Public Comments for ICR 202311-1670-001

Author Full Name : Moti Gindi **Received Date :** 12/17/2023 10:17 AM

Comments Received :

Section III, clause 1

We suggest to expand clause 1 b) to cover also developers behavior, as following (suggested changes marked in ***):

b) Regularly logging, monitoring, and auditing trust relationships used for authorization and access:
i) to any software development and build environments; and
ii) among components within each environment;
iii) *** the actual (normal and suspicious) developers behaviors and actions (code commits, material changes, configuration changes, etc) ***

Rationale:
Multiple supply chain attacks are based on stealing benign developer credentials or based on malicious insiders. In both cases, infected malicious code or actions to the software development and build environments - would have been deemed benign, as they are based on the justified developers authorizations. We therefore suggest to emphasize that logging and monitoring is a must also for the actual actions and behaviors of the developers, not only for authorization. This will be a must-have tool to identify malicious actions and prevent them, or investigate the impact of these actions to understand the scope of breach after the incident was discovered.