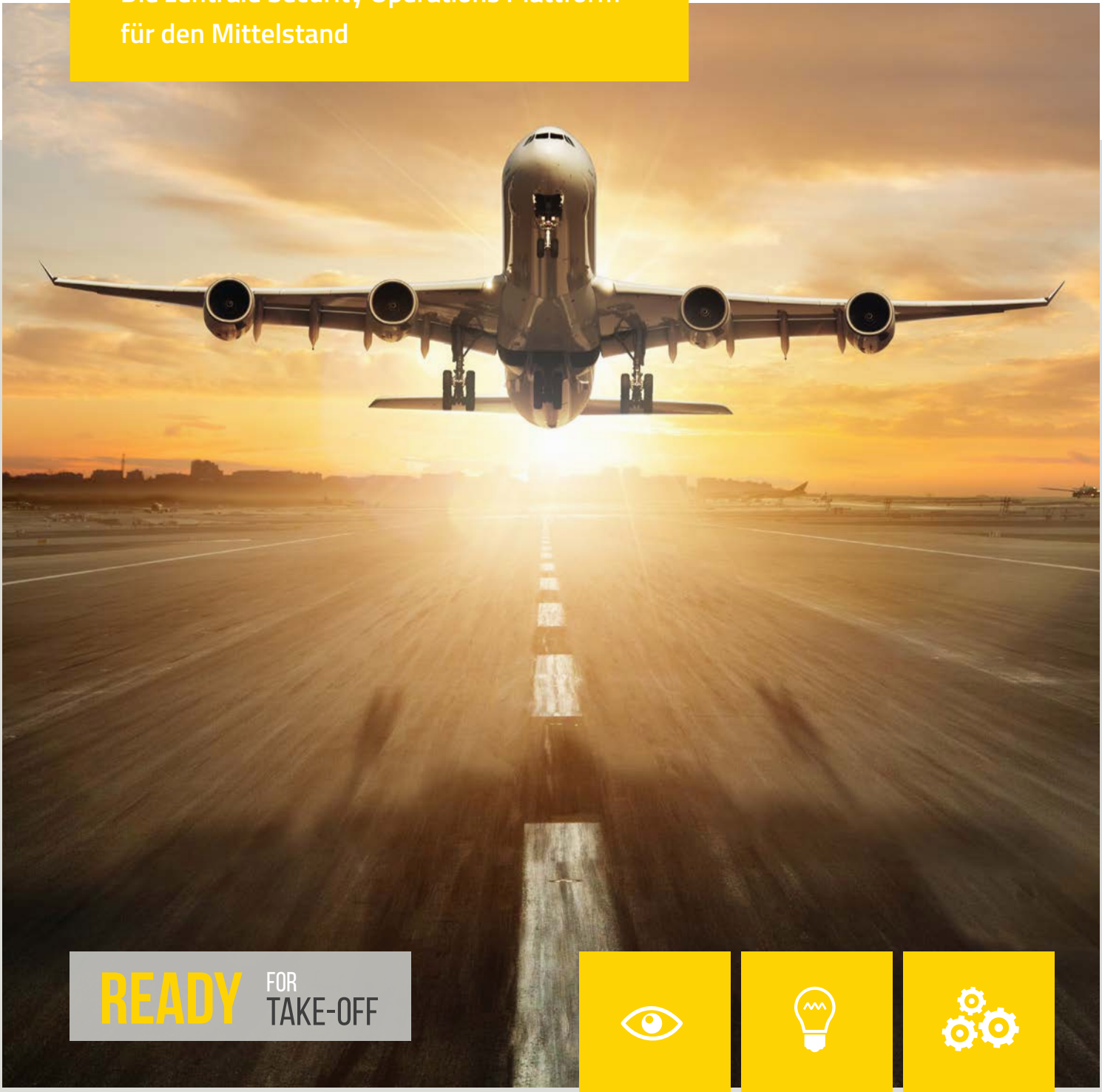
Sehen. Verstehen. Agieren.

00

DTS COCKPIT

Die zentrale Security Operations Plattform für den Mittelstand



READY FOR TAKE-OFF

SEHEN

VERSTEHEN

AGIEREN

WHITEPAPER
JULI 23

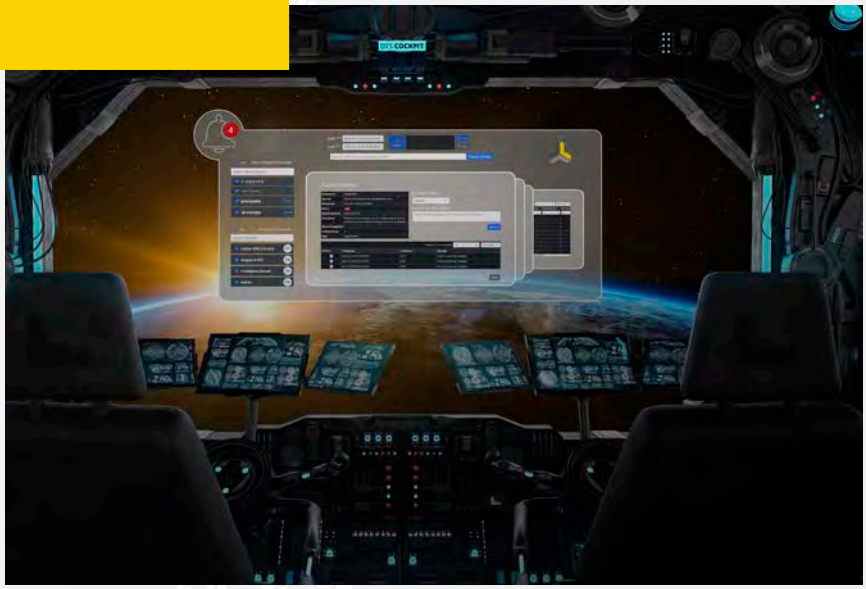
CONTENTS

03

Sehen. Verstehen. Agieren.

DTS COCKPIT SERVICE GUIDE

Die zentrale Security Operations Plattform für den Mittelstand



UNSERE MISSION

Mit unserer Security Operations Plattform helfen wir Unternehmen, Cyberrisiken abzuwehren, Ihr Unternehmen proaktiv zu schützen und Ihre Sicherheitslage kontinuierlich zu verbessern.

In Deutschland werden jährlich mehr als 8,5 Milliarden Euro für die IT-Sicherheit ausgegeben. Es gibt unzählige Sicherheitslösungen und -dienstleistungen auf dem Markt und nahezu jedes Unternehmen setzt nach dem „Best-of-Breed-Ansatz" verschiedene Produkte ein. Trotzdem nimmt die Zahl der Cyberangriffe stetig zu und insbesondere eine 24/7-Sicherheit mit zeitkritischer Reaktion wird nur selten gewährleistet. Was sind die Gründe für diese Entwicklung?

