









# Day 2 - Immersion Day - Security

8:30 AM - 9:30 AM		<b>[0 - General] AWS Shared Responsibility Model and Security Foundations</b> This content provides an overview of AWS security including high level details on AWS infrastructure. The content also touches on the shared responsibility model.
9:30 AM - 10:30 AM		<b>[0 - General] Best Practices for Security at Scale</b> What does a bad day on AWS look like and how can you have a good day?
10:30 AM - 10:45 AM		<b>Break</b> Take a minute to relax...
10:45 AM - 11:45 AM		<b>[0 - General] Security, Identity, and Compliance at AWS</b> This content provides an overview of security at AWS, and touches on services that address customer use cases.
11:45 AM - 12:45 PM		<b>Lunch</b> Enjoy your meal!
12:45 PM - 1:45 PM		<b>[Detection and Response] Using AWS Services for Incident Response</b> This content provides an overview of Incident Response capabilities using native AWS services.
1:45 PM - 3:45 PM		<b>[Detection and Response] Amazon GuardDuty Workshop</b> Amazon GuardDuty offers threat detection enabling you to continuously monitor and protect your AWS accounts, workloads, and data stored in Amazon Simple Storage Service (Amazon S3). GuardDuty analyzes continuous metadata streams generated from your account and network activity found in AWS CloudTrail Events, Amazon Virtual Private Cloud (VPC) Flow Logs, and domain name system (DNS) Logs. GuardDuty also uses integrated threat intelligence such as known malicious IP addresses, anomaly detection, and machine learning (ML) to more accurately identify threats. In this workshop, learn the basics of Amazon GuardDuty and dive deep into different use cases and scenarios.
3:45 PM - 4:00 PM		<b>Q&amp;A</b> Any questions?

90M

---

4:00 PM -  
4:15 PM



Conclusion & Next Steps

Here are some resources for you until next time...

---