When is it appropriate to use containers in cloud deployments, and what are the security benefits of doing so?

It's important that organizations to reduce overhead costs on infrastructure like underutilized VMs and human resources, especially since most application or services only leverages small parts of the OS kernel. With the use of containers, we can be more efficient by creating containers for each application or service and shared common resources like OS kernel and core libraries with other containers.

We used containers in one of my projects on the cybersecurity bootcamp. For the first part of our project, we had to initially deploy a container in our provisioner machine that would help us automate container deployments in another environment. The tool that we used to automate container deployment is ansible. Once we had ansible container installed, we were able to leverage the ansible tool and container technology to deploy and configured DVWA, ELK containers on different servers. The DVWA container contains components to host the DVWA web pages. In addition, the ELK container contains components to hosts and manages our Elastic and Kabana services.

We thought this was ab appropriate use for containers because we were able to leverage on store containers or download containers that were created by other people. As well it makes it extremely fast and easy to install complex server configurations like our DVWA web pages and ELK servers. In addition, by using containers if one our container is attacked or has a problem, it can be killed and regenerated as needed without the website or services going down.

To give you some details on our solution, our initial container deployment on the provision machine, we had to install the docker package first. To ensure that we install the proper containers, we only need to know the name of the image maker and image name. In our case, we are getting the container from cyberxsecurity/ansible. Once the ansible container has been deployed, we had to verify if the container has been installed properly. To verify that it was running correctly, we execute docker ps command and it will list all the containers that you have installed and running. We were able to leverage the ansible tool by creating different playbook files to deploy DVWA containers and ELK containers to different servers.

We could have achieved the same output without using containers by manually configuring each VM machine to its spec. However, the utilization of the VM might be underutilized and wasting resources. By going container route, containers can share OS resources while remaining isolated, allowing each one to focus exclusively on its own state so that no resources are wasted. As a result, we can deploy multiple containers to utilize the VM better. As well the ability to be easily created and destroyed to save on human resources cost. However, containers does not scale vertically. Hence finding a good balance on number containers in a VM is very important because we do not want to overutilized or underutilized resources in a VM.