

Rapport du SOC

SECURITY OPERATION CENTER

Version 1 le 28 mars 2019

I. Classification du SOC

- N1:
la première tâche 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 vulnérabilités
 - ◆ 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 événements.
 - Il possède plus d'expertise sur les méthodes d'attaques; et il a aussi des qualités rédactionnelles et de synthèse.
- N4:
Il s'agit du poste de chef de SOC avec des qualités managériales et techniques. Ses principales activités sont:
 - ◆ management de l'équipe opérationnelle du SOC
 - ◆ respect de SLA Service Level Agreements du SOC
 - ◆ garant de la bonne application du processus: Gestion des incidents, Optimisation des traitements, suivis des demandes et des changements
 - ◆ garant de la stratégie technique du SOC
 - ◆ animation des revues hebdomadaires et mensuelles
 - ◆ définition et suivi des indicateurs de performance du SOC et mise en place des tableaux de bord
 - ◆ gestion des escalades et crises
 - ◆ rédaction des rapports d'activités (tendances et statistiques opérationnelles des cybermenaces)
 - ◆ gestion de la communication du SOC vers les autres entités de l'entreprise
 - ◆ réalisation des opérations de niveau 2 et 3

II. CSIRT

Computer Security Incident Response Team, c'est un centre d'alerte et de réaction aux cyberattaques. Les tâches prioritaires sont :

- Centralisation des demandes d'assistance à la suite de cyberattaques: réception des demandes, analyse des symptômes et éventuelles corrélations des incidents
- Traitement des alertes et réactions aux cyberattaques
- Etablissement et maintenance d'une base de données des vulnérabilités
- Prévention par diffusion d'informations pour minimiser les risques d'incidents

III. CERT

Computer Emergency Response Team, avec le même acronyme CSIRT

IV.

X. Annexes

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