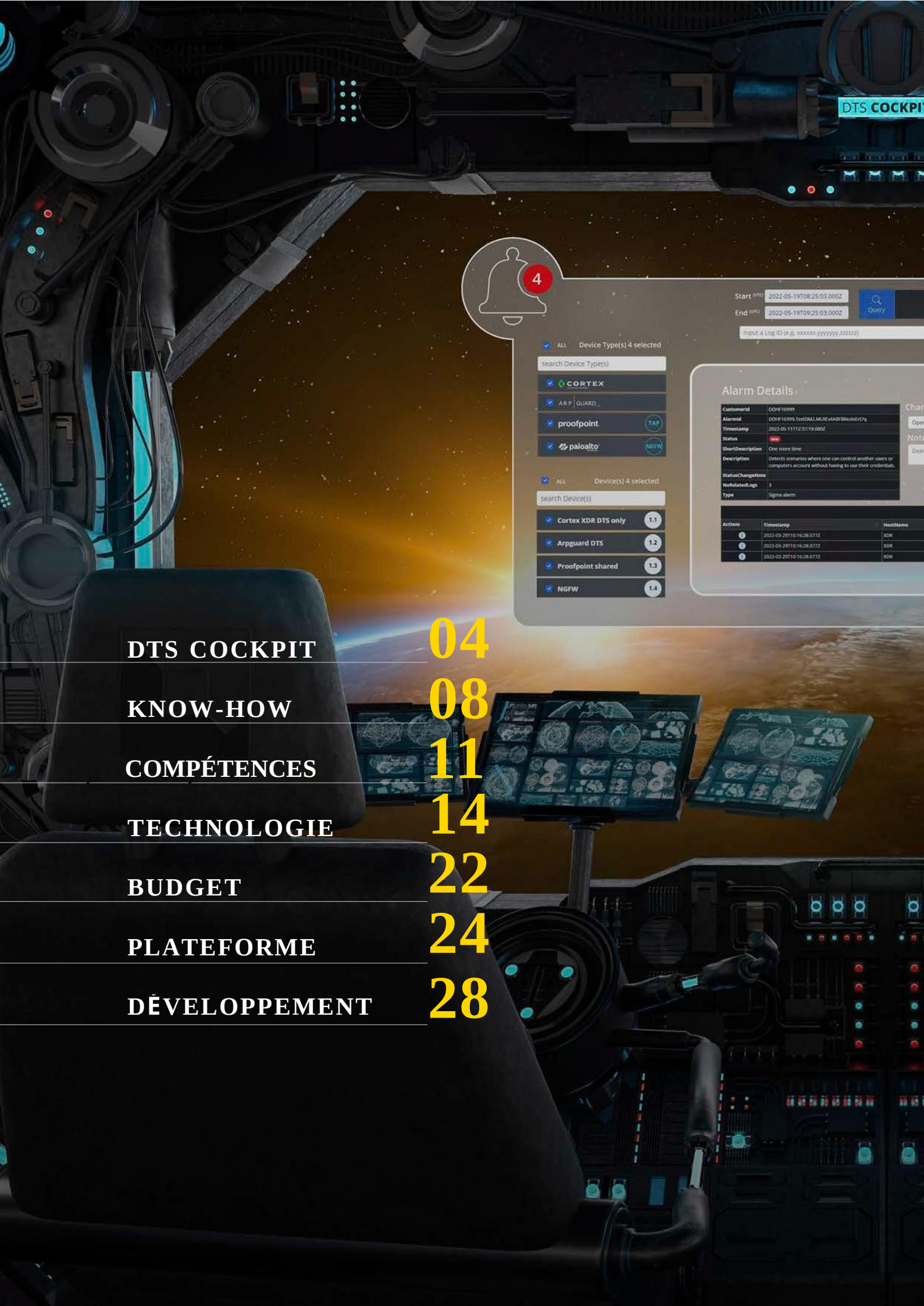
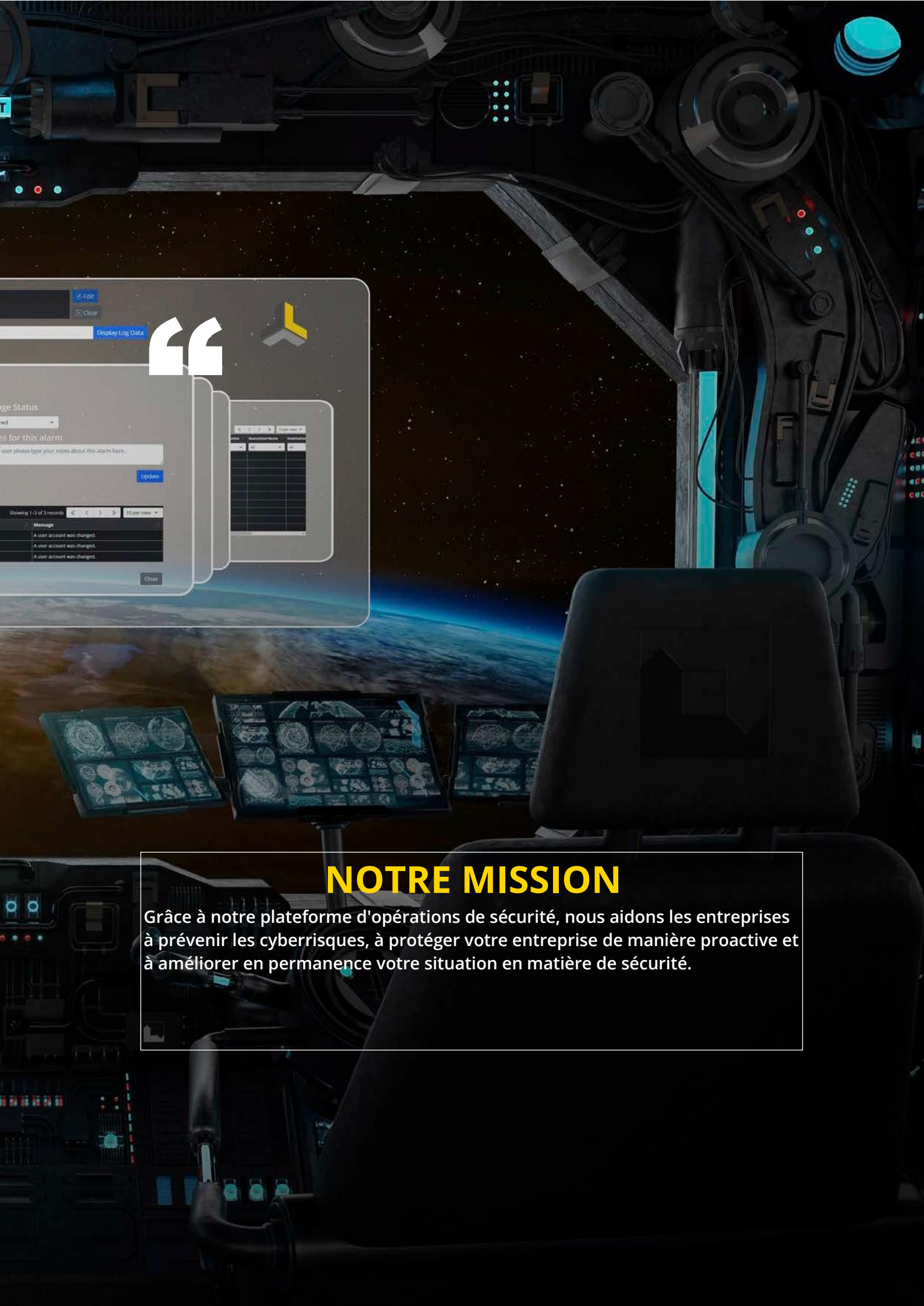
DTS Cockpit

