Comparative Analysis of Splunk vs. AWS Native Monitoring Tools for Cloud Security and Threat Detection

MSc Research Project
Cloud Computing

Umadevi Mala
Student ID: x23187344

School of Computing
National College of Ireland

Supervisor: Shaguna Gupta

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Umadevi Mala
Student ID:	x23187344
Programme:	Cloud Computing
Year:	2024
Module:	MSc Research Project
Supervisor:	Shaguna Gupta
Submission Due Date:	18/12/2024
Project Title:	Comparative Analysis of Splunk vs. AWS Native Monitoring Tools for Cloud Security and Threat Detection
Word Count:	4250
Page Count:	26

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Umadevi Mala
Date:	28th January 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Comparative Analysis of Splunk vs. AWS Native Monitoring Tools for Cloud Security and Threat Detection

Umadevi Mala
x23187344

Abstract

Cloud security monitoring remains critical and challenging for organizations as cyber threats have continued to evolve. While previous research by the authorAnanthapadmanabhan and Achuthan (2022) explored threat detection using Splunk in cloud environments, there has been limited comparative analysis between the third-party security information and the event management (SIEM) solutions and native cloud monitoring tools. This research will address this gap by thoroughly comparing Splunk and AWS native monitoring tools, focusing on their effectiveness in threat detection and analysis. The experimental evaluation assessed both platforms across three key security scenarios: unauthorized login attempts, data exfiltration, and malware detection. The results demonstrate that while AWS native tools generally provided faster detection times, Splunk consistently achieved higher precision and recall rates. And For unauthorized login attempts, Splunk achieved 97% precision and 98% recall compared to AWS's 94% precision and 95% recall, although AWS detected events marginally faster (6 seconds vs. 8 seconds). Similarly, in data exfiltration scenarios, Splunk showed superior accuracy with 95% precision and recall, outperforming AWS's 89% precision and 90% recall, despite AWS's quicker detection time (10 seconds vs. 13 seconds). We will see how these findings will provide valuable insights for organizations' decisions about cloud security monitoring strategies. It also suggests how AWS native tools offer speed advantages, whereas Splunk delivers more comprehensive and accurate threat detection capabilities, helping organizations optimize their cloud security posture against emerging threats.

1 Introduction

Today, cloud computing has been a cornerstone of every organization and the global market of public cloud services is predicted to grow to $623. 3 billion by 2023. Saying this, we can underscore that the introduction of cloud technology has been filled with a host of opportunities that are regarded as forcible in the context of scalability, flexibility, and cost efficiency. However, through remaindering, it has also opened a new threat area for security and expanded the attack vectors for cyber threats. Cloud computing is rising tremendously in popularity; so is the number and the severity of cyber threats towards them. According to Chandran et al. (2015), the IT security measures that were used earlier in cloud computing security are not adequate to address new threats affecting clouds. This raises the

need for more optimal and cloud-adequate security monitoring as well as threat detection technologies and concepts. Thus, threat modelling and threat intelligence are two of the most crucial factors that should be incorporated into cloud security. In a paper by Tatam et al. (2021), the authors introduced the different approaches to threat modelling and particularly touted the application of threat modelling as useful for discovering common threats in cloud contexts. However, it is to be noted that the kind of threat models used conventionally often have a limited scope of predefined attack vectors and do not fully encapsulate the real-time cloud threats, as coined in Ananthapadmanabhan and Achuthan (2022) in their paper "Threat Modeling and Threat Intelligence System for Cloud using Splunk. "
To overcome this limitation, it was suggested in Ananthapadmanabhan and Achuthan (2022) the use of a combined system based on Splunk for threat modelling and real-time threat intelligence in a cloud environment. This approach used the MITRE ATT&CK framework to classify threats on the basis of attack actions and behaviours and Splunk's ability to carry out real-time log analysis to identify live threats and abnormal behaviours in cloud systems. Although combining them has great benefits, this raises the question of whether third-party tools such as Splunk for information security SIEM are better than cloud monitoring tools from cloud service providers such as Amazon Web Services (AWS). There are several basic yet effective tools you can use for monitoring and logging in AWS, such as Amazon CloudWatch and AWS CloudTrail services, as well as AWS security services. These native tools are tightly embedded into the AWS environment, and they offer out-of-the-box advanced monitoring.

