International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V71I4P103

Volume 71 Issue 4, 14-18, April 2023
© 2023 Seventh Sense Research Group®

Original Article

Future-Proofing Security: AWS Security Hub and Service Now Integration

Ashok Kumar Padmaraju

Leading BioPharma Industries, Raleigh, NC, USA

Received: 21 February 2023 Revised: 24 March 2023 Accepted: 05 April 2023 Published: 15 April 2023

Abstract - *Primary The article "Future-Proofing Security: AWS Security Hub and ServiceNow Integration" explores the benefits of integrating AWS Security Hub with ServiceNow SIEM for businesses seeking to improve their security posture. The article highlights the challenges organizations face in today's complex threat landscape. It discusses how integrating these two tools can help businesses avoid emerging threats. The report also offers a detailed overview of AWS Security Hub and ServiceNow SIEM. It outlines how they work together to provide a comprehensive security solution. Ultimately, the article offers practical insights on maximizing their business's security efficiency by integrating these two tools.*

Keywords - *AWS Security Hub, Cloud Security Monitoring, Future-Proofing Security, Incident Management, ServiceNow SIEM.*

1. Introduction

In today's ever-evolving security landscape, organizations need a robust security framework that promptly detects and respond to threats. Integrating AWS Security Hub and ServiceNow provides a powerful solution for organizations to maximize their security efficiency. This integration allows security teams to detect and respond to threats promptly, streamline their security operations, and manage compliance more efficiently. Digital landscape, cybersecurity threats are becoming more sophisticated and challenging to detect. To protect themselves and their customer's data must ensure that their security measures keep up with the evolving threat landscape. AWS Security Hub and ServiceNow SIEM are potent tools to help businesses future-proof their security posture.

As organizations adopt cloud-based infrastructure, ensuring the cloud environment's security is well-managed and maintained is crucial. Security incidents can occur anytime, and detecting and responding promptly to mitigate the risks is essential. Amazon Web Services (AWS) provides several security tools to help organizations maintain the security of their cloud environment. AWS Security Hub is a central hub for managing security compliance. It provides a unified view of security alerts and compliance status across the organization. Integrating AWS Security Hub with ServiceNow Security Information and Event Management (SIEM) solution can help organizations manage their security alerts efficiently. This article will explore how AWS Security Hub integrates with the ServiceNow SIEM solution.

2. Exploring the State of the Art: A Comprehensive Literature Review on AWS Security Hub and Service Now Integration for Future-Proofing Security

AWS Security Hub and ServiceNow integration is a topic of growing importance in cybersecurity. As organizations increasingly rely on cloud services, they face the challenge of securing their data and infrastructure from various cyber threats. The integration of AWS Security Hub and ServiceNow aims to provide a comprehensive security solution to help organizations future-proof their security infrastructure.

Several studies have explored the benefits and challenges of AWS Security Hub and ServiceNow integration. In a recent survey of AWS, the authors highlight the importance of automating security processes to enable organizations to identify and remediate security issues quickly. The integration of AWS Security Hub and ServiceNow provides a centralized platform for managing security incidents, enabling security teams to gain greater visibility and control over their security infrastructure.

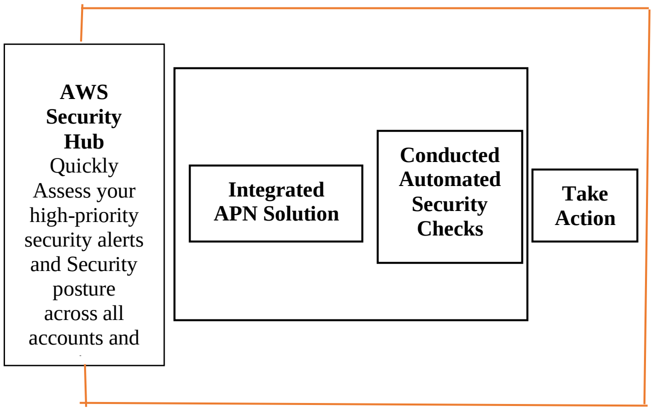
Another study by ServiceNow highlights the benefits of integrating ServiceNow's IT Service Management (ITSM) solution with AWS Security Hub. The authors note that the integration can help organizations streamline their security incident management processes, enabling security teams to identify and respond to security incidents more effectively.

