SEHEN. VERSTEHEN. AGIEREN. VALIDIEREN. OPTIMIEREN.

00

DTS COCKPIT

Die zentrale 24/7 Security Operations Plattform
für den Mittelstand

WHITEPAPER
JUNI 24

INHALT

SEHEN. VERSTEHEN. AGIEREN. VALIDIEREN. OPTIMIEREN.

03

DTS COCKPIT SERVICE GUIDE

Die zentrale 24/7 Security Operations Plattform für den Mittelstand

UNSERE MISSION

Mit unserer Security Operations Plattform helfen wir Unternehmen, Cyberrisiken abzuwehren, sich proaktiv zu schützen und die eigene Sicherheitslage kontinuierlich zu verbessern.

In Deutschland werden jährlich mehr als 8,5 Milliarden Euro für IT-Sicherheit ausgegeben. Unzählige Sicherheitslösungen und -dienstleistungen auf dem Markt und nahezu jedes Unternehmen setzt nach dem „Best-of-Breed-Ansatz“ verschiedene Produkte ein. Dennoch nimmt die Zahl der Cyberangriffe stetig zu und insbesondere eine 24/7-Sicherheit mit zeitkritischer Reaktion wird nur selten gewährleistet.

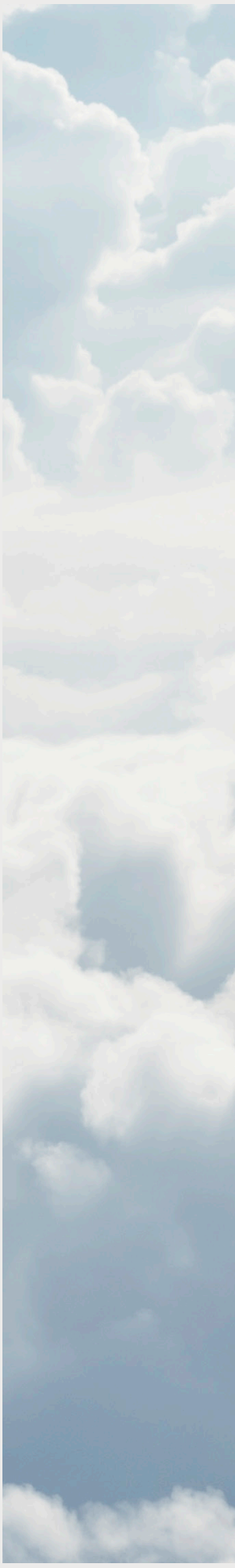
Was sind die Gründe für diese Entwicklung? Die Angriffe werden immer raffinierter und komplexer, erfolgen zu jeder Zeit, auf allen Geräten und auf unterschiedlichste Art und Weise.
Weitere Bedrohungen sind die mangelnde Transparenz und Alarmbereitschaft sowie fehlendes Know-how.

OUR VISION. YOUR FUTURE.

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. Die Security Operations Plattform 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."



HAND AUFS HERZ

HABEN SIE EINEN 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 stehen diese Eckpfeiler gebündelt zur Verfügung .Wie geht das? DTS macht esmöglich, mit dem DTS Cockpit als 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 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-EXPERTISE SEIT ÜBER 40 JAHREN.

Unabhängig vom Ausmaß eines erfolgreichen Cyberangriffs wird dieser 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 diesen Anforderungen nicht gerecht.

Je mehr voneinander unabhängige Security-Lösungen man eingesetzt werden, 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 ein modernes Detection & Response zum Tragen kommen und sich nahtlos in die bestehenden Systeme integrieren.

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 vorausgesetzt.

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, Agieren, Validieren und Optimieren als „All in One" - nur so funktioniert modernste Cyber Security. Weg vom passiven, dezentralen Daten sammeln, hin zur aktiven, zentralen Sichtbarkeit und Steuerung – Vom Mittelstand für den Mittelstand und „Made by DTS"!

07

TRUE EXPERTS DETECT EVERYTHING

KNOW-HOW

Als langjährig erfahrener IT-Security-Softwarehersteller haben wir 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 Sicherheitskonzeptes vereint und dennoch bezahlbar ist.

