|  |  |
| --- | --- |
| **Server & Cloud Security**  Diploma in CSF/IT  Oct 2022 | Week 6 |
| Tutorial |
| **Cloud Operations Security** | |

1. Logging and Monitoring are the two important aspects of cloud operations security. Briefly describe the differences between logging and monitoring.

|  |
| --- |
| * Logging tells you what happened, and gives you the raw data to track down the issue. * Monitoring tells you how your application is behaving and can alert you when there are issues. |

1. Briefly explain the similarity and difference between AWS CloudTrail and CloudWatch.

|  |
| --- |
| * Similarity: Both CloudTrail and CloudWatch are monitoring services. * Difference:   + CloudWatch focuses on the activity of AWS services and resources, reporting on their health and performance.   + CloudWatch: “What is happening on AWS?”   + CloudTrail is a log of all actions that have taken place inside your AWS environment.   + CloudTrail: “Who did what on AWS?” |

1. With reference to the statement - “Not all events are incidents in need of immediate remedy”, briefly discuss the difference between events and incidents.

|  |
| --- |
| * An event is an observed change to the normal behavior of a system, environment, process, workflow or person. * An incident is an event that negatively affects the confidentiality, integrity, and/or availability (CIA) at an organization in a way that impacts the business. * One example of event that does not turn into incident is: Web browser crashes or device reboots are events. Most of them don't turn into incidents. |

- The End -