Incident Response

PRESENTATION BY:
S.SURESH
CLOUDSIKSHA

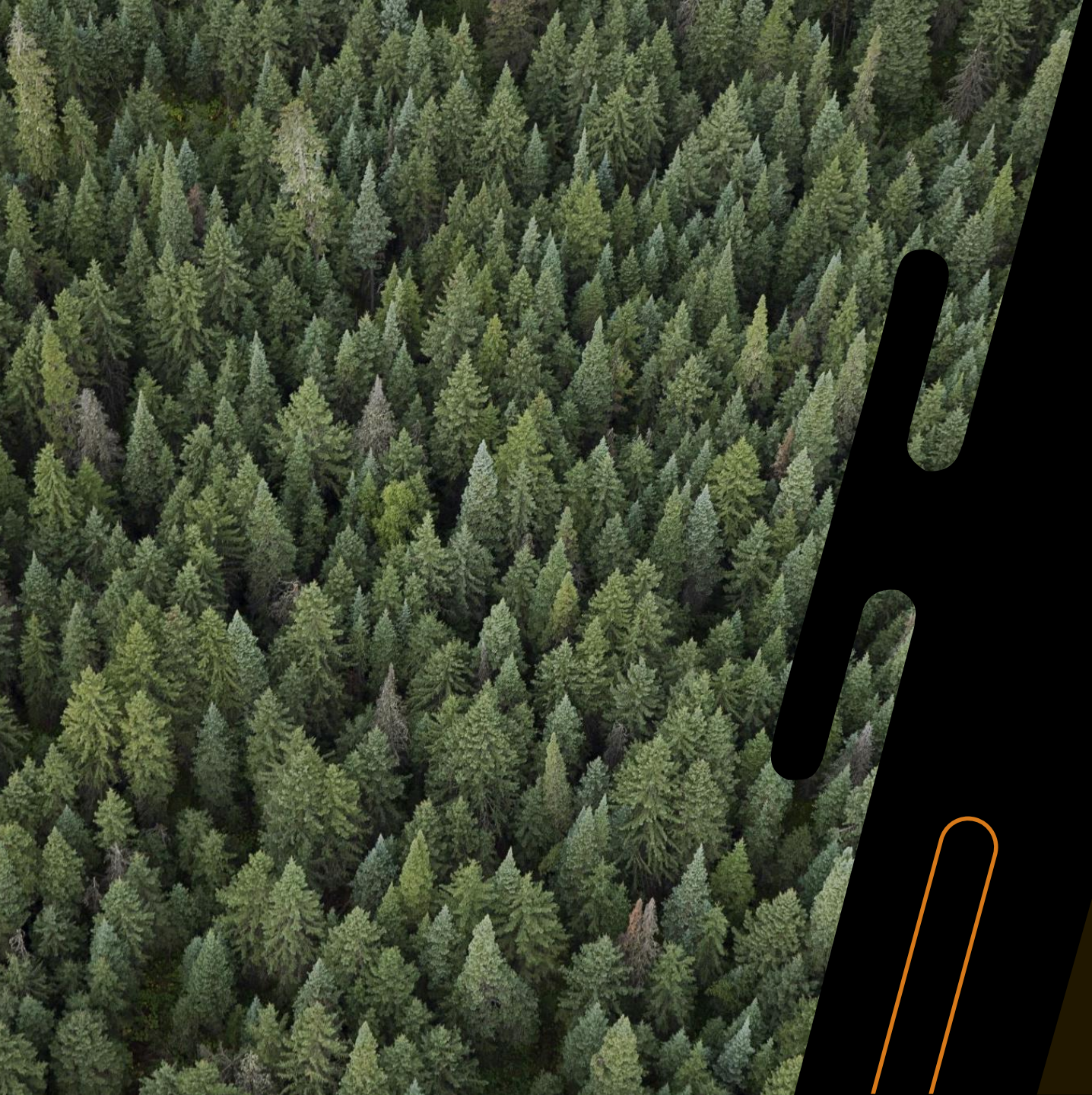
Incident & Incident Response

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 Finding
- AWS Detective

AWS Abuse Notice

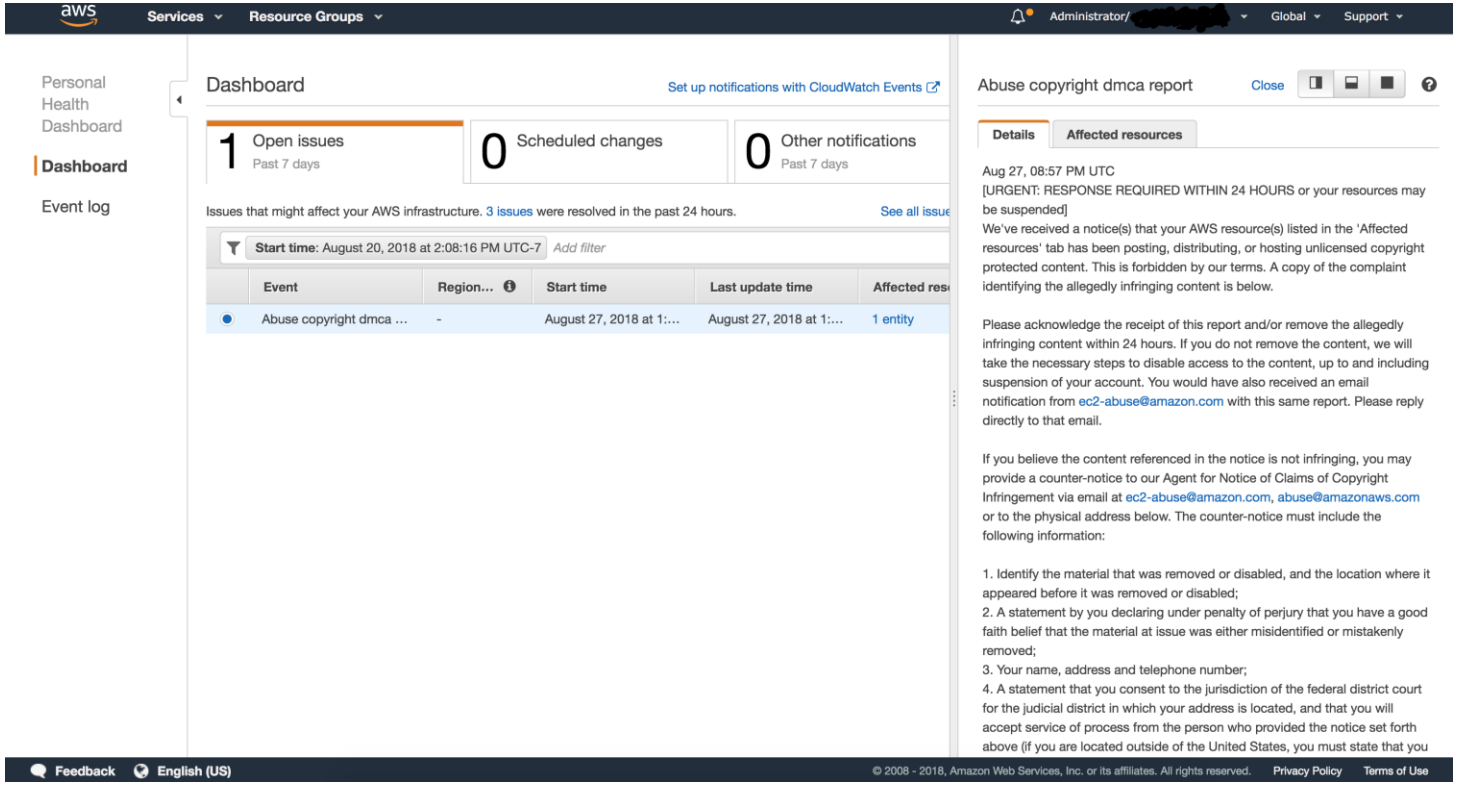
AWS does not allow customers to perform certain activities

- 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



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

Services that help in Incident Response

AWS Guard Duty

Detective

Thank you