**Automating Incident Response**

[Security]

**Introduction**

I will create an automated incident response playbook and execute it when a compromised instance is detected. I will implement the automated IR playbook via a single lambda function

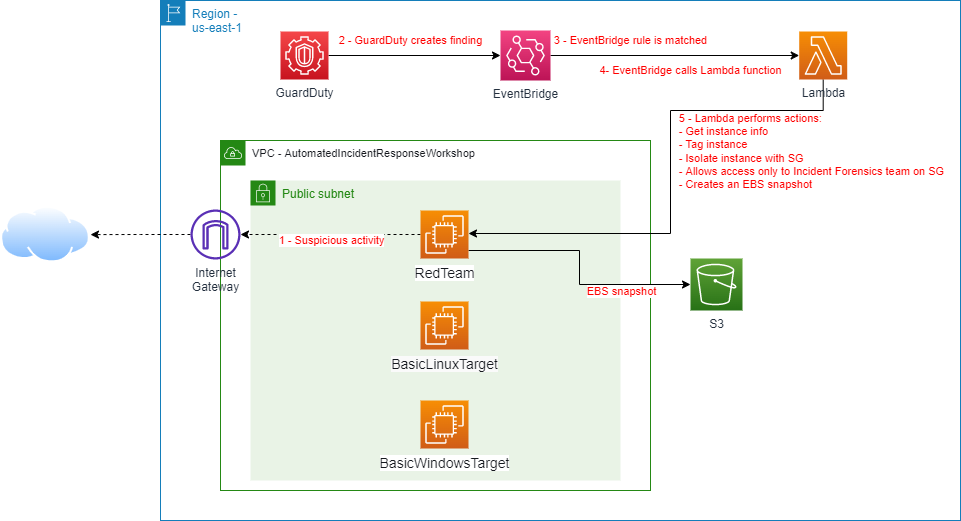
**Project Description – Scenario**

An adversary injected an OS command in an application and exploited any vulnerability, executing arbitrary code on the instance to reach a web server anonymously on their network. They were successful in compromising the instance. Also, they will attempt to perform bitcoin mining and connect to a known malicious IP address.

**Solution – Proposal**

Configure automated remediation tasks, simulate those attacks, and analysing the results.

