[redacted] [redacted]
Subject: EXT :FW: Feedback on NIST Cybersecurity Framework 2.0 concept paper
Date: Thursday, March 9, 2023 1:47:14 PM
Attachments: CSF_2.0_Concept_Paper_01-18-23.pdf

FYI

[redacted]
Sent: Monday, February 13, 2023 10:59 PM
To: cyberframework <cyberframework@nist.gov>
[redacted]
Subject: Feedback on NIST Cybersecurity Framework 2.0 concept paper

Hi, glad to see that NIST Cybersecurity Framework 2.0 will be put forward in the near future.

As a CSF 1.0 practitioner, I have witnessed the huge security improvements across my company during the past three years. Thanks a lot for your selfless contribution to global cybersecurity. However, the cybersecurity threats and business styles constantly change over the time. As it can be seen, the cloud services are becoming widespread in the modern days, followed by many specific threats and risks. To better cope with cloud security, I hope the following points are included in CSF 2.0:

1. Cloud-based Incident Response

Due to the varied cloud deployment models and the division of responsibilities between the cloud service provider and customer, many difficulties may be encountered in the cloud-based incident response, e.g. security monitoring, evidence investigation and collection.

2. Cloud-based DR/BCM

DR/BCM is a requisite not only in the traditional IT infrastructure but also in the cloud environment. How to carry out proper DR/BCM drill on VMs shall be clearly conveyed.

3. Cloud-based supply chain management

Thank you!

Cao Kunpeng
Cybersecurity
Quality Dept./ Engineering & Service Operation Division
ZTE Corporation
[redacted]