# Security Best Practices Mapped to NIST 800-53

| Security Best Practice | Severity | June | July | August |
|---|---|---|---|---|
| IAM User Policies with Full Admin Privileges | High | 5 | 5 | 6 |
| IAM Role Policies with Full Admin Privileges | High | 40 | 45 | 50 |
| IAM Users with Console Access with Initial Access Keys | High | 6 | 6 | 6 |
| EC2 Instances with Embedded Credentials | High | 14 | 16 | 17 |
| EC2 Instances without attached IAM Profile Role | High | 30 | 25 | 15 |
| IAM Policies Granted to IAM Users | Med | 40 | 45 | 45 |
| CloudTrail logs are not encrypted at rest | Med | 100 | 200 | 250 |
| Security Questions not Registered | Med | 10 | 15 | 18 |
| Rotation not Enabled for Customer Created CMKs for KMS Encryption | Low | 1 | 1 | 1 |
| CloudTrail Log File Validation not Enabled | Low | 1 | 1 | 1 |

# ADDITIONAL SECURITY RECOMMENDATIONS FROM PTP

- Account Issues – 4
- Network Issues – 2
- Cloud Service Issues - 1

# Security Best Practices – PTP Recommendations

## Account Issues

| Best Practice | PTP Score | May | June | July | August |
|---|---|---|---|---|---|
| IAM Password Policy Disabled | 10 | 18 | 12 | 14 | 14 |
| IAM Admin Users Not Utilizing Multi-Factor Authentication | 10 | 17 | 13 | 13 | 13 |
| Root AWS Accounts Not Utilizing Multi-Factor Authentication | 10 | 19 | 13 | 11 | 12 |
| Passwords not Reset for > 90 Days | 8 | 18 | 17 | 17 | 20 |

# Security Best Practices – PTP Recommendations

## Network Issues

| Best Practice | PTP Score | May | June | July | August |
|---|---|---|---|---|---|
| Network ACLs Allowing All Inbound Traffic | 8 | 300 | 200 | 250 | 275 |
| Blocklisted IP Address Making API Calls | 8 | 1 | 1 | 1 | 0 |

# Security Best Practices – PTP Recommendations

## Cloud Service Issues

| Best Practice | PTP Score | May | June | July | August |
|---|---|---|---|---|---|
| S3 Buckets Do Not Have Default Encryption Enabled | 8 | 50 | 40 | 40 | 30 |