International Journal of Core Engineering & Management
Volume-7, Issue-09, 2024 ISSN No: 2348-9510

INTEGRATED AWS SECURITY SERVICES FRAMEWORK FOR ENHANCED PROTECTION OF CLOUD-HOSTED WEB APPLICATIONS

Vivek Somi,
Technical Account Manager
Amazon Web Services

Abstract

As cloud computing is gaining popularity, organizations choose providers like Amazon Web Services (AWS) to support website and application platforms and store important information. Nevertheless, many security issues come from the insecure configuration and inconsistent deployment of security measures, leading to breaches and non-compliance. This paper outlines an AWS Security Integration Framework that would assimilate vital components of AWS security services into a coherent security structure of cloud-hosted web applications. The framework focuses on five core components: User management, network security, data protection, threat identification and mitigation, and compliance and reporting. These AWS services include Identity and Access Management (IAM), Web Application Firewall (WAF), Key Management Service (KMS), and GuardDuty, which provide secure threat detection and centralized security. The above implementation in a sample cloud environment established that the framework successfully minimizes security vulnerabilities, improves service functionality, and meets statutory requirements. This integrated security method proved efficient in eliminating delays and blunders in security operations. The suggested framework provides the concept needed for cloud security professionals to systematically implement security services from the Amazon Web Services portfolio. For future work, we plan to include other AWS services, for instance, beyond what we used in our research, to enhance the threat detection mechanisms within the framework of the proposed framework, which also needs to be extended to include a multi-cloud environment as it becomes a new frontier of cloud security.

Keywords: framework, Amazon Web Services (AWS), web application, services, threat, risk.

I. INTRODUCTION

Software as a service, further known as cloud computing, has dramatically changed the way organizations implement their IT systems by providing tangible advantages, including infinite expandability, versatility, and affordability. With cloud adoption on the rise, companies shift more workloads from their premises to the cloud and use the cloud to host web applications, store highly confidential data, and perform crucial operations [1]. However, this has brought about increased adoption of cloud computing and has provided a loophole to security threats. This model of security is ideal for organizations since they have to be responsible for the protection of resources in the cloud while the service providers handle the environment in which the resources reside [2]. Such distribution of responsibilities means that misconfigurations are made, openings for attacks, and intrusions are created if well handled.

This is one of the most effective areas that need to be protected in a cloud system. Web applications, most of the time, are the interface between the cloud infrastructures and the public; therefore, they are prone to risks like data leakage, cross-site scripting, and denial-of-service attacks [3]. A high number of organizations, 45%, have been found to have suffered a cloud-based data breach or have failed an audit on cloud-hosted data and applications, up by 10% from the previous year, a 2022 report suggests [4]. Moreover, the increasing popularity of multi-cloud deployments, where 72% of organizations work with multiple IaaS providers, put added pressure on the security of clouds [5, 6]. The fact that security is now across various platforms means that there is complexity in ensuring that policies remain constant, compliance, and threat detection. Due to the importance of the resources put into the web applications, application and cloud security for web applications that are cloud hosted must be well implemented. It can be seen from data collected in 2022 that customer data privacy and protection are still the focal areas of organizations, with 43% focus and third-party risks with 58% concern [7]. These are some of the reasons why organizations ought to adopt a well-architected model of security that incorporates different security tools and services.

AWS, being one of the leading CSPs in the world, presents an effectively broad security service that aims to facilitate the protection of organizations' cloud platforms [8]. They encapsulate a wide variety of security processes, which might involve identification, encryption, threat detection, and compliance. AWS has more robust compliance programs and SOC reports that cater to 154 services that the business offers through SOC systems and organizational controls [9]. Of course, like any cloud computing platform, AWS comes equipped with a variety of security tools; nevertheless, companies' most significant challenges lie not in a lack of tools but in issues tied to their implementation. In an effort to address these threats, design broad security objectives, as well as remain in compliance with the rules and regulations of the AWS security services, this paper advanced a framework for the comprehensive integration of AWS security services into the security architecture of web applications.

II. RELATED WORK

Different cloud security frameworks have developed alongside the rise of cloud computing to address the particular concerns crafted by cloud environments. Cloud Security Alliance (CSA) Cloud Control Matrix and other standalone frameworks exist, and they offer a collated and detailed set of security controls designed for cloud environments [10]. However, these controls cover, at a high level, key areas such as data protection, identity management and incident response. Like Microsoft Azure, other cloud platforms also have their security benchmarks, which help organizations secure cloud deployments [11].

