



Case Study

# NBA Team Adopts Azure Sentinel for a Modern Security Slam Dunk

## The client

The client is a U.S. professional basketball team founded nearly 50 years ago that competes in the National Basketball Association (NBA). Although the team had limited success for many years, the past decade or so have been favorable, with more than several playoff appearances and division titles.

## The challenge: Execute a seamless transition to a new security platform

During initial client conversations it was uncovered that the team organization had a legacy Security Information and Event Management (SIEM) system they were looking to replace upon contract expiration. They were interested in adopting Azure Sentinel® to take advantage of the latest cloud-native functionality for managing their cybersecurity risk.

To put the pressure on, it was required that we execute the transition with no outages, as the move would occur during the NBA season. The project would also need to be fast-tracked. What could have easily taken eight weeks to complete would need to be done in four.

### Industry:

Professional sports

### CDCT provided:

- Custom-built Azure Sentinel environment
- Solution design, configuration, and optimization
- Transition planning for security operations
- Deployment and implementation

### CDCT services:

- Consulting Services
- Migration and Professional Services

## The solution: A customized Azure Sentinel environment for enhanced protection and incident management

The client leveraged CDCT's cloud architects to provide an accelerated implementation of Azure Sentinel for both cloud and on-premises protection of sensitive assets. Our team worked closely with Microsoft throughout the project, which enabled us to deploy the latest SIEM technology.

We performed a full investigation of the client's AlienVault® setup, including customizations and alerts. We then near-replicated the environment in Azure Sentinel, reproducing the alerts and mirroring the functionality. Together, with the client's IT department, we ensured that all AlienVault data feeds rerouted to Azure Sentinel, which required implementation of a new data forwarder using Azure® Infrastructure as a Service (IaaS).

By leveraging the client's existing technical investments and understanding the elements they wanted to stay consistent — a like-for-like environment, with improved capabilities — Insight made the changeover as seamless and cost-effective as possible.

## The benefits: Better defense, and better offense, with an intelligent and optimized security environment

The client now has a platform in which all future workloads can be secured through the dynamics of artificial intelligence at scale, automated incident response, and investigative toolsets. Their state-of-the-art SIEM and modern security operations are setting a new standard for fellow sports teams.

Their IT organization now has a better understanding of their data and unusual activity with custom reports (i.e., workbooks) in Azure Sentinel. Security data generated anywhere in their IT environment is aggregated in one centralized location for optimal visibility and analysis. More, better targeted alerts were created to help identify abnormalities and accelerate incident response.

The time it takes the client to generate a daily report of security issues has been greatly reduced, since Azure Sentinel is able to reproduce alerts that were generated in other Azure security products like Microsoft® Cloud Access Services. The efficiencies realized have enabled the client to transition two full-time employees away from hardware monitoring to solely incident management. Their overall security posture and awareness of their IT environment have heightened, to put them heads and shoulders above the rest.

### Benefits:

- Fewer manual processes for incident response
- Increased visibility via a single pane of glass
- Intelligent threat detection and hunting
- Ongoing platform improvements by Microsoft

Advanced security capabilities



Scalable, cloud-based security



Significant cost savings over time

©2020, Insight Direct USA, Inc. All rights reserved. All other trademarks are the property of their respective owners.  
CS-LAC-1.0.01.20

insightCDCT.com | insight.com