QUODAGIS
Managed Services

eBook

10 bonnes raisons de se doter d'un NOC

Network Operation Center - Centre d'Exploitation Infrastructure et Réseaux

Par Gérard GOMEZ

10 bonnes raisons de se doter d'un NOC

Network Operation Center - Centre d'Exploitation Infrastructure et Réseaux

Les avantages du NOC dans l'application de la politique IT (normes, sécurité, …) sont les suivants :

1. Maintien en conditions opérationnelles du SI et de l'IT - Découverte, surveillance, maintenance et évaluation (Serveurs, réseaux, équipements, logiciels et postes de travail)
2. Installations de logiciels, dépannage/support et gestion des mises à jour y compris systèmes, logiciel et antivirus, pour les serveurs, réseaux et postes de travail
3. Gestion de la sauvegarde et du stockage
4. Services de gestion de messagerie
5. Surveillance et gestion du pare-feu et du système de prévention des intrusions
6. Gestion et analyse antivirus et correction
7. Gestion des correctifs et liste blanche
8. Analyse des menaces partagées
9. Installation et Gestion de solution trafic voix et vidéo (Téléphonie IP, ConfCall, WebConf, SVI,…)
10. Optimisation et reporting de qualité de service - Rapports sur les performances et recommandations d'amélioration

Mais qu'est-ce qu'un NOC ?

Un centre d'exploitation de réseau ou infrastructure IT et SI, ou NOC pour Network Operation Center, est un lieu focal où les techniciens informatiques s'appuient sur des logiciels de surveillance et de gestion à distance pour surveiller le Système d'Information, particulièrement les applications métier et l'infrastructure IT (Réseaux, Serveurs, Équipements et Postes de Travail).

Les équipes NOC sont fortement sollicitées dans le cadre des services informatiques managés, et c'est une formidable proposition de valeur pour de nombreux fournisseurs de services managés (MSP - Managed Services Provider).

Les équipes techniques du NOC gardent un œil vigilant sur les équipements IT et les logiciels qu'elles surveillent et gèrent. Elles résolvent en totale autonomie les incidents qui surviennent et prennent des mesures préventives pour éviter que de nombreux autres incidents ne se produisent.

Elles sont également fortement impliquées dans les actions de sécurité de haut niveau et les opérations de sauvegarde et de reprise après sinistre, **en garantissant jusqu'à une disponibilité 24x7x365 pour les Clients d'un MSP.**

Quels sont les rôles et responsabilités d'un technicien NOC ?

Les ingénieurs et techniciens du NOC sont responsables de la surveillance de la santé, de la sécurité et de la capacité du système d'information (SI) et des infrastructures (IT) dans l'environnement du Client.

Ils prennent des décisions et opèrent des ajustements **pour garantir les performances de l'infrastructure et des réseaux, et une productivité optimale.** Lorsqu'une action ou intervention du MSP est requise, les techniciens du NOC peuvent créer des alertes (ou «tickets») qui identifient et classent l'incident en fonction de la gravité, du type d'alerte et d'autres critères.

En fonction de la relation entre le NOC et le Client, les équipes techniques peuvent ensuite travailler ensemble pour résoudre l'incident (et identifier sa cause première pour éviter de futurs incidents – Gestion des problèmes ITIL®). L'équipe NOC utilise un logiciel de gestion des services commun avec les autres services de la DSI (ITSM).

Les techniciens sont organisés en fonction de « niveaux », qui indiquent la gravité et la difficulté des incidents qu'ils peuvent adresser.

Les niveaux sont numérotés de 1 (incidents plus faciles à résoudre, incidents mineurs et incidents documentés – Gestion des erreurs connues ITIL ®) et augmentent avec leur capacité à traiter le plus compliqué des incidents informatiques.

Par exemple, en cas de panne matérielle, une alerte peut être affectée à un technicien de niveau 1 dans un premier temps.