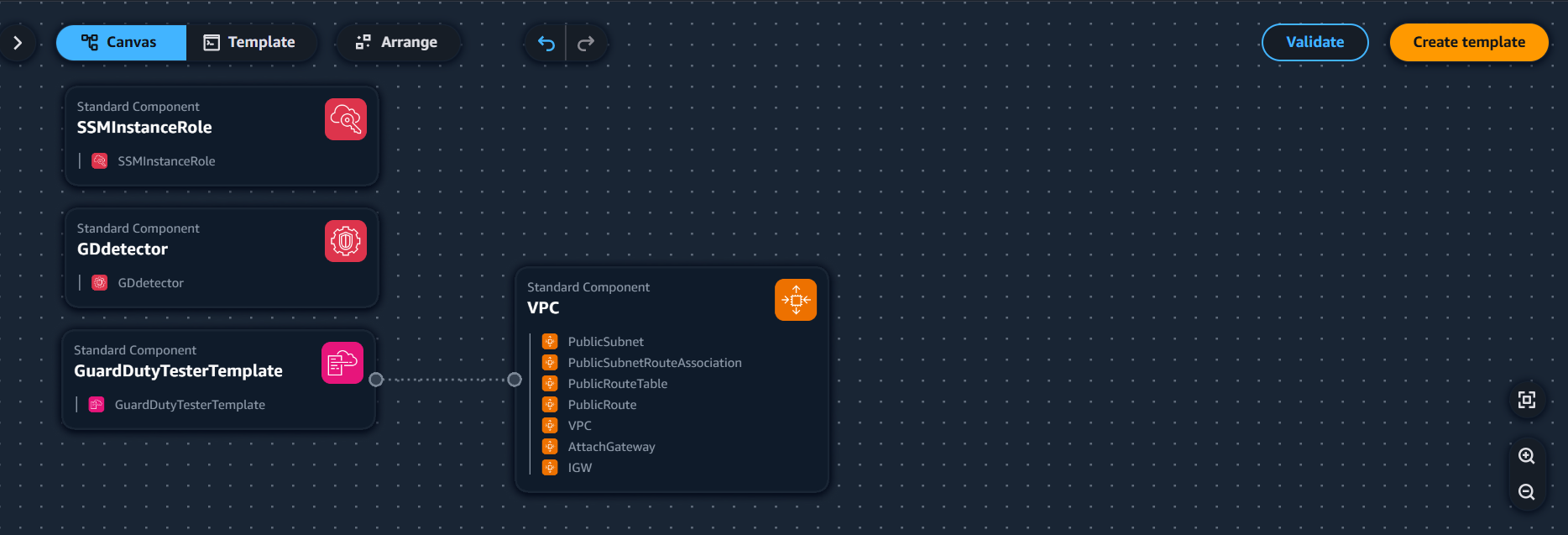
**Architecture Overview - Depiction**



**Setup and Environment configuration**

I will enable Amazon GuardDuty and deploy a CloudFormation template to create a sample infrastructure to simulate an attacker and a target.

**Deploy the CloudFormation stack**

****

**Set up Security Group for isolation and forensics**

**A screenshot of a computer

Description automatically generated**

Note: The Security Group ID will be used as an environment variable in the Lambda function.



All outbound rules removed.

The core value is transforming a traditionally reactive security process into an automated, proactive defence system that can respond to threats in real-time while providing valuable insights for future security improvements with benefits such as Proactive security posture, Operational efficiency, Threat intelligence enhancement, Cost prevention, Compliance support

**Policy Creation**

**A black screen with a black background

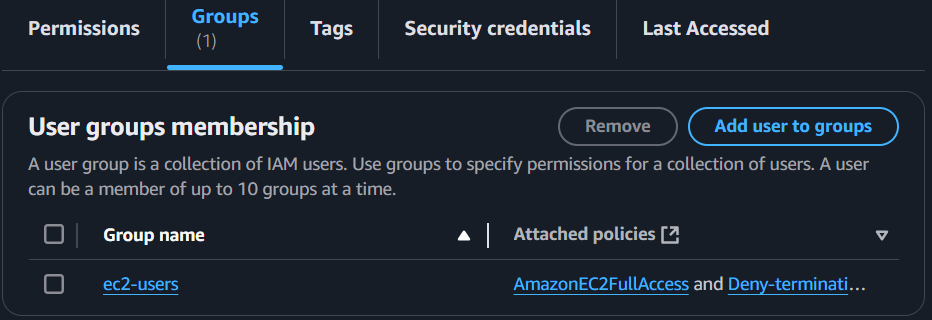
Description automatically generated**

**Group Creation & Policy attachments**

A screenshot of a computer

Description automatically generated

**User Creation & Group assignment**

****

The users with this policy will not be able to terminate the instance, based on the attached policy permissions

**Configure Response**

In this step I will implement an automated incident response action with a single lambda function, this will execute the remediation.

