Rapport du SOC

SECURITY OPERATION CENTER

Version 1 le 28 mars 2019

I. Classification du SOC

- N1:
  la première tache consiste à formaliser et enregistrer le contexte de l'incident. Et puis débrouiller et pré-qualifier les incidents et les alertes. En général, les activités sont cadrées par des procédures.

- N2:
  Il est chargé de 3 activités principales:
  - traiter des incidents issus du centre de supervision, mettre en place des règles de corrélation pour la détection et suivre l'incident
  - veiller sur des cybermenaces et les vulnérablités
  - Rédiger des rapports de suivis d'activités

- N3:
  - Il est à même de mener l'investigation à partir de signaux faibles et de faire de la recherche exploratoire sur l'ensemble des évènements.
  - Il possède plus d'expertise sur les méthodes d'attaques; et il a aussi des qualités rédactionnelles et de synthèse.

II.

X. Annexes
SDM: Service Delivery Manager, Déployer les processus de gestion des services informatiques.