GuardDuty

Amazon GuardDuty is a managed, continuous **threat detection service** designed to help you identify malicious or unauthorized activity in your AWS accounts, workloads, and services. GuardDuty exists to address the growing need for proactive and automated security monitoring across cloud environments, where manual threat detection can be both time-consuming and ineffective against increasingly sophisticated attacks.

The service leverages machine learning, anomaly detection, and integrated threat intelligence from sources like AWS Security Hub, AWS Web Application Firewall (WAF), and global threat databases to detect a wide range of security issues. These include unusual API calls, unauthorized access attempts, suspicious network traffic patterns, and potential data exfiltration.

Basically, GuardDuty is designed to reduce the complexity of threat detection by providing organizations with real-time security findings without the need to manage or deploy additional infrastructure.

Additionally, GuardDuty can also be used to enable fast and/or automated responses to potential threats, with integration support for event-driven workflows and initiating lambda functions for the purposes of automated remediation or prevention of the detected threads.