Security

Đà Nẵng, năm COVID thứ 2

AWS Shield:

- DDoS Protection
- AWS Shield Standard: Free Service.
- AWS Shield Advanced: Paid Service.
- You can add protection for any of the following resource types:
  - CloudFront distributions
  - Route 53 hosted zones
  - ELB load balancers
  - EC2 Elastic IP addresses.
  - AWS Global Accelerator accelerators

AWS WAF:

- Web Application Firewall for CloudFront, API Gateway, Application Load Balancer, or AppSync GraphQL API.
- Web ACL: a set of rules in AWS WAF to protect your AWS resources.
- Each rule requires at least one top-level statement, which might contain nested statements at any depth, depending on the rule and statement type.
- Statements can be combined using AND, OR or NOT.

- Examples of criteria in the statements:
  - Scripts or SQL code that are likely to be malicious, like cross-site scripting (XSS) or SQL injection.
  - IP addresses or address ranges that requests originate from.
  - Country or geographical location that requests originate from.
  - Strings that appear in the request, like in the User-Agent header or the query string. Supports use of regular expressions (regex).
  - Request size limit.

- Each rule contains action to take if a web request meets the criteria:
  - Count. You can insert custom headers into the request and you can add labels that other rules can match against.
  - Allow. You can insert custom headers into the request before forwarding it to the protected resource.
  - Block. You can customize the response. Default response is HTTP 403 (Forbidden).
- Labels:
  - A label is metadata that a rule can add to matching web requests.
  - Rules can also match against labels when they inspect web requests.
  - Labels allow a matching rule to communicate results to the rules that are evaluated later in the same web ACL.

- You can use rules individually or in reusable rule groups.
- AWS Managed Rules and AWS Marketplace sellers provide managed rule groups for your use.
- You can add a scope-down statement inside some rules: narrows the scope of the requests that the rule evaluates. Can be also applied to rate-based rules.
- Bot Control: helps you manage bot activity to your site by categorizing and identifying common bots.
- For a CloudFront distribution, AWS WAF is available globally, but you must use the region US East (N. Virginia) for all of your work.
- Uses web ACL capacity units (WCU) to calculate and control the operating resources that are required to run your rules, rule groups, and web ACLs.

Amazon Inspector:

- Assesses applications for exposure, vulnerabilities, and deviations from best practices.
- Assessments can be automated to integrate with deployment pipelines.
- Optional agent on EC2 instances: collects installed package information and software configuration.
- You can use Amazon Inspector to assess your assessment targets (collections of AWS resources) for potential security issues and vulnerabilities.
- Compares the behavior and the security configuration of the assessment targets to selected security rules packages.

- A rule is a security check that Amazon Inspector performs during the assessment run.
- Rules are grouped into distinct rules packages either by category, severity, or pricing.
- Rule Severity: High, Medium, Low or Informational.
- Available rule packages:
  - Network Reachability (network assessment).
  - Common vulnerabilities and exposures (host assessment).
  - Center for Internet Security (CIS) Benchmarks (host assessment).
  - Security best practices for Amazon Inspector (host assessment).

Amazon GuardDuty

- A continuous security monitoring service that analyzes and processes the following Data sources:
  - VPC Flow Logs,
  - CloudTrain Event Logs.
  - CloudTrail management Events,
  - CloudTrail S3 Data Event,
  - DNS logs.

- Uses threat intelligence feeds, such as lists of malicious IP addresses and domains, and machine learning to identify unexpected and potentially unauthorized and malicious activity within your AWS environment.
- This can include issues like escalations of privileges, uses of exposed credentials, or communication with malicious IP addresses, or domains.
- For example, GuardDuty can detect compromised EC2 instances serving malware or mining bitcoin.
- Also monitors AWS account access behavior for signs of compromise, such as unauthorized infrastructure deployments, like instances deployed in a Region that has never been used, or unusual API calls, like a password policy change to reduce password strength.
- Can trigger remediation actions.
- Supports a Trusted IP list and multiple Threat lists (lists of known malicious IPs).

AWS Security Hub:

- Provides you with a comprehensive view of your security state in AWS.
- Helps you check your environment against security industry standards and best practices.
- Collects security data from across AWS accounts, services, and supported third-party partner products.
- Consumes, aggregates, organizes, and prioritizes findings from AWS services that you have enabled, such as Amazon GuardDuty, Amazon Inspector, Amazon Macie and AWS partner security products.
- Helps you analyze your security trends.
- Identify the highest priority security issues.
- Correlates findings across providers to prioritize the most important ones.
- Supports integration with Amazon EventBridge. To automate remediation of specific findings, you can define custom actions to take when a finding is received.