

Cloud Security Incident Response Plan for Cromulent Innovations

(Prepared exclusively for Cromulent Innovations by InterSlice, Inc.)

1. Introduction

This Cloud Security Incident Response Plan (CSIRP) is designed to guide the response to a security incident involving Cromulent Innovations' cloud infrastructure on AWS. This plan focuses on leveraging AWS services such as CloudTrail, CloudWatch, GuardDuty, and Lambda to detect, respond to, and mitigate security threats, specifically addressing the simulated event of a brute force attack on a Linux server EC2 instance.

2. AWS Components Overview

AWS CloudTrail: Provides event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. It helps in auditing, compliance, and governance.

AWS CloudWatch: Monitors AWS resources and applications in real time, providing metrics, logs, and alarms to detect anomalies and take automated actions.

AWS GuardDuty: A threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect AWS accounts and workloads.

AWS Lambda: A serverless compute service that runs code in response to events and automatically manages the compute resources required by that code.

3. Incident Response Steps

3.1 Preparation

- **Security Best Practices:** Ensure all AWS security best practices are followed, including IAM roles and policies, security groups, and network ACLs.
- **Logging and Monitoring:** Confirm that CloudTrail is logging all activities and CloudWatch is monitoring critical metrics and logs.
- **GuardDuty Configuration:** Ensure GuardDuty is enabled and properly configured to detect potential threats.
- **Lambda Function:** Prepare a Lambda function to respond automatically to certain security incidents, such as isolating a compromised instance.

3.2 Identification

1. **Detect Anomalous Activity:**

- GuardDuty detects potential brute force attack activities on the Linux server EC2 instance and generates a finding.
- CloudWatch Logs capture login attempts and detect a pattern indicative of a brute force attack.

2. **Alerting:**

- CloudWatch Alarm triggers based on predefined metrics (e.g., number of failed login attempts).
- Notifications are sent to the security team via Amazon SNS (Simple Notification Service).

3.3 Containment

1. **Automated Containment:**

- Lambda function is invoked upon receiving a GuardDuty finding or CloudWatch Alarm.
- The Lambda function can take actions such as isolating the affected EC2 instance by modifying its security group or network ACLs to block traffic from the malicious IP addresses.

2. **Manual Containment:**

- If necessary, the security team manually intervenes to isolate the affected instance and review security groups and network ACLs.

3.4 Eradication

1. **Identify Root Cause:**

- Use CloudTrail logs to trace the source of the attack and identify how the attacker gained access or attempted the brute force attack.

2. **Remediation Actions:**

- Patch vulnerabilities on the Linux server.
- Update IAM roles and policies to follow the principle of least privilege.
- Modify security group rules to implement more stringent access controls.

3.5 Recovery

1. **Restore Services:**

- Ensure the affected instance is clean and secure before restoring it to service.
- Monitor the instance closely for any signs of persistent threats.

2. **Validation:**

- Conduct a thorough review of the incident to confirm that the threat has been eradicated.
- Validate that all systems are functioning normally and securely.

3.6 Lessons Learned

1. **Incident Report:**

- Document the incident details, including detection, response actions, and lessons learned.

2. **Review and Improve:**

- Analyze the response process and identify areas for improvement.
- Update the incident response plan and security measures based on the findings.

4. AWS Components Connections

- **CloudTrail** logs API activity and sends data to CloudWatch Logs.
- **CloudWatch** monitors log data and triggers alarms based on predefined metrics.
- **GuardDuty** continuously analyzes AWS resources and logs to detect threats and sends findings to CloudWatch Events.
- **Lambda** is invoked by CloudWatch Alarms or GuardDuty findings to execute response actions, such as modifying security groups or sending notifications.

