DIE LÖSUNG IM ÜBERBLICK

Threat Detection & Hunting

Die Erkennung komplexer Angriffe erfordert eine umfassende Sichtbarkeit in alle Bereiche der eigenen IT-Infrastruktur. Profitieren Sie von bestmöglicher Transparenz, um stets einen Schritt voraus zu sein.

Schnelle Erkennung für eine schnelle Behebung

Bei Angriffen und Bedrohungen kommt es vor allem auf schnelle Erkennung an. Daher überwacht unser Managed Security Service *Threat Detection & Hunting (TDH)* den Sicherheitsstatus Ihrer IT-Umgebung rund um die Uhr, erkennt und bewertet Gefährdungen, und liefert qualifizierte Warnungen mit Empfehlungen zur Abwehr.

Ein umfassendes Lagebild über alle Domänen

Angriffe können ihren Ursprung in den verschiedensten Bereichen innerhalb und außerhalb Ihres Unternehmens haben. Deshalb binden wir Ihre Security-Systeme an unsere zentrale Analyse-Plattform an. Auf diese Weise kann unser Team aus Expert:innen potenzielle Bedrohungen über ihr gesamtes Netzwerk hinweg erkennen, bewerten und Sie in der Behebung unterstützen.

Maximale Sicherheit, minimierter Aufwand

Nicht jede Bedrohung hat den gleichen Stellenwert. Risikogetriebene Differenzierung und Priorisierung sind essenziell, um zeitnah auf kritische Bedrohungen reagieren zu können. Durch exklusive Threat Intelligence und smarte Threat Hunting-Mechanismen hilft unser Managed Security Service dabei, Ihren Aufwand zu reduzieren.

Ihre Vorteile auf einen Blick

24/7-Überwachung
Dank verlässlicher Rund-um-die-Uhr-Überwachung Ihrer Systeme können Sie sicher sein, zu jeder Zeit über kritische Alarme informiert zu werden.

Maximaler Datenschutz
Unsere Servicearchitektur speichert Ihre Daten in Ihrer eigenen Infrastruktur und überträgt nur alarmrelevante Informationen. TDH wird, zertifiziert nach ISO 27001 und TISAX, aus Berlin erbracht.

Exklusive Threat Intelligence
Dank der DCSO Community und unserem exklusiven Netzwerk verfügen wir über Zugang zu aktuellsten und für den deutschen Markt relevantesten Bedrohungsinformationen.

DCSO

Endpunkte als Einfallstor

Ihre Endpunkte sind kontinuierlich das Ziel von Angriffen. *TDH for Endpoint* nutzt etablierte Endpoint Detection & Response-Tools, um Sicherheitsvorfälle zu erkennen, korrelieren und analysieren. Im Falle einer Kompromittierung stoppen wir den Angriff, um Ihnen Zeit zur Reaktion zu verschaffen.

Volle Transparenz Ihres Datenverkehrs

Angreifende umgehen zunehmend Endpunkt-basierte Abwehrmaßnahmen. *TDH for Network* untersucht Ihren Netzwerkverkehr und relevante Log-Dateien auf Kompromittierung. Dadurch spüren wir gezielt Angriffs-muster auf und stellen zeitnah fundierte Handlungs-empfehlungen bereit.

Erstklassige Netzwerksensorik

Unsere Hochleistungs-sensoren überwachen Ihren Datenverkehr und suchen nach Bedrohungsindikatoren, die ständig aktualisiert werden.
Dank der exklusiven Kombination aus frei verfügbaren sowie vertraulichen Quellen sichern unsere Sensoren Ihre Netzwerkverkehr bestmöglich ab.

Von Erkennung bis Remediation

Alarmierung

Angeschlossene Sicherheitssysteme melden einen Alarm an das DCSO Security Operations Center (SOC). Das SOC stellt den Kontext und die Anreicherung von Warnmeldungen sowohl automatisiert als auch durch Analyst:innen bereit. Dabei kommen aktuelle Bedrohungsdaten, Informationsdatenbanken (z. B. passive DNS) und weitere Datenquellen zum Einsatz. Dieser Analyseprozess erfolgt rund um die Uhr.

Automatisierte Analyse

Unsere Sicherheitsplattform ordnet den Alarm automatisch in den Kontext ein und ermittelt den Schweregrad. In diesem Schritt korrelieren wir Warnungen über alle angeschlossenen Ereignisquellen hinweg. Unser Team reichert diese Warnungen mit zusätzlichen Datenquellen sowohl aus der Kundeninfrastruktur als auch aus externen Quellen an.

Manuelle Analyse

Die erfahrenen DCSO-Analyst:innen bewerten die Warnung und bestätigen den Schweregrad. Durch die manuelle Bewertung, die ebenfalls 24/7 erfolgt, erzeugen wir ein vollständiges Lagebild.