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

Der Schlüssel dazu ist die herstellerübergreifende Einbindung der Komponenten „Data Collector" und „Data Manager" in einem System. Durch die Verknüpfung dieser Aspekte haben wir eine kollaborative IT-Security-Architektur entwickelt. Das Ergebnis ist eine 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

BESSER, SCHNELLER UND INNOVATIVER MIT DTS.

SECURITY OPERATIONS PLATTFORM MIT CYBER SECURITY ALS PROZESS

Weltweit gibt es zahlreiche Anbieter, die Ihnen Security Operations in allen Formen und Farben versprechen. Wir sind einer der wenigen, die wirklich alle Bereiche der Sicherheit abdecken - lückenlos. Wir bieten ganzheitliche Security Operations am Endpoint, im Netzwerk und in der Cloud. Sehen, Verstehen, Agieren, Validieren und Optimieren - alles aus einer Hand.

01 SEHEN

Man kann nichts schützen, was man nicht sieht.

Zusammenführung der Lösung, um eine vollständige Transparenz zu erreichen und eine einheitliche Datenbasis zu schaffen

02 VERSTEHEN

Man findet nichts, wenn man nicht richtig sucht.

Identifizierung, Analyse und Reaktion auf Bedrohungen durch das DTS SOC

03 AGIEREN

Agieren, statt zu reagieren.

Aktives Handeln und Abwehren von Angriffen durch angebundene Data Manager

04 VALIDIEREN

Teamwork.

Überprüfung der eingesetzten Lösungen und Prozesse zur proaktiven Identifizierung potenzieller Einfallstore

05 OPTIMIEREN

DTS steht Ihnen als Coach zur Seite.

Gemeinsame, fortlaufende Optimierung der IT-Sicherheitslandschaft

VOM MITTELSTAND FÜR DEN MITTELSTAND

SICHER MIT MANAGED SERVICES SPAREN

09 – 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 der Betrieb eines SOC ist teuer. Für mittelständische Unternehmen lohnt es sich daher in der Regel nicht, ein eigenes SOC zu unterhalten. Mit dem DTS Cockpit stellen wir Ihnen die Technologie bereit, analysieren die Alarme und kümmern uns kontinuierlich um ihren sicheren Betrieb.

Beim DTS Cockpit sind alle wichtigen Komponenten und Aspekte von Anfang an im Managed Service enthalten und müssen nicht durch Add-ons ergänzt werden.Sie wissen direkt was Sie bekommen, in welchem Umfang, zu welchen Kosten.

PROFITIEREN SIE DOPPELT:

FINANZIELL UND VOM EXPERTEN-WISSEN DER SPEZIALISTEN

WIR LEBEN „EASY TO USE & EASY TO PAY“.

WEE SEE. WE DO. SAFE.

FACH-KRÄFTE

IT-FACHKRÄFTEMANGEL SO HELFEN WIR IHNEN

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

Bedrohungserkennung 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 vorgesehen.

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

+450 MITARBEITENDE

4 SOC
Athen, Hamburg, Herford, Thessaloniki

2 DATACENTER
Herford, Münster

+1400 MANAGED SERVICES KUNDEN

+ 20 JAHRE SOFTWARE BY DTS

IN 6 LÄNDERN VERTRIEB

THINKING BEYOND TECHNOLOGY

TECHNOLOGIE

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. Ziel: kontinuierliche Verbesserung der Sicherheitslandschaft und das Vermeiden weiterer Vorfälle.

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, dieu. a. aus SIEM, MDR und SOAR besteht.

ARP-GUARD

NETWORK ACCESS CONTROL AS A SERVICE

Mit ARP-GUARD Network Access Control erhalten ausschließlich autorisierte und eindeutig identifizierte Geräte Zugang zum Netzwerk. ARP-GUARD protokolliert jeden einzelnen Zugriff in Echtzeit, die Position der Ressource und den Zeitpunkt jedes Netzwerkzugriffs. 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 FUSION HUB

Die Basiskomponente der Plattform besteht aus mehreren Teilen, die immer 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 Log-Quellen. Diese Daten werden analysiert und Alarme können daraus abgeleitet werden. Unter anderem können nachfolgende Data Collectoren aktuell integriert werden. Die Auswahl der Data Collectoren wird laufend 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 vor allem 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 kontinuierlich erweitert:

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

DTS INCIDENT RESPONSE SERVICE

DTS-Eingreiftruppe, mit tiefem Fachwissen, passender Notfall-Infrastruktur, die Ihre zeitkritische Geschäftskontinuität sicherstellen, ohne dass Sie hohe Stundenkontingente einkaufen müssen, mit unschlagbaren 24/7-Service-Zeiten und Sichtung sowie Bewertung bestehender Notfallpläne inklusive.

DTS NETWORK INSIGHTS

Ermöglicht die passive Datensammlung auf Netzwerkebene, ohne dass herstellerspezifische Flow-Technologien erforderlich sind. Dies ermöglicht eine optimale und vollständige Sichtbarkeit und Interaktion im Netzwerk.

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 isolierten Endpoints

DTS MICROSOFT DEFENDER FÜR ENDPOINT SERVICE

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

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

COMBINING RED & BLUE TEAMS

RED, BLUE & PURPLE TEAMING MIT DTS!

Trotz enormer Investitionen in Security Produkte und Prozesse werden Unternehmen immer wieder Opfer von Hackerangriffen. Die Ursache liegt häufig in mangelndem Wissen über die Angriffsmethoden der Cyberkriminellen oder auch „Advanced Persistent Threats (APT)“. Um sicherzustellen, dass ein Unternehmen den aktuellen Bedrohungen standhalten kann, ist es wichtig zu verstehen, welche „Tactics, Techniques and Procedures (TTP's)“ bei einem Cyberangriff angewendet 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 generelle Defizite können durch das Cyber Defense Team regelmäßig adressiert werden, mit dem Ziel, das Risiko erfolgreicher Cyberangriffe kontinuierlich zu reduzieren.

Die Zusammenarbeit der drei Teams - Red, Blue und Purple - ist von entscheidender Bedeutung. Werfen wir einen genaueren Blick darauf:

RED TEAM

Meister der Strategie, des Angriffs & des taktischen Denkens

- Schwachstellenjäger
- Angriffssimulatoren
- Hacker-Mentalität

Das Red Team sind spezialisierte Sicherheitsteams, die eine kritische und unabhängige Überprüfung durchführen, indem sie die Rolle potenzieller Angreifer übernehmen.

Sie führen Bedrohungssimulationen, Penetrationstests oder Übungen durch, um Schwachstellen in einem System oder einer Organisation aufzudecken. Sie nehmen die Perspektive eines Angreifers ein und versuchen, Sicherheitslücken oder potenzielle Risiken zu identifizieren, die andere Teams möglicherweise übersehen haben.

Aus den Ergebnissen werden Handlungsempfehlungen abgeleitet, um die Widerstandsfähigkeit der Organisation gegenüber potenziellen Bedrohungen zu erhöhen, ihre Verteidigungsfähigkeiten zu verbessern und proaktiv auf Bedrohungen zu reagieren.

