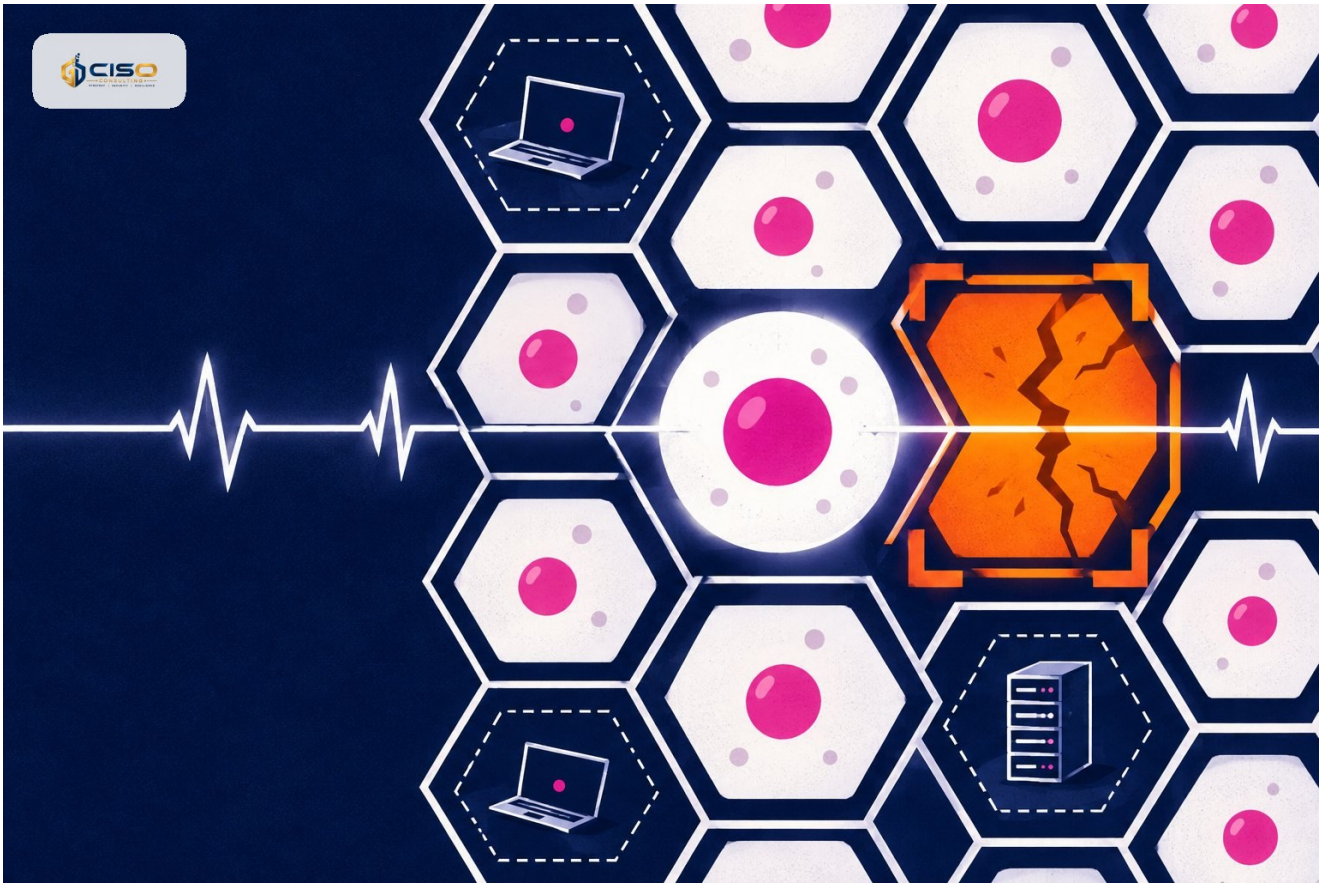
# نهج معهد للأورام تجاه التقنية الخفية: الاحتواء عبر التقسيم الدقيق للشبكة



يشرح معهد إيطالي للأورام كيف يتيح له التقسيم الدقيق للشبكة والثقة المعدومة عزل النظام المصاب وضبط التقنية الخفية في البحث العلمي واستمرار رعاية المرضى.

- يتيح التقسيم الدقيق عزل الجزء المصاب من الشبكة دون إيقاف المستشفى بأكمله.
- حظر التقنية الخفية في البحث كثيراً ما يُبعد الأجهزة عن رؤية تقنية المعلومات؛ لذا يُعتمد مبدأ الرؤية أولًا ثم الحوكمة.
- لا يُقطع التعاون مع الشركاء الأضعف أمنياً، بل يُضيَّق وصولهم وفق أقل الصلاحيات والمصادقة القوية والوصول المحدود زمنياً.
- يعمل التقسيم كضابط تعويضي للأجهزة الطبية المعتمدة التي يصعب تحديثها بحرية.
- تُفصل بيئات البحث عن البيئات السريرية مع إخفاء الهوية المستعار وضبط الوصول.

في حوار مع موقع Help Net Security، يوضح روكو سافيانو، مدير التحول الرقمي في المعهد الوطني للأورام (INT) في إيطاليا، كيف توازن مستشفى الأورام بين استمرارية العمل السريري والأمن السيبراني. وفكرته المحورية: اعزل المشكلة لا المستشفى.

## الاحتواء بدل الإيقاف

يطبّق المعهد مبدأ الثقة المعدومة بحيث يتواصل كل نظام مع الموارد التي يحتاجها فقط، فلا يمنح جهاز عمل مصاب المهاجم طريقاً إلى الأنظمة السريرية أو المختبرات أو الأجهزة الحرجة. وفي الحوادث السيبرانية يضيف إيقاف الشبكة الأوسع مشكلة فوق الهجوم نفسه، لذلك يفضّل المعهد **التقسيم الدقيق للشبكة** لاحتواء الاختراق مع استمرار الرعاية.

وتُصمَّم الاستمرارية ولا تُرتجل: تكرار الأنظمة، وتوافر عالٍ، وإجراءات للتعطل، ووسائل وصول طارئة. وإذا تعذر على الممرضة فتح خطة العلاج الكيميائي فلا يُعطى شيء اعتماداً على الذاكرة، بل تُستخدم مصادر بديلة مصرّح بها وتُجرى فحوص سريرية، ثم تُسوّى الأحداث في النظام لاحقاً.

## البحث والشركاء والأجهزة

يرى سافيانو أن حظر التقنية الخفية كثيراً ما يفشل لأنه يُخرج الأجهزة من نطاق رؤية تقنية المعلومات. لذا يوفّر المعهد بيئات بحثية آمنة وسهلة، ويفترض ظهور أنظمة غير متوقعة، فيضمن التقسيم ألا يصل نظام جديد أو هش تلقائياً إلى بقية المؤسسة.

أما الشركاء فالاتصال لا يعني الثقة؛ ويفضّل المعهد منصات معزولة ومصادقة قوية ووصولًا محدود المدة وبيانات بأسماء مستعارة وأقل الصلاحيات، ويمكنه تضييق نطاق الشريك الأضعف بدل إنهاء التعاون.

ويعدّ لائحة الأجهزة الطبية الأوروبية (MDR) الأكثر عبئاً إجرائياً فيما يخص الأجهزة المعتمدة، إذ يجب أن تراعي التحديثات قيود المصنّع، فيصبح التقسيم ضابطاً تعويضياً. ويرى أن توجيه NIS2 دفعهم إلى تفكير أعمق في المخاطر والمرونة وسلسلة التوريد والاستجابة للحوادث.

## ما يجب فعله الآن

1. حدّد الأنظمة السريرية والبحثية والإدارية التي تحتاج فعلًا إلى التواصل فيما بينها، وقيّد بقية المسارات.
2. ضع وجرّب إجراءات التعطل والوصول الطارئ للأنظمة السريرية الحرجة، بما يشمل تسوية السجلات لاحقاً.
3. عند تعذر تحديث الأجهزة الطبية سريعاً، طبّق التقسيم كضابط تعويضي موثّق.
4. امنح الأطراف الثالثة وصولًا محدود المدة بأقل الصلاحيات ومصادقة قوية، وأخفِ هوية البيانات البحثية بأسماء مستعارة حيثما أمكن.
5. استبدل الحظر الشامل لأدوات البحث غير المعتمدة ببديل آمن وسريع مع اكتشاف الأجهزة غير المُدارة.
6. واءم خطط التقسيم واحتواء الحوادث مع متطلبات الضوابط الأساسية للأمن السيبراني (NCA ECC) ونظام حماية البيانات الشخصية (PDPL).