Therefore, this research will utilize the foundation laid by Ananthapadmanabhan and Achuthan (2022) by carrying out a comparison of Splunk and AWS native monitoring tools for threat detection in cloud computing environments. Consequently, reaffirming the motivations for the current research, this paper compares and contrasts the effectiveness and practical usability of the two approaches to CS monitoring to offer dependable guidance for organizations concerned with the improvement of their Cloud computing security systems.

1.1 Problem Statement

Cloud computing's fast market transition has increased cyber hazards, exposing organizations to major security threats. Cloud environments introduce problems that traditional IT security methods fail to handle effectively. This research reveals an important void regarding the evaluation of cloud security monitoring tools by contrasting Splunk with native AWS monitoring tools, as these solutions power effective threat detection and response capabilities.

1.2 Objective

This research performs a detailed evaluation of Splunk and AWS native monitoring solutions with respect to cloud security and threat identification methods. The study evaluates log collection efficiency along with threat analysis capabilities, whereas real-time detection mechanisms alongside threat intelligence framework implementation (MITRE ATT&CK) combined with usability aspects along with scaling capabilities and total cost evaluation. The research presents business-ready information that helps organizations improve their cloud monitoring tactical approaches.

1.2.1 Research Question

How do Splunk's cloud monitoring and threat detection capabilities compare to AWS native monitoring tools in terms of effectiveness, usability, and integration with advanced threat intelligence frameworks?

In order to answer this research question, the following setup of the test environment will be arranged: two AWS servers will be used, one running the test application and the second remaining idle. Server and application logs are to be gathered with the help of Splunk and AWS native monitoring tools. The research will evaluate various aspects of both monitoring solutions, including The research will evaluate various aspects of both monitoring solutions, including:

- To achieve the best results, the solution should have a powerful logger with data analysis capabilities
- Application of real-time threat identification and notification.
- The inclusion into threat intelligence frameworks, like MITRE ATT&CK
- , States that one of the main impacts of VoIP would be ease of use, usability, and easy configuration of the communication system.
- Complexity and Compliance overhead
- Cost considerations

1.3 Significance and scope of the Study

The investigation holds substantial value because it provides solutions to address escalating cyber threats alongside rising requirements for advanced cloud security monitoring systems. The study's comparison between Splunk and native AWS security tools boosts our understanding regarding organizational strategies to maximize their cloud security postures. The research outcomes will help decision makers identify security-aligned monitoring tools which enhance their threat detection capabilities and response mechanisms.

The study conducts a comparison study between Splunk and AWS native monitoring tools as they operate within cloud computing frameworks. The research will require the creation of two AWS servers: one hosting a test application and one remaining empty for log collection at both servers. This assessment of third-party monitoring tools includes an evaluation of logging capabilities alongside real-time threat identification mechanisms along with integration with threat intelligence frameworks as well as usability and compliance prerequisites and system complexity factors and total cost. This research exclusively targets cloud computing environments and will not investigate third-party monitoring solutions or discuss non-Cloud infrastructure systems.

2 Related Work

2.1 Cloud Security Monitoring and Threat Detection

Due to the current high speed adoption of cloud computing, there is high risks to organizations' digital assets and data through insecurity therefore advanced security monitoring as well as threat detection are essentials. With a continuous growth and expansion of the cloud infrastructures and their distribution over the wide-area network, the prior security measures and architectures are often found to be inadequate in order to counter the emerging threats and security risks. Alhebaishi et al. (2017) provided a good survey on threat modeling of the cloud data center infrastructures and thereby identify the challenges associated with threat modeling in cloud computing being a distributed infrastructure. In their research, they pointed out the fact that their security model in cloud computing is the shared responsibility model and that has introduced more security issues that organizations have to deal with. For instance, in the case of cloud service providers, it is their duty to ensure the infrastructure's security to which the customer is connected to but the customer has the responsibility for the application and data security. Based on the division of labor that has been presented above, it means that security monitoring and threat identification require integration.

