



Evolving cyber challenge: risks and implications

Peter Broadhurst, SVP Safety and Security



Maritime Cyber Resilience

Maxwell Cooter
February 13, 2015

Royal Navy under threat from cyber-attacks

Share this article: [f](#) [t](#) [in](#) [g+](#) [p](#) [e](#) [m](#)

The Royal Navy is under an increasing danger of cyber-attack and the government should ramp up training to deal with the threat.

That's according to a report from researchers at the University of Lancaster who found that maritime systems were especially susceptible to computer attacks and that ageing systems and a lack of training were particular barriers.


Security consultant Brian Honan said that all navies, indeed all shipping companies, were vulnerable to these threats. "What the report highlights is that many ships use Windows XP or Windows Server 2003 – one of which Microsoft



Royal Navy under threat from cyber-attacks

Students Take Control of \$80 Million Superyacht Using Fake GPS Signals

David Pecking
Texas A&M University



They—Texas did something smart! By sending fake GPS data to a superyacht's navigation system, University of Texas students were able to override the actual GPS signals and send an \$80 million ship veering off course without setting any dangerous whatsoever.

Plenty of phish in the sea

Published on June 15, 2015 by David Rider · No Comments

Shipping industry again warned of cyber threat.

Plenty of phish in the sea

Advancement in broadband technologies and the move towards 'Big Data' will leave the maritime industry vulnerable to cyber-crime unless it develops a better awareness of ICT security and adopts security best practice, warns ESC Global Security's head of cyber security division.



GIZMODO

Ships Have Black Boxes—And Apparently, They're a Cinch to Hack

Ben Luhn
Panda Security



Voice, navigation, and radar data aboard ships are all at risk, according to an expert who claims that some devices that contain sensitive ship information just aren't secure enough. This could be good news for pirates and spies, and bad news for the good guys.

Cyber Attack Targets Tankers

By MarEx 2015-05-20 04:40:23

IT company Panda Security has released Operation Oil Tanker: The Phantom Menace, a report that details a malicious and largely unknown targeted attack on oil tankers.

First discovered by Panda Security in January 2014, the ongoing attack on oil cargo began in August 2013 and is designed to steal information and credentials for defrauding oil brokers.

Despite having been compromised by this cyber attack, which Panda has dubbed "The Phantom Menace", none of the dozens of affected companies have been willing to report the invasion and risk global attention for vulnerabilities in their IT security networks.