Die Gründe liegen auf der Hand: Die Angriffe werden immer ausgefeilter und vielschichtiger, erfolgen zu jeder Zeit, auf allen Geräten und auf unterschiedlichste Art und Weise.
Weitere Bedrohungen sind die mangelnde Transparenz und Alarmbereitschaft sowie das fehlende Know-how.

We see. We do. Safe!

OUR STATEMENT!

KAI MALLMANN
CEO

„Seit über 20 Jahren profitieren unsere Kunden von unseren eigens entwickelten Softwarelösungen und -plattformen. Mit DTS Cockpit haben wir nun eine revolutionäre, bezahlbare Plattform entwickelt, mit der wir in der Lage sind, einen eigenständigen Weg zu gehen und den klassischen Markt zu durchbrechen – weg vom klassischen Reseller-Markt, hin zu einer ganzheitlichen Plattform. DTS Cockpit gibt Ihnen 24/7 volle Transparenz über Ihre IT-Sicherheitslage. Die einfache Usability kombiniert mit unseren innovativen und bezahlbaren Managed Services für den Mittelstand, machen die Plattform einzigartig. Wir sind Ihr Ansprechpartner von Anfang an und entlasten Ihre IT-Abteilung. Als Softwarehersteller kombinieren wir eigene Lösungen und Plattformen mit Expertise, klaren Lösungsansätzen, spezifischen Anforderungen und Bedürfnissen."

„BIS 2024 WERDEN UNTERNEHMEN, DIE EINE CYBERSECURITY-MESH-ARCHITEKTUR EINFÜHREN, UM SICHERHEITSTOOLS ZU INTEGRIEREN UND ALS KOLLABORATIVES ÖKOSYSTEM ZU ARBEITEN, DIE FINANZIELLEN AUSWIRKUNGEN EINZELNER SICHERHEITSVORFÄLLE UM DURCHSCHNITTLICH 90% REDUZIEREN."

Gartner aus: Top Strategic Technology Trends

HAND AUFS HERZ

HABEN SIE DEN ÜBERBLICK ÜBER IHRE IT-SICHERHEITSLÖSUNGEN UND WIRKLICHE SICHTBARKEIT IN IHRER IT-LANDSCHAFT?

VERFÜGEN SIE ÜBER EIN ECHTES VERSTÄNDNIS BZGL. IHRER IT-SICHERHEITSLAGE?

KÖNNEN SIE ZEITKRITISCH UND ZIELGERICHTET AUF IT-SECURITY-NOTFÄLLE REAGIEREN?

IHNEN FEHLEN DIE RESSOURCEN UND DAS FÜHRENDE KNOW-HOW FÜR EIN EIGENES 24/7 SECURITY OPERATIONS?

Um dagegen eine optimale Strategie zu entwickeln, müssen die vier Eckpfeiler eines Sicherheitskonzepts stets gegenübergestellt werden: Fachkräfte, Know-how, Technologien und die damit verbundene wirtschaftliche Betrachtung.

Im Idealfall sind diese Eckpfeiler gebündelt verfügbar. Wie das geht? Die DTS macht es möglich, mit dem DTS Cockpit als den Managed-Service-Meilenstein im Bereich Cyber Security

MALTE ÖRMANN
Sales Director

"Unternehmen setzen durchschnittlich mehr als 37 unterschiedliche Produkte und Tools ein, um den aktuellen Cyber-Risiken entgegenzuwirken. Dabei kommt es häufig vor, dass jede Lösung ein eigenes Informationssilo bildet. Gerade für komplexe und zielgerichtete Angriffe ist dies jedoch fatal! Mit dem DTS Cockpit bieten wir unseren Kunden nicht nur die Möglichkeit alle Informationen zentral zu bündeln, sondern gehen direkt zwei Schritte weiter: Unsere SOC Analysten behalten auch jederzeit den Überblick über auftretende Alarme und agieren in kürzester Zeit wenn Handlungsbedarf besteht. Um Cyberangriffe erfolgreich abzuwehren, arbeiten wir wie Hacker - rund um die Uhr!"

DTS Cockpit

FACHKRÄFTE | TECHNOLOGIE | KNOW-HOW | BUDGET

UNSER KNOW-HOW. IHR VORSPRUNG. IT-KNOW-HOW SEIT ÜBER 40 JAHREN.

Egal, welches Ausmaß ein erfolgreich durchgeführter Cyberangriff aufweist, er wird zu spät erkannt, es entstehen massive Schäden, eine Unterbrechung der Geschäftstätigkeit, Lösegeldforderungen oder der komplette Produktionsstopp können die Folgen sein. Hinzu kommt, dass Angreifer stets die Möglichkeit haben, Zugänge und Daten erneut zu nutzen, zu beschädigen oder Folgeangriffe zu starten.

Die Ursachen eines Cyberangriffs sind hinreichend bekannt: Nicht durchgeführte Updates, fehlende Security Awareness und Expertise, keine standardisierte Sicherheitspolitik und Kontrollinstanz, hoher administrativer Pflegeaufwand, fehlende Ressourcen sowie Lösungen, die für den Mittelstand oftmals wirtschaftlich nicht händelbar sind und hohe Investitionskosten mit sich bringen.
Dezentrale „Best of Breed" Insellösungen erfüllen diese Anforderungen nicht.

Je mehr voneinander unabhängige Security-Lösungen man einsetzt, desto schwieriger wird es auf einen Cyberangriff zu reagieren. Somit stehen Unternehmen vor der Herausforderung, die Anzahl ihrer Lösungen zu konsolidieren, eine Drittanbieter-Integration über Schnittstellen zu ermöglichen oder einheitliche Datenstandards durch eine übergreifende Plattform-Strategie zu gewährleisten. Nur so kann im Anschluss auch eine moderne Detection & Response greifen und sich nahtlos in die bestehenden Systeme einfügen.

Zudem haben die meisten Unternehmen keinen vollständigen Überblick über ihre Sicherheitsinfrastruktur und sind mit mehr als 10.000 Alarmen pro Tag konfrontiert, was zu Alarmmüdigkeit und Sicherheitslücken führt.

Dabei gibt es hervorragende Lösungen. Von Antivirenschutz, Next-Generation-Firewalls bis hin zu Zero Trust als Gesamtkonzept. Auch die Stärkung der Human Firewall schreitet mit großen Schritten voran. Es gilt, Mensch und Technologie enger zu verzahnen und somit eine optimale Cyber Security zur Verfügung zu stellen, um Anwender und die eigenen Daten zu schützen.

Ein Security Operations Center (SOC) kann hier ebenfalls Abhilfe schaffen. Doch nicht jedes Unternehmen kann sich einen zentralen Sicherheitsleitstand aufbauen und rund um die Uhr betreiben, da dies teuer und zeitaufwendig ist sowie ein hohes Maß an Wissen voraussetzt.