Furthermore, a study by Gartner highlights the importance of integrating security and IT operations. The authors note that integrating security and IT operations can help organizations improve their security posture by enabling them to quickly identify and remediate security issues. The integration of AWS Security Hub and ServiceNow can help organizations achieve this goal by providing a centralized platform for managing security incidents.

The integration of AWS Security Hub and ServiceNow is a topic of growing importance in the field of cybersecurity. Several studies have highlighted the benefits of this integration, including improved visibility, streamlined incident management processes, and improved security posture. As organizations face evolving cyber threats, integrating AWS Security Hub and ServiceNow can help them future-proof their security infrastructure and stay ahead of potential threats.

3. Overview of AWS Security Hub

The AWS cloud, or Amazon Web Services cloud, is a suite of on-demand cloud computing services provided by Amazon. AWS offers various services, including computing, storage, database, analytics, machine learning, and more. These services enable businesses to run applications and services without managing their infrastructure, providing greater agility and scalability. AWS cloud offers companies a flexible and cost-effective solution for running their IT infrastructure. By using the AWS cloud, businesses can eliminate the need for physical data centers, which require significant capital investment and ongoing maintenance costs. With AWS cloud, companies can pay for only the resources they use, reducing costs and increasing agility.


AWS Security Hub
Quickly Assess your high-priority security alerts and Security posture across all accounts and
Integrated APN Solution
Conducted Automated Security Checks
Take Action

AWS Security Hub is a security management service that provides a centralized view of security alerts and compliance status across AWS accounts. Security Hub aggregates and prioritizes security alerts from various AWS services, including Amazon GuardDuty, Amazon Inspector, and Amazon Macie. It also integrates with third-party security tools such as vulnerability scanners and intrusion detection systems. Security Hub provides a dashboard that shows an overview of security and compliance status across all AWS accounts. The dashboard displays security findings and compliance status categorized by severity, resource type, and compliance standard. Security Hub also provides a compliance dashboard that shows the compliance status of resources against various compliance standards, such as HIPAA, PCI DSS, and CIS AWS Foundations Benchmark.