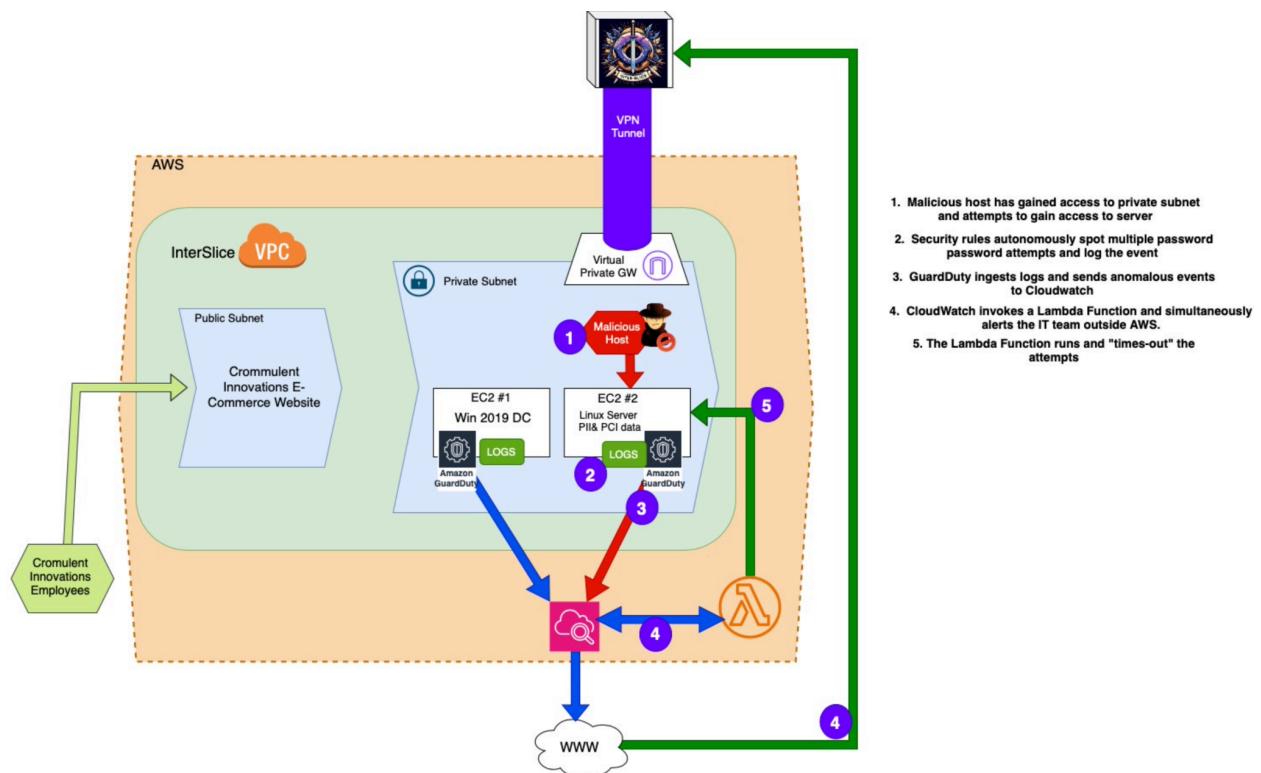
5. Simulated Event Process

1. **Simulated Attack:** A malicious host attempts to brute force the password on the Linux server.
2. **Detection:** GuardDuty detects the anomalous behavior and generates a finding.
3. **Alerting:** CloudWatch triggers an alarm and notifies the security team.

4. **Containment:** Lambda function is invoked to isolate the instance and block the malicious IP.
5. **Eradication:** The security team investigates and remediates vulnerabilities.
6. **Recovery:** The instance is restored to service after ensuring it is secure.
7. **Lessons Learned:** An incident report is created and the response process is reviewed.


By following this incident response plan, Cromulent Innovations can effectively manage and mitigate security incidents within their AWS environment, ensuring robust protection for their cloud infrastructure.

Diagram A.



References:

Here are some references that can help you understand the significance of having a cybersecurity incident response plan:

1. [[Incident-Response-Plan-Basics_508c.pdf \(cisa.gov\)](#)]: This document from the Cybersecurity and Infrastructure Security Agency (CISA) provides the basics of creating an incident response plan.
2. [ How to create a Cyber Security Incident Response Plan webinar]: This YouTube video offers a visual explanation of the incident response process.
3. [<https://www.bluevoyant.com/knowledge-center/what-is-incident-response-process-frameworks-and-tools>]: This article from BlueVoyant discusses the incident response process, frameworks, and tools.
4. [<https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance>]: This article from ISACA provides guidance on conducting cybersecurity incident response exercises.

I hope these resources are helpful to you.

Date	Employee	Change
05/28/24	Julian Pena	“SOP: Cybersecurity Incident Response Plan”