**Create IAM Policies & Roles**

This policy is for the execution role

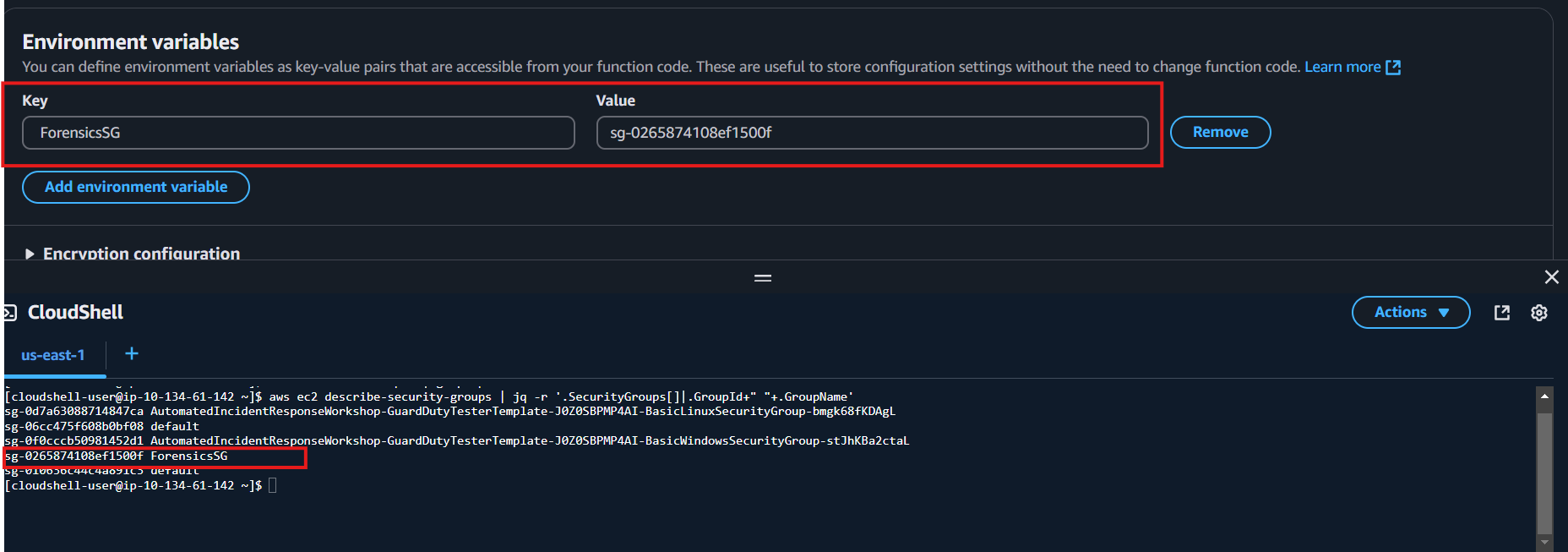
A screenshot of a computer

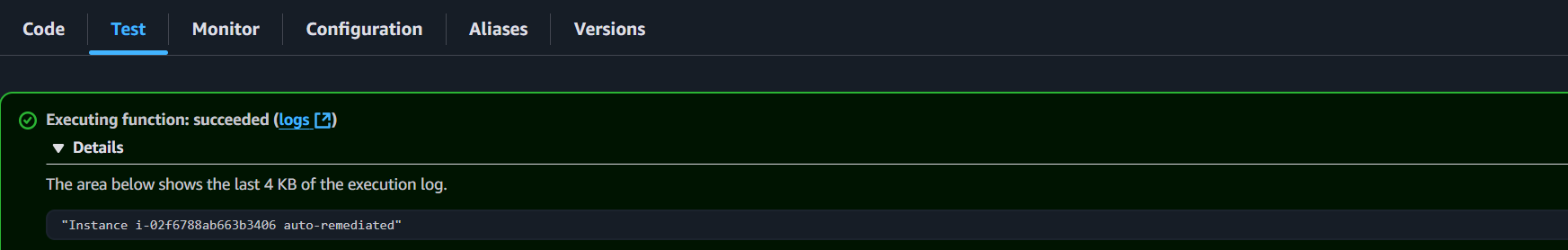
Description automatically generated

A screenshot of a computer

Description automatically generated

**Lambda Function Creation, Env variables & Test**

****

****

**Manual test – after execution the following happened**

When this event triggers the Lambda function, it will:

1. Identify the compromised instance (i-02f6788ab663b3406)
2. Enable termination protection on it
3. Tag it as isolated
4. Move it to the forensics security group
5. Take snapshots of all its volumes

