VECTRA
SECURITY THAT THINKS.®

CASE STUDY

Sports Data Company quickly identifies True Positive with Detect for AWS

Overview

This sport data analysis company, initially founded to crawl betting websites to find betting odds, now works directly with sports betting companies to run data analytics that design the odds they offer customers, to track for irregularities that suggest match fixing, and to provide their recently added video streaming services.

These activities are very computationally expensive, as complex algorithms are run across large amounts of data. To maintain a smooth operation system, the data analysis company relies on AWS to host huge amounts of proprietary information in their databases, and AWS contains their critical infrastructure. Any outage in their AWS infrastructure would render them completely unable to meet their customer contractual obligations and have a huge business impact.

It became clear they needed a better detect and response tool, and the company's team migrated to Vectra Detect for AWS, an AI-driven solution that uses behavioral models to find and stop attacks without disrupting operations.

Organization

Sports Data Analysis Company

Industry

Technology Services

Challenge

Received alerts from GuardDuty that were not actionable, leaving them with a lack of visibility in their AWS activity

Selection Criteria

An AI-driven solution that uses behavioral models to find and stop attacks without disrupting operations

Results

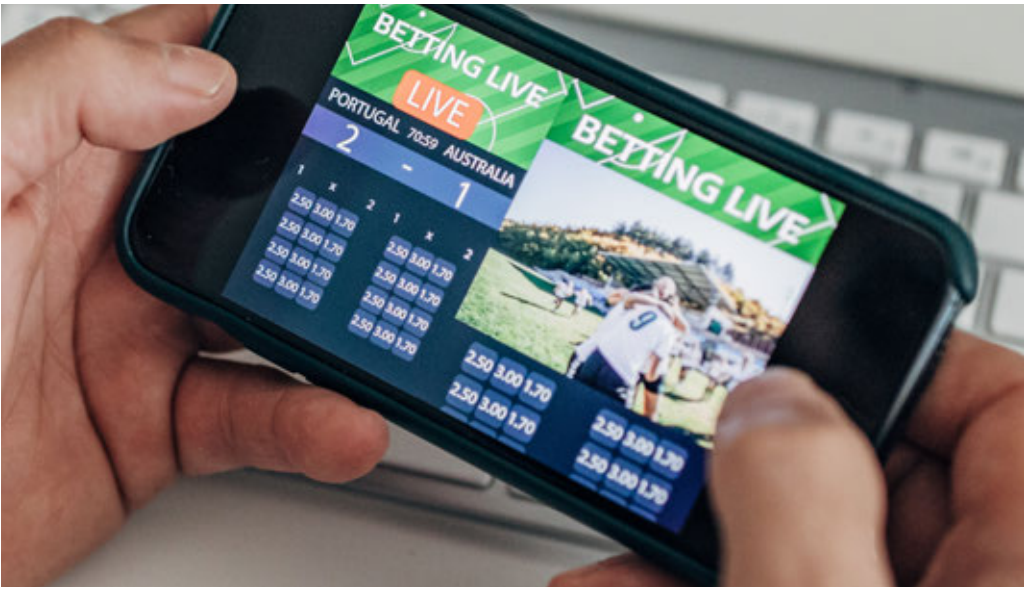
- Vectra Detect for AWS flagged a new user performing a number of highly suspicious activities, and the team later determined it was a secret pen test being performed.
- Vectra Detect for AWS spotted a True Positive where a Kubernetes cluster was making some EC2 instances publicly available over HTTPS.

Making the switch

The company runs large Kubernetes clusters in AWS, giving them huge flexibility in their org as they scale up and down to match the demand for their services. They have many EC2 instances to host these K8s clusters and use S3 buckets for storing their data and video offerings. To maintain their systems, the company has a collection of AWS admins who make hundreds of changes a day via their continuous integration platform.

To help keep an eye on things, the company used GuardDuty for detection and response in AWS. The security team received alerts from GuardDuty that weren't actionable, leaving them with a lack of visibility in their AWS activity. "They are also very reliant on Kubernetes, but don't have any visibility at all into the activity that goes on here," recalls the company's Lead SOC Analyst.

It became clear they needed a better detect and response tool, and the company's team migrated to Vectra Detect for AWS, an AI-driven solution that uses behavioral models to find and stop attacks without disrupting operations.



Detect for AWS in action

Deployment of Detect for AWS was incredibly straightforward, and Vectra immediately showed value, spotting a True Positive where a Kubernetes cluster was making some EC2 instances publicly available over HTTPS.

"It's a good catch," says their Senior Analyst. "This was actually a new kubernetes cluster, which people were migrating from one account to another, and forgot to set up the stack correctly."

> "This was actually a new kubernetes cluster, which people were migrating from one account to another, and forgot to set up the stack correctly."
>
> **Senior Analyst**
> *Sports Data Analysis Company*

"Port 443 was being opened completely to the public and in this case, it wasn't intended to expose that.

The key part was exposing this to all IPs. The service was meant to be opened just to a specific whitelisted IP in an Elastic Load Balancer, not all IPs. Which meant that anyone from any IP could have accessed all information in this Kubernetes cluster.

Thanks to that report we were able to find a significant blind spot, so we greatly appreciate Vectra for alerting us on this!"

Detect for AWS's complete visibility into their entire setup only required 10 minutes to set up and Vectra's Instant Investigation showed all the EC2's activity with 2 quick clicks. The Senior Analyst continued, "This is where I really see the value, because this is an example of a blind spot we had, which really kept me awake at night." When the analyst tried to find these activities in their AWS console, the EC2 instance wasn't listed, as it had been torn down after it had performed its migration work, which meant that without Detect for AWS, they would have never known this machine existed.

A Good Day Gets Better

As security analysts were investigating the above issue, Vectra Detect flagged a new user performing a number of highly suspicious activities which might have been related to the original incident. Even though this activity was being performed in several different regions, with different assumed identities, Vectra's Kingpin technology was able to pull all these activities back to a single actor, and the detection said exactly who this was.

A quick check of the company's org chart showed this person didn't work in the company! After contacting the audit department to ask what this might be, it turned out that Vectra had caught their secret pentest team on day 1 and raised it as a critical issue. "Really nice that you caught this, I happen to know exactly who this is, and what he's up to but it's great to see," recalled the Senior Analyst.

Control Plane Detection and Response is Key

Detect for AWS is a crucial cog in the security of this company's cloud infrastructure, offering defense in depth of the management plane as continuous integration of new configuration changes makes it impossible to proactively monitor and shut down activities.

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai