

[Redacted]

To:

[Redacted]

[cyberframework](#)

Subject:

NIST CSF 2.0 Core - Feedback

Date:

Monday, May 8, 2023 12:03:54 PM

Hello,

After having read the proposal I feel that the draft is missing important aspects of CTI. In my, and many others' view, CTI or intelligence analysis should be its own function, for example "predict".

Why?

CTI help decision makers make informed security decisions.

It 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

These are missing from the proposal, yet they are critical parts of day to day security operations.

Kind Regards,

Freddy Murstad

Senior Threat Intelligence Analyst



[Redacted]

[Redacted]