In their work, the authors that introduced a research methodology that could be used to ascertain possible threats in cloud data centers with an understanding of their multitenancy. They stated that the older methods of threat modeling might not be sufficient enough to capture the nuances of the cloud infrastructures because such infrastructures are multi-tenant and are capable of dynamically scaling their resources, and shifting their workload across physical regions at short intervals. This nature of cloud environments is dynamic thus the need for constant monitoring and real-time extrapolation of threats to correspond with the dynamic conditions in the cloud environment. Expanding the research from Alhebaishi et al. (2017), the author discussed and investigated more about the measures towards the prevention of cyber attacks and the effectiveness of the preventive measures in cloud computing environment. In their studies, they found that threat intelligence capabilities should be incorporated with the monitoring solutions to improve the indicators for identifying APTs. They stated that the conventional security methods of response to threats are ineffective in the case of APTs, which are fundamentally strategic, step-by-step attack systems.

Another reference architecture for cloud computing security was made by Farhat & Seceleanu, which divided cloud security into several layers, namely monitoring, threat intelligence and response. They pointed out that it is necessary to go beyond the analysis of raw logs and use more complex correlation mechanisms that can diagnose retreated patterns typical for complex attacks. This integration of threat intelligence with monitoring corresponds to the scheme proposed by Ananthapadmanabhan and Achuthan (2022)n in their system based on Splunk constructor, which uses the matrix MITRE ATT&CK to classify and analyze possible threats; The dissimilar approach to the described solutions, Alam (2020) explored the position of cloud computing in information technologies and discussed the problematic situation associated with the secur In another study by Alom et al. Alam (2020), the authors stressed the significance of developing new solutions for security concerning cloud platforms while pointing at the nature of multi-tenancy and resource sharing particular to such settings. The author proved valid the perspective on the fact that although conventional security tools and approaches are not completely ineffective in the context of cloud security, they need to be modified or even replaced.

Alam and his colleagues' research Alam (2020) concerned some of the principal limitations of traditional approaches to security operations, such as Security Information and Event Management (SIEM) systems, like Splunk, for monitoring cloud environments and raised concerns about the efficiency of native cloud security solutions contrary to the cloud-designed tools for security monitoring. The author advised that cloud-native applications could be more favorable if it comes down to integration, scalability, and real-time contention. Nonetheless, Alam (2020) also noted that the third-party SIEM tools are more relevant in terms of analytics and cross-platform compatibility that are significant, especially in case of hybrid and multi-cloud environment.

2.2 Threat Modeling and Intelligence Frameworks

Threat modeling and intelligence frameworks are considered to be the counterparts of traditional approaches to attack vectors' identification, classification, and elimination and can be used to improve cloud security significantly. Both of these frameworks provide organizations with the shared language and approach for evaluating and mitigating security risks in a cloud space. From the previous research that has been fronted by Georgiadou et al. (2021) in the year 2021 specifically in the article MITRE ATT&CK framework, they have established how the use of frameworks such as the MITRE ATT&CK can incur much benefits in the categorization of risks in cloud environments. The authors stated that due to the highly detailed classification of the tactics and techniques used by adversaries, MITRE ATT&CK is a valuable framework for threat modelling and risk analysis for organizations.

They also acknowledged that the theoretical framework assist in assessing the correlation between real-world attacks and specific countermeasures, thus helping organizations to focus on the right areas in their security plan. They also pointed out the usefulness of the framework in the fact that it is constantly adapted and developed along with the help of the community to meet the current threats. This perfectly reflects the highly fluid nature of cloud environments in which new threats and ways of attacks may appear soon. The study by Pandi et al. (2020) on the other hand amassed capabilities, threats, and forensic on distributed cloud environments by outlining the STRIDE methodology. The authors' work helped to give a brief about various threat modeling methodologies and how they could be used in cloud environments. The STRIDE methodology involving the threats that may be met which are Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege are efficient in providing a structure upon which the potential threats may be developed.

Thus, the authors of the work Pandi et al. (2020) who results are described in this section stated that the STRIDE methodology is easy to apply, and covers all potential threats that can occur in cloud environments and due to the variety of services and their deployment models that are used in cloud systems, the threat analysis can be challenging. But as trivia that Ananthapadmanabhan and Achuthan have rightly identified, cloud threats are not easily definable and, therefore, cannot be easily modeled using traditional models like STRIDE. Adding to the various steps of the STRIDE methodology, Urias et al. (2018) presented a candidate cloud threat model with a comprehensive description of threats and measures for their prevention. Their stance was effective as it offered a method of dealing with cloud-specific threats by extending the STRIDE categories to the peculiarities of cloud environments. For instance, they elaborated on what they called "Information disclosure" to cover concerns such as data localization and multi-tenancy that are peculiar to the cloud strategy.