DTS verfolgt hier, über ein eigenes herkömmliches SOC hinaus, einen einzigartigen Lösungsansatz und stellt für Unternehmen jeder Größe das DTS Cockpit als Managed Service bereit. Sehen, Verstehen und Agieren als „All in One" - nur so funktioniert modernste Cyber Security. Weg vom passiven, dezentralen Daten sammeln, hin zur aktiven, zentralen Sichtbarkeit und Steuerung. Mit uns ALLES SEHEN, VERSTEHEN und WIRKLICH AGIEREN – Vom Mittelstand für den Mittelstand und „Made by DTS"!

07

True Experts detect Everything

KNOW-HOW

Ein Flugzeug benötigt funktionierende Technologien, eine erfahrene Crew und eine übergeordnete Flugsicherung, um seinen Zweck zu erfüllen und den reibungslosen Ablauf sicherzustellen. Schlussendlich läuft jedoch alles im Cockpit als Kontroll- und Steuerungszentrale zusammen.

Diesen Ansatz haben wir als langjährig erfahrener IT-Security-Softwarehersteller aufgegriffen und etwas Einzigartiges entwickelt: ein herstellerunabhängiger Zusammenschluss von Sicherheitslösungen zu einer zentralen 24/7/365 Security Operations Plattform! Das DTS Cockpit macht die Sicherheitslandschaft vollständig sichtbar und ermöglicht zentrale, automatisierte Aktionen bzw. Reaktionen - permanent überwacht, analysiert und gesteuert durch unser eigenes DTS Security Operations Center (SOC).

Die Lösung ist eine ganzheitliche Strategie, die alle elementaren Eckpfeiler eines echten Sicherheitskonzept vereint und dennoch bezahlbar ist.

Als Pionier auf diesem Gebiet kombiniert DTS Cyber Security Know-how sowie modernste Technologien für Sichtbarkeit, Diagnose, Analyse und Verteidigung übersichtlich auf einer eigens entwickelten Plattform „Made in Germany".

Der Schlüssel ist hierbei die herstellerübergreifende Einbindung der Komponenten „Data Collector" und „Data Manager" in einem System. Mit der Verknüpfung dieser Aspekte haben wir eine kollaborative IT-Security-Architektur entwickelt. Das Ergebnis ist Datensammlung und Management auf einer zentralen Plattform, mit einheitlicher Datenbasis, Orchestrierung und Steuerung. Dies ermöglicht eine echte Transparenz und schnelle, zentrale Aktionen und Reaktionen – aus der deutschen, zertifizierten DTS Cloud.

DTS COCKPIT

DATACENTER
Herford, Münster

bündelt und orchestriert herstellerunabhängig die vorhandenen IT-Security-Lösungen, macht die Sicherheitslandschaft vollständig sichtbar und ermöglicht zentrale, automatisierte, direkte Aktionen bzw. Reaktionen als Managed Service

DATACOLLECTOR

sammelt verschiedene Log-Quellen, analysiert diese und generiert Alarme

DATAMANAGER

steuert aktiv und führt Reaktionen innerhalb der IT-Umgebung aus

NEXT LEVEL CYBER SECURITY MIT DTS COCKPIT

01 SEHEN

Man kann nichts schützen, was man nicht sieht.

Haben Sie die notwendigen Anwendungen und Services, um Ihre eigene IT-Landschaft sehen zu können? Haben Sie stets einen Überblick sowie Transparenz über die Aktivitäten der eingesetzten Lösungen?

02 VERSTEHEN

Man findet nichts, wenn man nicht richtig sucht.

Obwohl Sie einen Überblick haben, können Sie hochentwickelte Bedrohungen entdecken? Und falls Sie etwas finden, können Sie es klassifizieren, die Zusammenhänge verstehen und bewerten?

03 AGIEREN

Agieren, statt zu reagieren.

Meist ist es zu spät, bis der Alarm Ihre Rufbereitschaft erreicht. Sind sie in der Lage, auf identifizierte Bedrohungen schnell und angemessen zu reagieren?

SEHEN: VOLLSTÄNDIGE TRANSPARENZ & EINHEITLICHE DATENBASIS

VERSTEHEN: PROAKTIVE BEDROHUNGSIDENTIFIKATION & -ANALYSE DURCH DTS SOC

AGIEREN: ZEITKRITISCHE, DIREKTE AKTIONEN DURCH INTEGRIERTE DATA MANAGER & DTS SOC

VOM MITTELSTAND FÜR DEN MITTEL-STAND

09

Sicher mit Managed Services sparen

BUDGET

Lange Zeit lag es im Trend ein eigenes Security Operations Center (SOC) aufzubauen. Dort arbeiten Security-Analysten, welche Warnmeldungen rund um die Uhr überwachen und auswerten. Doch ein SOC zu betreiben ist teuer. Für mittelständische Unternehmen lohnt es sich daher in der Regel nicht, ein eigenes SOC zu unterhalten. Beim DTS Cockpit stellen wir Ihnen die Technologie bereit, analysieren die Alarme und kümmern uns kontinuierlich um ihren sicheren Betrieb. Als Managed Service erhalten Sie eine monatliche Abrechnung mit einer klaren Kostenstruktur.

PROFITIEREN SIE DOPPELT:

FINANZIELL UND VOM EXPERTEN-WISSEN DER SPEZIALISTEN

DTS Cockpit

Sehen. Verstehen. Agieren. Eine ganzheitliche Cyber-Security-Strategie.

Easy to Use. Easy to Pay.

FACH-KRÄFTE

10

IT-FACHKRÄFTEMANGEL - SO HELFEN WIR IHNEN

Bedrohungssuche ist zeitaufwendig und Cyberangriffe sind unvorhersehbar. IT-Experten, die mit Aufgaben und Prioritäten jonglieren, stoßen schnell an ihre Grenzen und beginnen zu reagieren, statt zu agieren. Die strategische Planung bleibt dabei auf der Strecke und Projekte dauern länger als geplant. Das DTS Cockpit ermöglicht es Ihnen, Ihre Teams zu entlasten, um sich auf die wesentlichen Aufgaben zu konzentrieren und somit Ihren Geschäftserfolg voranzutreiben.

„MANAGED SERVICES" BEDEUTET, DASS SIE EIN 24/7-ALL-IN-ONE-PAKET ERHALTEN

Die hochqualifizierten Analysten, Administratoren und Cyber-Security-Experten der DTS bieten mit dem 24/7 Managed Detection & Response Service rund um die Uhr Sicherheit. An vier europäischen Standorten werden Cyberbedrohungen aktiv überwacht und analysiert, Reports erstellt und Sofortmaßnahmen ergriffen. Hochmoderne IT-Systeme unterstützen und liefern dem DTS Cockpit wichtige Daten zur Erkennung und Entfernung von IT-Schwachstellen, Alarmierung & Einleiten von Abwehrmaßnahmen, Security Assessments, Ereignis- und Protokollmanagement, Compliance-Einhaltung u.v.m.