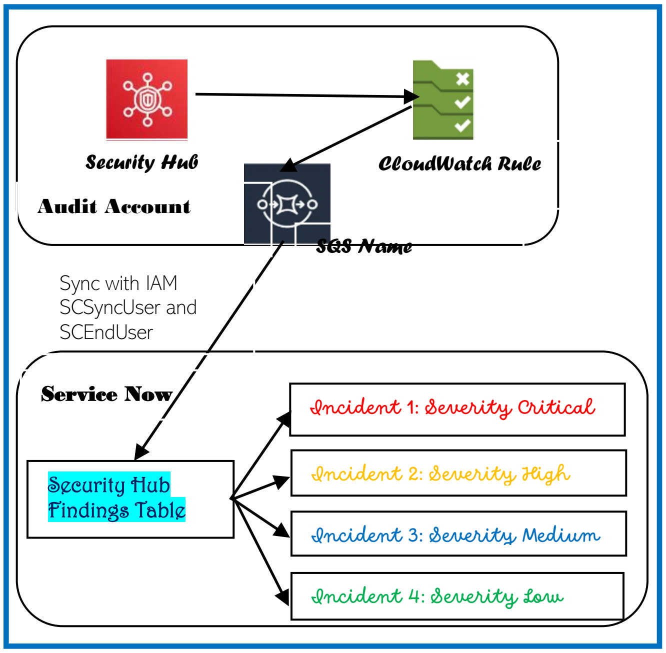
4. Overview of ServiceNow SIEM Solution

ServiceNow SIEM, or Security Information and Event Management, is a security solution provided by ServiceNow, a leading IT service management (ITSM) platform. ServiceNow SIEM delivers real-time analysis of security events using machine learning algorithms, enabling security teams to detect and respond to threats promptly. ServiceNow SIEM is designed to provide businesses with a powerful solution for managing security incidents. The solution offers real-time analysis of security events and enables security teams to detect and respond to threats promptly. ServiceNow SIEM aggregates security events and alerts from multiple sources, including network devices, servers, applications, and cloud infrastructure. The solution uses machine learning algorithms to analyze security events and signals in real-time, enabling security teams to detect and respond to threats promptly.

ServiceNow SIEM is a security information and event management solution that analyzes security events and alerts. SIEM solutions collect and analyze log data from various sources, including network devices, servers, and applications, to promptly detect and respond to security incidents. ServiceNow SIEM provides a central dashboard that displays security events and alerts. The dashboard summarizes security incidents categorized by severity, source, and type. ServiceNow SIEM also provides real-time analysis of security events using machine learning algorithms to detect anomalies and potential security incidents.

5. Integration of AWS Security Hub with ServiceNow SIEM

Integrating AWS Security Hub with ServiceNow SIEM enables organizations to manage security incidents more efficiently by providing a centralized view of security alerts and compliance status. ServiceNow SIEM can automatically receive security alerts from AWS Security Hub and create incidents in the ServiceNow platform. This integration enables security teams to respond to security incidents quickly and efficiently.


Security Hub
CloudWatch Rule
Audit Account
SQS Name
Sync with IAM SCSyncUser and SCEndUser
Service Now
Security Hub Findings Table
Incident 1: Severity Critical
Incident 2: Severity High
Incident 3: Severity Medium
Incident 4: Severity Low

The integration of AWS Security Hub and ServiceNow SIEM involves the following steps:

1. Create an AWS Security Hub account and enable the integration with ServiceNow SIEM.
2. Configure ServiceNow SIEM to receive security alerts from AWS Security Hub. This configuration involves creating an AWS Security Hub webhook that sends security alerts to ServiceNow SIEM.
3. Create a ServiceNow Incident Management integration to receive security alerts from AWS Security Hub. This integration enables ServiceNow SIEM to create incidents automatically when it receives security alerts from AWS Security Hub.
4. Test the integration to ensure ServiceNow SIEM receives security alerts and incidents created correctly.

6. Seven Steps to Strengthen AWS Security Hub and Service Now Integration Implementation

Implementing AWS Security Hub and ServiceNow integration requires careful planning and execution to ensure it is configured effectively. Here are some recommended implementation steps:

Step 1. Assess Your Current Security Infrastructure: The first step is to assess your current security infrastructure to identify gaps and areas for improvement. You should review your existing security tools, processes, and policies to determine what needs improvement or added to protect your data and infrastructure.

Step 2. Plan Your Integration Strategy: The next step is to plan your integration strategy. It involves identifying the AWS services and ServiceNow modules you want to integrate, defining the integration workflows, and setting up the necessary connectors and APIs.

Step 3. Configure Your AWS Security Hub: You need to configure your AWS Security Hub to enable the integration with ServiceNow. It involves setting up the necessary IAM roles, permissions, and AWS Security Hub standards.

Step 4. Configure Your ServiceNow Instance: You need to configure your ServiceNow instance to enable the integration with AWS Security Hub. It involves setting up the necessary ServiceNow tables, fields, and workflows to receive and process security incident data from AWS Security Hub.

Step 5. Test Your Integration: Once you have configured your AWS Security Hub and ServiceNow instance, you should test the integration to ensure it works correctly. You should try the integration workflows, incident management processes, and reporting capabilities to ensure the integration effectively captures and processes security incidents.

Step 6. Monitor and Fine-Tune Your Integration: After implementing and testing the integration, you should continue to monitor and fine-tune it to ensure it performs effectively. You should regularly review the integration workflows, incident management processes, and reporting capabilities to identify areas for improvement and optimize the integration's performance.