La plateforme d'opérations centrale de sécurité pour les PME

WHITEPAPER
Juillet 2023





NOTRE MISSION

Grâce à notre plateforme d'opérations de sécurité, nous aidons les entreprises à prévenir les cyberrisques, à protéger votre entreprise de manière proactive et à améliorer en permanence votre situation en matière de sécurité.

DTS Cockpit Service Guide

Voir. Comprendre. Agir.

La plateforme centrale d'opérations de sécurité

Nous avons développé une plateforme révolutionnaire et abordable, et ce n'est qu'un début pour nous. La solution nous donne la possibilité de suivre une voie indépendante et de rompre avec le marché classique. Nous nous éloignons du marché classique des revendeurs pour aller vers une plateforme globale. Avec notre DTS Cockpit, vous obtenez une transparence totale de votre situation en matière de sécurité informatique, 24 heures sur 24 et 7 jours sur 7. Ce qui rend la plateforme si unique, c'est sa simplicité d'utilisation, nos services gérés et son prix abordable pour les PME. Nous sommes votre interlocuteur dès le début et nous déchargeons votre service informatique.

Kai Mallmann, CEO

En France, le coût financier moyen pour une PME d'une cyberattaque est estimé entre 300K€ ou 500K€. Pour les petites et moyennes entreprises, cela peut représenter un énorme impact financier difficilement surmontable.

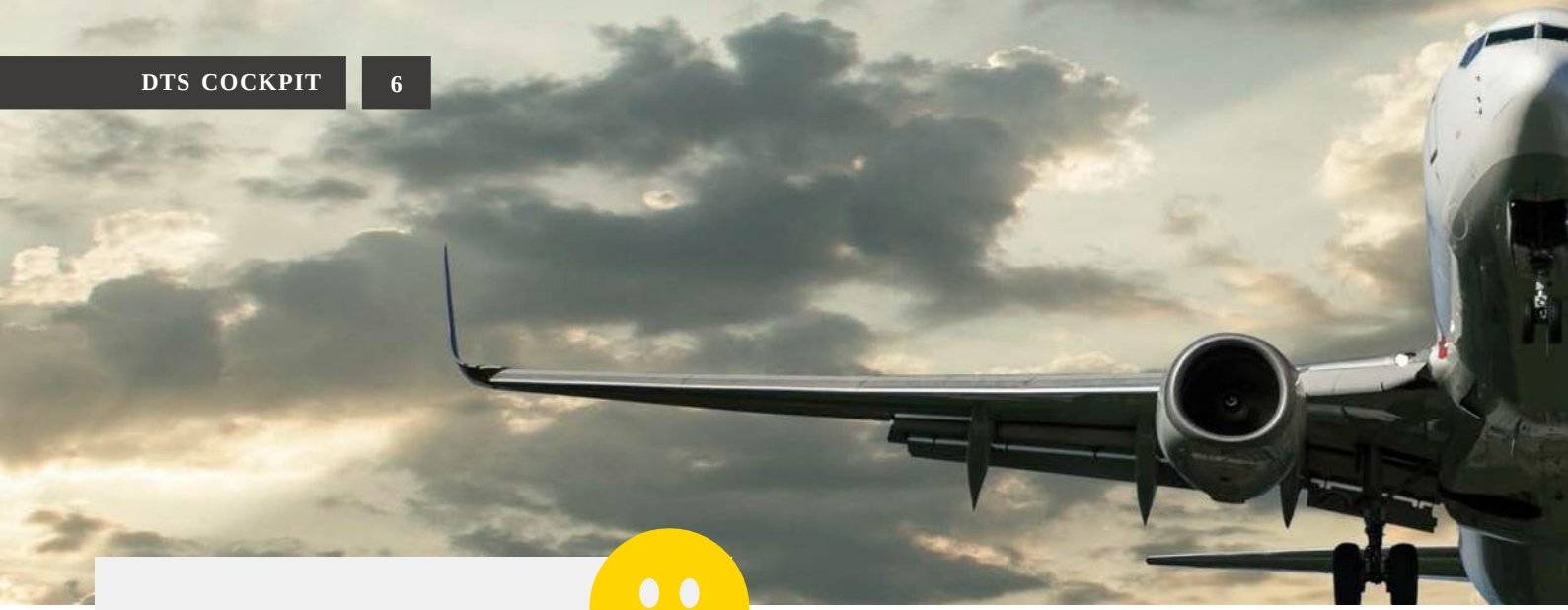
Il existe d'innombrables solutions et services de sécurité sur le marché et presque toutes les entreprises utilisent une grande variété de produits basés sur l'approche « le meilleur de leur catégorie». Néanmoins, le nombre de cyberattaques ne cesse d'augmenter et, surtout, une sécurité 24h/24 et 7j/7 avec des réactions critiques ne peut que rarement être garantie. À quoi est liée cette évolution?

Les raisons sont en réalité assez évidentes : les attaques deviennent de plus en plus sophistiquées, plus complexes et ont lieu à tout moment, en tout lieu, sur n'importe quel appareil et de différentes manières. À ces menaces très développées s'ajoutent également un manque de transparence et de visibilité, mais aussi une lassitude face aux alarmes et, enfin et surtout, un manque de savoir-faire.

En revanche, afin de développer une stratégie optimale, il faut toujours comparer quatre pierres angulaires d'un concept de sécurité : les spécialistes, le savoir-faire, les technologies et les considérations commerciales associées.

Le cas idéal : ces pierres angulaires sont regroupées et disponibles.

DTS rend cela possible avec le **DTS Cockpit** comme référence en matière de services gérés dans le domaine de la cybersécurité.