Davon profitieren Sie gleich mehrfach: Wir entlasten Sie bei der Administration sowie beim 24/7 Betrieb, stellen Ihnen höchstes Cyber Security Know-how zur Verfügung, unterbinden Angriffe durch umgehende Reaktionen und Sie können sich auf Ihre Kerngeschäftsprozesse konzentrieren.

14 STANDORTE

2 LÄNDER

400 MITARBEITENDE

4 SOC
Athen, Hamburg, Herford, Thessaloniki

2 DATACENTER
Herford, Münster

+1400 MANAGED SERVICES KUNDEN

+20 JAHRE SOFTWARE BY DTS

Thinking beyond technology

TECHNO-LOGIE

01 SAMMELN

Alle Sicherheitsereignisse werden gesammelt, ausgewertet und für einen bestimmten Zeitraum gespeichert, um zukünftige Analysen zu ermöglichen.

02 VERARBEITEN

Potenzielle Vorfälle, die durch die automatische Analyse-Engine identifiziert wurden, sind sofort Gegenstand weiterer Untersuchungen durch unsere DTS SOC-Analysten. Andere Sicherheitsereignisse, die erfasst, aber nicht von der automatischen Analyse-Engine identifiziert wurden, werden für zukünftige Untersuchungen aufbewahrt.

03 ZUSAMMENFÜHREN

Überwachen und Analysieren der Endpunktumgebung des Kunden an einem zentralen Punkt (Cockpit). Alle gesammelten Daten der eingebundenen Lösungen werden hier zentral zusammengeführt.

04 ANALYSIEREN

Das DTS SOC-Team hat Verfahren zur Untersuchung von Vorfällen eingeführt, die eine einheitliche Methodik zur Analyse von Vorfällen gewährleisten.

05 WARNEN

Die Benachrichtigungspräferenzen des Kunden werden vorab festgelegt (d.h. Benachrichtigungen nur bei bestätigten Ereignissen oder bei allen verdächtigen Alarmen).

Kategorien von Störungsmeldungen:

- *Sicherheitsalarm wird durch automatische Analyse als verdächtig eingestuft*
- *Bedrohungsanalytiker identifiziert einen potenziellen Vorfall auf der Grundlage einer ersten Untersuchung*
- *Aufgrund weiterer Untersuchungen durch den Bedrohungsanalytiker wird ein Vorfall, eingestuft und an den Incident Response Analyst (IR) weitergeleitet*

Falls erforderlich, bestätigt der IR-Analyst, dass es sich bei dem Vorfall um eine Sicherheitsverletzung oder eine Malware-Aktivität handelt, und führt IR-Protokolle ein.

06 REAGIEREN

- *Analyst führt die vorab genehmigten Reaktionsmaßnahmen durch*
- *Passendes Protokoll wird während des Einrichtens erstellt, um die Berechtigung für die von den Analysten genehmigten Reaktionsmaßnahmen zu dokumentieren*
- *Eindeutige Bedrohungen werden sofort beseitigt*

07 VERSTEHEN

Die gesamte Systemlandschaft wird erfasst. So werden Zusammenhänge verstanden.

08 VERMEIDEN

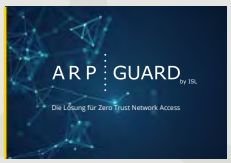
Aus den Ereignissen lernen: Durch die kontinuierliche Verarbeitung können Vorfälle im Vorfeld erkannt und vermieden werden. Continuous Offensive Security Service Mittel zur kontinuierlichen Verbesserung der Landschaft und damit zur Vermeiden von Vorfällen.

TECHNIK DIE BEGEISTERT

PROFITIEREN SIE VON DEN STÄRKEN DER EINZELNEN KOMPONENTEN

Beim Einsatz des DTS Cockpit werden alle Gegebenheiten der individuellen IT-Infrastruktur berücksichtigt. Täglich laufen Hunderte von Alerts auf. Die Analysten müssen entscheiden, welche Meldungen tatsächlich auf Bedrohungen hinweisen. Identifiziert eine solche Level-1-Analyse Anzeichen für einen Angriff, folgt eine tiefere Untersuchung. All das erfordert Zeit und Expertise. Dazu kommt, dass Security-Experten auf dem Arbeitsmarkt schwer zu finden sind. Somit spielt die technische Kompetenz eine wesentliche Rolle.

DTS Cockpit bietet einen branchenweit einzigartigen Service, bündelt die einzelnen Lösungen und liefert eine umfassende Übersicht über das Netzwerk. Sie ist eine hybride Plattform, die aus SIEM, MDR und SOAR besteht.



ARP-GUARD
NETWORK ACCESS CONTROL

Mit ARP-GUARD Network Access Control erhalten ausschließlich autorisierte und eineindeutig identifizierte Geräte Zugang zum Netzwerk. ARP-GUARD erfasst jeden einzelnen Zugriff in Echtzeit, die Position der Ressource und den Zeitpunkt jedes Netzwerkzugriffes. Netzwerkanomalien können auf diese Weise erkannt, gemeldet und mit unserem intelligenten Schwachstellen- und Risikomanagement in Echtzeit bewertet und behoben werden. Die Orchestrierung der gesamten Netzwerkumgebung geschieht an zentraler Stelle und ermöglicht die Definition von spezifischen Regelwerken für verteilte Standorte. In separaten VLANs werden zudem sensible Bereiche geschützt und die Zuweisung der Geräte erfolgt nach einem festgelegten Regelwerk.

LOG STORAGE

Der Log Storage dient der Datenaufbewahrung innerhalb der Cockpit Plattform. Protokolldaten werden erst bei Erreichen dieser Kapazitätsgrenze gelöscht. Diese Kapazitätsgrenze lässt sich beliebig erweitern. Demnach hängt die Aufbewahrungsdauer von der Frequenz und dem Volumen der eingehenden Protokolldaten ab. Sollten mehr Daten in das Cockpit transferiert werden, werden diese nicht verworfen, sondern der Aufbewahrungszeitraum der vorhandenen Protokolldaten entsprechend reduziert und die ältesten Protokolldaten werden verworfen.

