CKS : Complete Certification Guide

Understanding Behavioral Analytics

Levelup360 : anshulc55@icloud.com

Behavioral Analytics

- ➢ Behavioral Analytics is a Process of observing what is going on in the System and identify abnormal and potentially malicious attacks.

- ➢ Behavioral analytics can be done manually or using automation tools.

- ➢ It's not realistic to manually keep an Eye on all the things 24*7, so it is recommended to use the automation Tools for Behavioral Analytics.

Behavioral Analytics Tool

- ➢ **Falco** is a Behavioral Analytics tool.
- ➢ This is a Open-Source tool created by **Sysdig**.
- ➢ Falco Monitor the Linux system Runtime calls and raise alert on any suspicious activity based of the configuration.
- ➢ User can use Falco to detect the Suspicious activity, and response quickly.

Behavioral Analytics Examples

- **Privileged Escalation**
  - A privileged container attempting to escalate privilege.
- **Binaries**
  - Execution of suspicious binaries using container, which is not expected.
- **File Access**
  - Read or write to files at / , /usr, /bin etc known location.

Thank You…

Don’t be the Same! Be Better!!!