1 AWS Security Fundamentals Cheatsheet

This cheatsheet was created by Rami McCarthy and Joshua Dow for the BASC 2019 AWS Security Fundamentals workshop.

1.1 AWS Built-in Security Tools

1. CloudTrail - view recent events and log AWS API calls
2. Trusted Advisor - audit best practices for use of AWS
    - Seven free security checks
    - Additional ~10 security checks add a 3% premium to AWS costs
        - May be worth it just for the “Exposed Access Keys” rule
    - Make sure you setup notifications to monitor state
3. GuardDuty - threat detection based on event analysis and baselining
    - 30 day free trial, then priced by volume of processing
4. Inspector - automated security assessment of AWS hosted applications
    - Free for 90 days + 250 of each assessment, then .10-.30$ per assement
    - Set standards and validate adherence
5. SecurityHub - collates security alerts across accounts, AWS tools, and AWS partner tools
    - Set custom response and remediation workflows with cloudwatch
    - Integrate with AWS Partners
6. Macie - ML for sensitive data discovery, classification, and protection
    - Machine Learning on where sensitive information is located and how it’s accessed
        - Only supports S3 currently
        - Prohibitively expensive

1.2 AWS Best Practices

1. Enable Built-in Security Tools
2. Secure Logging
    - Replicate logs to an unlinked account
        - Minimized access to these secured logs to only key personnel
    - Enable versioning on the bucket with MFA-delete
    - Make sure you enable CloudTrail in all regions
    - Setup CloudWatch metrics and alarms for major violation cases
3. Secure Public Access
    - Setup block public access for supported services (S3, EMR)
        - This can be enabled “going forward”
        - Use Trusted Advisor to audit
    - Check external exposure of EC2s (i.e ElasticSearch)
    - Secure deployed resources
        - EC2s and S3 buckets should have an ELB or CloudFront in front of them
            - Standardizing logging access
            - Allows chaining AWS services (Shield, WAF, etc.)
4. Secure Authentication
    - Roles > IAM Credentials > Username/Password Authentication
    - For applications, use EC2 roles, don’t use an IAM account
        - This is easy with the AWS SDK
        - Watch out for SSRF

- Only give users STS assume role permissions
- For development
  - Developer should get fresh, temporary credentials each day
  - Developers should not be able to push to ECR from their laptops
  - Use DevOps so that CI/CD always does build/deployment

5. Secure MFA
   - Hardware Tokens > One-Time Password > SMS

1.3 Third-Party Tools

1. Prowler
   - CIS AWS Benchmark (49 checks) + 40 additional checks including related to GDPR and HIPAA.
2. ScoutSuite
   - Multi-Cloud support with over 100 checks
3. Cloudmapper
   - ~50 checks, some unique from other tools

1.4 Resources

- Scott Piper – https://summitroute.com/ - @0xdabbad00 - AWS Security Maturity Roadmap
- Toni de la Fuente - AWS Security Tool Arsenal - @ToniBlyx
- Rhino Security - https://rhinosecuritylabs.com/blog/?category=aws
- Cloudonaut - https://cloudonaut.io/aws-security-primer/
- Corey Quinn - https://www.lastweekinaws.com - @QuinnyPig
- Teri Radichel - https://2ndsightlab.com/ - @TeriRadichel