Telecommunications (Security) Act 2021.
How Trusted Compute from CyberHive enables compliance with the principle of 'Assumed Compromise'

The Telecommunications (Security) Act 2021 sets out the following key concepts:

The principle of 'assumed compromise'
1.11 Providers should establish the principle of 'assumed compromise'. This means that providers should normally assume network oversight functions to be subject to high-end attacks, which may not have been detected by the provider, and implement business practices which, by their nature, make it difficult for an attacker to maintain covert access to these functions. This can be achieved through establishing secure platforms which implement trusted boot, and periodically rebuilding the functions to an up to date known-good state.

Management functions for network oversight functions
1.12 In addition, given that security compromises affecting network oversight functions are likely to have a significant impact on the proper operation of the network, the management functions used to manage network oversight functions should have enhanced protections, including using dedicated management functions, a segregated management plane and an enhanced control set.

Approach to monitoring and analysis
1.13 Under Regulation 6, providers must take such measures as are appropriate and proportionate to monitor and analyse both access to security critical functions and their operation, and investigate any anomalous activity. Given the essential role of network oversight functions, the use of these functions and the systems that manage them should be subject to an enhanced level of monitoring, including real-time monitoring of changes to network oversight functions and monitoring for signs of exploitation.

These concepts put a significant burden on providers to not only protect against undetected attacks, create new segregated management layers and implement enhanced monitoring but also to prove how they achieve compliance.

CyberHive Trusted Compute has been developed with a 'secure by design' Trusted Computing approach. This patented technology, developed in conjunction with the University of Oxford, creates a hardware backed, distributed allow list that continually attests what is configured and running on the hardware. The **Trusted Compute** kernel module starts at boot and attests the platform configuration is in a known good state. **Trusted Compute** continues to run, and as new programs start, they are audited in real time and validated against the allow list.

CyberHive Ltd
T: +44 (0)1635 881 881 (Office)
www.cyberhive.com

A Trusted Platform Module (TPM) or equivalent secure enclave is used as the root of trust ensuring proof that the system is always running in a known good state.

Trusted Compute has its own, separate management plane which can be administered independently of the operating system providing segregation of duties for management oversight.

The **Trusted Compute** dashboard alerts in real time any changes which deviate from the known good state and details exactly which file, or configuration is not in compliance. This enables users to immediately pinpoint the source of any exploitation and enables rapid remediation.

For more information

Contact CyberHive today for a demonstration of how Trusted Compute enables compliance with the Telecommunications Act 2021.

info@cyberhive.com
www.cyberhive.com

CyberHive Ltd
T: +44 (0)1635 881 881 (Office)
www.cyberhive.com