43%

Crew sailed on a vessel that has been compromised by a cyber incident

90%

Crew had never received any cyber security training or guidelines

95%

Breaches are caused by human errors

The maritime industry is not yet fully prepared

Shipping must take measures to become cyber resilient

Potential risks

Loss of information

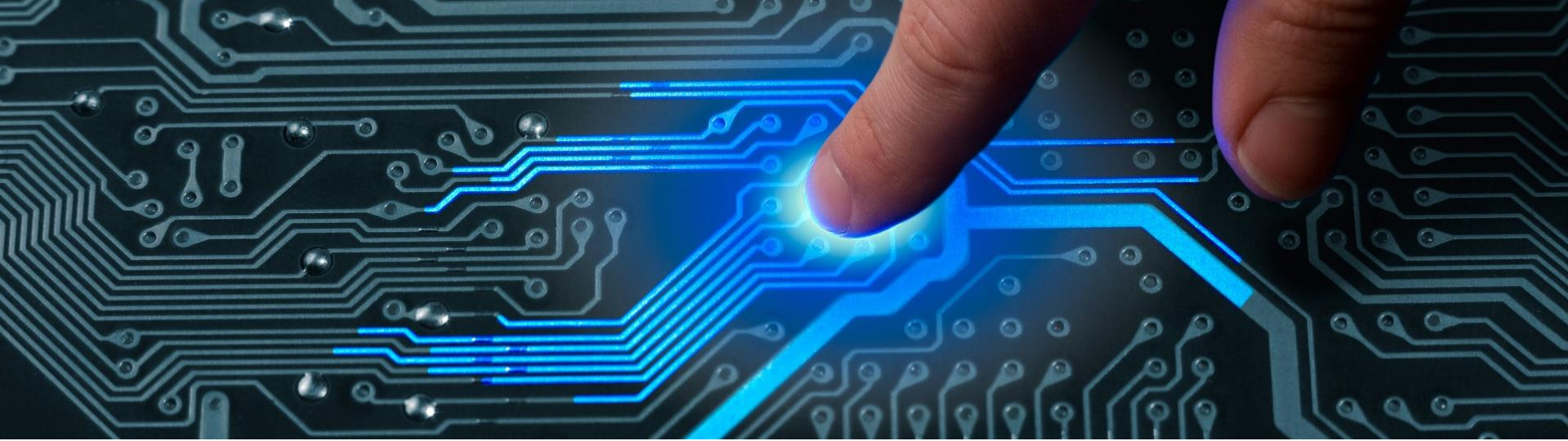
Interruption of operations

Loss of reputation

Privacy impact

No insurance cover

Financial impact



Inmarsat is
building a
portfolio of
security
services

**Awareness
and training**

**End point
and network
security**

**Consultancy
and
compliance**

Mitigation

