**Incident Response Playbook Template**

**Incident Type**

**Introduction**

**Summary of the playbook**

**Part 1: Acquire, Preserve, Document Evidence**

**Part 2: Contain the Incident**

**Part 3: Eradicate the Incident**

**Part 4: Recover from the Incident**

**Part 5: Post-Incident Activity**

**Additional Resources**

**Incident Response**

[**https://aws.amazon.com/blogs/security/how-get-started-security-response-automation-aws/**](https://aws.amazon.com/blogs/security/how-get-started-security-response-automation-aws/)[**https://docs.aws.amazon.com/whitepapers/latest/https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/welcome.html**](https://docs.aws.amazon.com/whitepapers/latest/https:/docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/welcome.html)[**https://aws.amazon.com/blogs/security/how-to-automate-incident-response-in-aws-cloud-for-ec2-instances/**](https://aws.amazon.com/blogs/security/how-to-automate-incident-response-in-aws-cloud-for-ec2-instances/)[**https://aws.amazon.com/blogs/security/forensic-investigation-environment-strategies-in-the-aws-cloud/**](https://aws.amazon.com/blogs/security/forensic-investigation-environment-strategies-in-the-aws-cloud/)[**https://aws.amazon.com/blogs/security/how-to-automate-forensic-disk-collection-in-aws/**](https://aws.amazon.com/blogs/security/how-to-automate-forensic-disk-collection-in-aws/)[**https://aws.github.io/aws-eks-best-practices/security/docs/incidents/**](https://aws.github.io/aws-eks-best-practices/security/docs/incidents/)[**https://docs.aws.amazon.com/guardduty/latest/ug/guardduty-remediate-kubernetes.html**](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty-remediate-kubernetes.html)