



Services de surveillance de la sécurité d'entreprise

Les entreprises subissent une pression constante en matière de protection de leurs données et systèmes critiques.

S'assurer du respect des réglementations en vigueur est la clé d'une stratégie de sécurité efficace mais la plupart des entreprises ne parviennent pourtant toujours pas à surveiller leurs réseaux en continu. Trop souvent, elles s'en remettent à leurs équipes internes pour assurer un suivi 24h/7j des systèmes, ce qui laisse apparaître des failles, voire une incapacité totale à analyser les logs.

Or, les réglementations PCI DSS, HIPAA, SOX et autres exigent un suivi constant de ces logs. Et en cas d'infraction, les sanctions peuvent être très sévères.

C'est pourquoi les services de surveillance de NTT Security vous proposent un monitoring et des analyses 24h/7j de vos logs, afin d'assurer votre conformité.

Une surveillance assurée par des experts

Nous décortiquons les logs de quasiment tous les systèmes capables d'en générer, y compris vos applications, vos bases de données, vos terminaux, vos pare-feux, vos systèmes de détection et de prévention des intrusions (IDS/IPS) et de gestion unifiée des menaces (UTM), vos pare-feux d'applications web (WAF), vos systèmes de monitoring de l'intégrité des fichiers (FIM) et autres équipements réseau. Nous enrichissons ensuite ces données d'informations contextuelles sur les vulnérabilités, la géolocalisation d'adresses IP, les hôtes malveillants et les utilisateurs privilégiés et standard. Au final, vous bénéficiez d'une surveillance de tous les instants, en accord avec votre politique de

sécurité interne, les bonnes pratiques en vigueur et vos obligations réglementaires.

Surveillance de la sécurité : deux niveaux de services partageant des caractéristiques communes

Nos services de surveillance se déclinent en deux formules : Enterprise Security Monitoring Standard et Enterprise Security Monitoring Enhanced. Dans tous les cas, vous bénéficiez d'une surveillance 24h/7j, assurée par nos centres opérationnels de sécurité dédiés. Chaque formule se base sur la Cyber Threat Intelligence (CTI) du Global Threat Intelligence Center (GTIC) de NTT Security.

Enterprise Security Monitoring Standard

La formule Standard a été spécialement conçue pour les entreprises soumises à des exigences de conformité sur un noyau dur de technologies de sécurité. Il comprend un suivi 24h/7j basé sur des règles de détection standard appliquées à toutes ces technologies. Ce service cloud vous propose également un monitoring et des interventions de base réalisées par nos centres opérationnels de sécurité, avec escalade de l'incident vers vos équipes pour des investigations plus poussées ou le classement du dossier.

Pour le suivi et le maintien de votre conformité, nous nous appuyons sur notre propre plateforme.

Le service Standard comprend également l'accès à un portail personnalisé pour une communication efficace des événements, à un tableau de bord des services et à des rapports de conformité technique et opérationnelle.

Avantages des services de surveillance de NTT Security

- Suivi actif et reporting détaillé de conformité aux lois et réglementations pour éviter toute infraction
- Protection 24h/7j des données et systèmes de votre entreprise avec service de monitoring et d'intervention dans le cloud
- Accès à plusieurs centres opérationnels de sécurité (SOC) pour une disponibilité 24h/7j
- Escalade des événements de sécurité et alertes contextualisées
- Cas d'utilisation et règles d'alerte personnalisables en fonction de vos exigences métiers
- Optimisation de la surveillance de votre sécurité via NTT Security Enterprise Security Program Services (ESPS)
- Formules flexibles pour une évolution au fil de votre croissance

Enterprise Security Monitoring Enhanced

Notre service Enhanced a été spécialement conçu pour les entreprises soumises à des exigences de conformité complexes sur un vaste ensemble de technologies de sécurité. Nous répondons à des besoins complexes, notamment par la création de règles de corrélation et de notification en phase avec des exigences métiers très spécifiques. Actuellement, nous supportons plus de 200 technologies de divers fournisseurs.

Ce service comprend un suivi 24h/7j assuré par nos centres opérationnels de sécurité mondiaux. Notre équipe identifie les événements à risque, puis les soumet à examen et validation par des analystes certifiés de niveaux 1 et 2. Une fois validés, ces événements vous sont transmis sous la forme de rapports d'incident de sécurité pour une investigation plus approfondie.

Notre service Enhanced bénéficie également de l'appui direct du Global Threat Intelligence Center (GTIC) de NTT Security. Il comprend l'accès à un portail personnalisable pour une communication efficace des événements et incidents de sécurité, à un tableau de bord des services et à des rapports de conformité technique et opérationnelle.

Graphique 1 : Enterprise Security Monitoring Standard vs. Enterprise Security Monitoring Enhanced : comparatif des fonctionnalités

Fonctionnalité	Enterprise Security Monitoring Standard	Enterprise Security Monitoring Enhanced
Accès 24h/7j aux centres opérationnels de sécurité	✓	✓
Soutien direct du Global Threat Intelligence Center de NTT Security		✓
Profil de conformité sécuritaire standardisé	✓	
Profil de conformité sécuritaire personnalisé pour un large éventail d'équipements		✓
Rapports d'incident de sécurité revus par un analyste ¹	✓	✓
Portail web personnalisable	✓	✓
Reporting de monitoring et de conformité personnalisable	✓	✓
Accès aux données des événements et incidents de sécurité des 90 derniers jours	✓	✓
[Option] Recherche sur les logs bruts		✓
[Option] Gestion et stockage sécurisés des logs sur le long terme	✓	✓

L'entreprise NTT Security

NTT Security est la branche et centre d'excellence sécurité du groupe NTT. Nous mettons notre expertise au service des entités du groupe NTT en délivrant des solutions métiers résilientes pour accompagner leurs clients dans leur transformation numérique. Forte de ses 10 centres opérationnels de sécurité (SOC), ses 7 centres de R&D et plus de 1 500 experts en sécurité, NTT Security intervient chaque année sur des centaines de milliers d'incidents à travers six continents.

Pour optimiser l'utilisation de nos ressources locales et libérer le potentiel de nos capacités mondiales, nous offrons un ensemble adapté de services de sécurité managés (MSS) mais également de conseil stratégique ou technologique aux entreprises. NTT Security fait partie intégrante du groupe NTT (Nippon Telegraph and Telephone Corporation), l'une des plus grandes entreprises de TIC au monde. Visitez www.nttsecurity.com/fr-fr pour en savoir plus sur NTT Security ou www.ntt.co.jp/index_e.html pour le groupe NTT.

1. Le service Enterprise Security Monitoring Standard automatise le reporting des événements quasi-avérés, mais sollicite l'avis d'un analyste de sécurité dans certains cas particuliers.