EnBW Cyber Security

Monitoring und Detection Services

Security-Suite innerhalb einer IT-Landschaft durch Analyse von Logdaten, Machine-Learning und Data-Enrichment

- **Erkennung und Monitoring von potenziellen Sicherheitsvorfällen (SIEM)**
  - Hohe Anzahl sicherheitsrelevanter Logquellen, z.B. Windows, Linux, Anti-Virus Software
  - Systematische Loganalyse in Echtzeit auf Basis von Mitre & Attack-Framework
- **Advanced Threat Protection Agent (ATD / UEBA / XDR)**
  - Erkennung von Angriffsmustern auf Basis der Cyber-Kill Chaine
  - Detektion durch Anomalie-Erkennung und Baselining Verfahren
- **Threat Intelligence und Data Enrichment (TI)**
  - Anreicherung von sicherheitsrelevanten Ereignissen durch zeitnahe Informationen (first day)
  - Tiefere Analysen und Quellen zur Bewertung eingehender sicherheitsrelevanter Ereignisse
- **Hohe Transparenz durch hohe Integration des Kunden**
  - Security-Kundencockpit mit allen relevanten Informationen und Tickets
  - Mitwirkung bei der Ticketbearbeitung durch Handlungsempfehlungen und regelmäßige Servicemeetings
- **Eingehende Alarme werden durch Fachspezialisten analysiert und bewertet.**

Zielgruppe

Große Systemlandschaften

Mittelständische Unternehmen

Energie- und Wasserversorger sowie KRITIS-Unternehmen

Kundenmehrwert

Daten bleiben beim Kunden

Hohe Transparenz

Starke Security-Suite aus einer Hand

Partizipation am Security Operations Center der EnBW

Preismodell

in Abhängigkeit von Größe und Wachstum (Pay As You Grow)

Software oder Hardware Appliances

EnBW Cyber Security GmbH
Ein Unternehmen der EnBW
Durlacher Allee 93
76131 Karlsruhe

www.enbw.com/cybersecurity
cybersecurity@enbw.com
0800 0 KRITIS