

– Presseinformation der Controlware GmbH –

**Controlware bietet maßgeschneidertes Threat Hunting als Managed Service an**

**Dietzenbach, 3. August 2022 – Controlware erweitert das Portfolio von Cyber Defense Services: Der Systemintegrator und IT-Dienstleister unterstützt seine Kunden mit maßgeschneiderten Threat Hunting Services bei der proaktiven Suche nach bislang unentdeckten Angreifern im Netzwerk.**

Jedes Unternehmen kann heute in das Visier von Hackern, Wirtschaftsspionen oder Erpressern geraten – und wenn diese einmal ins Netzwerk eingedrungen sind, ist das Schadenspotenzial enorm: „Cyberkriminelle versuchen heute, möglichst lange unentdeckt zu bleiben. Sie bewegen sich lateral durch die Umgebung, öffnen zusätzliche Hintertüren und eskalieren geduldig ihre Rechte, bis sie Zugang zu den wertvollsten Assets erhalten“, beschreibt Benjamin Heyder, Cyber Defense-Experte bei Controlware, die Anatomie moderner Angriffe. „Nach aktuellen Schätzungen bleiben Angreifer heute im Schnitt zwei Monate unentdeckt – und können in dieser langen Zeitspanne sehr viel Schaden anrichten. Um das zu verhindern, unterstützen wir unsere Kunden mit passgenauen Threat Hunting Services bei der Lokalisierung von cyberkriminellen Aktivitäten in ihren Netzwerken, und helfen ihnen, diese zeitnah zu stoppen.“

Im Rahmen der Threat Hunting Services stellt Controlware den Kunden ein Team erfahrener Security-Experten zur Seite, die die Aktivitäten und Vorgänge im Netzwerk analysieren und mit bekannten Tools, Techniken und Prozessen (TTPs) der Angreifer abgleichen. Die Analysten nutzen dabei leistungsfähige KI-gestützte Analyse-Technologien, um die neuralgischen Punkte im Netzwerk zu überwachen. Hierzu gehören insbesondere:

- Lösungen für **Endpoint Detection and Response (EDR)**, die die Endpoints im Netzwerk durchgehend auf Anhaltspunkte für cyberkriminelles Verhalten überwachen
- Lösungen für **Cross-Layered Detection and Response (XDR)**, die Netzwerk- und Security-Systeme überwachen und Metadaten wie E-Mails und Cloud-Workloads auswerten

Die mit diesen Technologien gesammelten Informationen werden mit umfangreicher Threat-Intelligence führender Hersteller angereichert und mit den im MITRE ATT&CK Framework dokumentierten TTPs abgeglichen. Automatisierte Analysen der Daten ermöglichen es den Experten im Controlware Cyber Defense Center anschließend, Hinweise auf eine erfolgreiche Kompromittierung zu identifizieren und die Cyber-Bedrohungen im Netzwerk zuverlässig zu lokalisieren und abzuwenden.



Benjamin Heyder erklärt: „Threat Hunting entwickelt sich immer mehr zu einem zentralen Baustein moderner Security-Architekturen – ist aber sowohl mit Blick auf die technologischen Komponenten als auch mit Blick auf die Daten-Analyse eine überaus anspruchsvolle Disziplin. Erfahrungsgemäß tun sich selbst erfahrene Security-Teams oft schwer damit, die Flut an eingehenden Threat-, Kontext- und Log-Informationen in geordnete Bahnen zu lenken und auszuwerten. Managed Services sind hier eine sehr gute Alternative: Es muss weder internes Know-how aufgebaut noch in eigene Hardware- oder Software-Lösungen investiert werden – und trotzdem mit der Gewissheit, dass Angreifer im Netzwerk nicht lange unentdeckt bleiben.“

### **Hintergrund: Das Controlware Cyber Defense Center (CDC)**

Controlware betreibt ein eigenes ISO 27001-zertifiziertes Cyber Defense Center in Deutschland, das Kunden bei der Erkennung, Bewertung und Abwehr von Cybergefahren unterstützt. Zu den im CDC bereitgestellten Cyber Defense Services gehören beispielsweise Vulnerability Management Services, Log-Analysen, EDR-Services und Dienstleistungen im Bereich Threat Detection. Das Portfolio ist modular aufgebaut und bietet Kunden die Möglichkeit, ihre Leistungspakete individuell zusammenzustellen und am konkreten Schutzbedarf auszurichten. Dabei können die Angebote auch flexibel mit weiteren Leistungen aus den Bereichen Systemintegration und Beratung kombiniert werden.

Mehr Informationen unter: <https://www.controlware.de/services/cyber-defense-services.html>

### **Über Controlware GmbH**

Die Controlware GmbH, Dietzenbach, ist mit mehr als 800 Mitarbeitern und einem Umsatz von ca. 330 Mio. Euro einer der führenden unabhängigen Systemintegratoren und Managed Service Provider in Deutschland. Das 1980 gegründete Unternehmen entwickelt, implementiert und betreibt anspruchsvolle IT-Lösungen für die Data Center-, Enterprise- und Campus-Umgebungen seiner Kunden. Das Portfolio erstreckt sich von der Beratung und Planung über Installation und Wartung bis hin zu Management, Überwachung und Betrieb von Kundeninfrastrukturen durch das firmeneigene ISO 27001-zertifizierte Customer Service Center. Zentrale Geschäftsfelder der Controlware sind die Bereiche Network Solutions, Collaboration, Information Security, Application Delivery, Data Center & Cloud sowie IT-Management. Controlware arbeitet eng mit national und international führenden Herstellern zusammen und verfügt bei den meisten dieser



Partner über den höchsten Zertifizierungsgrad. Das starke Unternehmen unterhält ein flächendeckendes Vertriebs- und Servicenetz mit 16 Standorten in DACH.

Im Bereich der Nachwuchsförderung kooperiert Controlware mit renommierten deutschen Hochschulen und betreut durchgehend um die 50 Auszubildende und Studenten. Zu den Unternehmen der Controlware Gruppe zählen die Controlware GmbH, die ExperTeach GmbH, die Networkers AG und die productware GmbH.

**Pressekontakt:**

Stefanie Zender  
Controlware GmbH  
Tel.: +49 6074 858-246  
Fax: +49 6074 858-220  
E-Mail: [stefanie.zender@controlware.de](mailto:stefanie.zender@controlware.de)  
[www.controlware.de](http://www.controlware.de) (Homepage)

**Agenturkontakt:**

Michal Vitkovsky  
H zwo B Kommunikations GmbH  
Tel.: +49 9131 812 81-25  
Fax: +49 9131 812 81-28  
E-Mail: [michal.vitkovsky@h-zwo-b.de](mailto:michal.vitkovsky@h-zwo-b.de)  
[www.h-zwo-b.de](http://www.h-zwo-b.de) (Homepage)

