

Kundenreferenz

Umsetzung der KRITIS Anforderungen im Gesundheitswesen

Endpoint Protection, Detection & Response im Managed Service 24x7



Auf einen Blick

Kunde:
DRK Blutspendedienst
Baden-Württemberg - Hessen
gemeinnützige GmbH

Branche:
Healthcare

Firmensitz:
Mannheim, Deutschland

- Leistungen:**
- Managed Threat Detection [endpoint] 24x7)
 - Managed Endpoint Security [protect]
 - Threat Hunting

Deutsches Rotes Kreuz 
DRK-Blutspendedienst
Baden-Württemberg | Hessen
gemeinnützige GmbH

Das Unternehmen

Der DRK-Blutspendedienst Baden-Württemberg - Hessen und seine Tochtergesellschaft DRK-Blutspendedienst Nord-Ost gemeinnützige GmbH sind der größte Verbund der DRK-Blutspendedienste in Deutschland. In Baden-Württemberg und Hessen sind wir für die Versorgung der Kliniken und Praxen mit Blutpräparaten zuständig. An den Standorten Baden-Baden, Frankfurt, Kassel, Mannheim und Ulm unterhält der DRK Blutspendedienst Baden-Württemberg - Hessen eigene Institute. In Kooperation mit der Uniklinik Tübingen wird das Zentrum für klinische Transfusionsmedizin betrieben, in Heidelberg zusammen mit dem Universitätsklinikum Heidelberg das Institut für Klinische Transfusionsmedizin und Zelltherapie Heidelberg. Bundesweit sind sechs DRK-Blutspendedienste in der Versorgung der Bevölkerung mit Blutpräparaten tätig.

Ausgangssituation

Der Kunde hat eine Plattform gesucht, die sich zusammen mit den zu erbringenden Betriebsleistungen einfach in die bestehende Infrastruktur integrieren lässt und KRITIS Anforderungen hinsichtlich Datenschutz und Datenhaltung erfüllt.



Das sagt der Kunde:

» Im Rahmen der selbst durchgeführten Tests haben uns die hohe Erkennungsrate und der aktuelle technologische Stand des Systems überzeugt. Mit den dazu passenden umfassenden Managed Security Services sehen wir uns bestens gegen Cyberangriffe gewappnet! «

Eingesetzte Software:

- Cybereason Enterprise

Lösung

Im Rahmen eines Evaluierungsprozesses wurden verschiedene Hersteller technisch beleuchtet. Dabei überzeugte Cybereason vor allem in den beiden Punkten Installation/Deployment, als auch in der einfachen Übersicht und Detailtiefe der gelieferten Angriffsinformationen.

Durch den Betrieb und die Analyse der aufkommenden Events durch das Orange Cyberdefense Team konnten die Erkennungs- und Antwortzeiten drastisch reduziert werden. Darüber hinaus erhöht sich das Schutzniveau gegenüber der vorher eingesetzten NextGen AV signifikant, besonders gegenüber Ransomware und Datenverlust.

Vorteile

Die KRITIS Anforderungen hinsichtlich Datenschutz und Datenhaltung sind erfüllt und der Betrieb erfolgt DSGVO-konform aus Deutschland heraus. Die Host Cross Correlation reduziert die Anzahl der Incidents und damit den erzeugten Aufwand signifikant.

Die Lösung mit dem Service hat ein gutes Verhältnis von Aufwand und Schutzfunktion und bietet einen zuverlässigen Schutz vor Ransomware und Datenverlust ohne großen internen Aufwand.

Über Orange Cyberdefense

Orange Cyberdefense ist eine Geschäftseinheit der Orange Group, welche sich der Cybersecurity widmet. Als führender Anbieter für Cybersecurity ist unser Bestreben eine sichere digitale Gesellschaft aufzubauen. Wir bieten unseren Kunden Consulting, Solutions und Managed Security Services. Speziell mit unseren Managed Detection & Response und Threat Intelligence Services helfen wir unseren Kunden Bedrohungen zu erkennen, Risiken zu identifizieren und auf Vorfälle angemessen zu reagieren. Mit über 2.100 Mitarbeitern in weltweit 19 Ländern sind wir stets dort, wo unsere Kunden uns brauchen. Erfahren Sie mehr auf unserer Website.