Cependant, après une inspection et un diagnostic plus approfondi, si l'incident dépasse le sujet de matériel défectueux par exemple, le ticket peut être transmis à un technicien de niveau 2 ou de niveau 3.

Les techniciens des NOC surveillent et recherchent constamment des activités « anormales » sur le SI ou l'IT, effectuent des ajustements techniques et peuvent mobiliser des ressources étendues - certaines qui ne seraient utilisées que rarement par un service informatique interne - pour répondre aux situations d'urgence.

Combler le déficit de compétences et évoluer avec un NOC

Compte tenu du déficit de compétences informatiques et de la pénurie de techniciens qualifiés et expérimentés capables de gérer le niveau 1 à 3, faire appel à un fournisseur de services managés (MSP) et son NOC est une option plus efficace et plus rentable que l'embauche de techniciens.

Compte tenu du manque de compétences, pour de nombreuses DSI, il est extrêmement difficile, voire tout simplement impossible, de doter leur entreprise de suffisamment de techniciens possédant les compétences requises pour développer leur IT et SI de manière « rentable ».

Et, compte tenu de la forte demande pour ces techniciens, les bons techniciens ont un salaire qui a également augmenté proportionnellement, ce qui rend les optimisations économiques encore plus difficiles à réaliser tout en essayant de se doter de personnel.

De fait, un NOC élimine le déficit de compétences en offrant toutes les ressources et compétences dont une DSI aurait besoin dans son personnel technique pour un montant forfaitaire mensuel ou maîtrisé (Unités d'œuvre).

SD, NOC ou SOC ?

Malgré les nombreuses caractéristiques d'un Network Operations Center, il y a une chose qu'il n'est absolument pas : un service d'assistance et de support (Centre de services - Help Desk – Service Desk). Il s'agit d'une distinction importante, que peut facilement confondre un Client ou sa DSI si elle n'est pas correctement expliquée.

La grande différence ? Un service d'assistance interagit avec les Clients finaux ; un NOC interagit avec les équipes la DSI, internes ou externes.

Le NOC assure la maintenance back-end, la résolution des incidents et le support, afin que le fournisseur de services managés puisse répondre aux incidents à mesure qu'ils surviennent et garantir la disponibilité au Client.

Le service d'assistance, d'autre part, est un centre de services - conçu pour répondre aux questions de première ligne directement des Clients finaux qui rencontrent un incident ou expriment une demande.

Un fournisseur de services managés (MSP) propose certainement des services complémentaires d'assistance et de support avec son Service Desk. En d'autres termes, si un utilisateur final (end-user) a un incident, il peut appeler le service d'assistance du MSP (Service Desk). Si le SI ou l'IT subit un incident, rupture ou dégradation de service, c'est le NOC qui détectera et interviendra.

Bien qu'ils puissent sembler ou être similaires, il existe des différences majeures dans les objectifs d'un centre d'exploitation de réseau (NOC) et ceux d'un centre d'opérations de sécurité, autrement appelé SOC (Security Operation Center).

Un NOC et un SOC ont en commun des critères clé : ils doivent travailler avec la DSI pour résoudre les incidents informatiques, et jamais avec l'utilisateur final (end-user).

Cependant, lorsqu'**un NOC se concentrera sur la surveillance et la maintenance à distance de l'environnement informatique** d'un Client pour respecter les SLA et garantir la disponibilité du Client sans dysfonctionnement technique, **un SOC sera beaucoup plus axé sur la sécurité**. Les SOC surveillent les vulnérabilités, les vecteurs et angles d'attaque et les menaces émergentes sur un réseau Client. Les équipes du SOC sont prêtes à détecter les anomalies et à atténuer les cyberattaques à mesure qu'elles surviennent.

