AWS Security Hub: Overview and Best Practices

Why Use AWS Security Hub

AWS Security Hub is a comprehensive security service that provides you with a central view of your security posture across your AWS accounts. It allows you to aggregate, prioritize, and act on findings from various AWS security services, as well as partner solutions. Here's why and how you should use AWS Security Hub:

1. Centralized Security Visibility

Security Hub aggregates and normalizes findings from various AWS services such as Amazon GuardDuty, AWS Inspector, and Amazon Macie, providing a centralized and standardized view of your security posture.

2. Automated Compliance Checks

Security Hub automates continuous compliance checks against the AWS best practices and industry standards (such as CIS AWS Foundations Benchmark), helping you identify and remediate potential security vulnerabilities.

3. Prioritized Security Alerts

Findings in Security Hub are normalized and prioritized, allowing you to focus on the most critical issues first. This helps in efficient resource allocation for remediation efforts.

4. Integration with AWS Config

Security Hub integrates with AWS Config, providing you with a historical view of your security findings and changes to your AWS resources over time.

5. Custom Actions and Insights

You can create custom actions in Security Hub to automate response or remediation processes based on specific findings. This allows for a more automated and efficient security workflow.

6. Integration with Partner Solutions

Security Hub allows you to integrate with third-party security tools and solutions, extending its capabilities beyond AWS-native services.

Pros and Cons of AWS Security Hub

Pros:

1. **Centralized Security Visibility**: Offers a unified view of security findings across multiple AWS accounts.

2. **Automated Compliance Checks**: Streamlines compliance monitoring and provides insights into adherence to security best practices.

3. **Prioritization and Normalization**: Helps prioritize and normalize findings, allowing for efficient remediation.

4. **Integration with AWS Services**: Integrates with various AWS security services, providing a comprehensive security solution.

5. **Custom Actions**: Enables the creation of custom actions for automated response to security incidents.

6. **Partner Integrations**: Supports integration with third-party security solutions for a more holistic security approach.

Cons:

1. **Costs**: While AWS Security Hub has a free tier, additional charges may apply based on the number of findings ingested and the use of certain premium features.

2. **Learning Curve**: Configuring and managing Security Hub effectively may require some learning, especially for organizations new to AWS security services.

3. **Dependency on Other AWS Services**: The effectiveness of Security Hub depends on the availability and proper configuration of other AWS security services.

Cost of AWS Security Hub

Prepackaged security standards are available for Security Hub, such as the CIS AWS Foundations Benchmark, AWS Foundational Security Best Practices, National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5, and the Payment Card Industry Data Security Standard (PCI DSS). Conducting security checks against these standards can help evaluate the security posture of your AWS accounts and resources. These prepackaged standards are collections of controls that Security Hub continuously evaluates to identify if any accounts or resources deviate from the defined security best practices. The evaluation of a control against a single AWS resource is referred to as a security check, and it results in a finding that shows the result of the check. You are only charged once for a check when identical controls that are common across different standards are evaluated against the same resource.

Pricing:

First 100,000 checks/month	$0.0010 per check
Next 400,000 checks/month	$0.0008 per check
Over 500,000 checks/month	$0.0005 per check

Security Hub security checks leverage configuration items recorded by AWS Config. AWS Config is required for these security checks, and configuration items are priced separately from Security Hub. Please see Config pricing for details.

It's important to regularly review the AWS pricing page for the most up-to-date information on AWS Security Hub costs and consider how your organization's usage may impact overall expenses.

In summary, AWS Security Hub is a valuable tool for organizations seeking to enhance their security posture on AWS. The pros, including centralized visibility and compliance automation, often outweigh the cons, and careful consideration of costs is essential for effective budget management.

AWS Documentation