CUSTOMER PAINS

- **Avez-vous un aperçu total de vos solutions de sécurité informatique ?**
- **Disposez-vous d'une réelle visibilité et compréhension de votre portfolio de sécurité informatique ?**
- **Pouvez-vous réagir aux urgences en matière de sécurité informatique de manière rapide et ciblée ?**
- **Souhaitez-vous regrouper votre architecture de sécurité sur une plateforme centrale ?**
- **Vous souhaitez « tout d'un coup d'œil » et « 24h/24h » en tant que service géré ?**
- **Vous manquez de ressources et de savoir-faire pour vos propres opérations de sécurité 24h/24 et 7j/7 ?**
- **Vos coûts d'investissement pour une stratégie de sécurité informatique optimale sont trop élevés ?**

Quelle que soit l'ampleur d'une cyberattaque réussie, si elle est détectée trop tard et peut entraîner des dégâts considérables, une interruption des activités commerciales, des demandes de rançon ou un arrêt complet de la production. De plus, les attaquants ont toujours la possibilité de réutiliser les accès et les données, de les endommager ou de lancer des attaques ultérieures.
Les causes d'une cyberattaque sont bien connues : mises à jour non effectuées, manque de sensibilisation et d'expertise en matière de sécurité, pas de politique de sécurité standardisée, pas d'autorité de contrôle, effort de maintenance administrative élevé, manque de ressources, tactiques d'attaque sophistiquées, solutions pour les entreprises de taille moyenne qui ne sont pas négociables et entraînent des coûts d'investissement élevés.

Plus vous utilisez des solutions de sécurité indépendantes, plus il devient difficile de réagir rapidement à une cyberattaque. Mettre en œuvre de la flexibilité dans une architecture de pointe et ajouter une couche de sécurité supplémentaire à celle existante est disproportionnellement coûteux et difficile à coordonner. Les entreprises sont confrontées au défi de savoir comment consolider le nombre de leurs solutions, permettre l'intégration de tiers via des interfaces ou garantir des normes de données uniformes grâce à une stratégie de plateforme globale.

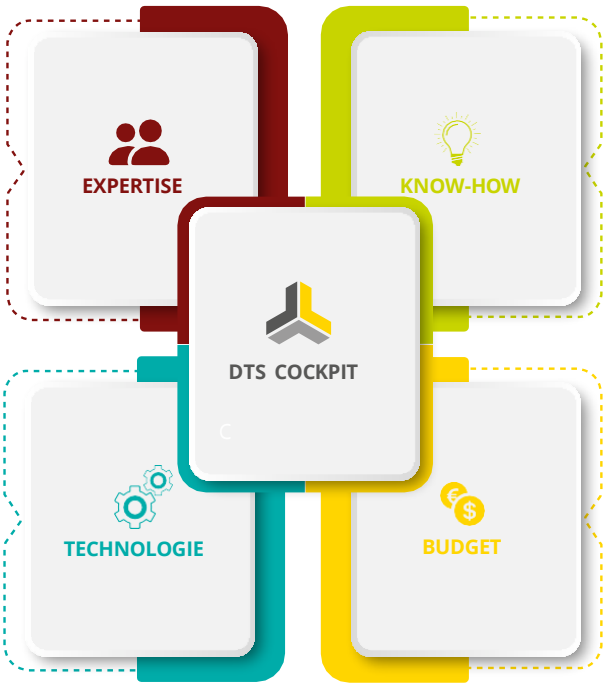
C’est la seule façon pour que la détection et la réponse modernes puissent prendre effet et s’intégrer de manière transparente dans les systèmes existants.

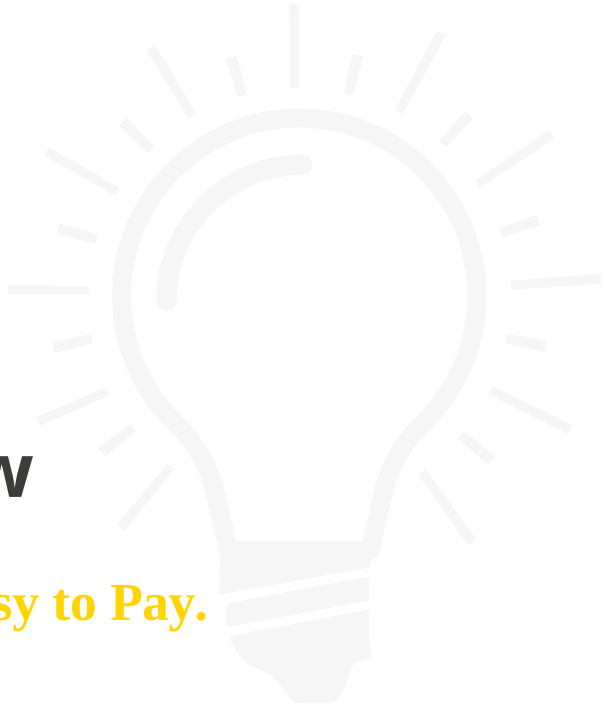
La plupart des organisations ne disposent pas non plus d’une visibilité complète sur leur infrastructure de sécurité et sont confrontées à plus de 10 000 alarmes par jour, ce qui entraîne une lassitude face aux alarmes et des vulnérabilités en matière de sécurité.

Il existe d’excellentes solutions à cela. En commençant par la protection antivirus, les Firewalls de nouvelle génération jusqu'au Zero Trust en tant que concept global. Le renforcement du Firewall humain progresse également à grands pas. Il est important de mieux associer les personnes et la technologie et de garantir ainsi une cybersécurité parfaitement coordonnée pour protéger les utilisateurs et leurs propres données.

Un centre d’opérations de sécurité **(Security Operations Center)** peut également aider ici. Cependant, toutes les entreprises ne peuvent pas mettre en place un centre de contrôle de sécurité central et le faire fonctionner 24 heures sur 24, car cela coûte cher, prend du temps et nécessite un haut niveau de connaissances.

DTS poursuit une approche de solution unique qui va au-delà d'un SOC conventionnel et fournit le **DTS Cockpit** en tant que service géré pour les entreprises de toutes tailles.





