Dear NIST.

A short note on one specific area of the new CSF 2.0 proposal

We remain surprised that Cyber Threat Intelligence is not either its own category or has a more significant presence generally in subcategories. As a generally accepted standard practice to have intelligence led security operations, to have an operational and strategic intelligence capability to drive strategy and tactical intelligence to support detection and response, it seems odd not to have it more prominent and defined.

We would recommend that, as we see international legislation mandate intelligence functions it should be its own 'Predict' function or at the very least a Category of Identify

CTI help assess and predict current and future threats. It helps inform security control decisions based on threat actor TTPs. It informs testers and red-teams on attack TTPs to simulate in their tests. It supports incident response with attribution and assessment of other or TTPs and helps defence detection at a technical indicator and behaviour levels – all of this remains missing from CSF but is a critical part of our day to day security operations.

Best regards

Rob

Rob Dartnall

SA