NYU

# Automated Forensic Solution for AWS EC2 Instances

## Final Project

**CS-GY 9223: Cloud Security Prof.**

**Catherine Dodge, Prof. Rima Tanash**

Details :
Vishnu Vardhan Ciripuram
(vc2499@nyu.edu)

**1. Problem Statement - What is the problem you're trying to solve with your solution**

Our project aims to create a reliable and automated forensic solution specifically designed for AWS EC2 instances. The objective is to streamline memory and data acquisition, maintain the accuracy of the evidence gathered, and conduct a thorough analysis of system actions to enhance security and help conduct forensic investigations.

**2. Initial proposal/design - What was your initial proposed solution to address the problem**

The initial option presented was to assess the effectiveness of AWS's Automated Forensics Orchestrator for Amazon EC2. The system employs a fusion of SecurityHub, EventBridge, and Lambda functions to automate the generation of forensic snapshots. For safe storage, AWS services like EBS snapshots and S3 were recommended. Additionally, a DynamoDB was configured to gather information about the system's operations.

**3. Issues encountered - What were the problems you encountered (if any) along the way to do the implementation**

There were problems with the CDK script, specifically the absence of an IAM role. Furthermore, there were difficulties in setting session roles to possess the necessary presumed access. The system is compatible exclusively with Python version 3.9. Additionally, it was discovered that having a specialised AWS account just for forensic tasks is necessary, significantly impacting the data collection process.

**4. Final design - what adjustments to your initial proposal did you make to get to your implementation**

Our project aims to provide a simple and effective way of capturing memory from AWS EC2 instances in the event of a security incident. This process entails utilising Amazon CloudWatch to observe indicators such as elevated CPU utilisation, triggering an Amazon SNS alert that initiates an AWS Lambda function. This function executes a memory capture script using AWS Systems Manager Agent (SSM). The output, which is a memory dump, is safely stored in an Amazon S3 bucket for future study. The smooth integration of these components ensures a quick and reliable collection of data for forensic analysis.

**5. Lessons learned/Future work - What would you have done differently, knowing what you know now? What additional features would you have implemented if you had more time?**

**Lesson Learned:**

- IAM Role Configuration: Ensure accurate validation of IAM role configurations in CDK scripts to prevent issues related to missing roles.
- Session Role Permissions: Verify that session roles possess the required assumed access permissions for successful operations.
- Testing Protocols: Emphasize testing in a controlled environment before deployment to detect potential problems early and ensure system stability.

**Future Work:**

- Enhanced Monitoring and Alerting: Integrate additional AWS services, such as AWS CloudWatch logs, to improve monitoring and alerting capabilities.
- Advanced Analysis Features: Develop features for identifying malware or adversary actions in forensic data to enhance security measures.
- Machine Learning Integration: Incorporate machine learning techniques to detect anomalies in system activity, improving the detection of security threats.
- Exploration of Capture Frameworks: Research and implement other disk and memory capture frameworks beyond LiME and Volatility to expand forensic capabilities.

**Architecture**:

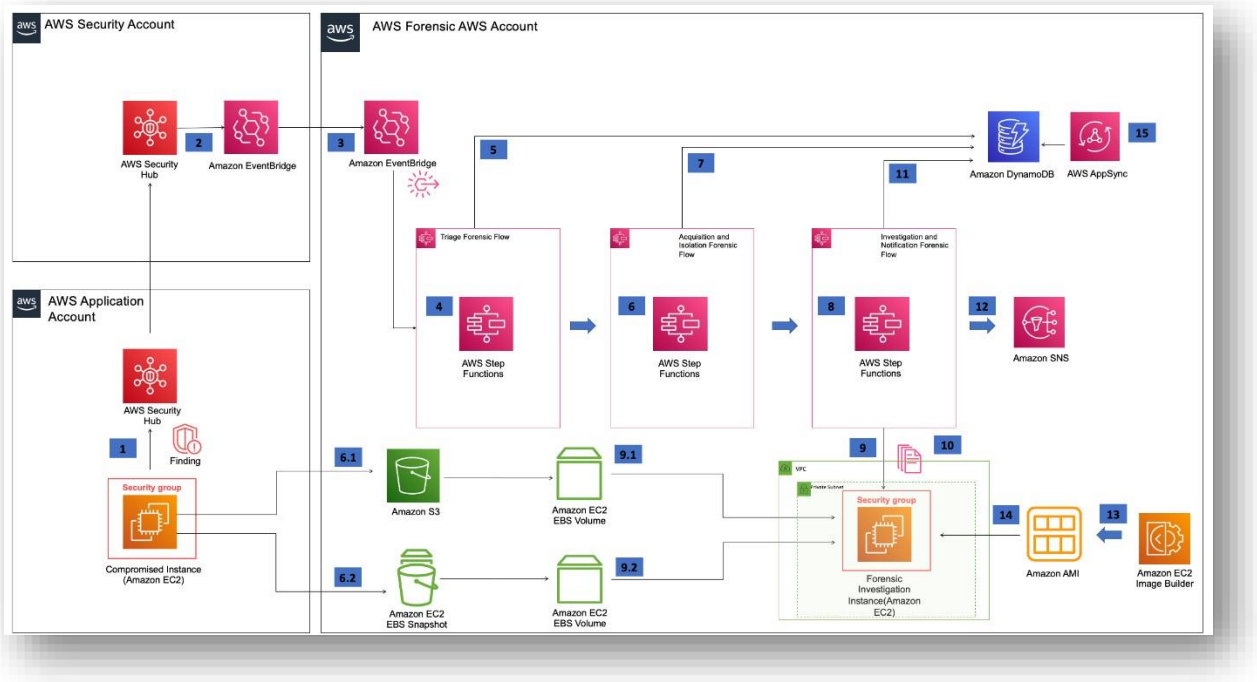


Figure 1: EC2 Forensic Orchestrator Solution Architecture

**References**:


[1] AWS Solutions, "Forensic memory and disk acquisition service," 2024, last accessed May 2, 2024. [Online]. Available: https://docs.aws.amazon.com/solutions/latest/automated-forensicsorchestrator-for-amazon-ec2/forensic-memory-and-disk-acquisition-service.html

[2] AWS Security Blog, "How to automate forensic disk collection in AWS," 2024, last accessed May 2, 2024. [Online]. Available: https://aws.amazon.com/blogs/security/how-to-automate-forensicdisk-collection-in-aws/

[3] AWS Solutions, "Automated Forensic Orchestrator for Amazon EC2," 2024, last accessed May 2, 2024. [Online]. Available: https://github.com/aws-solutions/automated-forensic-orchestrator-foramazon-ec2

[4] AWS Solutions Library, "Automated Forensics Orchestrator for Amazon EC2," 2024, last accessed May 2, 2024. [Online]. Available: https://aws.amazon.com/solutions/implementations/automatedforensics-orchestrator-for-amazon-ec2/