VECTRA
SECURITY THAT THINKS.®

CASE STUDY

Fortune 500 Company Uses AI to Slam the Door on Cyberattack

One of the world's leading consumer packaged goods (CPG) companies thrives on being a cloud-first enterprise while running a huge amount of activity through Amazon Web Services (AWS). This global operation is packed with more than 50,000 EC2 instances, millions of Lambda services and thousands of users assuming millions of roles across the environment. Not only do they store massive amounts of personal identifiable information (PII), but they also run business-critical operations that include key portions of HR data for tens of thousands of employees.

The company's SecOps team has taken the necessary steps to protect its environment with Cloud Workload Protection Platform and Cloud Security Posture Management, but still have reason to be concerned about post-exploitation coverage as they haven't been hugely successful with their attempts to build their own rules in house.

Fortunately, this diligent team is aware of the areas that need attention in order to stay on the offensive against any potential attacks—especially in their critical AWS infrastructure. And this is exactly why the team identified Vectra Detect for AWS as a solution that would be able to help them make sure any threats in the environment would quickly be detected and remediated. It just so happens that Detect for AWS quickly proved its value—gaining coverage in a matter of minutes—and then soon after when the company was infiltrated by a malicious actor in early 2022.

Organization

Fortune 500 Consumer Goods Company

Industry

Consumer Goods & Retail

Challenge

Needed a tool that could protect the amount of activity in their critical AWS infrastructure

Results

- Detect for AWS gained coverage within a few minutes and flagged the suspicious use of credentials early on
- With just one click, this security team was able to open Instant Investigations with Vectra and immediately see what other activity the malicious user had performed around the time of the suspicious activity.

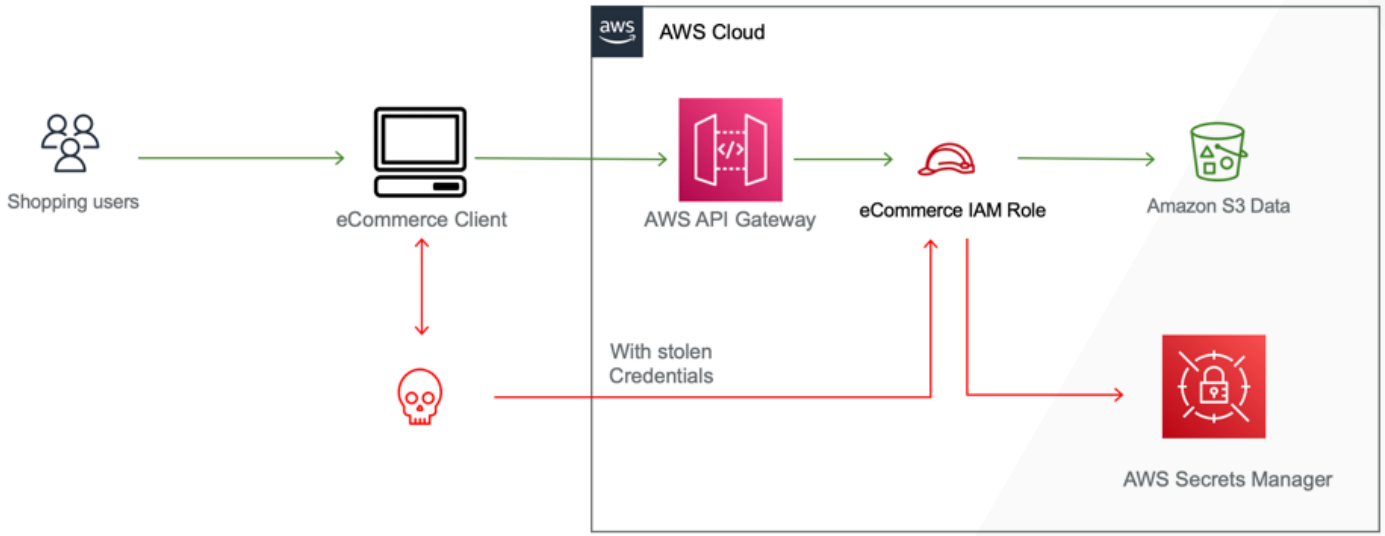
Detect for AWS quickly proved its value—gaining coverage in a matter of minutes—and then soon after when the company was infiltrated by a malicious actor in early 2022.

Ecommerce Stack Comes Under Attack

It turns out that an attacker gained access to a set of user credentials—most likely by inspecting the source code of the ecommerce application. In theory, credentials in code should have been caught by static code analysis, but herein lies the limitation of preventive measures. This allowed the attacker to leverage the credentials to access a customer-facing application. And while the permissions of this ecommerce user should have been limited to interacting with S3 bucket data—the user was able to successfully interrogate the AWS Secrets Manager and pull the details on all of the secrets that were stored on this AWS account – again, demonstrating that in large complex deployments it is impossible to get access policies airtight.

With access to these secrets, there is no telling what other resources and services the attacker would be able to access through lateral movement techniques. How many points of persistence could the attacker establish? Or how big of an impact would be made?

Fortunately, Detect for AWS flagged the suspicious use of credentials early on—from the ocean of daily activity—nearly half a billion actions each day.



Detect for AWS flagged the suspicious use of credentials early on—from the ocean of daily activity—nearly half a billion actions each day.

How did SecOps Get to the Bottom of this?

- Once the Detect dashboard flagged the AWS principal, the analyst was able to quickly understand what activity Vectra found suspicious.
- The analyst wanted to learn more about this account. Vectra's Kingpin identity attribution technology helped connect the dots right away.
- In order to understand the breadth of the incursion, the analyst wanted to see what other activity the attacker engaged in (with these credentials). Normally, this would take a couple of hours, as they had to pivot to their SIEM, formulate a query to pull the related data, and then parse the jumble of assumed roles that were involved. But with just one click, they were able to open Instant Investigations with Vectra and immediately see what other activity the user had performed around the time of the suspicious activity.

The malicious activity stood out like a sore thumb. This ecommerce user typically interacted exclusively with s3 buckets, and always did so from the AWS IP space—whereas suddenly the analyst could see Secrets interactions coming from a completely novel IP space, which was in fact from the TOR IP space.

How did SecOps Respond?

Within two minutes of opening the detection, they were completely confident this activity was malicious and were able to respond immediately by rotating the Secrets that had been accessed and resetting ecommerce credentials. It was shut down before it could have a serious impact on their organization.

Sophisticated, and Now Secure AWS Environment

This organization has an extremely sophisticated AWS footprint, and a mature security practice with traditional cloud-security measures for prevention and compliance in place. However, no amount of CSPM could have caught this activity, as the ecommerce user was designed to perform activity on behalf of other users. While the least privileged activity should have been in place limiting the ability of the user to interact with Secrets, one small misconfiguration is all it took for the attacker to get a foothold.

Ultimately it takes an active threat detection platform with a deep understanding of attacker behavior and AI modeling to be able to surface such threats, and then deliver a one-stop-shop experience for the SOC.

Sign up for a free Detect for AWS eval today and the bring the power of Vectra's game-changing threat detection and response to your SecOps.

For more information please contact us at sales-inquiries@vectra.ai.

Email info@vectra.ai vectra.ai