Anwenderbericht

Infrastruktur mit Durchblick

HENSOLDT Optronics GmbH

Sitz in Oberkochen

ca. 450 Mitarbeiter

vormals: Airbus DS Optronics GmbH

Entwicklung, Herstellung und Vertrieb von optronischen Geräten und Systemen von höchster Präzision und Zuverlässigkeit.

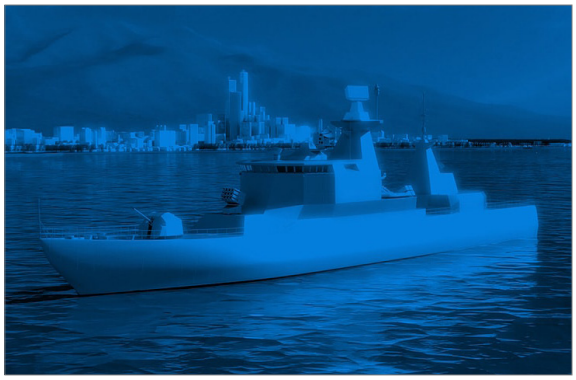
Anwenderbericht HENSOLDT Optronics GmbH

Im Jahr 2016 entscheidet sich die HENSOLDT Optronics GmbH dazu, **eine SIEM-Lösung zu implementieren**. Ausschlaggebend für diese Entscheidung ist das Outtasking der IT-Sicherheitsinfrastruktur an die Thinking Objects GmbH, in dessen Rahmen die Notwendigkeit von Sicherheitssensoren für das Netzwerkmonitoring klar wird.

HENSOLDT – Innovationen für eine sicherere Welt

HENSOLDT ist ein **globaler Pionier der Technologie und Innovation** im Bereich der Verteidigungs- und Sicherheitselektronik. Das Unternehmen zählt zu den Marktführern auf dem Gebiet ziviler und militärischer Sensorlösungen und entwickelt auf der Basis disruptiver Ansätze für Datenmanagement, Robotik und Cyber-Sicherheit neue Produkte zur Bekämpfung der steigenden Bedrohungen. HENSOLDT erzielt mit etwa 4.300 Mitarbeitern einen Jahresumsatz von rund 1 Milliarde Euro.

Das **Portfolio von HENSOLDT umfasst verschiedene Sensortechnologien**, deren Kombination eine erhebliche Steigerung der Detektionsleistung mit sich bringt. HENSOLDT ist unter anderem in folgenden Bereichen tätig: Schutz von Grenzen und kritischen Infrastrukturen, Flugabwehr, Missionsmanagement, Selbstschutz von Luftfahrzeugen, Fahrzeug- und Konvoischutz, Signalaufklärung und Datenlinks sowie Nachtsichtgeräte, Laserentfernungsmesser und optronische Zieleinrichtungen. Daneben umfasst die HENSOLDT-Produktpalette auch Missionsavionik, wie etwa Avionikcomputer, Missionsplanungs- und Autopilotsysteme.



Präzise Informationen und klare Sicht.

HENSOLDT deckt mit seinem breit gefächerten Portfolio alle Verteidigungs- und Sicherheitsmissionen ab und sichert die Überlegenheit seiner Kunden bei der Überwachung des gesamten elektromagnetischen Spektrums. Die **Lösungen des Unternehmens werden auf verschiedenen Plattformen eingesetzt**, darunter Hubschrauber, Flugzeuge, Drohnen, Schiffe, U-Boote, Panzerfahrzeuge und Satelliten.

Gesamtüberblick der Basisinfrastruktur

Ziel von HENSOLDT Optronics ist es, **mit Hilfe von Sicherheitssensoren das Netzwerkmonitoring zu verbessern**. Um dieses Ziel zu erreichen, schlägt die Thinking Objects eine SIEM-Lösung von LogRhythm vor.

Ein SIEM (Security Information and Event Management) setzt auf einem Log Management auf. Es korreliert die Daten verschiedener Log-Quellen und erkennt aufgrund dieser Korrelation verschiedene sogenannte „Events". Diese werden anschließend durch das SIEM aufgrund ihrer Kritikalität bewertet. Je nach Bewertung lösen **hoch kritische Sicherheitsvorfälle dann einen Alarm aus, um den vordefinierten Einsatzplan zu starten**.

Aufgrund der erfolgreichen Zusammenarbeit im vorhergehenden Projekt entscheidet sich die HENSOLDT Optronics dafür, die Thinking Objects auch mit der Umsetzung des anstehenden Projekts zu beauftragen.

„Die notwendige Phase der intensiven Auseinandersetzung mit unseren eigenen Anforderungen und Risiken hat uns darüber hinaus die gewünschte höhere Sensibilität für das Thema Sicherheit verschafft – eine günstige Nebenwirkung."

Jochen Scheuerer, Head of IT Optronics, Head of Infrastructure and IT Operation HENSOLDT Group

Erfolgsfaktoren:

- **Zukunftsorientierung** der implementierten Lösung
- Ermittlung des **individuellen Use-Case** des Kunden
- Erfolgreiche **Zusammenarbeit bereits im vorherigen Projekt**
- Regelmäßige **Prüfung, Analyse, Bewertung und Kategorisierung** möglicher IT-Sicherheitsrisiken oder Auffälligkeiten bereits während des Projektes

Im Firmennetzwerk von HENSOLDT Optronics gibt es **zum Startzeitpunkt des Projekts bereits eine zuverlässige Basissicherheit**. Da es vor allem im Bereich der Verteidigungs- und Sicherheitselektronik besondere Anforderungen zu beachten gilt (z.Bsp. Exportkontrolle), soll die vorhandene Sicherheit weiter erhöht werden. Vor allem ein ausgeprägtes Reportingwesen ist dabei von hoher Wichtigkeit. Mit Hilfe eines SIEM wird **eine übersichtliche Aufarbeitung der Daten gewährleistet**, was mehr Transparenz und schnelleres Reagieren ermöglicht.