Know-How

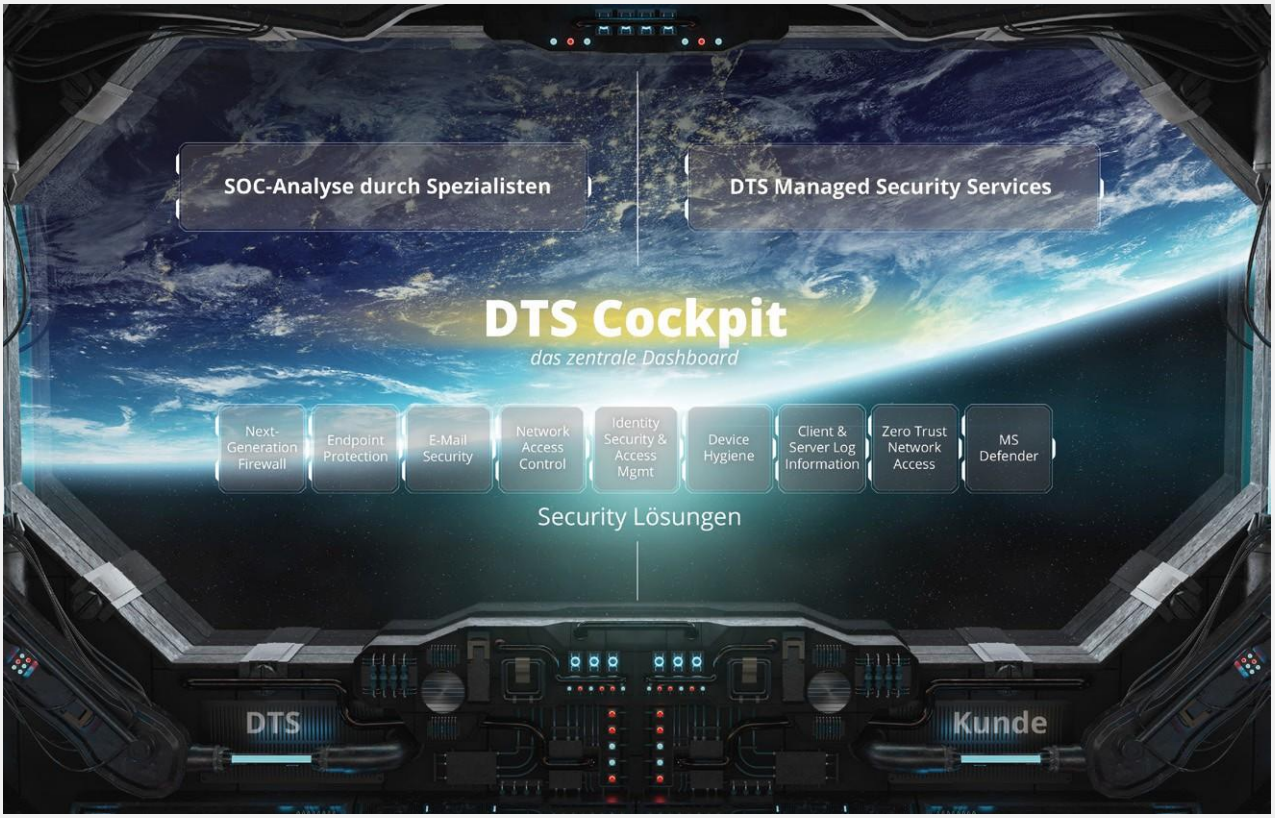
Easy to Use. Easy to Pay.

Les avions ont besoin d'une technologie fonctionnelle, d'un équipage expérimenté et d'un système de contrôle du trafic aérien de niveau supérieur pour remplir leur objectif et garantir le bon fonctionnement des opérations. Mais en fin de compte, tout est réuni dans le cockpit, qui constitue le centre de commande et de direction.

En tant que fabricant de logiciels de cybersécurité, nous avons adopté cette approche et créé quelque chose d'unique. Une combinaison indépendante du fabricant de vos solutions de sécurité dans une plate-forme centrale d'opérations de sécurité 24h/24, 7j/7 et 365j/an! Le DTS Cockpit rend le paysage de sécurité complètement visible et permet des actions et des réactions centralisées et automatisées – surveillées, analysées et contrôlées en permanence par notre centre d'opérations de sécurité (SOC) DTS.

La solution est une stratégie globale qui combine toutes les pierres angulaires d'une véritable stratégie de sécurité et qui reste abordable.

Pionnier dans ce domaine, DTS combine savoir-faire en matière de cybersécurité et technologies de pointe en matière de visibilité, de diagnostic, d'analyse et de défense sur une plateforme spécialement développée « Made in Germany ».



DTS Cockpit: Voir. Comprendre. Agir. Une stratégie globale de cybersécurité.

La clé ici est l'intégration entre fabricants des composants « **Data Collector** » et « **Data Manager** » dans un seul système. Cela permet une réelle transparence et des actions centrales du DTS Cloud.

DTS COCKPIT

DATACENTER
Herford, Muenster

regroupe et orchestre les solutions de sécurité informatique existantes, quel que soit leur fabricant, rend le paysage de sécurité entièrement visible et permet des actions et des réactions centrales, automatisées et directes en tant que Managed Service.

DATA COLLECTOR

collecte diverses sources de journaux, les analyse et génère des alertes.

DATA MANAGER

contrôle et exécute activement des réactions au sein de l'environnement informatique.

Next Level Cyber Security avec DTS Cockpit:

Voir. Comprendre. Agir.

1.

VOIR

Vous ne pouvez pas protéger ce que vous ne pouvez pas voir. Disposez-vous des applications et des services nécessaires pour pouvoir visualiser votre propre paysage informatique ? Et avez-vous toujours une vue d'ensemble et une transparence sur les activités des solutions utilisées ?

2.

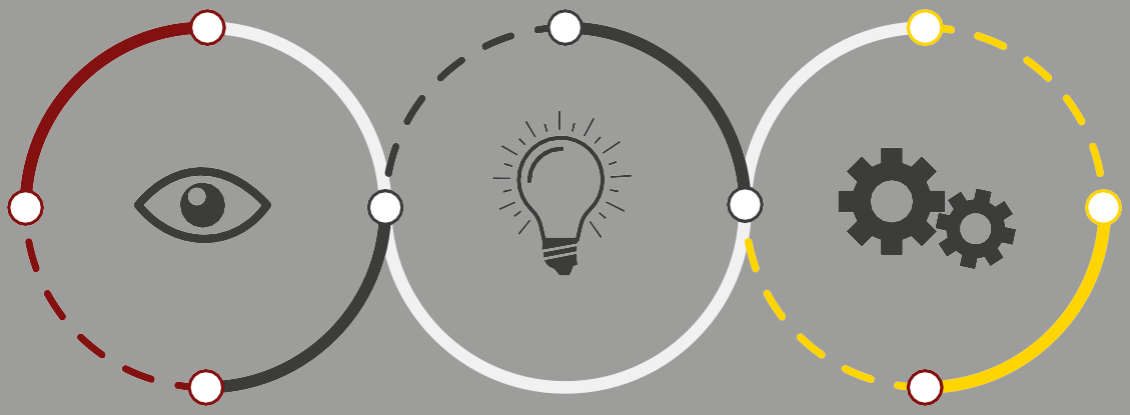
COMPRENDRE

Vous ne trouverez rien si vous ne cherchez pas correctement. Même si vous avez une vue d'ensemble, pouvez-vous repérer les menaces avancées ? Et si vous trouvez quelque chose, pouvez-vous le classer, comprendre et évaluer les connexions ?

3.

AGIR

Agir au lieu de réagir. Êtes-vous capable de réagir assez rapidement aux menaces identifiées avant que ce soit trop tard ?



Voir. Comprendre. Agir.

Expertise

Pénurie de compétences informatiques : comment nous pouvons vous aider.

La chasse aux menaces prend du temps et les cyberattaques sont imprévisibles. Les professionnels de l'informatique qui jonglent avec plusieurs tâches et priorités atteignent rapidement leurs limites et commencent à réagir au lieu d'agir. La planification stratégique est abandonnée et les projets prennent plus de temps que prévu. Le DTS Cockpit vous permet de soulager vos équipes afin qu'elles puissent se concentrer sur les tâches essentielles et ainsi piloter la réussite de votre entreprise.

