AWS GuardDuty

GuardDuty is Amazon’s intrusion detection system for AWS. It “is a threat detection service that continuously monitors, analyzes, and processes specific AWS data sources and logs in your AWS environment.” It utilizes “threat intelligence feeds, such as lists of malicious IP addresses and domains, and machine learning (ML) models to identify unexpected, and potentially unauthorized activity.”

For the question of anomaly-based or pattern-based detection, I wasn’t able to find a source that definitively described GuardDuty as one or the other, but as far as I can tell the answer is likely that it utilizes a combination of both. As an example, the source mentions that it is capable of detecting “Escalation of privileges, use of exposed credentials, or communication with malicious IP addresses and domains”, all of which, at least to me, seem to fall under the pattern-based umbrella. But it is also able to do things like monitoring “AWS account access behavior for signs of potential compromise, such as unauthorized infrastructure deployments – instances deployed in a Region that has not been used before”, all of which sound like what you would expect from an anomaly-based system.

Source: <https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html>