What and Who is SensorFu?

Background:
SensorFu Beacon is a cornerstone Cyber SecOps innovation from the team that found the **Heartbleed** virus using their zero-day vulnerability test suite – *Defensics*. The SensorFu team is based in Oulu, Finland – home to CyberSec Tools development since the early 2000's

Why SensorFu:
Identify and remediate network vulnerabilities, leaks before they become attack-vectors into your organisation. To gain control of operations and information technology networks and systems, C&C bot/nets are most effective in being placed and silently present (living off the land). They do, however, require contact beyond the target network to be effective in their objective. That is usually done by exploiting leaks from the hosting network through firewalls, airgaps, enabled mostly by human misconfiguration, oversight or insider action.

How:
SensorFu is a new paradigm in vulnerability and penetration/leakage testing that works from ***the inside out*** to find data exfiltration and ingress/egress points, in real-time, across all layers of your network.
Multiple configuration options give your organisation full control over the desired level of trust, detection and alert capabilities. SensorFu is a trusted test agent operating in a closed system paradigm.

Critical Infrastructure Networks:
Governments, globally, have or are implementing cyber security compliance legislation for "Critical Infrastructure" which has broad application and consequences for owners, operators or custodians of that infrastructure.

- Energy (Distribution, Generation an Storage)
- Water (Supply and Treatment)
- Communications (Wireless and Wireline)
- Defence industry (Operations and Supply)
- Banking and finance
- Transport
- Manufacturing
- Data and the Cloud
- Education, research and innovation
- Food and grocery logistics
- Health
- Space

SensorFu Beacon is a cost effective tool to assure OT/IT networks are cyber-secured to their designed specifications and is easily, quickly, integrated to SOC tools and processes, delivering value within hours, days from turn-on

SensorFu in action

SensorFu is operational in a number of European and US utilities and enterprises. SensorFu has successfully undertaken NATO CyberSec exercises "Locked Shields' in 2019, 2021, 2022 (Winner) and 2023

https://ccdcoe.org/exercises/locked-shields/

https://ccdcoe.org/news/2022/finland-wins-cyber-defence-exercise-locked-shields-2022/

https://www.youtube.com/watch?v=Dwvc5y1eHdg

https://www.youtube.com/watch?v=daDNcE9Ha6k

https://youtu.be/jYEmcGvEuzQ

For more information on ***SensorFu*** or registering for a trial, email contact@connectpacific.com (Australian Partner) or call +61 413 208 744

connectpacific

Cyber Security, Perimeter Control Validation of OT/IT networks

Network segmentation enables an organisation to reduce cybersecurity risk and acts as a vital first step towards defining and implementing a ***zero-trust security*** policy.

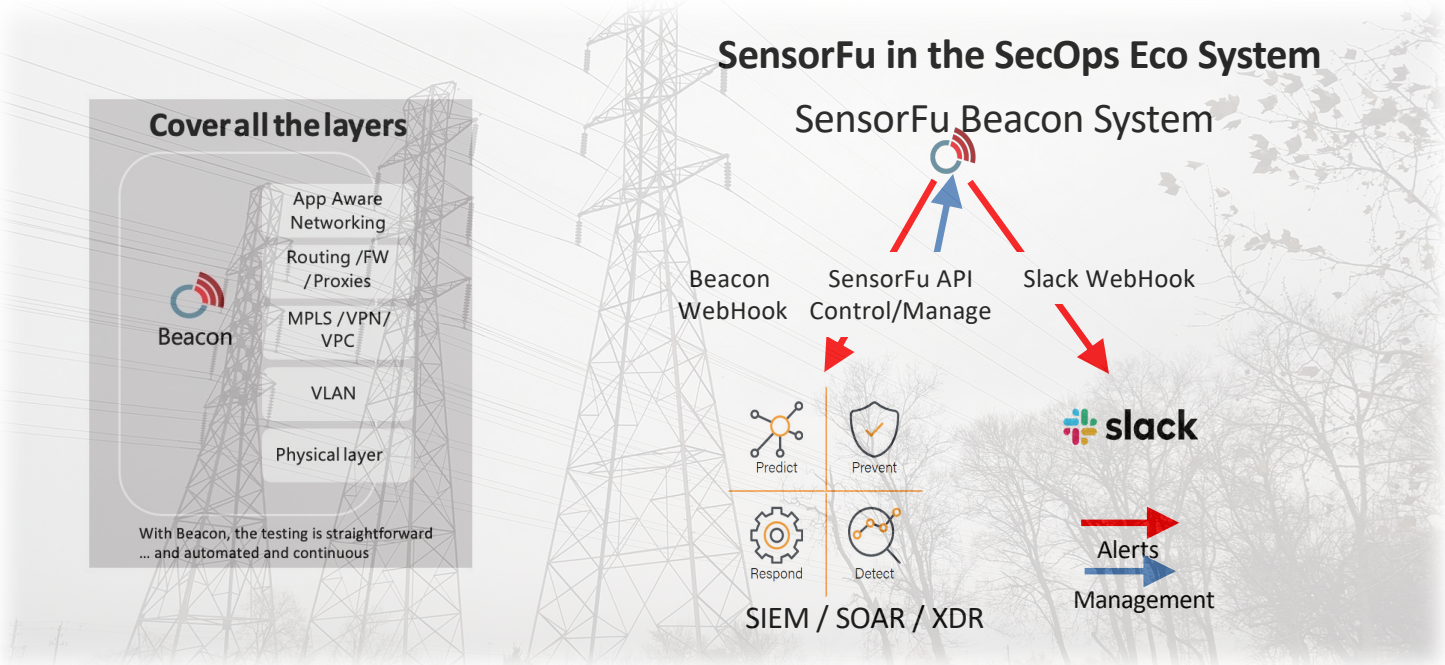
- You rely on it for your business protection.
- You may call it access control lists, isolation, segregation, segmentation, partitioning or sandboxing.
- Critical Infrastructure protection, privacy, payment safety, legislation or your peace of mind may require it.

But, how do you know it's working properly?

SensorFu Beacon operates as a closed system, where ***Beacons*** are placed within a segregated/segmented network either as hosted software on a workstation, or router/switch or as a stand-alone appliance connected to a switch or router behind the firewall or air-gap. A Beacon will **continuously** attempt to escape that network to the SensorFu ***Home***, a trusted system within the organisation, but outside the segmented network(s). An escape event can then be assessed by a SIEM/SOAR/XDR and Analyst and the "leakage" remediated as needed.

Validate that your OT/IT **network segmentation** and cyber-hygiene is effective by continuously testing for:

- *TCP and UDP leaks over IPv4 and IPv6 across all ports*
- *DNS Tunnelling using name server infrastructure to covertly sneak out*
- *Broadcasting triggering improper routing decisions in multi-homed devices*
- *Spoofing of IP packets to bypass firewalls and routers*
- *Strength of ICMP firewall configuration*
- *Strength of IP payload protocol management*



connectpacific