„Managed Services“ signifie que vous bénéficiez d'un forfait tout-en-un 24h/24 et 7j/7.

Les analystes, administrateurs et experts en cybersécurité hautement qualifiés de DTS offrent une sécurité 24 heures sur 24 avec le Managed Detection & Response 24h/24 et 7j/7. Sur quatre sites européens, les cybermenaces sont activement surveillées et analysées, des rapports sont créés et des mesures immédiates sont prises. Des systèmes informatiques de pointe prennent en charge et fournissent au DTS Cockpit des données importantes pour reconnaître et supprimer les vulnérabilités informatiques, alerter et lancer des mesures défensives, des évaluations de sécurité, la gestion des événements et des journaux, la conformité et bien plus encore.

Vous en bénéficiez de plusieurs manières : nous vous soulageons de l'administration et du fonctionnement 24h/24 et 7j/7, nous fournissons le plus haut niveau de savoir-faire en matière de cybersécurité, prévenons les attaques par des réactions immédiates et vous pouvez vous concentrer sur vos processus commerciaux clés.

EMPLOYÉES

350

14 **LIEUX**

2 **PAYS**

SOC

Athènes, Hamburg, Herford, Thessaloniki

DATACENTER

Herford, Muenster

ISO 27001-Zertifikat

Technologie

Bénéficiez des atouts de chaque composant.

Lors de l'utilisation du DTS Cockpit, toutes les circonstances de l'infrastructure informatique individuelle sont prises en compte. Des centaines d'alertes sont générées chaque jour et les analystes doivent décider quels messages indiquent réellement des menaces. Si une telle analyse de niveau 1 identifie des signes d'attaque, une enquête plus approfondie s'ensuit. Tout cela demande du temps et de l'expertise, et les experts en sécurité sont difficiles à trouver sur le marché du travail. La compétence technique joue donc un rôle important.

DTS Cockpit offre un service unique dans le secteur, regroupe les solutions individuelles, fournit une vue d'ensemble globale et montre ainsi ce qui se passe dans votre réseau. Il s'agit d'une plateforme hybride de SIEM, MDR et SOAR.


Processus continu de protection
Éviter
Comprendre
Collecter
Réagir
Procéder
Analyser
Avertir
Fusionner

ARP-GUARD Network Access Control

Avec **ARP-GUARD Network Access Control**, seuls les appareils autorisés et identifiés de manière unique ont accès au réseau. ARPGUARD enregistre chaque tentative d'accès en temps réel, l'emplacement de la ressource et l'heure de chaque accès au réseau. De cette manière, les anomalies du réseau peuvent être détectées, signalées puis évaluées et corrigées en temps réel grâce à notre gestion intelligente des points faibles et des risques. L'orchestration de l'ensemble de l'environnement réseau s'effectue en un point central et permet la définition d'ensembles de règles spécifiques pour les emplacements distribués. La segmentation en zones VLAN distinctes offre une protection aux zones sensibles. Les appareils sont attribués de manière dynamique et selon des règles.

Composant de base - Cockpit

Le composant de base de la plateforme se compose de plusieurs parties, qui sont toujours livrées sous forme de bundle.

Ceux-ci sont:

- Cloud SIEM pour la connexion et l'analyse des sources de données, y compris 1TB Log Storage.
- **ARP-GUARD Network Access Control** (licences) incluant le Data Manager en tant qu'acteur.
- **Service SOC DTS** 24h/24 et 7j/7 par des analystes pour évaluer en permanence et répondre aux alertes émergentes.

Log Storage

Le **Log Storage** est utilisé pour le stockage des données au sein de la plateforme du **Cockpit**. Les données du journal ne sont supprimées que lorsque cette limite de capacité est atteinte. Cette limite de capacité peut être étendue à volonté. Par conséquent, la période de conservation dépend de la fréquence et du volume des données de journal entrantes. Si davantage de données sont transférées vers le Cockpit, celles-ci ne sont pas supprimées, mais la durée de stockage des données existantes est réduite en conséquence et les données les plus anciennes sont supprimées.

Data Collector

Les Data Collectors sont utilisés pour collecter des données à partir de diverses sources de log. Ces données sont analysées et des alarmes peuvent être générées à partir de celles-ci. Des collecteurs de données existent actuellement pour les composants suivants et sont constamment développés :

- Windows Logs der Endpoints
- Palo Alto Networks Next-Generation Firewalls Checkpoint Firewalls
- FortiNet Firewalls

Data Manager

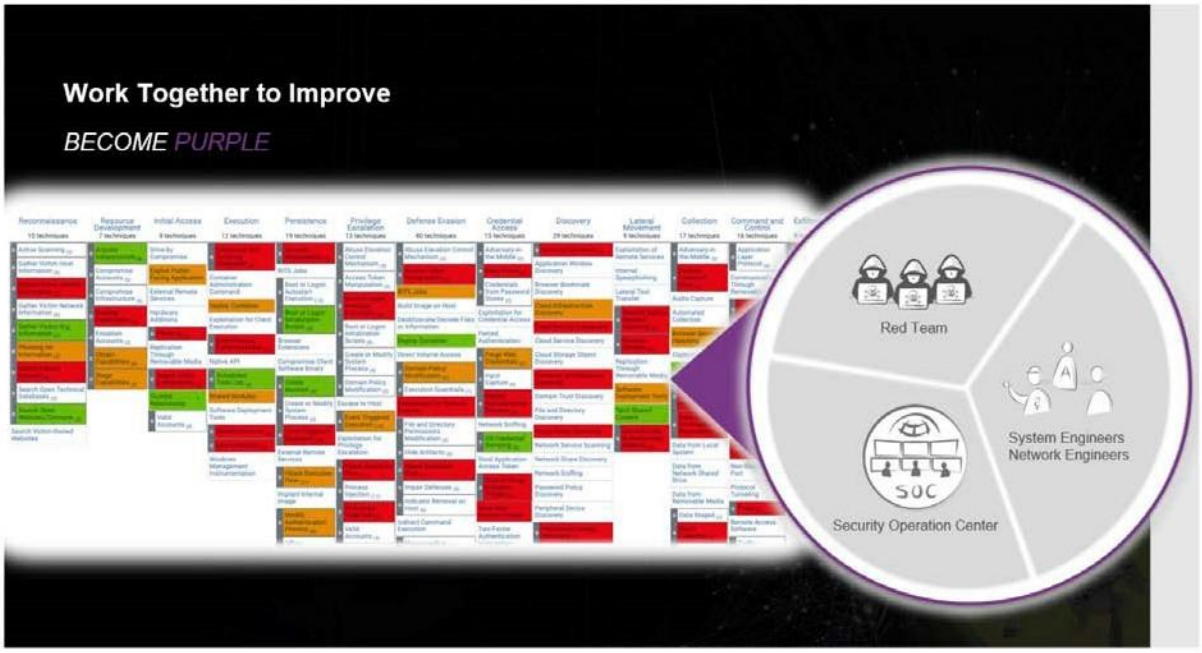
Les Data Managers vont bien au-delà des fonctions du collecteur de données. En plus de collecter des informations sur les données, le Data Manager est principalement utilisé pour contrôler activement les composants connectés et pour effectuer les réactions appropriées au sein de l'environnement client. Les Data Managers existent actuellement pour les composants suivants et sont constamment étendus et bien d'autres sont ajoutés :

