

**DTS****Managed Detection and Response (MDR)**

# Managed Detection and Response

*Le monde de la cybersécurité d'aujourd'hui se caractérise par une menace en constante évolution. Les cybercriminels développent sans cesse de nouvelles techniques et méthodes pour accéder aux réseaux. Il est donc de plus en plus difficile pour les entreprises de protéger leurs systèmes informatiques. Selon des études récentes, il faut actuellement en moyenne 280 jours pour détecter et contenir une violation de données. Le plus grand défi pendant la détection et de la réaction est probablement, que de nombreuses entreprises n'ont pas la possibilité de mettre en place 24h/24 une équipe hautement qualifiée, car cela est très coûteux et prend beaucoup de temps. Pour pouvoir réagir à de telles menaces, il faut de nouvelles technologies, de nouveaux processus et de nouvelles compétences sont nécessaires 24 heures sur 24, 365 jours par an. Ainsi, le DTS Managed Detection and Response (MDR) est une solution idéale.*

- Détection, surveillance et réaction 24/7/365 gérée
- 4 sites SOC en Europe avec du personnel formé, spécialisé et certifié
- Automatisé, Analyse & réaction basé sur la technologie
- Recherche de menaces proactive et constante
- Analyse de causes, délimitation et Résolution des processus
- Détection de menaces sur la base des informations provenant des principaux plateformes de Threat intelligence
- Enquêtes électroniques légales
- Gestion de l'état- général, l'état de santé et du système de disponibilité



## Palo Alto Networks Cortex XDR Pro

DTS MDR utilise la technologie unique de Palo Alto Networks Cortex XDR Pro comme élément essentiel du service. Avec Cortex XDR Pro, vous stoppez les nouvelles attaques grâce à la première plateforme de détection étendue ouverte et basée sur l'IA du secteur et de réponse qui prend en compte toutes vos données de point final, de réseau et de cloud. Elle offre non seulement la possibilité en tant que solution Endpoint Detection and Response (EDR), d'exécuter une approche Prevention First sur l'Endpoint, mais aussi de collecter simultanément des informations précieuses sur le point d'accès afin de détecter les attaques ciblées. En outre, la solution Cortex XDR Pro permet, grâce à une technologie unifiée et entièrement intégrée, de prévenir, de détecter et d'empêcher de manière fiable les menaces des menaces - du réseau au cloud en passant par les points finaux et les sources de données tierces.

### Identifier les attaques à un stade précoce et les combattre de manière conséquente

Le partenariat stratégique avec Palo Alto Networks permet à DTS de fournir une technologie de pointe grâce à des services stratégiques ennobliés.

Le service DTS Managed Detection and Response (MDR) permet d'évaluer le degré de maturité de votre programme de sécurité en termes d'augmenter considérablement la détection et la réponse aux menaces. Il offre à cet effet une combinaison d'expertise hautement qualifiée et une technologie de premier ordre pour une détection rapide des menaces dynamiques dans tout l'écosystème du client. Le service DTS MDR offre une surveillance des menaces et une défense 24h/24, 7j/7 et 365j/an, assurées par nos Security Operations Center (SOC) experts. Cette combinaison efficace de technologie et de surveillance active par des experts, garantit une détection rapide des cyber-attaques potentielles et la mise en place immédiate de contre-mesures. DTS offre tous les avantages d'un propre SOC de premier ordre, 24 heures sur 24 et 7 jours sur 7, sans les coûts élevés, la complexité, les difficultés que cela implique et les défis liés à la mise en place et à l'exploitation d'un SOC propre. Allégez la charge de travail de votre équipe, pour qu'elle puisse se concentrer sur les véritables processus clés de l'entreprise.

Les services DTS Managed Detection and Response étendent l'approche Prevention First basée sur la technologie pour lancer des mesures de détection essentielles en cas d'urgence - gérées par des experts en cybersécurité disposant d'une expertise technique avérée et d'une longue expérience.