Secure Core

Service benefits to shipowners

Addressing multiple threats



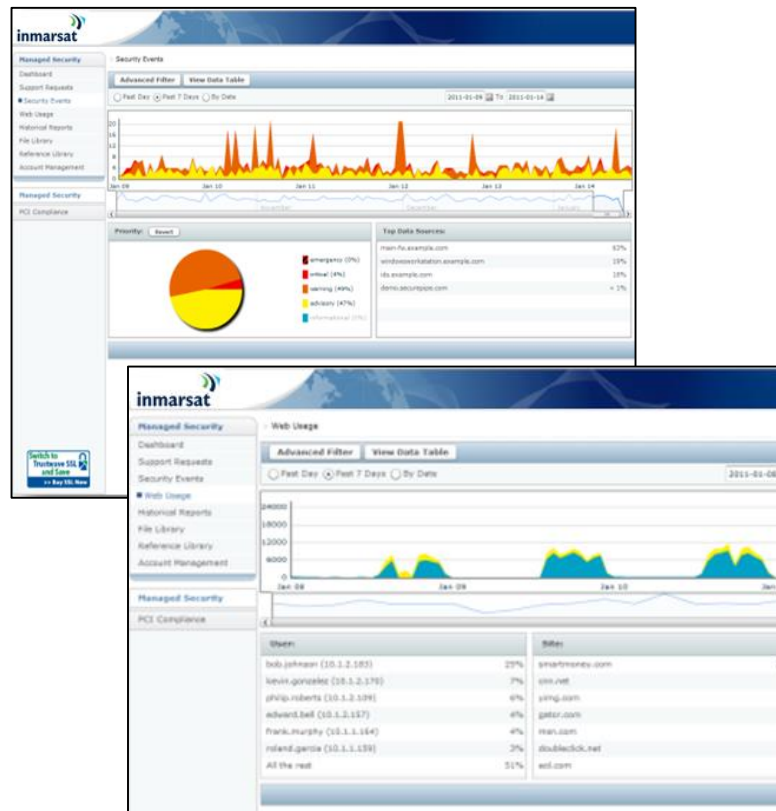


Inmarsat's UTM cyber service

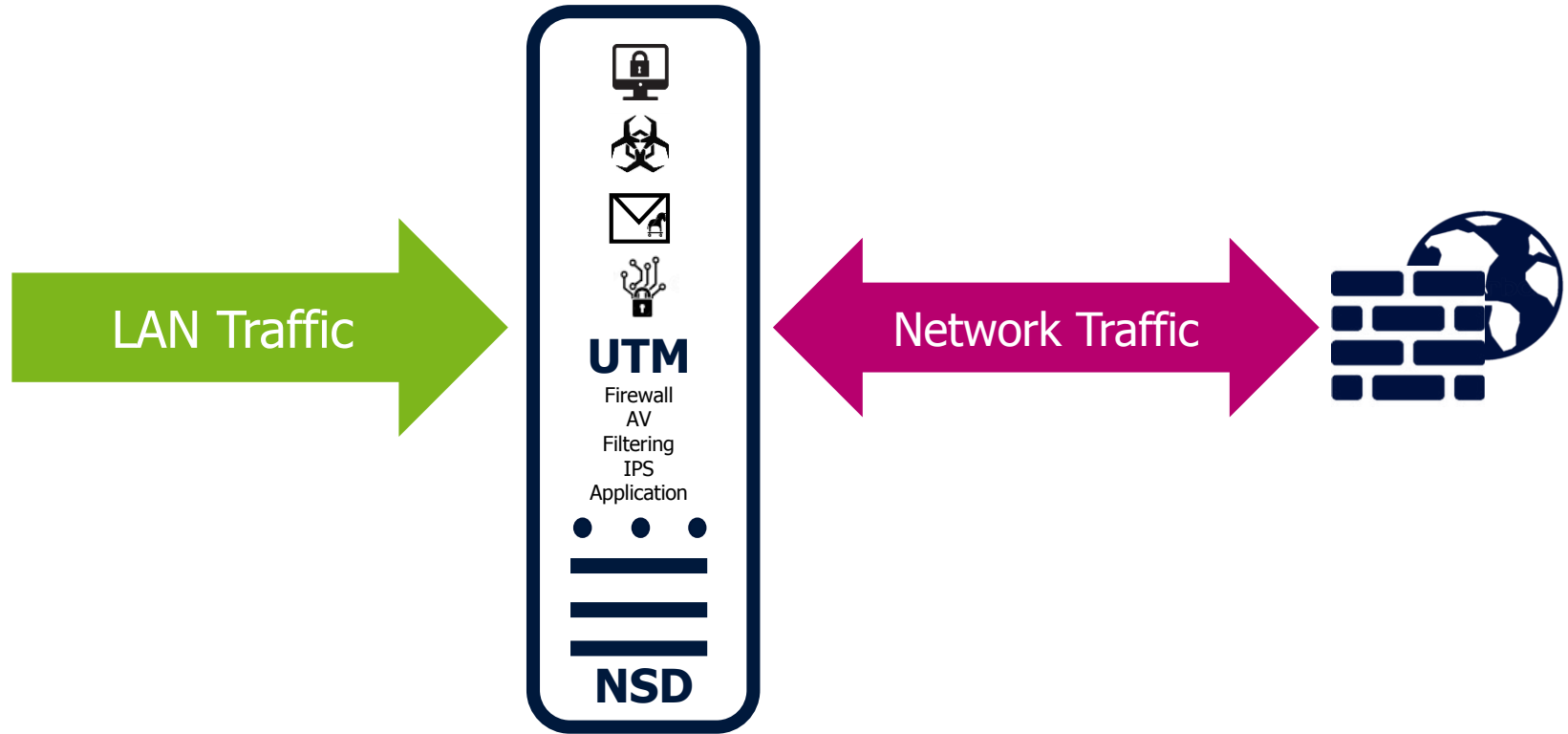
Managed UTM service

Addressing multiple threats

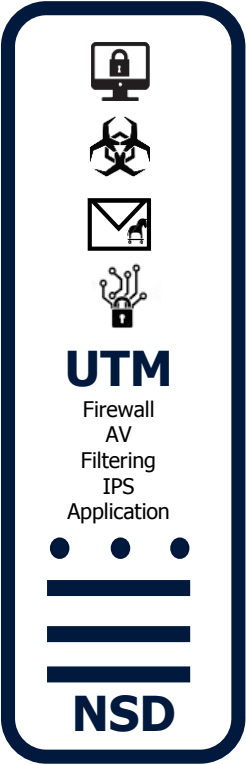
- Securing on-vessel IT network through a single appliance which is consolidated in the onboard controller, the NSD or sNSD
 - Stateful Inspection Firewall
 - Web content filtering
 - Application control
 - Intrusion Prevention Systems
 - Gateway anti-virus
- Managed and controlled from the Secure Operation Centre to ensure highest levels of protection



