**Examining Sample GuardDuty Findings**

### Introduction

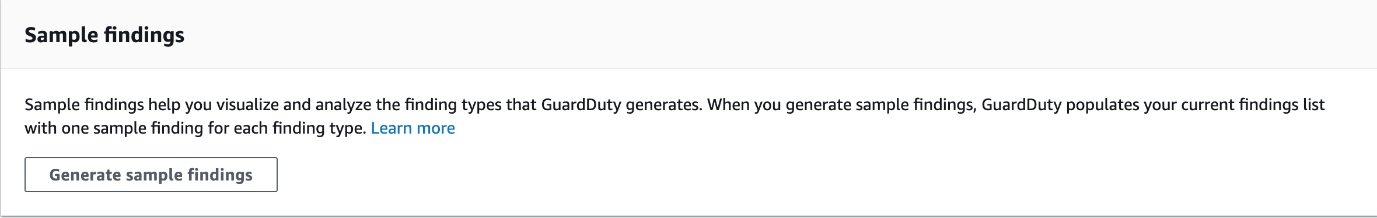
To learn about the types of threats that GuardDuty can find, you will generate sample findings in this lab step. The findings are simulated, but allow you to view details and illustrate the three different severity levels in GuardDuty: high, medium, and low. In addition to the sample findings, you can find [descriptions of what each finding relates to in the GuardDuty documentation](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types.html).

### Instructions

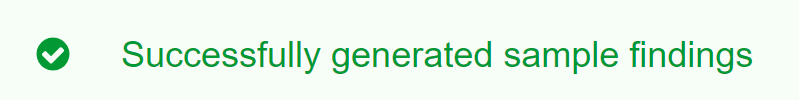
1. Click on **Settings**in the GuardDuty Console sidebar.

You can ignore any error that appears regarding not being authorized to perform IAM requests.

2. Click on **Generate sample findings**:

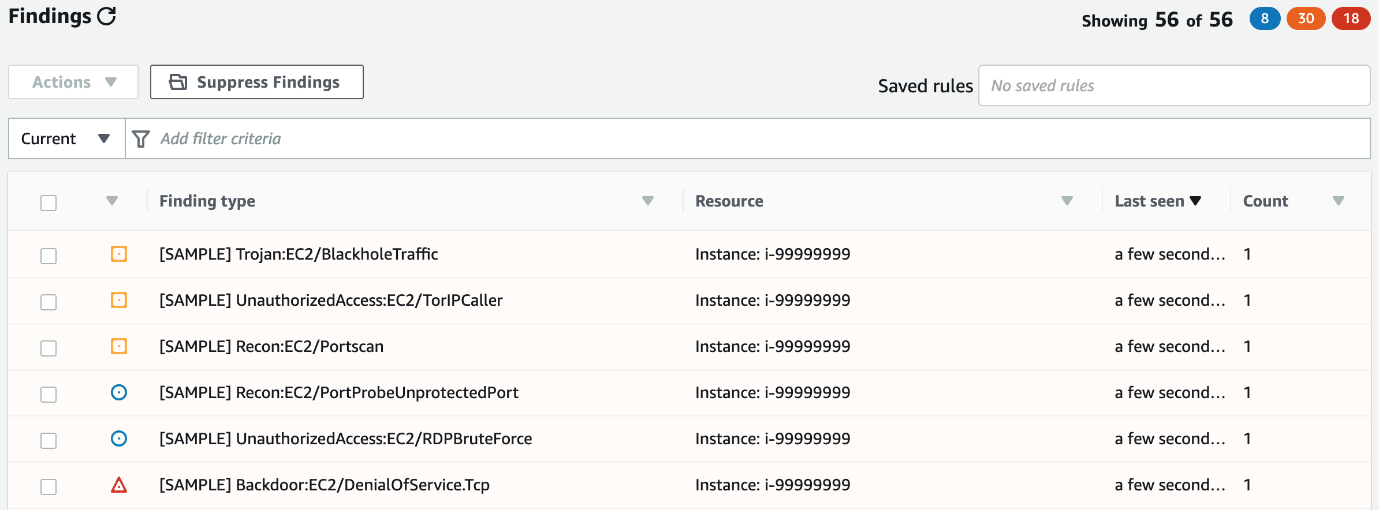


After a few seconds a success banner appears:



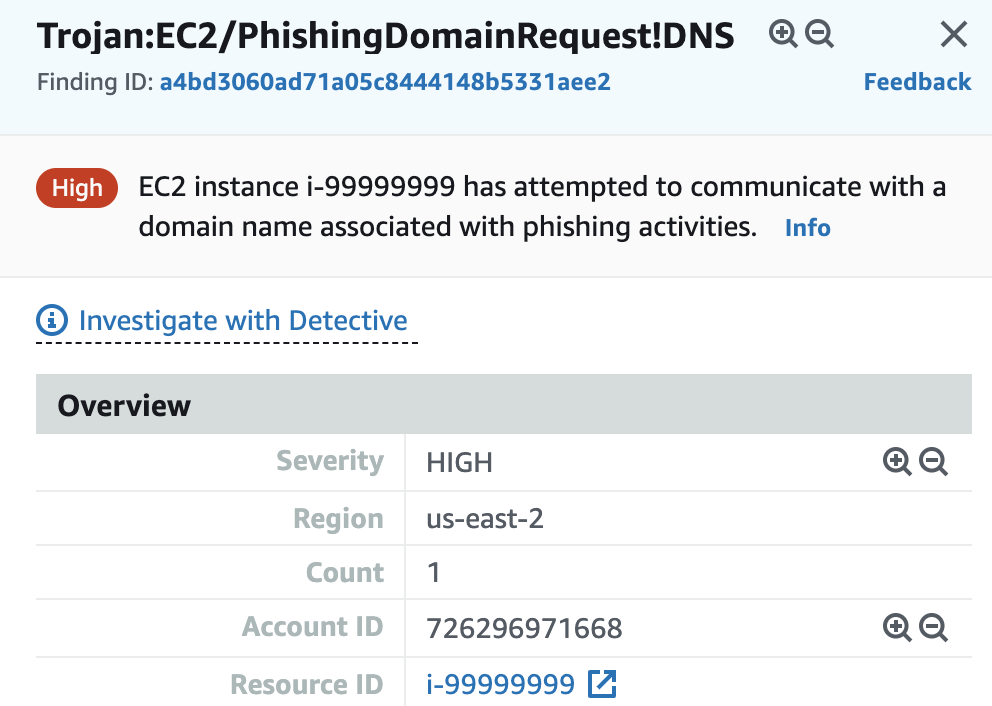
3. Click on **Findings** in the GuardDuty sidebar.

Notice the table is full of various findings that begin with **[SAMPLE]**:



4. Read through the different sample findings to see what kind of threats GuardDuty can identify.

5. Select a few findings and inspect the details panel that appears:



The details are divided into several sections: Summary, **Resource affected**, **Action**, **Actor**, and **Additional information**.

### Summary

In this lab step, you generated and examined sample GuardDuty findings. Although this Lab focuses on EC2 threats, you have also seen in the sample findings that GuardDuty can also identify IAM threats by using CloudTrail logs.