

Steps for ThreatAlert-gss parent CloudFormation

1. Create a S3 bucket and name it “threatalertgss”
2. Put the 4 files in there (ThreatAlert-gss, ThreatSplunknSG, PaloAlto, and TASecurityServers)
   1. <https://github.com/stackArmor/Threat-Alert>
   2. ThreatAlert-gss is the parent stack
   3. ThreatSplunknSG, PaloAlto, and TASecurityServers are the three child stacks
      1. ThreatSplunknSG contains Threat Alerts, Splunk, and security groups
      2. PaloAlto contains Palo Alto
      3. TASecuritySevers contains Acunetix, Nessus, Jira, Okta, and SonarQube
3. Create a S3 bucket and name it “[customername]-paloaltoconfig-bucket”
4. Run the stack using ThreatAlert-gss (the parent stack)
5. Determine VPC (default is 10.0.0.0/24)
6. Determine FedRAMP (default is FedRamp-Moderate)
   1. This currently just tag server that the level of FedRamp based on this parameter
7. Put in the CIDR block for external access to the Remote Desktop Gateways
8. Select keypair
9. Change TAS3BucketName based on step 1
10. Put in the password for the DomainAdmin (needs symbol) and MicrosoftADPW
11. Change the DomainDNSName to the desired DNS. Default is “threatalert.stackarmor.com”
12. Change the instance types if desired
13. Change S3BucketNameP based on step 3
14. Enter DSMAdminPass and the number of DSM Protected Instances

