MANAGED SECURITY SERVICES

FERNAO

endpoint detection & response (EDR)

IHRE VORTEILE

- → Intelligente Malware-Erkennung und umfassende, automatisierte Analysen
- → Threat Analysten Team für die manuelle Untersuchung
- → Optional: Inkludierte Next Generation AV-Lösung
- → Reduzierung der administrativen Aufwände
- → Einfache Verwaltung durch zentrale Plattform
- → Monatliche Reports
- → 24x7x365 Service – Active Monitoring und Case Management
- → Datenspeicherung und Betrieb in zertifizierten Rechenzentren in Europa

DIE WICHTIGEN VORTEILE DES FERNAO ENDPOINT DETECTION & RESPONSE SERVICES AUF EINEN BLICK

- → Analyse von Ereignissen durch Spezialisten
- → Erweiterung des vorhandenen signaturbasierten AV-Schutzes
- → Entlastung der IT-Ressourcen
- → Schnelle Reaktion auf Incidents
- → Direkte Eingrenzung von betroffenen Systemen

SCHÜTZEN SIE IHRE SYSTEME IMMER NOCH MIT SIGNATURBASIERTER ANTI-VIREN-SOFTWARE? GAB ES BEREITS EINEN RANSOMEWARE AUSBRUCH?

Klassische Anti-Viren-Programme erkennen Viren, Mal- und Ransomware anhand bekannter Signaturen. Schon die kleinsten Veränderungen am Programm- bzw. Schadcode reichen daher aus, um unerkannt ins Unternehmen zu gelangen und damit erheblichen Schaden anzurichten. Schadprogramme ändern sich permanent und daher sind signaturbasierte AV-Lösungen nicht mehr ausreichend.

Endpoint Detection & Response Lösungen gehen einen Schritt weiter. Neben der reinen signaturbasierten Prüfung erfolgt eine zusätzliche tiefere Überprüfung auf Basis moderner und intelligenter Technologien und der menschlichen Komponente. Threat-Analysten reagieren proaktiv auf Incidents und untersuchen kritische Ereignisse auf Auswirkung und Schadenpotenzial. Nur so ist ein Schutz vor den so genannten Zero Day Angriffen möglich. Der Fokus liegt **weniger auf Prävention**, sondern auf der **Detektion und Reaktion**.

FERNAO **endpoint detection & response** wird in zertifizierten, europäischen Rechenzentren betrieben. Mithilfe fortschrittlicher Analyse-Methoden wie maschinellem Lernen, werden Verhaltensmuster bisher unbekannter Dateien untersucht, so dass potenzielle Malware rechtzeitig erkannt und deren Verbreitung unterbunden werden kann. Bei der Analyse und Bewertung neuer Funde unterstützen Sie die Experten des Professionell Service von magellan netzwerke und Cybereason.

Ablauf

- → Initiales Rollout durch Cybereason
- → Übergabe an Cybereason MDR Essentials
- → 24x7 Case Management
- → Mitteilung bei kritischen Incidents durch Cybereason
- → Automatisches Threat Hunting
- → Monatliche detaillierte Management Reports mit Findings

Sowohl FERNAO **endpoint detection & response** als auch FERNAO **managed threat detection & alerting** haben als Ziel, bisher unbekannte Malware zu erkennen und deren Ausbreitung zu verhindern, jedoch mit völlig unterschiedlichen Technologien. Mit einer Kombination aus beiden Services erreichen Sie eine Effektivität, die weit über traditionelle Branchenlösungen hinausgeht, die heute bei Unternehmen, Behörden und Institutionen weltweit im Einsatz sind.

