AWS re:Start

LAB

Monitor an EC2 Instance

Logging and monitoring are techniques implemented to achieve a common goal. They work together to help ensure that a system's performance baselines and security guidelines are always met. Logging refers to recording and storing data events as log files. Logs contain low-level details that can give you visibility into how your application or system performs under certain circumstances. From a security standpoint, logging helps security administrators identify red flags that are easily overlooked in their system.

Monitoring is the process of analyzing and collecting data to help ensure optimal performance. Monitoring helps detect unauthorized access and helps align your services' usage with organizational security.

In this lab, you create an Amazon CloudWatch alarm that initiates when the Amazon Elastic Compute Cloud (Amazon EC2) instance exceeds a specific central processing unit (CPU) utilization threshold. You create a subscription using Amazon Simple Notification Service (Amazon SNS) that sends an email to you if this alarm goes off. You log in to the EC2 instance and run a stress test command that causes the CPU utilization of the EC2 instance to reach 100 percent.

This test simulates a malicious actor gaining control of the EC2 instance and spiking the CPU. CPU spiking has various possible causes, one of which is malware.

aws re/start