Although there are frameworks available for this, the problem of cloud security implementation hinders most organizations. Cloud security incidents were caused by misconfigurations more often than any other resource exposed or access misuse involving credentials or non-credentials [12]. This emphasizes the need for appropriate configuration and tools that continuously monitor cloud environments for vulnerabilities and misconfigurations.

International Journal of Core Engineering & Management
Volume-7, Issue-09, 2024 ISSN No: 2348-9510

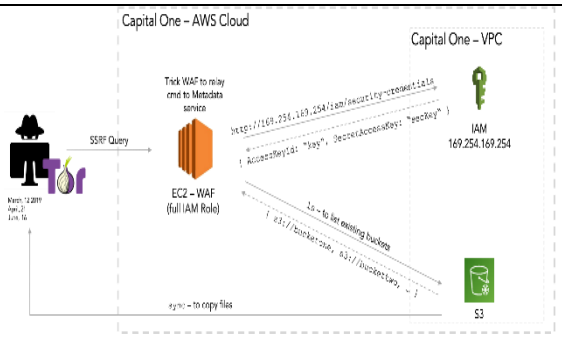

Figure 1: Over-Permissioned Cloud Resources
Source: Adapted from [12]

The services in these areas include AWS Identity and Access Management (IAM), AWS Key Management Service (KMS), AWS Web Application Firewall (WAF), AWS GuardDuty, and more [13]. Each service adds critical security capabilities, yet too many organizations need to integrate them into a complete, unified security strategy where they can fully leverage the capability.

However, while the literature devoted to security specifics for various AWS services (e.g., IAM for permissions, GuardDuty for threat detection) does exist, more work must be presented on a holistic perspective of AWS security [14]. However, few of these studies have addressed the issue of integrating these services into a unified security framework. Since cloud security is not just the sum of securing individual components, the need to treat this gap in the literature is considerable. Rather than relying on disjointed security services, AWS security services can be integrated into a single framework that will allow organizations to manage security risks more effectively, perform better operations, and even comply with regulatory standards.

III. PROPOSED AWS SECURITY INTEGRATION FRAMEWORK

In light of the foregoing security risks that are inherent with the cloud-hosted web application, this paper seeks to present an AWS Security Integration Framework that will afford end-to-end security. The framework focuses on five core components: identity and access management, network security, data protection, threat detection and response, and compliance and auditing [15]. All of them utilize several fundamental AWS security services to address a certain level of security issues, and the interfaced application of these services means the unified use of security measures in the cloud space.

The core of this framework is AWS Identity and Access Management (IAM) that allows prescriptive control of access for certain resources of the cloud. When applied at the foundation of an organization, Principle of Least Privilege entails granting users and systems as few permissions as possible so they can only accomplish the activities required of them and nothing else [16]. Moreover, IAM offers MFA and is compatible with AWS SSO, which adds even more protection in order to control access to AWS services.

International Journal of Core Engineering & Management
Volume-7, Issue-09, 2024 ISSN No: 2348-9510

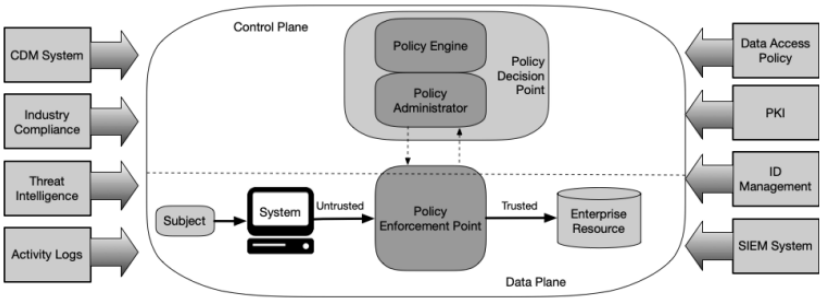

Figure 2: Core Zero Trust Logical Components
Source: Adapted from [16]

To be specific for the network security, the AWS Web Application Firewall (WAF) serves a major purpose of safeguarding the web applications from the threats like SQL injection attacks and cross-site scripting. The market size for Web Application Firewall market is USD 4.7 billion in the year 2022 and it will reach a growth rate of (CAGR) 14.2% in the year 2023-30 [17]. AWS WAF provides an opportunity for organizations to develop their own rules that help to filter and track HTTP and HTTPS requests and preventing them from the access of the application. More so, AWS Shield offers mitigation against DDoS attacks making web applications available during large attack times.