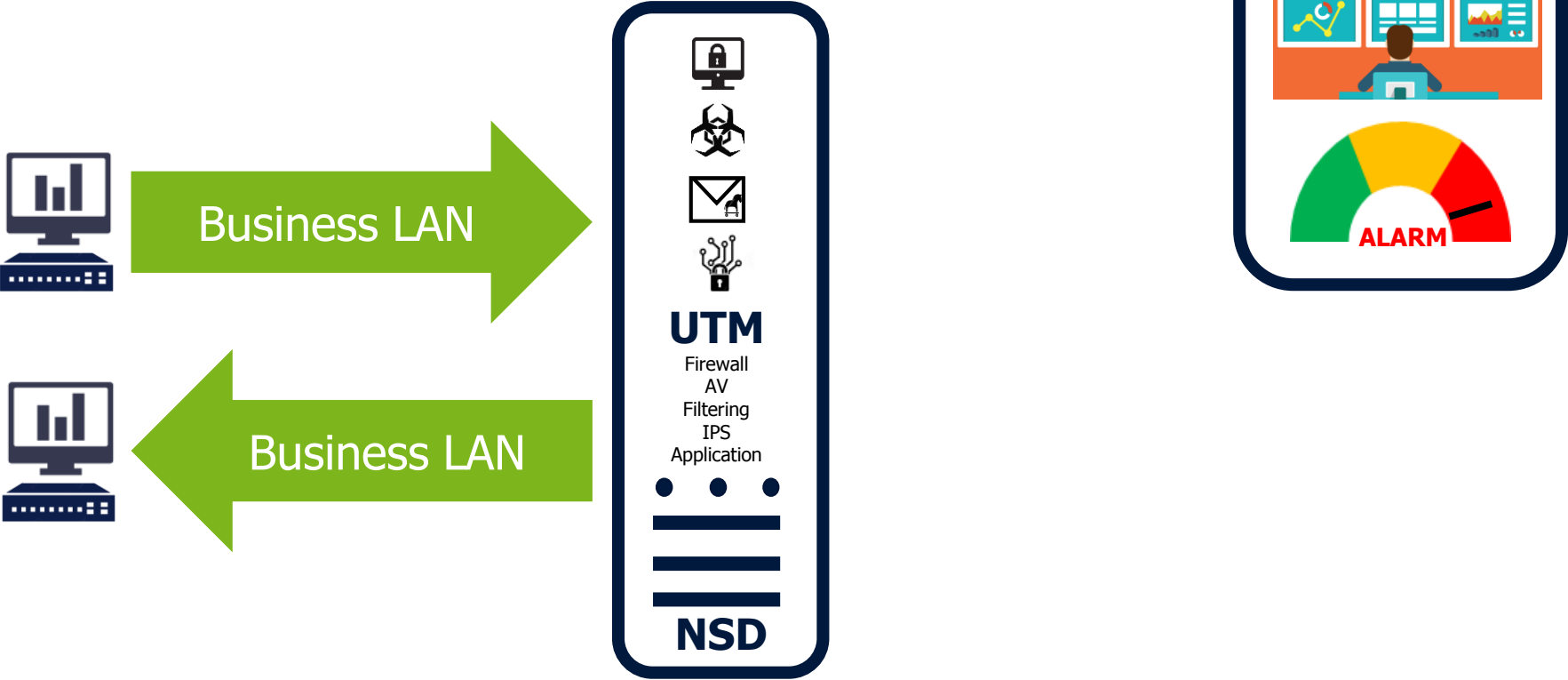
Inmarsat UTM for Fleet Xpress



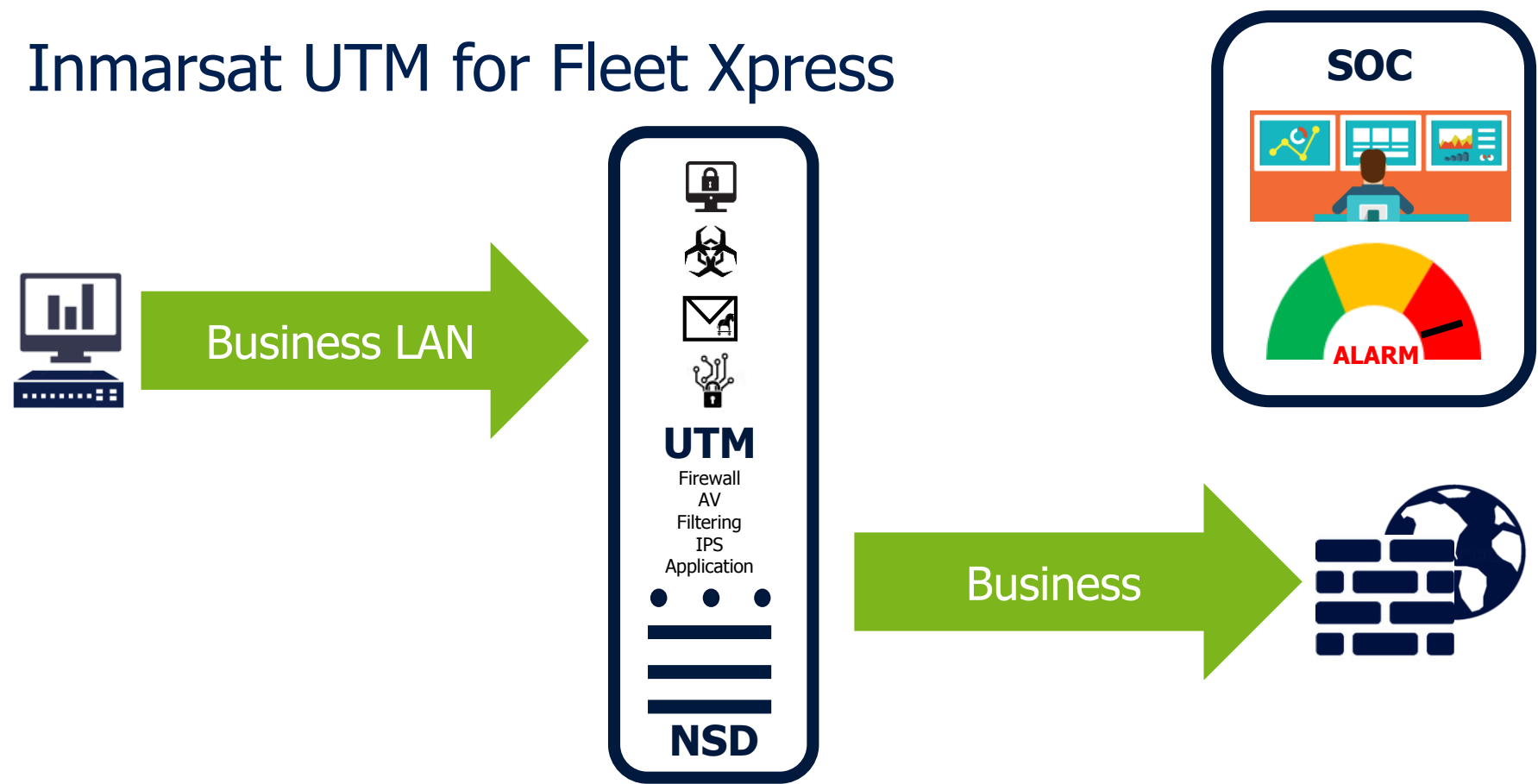
Inmarsat UTM for Fleet Xpress



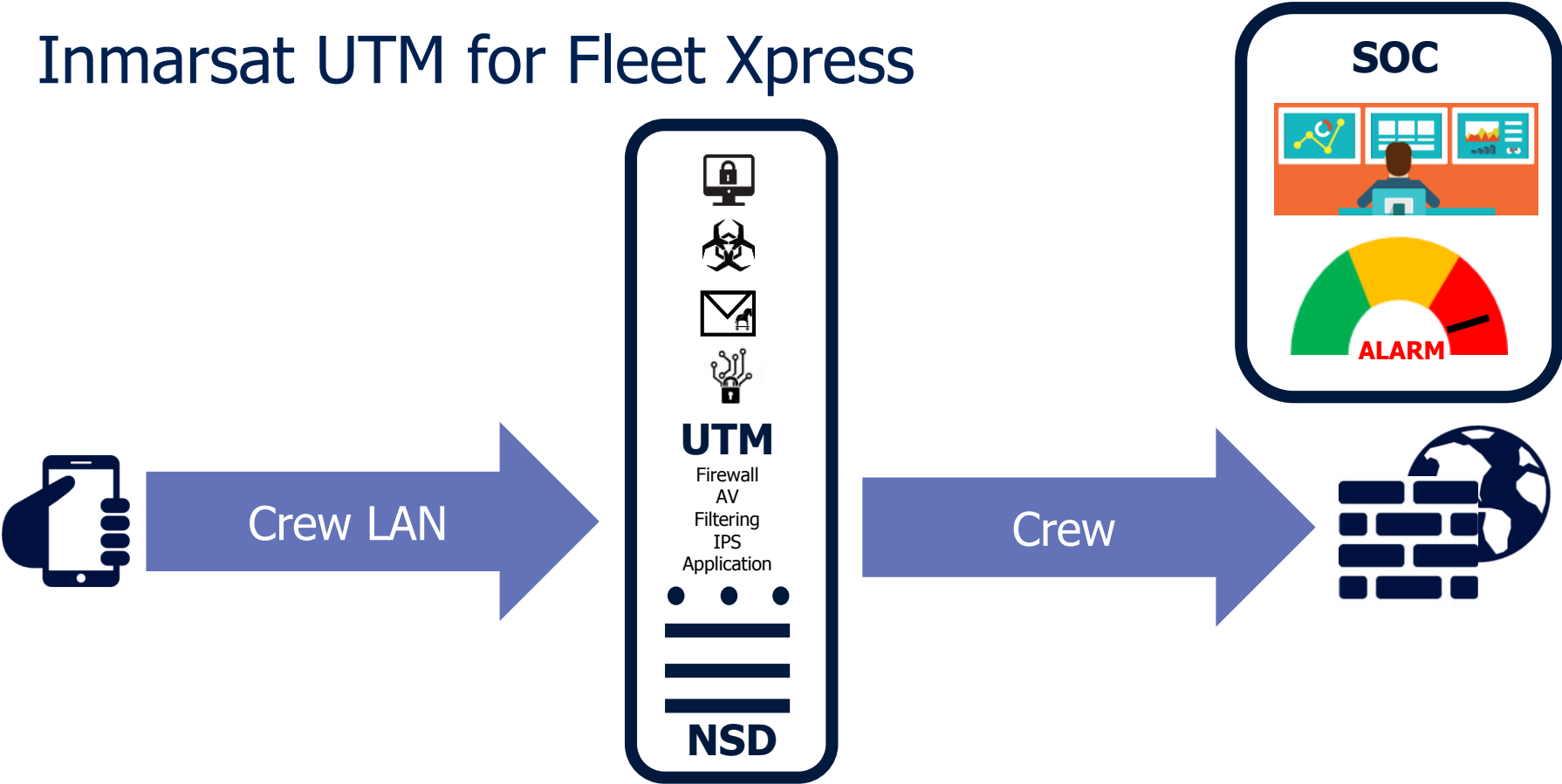
Inmarsat UTM for Fleet Xpress



