالباً ما تكون تقارير خاصوخة (ad-hoc) ومفرطة في التفاصيل التقنية.

النتيجة هي «Information Over-Load» (فيضان المعلومات)، مما يؤدي إلى شل قدرة الإدارة على اتخاذ قرارات واضحة.

يجب أن تلتزم التقارير الفعالة بمبدأ **«الحاجة إلى المعرفة»** (Need to Know)، حيث تجيب بوضوح على أسئلة العمل المحددة.

نموذج التقرير الفعّال: ثلاثة محاور جوهرية لاتخاذ القرار

يجب أن تنتظم التقارير الفعالة حول ثلاثة مواضيع جوهرية لتلبية احتياجات الإدارة العليا:

الاستخبارات حول التهديدات لأمن المعلومات

ما هي المخاطر الجديدة والناشئة التي تواجهنا؟

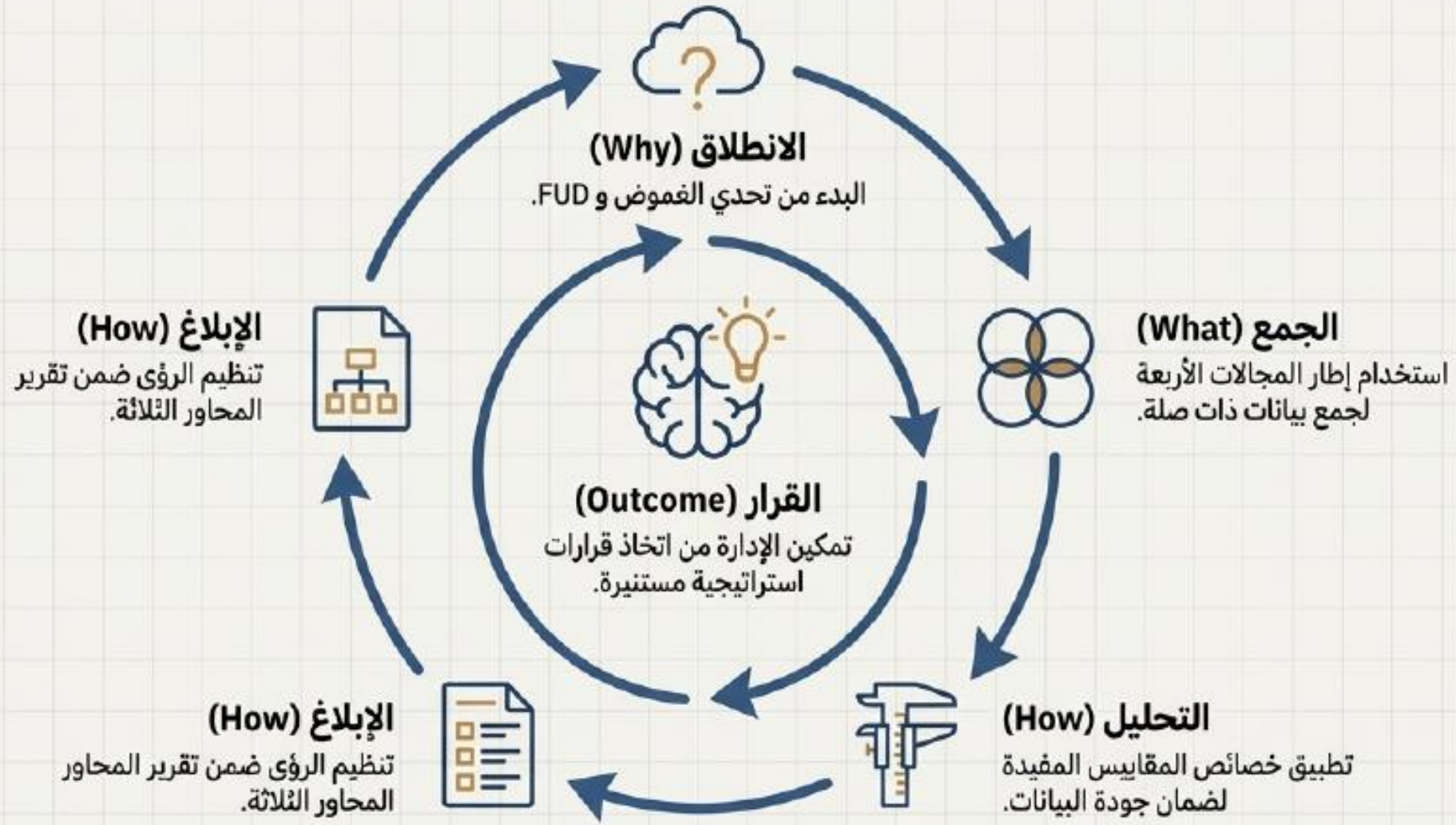
الاتجاهات الحالية

كيف يبدو أداؤنا الأمني الحالي بالمقارنة مع الفترات السابقة؟

التنبؤات (مؤشرات المخاطر الرئيسية)

إلى أين تتجه المخاطر الرئيسية وما الذي يجب أن نستعد له؟

من البيانات إلى القرار: دورة القياس المتكاملة



الهدف النهائي: الإشراف المستنير على أصول المعلومات

إن الهدف من القياس ليس إنشاء الرسوم البيانية، بل هو تمكين الإدارة من الإشراف الفعَّال على أصول المعلومات الحيوية للمؤسسة.

المقاييس الفعالة تحول أمن المعلومات من كونه مجرد تكلفة إلى عامل تمكين استراتيجي.

إنها الأداة التي تسمح لنا بالإجابة بثقة على السؤال الأساسي:
«هل كان مستوى أمننا في الشهر الماضي أفضل مما كان عليه في هذا الوقت من العام الماضي؟».