

PART 2

1) Backdoor: EC2/Spambot:

Ec2 Instance is communicating on an unusual port 25 with a remote host.

Solution:



Check Inbound rules configured in the security group attached to the EC2 Instance and remove Custom Port 25 if it is not intended.

□	-	sgr-0cdfbdf1bfd345e01	IPv4	SMTP	TCP	25	0.0.0.0/0	-
---	---	-----------------------	------	------	-----	----	-----------	---

2) CloudWatch Alarm: CIS Sign-in without MFA:

Solution:



Activate MFA for the given account using IAM Service and use Authenticators like Google Authenticator or Duo as a Primary device for MFA.

Security alerts

⚠ The root user for this account does not have Multi-factor authentication (MFA) enabled. [Enable MFA](#) to improve security for this account.

Manage MFA device

Choose the type of MFA device to assign:

☒ **Virtual MFA device**
Authenticator app installed on your mobile device or computer

☐ **U2F security key**
YubiKey or any other compliant U2F device

☐ **Other hardware MFA device**
Gemalto token

For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#)

Cancel

Continue

Set up virtual MFA device



1. Install a compatible app on your mobile device or computer

See a [list of compatible applications](#)

2. Use your virtual MFA app and your device's camera to scan the QR code



Alternatively, you can type the secret key. [Show secret key](#)

3. Type two consecutive MFA codes below

MFA code 1

MFA code 2

[Cancel](#)

[Previous](#)

[Assign MFA](#)

3) Cryptocurrency: BitCoinToolB!DNS

Solution:



If AWS Guard Duty is signaling about the EC2 instance querying domain names related to bitcoin related activity. We can take following actions to mitigate the issues.



Determine which domain name or IP address triggered the signal.



Identify the process which requested the domain name or particular IP.



Find whether it is intended or unintended for the process to query the domain name.



Remove particular domain name or ip address from the process or application.



Blacklist those ip addresses in firewall.