Step 7. Train Your Security Team: Finally, you should train your security team on how to use the integrated platform effectively. Your team should be familiar with the integration workflows, incident management processes, and reporting capabilities, enabling them to identify and respond to security incidents quickly and effectively.

By following these implementation steps, organizations can effectively implement AWS Security Hub and ServiceNow integration and future-proof their security infrastructure. The integration provides a comprehensive security solution that enables organizations to gain greater visibility and control over their security infrastructure, streamline incident management processes, and automate security processes. With careful planning, execution, and monitoring, organizations can effectively implement this integration and better protect their data and infrastructure from evolving cyber threats.

7. Benefits of Integrating AWS Security Hub with ServiceNow SIEM

Integrating AWS Security Hub with ServiceNow SIEM provides several benefits for organizations, including:

7.1. Centralized View of Security Alerts

Integrating AWS Security Hub with ServiceNow SIEM provides a centralized view of security alerts across all AWS accounts. This integration enables security teams to manage security incidents more efficiently by providing a single platform for monitoring and responding to security alerts.

7.2. Improved Visibility

The integration provides comprehensive visibility into an organization's security infrastructure, including cloud services, network devices, and endpoints. This visibility enables security teams to identify security threats and vulnerabilities more quickly and take action to remediate them.

7.3. Real-time Analysis of Security Events

ServiceNow SIEM provides real-time analysis of security events using machine learning algorithms. This analysis enables security teams to detect and respond to security incidents promptly.

7.4. Streamlined Incident Management

The integration streamlines incident management processes, enabling security teams to identify and respond to security incidents more effectively. The integration enables automatic ticket generation in ServiceNow, allowing security teams to assign and track incidents quickly.

7.5. Automated Security Processes

The integration automates security processes, enabling organizations to identify and remediate security issues quickly. Automated processes reduce the workload on security teams, allowing them to focus on more critical tasks.

Compliance Management: AWS Security Hub provides a compliance dashboard that shows the compliance status of resources against various compliance standards, such as HIPAA, PCI DSS, and CIS AWS Foundations Benchmark. Integrating AWS Security Hub with ServiceNow SIEM enables security teams to manage compliance status more efficiently by providing a single platform for monitoring and managing compliance.

7.6. Improved Collaboration

Integrating AWS Security Hub with ServiceNow SIEM enables security teams to collaborate more efficiently by providing a single platform for managing security incidents. This collaboration allows security teams to respond to security incidents promptly and efficiently.

7.7. Reduced Operational Costs

Integrating AWS Security Hub with ServiceNow SIEM enables organizations to reduce operational costs by automating incident creation and reducing the time required to respond to security incidents. This automation allows security teams to focus on critical security incidents and reduce the time necessary to manage routine security incidents.

8. Conclusion

Integrating AWS Security Hub with ServiceNow SIEM enables organizations to manage security incidents more efficiently by providing a centralized view of security alerts and compliance status across all AWS accounts. This integration allows security teams to respond promptly and efficiently, reducing the risks associated with security incidents. AWS Security Hub provides a comprehensive view of security alerts and compliance status. In contrast, ServiceNow SIEM delivers real-time analysis of security events using machine learning algorithms. Integrating these two solutions enables organizations to manage security incidents more efficiently, reducing the risks associated with security incidents and improving compliance management.