BLUE TEAM

Leidenschaft für die Verteidigung

- Sicherheitswächter
- Bedrohungsbekämpfer
- Verteidigungsexperten

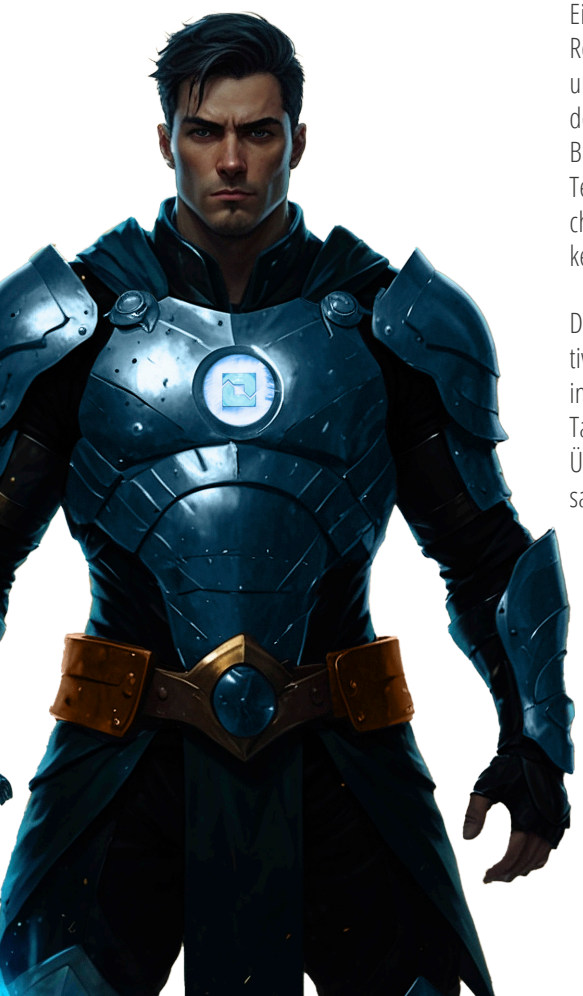
Das Blue Team ist ein Team, das für Verteidigung und Sicherheit verantwortlich sind. Im Gegensatz zum Red Team, welches Schwachstellen und Sicherheitslücken identifiziert, konzentriert sich das Blue Team auf die Erkennung, Analyse und aktive Verhinderung von Angriffen um die Sicherheit des Systems oder der Organisation zu verbessern.

Sie führen regelmäßige Überwachungs-, Analyse- und Reaktionsaktivitäten durch, um potenzielle Bedrohungen zu identifizieren, Angriffe abzuwehren, die Integrität der Systeme zu gewährleisten und die Abwehrfähigkeiten kontinuierlich zu verbessern.

PURPLE TEAM

Coach

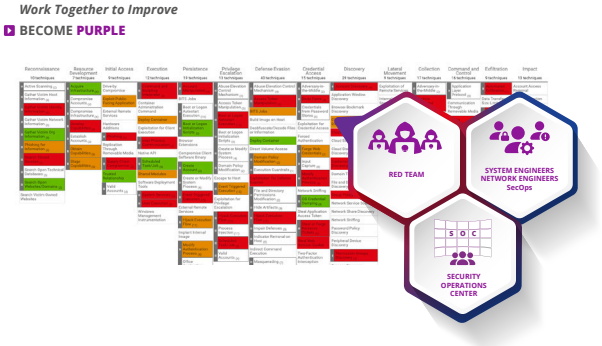
- Gemeinsame Verteidigung
- Synergie zwischen Offensive (Red) & Defensive (Blue)



Das Purple Team ist eine Symbiose, die sowohl Elemente des Red Teams als auch des Blue Teams in sich vereint. Ziel ist es, die Sicherheit einer Organisation ganzheitlich zu verbessern. Im Gegensatz zu den beiden anderen Teams, die traditionell getrennt arbeiten, kooperiert das Purple Team, um Synergien zwischen Offensive (Red) und Defensive (Blue) Ansätzen zu schaffen.

Ein Purple Team kombiniert die Fähigkeiten des Red Teams, Schwachstellen zu identifizieren und Angriffsszenarien zu simulieren, mit den defensiven Maßnahmen und Strategien des Blue Teams. Dies ermöglicht es dem Purple Team, Angriffssimulationen durchzuführen, Sicherheitskontrollen zu testen und die Wirksamkeit von Abwehrmechanismen zu überprüfen.

Das Hauptziel des Purple Teams ist es, die Effektivität der Sicherheitsmaßnahmen zu erhöhen, indem es sowohl offensive als auch defensive Taktiken kombiniert und einen umfassenden Überblick über die Sicherheitslage der Organisation bietet. Durch diese enge Zusammenarbeit können Schwachstellen schneller erkannt, Risiken besser eingeschätzt und die Reaktionsfähigkeit auf Sicherheitsvorfälle verbessert werden.



WAS MACHT UNSEREN GANZHEITLICHEN UND PROAKTIVEN ANSATZ SO EINZIGARTIG?

