Case Study

Global Travel Leader Optimizes Security With Azure Sentinel and Managed Security Services

The client

For more than 100 years, the company has produced high-quality, innovative travel accessories that celebrate design and technology. The company sells products to more than 100 countries worldwide and employs more than 14,000 people.

The challenge: Reduce alerts and fatigue and improve global threat intelligence without going over budget

The company leveraged a traditional Security Information and Event Management (SIEM) solution and a third-party managed security services provider. However, they believed that both the technology and provider offered little real value. There continued to be an excessively high number of alerts, leading to alert fatigue and misused resources, with no ability to correlate signals and alerts from devices across their IT environment.

While the company hoped to find a new solution and provider that would optimize resources more efficiently and provide more security intelligence, the bottom line was a nonnegotiable factor. The travel industry has been sizably impacted by the COVID-19 outbreak and its aftermath. Any additional costs needed to be well justified.

Industry:

Travel

CDCT provided:

- Strategic engagement reviewing business and security objectives and requirements
- Solution demo, design, and architecture
- Customized implementation plan spanning 4 global regions
- Azure Sentinel deployment and executive training
- Onboarding to Managed Security services and continued optimization

CDCT services:

- Security services
- Managed Security services

The solution: Tailored architecture, implementation, and service delivery

The client wanted better actionable data from their SIEM solution and managed services provider. They needed a complete solution that was scalable to their global footprint. They also needed to ensure any investments were aligned with modified budgets to ensure the business remains viable throughout and beyond the pandemic.

After preliminary conversations reviewing requirements, capabilities, implementation, and a solution demo, the client decided to move forward with Managed Security services from Insight Cloud + Data Center Transformation (CDCT). Our services leverage a combination of automated tools within Azure Sentinel™, ServiceNow®, and threat intelligence feeds, and the expertise of our security analysts and threat hunters. Of particular interest to the client were the machine learning capabilities of Azure Sentinel, which allow our team and the client to respond to more meaningful alerts.

Services include:

- Monitoring the client's network
- Ingesting data from security appliances
- Analyzing and alerting via ServiceNow
- Investigating validated threats
- Advising on containment, remediation, and resolution steps

Prior to service rollout, we determined that the client had a primary need in the North America and Asia regions. We created an overall architecture for implementation, created and configured instances, connected data points and enabled rules, and delivered training to key personnel, followed by onboarding to Managed Security services. We are currently fine-tuning service delivery in these regions, with plans to roll out service to Europe and Latin America regions in 2021.

A robust and scalable security environment with the latest tool sets and a skilled security services team

The new solution and services are helping the client reduce risk and make security costs more predictable. Intelligent tools and an expert managed services team result in fewer alerts and less "noise" overall, letting the client stay focused on security incidents that really matter, as well as other, higher-level IT objectives. Data remains in the client's environment, alleviating data privacy concerns and reducing any risk of exposure or loss through transference. The client benefits from round-the-clock security they don't need to micromanage, with a framework that can scale to anywhere around the world.

The client has been extremely pleased with the Insight CDCT team's flexibility and depth of knowledge. The CIO reports, "From the onset, Insight demonstrated why Microsoft recommended them as their top partner for managed SIEM needs using Azure Sentinel." And the pandemic and its impacts didn't hold us back, either. "In spite of a challenging global environment, the Insight team delivered on time and on budget. We feel we've gained a lasting partnership with Insight," says the CIO.

Benefits:

Better security **on a global scale**

Fewer alerts and less "noise"

Actionable data and intelligence to improve use of resources

On-budget security solution that makes costs more predictable

Seamless transition from legacy to new SIEM

Expert team managing security environment **24/7/365**

Insight | Cloud + Data Center Transformation

insightCDCT.com | insight.com