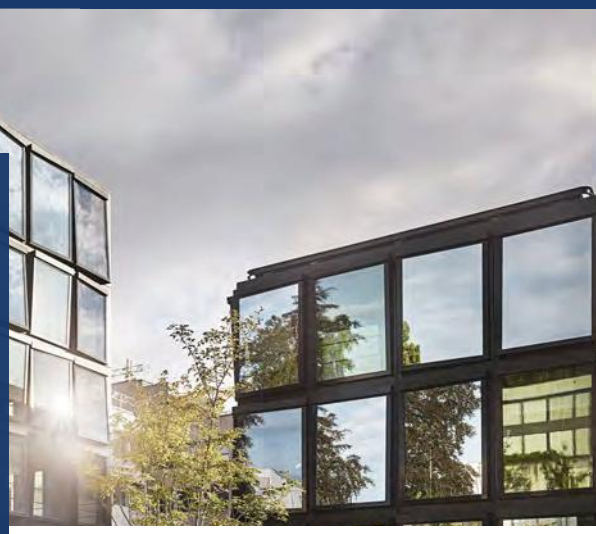
LC SYSTEMS

THE DATA COMPANY

Success Story



Vertrauenssache:

Helvetia übergibt die Analyse von Cyber-Anomalien an LC Systems

helvetia

Helvetia Gruppe
Helvetia Versicherungen mit Sitz in St. Gallen hat sich seit 1858 zu einer erfolgreichen Versicherungsgruppe mit über 12'000 Mitarbeitenden und mehr als 7 Millionen Kundinnen und Kunden entwickelt. Mit Begeisterung entwickelt und erschliesst Helvetia Geschäftsmodelle und treibt das eigene Geschäft kraftvoll und zukunftsgerichtet voran. Sie handelt in all ihrem Wirken vorausschauend und verantwortungsvoll: zugunsten ihrer Aktionäre, ihrer Kundinnen und Kunden und Mitarbeitenden sowie ihrer Partner, der Gesellschaft und Umwelt. In der Schweiz ist Helvetia die führende Schweizer Allbranchenversicherung. Im Segment Europa mit den Ländern Deutschland, Italien, Österreich und Spanien verfügt das Unternehmen über fest verankerte Marktpositionen für überdurchschnittliches Wachstum. Im Segment Specialty Markets bietet Helvetia weltweite massgeschneiderte Spezial- und Rückversicherungsdeckungen an. Bei einem Geschäftsvolumen von CHF 11.1 Mrd. erzielte Helvetia im Geschäftsjahr 2022 ein IFRS-Ergebnis nach Steuern von CHF 614.4 Mio. Die Aktie der Helvetia Holding AG wird an der Schweizer Börse SIX Swiss Exchange gehandelt.

LC Managed Security Service: vom SIEM zum SOAR
Im Jahr 2022 beauftragte Helvetia LC Systems als Managed Security Service Provider (MSSP), die Bearbeitung von Security Alerts auf Level Tier 1 zu übernehmen. Vor der Übernahme des Services wurden in einer Einführungsphase 5'000 Security Alerts pro Monat verifiziert, normalisiert und qualifiziert. Dadurch konnten nach Abschluss dieser Phase die Alerts auf 1'000 pro Monat reduziert werden.

Diese 1'000 Security Alerts decken verschiedene IT-Sicherheitsthemen ab, darunter:

- Client Security (Endpoint Detection & Response sowie Antivirus)
- Netzwerk Security (Network Detection & Response)
- Cloud Security (Office 365, Sentinel, GuardDuty)
- SIEM Use Cases

Daraufhin hat LC Systems eine SOAR-Plattform (Security Orchestration, Automation and Response) aufgebaut, um zukünftig die Security Workflows zu orchestrieren und Aufgaben zu automatisieren.

Diese Plattform ermöglicht eine effiziente Analyse und Bearbeitung von Sicherheitsvorfällen von einer zentralen Oberfläche aus. Dabei werden Entscheidungen und Massnahmen teilweise automatisiert durchgeführt.

Ein wichtiger Bestandteil der SOAR-Plattform bilden dabei die Working Instructions und Playbooks. Zunächst wurden spezifische Anleitungen für die zehn am häufigsten auftretenden Vorfälle erstellt, implementiert, getestet und automatisiert. Zudem bietet die zentralisierte Plattform ein umfassendes Reporting und

gewährleistet die Nachvollziehbarkeit der durchgeführten Massnahmen. Dies ist insbesondere als Nachweis für das Sicherheits-Management, Audit und Behörden wie die FINMA von grosser Bedeutung. Die transparente Dokumentation und die Möglichkeit, Berichte in Echtzeit zu generieren, stellen sicher, dass Helvetia den immer stringenteren regulatorischen Anforderungen im Bereich Cyber entspricht.