DTS hat als einziger Anbieter für Security Operations ein eigenes Spezialisten-Team für Purple Teaming, welches innerhalb des DTS Cockpits kontinuierlich blinde Flecken und Sicherheitslücken in Ihrer Sicherheitsarchitektur identifiziert und durch Roadmaps und Handlungsempfehlungen als „Coach" stetig das Sicherheitsniveau erhöht. Andere Anbieter stellen lediglich einmalige Lösungen bzw. Analysen zur Verfügung. Wir gehen mehrere Schritte weiter und verstehen Cyber Security als kontinuierlichen Prozess.

- Weltweit einzigartig: DTS Purple Teaming in Kombination mit der 24/7 Security Operations Platform
- Kombination von Offensive und Defensive: Einzigartige Verbindung der Stärken von Red Teaming (erfahrene SOC-Analysten) und Blue Teaming (zertifizierte Sicherheitsspezialisten) zu einer effektiven Sicherheitsstrategie
- Innovativer Coaching-Ansatz: Stets an der Seite des Kunden als Coach zur gezielten Weiterentwicklung
- Cyber Security als Prozess: Umsetzung von Sicherheitsmaßnahmen als kontinuierlicher Optimierungsprozess
- Roadmaps und Handlungsempfehlungen: Individuelle Ansätze und Lösungen, die spezifisch auf die jeweilige Kundenumgebung und -anforderung zugeschnitten sind
- Proaktive Sicherheit: Fokus auf Prävention und proaktive Maßnahmen an statt nur auf reaktive Lösungen

NEXT LEVEL CYBER SECURITY: MIT DTS RED, BLUE & PURPLE TEAMING ONE STEP AHEAD

DEFEND TODAY. SECURE TOMORROW.

EINZIGARTIG. KOMPETENT. ZUKUNFT.

INCIDENT RESPONSE SERVICES
- Präventive Verteidigung, schnelle Einschätzung der Bedrohungslage, Reaktion, Analyse & Wiederherstellung

PLANBARER PREIS
- Transparentes Preismodell
- Einzigartig, schnell, bezahlbar & kosteneffektiv

MADE IN GERMANY
- EU-DSGVO-konform
- DTS Private Cloud

PROVIDING THE MISSING LINK
- Sukzessive Beseitigung von „blinden Flecken“ durch Purple Teaming

KONTINUIERLICHE VERBESSERUNG
- Enge Zusammenarbeit, um eine optimale Sicherheitsstrategie zu entwickeln
- Regelmäßige Purple Team Trainings messen Reifegrad der Incident Response & optimieren diesen

HERSTELLERUNABHÄNGIGKEIT
- Verbindungswerkzeug & Schutz getätigter Investitionen

SECURITY SOFTWARE BY DTS SINCE 2001
- Über 1.000 Kunden nutzen unsere eigenen Softwarelösungen!
- Über 750 Kunden nutzen IT-Security Soft wareprodukte „Made by DTS“!
- 24/7/365 Services!

4 SOC-EU-STANDORTE
- Überwachung Ihrer IT-Infrastruktur rund um die Uhr
- Herford, Hamburg, Athen, Thessaloniki
- Hochqualifizierte & erfahrene SOC-Analysten

DTS NETWORK INSIGHTS
- Transparenz im Netzwerk durch Netzwerk-Monitoring

ERFÜLLUNG VON NIS2, KRITIS & NIST COMPLIANCE-MASSNAHMEN
- Incident Management: Erkennung, Analyse, Eindämmung & Reaktion in einer Lösung
- Business Continuity Management: Geschäftskontinutät mit DTS Incident Response
- Cyber Risk Management: Aufbau & Bewertung von Maßnahmen durch DTS Purple Teaming
- Hosting in DE & Erbringung aus EU

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.