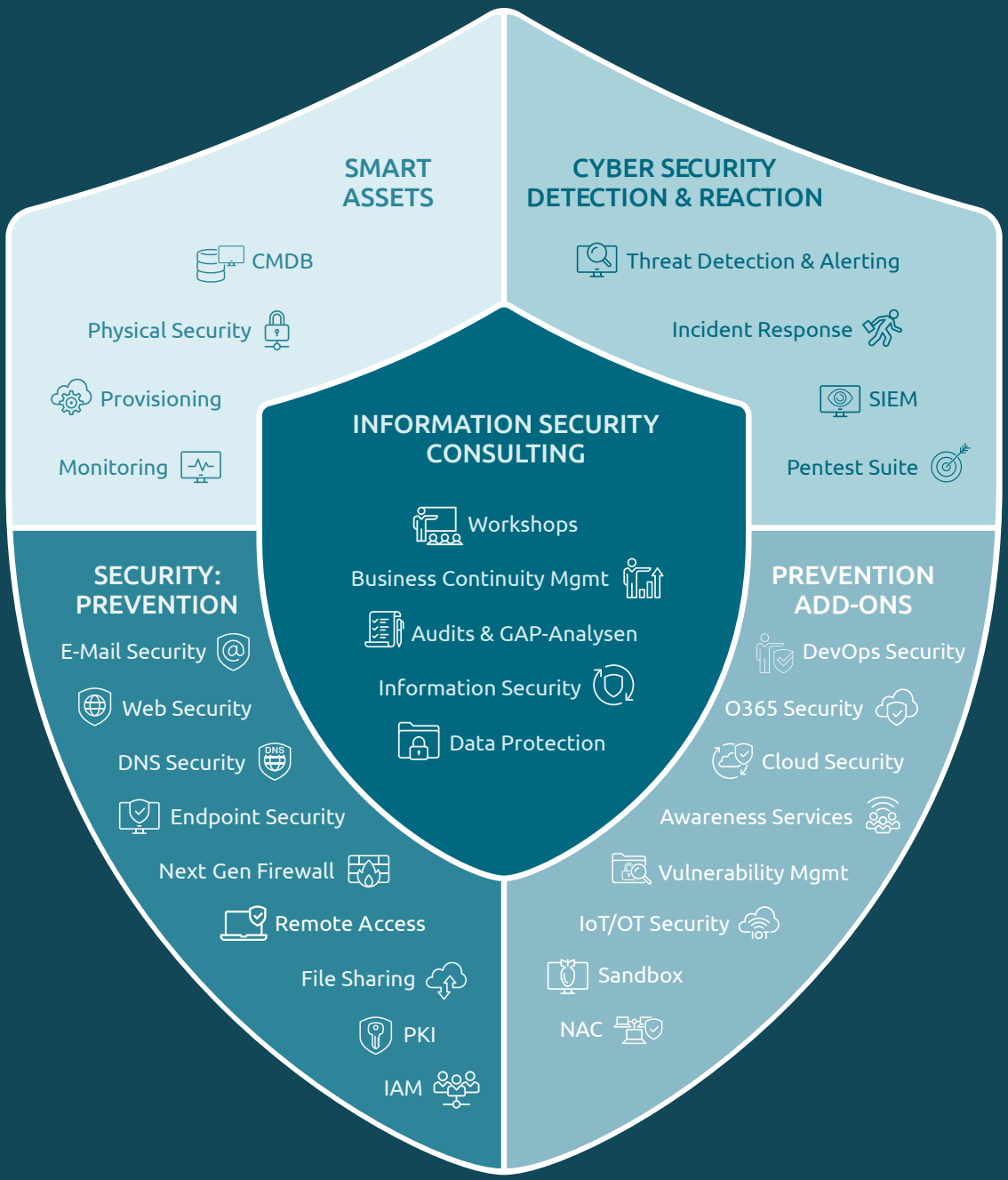
FERNAO Networks GmbH
Albin-Köbis-Straße 5 | 51147 Köln
+49 2203.92263-1 | info@fernao.com

FERNAO NETWORKS

MANAGED SECURITY SERVICES

Genügend Zeit und immer die richtige fachliche Ressource verfügbar haben: Das sind großen Herausforderungen der heutigen Unternehmens IT. Zu diesem Zweck haben wir unser Cyber Defense and Operation Center (CDOC) stetig weiterentwickelt. Vom qualifizierten 24x7 Support über einer Reihe von Hosting- und Management Services bis hin zu unseren Managed Security Services (MSS) verfolgen wir nur ein Ziel: Unseren Kunden die Arbeit zu erleichtern und dabei entsprechend Ihren Anforderungen zu skalieren. Im Fokus unserer Arbeit steht dabei stets die Minimierung des Risikopotentials Ihrer Organisation.

MANAGED SECURITY SERVICES SHIELD



FERNAO Networks GmbH
Albin-Köbis-Straße 5 | 51147 Köln
+49 2203.92263-1 | info@fernao.com

cloud services MADE IN GERMANY

FERNAO NETWORKS