

Cloud IR

Improve response capabilities within the cloud.

Over the last decade, the rise of cloud services has significantly changed the role and requirements of Incident Response (IR) teams. The shift from on-prem to cloud environments—oftentimes using multiple cloud providers simultaneously—adds complexity to managing data volume and accessibility in tandem with mitigating evolving cyber threats. Today's incident responders require specialized security skills that apply foundational IR concepts and techniques within respective cloud domains.

What is the Cloud IR Course?

CyberVista's Cloud IR course is designed to introduce and familiarize security professionals with the requisite cloud incident response functions and capabilities. This course will review Incident Response as a function within the cloud environment. Practitioners will work their way through both Amazon Web Services (AWS) and Microsoft Azure environments while learning about further cloud concepts and technologies. Lastly, this course will cover the ELK stack and the importance it plays within IR functions in the cloud.

It is recommended that participants have at minimum a Security+ certification or have completed CyberVista's Cloud SOC course.



CyberVista's Cloud IR course

Who should take this course?

- **Incident Responders or Forensics Analysts**
- **Cybersecurity Analysts**
- **Cyber Incident Response Analysts**
 - » **Current IR Security Professionals:** Those who want to refamiliarize themselves with AWS/Azure incident response processes and techniques.
 - » **New IR Security Professionals:** Those who need an introduction to IR in the cloud along with exposure to the AWS/Azure platforms.
 - » **Security Management:** Those who want to familiarize themselves with Cloud IR concepts and be more fluent in Cloud IR literacy.

Benefits of Training

- Modular training lessons to easily digest concepts and techniques
- Course developed for professionals to improve IR abilities immediately
- Demonstrate IR techniques and processes in real cloud environments that are applicable to organizations of all sizes

Course Domains

1



INCIDENT RESPONSE IN THE CLOUD

This domain covers an overview of the incident response process and the roles and responsibilities of the IR team in a cloud environment.

2



FORENSICS IN AWS

This domain covers the processes and techniques used when conducting forensics on the AWS platform. Additionally, we cover how evidence is collected and the impact on security presented by containers and databases.

3



FORENSICS IN AZURE

This domain covers the processes and techniques used when conducting forensics in the Azure platform. We cover imaging techniques and Azure tools that help facilitate IR investigations.

4



ELK STACK IN IR

This domain covers an overview of the ELK Stack, the projects that comprise it, and example demos of the ELK Stack in use.

What's included?

A full featured learning management system (LMS) enables both leaders and participants to access training materials throughout the program while also tracking progress and performance. This course also includes:

- **Diagnostic Assessment:** Easily administer a diagnostic assessment used to determine each team member's strengths and weaknesses.
- **Video Lesson Library:** Modular and engaging on-demand video lessons.
- **Expert Interviews:** Interviews with cybersecurity and IT leaders to provide context and real-world examples.
- **Knowledge Check Assessments:** Short, micro-quizzes throughout the lesson content to ensure engagement and knowledge retention.
- **Practice & Hands-on Activities:** Take-home activities and optional hands-on labs to reinforce practical applications of security concepts.
- **Final Assessment:** Participants conclude training with a final assessment to demonstrate knowledge and skills gained.

Your workforce needs work.

Interested in learning more about how CyberVista's Cloud IR course can help your organization? Connect with our team for a free consultation.

For more information contact us at sales@cybervista.net or call 844-558-4782.

CyberVista