BASISKOMPONENTE
COCKPIT PLATTFORM

Die Basiskomponente der Plattform besteht aus mehreren Teilen, die stets als Bundle geliefert werden. Diese sind:

- Cloud-SIEM ermöglicht die Anbindung und Analyse der Datenquellen inklusive 1TB Log Storage
- ARP-GUARD Network Access Control (Lizenzen) inkl. Data Manager als Actor
- DTS 24/7 SOC Services durch Analysten zur kontinuierlichen Bewertung (und Reaktion, wenn gewünscht) der aufkommenden Alarme

DATA COLLECTOR

Data Collectoren dienen der Sammlung von Daten aus verschiedenen Logquellen. Diese Daten werden analysiert und Alarme können daraus abgeleitet werden. Folgende Data Collectoren können aktuell integriert werden. Die Auswahl der Data Collectoren wird ständig erweitert:

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

DATA MANAGER

Data Manager gehen weit über die Funktionen des Data Collectors hinaus. Neben der Sammlung von Dateninformationen dient der Data Manager hauptsächlich dazu, aktiv die angebundenen Komponenten zu steuern und entsprechend Aktionen innerhalb der Kundenumgebung auszuführen. Folgende Data Manager können aktuell integriert werden. Die Auswahl der Data Manager wird ständig erweitert:

- ARP-GUARD Network Access Control (inklusive in der Cockpit-Plattform)
- Palo Alto Networks Next-Generation Firewalls
- Palo Alto Networks Cortex XDR (Prevent und/ oder Pro)
- Proofpoint Targeted Attack Protection (TAP)
- Infinipoint Plattform
- LogRhythm SIEM
- MS Defender

REAKTIONS-MÖGLICHKEITEN	BESCHREIBUNG
Endpunkt Netzwerk Trennung	Ermöglicht die Isolation von registrierten Endpunkten vom Kundennetzwerk
Endpunkt Quarantäne	Ermöglicht die Isolation von registrierten Endpunkten vom Kundennetzwerk
Endpunkt Compliance Status	Setzt den Compliance Status eines Devices im Device Managemen voraus. Dies setzt den Infinipoint Datamanager voraus
Interaktive Sitzung am Endpunkt einleiten	Den Analysten ermöglichen, eine Befehlsgruppe auf dem Endpunktsystem zu öffnen
Dateien auf den Endpunkt herunterladen	Während des IR-Untersuchungsprozesses kann das Herunterladen von Tools erforderlich sein, um den Verstoß einzudämmen oder notwendige Informationen zu erfassen
Dateien am Endpunkt löschen	Entfernen von schädlichen Dateien auf den Endpunktsystemen
Sammeln von Dateien und Speicherplatz vom Host	Sammeln von Dateien und Speicher von Endpunkten

Combining Red & Blue Teams

CONTINUOUS OFFENSIVE SECURITY SERVICE

Trotz immenser Investitionen in Security Produkte und Prozesse werden Unternehmen regelmäßig gehackt. Die Ursache liegt oftmals in einem Mangel an Wissen über die Angriffsmethoden von Cyberkriminellen oder auch „Advanced Persistent Threats (APT)“. Um sicherzustellen, dass ein Unternehmen den aktuellen Bedrohungen standhalten kann, muss verstanden werden, welche „Tactics, Techniques and Procedures (TTP's)“ während eines Cyberangriffs angewandt werden.

Durch das kontinuierliche Security Testing innerhalb eines etablierten Zyklus, anhand von standardisierten Verfahren wie dem „Beobachten (Observe), Orientieren (Orient), Entscheiden (Decide), Handeln (Act) (OODA-Loop)“ wird langfristig die Erfassung der gesamten Organisationssicherheit ermöglicht. Angriffsmöglichkeiten, Schwachstellen und allgemeine Defizite können vom Cyber Defense Team regelmäßig adressiert werden, mit dem Ziel, das Risiko von erfolgreichen Cyberangriffen stetig zu verringern.

Warum ist Continuous Offensive Security Service nur in Kombination mit dem DTS Cockpit sinnvoll?

Als branchenweit einzigartiges Add-on ermöglichen wir den „Continuous Offensive Security Service“ in unserem DTS Cockpit. Andere Anbieter stellen lediglich einmalige Lösungen bzw. Analysen zur Verfügung. Wir gehen mehrere Schritte weiter und verstehen Cyber Security als kontinuierlichen Prozess.

Innerhalb der Testzyklen wird das Security Testing Schritt für Schritt intensiviert. Vom Vulnerability Assessment über Penetration Testing bis hin zu Red Team Operations oder Purple Team Testing, durchläuft Ihr Unternehmen verschiedenste Test-Cases. Das DTS Cockpit kombiniert „state-of-the-art“ Angriffstechniken mit entsprechenden Detektions- oder Präventionsmaßnahmen. Durch unseren SOC hat man zudem alle Schwachstellen im Blick. Alle Informationen werden korreliert und stehen allen Beteiligten zur Verfügung, um die gesamte Unternehmenssicherheit langfristig zu optimieren.

DTS Cockpit legt den Grundstein für das Purple-Teaming, das nicht nur die Cybersicherheit verbessert, sondern auch die Effizienz des teamübergreifenden Arbeitens.

Eine regelmäßige Überprüfung gewährleistet, dass Sicherheitsmaßnahmen wie geplant funktionieren. Zusätzlich können neue Angriffstechniken zeitnah in den Testzyklen etabliert werden, um Blindspots durch einmalige Sicherheitsüberprüfungen zu reduzieren.

In dem Zusatz-Service führen wir ein regelmäßiges IT-Security Assessment bei Ihnen durch, indem wir reale Cyberattacken simulieren und Ihre Sicherheitsarchitektur auf die Probe stellen – in kleinen Abschnitten und individuell auf die Umgebung abgestimmt. So erlangen wir zum einen das unverzerrte Abbild Ihrer Sicherheitslandschaft hinsichtlich Sichtbarkeit, Reaktionsfähigkeit sowie den Sicherheitslücken im System. Zum anderen haben wir ein tiefes Fachwissen über Cyberangriffe und arbeiten anhand der Ergebnisse gemeinsam mit Ihnen konstant an der Verbesserung des Sicherheitsniveaus.

Diese stetige Weiterentwicklung, mit klaren Roadmaps und transparenten Fortschritten, bietet Ihnen einen außergewöhnlichen Mehrwert. Wir sind fest davon überzeugt, dass nur ganzheitliche Plattformen, Services und Prozesse nachhaltig höchste IT-Sicherheit mit sich bringen.

1. **Branchenweit einzigartiger Mehrwert und IT-Security als Prozess**

2. **Kontinuierliche Ermittlung der Schwachstellen in Ihrer IT-Landschaft, in dem wir reale Cyberangriffe simulieren**

3. **Basierend auf den Ergebnissen gemeinsame Erarbeitung einer langfristigen Roadmap und klare Handlungsempfehlungen**

BECOME PURPLE

Work Together to Improve

Als Experten helfen wir Ihnen, reale Cyberangriffe zu verstehen, sich vorzubereiten und Ihr gesamtes IT-Sicherheitsniveau kontinuierlich und langfristig zu verbessern.