MANGELNDE TRANSPARENZ UND VERANTWORTLICHKEIT

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

VERZERRUNGEN

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

KOSTEN UND RESSOURCENBEDARF

Die Entwicklung und Implementierung von KI 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 und so Endpoint, Network und Cloud Detection vollständig abzudecken. 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 %igen 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

EVOLUTION DER CYBER SECURITY - DTS COCKPIT: DIE SECURITY OPERATIONS PLATTFORM

Das Herzstück unserer Security Operations Plattform ist der *DTS Cockpit Fusion Hub* mit unserem einzigartigen Purple Teaming als Basis. Es ist für Unternehmen jeder Größe geeignet, die mehrere Sicherheitslösungen im Einsatz haben und ihre bestehende IT-Infrastruktur transparenter gestalten möchten. Wir bieten „Sehen. Verstehen. Agieren. Validieren. Optimieren." als besonderen bezahlbaren Service: Ihre Sicherheitsarchitektur gebündelt auf einer zentralen Plattform, herstellerunabhängige Integration und Orchestrierung von führenden Data Collectoren & Managern, vollständige Transparenz, lückenlose Detection & Response, direkte Aktionen und Steuerung, erfahrenes und eingespieltes 24/7 SOC-Experten-Team, ARP-GUARD NAC, alles als Managed Service. Wir entlasten Sie maßgeblich, damit Sie sich auf Ihr Kerngeschäft konzentrieren können.

Und was, wenn wir Ihnen sagen, dass unser Cockpit nur der Anfang einer IT-Security-Reise mit DTS ist? Wir verkaufen Ihnen nicht einfach „ein Produkt" und danach viele weitere. Wir stellen Ihnen eine Sicherheitsplattform bereit, die wir in sämtliche IT-Security-Bereiche dediziert erweitern können – mit Lösungen und Services nach einem klaren Sicherheitskonzept. In diesem Sinne ist eine Security Operations Plattform in der heutigen Cyberwelt nicht nur wichtig, sondern unverzichtbar. Eine Investition in die DTS Security Operations Plattform ist eine Investition in die Zukunft -*„ready for take off"* mit DTS Cockpit!

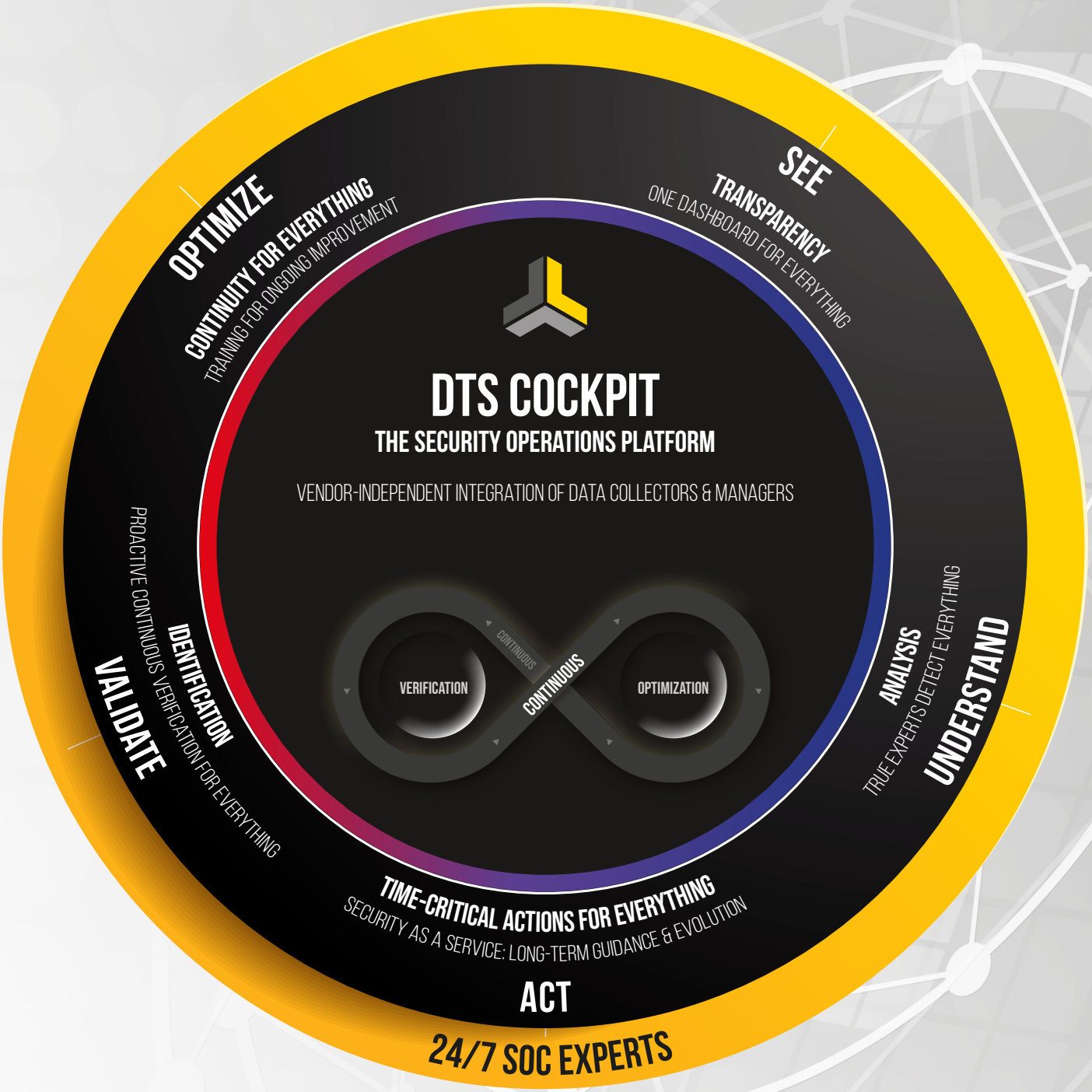
IHRE VORTEILE AUF EINEN BLICK:

Das DTS Cockpit hat einen klaren Fokus: vom Mittelstand für den Mittelstand! Wir ermöglichen Security Operations ...

... von einem EU-Anbieter, in der EU betrieben
... welches sich dem Mittelstand anpasst und nicht umgekehrt
... mit eigenen Top-Experten im SOC, Incident Response & Purple Teaming
... mit wirklicher Sichtbarkeit und Fachexpertise, die versteht was sie sieht
... mit wirklicher Handlungsfähigkeit
... welches Ihr Sicherheitsniveau auf ein neues Level hebt und gleichzeitig Ihr Team entlastet
... welches in zahlreichen Aspekten einzigartig und besonders am Markt ist
... ohne „Kleingedrucktes", als All-in-One und Easy to Use & Easy to Pay in einem ganzheitlichen 24/7 Managed Service vereint!

ARE YOU READY FOR TAKE OFF WITH DTS COCKPIT?

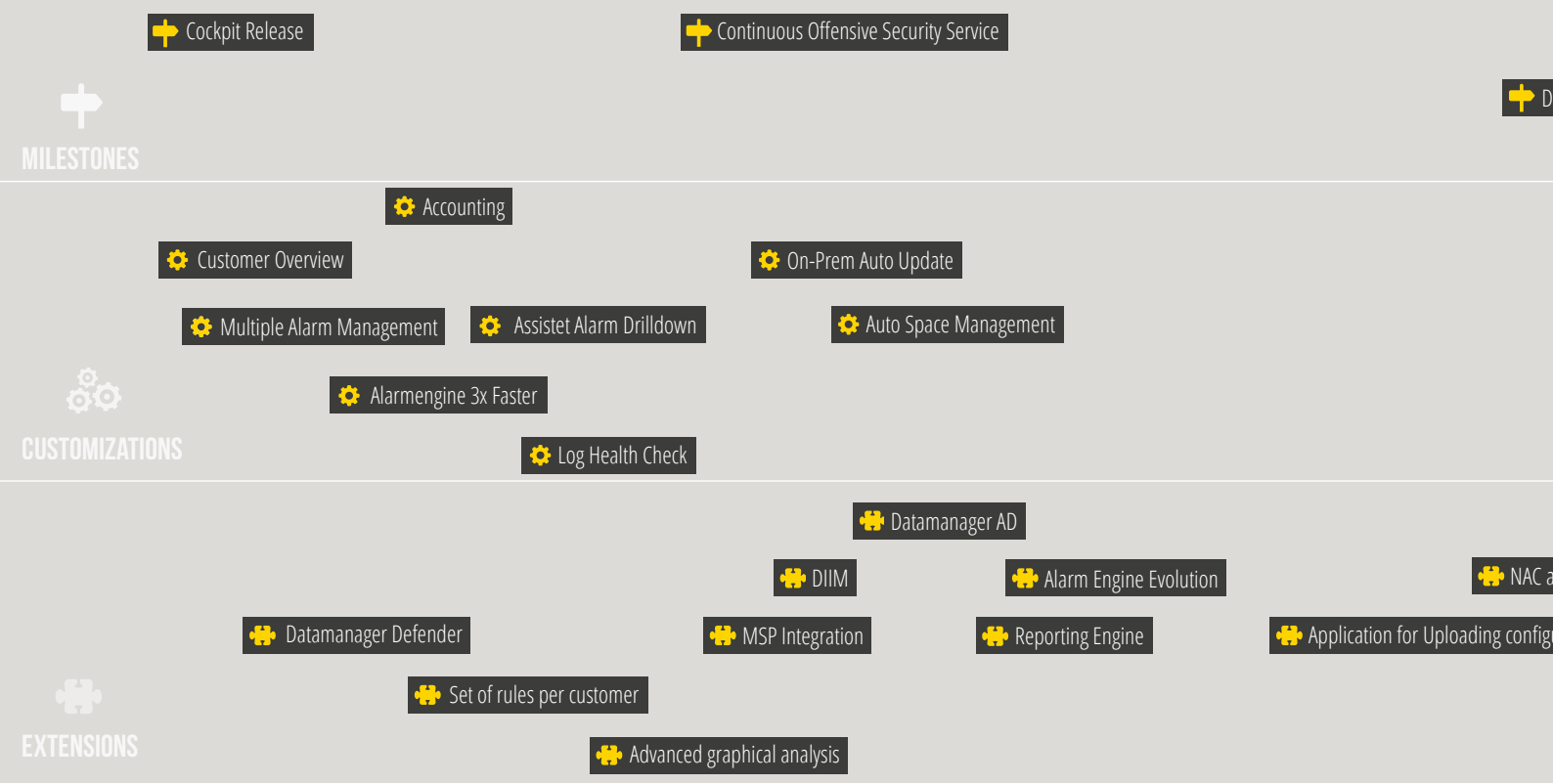
Steigen Sie mit uns ins Cockpit und machen Sie sich bereit für einen Flug in die Zukunft!


SEE
TRANSPARENCY
ONE DASHBOARD FOR EVERYTHING
UNDERSTAND
ANALYSIS
TRUE EXPERTS DETECT EVERYTHING
VALIDATE
IDENTIFICATION
PROACTIVE CONTINUOUS VERIFICATION FOR EVERYTHING