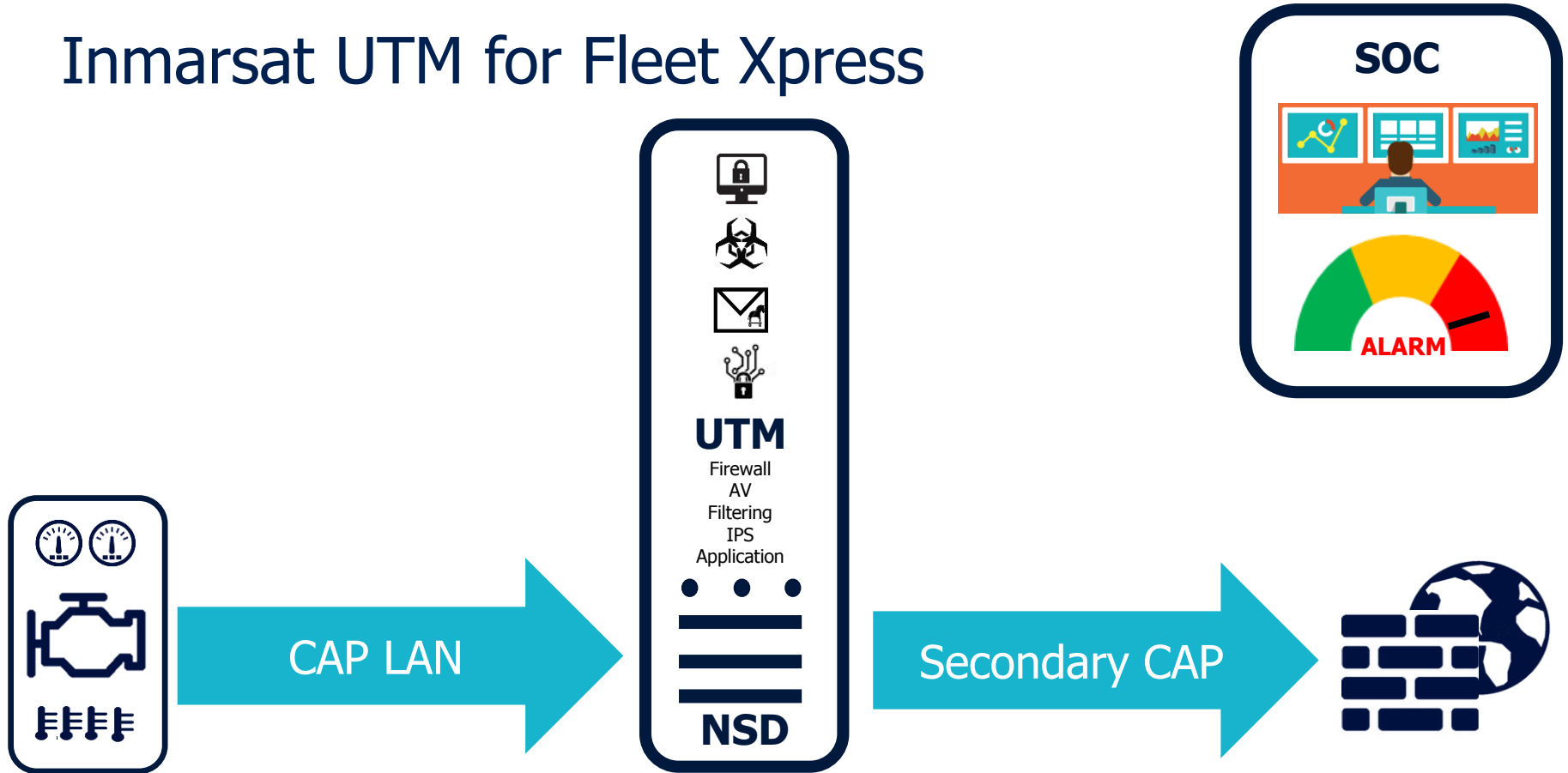
Inmarsat UTM for Fleet Xpress



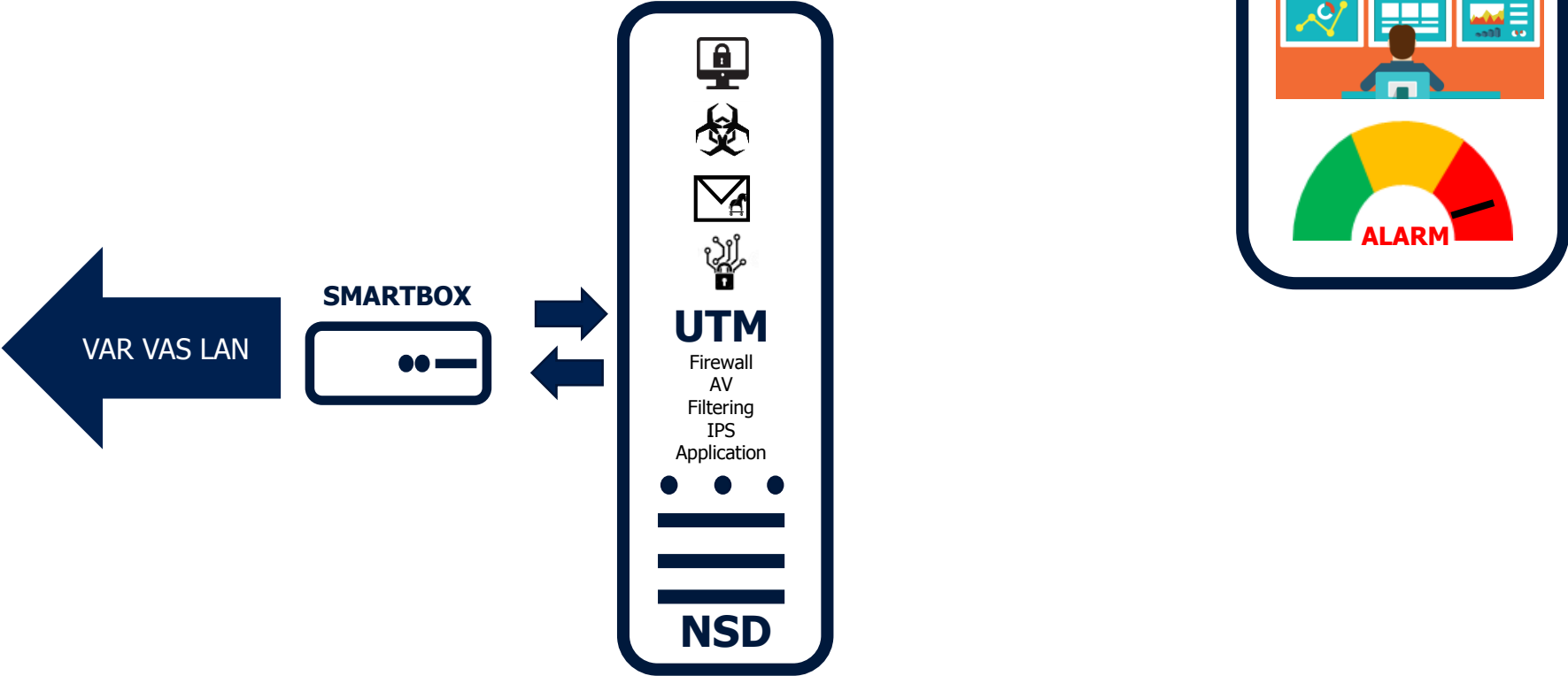
Inmarsat UTM for Fleet Xpress



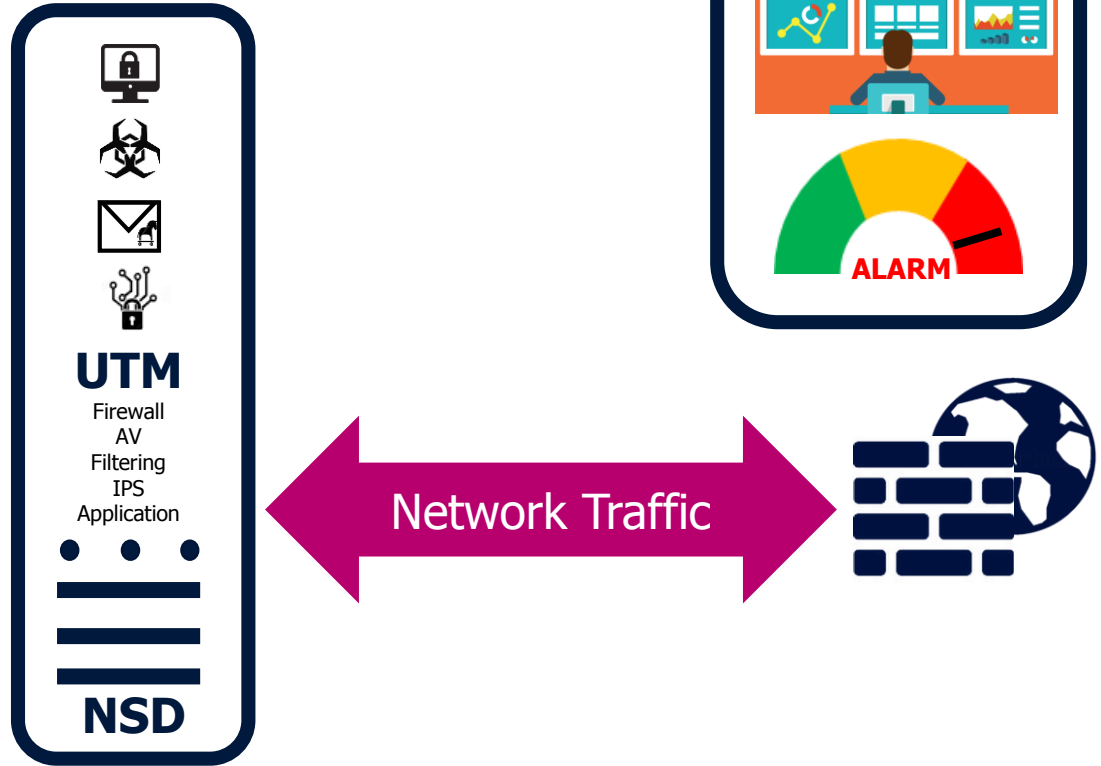
Inmarsat UTM for Fleet Xpress



Inmarsat UTM for Fleet Xpress



Inmarsat UTM for Fleet Xpress



Summary

Inmarsat UTM for Fleet Xpress

- > Inmarsat's UTM offers a consolidated range of security functions in a single device
- > The UTM is part of a Managed Security Service backed by security experts
- > The managed UTM service provides perimeter security controls as the core component of an overall "defense in depth" security strategy
- > Security event data is readily available via the Security Operations Centre portal
- > Proactive security event management can generate alarms to report in real-time
- > The managed service has no impact on the customer bandwidth



Thank you

Peter Broadhurst, SVP Safety and Security