- ARP-GUARD Network Access Control (inclus au Cockpit)
- Palo Alto Networks Next-Generation Firewalls
- Palo Alto Networks Cortex XDR
- Proofpoint Targeted Attack Protection (TAP)
- Infinipoint Plattform
- LogRhythm SIEM
- MS Defender

RÉACTIONS POTENTIELLES	DESCRIPTION
Endpoint Network Separation	Permet aux Endpoints enregistrés d'être isolés du réseau client
Endpoint Quarantine	Restreindre l'accès réseau aux Endpoints à l'infrastructure de gestion des Endpoints uniquement.
Endpoint Compliance Status	Définit l'état de conformité d'un appareil dans Device Management. Cela nécessite le Infinipoint Datamanager
Lancer une session interactive sur Endpoint	Permettre aux analystes d'ouvrir un panneau de commande sur Endpoint.
Télécharger des fichiers sur Endpoint	Au cours du processus d'enquête IR, il peut être nécessaire de télécharger des outils pour contenir la violation ou collecter les informations nécessaires.
Supprimer des fichiers sur Endpoint	Suppression des fichiers malveillants sur Endpoint système.
Collecter de fichiers et d'espace disque auprès de Host	Collecter les fichiers et le stockage à partir des systèmes Endpoint

Continuous Assessments

Malgré d'énormes investissements dans les produits et processus de sécurité, les entreprises sont régulièrement piratées. La raison en est souvent un manque de connaissance des techniques d'attaque utilisées par les cybercriminels ou encore des menaces persistantes avancées (**Advanced Persistent Threats**). Afin de s'assurer qu'une entreprise peut résister aux menaces actuelles, il faut comprendre quelles "tactiques, techniques et procédures" (TTP) sont utilisées lors d'une cyberattaque. Grâce à des tests de sécurité continus dans un cycle établi, en utilisant des procédures standardisées telles que "Observer (Observer), Orienter (Orienter), Décider (Décider), Agir (OODA-Loop)"), permettent de prendre en compte l'ensemble de la sécurité organisationnelle. Les possibilités d'attaque, les points faibles et les déficits généraux peuvent être traités régulièrement par l'équipe de cyberdéfense dans le but de réduire en permanence le risque de réussite des cyberattaques.



Pourquoi Continuous Assessments ne sont-ils utiles qu'en combinaison avec le DTS Cockpit ?

Avec Continuous Assessments, vous disposez d'une combinaison unique dans le secteur, qui n'est imbattable et surtout abordable qu'avec le DTS Cockpit. Les tests de sécurité sont intensifiés étape par étape au cours des cycles de test. De Vulnerability Assessment au Penetration Testing en passant par les opérations de l'équipe rouge ou les tests de l'équipe violette, votre entreprise effectue une grande variété de cas de test.
En combinaison avec le DTS Cockpit, les techniques d'attaque les plus modernes peuvent être immédiatement converties en mesures de détection ou de prévention appropriées. Toutes les informations sont corrélées et sont disponibles pour toutes les personnes impliquées afin d'optimiser la sécurité de l'ensemble de l'entreprise à long terme.

DTS Cockpit pose les bases du Purple Teaming, qui améliore non seulement la cybersécurité, mais également l'efficacité du travail entre équipes.

Dans le même temps, des contrôles réguliers garantissent que les mesures de sécurité fonctionnent comme prévu. En outre, de nouvelles techniques d'attaque peuvent être mises en place rapidement au cours des cycles de test afin de réduire les angles morts grâce à des contrôles de sécurité ponctuels. Utilisez le point de vue de l'attaquant pour protéger votre entreprise contre des menaces réalistes et garder le contrôle des mesures de cybersécurité. De cette façon, vous pouvez identifier immédiatement vos lacunes et gagner ainsi en transparence. Le paysage informatique de l'entreprise fait l'objet d'une analyse continue. Nous vous donnons des recommandations claires, établissons une feuille de route pour vous et en même temps votre niveau de sécurité est considérablement augmenté.

Où positionner le DTS Cockpit ?

XDR & MDR (Extended & Managed Detection and Response)

- XDR: Collecter, corréler et analyser les données provenant de sources d'informations ciblées telles que les Endpoint, les Cloud-Workloads, les réseaux et la messagerie électronique via des outils d'automatisation et d'IA.
- Les services MDR combinent analyses et renseignements sur les menaces avec une expertise humaine.
- Une plateforme de sécurité XDR comme Contrôle de sécurité 24h/24 et 7j/7 pour les entreprises qui ne disposent pas de leur propre Security Operations Center.

Comparer Cockpit

- Connection XDR Prevent & Pro
- Possibilité d'intégrer plusieurs sources provenant de nombreux fournisseurs différents
- Le Cockpit est nettement plus rentable

SIEM (Security Information and Event Management)

- Surveillance et analyse en temps réel des événements, ainsi que suivi et journalisation des données de sécurité dans une vaste base de données
- Système de coordination des données pour gérer les menaces en constante évolution

Comparer Cockpit

- Possibilité d'action/réaction : Intervention active des Data Managers & de nos analystes
- Cockpit connecte moins de sources, mais des sources avec un contenu précieux
- Le Cockpit est nettement plus rentable

SOAR (Security Orchestration Automation and Response)

- Kompatible Programme, die aus unterschiedlichsten Quellen Daten über Sicherheitsbedrohungen einsammeln
- Ermöglicht automatische Reaktion ohne menschliche Eingriffe auf bestimmte Sicherheitsereignisse
- SIEM & SOAR Verbindung: Markt wird voraussichtlich für die beiden Produktlinien zusammenwachsen -> insbesondere wenn SIEM-Anbieter beginnen ihre Lösungen um SOAR-Funktionen zu erweitern

Comparer Cockpit

- Intervention après consultation et avec accompagnement humain (analystes SOC) -> peut couvrir plus de scénarios
- Le Cockpit est beaucoup plus rentable

Cyber Security Mesh

Gartner définit le maillage de cybersécurité comme « une approche conceptuelle moderne de l'architecture de sécurité qui permet aux entreprises distribuées de déployer et d'étendre la sécurité là où elle est

DTS Cockpit

- Préparer l'avenir : votre entreprise peut réagir aux futurs risques de sécurité en sélectionnant et en intégrant spécifiquement nos technologies et services pour la cybersécurité.
- Combler les lacunes : grâce aux normes de sécurité actuelles et nouvelles, vous pouvez combler les lacunes de sécurité dues aux vulnérabilités et aux vulnérabilités de diverses solutions.
- Experts en cybersécurité : les solutions de sécurité actuelles sont souvent une composition de plusieurs solutions individuelles qui apportent certains avantages et fonctionnalités. Cockpit prend en compte cette modularité et laisse place à des solutions flexibles et évolutives qui s'adaptent aux évolutions.