Alles im Überblick

Bei unmittelbaren Bedrohungen ergreifen wir Maßnahmen, um Ihre Systeme zu schützen und den Angriff zu stoppen. Die bedrohungsspezifischen Tickets erhalten Sie in Ihrer Case-Management-Lösung, über die Sie mit unseren Analyst:innen kommunizieren und zusätzliche Empfehlungen anfordern können. Die Tickets enthalten:

- Analyse der Warnung
- Bewertung der Priorität
- Direkt umsetzbare Empfehlungen zur Bedrohungsbekämpfung
- Auflistung der betroffenen Ressourcen und der für die Erkennung genutzten Mittel

TDH Complete

TDH for **Endpoint**

+

TDH for **Network**

Umfassende Sicherheit für Ihr Unternehmen

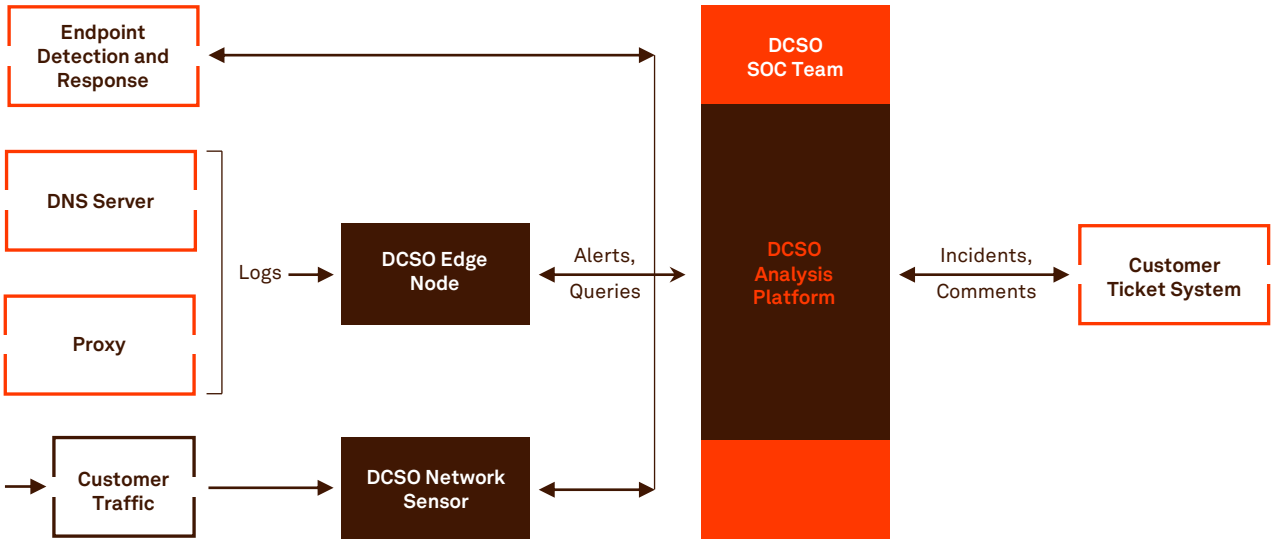
Unsere Komplettlösung *TDH Complete* ermöglicht die Korrelation von Endpunkt- und Netzwerkdaten sowie zusätzlicher Kontextinformationen für maximale Sichtbarkeit und effiziente Gefahrenabwehr. Dazu gehört auch, dass wir Bedrohungen verlangsamen bzw. eindämmen, indem wir in Ihrer IT-Umgebung aktiv werden. Bei Erkennung von auffälligem Verhalten greifen wir ein und isolieren z. B. die betroffenen Endgeräte oder sperren kompromittierte Konten – so können Bedrohungen proaktiv vermieden werden. Ganz nach Ihrem Bedarf können Sie aber auch auf unsere einzelnen Servicemodule *TDH for Endpoint* und *TDH for Network* zurückgreifen.

Unterstützte Produkte

Alarmquellen	Log- und Datenquellen	Ausgehende Anbindungen
Microsoft Defender for Endpoint	Zscaler Internet Access	Atlassian Jira
Crowdstrike Falcon Endpoint	DNS und Proxy Server	ServiceNow-Plattform
DCSO Managed Visibility	fakultativ weitere Datenquellen	API

Servicearchitektur

Alle Systeme werden mit der zentralen, von uns betriebenen Security Operations Center (SOC)-Plattform verbunden, um eine quellenübergreifende Analyse von Sicherheitsereignissen zu ermöglichen. Mithilfe dieser SOC-Plattform bewerten erfahrene DCSO-Analyst:innen potenzielle Bedrohungen über alle angeschlossenen Quellen hinweg.



DCSO

Threat Detection & Hunting

Optimale Transparenz, um Angreifenden stets einen Schritt voraus zu sein.

- 24/7-Beobachtung für schnelle Reaktion
- Maximale Sicherheit, dank erstklassiger Netzwerksensorik
- Alarme und Handlungsempfehlungen direkt in Ihr Case-Management-System
- Erfahrene Analyst:innen plus exklusive Threat Intelligence
- Cybersicherheit von der deutschen Wirtschaft für die deutsche Wirtschaft

Warum DCSO?

Seit 2015 bietet die DCSO modernste Threat Intelligence-, Incident Response- und Managed SOC-Services sowie Technologieberatung an und ist nach ISO 27.001 und TISAX zertifiziert.

- SOC-Betrieb in Berlin
- Vier Millionen aktive IoCs
- Fünf aktive Communities mit 100 Treffen im Jahr

ISO 27001 Zertifiziertes Informationssicherheits-Managementsystem
www.tuev-sued.de/ms-zert

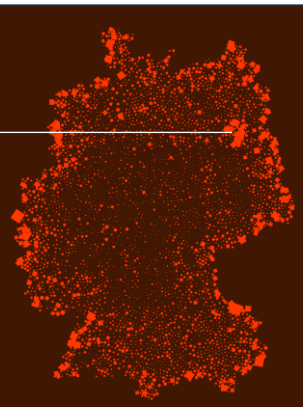
SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

Allianz für Cyber-Sicherheit Partner

Diese Unternehmen vertrauen der DCSO

Allianz · BASF We create chemistry · BAYER · VOLKSWAGEN AKTIENGESELLSCHAFT

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
EUREF-Campus 22
10829 Berlin
sales@dcso.de



Erfahren Sie mehr auf dcso.de