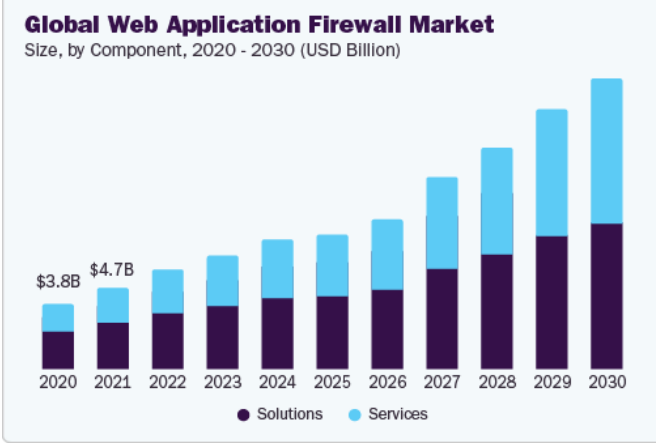

Figure 3: Global web application firewall market
Source: Adapted from [17]

Another important aspect of the proposed framework is data protection which is valuable in view of the growing concern of data privacy and security. According to the recent survey conducted, the biggest concern of cloud security among 69% of the organizations was data loss and leakage [18]. AWS KMS supplies organisations with advance encryption solutions, making it possible to make vital data secured while in storage, as well as in transit. Being a service of AWS, it links with others like S3 and RDS to make data capture, storage and processing fully encrypted [19]. This becomes significant for the organizations that experience reporting mechanism regulations like GDPR or HIPAA in their operations.

International Journal of Core Engineering & Management
Volume-7, Issue-09, 2024 ISSN No: 2348-9510

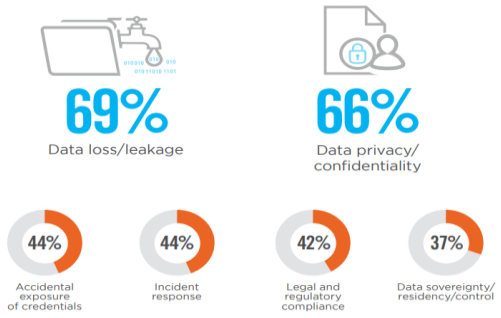

Figure 4: Misconfigurations that lead to Breaches
Source: Adapted from [18]

AWS GuardDuty and Amazon Inspector are the services necessary to identify and protect against threats in the cloud environment's security. Within the AWS ecosystem, GuardDuty leverages machine learning and threat intelligence for threat identification including instance threats, such as unauthorized access or malicious traffic, whereas Amazon Inspector identifies AWS resource libraries [20]. In total these services allow for comprehensive real-time view to occurrence of any threatening conditions in the cloud environment so that the organizations can effectively combat the risks.

AWS CloudTrail and AWS Security Hub are used for compliance and auditing. The CloudTrail captures all activities done within the AWS environment and therefore can be used for security analysis, to monitor for security threats or even to investigate compliance issues. AWS Security Hub – it is the tool providing the centralized view of the security across the AWS environment and bringing the security findings from different services into a single location for management of the security and compliance teams' security-alerting and investigation processes [21].

IV. IMPLEMENTATION OF KEY AWS SECURITY SERVICES

According to the AWS Security Integration Framework, proposed in this paper, every security service is to be configured and incorporated into the general cloud architecture. For instance, AWS GuardDuty is automatically enabled and continually assesses AWS resources for suspicious activities by leveraging ML and information from AWS partners [22]. The use of automated security services, like GuardDuty was highlighted as a trend in AWS security. Meaning, that when threat detection and response are automated, then the time taken in the management of the security threats is minimized.

Likewise, AWS Web Application Firewall (WAF) is configured to shield web application against application layer threats. The current WAF market is still developing, meaning that during the next decade, this type of security will experience high demand due to the growing amounts and complexity of Web-based threats [23]. In AWS WAF, organizations can set up rules they want to use to block traffic that might otherwise disrupt a website, such as SQL injection attacks or cross-site scripting.

