SOLUTION OVERVIEW

Threat Detection & Hunting

Detecting complex attacks requires comprehensive visibility across all areas of your IT infrastructure. Benefit from maximum transparency to always stay one step ahead.

Fast detection for fast remediation

Fast detection is what matters most in case of attacks and threats. Our Managed Security Service Threat Detection & Hunting (TDH) monitors the security status of your IT environment 24/7, detects and assesses threats, and issues qualified alerts with remediation recommendations.

A coherent picture across all domains

Attacks can originate from a wide variety of sources inside or outside your company. That's why we connect your security systems to our central analysis platform. This enables our team of experts to detect and assess potential threats across the entire network and integrate appropriate notifications directly into your remediation processes.

Maximum security, minimized effort

Not all threats are created equal. Therefore, risk-driven differentiation and prioritization are essential for a prompt reaction to critical threats. With exclusive threat intelligence and smart threat hunting mechanisms, our managed security service reduces efforts at your end.

Your benefits at a glance

24/7 monitoring

You will be informed about critical alerts at any time thanks to reliable round-the-clock monitoring of your systems.

Maximum data protection

Our service architecture stores your data in its own infrastructure and transmits only relevant information. Certified according to ISO 27001 and TISAX, TDH is provided from Berlin.

Exclusive Threat Intelligence

Thanks to the DCSO Community and our exclusive network, we have access to the latest threat intelligence which is most relevant to the German market.

DCSO

Endpoints are entry points

Endpoints often are the first targets of an attack. *TDH for Endpoint* leverages established endpoint detection and response tools to identify, correlate, and analyse security events. It also enables rapid triage in the event of a compromise.

Full data traffic transparency

Attackers increasingly circumvent endpoint-based defense. *TDH for Network* examines network traffic and relevant log files. This enables a targeted detection of attack patterns and the timely provision of sound advice for quick, targeted remedial action.

Cutting-edge network sensor technology

Our high-performance sensors monitor your traffic and seek threat indicators which are constantly updated.
Thanks to the exclusive combination of freely available as well as confidential sources, our sensors provide maximum security for your network traffic.

From detection to remediation

Alert notification

Connected security systems report an alert to the DCSO Security Operations Center (SOC). The SOC provides context and enrichment of alerts both automatically and through analysts. This involves the use of current threat data, information databases (e.g., passive DNS) and other data sources. The analysis process runs 24/7.

Automated analysis

Our security platform automatically contextualizes the alert and determines the severity. In this step, we correlate alerts across all connected event sources. Our team enriches these alerts with additional data sources from both the customer infrastructure and external sources.

Manual analysis

Our expert analysts assess the alert und confirm its severity. Through this manual assessment, which is also conducted 24/7, we produce a comprehensive picture of the situation.

Keeping everything in view

In case of immediate threats, we take action to protect your systems and stop the attack. You receive threat-specific tickets via your case management solution which you can use to communicate with our analysts and request additional recommendations. The tickets include:

- Alert analysis
- Priority assessment
- Actionable recommendations for threat remediation
- List of affected resources and means used for detection

TDH Complete

TDH for **Endpoint**

+

TDH for **Network**

Comprehensive security for your business

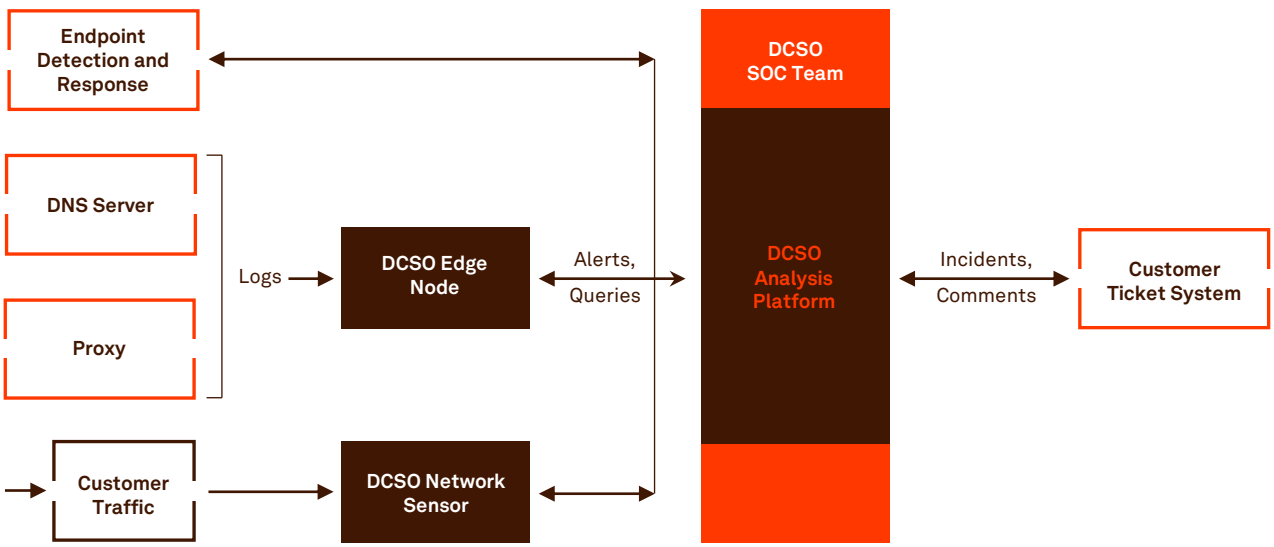
Our all-in-one solution *TDH Complete* correlates endpoint and network data as well as additional contextual information for maximum visibility and efficient threat prevention. This includes slowing down or mitigating threats by becoming active in your IT environment. If suspicious behavior is detected, we will take action and, for instance, isolate the affected devices or block compromised accounts – this way, threats can proactively be prevented. However, you can also draw on our individual service modules *TDH for Endpoint* and *TDH for Network*, depending on your business' specific needs.

Compatible products

Alert sources	Log and data sources	Outbound connections
Microsoft Defender for Endpoint	Zscaler Internet Access	Atlassian Jira
Crowdstrike Falcon Endpoint	DNS and proxy servers	ServiceNow Platform
DCSO Managed Visibility	Further optional data sources	API

Service architecture

All systems are connected to the central DCSO-operated Security Operations Center (SOC) platform to allow a cross-source analysis of security events. Utilizing this SOC platform, our expert analysists assess potential threats across all connected sources.



DCSO

Threat Detection & Hunting

Maximum transparency to always stay one step ahead of attackers

- 24/7 monitoring for rapid reaction
- Maximum security thanks to cutting-edge network sensor technology
- Alerts and recommended actions directly in your case management system
- Expert analysts plus exclusive threat intelligence
- Cyber security by the German economy for the German economy

Why DCSO?

Since 2015, DCSO offers state-of-the-art threat intelligence, incident response and managed SOC services as well as technology consulting and is certified according to ISO 27.001 and TISAX.

- SOC operation in Berlin
- Four million active IoCs
- Five active communities with 100 meetings per year

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

These companies trust DCSO

Allianz · BASF We create chemistry · BAYER · VOLKSWAGEN AKTIENGESELLSCHAFT

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

Learn more at dcso.de