SVA REFERENZ-PROJEKT //
BARMHERZIGE BRÜDER KRANKENHAUSVERBUND

GEWAPPNET GEGEN CYBER-ANGRIFFE: ELASTIC SIEM FÜR KRITIS

Der Krankenhausverbund der BarmHERZigen Brüder setzt auf eine skalierbare Lösung und SVA Expertise.

AUF EINEN BLICK

AUFGABE

Aufbau einer SIEM-Lösung (Security Information and Event Management) zur Angriffserkennung

SYSTEME UND SOFTWARE

> Elastic Security

VORTEILE

> Schrittweise Einführung und Wissenstransfer im Projektverlauf

> Kosteneffiziente, skalierbare End-to-end Security für SIEM, SOAR, EDR/XDR, Threat Intelligence und Cloud Security

> Alles aus einer Hand von SVA

BARMHERZIGE BRÜDER KRANKENHAUSVERBUND

Mit seinen Krankenhäusern in München, Regensburg, Schwandorf und Straubing bietet der Krankenhausverbund der BarmHERZigen Brüder mit 2.150 Planbetten eine qualitativ hochwertige Patientenversorgung für die Region. Spitzenmedizin trifft bei den Barmherzigen Brüdern Menschlichkeit. Denn der zentrale Ordenswert ist die Hospitalität, die gelebte Gastfreundschaft. Der Mensch steht stets im Mittelpunkt. Hochleistungsmedizin wird mit einem ganzheitlichen Verständnis des Menschen verbunden.

HINTERGRUND: SICHERE KRITIS

Betreiber kritischer Infrastrukturen (KRITIS) sind gemäß IT-Sicherheitsgesetz verpflichtet, ab dem 01.05.2023 Systeme zur Angriffserkennung (SzA) einzusetzen. Diesen Standards wollte auch der Krankenhausverbund entsprechen und zudem sollten aufgrund der allgemeinen und perspektivisch steigenden Bedrohungslage umgehend geeignete Maßnahmen implementiert werden. Dabei war es wichtig, dass das interne Team für Security Operations (SOC) zukünftig die neue Lösung selbst betreiben kann.

LÖSUNG: SIEM MIT ELASTIC

Als langjähriger IT-Partner des Krankenhausverbunds der BarmHERZigen Brüder wurde die SVA für das Konzept, die Implementierung und den Anlaufbetrieb eines passenden SzA ausgewählt. Im ersten Schritt lag der Fokus auf einer effizienten Einführung, bei der die Evaluierung relevanter Use Cases, Datenanbindung und Datenhaltung und die Gesamtarchitektur mit Ausfallsicherheit, Erweiterbarkeit und Automatisierung einbezogen wurden. Mit der Entscheidung für die Plattform Elastic SIEM wird der hausinternen IT ein umfassendes Werkzeug an die Hand gegeben, mit dem die IT-Umgebung effizient überwacht und gesichert wird.

BARMHERZIGE BRÜDER
Krankenhausverbund

elastic

VEREINFACHTE ADMINISTRATION

Elastic bietet nicht nur eine umfassende Automatisierung mit der zentralen Management-Komponenten ***Fleet***, die die Konfigurierung und Steuerung aller Elastic Agents einfach und schnell über die Weboberfläche von Kibana ermöglicht. Dank Endpoint Security (EDR/XDR) mit ***Elastic Defend*** stehen außerdem Funktionen für die Prävention, Echtzeit-erkennung und Reaktion auf Bedrohungen zur Verfügung, ergänzt durch ***Elastic Threat Intelligence*** als Plattform für Bedrohungserkennung und -analyse. Aus den ca. 700 von Elastic bereitgestellten ***Detection Rules*** wurden – maßgeschneidert und effektiv – die für die Lösung des Krankenhausverbundes relevanten ausgewählt und mit umgebungs-spezifischen ergänzt.

Die Implementierung und Einführung der neuen Lösung umfasste im Verlauf von sechs Monaten die Anbindung von unterschiedlichsten Datenquellen, verteilt über rund 1.000 Server, Netzwerk- und Endnutzergeräte über alle Unternehmens-Standorte hinweg. Es werden nun täglich etwa zwei Milliarden neue Events mit einem geplanten Datenvolumen von 120 TB ausgewertet, im Elastic SIEM Cluster auf zehn Elasticsearch-Servern verteilt. Durch diese Verteilung wird eine maßgeschneiderte Skalierbarkeit und Performance geboten, die steigenden Datenraten und Anforderungen problemlos begegnen kann. Darüber hinaus erhöht der Clusteransatz die Ausfallsicherheit, da die Daten beim Ausfall eines Servers weiterhin auf anderen verfügbar sind. Da die Architektur zudem die Verar-beitungsleistung und -geschwindigkeit optimiert, wird auch die Bearbeitung von Abfragen der Security-Analysten im SOC in Echtzeit gewährleistet.

WISSENSTRANSFER UND SVA KNOW-HOW

Dank des Wissenstransfers durch die SVA Experten im Projektverlauf ist das SOC-Team des Krankenhausverbunds der BarmHERZigen Brüder nun in der Lage, das SIEM-System und den Elastic Stack selbst weiter zu betreiben und zukünftige Use Cases eigenständig umzusetzen. Dazu zählt unter anderem die Anbindung von zusätzlichen Datenquellen, die Erstellung von Visualisierungen und Dashboards sowie die Umsetzung von Detection Rules und Alerts.

Die maßgeschneiderte Plattform Elastic SIEM bietet dem Krankenhausverbund der BarmHERZigen Brüder nun ein kosteneffizientes Fundament für eine vollumfassende Sicherheitslösung, die das SOC-Team befähigt, auch in Zukunft einen sicheren IT-Betrieb zu gewährleisten.

KONTAKT
SVA System Vertrieb
Alexander GmbH
Borsigstraße 26
65205 Wiesbaden
Tel. +49 6122 536-0
mail@sva.de
www.sva.de

BARMHERZIGE BRÜDER
Krankenhausverbund

elastic