Another main service of the framework is Amazon Inspector, which is employed to evaluate the

International Journal of Core Engineering & Management
Volume-7, Issue-09, 2024 ISSN No: 2348-9510

security of AWS assets by means of identifying security weaknesses and non-compliance with guidelines. With the help of Inspector, one can solve misconfigurations that were accounted for 65% of cloud security incidents in 2022 [24]. With Inspector added into the security structure, organizations can have their cloud settings scrutinized for any vulnerabilities with steady tracking.

Sensitive data encryption is supplied by AWS Key Management Service (KMS). Given the significant focus on data security, especially in sectors subject to regulatory constraints, KMS is especially important in guaranteeing that data is encrypted both at rest and in transit. Monitoring security policy compliance then comes via AWS CloudTrail and AWS Security Hub [25]. By tracking every API activity inside the AWS environment, CloudTrail creates a comprehensive audit trail available to confirm industry standards compliance. By aggregating security results from GuardDuty, Inspector, and other AWS services into a centralised dashboard, AWS Security Hub helps companies more precisely control security warnings and compliance needs.

V. FRAMEWORK EVALUATION

A simulated cloud environment was built to assess the performance of the suggested AWS Security Integration Framework, consequently simulating the usual infrastructure of a web application hosted on AWS. Each of the security events including data threats and misconfiguration was presented to examine the effectiveness of the framework concerning threat identification and response. The main areas for the evaluation were time-to-detection and time-to-response, the number of successful and thwarted exploits, and compliance with external standards.

The findings of the evaluation showed that the integrated security framework enhanced the organization systems in kind and ended the threats in real-time accordingly. For instance, AWS GuardDuty, out of which one cannot view samples separated from AWS Web Hosting Service, plotted out unlawful entry notions in minutes [26]. In the same manner, simulated SQL injections were also prevented by AWS WAF from getting to the web application since it was able to block that kind of attack. Automated threat detection and reaction in the context of GuardDuty and WAF considerably helped to decrease the time needed to identify security threats and respond to them [27].

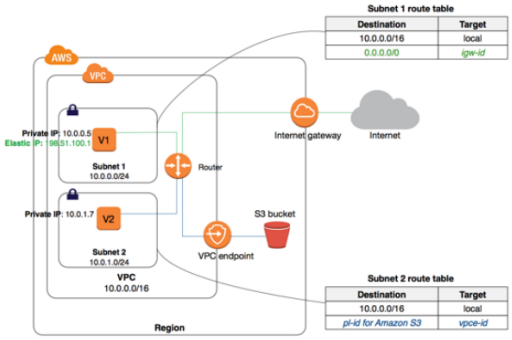

Figure 5: AWS Logical Topology
Source: Adapted from [27]

They also found out that the framework enhanced the process of performing operations through

the transformation of various security processes into automated operations. For instance, AWS Security Hub offered consolidated vantage points of all the security issues and the process assisted the security team in managing the incidents. This kind of integration helped in eliminating the challenges that come with using several security products and services to fortify the organization's security needs.

Regarding compliance, the framework maintained a perpetual state of policy compliance with the help of AWS CloudTrail and AWS Security Hub. CloudTrail allowed tracking of all activities in the AWS environment, whereas Security Hub integrated all security results into one. This made it easier to check whether the organization in question is conforming to regulatory measures and cut down the time to be taken through security assessments.

VI. RESULTS AND DISCUSSION

The outcome of the evaluation, therefore, show that the AWS Security Integration Framework is viable in reducing security threats and enhancing organizational performance. Implementing AWS security services operating under a common architecture offered protection of cloud-based hosted web applications, limiting the potential for an attack and limiting problems posed by security breaches. Of all the features of the framework, one of the biggest advantages is the automated identification of threats and their subsequent handling. AWS GuardDuty and WAF for example employ machine learning alongside predefined rules of analysis and response towards threat activity thus taking considerably less time to respond towards threats compared to a traditional process [28]. This is particularly important in cloud environments because attacks occur at incredible speed and on a large scale, it is possible to overcome traditional security measures.

