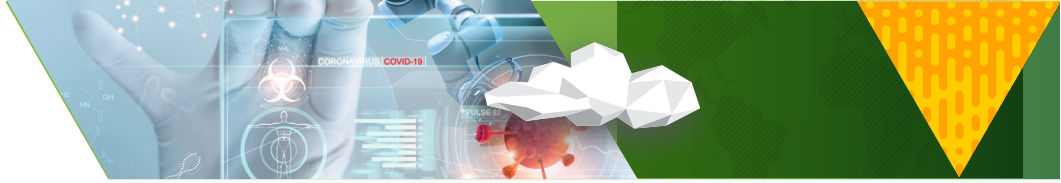
VECTRA
SECURITY THAT THINKS.®



CASE STUDY

Telecommunications company detects and responds to threats in the AWS cloud

Executive summary

This multinational telecommunications services company headquartered in Europe is one of the largest mobile network operators in the world by number of subscribers.

The company leverages Amazon Web Services (AWS) to host its data lake as well as to store network traffic for security forensics and compliance reporting.

At the same time, the Cognito® platform from Vectra® gives the telecom company a holistic view of threat behaviors in its enterprise network and data center, while arming its security team with vital network detection and response (NDR) capabilities for incident response, threat hunting and investigations.

A complex network

The telecom company's network spans over 10 geographic locations and multiple AWS virtual private clouds (VPCs). Securing and monitoring such a diverse footprint is no easy task.

In addition, the company is required to adhere to several different compliance policies. To accomplish this, telecom firm's security team relies on cloud-based Micro Focus ArcSight for big data security analytics and intelligence software for SIEM and log management.

To feed ArcSight, the telecom company uses Cognito Detect™ from Vectra to identify and respond quickly to hidden cyberattacks in its enterprise network and data center. Using AI-driven machine learning algorithms, Vectra detects unique threat behaviors that attackers cannot erase – even in encrypted traffic.

The telecom company's network spans over 10 geographic locations and multiple AWS virtual private clouds (VPCs). Securing and monitoring such a diverse footprint is no easy task.

Organization

Telecommunications company

Industry

Communications services

Challenge

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

Selection criteria

A platform that integrates with AWS and can detect and respond to threats evading their EDR solution

Results

- Visibility into all traffic flowing in its 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

All threats detected by Vectra are automatically prioritized based on risk and mapped to compromised hosts and users in the network.

The Vectra data is enriched with deep security insights and context about each attack and sent to ArcSight for deeper analysis and investigation.

The company also uses AWS-deployed Cognito Stream™ from Vectra to capture security-enriched metadata from all network traffic, which is sent to a data lake in AWS for threat hunting and investigation. A custom parser is in place to handle 15 types of metadata that have significant importance to the company.

The Vectra integration brings real-time detections as well as host threat and certainty scores from its enterprise and data center into the AWS-hosted ArcSight platform. This enables further correlation with information and events within ArcSight, such as usernames from Microsoft domain controllers.

The telecom company's security team can perform a fast, on-demand search for any threat behavior details from the ArcSight management console by leveraging the security-enriched network metadata collected and stored by the Cognito platform.

Strengthening endpoint detection with NDR

Although the company runs endpoint detection and response (EDR) software on its managed clients, this still leaves a large visibility gap for IoT devices, unmanaged BYOD hardware, and other devices that cannot support EDR software agents. EDR is also easily bypassed by sophisticated attackers.

Next to the visibility gap, the company knows that EDR is easily bypassed by cyberattackers and therefore Vectra NDR added an additional security layer to find attackers who have been able to bypass the EDR software.

The company decided to use the Cognito platform from Vectra to add another layer of security to find attackers who evade EDR. The Cognito platform detects and responds to threat behaviors in network traffic that are in flight, which provides complete coverage for all devices, regardless of client types.

Cloud-first deployments

The telecom firm takes a cloud-first approach to networking, and security is no different. Because its SIEM and security orchestration, automation and response (SOAR) implementations are cloud based, it also demanded an NDR solution with a cloud-centric deployment model.

Tight integration of the Cognito platform with AWS allows the company to deploy Vectra sensors – which are available in the AWS marketplace – in its VPCs.

Together with traffic mirroring on Amazon Machine Images (AMIs), the company has visibility into all traffic flowing in its VPCs. This includes all traffic going in and out as well as all intercommunication. And Vectra sensors are easily monitored for health and status via AWS Cloud Watch.

By uniquely combining data science and security research, Vectra provides threat detection as a next layer of defense in today's security infrastructure – from cloud/SaaS and data center workloads to users and every type of connected device.

For more information please contact a service representative at sales-inquiries@vectra.ai.

Email info@vectra.ai vectra.ai