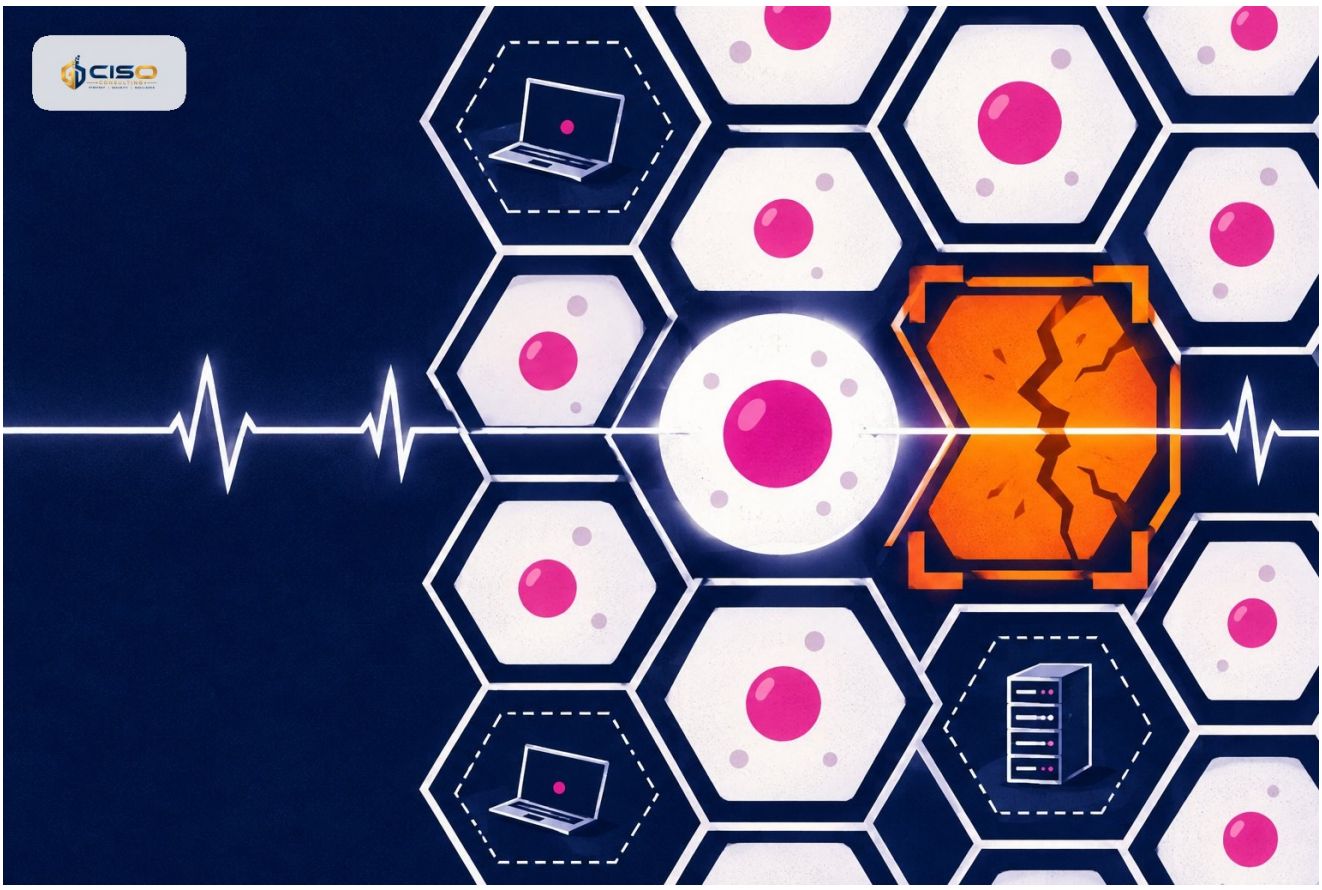
A cancer institute's approach to shadow IT: contain it with microsegmentation



An Italian cancer institute explains how microsegmentation and zero trust let it isolate a compromised system, govern shadow IT in research and keep patient care running during incidents.

- Microsegmentation lets the institute isolate a compromised part of the network without shutting down the whole hospital.
- Banning shadow IT in research often pushes devices out of IT's sight; the stated approach is to see first, then govern.
- Partners with weaker security are not cut off; their access is narrowed under least privilege, strong authentication and time limits.
- Segmentation acts as a compensatory control for certified medical devices that cannot be patched

freely.

- Research and clinical environments are kept separate, with pseudonymization and controlled access.

In an interview with Help Net Security, Rocco Saviano, Director of Digital Transformation at Istituto Nazionale Tumori (INT), describes how a cancer hospital balances operational continuity with cybersecurity. His central idea: isolate the problem, not the hospital.

Containment over shutdown

INT applies zero trust so that each system communicates only with the resources it needs. A compromised workstation should not give an attacker a path to clinical systems, laboratories or critical devices. In a cyber incident, shutting down the wider network would add a problem beyond the attack itself, so the institute prefers **microsegmentation** to contain the compromise while care continues.

Continuity is designed, not improvised: redundancy, high availability, downtime procedures and emergency access. If a nurse cannot open a chemotherapy plan, nothing is given from memory; authorised alternative sources and clinical checks are used, and events are reconciled afterwards.

Research, partners and devices

On shadow IT, Saviano says prohibition often fails because it moves devices out of IT's visibility. INT offers secure, simple research environments and assumes unforeseen systems may still appear. Segmentation means a new or vulnerable system does not automatically reach the rest of the organisation.

For partners, connection does not imply trust. INT favours segregated platforms, strong authentication, time-limited access, pseudonymised data and least privilege, and can shrink a weaker partner's perimeter instead of ending collaboration.

He calls the EU Medical Device Regulation procedurally burdensome where certified devices are concerned, since updates must respect manufacturer constraints. Segmentation then serves as a compensatory control. He credits NIS2 with pushing deeper thinking on risk, resilience, supply chain and incident response.

What to do now

1. Map which clinical, research and administrative systems genuinely need to communicate, and restrict all other paths between them.
2. Define and test downtime and emergency-access procedures for critical clinical systems, including reconciliation of records afterwards.
3. Where medical devices cannot be patched promptly, apply segmentation as a documented compensatory control.

4. Grant third parties time-limited, least-privilege access with strong authentication, and pseudonymise research data where possible.
5. Replace blanket bans on unapproved research tools with a fast, secure alternative and discovery of unmanaged devices.
6. Align segmentation and incident containment plans with NCA ECC and PDPL obligations.