The framework also increases operational effectiveness by consolidating security control at a centralized level. AWS Security Hub is the aggregator that gathers details on security investigation across different services provided by AWS; handling of incidents and compliance by the security team is done on the hub [29]. This eliminates the challenge of having to deal with different security tools and guarantees that the notices given by a security tool are responded to quickly. Configuring AWS security services right from the start can prove quite challenging first and foremost due to the lack of experience with cloud services. Furthermore, security tools in AWS offer comprehensive capabilities, however, organizations must not neglect their parts of responsibilities according to shared responsibility model. In a separate analysis, misconfigurations that are currently blamed for many cloud security breaches can still take place if the AWS environment is not set up correctly.

VII. CONCLUSIONS & FUTURE RESEARCH

The AWS Security Integration Framework as described in this study can be considered as one of the most appropriate to integrate security measures to protect the web applications which are hosted in the cloud. To ensure its security relevance, the framework incorporates five main AWS security services: IAM, WAF, KMS, GuardDuty, and Security Hub; based on which key security aspects like identity, data, threat, and compliance can be managed. By evaluating the implemented framework, it was evident that the plan successfully addressed threats that may hinder the

achievement of organisational goals and objectives as well as complicate project delivery considering current organisational structures, processes, and systems' compliance with legal requirements.

For cloud security practitioners, this provides a roadmap on how AWS security services can be deployed in an integrated and holistic approach. Due to the modularity of the approach, the framework can be incorporated within an organization step by step starting from IAM up to including more sophisticated services, including GuardDuty at this moment as well as Security Hub. All these characteristics make the framework ideal for the organization no matter the size and sector. Areas like further integration of the use of other AWS services which include services such as deep learning-based threat detection service have also been proposed for subsequent studies followed by the testing of the framework for setting up multi-cloud environments. Since cloud infrastructures are still developing, the demand for advanced and interconnected solutions to ensure security will increase, which is why this topic is important for the development of the cloud security field.

REFERENCES

1. S. Zhang et al., "Practical Adoption of Cloud Computing in Power Systems -Drivers, Challenges, Guidance, and Real-world Use Cases," IEEE Transactions on Smart Grid, vol. 13, no. 3, pp. 1–1, 2022, doi: https://doi.org/10.1109/tsg.2022.3148978.
2. S. Bankar, "Cloud Computing Using Amazon Web Services AWS," International Journal of Trend in Scientific Research and Development, vol. Volume-2, no. Issue-4, pp. 2156–2157, Jun. 2018, doi: https://doi.org/10.31142/ijtsrd14583.
3. M. M. Belal and D. M. Sundaram, "Comprehensive Review on Intelligent Security Defences in cloud: Taxonomy, Security issues, ML/DL techniques, Challenges and Future Trends," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 10, Nov. 2022, doi: https://doi.org/10.1016/j.jksuci.2022.08.035.
4. S. Zurier, "Nearly half of businesses had a cloud-based data breach or failed audit," SC Media, 2022. https://www.scworld.com/news/nearly-half-of-businesses-had-a-cloud-based-data-breach-or-failed-audit.
5. F. Hakamine, "What Are the Benefits and Limitations of Multi-Cloud?," www.okta.com, May 07, 2021. https://www.okta.com/blog/2021/05/what-are-the-benefits-and-limitations-of-multi-cloud/
6. Moe Yaziji, "Nearly 50% Of Businesses Had a Cloud-Based Data Breach or Failed Audit," SecureOps, Jun. 14, 2022. https://secureops.com/blog/cloud-security-451/.
7. V. Anant, L. Donchak, J. Kaplan, and H. Soller, "Consumer data protection and privacy," www.mckinsey.com, Apr. 27, 2020. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative
8. S. Park, Y. Lee, and W. Park, "Configuration Method of AWS Security Architecture That Is Applicable to the Cloud Lifecycle for Sustainable Social Network," Computer Networks and Communications, vol. 2022, Article ID 3686423, Dec. 2022. https://onlinelibrary.wiley.com/doi/10.1155/2022/3686423.
9. P. Sharma and R. Saxena, "Security Best Practices in AWS," IJFANS Int. J. Food Nutr. Sci., vol. 11, no. 02, pp. 1191, 2022.