Feinjustierung während des Projekts

Den Wünschen des Kunden, beispielsweise Datenströme zu überwachen, **Fehlkonfigurationen aufzudecken und unerwünschte Netzwerkaktivitäten zu unterbinden**, wird mit der SIEM-Lösung optimal entsprochen.

Die Anbindung der erforderlichen Log-Quellen und die Anpassung von Filtern, Dashboards und Alarmierungen werden von Thinking Objects für den Kunden eingerichtet und ausgewertet. **Dies dient dem Ziel das Netzwerkmonitoring übersichtlicher zu machen** und unterstützt somit auch ein proaktives Handeln.

Darüber hinaus beinhaltet der Service der Thinking Objects schon während der Projektumsetzung regelmäßige Prüfung, Analyse, Bewertung und Kategorisierung möglicher IT-Sicherheitsrisiken oder Auffälligkeiten anhand des LogRhythm SIEM-Dashboards. In einem kontinuierlichen Verbesserungsprozess werden Anforderungen abgeleitet und sofort umgesetzt. Zusätzlich wird im Rahmen des Projekts **ein Reportingwesen für die ISO 27001-Konformität und NIST Compliance** etabliert.

Herausforderung individueller Use Case

Eine Herausforderung besteht anfänglich darin, den für den Kunden individuellen Use Case aufzuzeigen. Dieser zeigt die **individuellen Anforderungen des Kunden sowie mögliche Lösungen** auf.

Der individuelle Anwendungsfall wird von Thinking Objects entwickelt und letztendlich während eines einwöchigen Proof-of-Concept dem Kunden erfolgreich präsentiert.

Die Einführung einer SIEM-Lösung stellt sowohl den Dienstleister als auch den Kunden vor die Herausforderung, sich **intensiv mit möglichen Risiken und Herausforderungen der internen IT-Sicherheit zu befassen**. Die Kenntnis hiervon und die Befähigung, passende Abfrage- und Abwehrmechanismen zu entwickeln, tragen maßgeblich zum Erfolg des Projekts bei.

Basisbetrieb und Managed SIEM Services

Nach erfolgreichem Abschluss des Projekts betreibt Thinking Objects für HENSOLDT Optronics **eine LogRhythm Appliance mit derzeit zehn Systemmonitoren** für die Standorte Oberkochen und Irene/Südafrika.

High Performance Technologie

Dabei wird der Basisbetrieb SIEM und ergänzend die Managed SIEM Services **im Rahmen des bestehenden Outtasking-Vertrags für IT-Sicherheitsinfrastrukturen übernommen.**

Während der Basisbetrieb regelmäßige Updates der eingesetzten Systeme enthält, bietet Thinking Objects ihrem **Kunden im Rahmen der Managed SIEM Services proaktive Alarmierung bei relevanten Sicherheitsvorfällen** im HENSOLDT-Netzwerk durch die Thinking Objects SIEM-Analysten. Dies wird zukünftig durch SIEM Add-Ons ergänzt. Dabei werden, ergänzend zum Basisbetrieb und den Managed SIEM Services, neue Log-Quellen gefunden und analysiert.

Nachhaltige Zusammenarbeit

Bereits beauftragt ist der Basisbetrieb SIEM durch Thinking Objects für 36 Monate. Ebenso sind **ergänzende Managed SIEM Services für 36 Monate und ein Dienstleistungskontingent von 20 Personentagen pro Jahr** für SIEM-Projektdienstleistungen geplant.

Weiterhin steht die Zusammenarbeit für diverse Infrastrukturthemen, wie **Endpoint Protection und Firewall NG** an.

Projektübersicht

Projektverantwortung:	Oliver Paukstadt, Thinking Objects GmbH (Projektleitung) Bernd Maier, Thinking Objects GmbH (Kundenbetreuung) Jochen Scheuerer, HENSOLDT Optronics GmbH (Head of IT Optronics, Head of Infrastructure and IT Operation HENSOLDT Group)
Lösungen und Produkte:	LogRhythm All-in-One Appliance, 3 Jahre Subscription
Zeitplan:	Juli 2016: Projektstart November 2017: Übernahme in den Betrieb

Firmenporträt Thinking Objects GmbH

Die inhabergeführte Thinking Objects GmbH mit Sitz in Korntal bei Stuttgart ist seit 1994 als kompetenter IT-Dienstleister und Systemintegrator mit den Schwerpunkten IT-Sicherheit, IT-Infrastruktur, Internet-Technologie sowie Betrieb und Support in Rechenzentren tätig.

Seit über 20 Jahren bietet Thinking Objects marktgerechte Lösungen zur Unterstüzung, Entlastung, Optimierung und Sicherung des IT-Betriebs in großen und mittelständischen Unternehmen sowie Konzernen.

Umfangreiche Betriebs- und Supportservices, die vom technisch qualifizierten Helpdesk bis zur vollständigen Ausgliederung der Betriebsverantwortung für die IT-Infrastruktur des Kunden reichen, sowie die Bereitstellung von IT-Fachkräften für den variablen Personalbedarf – von der zertifizierten Arbeitnehmerüberlassung bis hin zum Personal-Recruiting – runden das Leistungsspektrum der Thinking Objects GmbH ab.

Thinking Objects

Thinking Objects GmbH
Lilienthalstraße 2/1
70825 Korntal-Münchingen

+49 711 88770400
info@to.com
www.to.com