SECURITY IN AWS

Security in AWS is essential for protecting sensitive data, meeting compliance obligations, managing risks, and maintaining customer trust. By implementing robust security measures, organizations can safeguard their assets, ensure business continuity, and thrive in the cloud environment.

These are the two popular AWS services that play important role in ensuring security, compliance and governance within your AWS environment.

1. AWS CONFIG:

a. Configuration History:
AWS Config maintains a detailed history of configuration changes to resources over time. This allows you to track when changes occurred, who made them, and what the changes were.

b. Config Rules:
— Config Rules are a powerful feature that enables you to define and enforce guidelines for your AWS resource configurations. These rules can check for compliance with security policies, industry regulations, and operational best practices.

c. Resource Relationships:
— The Resource Relationships Graph in AWS Config provides a visual representation of how AWS resources are related. It helps you understand dependencies and relationships between resources.

d. Configuration Snapshots:
— AWS Config allows you to capture point-in-time snapshots of your resource configurations. These snapshots can be useful for

auditing, compliance checks, and understanding the state of resources at specific moments.

e. **Custom Rules and Remediation:**
— AWS Config supports the creation of custom Config Rules using AWS Lambda functions. This allows you to tailor the evaluation of configurations to your specific needs. Remediation actions can also be automated using AWS Systems Manager Automation.

CONFIGURATION:

Setting up AWS Config for security involves several steps, including creating a configuration recorder, defining rules to evaluate your resources, and setting up notifications.

Step 1: Enable AWS Config

1. Sign in to the AWS Management Console.
2. Navigate to AWS Config.
3. Choose Get Started.
4. Set up the configuration recorder:
    - Choose the resource types you want to monitor (e.g., EC2 instances, S3 buckets).
    - Select an S3 bucket to store configuration snapshots (create one if you don't have it).
    - Optionally, select an IAM role for AWS Config to use for permissions.
5. Choose Next.

Step 2: Set Up AWS Config Rules

1. After configuring the recorder, you'll set up rules.
2. In the AWS Config console, choose Rules.
3. Click on Add rule.
4. Select a rule to evaluate security best practices. For example, you can choose:
    - s3-bucket-public-read-prohibited: Checks that S3 buckets don't allow public read access.
    - ec2-instance-no-public-ip: Ensures that EC2 instances do not have public IPs assigned.

5. Configure the rule:
    - Specify the resource types.
    - Set any parameters required by the rule.
    - Choose the desired compliance types (e.g., compliant or non-compliant).
6. Click Add rule.

Step 3: Set Up Notifications (Optional)

1. You may want to set up notifications for compliance changes:
    - Go to Amazon SNS and create a topic.
    - Subscribe your email or another endpoint to the topic.
2. In AWS Config, navigate to Settings.
3. Under Notifications, specify the SNS topic you created.

Step 4: View Compliance Status

1. Go back to the AWS Config dashboard.
2. Click on Rules to see the compliance status of your resources.
3. You can view details of any non-compliant resources and take necessary actions.

2. AWS SECURITY HUB:

a. Aggregation of Findings:
— AWS Security Hub aggregates findings from various AWS security services, including Amazon GuardDuty, AWS Inspector, AWS Firewall Manager, and others. This centralizes security information and simplifies the monitoring of security alerts.

b. Prioritization and Insights:
— Security Hub prioritizes findings using its own insights and provides a dashboard that gives you a clear view of your security posture. Findings are categorized and prioritized based on severity, allowing you to focus on the most critical issues first.

c. Security Standards and Compliance:
— AWS Security Hub supports security standards like CIS AWS Foundations Benchmark. It helps you monitor your compliance with these standards and provides actionable recommendations to improve your security posture.

d. Integrated Remediation:
— For certain findings, AWS Security Hub provides integrated remediation actions. This means you can take immediate actions to remediate security issues directly from the Security Hub console.

e. Collaboration and Insights Across Accounts:
— Security Hub allows you to aggregate findings from multiple accounts, making it easier for security teams to collaborate and get a holistic view of the organization's security status.

CONFIGURATION:

Setting up AWS Security Hub is a great way to centralize security findings and improve your security posture.

Step 1: Enable AWS Security Hub

1. Sign in to the AWS Management Console.
2. Navigate to AWS Security Hub.
3. Click on Get Started.
4. Choose Enable Security Hub.
5. Review the settings and click Enable Security Hub.

Step 2: Configure Security Standards

1. After enabling, you'll be directed to the Security Standards page.
2. AWS Security Hub provides built-in standards, like:
    - CIS AWS Foundations Benchmark
    - PCI DSS
    - AWS Foundational Security Best Practices
3. Select the standards you want to enable by checking the boxes next to each.
4. Click Update to save your selection.

Step 3: Integrate with Other AWS Services

1. Amazon GuardDuty: Go to the GuardDuty console and enable it if it's not already active. GuardDuty findings will automatically be imported into Security Hub.
2. Amazon Inspector: Enable Amazon Inspector for vulnerability scanning on your EC2 instances and container images. Findings will flow into Security Hub.
3. AWS Config: Ensure AWS Config is set up to monitor resource compliance.
4. AWS CloudTrail: Ensure CloudTrail is enabled for logging API calls.

Step 4: Connect Third-Party Solutions (Optional)

1. If you have third-party security tools, you can integrate them with Security Hub.
2. In the Security Hub console, go to Integrations.
3. Select Third-Party Solutions and choose the desired solution.

4. Follow the specific integration instructions provided for each solution.

Step 5: Review Findings

1. Once everything is set up, navigate to the Findings page in Security Hub.
2. You'll see a consolidated view of security findings from all integrated services.
3. Findings can be filtered by severity, compliance status, and other attributes.

Step 6: Create Insights and Actions

1. Use the Insights feature to create custom views based on your security needs.
2. You can also create CloudWatch Events rules to trigger actions based on findings.
    - For example, you can trigger an AWS Lambda function to remediate specific findings.

Step 7: Set Up Notifications (Optional)

1. Use Amazon SNS to set up notifications for new findings.
    - Create an SNS topic and subscribe to it.
2. In Security Hub, go to Settings and configure the SNS topic for notifications.

Step 8: Continuous Monitoring and Response

1. Regularly check the Findings dashboard for new alerts.
2. Investigate and prioritize findings based on severity.
3. Implement remediation actions as needed and track them over time.

SUMMARY OF DIFFERENCES:

Feature/Aspect	AWS Config	AWS Security Hub
Primary Focus	Configuration management and compliance	Aggregation of security findings
Functionality	Tracks resource configurations and changes	Centralizes security alerts and findings
Rules	Customizable rules for compliance checks	Predefined standards and insights
Data Sources	Monitors AWS resource configurations	Integrates findings from multiple AWS services
Remediation	Automated remediation of non-compliant resources	Can trigger responses based on findings
Use Case Examples	Compliance audits, resource tracking	Threat detection, compliance assessment