https://ijfans.org/uploads/paper/48bfb9d4f9908a622aec57eaaaca18cb.pdf.
10. A. Pichan, "Digital Forensics Investigation Frameworks for Cloud Computing and Internet of Things," 2022. Accessed: Oct. 24, 2023. [Online]. Available: https://core.ac.uk/download/534131431.pdf
11. P. Wankhede, M. Talati, and R. Chinchamalatpure, "COMPARATIVE STUDY OF CLOUD PLATFORMS -MICROSOFT AZURE, GOOGLE CLOUD PLATFORM AND AMAZON EC2," Journal of Research in Engineering and Applied Sciences, vol. 05, no. 02, pp. 60–64, Apr. 2020, doi: https://www.researchgate.net/publication/342157054_COMPARATIVE_STUDY_OF_CLOUD_PLATFORMS_-MICROSOFT_AZURE_GOOGLE_CLOUD_PLATFORM_AND_AMAZON_EC2.
12. C. GmbH, "Five Common Cloud Security Threats and Data Breaches," codeshield.io, Jul. 15, 2021. https://codeshield.io/blog/2021/07/15/five_common_threats/
13. J. B. Almeida et al., "A Machine-Checked Proof of Security for AWS Key Management Service," Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, Nov. 2019, doi: https://doi.org/10.1145/3319535.3354228.
14. S.-J. Park, Y.-J. Lee, and W.-H. Park, "Configuration Method of AWS Security Architecture That Is Applicable to the Cloud Lifecycle for Sustainable Social Network," Security and Communication Networks, vol. 2022, pp. 1–12, Jan. 2022, doi: https://doi.org/10.1155/2022/3686423.
15. NIST, "The CSF 1.1 Five Functions," NIST, Apr. 2018, Available: https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions
16. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," Zero Trust Architecture, vol. 800–207, no. 800–207, Aug. 2020, doi: https://doi.org/10.6028/nist.sp.800-207.
17. GVR, "Web Application Firewall Market Size & Share Report, 2030," www.grandviewresearch.com, 2023. https://www.grandviewresearch.com/industry-analysis/web-application-firewall-market-report.
18. T. Bradley, "Why Misconfiguration Lead to Breaches - Cloud Security - Risk and Compliance," NSC42, Oct. 08, 2020. https://www.nsc42.co.uk/post/cloud-misconfiguration-leads-to-breaches
19. Amazon Web Services, "AWS Key Management Service: AWS KMS Cryptographic Details," Amazon Web Services, Inc., 2021. [Online]. Available: https://docs.aws.amazon.com/pdfs/kms/latest/cryptographic-details/kms-crypto-details.pdf.
20. S. Sarkar, "Security of Amazon Web Services," Mar. 3, 2017.
21. D. Soni, "CIS AWS Foundations Benchmark with AWS Security Hub," Medium, Apr. 16, 2021. https://sonidhaval.medium.com/cis-aws-foundations-benchmark-with-aws-security-hub-76cc7c2abe92.
22. C. Peiris, A. Kudrati, and B. Pillai, Threat hunting in the cloud : defending AWS, Azure and other cloud platforms against cyberattacks. Hoboken, New Jersey: John Wiley & Sons, Inc., 2021.
23. B. Zhang, J. Li, J. Ren, and G. Huang, "Efficiency and Effectiveness of Web Application Vulnerability Detection Approaches: A Review," ACM Computing Surveys, vol. 54, no. 9, pp. 1–35, Oct. 2021, doi: https://doi.org/10.1145/3474553.

24. B. Cozens, "Cloud Data Breaches: 4 Cloud Storage Security Threats - ThreatDown by Malwarebytes," ThreatDown by Malwarebytes, Jun. 08, 2022. https://www.threatdown.com/blog/cloud-data-breaches-4-biggest-threats-to-cloud-storage-security/.
25. A. Rajan, "AWS Security Best Practices — AWS Security Hub — #CloudSecurity," Medium, Mar.10, 2019. https://ashishrajan.medium.com/aws-security-best-practices-aws-security-hub-cloudsecurity-99a57096974f.
26. AWS, "User Guide Amazon Fraud Detector," Jun. 2023. Accessed: Nov. 24, 2023. [Online]. Available: https://docs.aws.amazon.com/pdfs/frauddetector/latest/ug/frauddetector.pdf
27. I. Routavaara, "Security monitoring in AWS public cloud," 2020. Available: https://www.theseus.fi/bitstream/handle/10024/341640/Opinnaytetyo_Routavaara_Ilkka.pdf?sequence=2
28. D. Shields, AWS Security. Simon and Schuster, 2022.
29. AWS, "AWS service integrations with Security Hub - AWS Security Hub," Amazon.com, Apr. 19, 2022. https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-internal-providers.html.