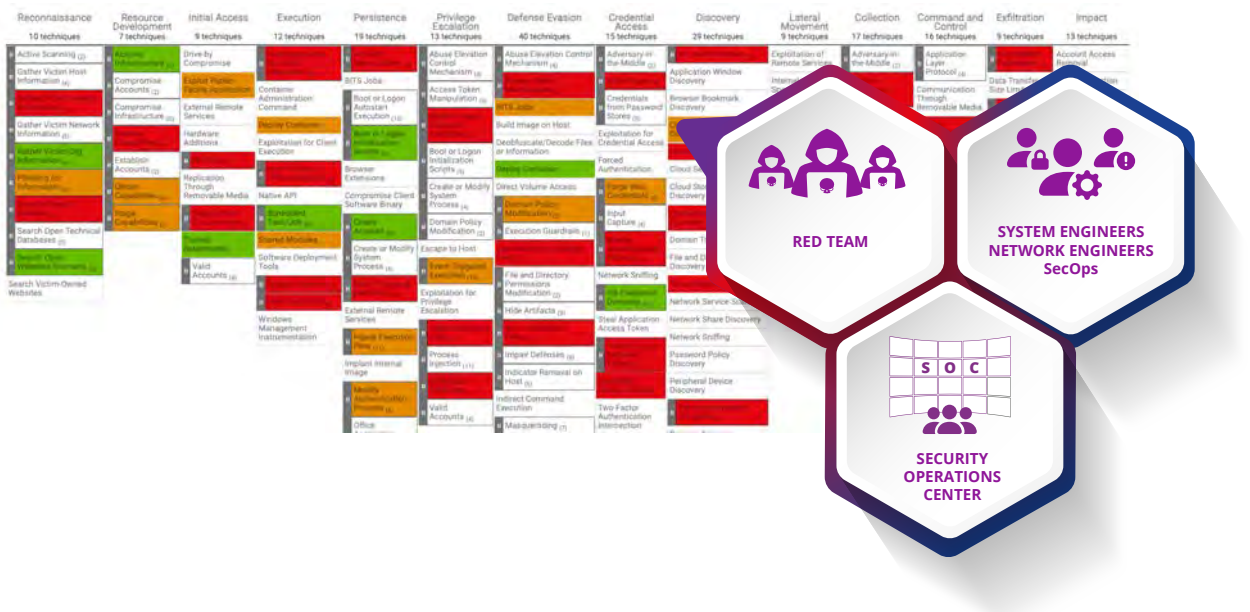
SUM UP

- DTS Cockpit (Vorbeugen, Erkennen, Überprüfen): Einführung von Präventions- und Detektionmaßnahmen und deren Überprüfung

- Continuous Offensive Security Service (Überprüfen, Erkennen, Verhindern): Überprüfung und Identifizierung eines Problems und Aufbau von Detektion- und Präventionsmaßnahmen

- Gezielte Nutzung der Ergebnisse, um mögliche Schwachstellen im Auge zu behalten, entsprechende Prozesse einzurichten und neue Lösungen passend in das Cockpit zu integrieren

Beides funktioniert nur, wenn der Cockpit-Service und Continuous Offensive Security Service zusammenarbeiten!



IHRE VORTEILE EINER GANZHEITLICHEN CYBER-SECURITY-STRATEGIE MIT DTS COCKPIT

REVOLUTIONÄRE KOMBINATION AUS PLATTFORM & 24/7 SERVICE

ZENTRALE SECURITY OPERATIONS PLATTFORM – „ALLES AUF EINEN BLICK“

HERSTELLERUNABHÄNGIGES BÜNDELN IHRER SICHERHEITSLÖSUNGEN

ECHTE SECURITY OPERATIONS EXPERTEN – RUND UM DIE UHR IM EINSATZ

40 JAHRE EXPERTEN-KNOW-HOW, SOC-PIONIER AN 4 EUROPÄISCHEN STANDORTEN, GANZHEITLICHE LÖSUNGEN FÜR 1.400 KUNDEN IM BEREICH MANAGED SERVICES

BEZAHLBARE LÖSUNG FÜR DEN MITTELSTAND MIT EINER KLAREN KOSTENSTRUKTUR

MANAGED SERVICE AUS DER DEUTSCHEN, ZERTIFIZIERTEN DTS CLOUD BEREITGESTELLT

Einzigartig. Kompetent. Zukunft

ARP-GUARD
als DTS-eigene NAC-Lösung im Service inklusive

CONTINUOUS OFFENSIVE SECURITY SERVICE
als branchenweit einzigartiger Mehrwert

BEZAHLBARE, INDIVIDUELLE TESTING-BAUSTEINE FÜR KONTINUIERLICHE SCHWACHSTELLENSUCHE

LANGFRISTIGE ROADMAP & HANDLUNGSEMPFEHLUNGEN

SICHERER ZUGANG MIT DTS IDENTITY

CYBER SECURITY ALS PROZESS: LANGFRISTIGE, STETIGE WEITERENTWICKLUNG DES SICHERHEITSNIVEAUS

KOSTENATTRAKTIVER AUSGLEICH FEHLENDER RESSOURCEN FÜR EIGENES SECURITY OPERATIONS

ENTLASTUNG IHRER IT-ABTEILUNG

FLEXIBEL: WIR PASSEN UNS IHREN BEDÜRFNISSEN AN, NICHT UMGEKEHRT!

KI IN DER CYBER SECURITY

Trotz der vielen Vorteile des Einsatzes von KI in der Cyber Security gibt es auch einige Risiken, die mit ihrem Einsatz verbunden sind.

DATENSCHUTZ- UND SICHERHEITSRISIKEN

KI-Systeme sammeln und analysieren große Mengen sensibler Daten, was das Risiko von Datenschutzverletzungen und Cyberangriffen erhöht.

VERZERRUNGEN

KI-Systeme können verzerrte Ergebnisse liefern, wenn sie auf unvollständigen oder voreingenommenen Daten trainiert werden.

MANGELNDE TRANSPARENZ UND VERANTWORTLICHKEIT

Die KI kann komplexe Entscheidungen treffen, deren Entscheidungsprozesse schwer nachvollziehbar sein können. Dies kann zu mangelnder Transparenz und Verantwortlichkeit führen.

KOSTEN UND RESSOURCENBEDARF

Die Entwicklung und Implementierung von Künstlicher Intelligenz erfordert oft erhebliche Investitionen in Technologie und Expertenwissen. Dies kann insbesondere für Unternehmen eine Herausforderung sein.

