NTT Security

Présentation de solution

Services de détection des cybermenaces

Aujourd'hui, les entreprises doivent faire face à des cybermenaces avancées et persistantes auxquelles aucun système de sécurité traditionnel ne peut résister.

La sophistication élevée de ces menaces allonge les délais de détection et de neutralisation, ce qui laisse aux cybercriminels davantage de temps pour atteindre leurs objectifs dans les environnements compromis. Plus longue est la détection, plus grave sera l'impact commercial de l'intrusion sur la réputation, l'image de marque et la valorisation en Bourse de l'entreprise, sans parler des sanctions financières et procès à son encontre.

Face à ce risque, aucune solution ou technique ne peut à elle seule détecter une attaque avancée. C'est pourquoi les services de détection des cybermenaces de NTT Security reposent à la fois sur diverses sources disponibles sur le marché et sur nos propres capacités d'analytique avancée, de traque et de détection des menaces.

Deux niveaux de service partageant des fonctionnalités communes

Pour vous aider à détecter les cybermenaces, nous proposons **Threat Detection Standard** et **Threat Detection Enhanced**. Ces deux services reposent sur le triptyque surveillance 24h/7j, traque et détection avancée des menaces, et cyberveille complète assurée par le Global Threat Intelligence Center (GTIC) de NTT Security.

Fini la masse de faux positifs générés par les solutions traditionnelles ! Quelle que soit l'option choisie, Threat Detection ne retient que les vraies menaces qu'elle vous signale directement sous la forme d'un rapport d'incident.

Nos analystes et nos systèmes automatiques traquent et examinent les menaces afin de mesurer leur impact et vérifier toute autre information associée à l'intrusion potentielle. Vous recevez ensuite un rapport de synthèse détaillé, assorti des recommandations d'actions à engager. À la clé : une réduction substantielle de vos délais d'intervention.

Analytique avancée

Parce que les menaces actuelles reposent sur des techniques en mutation perpétuelle, les services de détection ne peuvent se fier exclusivement aux méthodes traditionnelles. C'est pourquoi nos services de détection des cybermenaces s'appuient sur l'analytique avancée pour l'identification de comportements suspects. Grâce à la Cyber Threat Intelligence (CTI), au machine learning, à la corrélation avancée et à la modélisation des comportements malveillants, il est possible de détecter avec précision les menaces connues et inconnues.

Threat Detection Standard

Adossée aux capacités de détection des cybermenaces de NTT Security, cette option propose un service automatique et avancé aux entreprises en quête d'une solution d'entrée de gamme.

En cas d'incident quasi-avéré, vous recevez un rapport qui décrit clairement la violation de sécurité identifiée et émet des recommandations à l'attention de votre équipe d'intervention sur incident.

Les clients Threat Detection ont également accès à la CTI collectée en continu par NTT Security. Une fois une menace de sécurité identifiée et catégorisée comme incident, les informations la concernant sont mises à votre disposition.

Avantages des services de détection des cybermenaces de NTT Security

- Analytique avancée, y compris machine learning et modélisation des comportements malveillants pour la détection de cybermenaces échappant aux dispositifs de sécurité traditionnels
- Analystes de nos centres opérationnels de sécurité (SOC) et console d'analyse sur-mesure†
- Investigation avancée des incidents par des experts dotés de toutes les informations disponibles†
- Traque des menaces basée sur les événements†
- Support en cas d'incident, de la détection à la remédiation†

†Compris dans la formule Threat Detection Enhanced

Threat Detection Enhanced

Le service Enhanced s'appuie sur l'analytique avancée, la cyberveille et la traque des menaces pour détecter les attaques les plus sophistiquées.

Toute activité suspecte est transmise avec toutes ses données contextualisées à un analyste expérimenté, chargé de confirmer la menace et son impact. Vous recevez ensuite un rapport d'incident détaillé avec des recommandations d'actions spécifiques à engager.

Notre analyste en sécurité mettra à jour ce rapport d'incident et vous accompagnera dans vos activités de remédiation jusqu'à résolution complète de l'incident.

Fonctionnalités Threat Detection Enhanced

Intégration et collecte de preuves

Le niveau Enhanced permet une intégration de fournisseurs. L'intégration étroite à de multiples fournisseurs et technologies compatibles permet de collecter de multiples éléments de preuve (données de capture du trafic, logs des terminaux, traces d'exécution des malwares et informations contextuelles au-delà des simples sorties syslog).

Traque des menaces basée sur les événements

Dans le cadre de notre service Enhanced, nos analystes décortiquent les événements pour traquer les menaces à travers un large éventail de technologies. Grâce à la console d'analyse signée NTT Security, ils accèdent à l'intégralité des données de surveillance du client, des informations contextualisées et des éléments de preuve.

Services d'intervention

Les analystes NTT Security interviendront eux-mêmes afin de stopper la propagation des menaces dans l'environnement client. Ils pourront par exemple mener des interventions sur incidents à distance afin d'isoler les terminaux compromis, ou encore de bloquer l'accès au réseau des URL et adresses IP malveillantes.

Alliées à nos capacités de détection avancée des menaces, ces fonctionnalités de confinement offrent à nos clients un service complet de détection et d'intervention managées (Managed Detection and Response - MDR).

Figure 1 : Threat Detection Standard vs. Threat Detection Enhanced – comparatif des fonctionnalités

Fonctionnalité	Services de détection des cybermenaces	
	Threat Detection Standard	Threat Detection Enhanced
Accès 24h/7j aux centres opérationnels de sécurité	✔	✔
Services adossés au Global Threat Intelligence Center de NTT Security	✔	✔
CTI mise à jour en continu à partir des investigations en production	✔	✔
Analytique avancée basée sur le machine learning / la modélisation des comportements	✔	✔
Intégration de différents fournisseurs et collecte de preuves pour les principales technologies de sécurité[1]		✔
Investigation poussée des incidents de sécurité par nos analystes		✔
Traque des menaces basée sur les événements		✔
Rapports d'incident automatisés	✔	
Rapports d'incident basés sur des investigations poussées et une traque active des menaces		✔
Portail web personnalisable	✔	✔
Accès à 90 jours de données historiques sur les événements et incidents	✔	✔
[Option] Recherche dans les logs bruts des clients		✔
[Option] Gestion et stockage sécurisés des logs sur le long terme		✔
[Option] POD sur site[2]		✔
[Option] Intervention de NTT Security pour le confinement des terminaux compromis (à distance)[3] et/ou blocage de l'accès au réseau des URL/adresses IP malveillantes[4]		✔

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. Collecte et analyse des éléments de preuve supplémentaires comme les données de capture du trafic (PCAP), les rapports d'exécution des malwares et les enregistrements des hôtes.
2. Nous installons des POD chez les clients qui exigent ou préfèrent conserver leurs logs sur site. *3. Le confinement des terminaux requiert une solution de protection des terminaux managée par NTT Security.*
4. Le confinement des URL/adresses IP requiert une solution réseau managée par NTT Security