USP Cockpit

- Cockpit est directement un service et non un logiciel indépendant qui doit être utilisé par vous-même et est plus qu'une technologie utilisée.
- Ne pas être classé dans une seule catégorie -> Cockpit combine des fonctions essentielles de tous les domaines (XDR, SIEM, SOAR) afin que nous puissions fournir efficacement des services MDR.
- Plus étendu que XDR (entre SIEM et XDR), mais beaucoup plus granulaire dans les données qu'un XDR collecte également, combinées à l'orchestration et à la réponse de SOAR.

Budget

Des entreprises de taille moyenne pour les entreprises de taille moyenne

Depuis longtemps, il existe une tendance à créer votre propre centre d'opérations de sécurité (SOC). Des analystes de sécurité y travaillent, surveillant et évaluant les messages d'avertissement 24 heures sur 24.

Mais gérer un SOC coûte cher. Il n’est donc généralement pas intéressant pour les entreprises de taille moyenne de gérer leur propre SOC. Avec le DTS Cockpit, nous mettons à votre disposition la technologie, analysons les alarmes et assurons en permanence leur fonctionnement en toute sécurité. En tant que Managed Service, vous recevez un relevé mensuel avec une structure de coûts claire.

> **VOUS BÉNÉFICIEZ DOUBLE :**
> **FINANCIÈREMENT ET DE L'EXPERTISE DES SPÉCIALISTES.**

„D'ici 2024, les organisations adoptant une architecture maillée de cybersécurité pour intégrer des outils de sécurité et fonctionner comme un écosystème collaboratif réduiront l'impact financier des incidents de sécurité de 90% en moyenne."

Gartner de : Principales tendances technologiques stratégiques

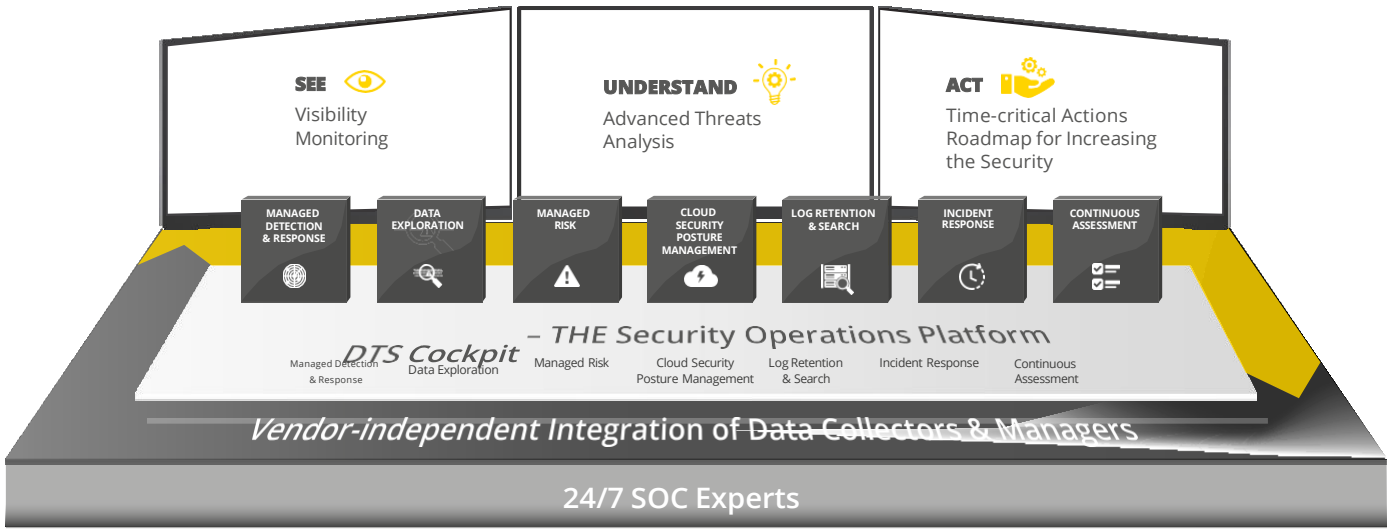
DTS Cockpit

Vos avantages

Une Stratégie globale de cybersécurité avec DTS Cockpit

- Combinaison révolutionnaire de plateforme et de service 24h/24 et 7j/7
- 40 ans de savoir-faire expert, pionnier SOC sur 4 sites européens, solutions globales pour 1.400 clients dans le domaine des Managed Services
- Solution abordable pour les entreprises de taille moyenne avec une structure de coûts claire
- Managed Service fourni à partir du cloud allemand DTS certifié
- Central All-in-One Security Operations Platform
- Orchestration de toutes les solutions de sécurité courantes
- Visibilité complète et base de données uniforme
- Transparence totale du paysage de la sécurité informatique
- Chasse aux menaces proactive et continue
- Actions et réactions directes et automatisées
- Rapport d'incident avec des recommandations d'action spécifiques
- Identification, analyse et réponse aux attaques 24h/24 et 7j/7 par les experts en opérations de sécurité du DTS SOC
- Inclut notre ARP-GUARD NAC spécialement développé pour une visibilité, un contrôle et une réaction maximum
- Technologies de pointe telles que SIEM, XDR, SOAR,etc.
- Accès sécurisé avec DTS Identity + Cybersécurité "Made in Germany"
- Composant essentiel d'une architecture de sécurité cohérente
- Service global d'un seul et même fournisseur
- Une plateforme pour tous les rapports
- Gestion continue des risques
- Détection des attaques en temps réel
- Un soulagement pour votre IT Department
- Relation client de confiance et fidélisation avec un seul interlocuteur
- Flexible : Nous nous adaptons à vous, et non l'inverse !
- Add-On: Intégration de Continuous Assessments - valeur ajoutée extraordinaire pour trouver des vulnérabilités et recevoir des recommandations d'actions pour combler les failles de sécurité et augmenter le niveau de sécurité.

Ce qui rend DTS unique, c'est la combinaison d'experts hautement qualifiés et de technologies de pointe. Ensemble, ils constituent la base de notre Security Operations Center, qui nous permet de protéger nos clients.



Easy to Use & Easy to Pay
All-in-One Platform & All-in-One Service
From Mid-sized for Mid-sized Companies

DTS Cockpit convient aux entreprises de toutes tailles qui utilisent plusieurs solutions de sécurité informatique, souhaitent rendre leur paysage/infrastructure informatique existant plus transparent et regrouper leur architecture de sécurité sur une plate-forme centrale, 24 heures sur 24 en tant que Managed Service avec l'expertise TOP de notre SOC 24h/24 et 7j/7.

