



OPERATIONAL TECHNOLOGY

A Radar System Does Not Get a Software Update at 2am. That Is the Problem.

Somewhere on a production floor right now, there is a controller running firmware from a decade ago, connected to a network everyone assumed was isolated. It has been running fine for years. That is exactly why nobody has looked at it closely.



The Real Exposure.

In 2017, malware known as Triton was found on the safety instrumented systems of a petrochemical plant in Saudi Arabia, the systems whose entire job is to shut a process down safely when something goes wrong. It was the first known attack built specifically to disable the safety net itself, not just the process it protects. Defence manufacturing and aerospace maintenance run on the same category of safety-critical control systems.

01

Adversarial attacks on machine learning

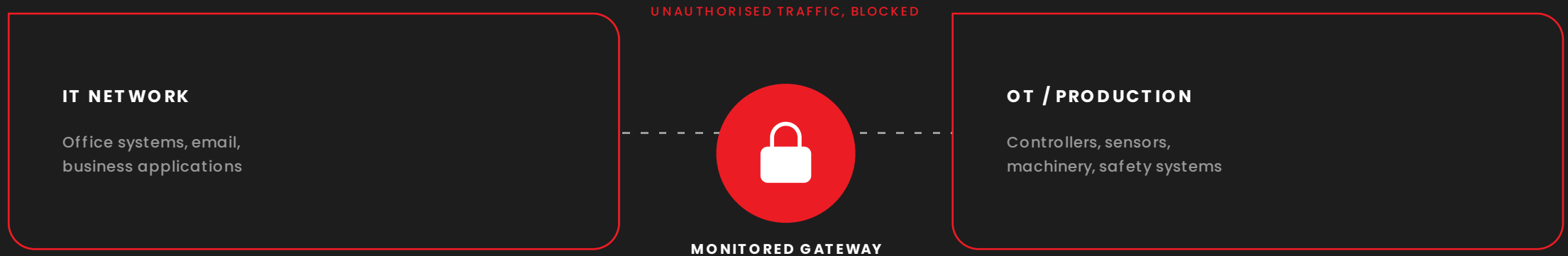
The systems that actually run radar, avionics maintenance lines, weapons manufacturing and shipyards were not built for a hostile network. As IT and OT increasingly connect to each other, that gap becomes the way in.

2010

In 2010, Stuxnet showed that an attack on physical equipment does not have to look like a typical cyberattack at all. It can look like a valve behaving strangely, or a machine running slightly out of tolerance.

02

The gap between IT and OT that most environments have not closed. —



Why It Matters at AAD

Aerospace and defence manufacturing runs on equipment that was never designed with a hostile network in mind, and much of it cannot be swapped out on a normal upgrade cycle. Treating OT security as an extension of IT security misses the point. We work on the floor, not just in the server room, because that is where the real exposure sits.

03

What did we do? ---

We assess and secure the systems that keep production, maintenance and logistics running, without stopping the line to do it.



OT and ICS/SCADA security assessments aligned with IEC 62443, run by people who understand that on a factory floor, safety comes before anything else.



IT/OT network segmentation design, so a compromise on the office network cannot reach the systems that actually matter.



Legacy system risk reviews for equipment that cannot simply be patched, replaced or taken offline for a scan.



Incident response planning built specifically for production environments, where downtime is measured in more than money.

A patch cycle built for laptops does not fit a machine that has been running since before the internet did. We work with the equipment you actually have, not the equipment a generic framework assumes you have.

DISystems – cybersecurity and GRC advisory across South Africa, the SADC region and internationally, in partnership with **Cyberantix™**

CONTACT US AT:
tsepang@disystems.co.za
 to setup a time for more details.