A screenshot of a computer

Description automatically generated

**Create EventBridge Rule – Custom event pattern**

**A black background with white text

Description automatically generated**

**A screenshot of a computer

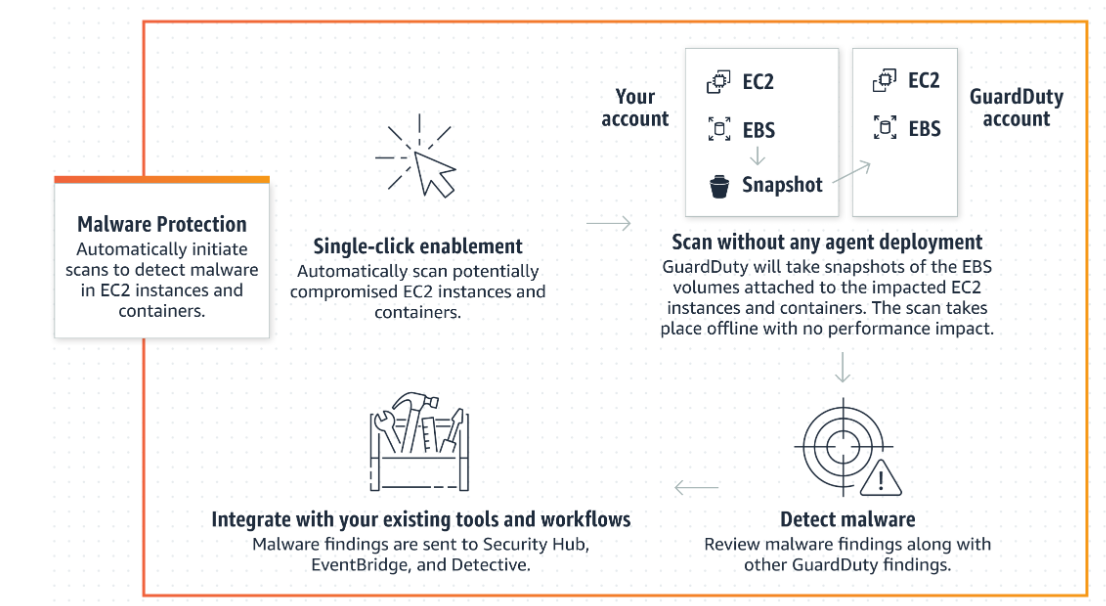
Description automatically generated**

The custom event pattern will catch outgoing anonymous (TOR) connections [identifying malware on the instance]

The selected target will be the lambda function – previously created.

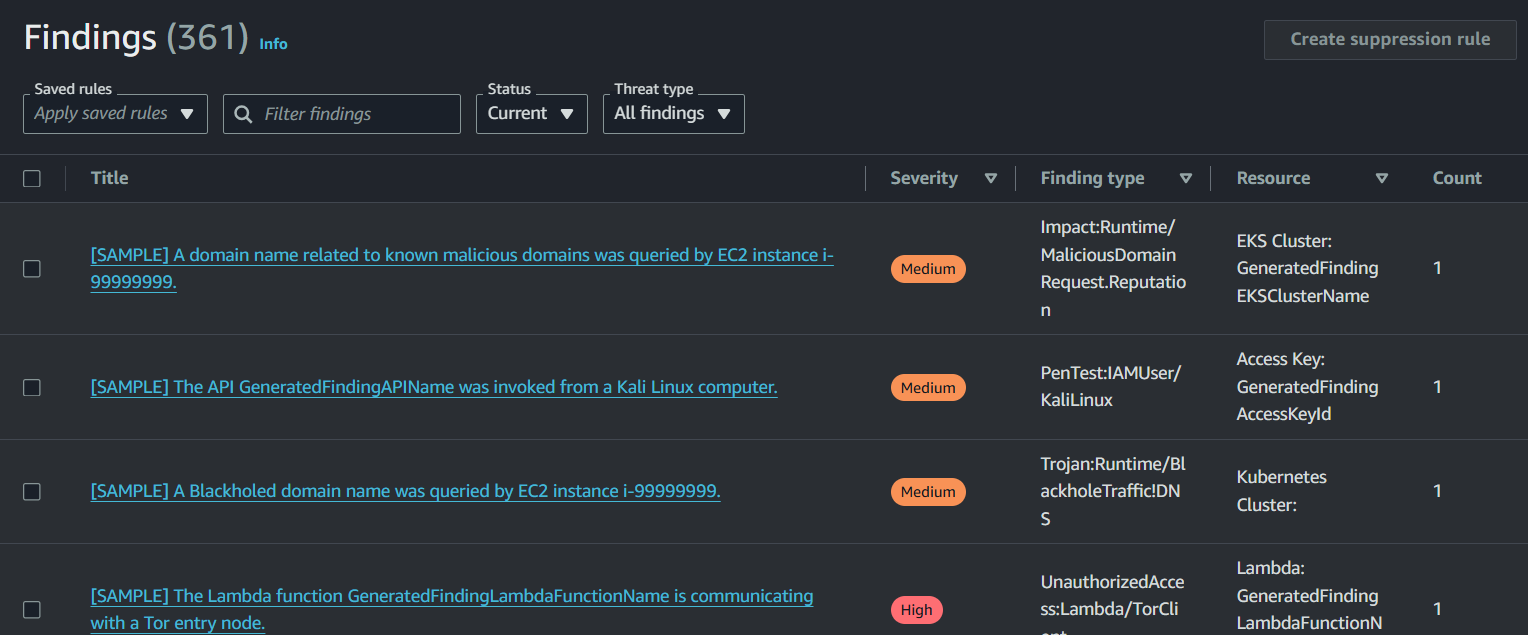
**Configure Automated Response**

In this section I will ingest sample findings using GuardDuty and use its input for the automated incident response process.