> «Zum Schutz der Helvetia ist neben dem umfassenden Sicherheitsdispositiv insbesondere eine effektive Überwachung, frühzeitige Erkennung und schnelle Reaktion matchentscheidend.»
>
> Peter Imhof, Chief Security Officer, Helvetia

LC Systems erbringt diesen Managed Security aus der Schweiz heraus mit eigenem qualifizierten und zertifiziertem Personal. Durch die enge Zusammenarbeit werden kontinuierlich neue Anforderungen umgesetzt. Durch diese Agilität konnten weitere wiederkehrende Vorfälle identifiziert und optimiert werden, um entsprechende Entscheidungen und Handlungen zu unterstützen. Die Implementierung einer zentralisierten SOAR-Plattform hat die Effizienz und Effektivität des Incident Managements weiter gesteigert.

Der Ursprung: vom betrieblichem Monitoring zur SIEM Plattform

Seit mittlerweile über einem Jahrzehnt setzt Helvetia erfolgreich Splunk zur effizienten Verarbeitung ihrer Logdaten ein. Die Plattform hat sich seit Beginn als äusserst vielseitig erwiesen und lieferte grossen Mehrwert in den Bereichen IAM, Application Monitoring und Reporting. Von Anfang an durfte LC Systems Helvetia beim Aufbau dieser Plattform unterstützen.

Helvetia hat LC Systems vor über drei Jahren beauftragt, ihre Splunk Plattform zu betreiben und kontinuierlich weiterzuentwickeln. Dies insbesondere im Bereich Security / SIEM, um gegenüber den steigenden Cyber-Bedrohungen gewappnet zu sein und den höheren Security-Auflagen gerecht zu werden.

Im Rahmen dieser Zusammenarbeit wurden kontinuierlich neue Datenquellen angebunden, einschliesslich Netzwerkdaten durch die Implementierung der NDR-Lösung Vectra. Darüber hinaus wurden zahlreiche neue Use Cases umgesetzt, bei denen Aspekte wie Cloud-Sicherheit, Audit-Anforderungen und FINMA-Vorgaben berücksichtigt wurden. Dadurch hat sich die Plattform zu einer Bereichs- und Linienübergreifenden Lösung entwickelt, welche die Nutzung von Synergien bei der Analyse von Log-Daten zu operativen und Cyber Security Zwecken optimal und unter Einhaltung strenger regulatorischer Auflagen ermöglicht. Helvetia konnte sich dabei stets auf einen Partner verlassen, der sowohl die Business- als auch die technologischen Anforderungen versteht und erfolgreich umsetzen kann.

> «LC Systems bietet uns einen echten Mehrwert bei der frühzeitigen Erkennung von Cyber-Bedrohungen. Wir schätzen insbesondere die flexible und enge Zusammenarbeit sowie die Kombination von Serviceintegration, aktuellem Cyber Know-How und pragmatischen Lösungsansätzen.»
>
> Dr. Bastian Schäfer, Head Group Cyber Defense, Helvetia

Durch diesen gemeinsamen Effort und die Integration der LC Security App, die von Haus aus mehr als 700 Use Cases gemäss dem MITRE ATT&CK Framework mitbringt und die bestehenden SIEM Use Cases ergänzte, stand Helvetia bereits frühzeitig ein umfassendes und lösungsorientiertes Detection Framework zur Verfügung. Diese Fortschritte haben dazu beigetragen, dass Helvetia effektiv potenzielle Cyber-Bedrohungen frühzeitig erkennen und geeignete Massnahmen ergreifen kann.

> «Der kombinierte Ansatz mit unseren professionellen Cyber Defense Center Services und den ergänzten LC Systems Basis Managed Security Services hat sich schon mehrfach bewährt und substantielle Incidents konnten so vermieden werden.»
>
> Peter Imhof, Chief Security Officer, Helvetia

LC Systems-Engineering AG . Zum See 1 . CH-9320 Arbon . Telefon +41 (0)58 360 80 60 . info@lcsystems.ch . www.lcsystems.ch
Office Basel: Reinacherstr. 129 . CH-4053 Basel . Tel. +41 (0)58 360 89 00 **Office Bern:** Schwarztorstr. 9 . CH-3007 Bern . Tel. +41 (0)58 360 84 00