Wir haben DIE Lösung. Machine Learning und Automatisierung gehören ebenso zum DTS Cockpit, wie echte, physische, top professionelle DTS SOC-Experten. Wir haben die bestmögliche Mischung gefunden, um ein 24/7 Managed Detection & Response höchster Qualität zu gewährleisten. Durch diese perfekte Abstimmung und ihre durchgehende Angriffsidentifikation, -analyse und -reaktion, profitieren Sie mehrfach: Wir entlasten Sie bei der Administration sowie dem eigenen rund-um-die-Uhr-SOC-Betrieb. Zudem stellen wir nicht nur eine reine Bereitschaft, sondern ein Höchstmaß an Know-how und Verständnis zur Verfügung und wehren Angriffe durch sofortige Maßnahmen ab.

KI DIE LÖSUNG FÜR CYBER SECURITY?

1. Investieren Sie in die Zukunft Ihrer IT-Sicherheitslandschaft.
Ein erfolgreicher Angriff aufgrund veralteter Technologie kostet Sie angesichts immer raffinierterer Bedrohungen ein Vielfaches.

2. Ausreichendes Budget und entsprechendes Know-how sind notwendig.
Angesichts der zahlreichen Vorteile, die der Einsatz von KI mit sich bringt, stellt sich die Frage, warum viele Unternehmen diese Technologie noch nicht implementiert haben. Gründe dafür sind die hohen Kosten, Bedenken hinsichtlich Compliance und Datenschutz sowie fehlendes Know-how.

3. Die bestmögliche Mischung.
Schwachstellen gibt es immer, kein System auf dem Markt kann 100-prozentigen Schutz bieten. Da selbst diese lernfähigen Systeme durch raffinierte Angriffsmethoden getäuscht werden können, sollten Sie sicherstellen, dass Sie einen Partner haben, der Sie proaktiv schützt und entlastet.

18

DIE PLATTFORM

Die zentrale Security Operations Plattform für den Mittelstand

Höchste Qualität. Made in Germany.

DTS ist eine einzigartige Kombination aus hoch qualifizierten Experten und führenden Technologien. Sie bilden die Grundlage unserer Security Operations Plattform, die es uns ermöglicht, unsere Kunden zu schützen.

DTS Cockpit ist für Unternehmen jeder Größe geeignet, die mehrere Sicherheitslösungen im Einsatz haben und ihre bestehende IT-Infrastruktur transparenter gestalten möchten. Es ermöglicht herstellerunabhängig die Anbindung aller gängigen Sicherheitslösungen als Data Collector und führt deren Daten zu einer vollständigen Security Information zusammen. Darüber hinaus können weltweit führende Security-Technologien, u. a. in den Bereichen Firewall, Endpoint Protection, Device Hygiene, E-Mail Security oder Network Access Control (NAC) als Data Manager für das zentrale, aktive Agieren eingesetzt werden. Das ebenfalls von uns entwickelte ARP-GUARD NAC ist bereits im Service inklusive, für optimale Visibilität und Interaktion im Netzwerk.

Wir bieten „Sehen. Verstehen. Agieren." in einem besonderen bezahlbaren Service: Ihre Sicherheitsarchitektur gebündelt auf einer zentralen Plattform, herstellerunabhängiger Zusammenschluss und Orchestrierung von führenden Data Collectoren & Managern, vollständige Transparenz, tiefes IT-Security-Verständnis, direkte Aktionen und Steuerung, erstklassiges und zertifiziertes 24/7 SOC, ARP-GUARD NAC im Service inklusive, alles als Managed Service. Wir entlasten Sie maßgeblich, damit Sie sich auf Ihr Kerngeschäft konzentrieren können.

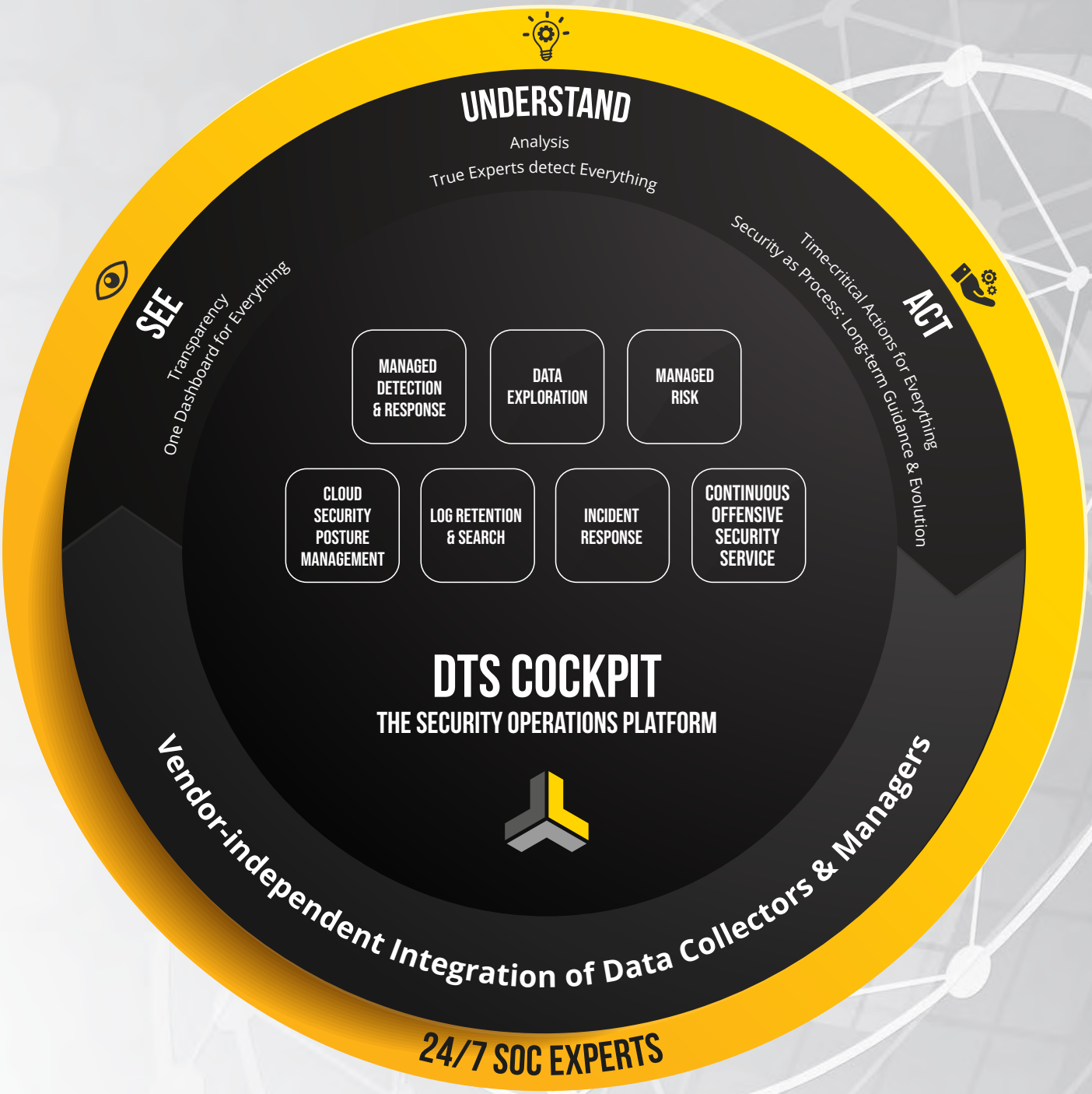
SEHEN, VERSTEHEN, AGIEREN ALS "ALL IN ONE" SECURITY OPERATIONS.