OPTIMIZE
CONTINUITY FOR EVERYTHING
TRAINING FOR ONGOING IMPROVEMENT
DTS COCKPIT
THE SECURITY OPERATIONS PLATFORM
VENDOR-INDEPENDENT INTEGRATION OF DATA COLLECTORS & MANAGERS
VERIFICATION
CONTINUOUS
CONTINUOUS
OPTIMIZATION
TIME-CRITICAL ACTIONS FOR EVERYTHING
SECURITY AS A SERVICE: LONG-TERM GUIDANCE & EVOLUTION
ACT
24/7 SOC EXPERTS

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. So entwickeln wir fortlaufend unsere Security Operations Plattform weiter. Seien Sie gespannt!



“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.

DTS Incident Response Services

DTS Client | DTS Cockpit 2.0

TS Network Insights

DTS Cockpit OT-Modul

DTS Client Integration | Einbindung in die neue DTS Security Plattform

Aktualisiertes Fusion Hub Dashboard

Neuer Data Manager SentinelOne

Weiterentwicklung von Network Insights

Fokus von derzeit Log-Centric hin zu Device-Centric

s a Service

uration files to Logstash

2024	2024	2024	2024	2025
QUARTAL 1	QUARTAL 2	QUARTAL 3	QUARTAL 4	

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de