With GuardDuty-initiated malware scan enabled, whenever GuardDuty generates [Findings that invoke GuardDuty-initiated malware scan](https://docs.aws.amazon.com/guardduty/latest/ug/gd-findings-initiate-malware-protection-scan.html), an agentless malware scan on the Amazon Elastic Block Store (Amazon EBS) volumes attached to the potentially impacted Amazon EC2 resource will initiate.

Sample findings help you visualize and analyze the finding types that GuardDuty generates.



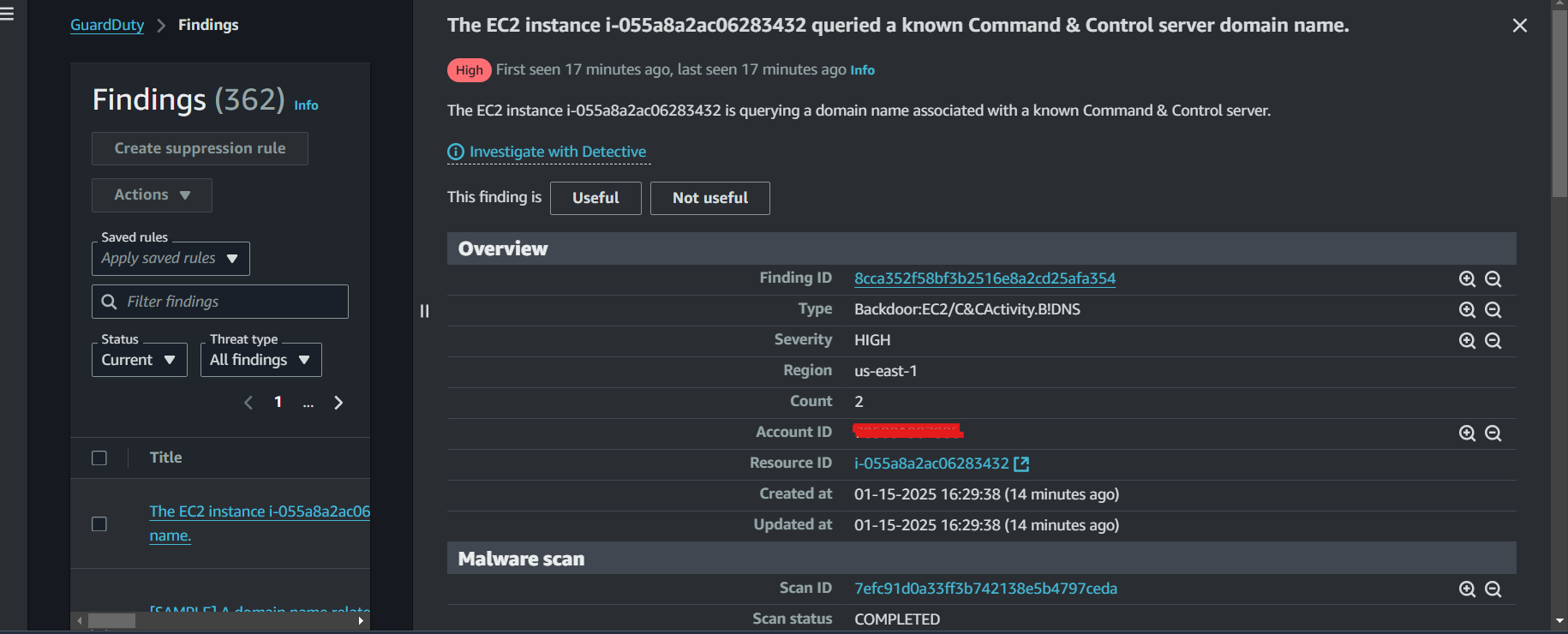
**Test Response**

I manually launched a Linux instance creating a new SG that allows SSH (22) access from your IP Address and called a fake domain.

A screenshot of a computer program

Description automatically generated

**GuardDuty generate findings.**



**Conclusion | Re-Cap**

* Perform automated basic incident response tasks for containment and gathering data for forensics.
* Understood possible actions to take and efforts involved.

**Done!**