VECTRA
SECURITY THAT THINKS.®

CASE STUDY

# Telecom Provider Relies on Vectra and AWS to Stop Hidden Cyberthreats

## Executive Summary

This multinational telecommunication services company headquartered in Europe, delivers services across Asia, Africa and the European continent. It is one of the largest mobile network operators in the world based on the number of subscribers.

The telecom provider leverages Amazon Web Services (AWS) to host its data lake, which stores network traffic for security forensics and compliance reporting. They also rely on the AI-driven Cognito® threat detection and response platform from Vectra® to identify early cyberattack behaviors in cloud, data center, IoT and enterprise networks.

This enables the security team at the telecom provider to hunt proactively for hidden cyberattacks, respond faster to security incidents and conduct highly conclusive forensic investigations to prevent data breaches.

Integrating Vectra with AWS allows the telecom provider to deploy Vectra sensors that are available in the AWS marketplace into its Amazon VPCs.

### Organization

Telecommunications company

### Industry

Communications services

### Challenge

Scan and monitor multiple geographic locations and AWS virtual private clouds (VPCs)

### Selection criteria

An AI-driven threat detection solution specifically built for AWS traffic and can detect and respond to threats evading their EDR solution

### Results

- Integration between Cognito and AWS allows the company to deploy Vectra sensors in AWS virtual private clouds (VPCs)
- Complete coverage for all devices, regardless of client types
- Real-time detections as well as host threat and certainty scores from its enterprise and data center

## A Complex Network

The telecom provider's network spans more than 10 geographies and multiple Amazon virtual private clouds (VPCs). Securing and monitoring such a diverse and expansive footprint is no easy task.

As a result, the telecom provider is required to follow and operate under several different compliance policies. To support this mandate, the security team relies on their AWS-hosted ArcSight platform for big data security analytics, security information and event management (SIEM) and log management.

The telecom provider leverages the Cognito platform to collect metadata from all cloud and network traffic and enrich it with deep security insights and context about attacks. This dramatically improves threat hunting, incident response and forensic investigations.

> Deployed in AWS, the Cognito platform ensures seamless integration with ArcSight to deliver precorrelated threat detections that enable the security team to pinpoint and mitigate in-progress attacks.

The telecom provider also uses a custom parser for 15 types of metadata that are critically important.

This integration feeds real-time threat detections to the AWS-hosted ArcSight platform where they are correlated with other data such as usernames from Microsoft domain controllers.

From the ArcSight management console, the security team can quickly search for insights and context about attacks in security-enriched metadata from the Cognito platform as well as other security details.

## Strengthening EDR with NDR

Although the telecom company is running endpoint detection and response (EDR) on its managed clients, this still leaves a large security gap in visibility for IoT, unmanaged devices, BYOD, and other devices that cannot support EDR software agents.

The company chose Vectra to close this security gap. The Cognito platform detects and responds to hidden attack behaviors in all cloud and network traffic, which ensures complete coverage for all devices, regardless of client type.

## Cloud-first Deployments

The telecom company takes a cloud-first approach to its network deployment, and security is no different. ArcSight and its security orchestration, automation and response (SOAR) solution are cloud based—the company wanted a cloud-centric threat detection platform as well.

Integrating Vectra with AWS allows the telecom provider to deploy Vectra sensors that are available in the AWS marketplace into its Amazon VPCs. Traffic mirroring on Amazon Machine Images (AMIs) provides visibility into all traffic flowing in and out of VPCs as well as intercommunication. The health and status of Vectra sensors are easily monitored via Amazon CloudWatch.

Vectra uses AI-derived machine learning to detect and respond automatically to attack behaviors in cloud, data center, IoT and enterprise environments. Detected threats are automatically triaged and prioritized based on certainty and risk, giving security teams a starting point for investigations, and the context needed when threat hunting.

Cognito collects relevant logs and metadata from all traffic and enriches it with deep security insights about every threat incident. This includes attacker location and activity, compromised hosts and user identities—and can identify whether or not the threat is part of larger attack campaign.

**For more information please contact us at info@vectra.ai.**

Email info@vectra.ai  vectra.ai