Overview:

By default, AWS users are not given permission to create or modify EC2 resources. If the user has not been given the permission through IAM policies they will not have the ability to perform tasks. If a user attempts to perform a task and has not been granted the permission they will receive the following error: *Client.UnauthorizedOperation.*

Discovery:

One of the best ways to be sure there are no unauthorized API calls is to log your API calls using CloudTrail. This will allow you to make sure users are only performing tasks they have been granted permission to.

AWS CloudTrail logs AWS API calls and related events made by or on behalf of an AWS account. The features can determine what actions users are taking as well as the resources they are using.

CloudTrail encompass' the history of calls made by using the AWS Management Console, AWS SDKs, command line tools, as well as, other higher-level AWS services, such as, Amazon EC2, Amazon EBS, and Amazon VPC.

More Information: https://aws.amazon.com/cloudtrail/

Remediation:

By looking at the logs you can determine many things, such as, when and what request was made.

Information that can be gathered from these logs include:

which users and accounts have used the services supported by CloudTrail.
Source IP address the calls were made from
When the calls occurred

CloudTrail can be used in conjunction with other applications by using the API. You can "automate trail creation for your organization, check the status of your trails, and control how administrators turn CloudTrail logging on and off."

More information can be found: http://docs.aws.amazon.com/awscloudtrail/latest/userguide/

Prevention:

Unauthorized API Calls can be prevented by ensuring the each IAM User has the correct permissions to use the services and make the calls necessary.