The Australian Government Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill)

Background:
The Australian Federal Government is introducing legislation that makes critical infrastructure stakeholders directly accountable for the cyber-risks throughout their operations.

What is SensorFu:
Security Control Validation - Highly cost effective, secure, focused, automated, continuous network vulnerability and penetration testing

Why:
Identify and remediate network vulnerabilities, leaks before they become attack-vectors into your organisation.

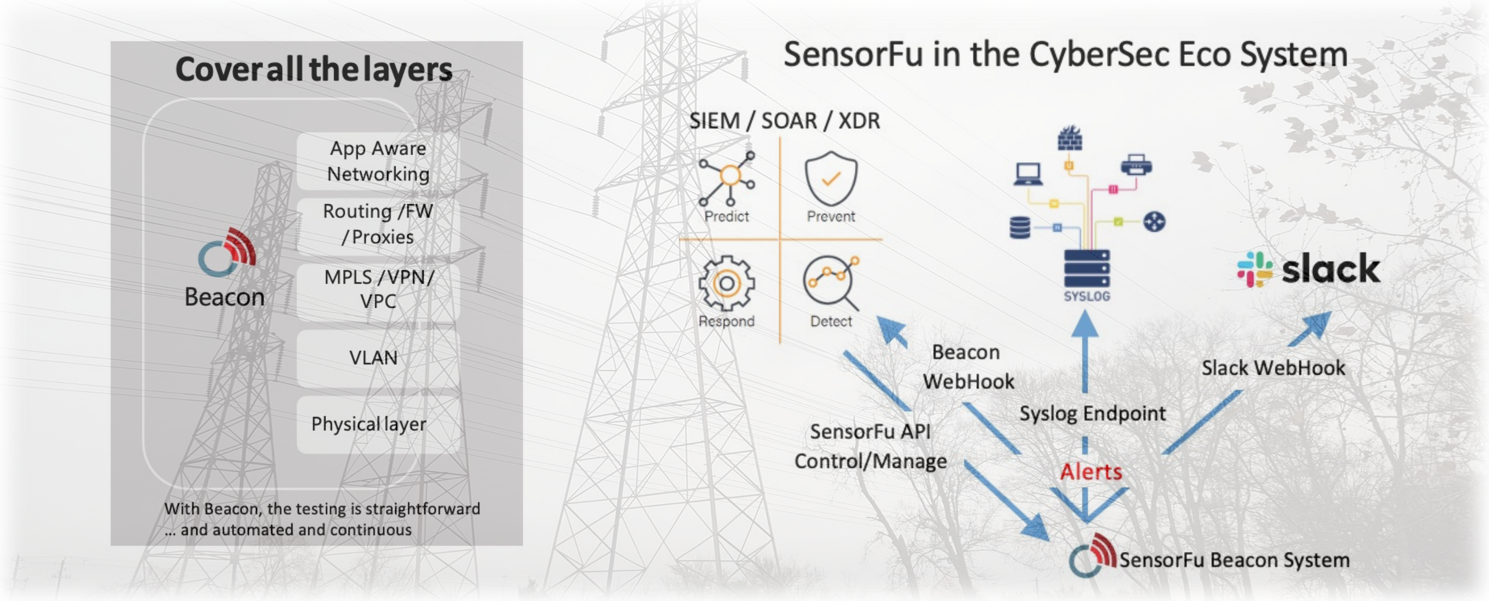
How:
SensorFu is a new paradigm in vulnerability and penetration testing that works from ***the inside out*** to find data exfiltration and ingress/egress points, in real-time, across all layers of your network. Multiple configuration options give your organisation full control over the desired level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

Network segmentation enables an organisation to reduce cybersecurity risk and acts as a vital first step towards defining 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 sanity may require it.
? ***But - do you know it is working correctly*** ?

Validate that your OT/IT network segmentation and cyber-hygiene is effective by efficiently 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



For more information on ***SensorFu*** or registering for a trial, email contact@connectpacific.com or call 0413 208 744

What and Who is SensorFu?

Background:
SensorFu is the latest in-operations innovation from the team that found the **Heartbleed** virus using the leading zero-day vulnerability test suite – Defensics. The SensorFu team is based in Oulu, Finland – home to CyberSec Tools innovation since the early 2000's

What is SensorFu:
Highly cost effective, secure, focused, automated, continuous network vulnerability and penetration/escape testing platform.
SensorFu is comprised of 2 elements – a network **Beacon** (software or appliance) and a **Home** which processes the escape information in real-time and makes it available via API's to existing SecOps tools

Why:
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 botnets are most effective in being placed and silently present. 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 and oversight.

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.

For people who like **analogies**, consider a boat that seems to allow water into the hull. There are 2 ways to ascertain the leak(s). The obvious (and usual) way is to inspect the hull from the outside – visual, x-rays, ultrasound. The other, not so obvious, is to lift the hull from the water, fill the hull to the water line and observe where the leak(s) come from. The water is trusted (you put it there to do a job) and because you know how it is leaking, the holes can be fixed appropriately to stop the leaks.

Critical Infrastructure Networks:
The Australian Government Security Legislation Amendment (Critical Infrastructure) Bill 2020, has broad application, with Critical Infrastructure being defined as networks and system supporting

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

SensorFu in action
SensorFu is operational in a number of Northern Europe utilities and enterprises. SensorFu has successfully undertaken NATO Cybersec exercise "Locked Shields 2019", as part of the Blue Team.
https://ccdcoe.org/exercises/locked-shields/
https://www.youtube.com/watch?v=Dwvc5y1eHdg