—

Was wäre, wenn man durch Security Operations langfristig und zielgerichtet das eigene Sicherheitsniveau weiterentwickeln könnte? Geht nicht? Geht!

ARE YOU READY FOR TAKE-OFF WITH DTS COCKPIT?

Steigen Sie mit uns ins Cockpit und machen Sie sich bereit für einen aufregenden Flug.


UNDERSTAND
Analysis
True Experts detect Everything
SEE
Transparency
One Dashboard for Everything
ACT
Time-critical Actions for Everything
Security as Process: Long-term Guidance & Evolution
MANAGED DETECTION & RESPONSE
DATA EXPLORATION
MANAGED RISK
CLOUD SECURITY POSTURE MANAGEMENT
LOG RETENTION & SEARCH
INCIDENT RESPONSE
CONTINUOUS OFFENSIVE SECURITY SERVICE
DTS COCKPIT
THE SECURITY OPERATIONS PLATFORM
Vendor-independent Integration of Data Collectors & Managers
24/7 SOC EXPERTS

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

ANJA KUHN
Manager Corporate Strategy and Development

Diese Aussage zeigt, wo heute oft die Schwachstelle in der Sicherheitsstrategie von Unternehmen liegt. Viele einzelne „Best-of-Breed“-Lösungen werden eingesetzt, ohne den Überblick zu haben oder Synergien zu nutzen. Genau hier setzt Cockpit an: Denn Cybersecurity-Mesh-Architecture-Lösungen, die Security-Tools bündeln und als kollaboratives Ökosystem funktionieren, sind bisher nur bei Enterprise-Lösungen zu finden. Doch anstatt einer wartungsintensiven Software anzubieten, die von einer überlasteten IT-Abteilung zusätzlich betreut werden muss, basiert unser Ansatz auf unserer langjährigen Erfahrung im Mittelstand und für den Mittelstand.
Entsprechend der Aussage von Gartner haben wir unser 24/7 Security Information & Operation Service Cockpit entwickelt. Es ist nicht nur eine einzigartige Cybersecurity-Mesh-Architektur, sondern auch wirtschaftlich attraktiv gestaltet. Durch die Kostentransparenz und den Wegfall von Erstinvestitionskosten für spezifische Security-Lösungen kann sich jeder Kunde seine Systemlandschaft nach seinen individuellen Bedürfnissen zusammenstellen (Best of Breed für jeden). Mit unserem Service übernehmen wir direkt das Handling und stellen Ihnen eine Gesamtlösung zur Verfügung, die Ihre Umgebung 24/7 sieht, versteht und bei Bedarf handelt.

Sicherheit, die den Unterschied macht.

ENTWICKLUNG

Unsere Idee war die Entwicklung einer technologischen Plattform, die einfach in der Anwendung und bezahlbar für Mittelstand ist. Das ist uns gelungen, aber es ist erst der Anfang. Die zentrale Operations Security Plattform wird mit vielen weiteren Features umfangreich ausgebaut und weiterentwickelt. Seien Sie gespannt!

2022	2023 QUARTAL 1	2023 QUARTAL 2

DTS COCKPIT ADD-ON-SERVICES

DTS CORTEX XDR MANAGEMENT SERVICE

DTS erbringt im Rahmen des Cockpit Service die Wartung der folgenden Aufgaben der XDR Plattform als Service für den Kunden:

- Verwaltung, Überprüfung und Anpassung des Regelwerks
- Reaktivierung von isolierter Endpoints

DTS MICROSOFT DEFENDER FÜR ENDPOINT MANAGEMENT SERVICE

DTS erbringt im Rahmen des Cockpit Service die Wartung der folgenden Aufgaben des Microsoft Defender als Service für den Kunden:

- Verwaltung, Überprüfung und Anpassung des Regelwerks
- Reaktivierung von isolierter Endpoints

ARP-GUARD

- **Zusätzliche Access + Lizenzen**
  Für den Fall, dass mehr Lizenzen angefordert werden, als für die Anzahl der User im Cockpit enthalten sind. Hierfür gibt es feste Staffelungen,die hinzugebucht werden können.
  - Network Access Control: Schutz vor unautorisierten Zugriffen
  - Regelwerk für das Netzwerk (vom Quarantäne-VLAN bis zur Port-Abschaltung)
  - Wahrung der Netzwerkintegrität bei heterogenen Netzwerkstrukturen
  - Hersteller- und technologieunabhängige Lösung (Multi-Vendor Strategie)

- **Upgrade Clusterlizenz**
  ARP-GUARD Cluster ermöglicht eine „ready-to work" Server-Replikation. Damit bietet ARP-GUARD Network Access Control eine erhöhte Aus fallsicherheit und Skalierbarkeit für kritische IT-Systeme.
  - Hochverfügbarkeit für sensible IT-Bereiche
  - Höchste Systemverfügbarkeit und -sicherheit für ein ausfallsicheres Gesamtsystem
  - Maximale Ausfallsicherheit für kritische Infrastrukturen
  - Sofortige Serverreplikation

- **Captive Portal**
  Das ARP-GUARD Captive Portal regelt den Netzwerkzugriff von Gast- oder Fremdkomponenten wie Smartphones und Notebooks und ergänzt damit ideal die in Cockpit enthaltene NAC-Lösung.
  - Sichere und komfortable Gastzugänge
  - BYOD für Mitarbeitende, Besucher*innen oder Wartungstechniker*innen
  - Gästeportal mit Selbstregistrierung
  - Integrierte dynamische Firewall

- **Ganzheitliche ARP GUARD Installation**
  Mit dieser Erweiterung werden die Punkte eingerichtet, die über den Umfang der ARP-GUARD Konfiguration im Rahmen eines Cockpit-Projektes hinausgehen. Diese Punkte sind jedoch für einen vollständigen NAC-Betrieb notwendig.

Coming Soon: Genereller ARP GUARD Service fürCockpit

DTS CLIENT

DTS COCKPIT 2.0

REPORTING ENGINE

ALARM ENGINE EVOLUTION

APPLICATION FOR UPLOADING CONFIGURATION FILES TO LOGSTASH

2023
QUARTAL 3

2023
QUARTAL 4

2024

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de