

Incident Response

CloudSiksha

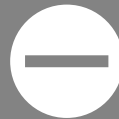
# Incident & Incident Response



Any event which poses a threat to security is an incident



Incident response is our response to such events



Sample incidents could be: failed attempt to break into the system, loss of a hard drive with sensitive data and so on



Incident response could be different for cloud than for our own data center, because we do not have control over hardware in the cloud

# Evidence Collection & RCA

- You can collect AWS Logs which can help in RCA
  - **VPC Flow Logs**
  - **Cloud Trail Logs**
  - **Guard Duty Logs**

# AWS Abuse Notice

- AWS does not allow customers to perform certain activities
  - **Port Scanning**
  - **Denial of Service Attack**
  - **Hosting of Copyrighted content**
  - **Distributing Malware**
  - **Intrusion Attempts**
- An abuse notice will send if the user is engaged in any of these activities
- If your systems are subjected to malicious attacks from AWS IPs you can submit an abuse notice

# Sample Abuse Notice Image

The screenshot displays the AWS Abuse console interface. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information. The left sidebar shows navigation options: 'Personal Health Dashboard', 'Dashboard', and 'Event log'. The main content area is titled 'Dashboard' and features three summary cards: '1 Open issues Past 7 days', '0 Scheduled changes', and '0 Other notifications Past 7 days'. Below these, a message states 'Issues that might affect your AWS infrastructure. 3 issues were resolved in the past 24 hours.' with a 'See all issues' link. A filter bar shows 'Start time: August 20, 2018 at 2:08:16 PM UTC-7' and an 'Add filter' button. A table lists the issues:

Event	Region...	Start time	Last update time	Affected res
Abuse copyright dmca ...	-	August 27, 2018 at 1:...	August 27, 2018 at 1:...	1 entity

The right-hand pane is titled 'Abuse copyright dmca report' and contains two tabs: 'Details' and 'Affected resources'. The 'Details' tab is active, showing the report timestamp 'Aug 27, 08:57 PM UTC' and the urgent message: '[URGENT: RESPONSE REQUIRED WITHIN 24 HOURS or your resources may be suspended]'. It explains that a notice has been received regarding infringing content and provides instructions for acknowledgment and removal. A list of four required steps for a counter-notice is provided at the bottom of the details pane.

**Details** | **Affected resources**

Aug 27, 08:57 PM UTC  
[URGENT: RESPONSE REQUIRED WITHIN 24 HOURS or your resources may be suspended]  
We've received a notice(s) that your AWS resource(s) listed in the 'Affected resources' tab has been posting, distributing, or hosting unlicensed copyright protected content. This is forbidden by our terms. A copy of the complaint identifying the allegedly infringing content is below.

Please acknowledge the receipt of this report and/or remove the allegedly infringing content within 24 hours. If you do not remove the content, we will take the necessary steps to disable access to the content, up to and including suspension of your account. You would have also received an email notification from [ec2-abuse@amazon.com](mailto:ec2-abuse@amazon.com) with this same report. Please reply directly to that email.

If you believe the content referenced in the notice is not infringing, you may provide a counter-notice to our Agent for Notice of Claims of Copyright Infringement via email at [ec2-abuse@amazon.com](mailto:ec2-abuse@amazon.com), [abuse@amazonaws.com](mailto:abuse@amazonaws.com) or to the physical address below. The counter-notice must include the following information:

1. Identify the material that was removed or disabled, and the location where it appeared before it was removed or disabled;
2. A statement by you declaring under penalty of perjury that you have a good faith belief that the material at issue was either misidentified or mistakenly removed;
3. Your name, address and telephone number;
4. A statement that you consent to the jurisdiction of the federal district court for the judicial district in which your address is located, and that you will accept service of process from the person who provided the notice set forth above (if you are located outside of the United States, you must state that you

Feedback | English (US) | © 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. | Privacy Policy | Terms of Use

# Dealing with Exposed Keys

- Keys can be exposed
  - When developers share keys
  - When keys are hardcoded in application
  - When keys are committed to Git Repository
- When you get to know a key is exposed
  - Find out the access levels associated with the key
  - Invalidate the credentials
  - Invalidate Temporary credentials if they were issued

# Compromised EC2 Instances



Lock down the instance



Take EBS Snapshot



Memory Dump



Perform Forensic Analysis to determine  
Root Cause

# Others



---

- Penetration Testing
- Pre-authorized scanning tools



Thanks



CloudSiksha