# Leidos utilise Splunk ITSI pour mieux gérer ses événements

## Résumé

Les 48 ans d'histoire de Leidos sont riches de missions prestigieuses : l'entreprise a notamment appuyé le programme de la navette spatiale américaine et contribué à la conception d'un yacht qui a remporté la Coupe de l'America. Aujourd'hui, ce leader des solutions scientifiques et technologiques, membre du Fortune 500, œuvre à relever des défis globaux dans les domaines de la défense, du renseignement, de la santé et d'autres marchés, et doit également résoudre ses propres problèmes pour veiller à ce que ses services soient toujours disponibles pour ses clients. Depuis le remplacement de sa solution de gestion des événements par Splunk® IT Service Intelligence (ITSI), le service IT interne de Leidos a constaté de multiples avantages :

- la supervision des infrastructures en temps réel à l'échelle de toute l'entreprise ;
- une solution robuste pour ouvrir les silos de données et corréler les événements ;
- des tableaux de bord adaptés à différents publics, des techniciens chargés de résoudre les problèmes aux décideurs principaux.

## Pourquoi Splunk

Le Directeur de la gestion des performances de Leidos, Don Mahler, déclare : « Nous avons une véritable passion pour la supervision de l'infrastructure. Le personnel opérationnel ne se concentre pas uniquement sur ce qui fonctionne ; il a besoin de savoir ce qui ne fonctionne plus. Dans de nombreux cas, les problèmes entraînent des dégradations des services plutôt que des interruptions de service à proprement parler. Pour le bien des opérations, il est essentiel de les devancer avant qu'elles ne s'aggravent. »

C'est un travail 24h/24, que M. Mahler divise en quatre domaines opérationnels où il utilise Splunk ITSI. Le premier est la connaissance de la situation : déterminer ce qui fonctionne et ce qui doit être réparé. La seconde est la planification des performances et de la capacité, qui consiste à examiner les performances des composants au fil du temps pour voir si l'espace, le processeur, l'utilisation des liens ou d'autres métriques dépassent des seuils dynamiques. Le troisième est la journalisation, pour des raisons d'investigation, de sécurité et de disponibilité. Le quatrième est celui des rapports sur la livraison des services, qui offrent à Leidos une visibilité en temps réel sur son environnement opérationnel.

L'épreuve de vérité consiste à trouver et à corriger les problèmes avant que les clients ne les rencontrent. Don Mahler était à la recherche d'une solution capable de réunir les silos des sous-départements, de l'IT et des fonctions métier, et de trier un déluge d'événements couvrant plus de 120 services IT, car il était confronté à de multiples défis.

leidos

### Secteur d'activité

- Technologie

### Scénarios d'utilisation Splunk

- Gestion des opérations IT
- Gestion des logs
- Securité

### Défis

- Nécessité de mise en place d'une capacité de supervision et réponse pour assurer un accès 24h/24, 7j/7 aux clients
- Un service IT balkanisé par la séparation des silos
- Nécessité de filtrer des milliers d'alertes et d'événements

### Impact sur l'entreprise

- Corrélation en temps réel et moteur de règles pour automatiser la gestion des événements
- Intégration transparente avec les systèmes de gestion, les applications et les extensions
- Tableaux de bord et glass tables faciles à partager et à personnaliser pour les vues des processus IT et métier

### Sources de données

- Application
- Périphérique
- Pare-feu
- Réseau
- Serveur

### Produits Splunk

- Splunk Enterprise
- Splunk IT Service Intelligence (ITSI)
- Splunk DB Connect
- Splunk App for Microsoft Exchange

## Au-delà de la gestion des logs : transformer les opérations du centre de données

Leidos a commencé par une petite licence Splunk Enterprise pour collecter les logs des routeurs et des switches. L'implémentation s'est rapidement élargie pour centraliser les alertes, les tickets, les informations sur le réseau, les modifications et les données de performances de milliers d'appareils ; toutes ces données non structurées sont désormais représentées visuellement dans des tableaux de bord Splunk Enterprise.

Autre grand avantage selon M. Mahler, la plateforme Splunk brise les silos en permettant aux équipes de voir les données de toute la pile de service. Non seulement les utilisateurs peuvent obtenir les informations dont ils ont besoin, mais le personnel des serveurs, par exemple, peut accéder aux données de pare-feu pertinentes.

« Je vois la plateforme Splunk comme le modèle de données unifié de l'environnement, et comme un outil qui peut être utilisé par chaque informaticien (et chaque membre des fonctions métier) pour obtenir des réponses sur les services informatiques. »

M. Mahler témoigne : « Je travaille dans la gestion informatique depuis plus de 20 ans et je n'ai jamais croisé un produit capable de faire cela. C'est la première fois que je peux vraiment effectuer une supervision de mon environnement IT hétérogène sur toute la hauteur de la pile : Splunk détient toutes les données et je peux toutes les analyser à l'aide des mêmes outils. »

## Gérer intelligemment les événements

L'étape suivante était naturellement la gestion des alertes. Leidos utilisait depuis plus de 15 ans une autre solution qui était non seulement obsolète mais aussi peu conviviale, avec un langage complexe de règles de back-end. L'entreprise voulait un produit moderne avec des corrélations prêtes à l'emploi et un moteur de règles capable de faire la distinction entre les événements critiques et mineurs.

La réponse : Splunk ITSI.

**« Nous avons tellement d'informations à portée de main grâce à Splunk… nous passons notre temps à résoudre les problèmes commerciaux de manière créative. »**

— Don Mahler, Directeur de la gestion des performances, Leidos

M. Mahler explique : « Certains jours, c'est un véritable déluge d'événements. Splunk les hiérarchise et nous éclaire non seulement sur les défaillances en cours mais aussi sur les éléments du système qui sont affectés par elles à l'instant où vous regardez l'écran des alertes. »

Outre les exigences de base telles que la consolidation des événements provenant d'un environnement IT hétérogène, la détection et l'élimination des doublons dans les alertes, la suppression des alertes résolues et leur conversion en événements exploitables, l'entreprise avait besoin de fonctionnalités supplémentaires, en particulier pour faire remonter automatiquement une alerte après un certain délai ou la supprimer si un périphérique est délibérément mis hors ligne. Leidos est parvenu à mettre tout cela en place avec Splunk ITSI.

Désormais, une vingtaine de systèmes de gestion, de Microsoft System Center Configuration Manager (SCCM) aux outils de gestion réseau SolarWinds, et plus de 4 500 éléments de configuration (CI) provenant de 120 services IT et 240 sites dans le monde, envoient leurs données à la plateforme Splunk ITSI de Leidos et aident ainsi l'entreprise à passer d'un volume quotidien d'alertes oscillant entre 3 500 et 5 000 à une cinquantaine de tickets exploitables par les opérations du réseau et du datacenter. La transmission des informations CMDB à Splunk ITSI permet d'afficher des alertes différentes en fonction des équipes.

Le résultat : un accès plus simple à des données plus pertinentes, et la possibilité pour les équipes de consacrer leur temps aux problèmes les plus importants. M. Mahler conclut : « Ma mission la plus importante, en fin de compte, est de veiller à ce que nous fassions une différence, que nous fournissions un service que les gens trouvent précis et pertinent. Vu que Splunk possède toutes les informations, chacun peut obtenir des réponses plus rapidement, plus précisément et plus efficacement. »



20-14987-Leidos-A4-102-CS_fr-FR