L'équipe hautement qualifiée de DTS SOC est présente à tout moment. Il combine la détection automatique des attaques, la surveillance active par des experts en cybersécurité, la détection rapide d'éventuelles cyberattaques et la mise en place en temps opportun de mesures adéquates. Le DTS Cockpit offre un avantage unique : notre Data Manager. Cela permet une réaction active et directe à votre paysage de sécurité informatique.

Nous offrons une cybersécurité fiable et abordable 24 heures sur 24, 7 jours sur 7, 365 jours par an, avec un petit nombre d'employés, une technologie de pointe et un accès à une expertise complète. Nous vous soulageons considérablement afin que vous puissiez vous concentrer sur votre cœur de métier.

Montez dans le Cockpit avec nous et attendez-vous à un vol passionnant!

„Attackers don’t think in silos. Organizations do.” Gartner

Cette déclaration de Gartner montre où réside souvent le point faible de la stratégie de sécurité d'une entreprise. De nombreuses solutions individuelles de pointe sont utilisées sans vision globale ni synergies. **C’est exactement là qu’intervient Cockpit** : parce que les solutions d’architecture maillée de cybersécurité qui combinent des outils de sécurité et fonctionnent comme un écosystème collaboratif n’ont jusqu’à présent été utilisées qu’avec des solutions d’entreprise. Mais au lieu de fournir des logiciels exigeant une maintenance élevée qu'un service informatique très occupé doit prendre en charge, notre approche s'appuie sur nos nombreuses années d'expérience dans et pour les entreprises de taille moyenne.

Conformément à la déclaration de Gartner, nous avons développé notre Security Information & Operation Service Cockpit 24h/24 et 7j/7 de telle manière qu'il s'agit non seulement d'une architecture maillée de cybersécurité unique, mais également conçue pour être commercialement attrayante. Grâce aux coûts transparents et au fait qu'il n'y a pas de coûts d'investissement initiaux pour des solutions de sécurité spécifiques, chaque client peut composer son paysage système en fonction de ses besoins individuels (le meilleur de sa catégorie pour chacun). Avec notre service, nous prenons directement en charge la prise en charge et vous proposons une solution globale qui voit votre environnement 24h/24 et 7j/7. comprend. et agit si nécessaire.

Anja Kuhn, *Manager Corporate Strategy and Development*

En moyenne, les entreprises utilisent plus de 37 produits et outils différents pour contrer les cyberrisques actuels. Il arrive souvent que chaque solution forme son propre silo d’informations. Or, cela s’avère fatal, surtout pour les attaques complexes et ciblées ! Avec le DTS Cockpit, nous offrons non seulement à nos clients la possibilité de regrouper toutes les informations de manière centralisée, mais nous allons également plus loin : nos analystes SOC suivent également à tout moment les alarmes qui se produisent et agissent dans les plus brefs délais en cas d'alarme. Afin de repousser avec succès les cyberattaques, nous travaillons comme des hackers – 24 heures sur 24 !

Malte Örmann, *Sales Director*

2023

2022

202
QUA

Cockpit Release

Customer Overview
Multiple Alarm Management

Datamanager Defender

Alarm engine 3x faster

Accounting

Set of rules per customer

Assists alarm drill down

Log Health Check

Extended Graph. analysis

Continuous Assessment

MSP Integratio

On-Prem Auto U

Au

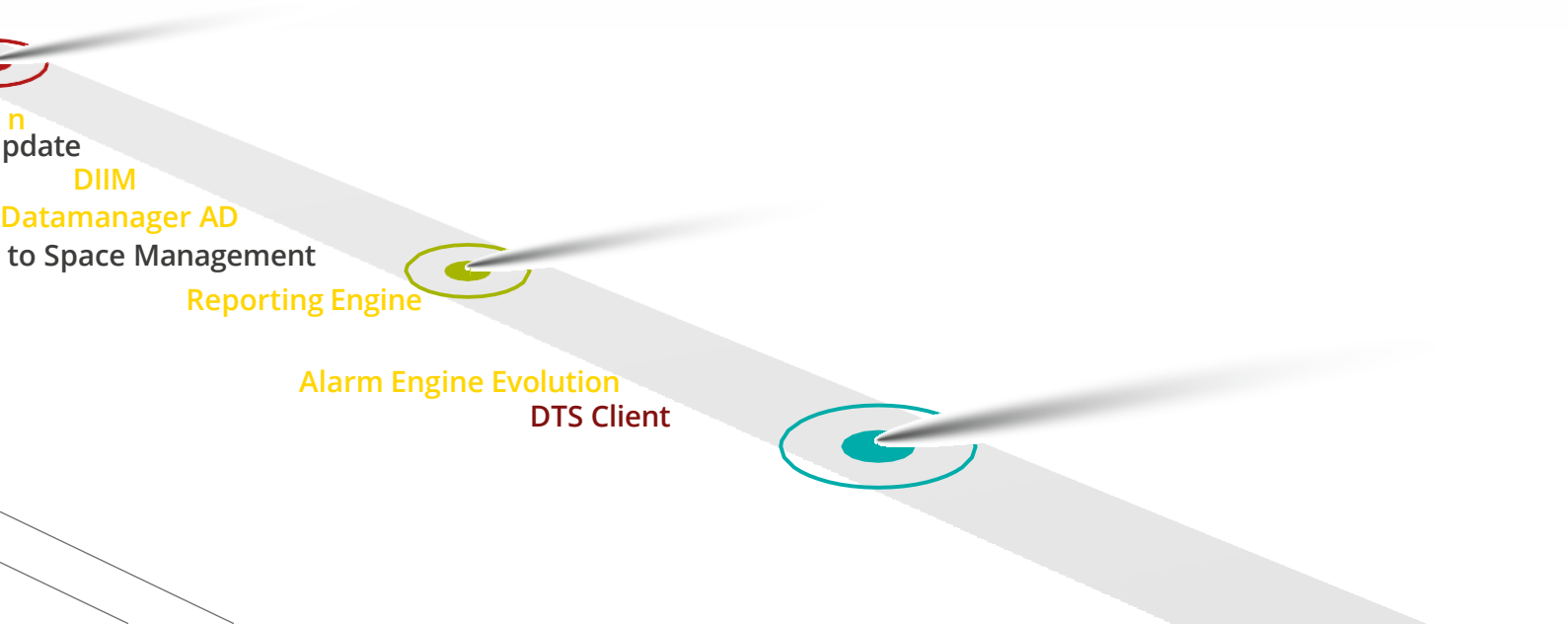
Ce n'est pas tout.
Cockpit est considérablement étendu et développé de manière intensive.
Soyez curieux!

AJUSTEMENTS
EXTENSIONS
ÉTAPES

2023
QUART 3

3
RT 2

2024



DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de