References

[1] Internet of Things (IoT). [Online]. Available: https://en.wikipedia.org/wiki/internet_of_things

[2] The AWS Website, 2021. [Online]. Available: https://aws.amazon.com/blogs/enterprise-strategy/new-possibilities-seven-strategies-to-accelerate-your-application-migration-to-aws

[3] The AWS Website, 2022. [Online]. Available: https://pages.awscloud.com/rs/112-TZM-766/images/AWS_Migration_8_Best_Practices_ebook_final.pdf

[4] The AWS Website, 2022. [Online]. Available: https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-retiring-applications/overview.html

[5] The AWS Website, 2022. [Online]. Available: https://aws.amazon.com/cloud-migration/how-to-migrate

[6] The AWS Website, 2022. [Online]. Available: https://d1.awsstatic.com/Migration/migrating-to-aws-ebook.pdf

[7] [Online]. Available: https://sacumen.com/case-studies/siem/servicenow-integration-with-siem-platform/

[8] Adrian Grigorof, CISSP, CISM, CRISC, CCSK Website. [Online]. Available: https://www.managedsentinel.com/siem-traditional-vs-cloud/

[9] [Online]. Available: https://www.bacancytechnology.com/blog/integration-in-servicenow

[10] The Gartner Website, 2022. [Online]. Available: https://www.gartner.com/en/conferences/hub/cloud-conferences/insights/how-to-build-a-cloud-center-of-excellence

[11] The Gartner Website, 2022. [Online]. Available: https://emtemp.gcom.cloud/ngw/globalassets/en/doc/documents/726566-innovation-insight-for-the-cloud-center-of-excellence.pdf

[12] The Cloud Security Alliance Website, 2022. [Online]. Available: https://cloudsecurityalliance.org/blog/2021/10/21/cloud-compliance-frameworks-what-you-need-to-know

[13] Mahesh M. Baradkar, Dr.Bandu B. Meshram, "A Survey on Cloud Security: Infrastructure as a Service," *SSRG International Journal of Computer Science and Engineering*, vol. 6, no. 6, pp. 17-21, 2019. [CrossRef] [Publisher Link]

[14] Blesson Varghese, and Rajkumar Buyya, "Next Generation Cloud Computing? New Trends and Research Directions," *Future Generation Computer Systems*, vol. 79, pp. 849-861, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[15] Ramesh Venkataraman, and Brian Terry, The AWS Website, 2021. [Online]. Available: https://aws.amazon.com/blogs/security/how-to-set-up-two-way-integration-between-aws-security-hub-and-servicenow/

[16] The Servicenow Website, 2019. [Online]. Available: https://www.servicenow.com/community/itsm-articles/amazon-web-services-security-hub-integration-to-servicenow-itsm/ta-p/2302520

[17] Sunil Gupta, AWS Security Automation: Penetration Testing and Security Assessment.

[18] Ten Easy and Effective Ways to Secure Your AWS Environment, Becky Weiss, AWS Invent, 2020. [Online]. Available: https://youtu.be/MCp2wB63UQI

[19] Anand Yadav, 7 Best Practices to Secure AWS S3 Storage, 2020. [Online]. Available: https://geekflare.com/aws-s3-security-tips/

[20] Identity Federation in AWS, Amazon Web Services, 2021.

[21] [Online]. Available: https://medium.com/@leticiamassae/integration-between-aws-security-hub-servicenow-f791a2f4cdbd

[22] [Online]. Available: https://www.infopulse.com/blog/aws-security-hub-soc-integrations

[23] [Online]. Available: https://www.servicenow.com/products/security-operations/what-is-siem.html

[24] Sharif MHU, and Datta R, Software as a Service has Strong Cloud Security, 2019. [Online]. Available: https://www.researchgate.net/profile/Haris_Sharif/publication/335232826_Software_as_a_Service_has_Strong_Cloud_Security/links/5d6466fc299bf1f70b0eb0f2/Software-as-a-Service-has-Strong-Cloud-Security.pdf

[25] Isaac Odun-Ayo, Chinonso Okereke, and Hope Orovwode, "Cloud Computing and Internet of Things: Issues and Developments," *Proceedings of the World Congress on Engineering*, vol. 1, 2018. [Google Scholar]

[26] [Online]. Available: https://docs.aws.amazon.com/securityhub/latest/userguide/standards-reference.html

[27] [Online]. Available: https://docs.aws.amazon.com/smc/latest/ag/sn-config-security-hub.html