La plupart des SOC utilisent un processus de gestion des informations et des événements de sécurité (SIEM) qui regroupe les informations de divers flux de données des systèmes axés sur la sécurité. Tout, depuis les systèmes de découverte de réseau et d'évaluation de la vulnérabilité, les systèmes de gouvernance, de risque et de conformité, les outils de test d'intrusion, les systèmes de détection et de prévention des intrusions, les systèmes de gestion des journaux ; L'analyse du comportement du réseau et bien plus est collectée et analysée par les techniciens SOC, qui sont eux-mêmes des experts en sécurité, formés et expérimentés.

Un partenariat silencieux !

Comme pour les SD et les SOC, lorsqu'un service informatique interne s'appuie avec une efficacité maximale sur le NOC d'un fournisseur de services managés (MSP), un utilisateur final (end-user) n'est même pas au courant de la présence du NOC.
Les techniciens NOC se coordonnent uniquement avec le fournisseur de solutions qu'ils prennent en charge (experts, éditeurs, constructeurs, fournisseurs), jamais directement avec un utilisateur final (end-user).
Cela crée une expérience utilisateur où le fournisseur de services managés (MSP) peut fournir en toute transparence un support de grande qualité et une résolution de incidents avec des ressources en apparence illimitées.

Faire ou faire-faire

Les coûts fixes de main-d'œuvre et d'infrastructure liées à la constitution d'une équipe interne sont généralement trop élevés à couvrir, tout en maintenant une entreprise rentable et en croissance. Même avec un personnel complet, il ne serait pas en mesure de se s'organiser pour prendre en charge les pics et creux de la demande tout en se préparant simultanément à la maintenance des tâches informatiques quotidiennes qui doivent être effectuées.

Au lieu de cela, le MSP qui dispose d'un NOC peut assumer la plupart des travaux techniques qui doivent être effectués quelle que soient la variabilité de la charge. Au lieu d'une opération interne lourde, un NOC agit comme une extension de la main-d'œuvre existante du service informatique interne, laissant le personnel technique de la DSI se concentrer sur des projets à forte valeur ajoutée et à fort retour sur investissement pour le Client.

Les Services Desk (SD), les Centres de Opérations Réseau (NOC) et les centres des opérations sécurité (SOC) fournissent de nombreux services - tous ont une valeur critique pour une DSI et les utilisateurs finaux - mais il y a peu de chevauchement dans leurs missions ou objectifs.

Au contraire, en sollicitant les services complémentaires chez un MSP, en s'appuyant sur ses équipes, ses compétences et ses offres pour profiter d'une gamme plus large de solutions et services, les DSI bénéficient d'un plus grand avantage opérationnel et économique qu'en tentant de fusionner les tâches associées à ces missions en une seule équipe hybride au sein de sa propre organisation.

A propos de QUODAGIS Managed Services

Vos équipes informatiques sont écartelées entre différentes missions et des attentes contradictoires. Il leur est difficile de se consacrer aux nouveaux projets et, en même temps, répondre aux demandes des utilisateurs au quotidien ou se concentrer sur les projets métier à forte valeur ajoutée pour votre entreprise.

QUODAGIS Managed Services est ce qu'on appelle un MSP : Managed Services Provider. Pour vous aider, QUODAGIS Managed Services propose des solutions de services managés et vous garantit les résultats concrétisés par des SLA, c'est-à-dire des engagements de niveaux de service.

Quels sont ces services ? La mise à disposition de personnel, sur site ou dans nos locaux, 2 centres de services, situés à Aurillac, et à Barcelone en Espagne, appuyés par nos bureaux de Paris et de Toulouse, pour des projets ponctuels ou un service récurrent, avec des équipes dédiées ou mutualisées, en plusieurs langues, pendant les heures ouvrées mais aussi sur des plages étendue, jours fériés, nuits et week-ends.

QUODAGIS s'appuie sur des méthodes et des pratiques reconnues du marché, des outils performants, et des équipes compétentes. Elles sont certifiées ITIL et QUODAGIS Managed Services est certifié ISO9001 et ISO27001.

Paris, Aurillac, Toulouse, Barcelone
+33 4 71 43 49 96 | managed-services.quodagis.fr | quodagis.fr