Imagine that you're creating a script that would check the state of all EC2 instances in your AWS account except for instances used by the security team. Describe how you would set up IAM to make sure that your script would have access (only) to the instance information needed.

I would define a policy that grants access permissions to the EC2 instances that are not associated with the security team. The policy would take the identifier of the EC2 instances and determine whether or not the script is eligible to access the information of the instance. As defined by the docs it is possible to use policies to define permissions for IAM identities. The JSON policy document can be used as a guideline for custom policies, like in case of this scenario.
A simple policy could be for instance denying access to AWS based on the IP address. This means that instances used by the security team could only be accessible when using specific IP addresses, this can simplify the distinction between specific instances as AWS itself handles the access control with the defined policy.
A different solution would be to create an IAM group, which is the collection of IAM users. These users have specific permissions as defined by the group. The members of the IAM group would have access to all instances. The group shall consist of all members of the security team. This way every other IAM user may not be able to access security team relevant instances.