Although in Urias et al. (2018), the author described the variety of threats related to clouds and provided a general framework for analyzing them, the main idea of the paper was more about the predefined attack ontology rather than the real-time threat detection and response. This is an area that implies that dynamic and static threat modeling should be used hand in hand to realize the cloud security fully. , however, based on the ontological approach, Andrei (2021) proposed threat modelling for cloud systems and offered an Academic Cloud Computing Threat Pattern (ACCTP) catalog. This work also highlighted the need to take into account different kinds of security sources and different security standards when coming up with a threat model for the security threats. In the same manner, Andrei et al. Andrei (2021) emphasized that ontological threat modeling is more malleable and agile to make room for new menacing elements in an organization's IT systems.

To overcome these shortcomings, the ACCTP catalog suggested by Andrei (2021) intended to combine the findings of different types of source knowledge: standard, literature, and case study. This provides the possibility to cover a greater number of threats but can also increase the level of difficulty in the implementation and further support of the approach.

2.3 SIEM Tools and Cloud Monitoring

There is a wealth of literature addressing the application of Security Information and Event Management (SIEM) tools such as Splunk in the context of cloud security since many organizations try to extend usage of such potent analytics instruments to improve their cloud security. With specific objective to demonstrate Splunk, Carasso (2012) have given a good account on how to use Splunk as tool in cloud monitoring and Security Analytics.

The narrative of this piece brought out aspects such as log aggregation, analysis and visualization that Splunk is proficient in; which are very vital in examination of cloud security. Carasso (2012) also highlighted the scalability of Splunk and the capacity to correlate data coming from various sources which makes it suitable for organisations with complex cloud structure where data can be spread over various systems and services of which some may contain data relevant for security analysis. The author explained how Splunk has enhanced the searching and analytical features to ensure that the security teams are in a position to identify patterns and abnormality that signifies threats. Carasso (2012)) also acknowledged on how Splunk can be extended through applications and extensions, which are useful in improving Splunk's cloud monitoring features based on the underlying cloud services API provided by various cloud providers.

Unlike third-party SIEM, Buddha and Beesetty (2019) discussed about the monitoring and integration service of AWS used by them in their paper on AWS application integration guide. Their work is really enlightened me about the other features of monitoring from AWS such as CloudWatch, CloudTrail, and others security services. Reading this material that provides the detailed breakdown of AWS' native monitoring features, one wonders if the third-party SIEM tools are even needed in AWS environments and what advantages the native solutions might offer. According to Source def, the tight coupling of AWS monitoring tools with other AWS services was noted in that it is very easy to collect and process data on an AWS infrastructure. They also stressed that native tools are cheaper than third-party tools since they are frequently available through the AWS subscription. Still, the authors pointed out that harnessing AWS's built-in monitoring tools might be somewhat less flexible regarding analytical depth and integration compatibility compared to Splunk SIEM, for instance.

Further extending the scenario, Larrea et al. (2015) explored the use of continuous integration tools for observing the application performance which is related to the cloud security monitoring. One of the key findings of their studies was that monitoring systems should be devised alongside the DevOps culture and CI/CD processes, a field in which native cloud tools can apparently benefit from closer cloud integration. According to Larrea et al. Larrea et al. (2015), the current security practice of evaluating cloud security in a periodical manner should be done away with, thus be replaced with a perpetuated examination facilitated by automation. They suggested that by embedding the security monitoring into the CI/CD process, organizations can find out the possible security holes and threats are previously detected at the development stage. This is particularly advantageous as most cloud environments tend to be dynamic and include a lot of changes as well as deployments.

The authors pointed out that popular third-party SIEM tools like Splunk do have robust analytics features but the native cloud monitoring tools may have better integration with cloud development/DevOps paradigms. At the same time, they also pointed that the best approach seems to be the use of native features and third-party extensions to cover all the aspects of security.

2.4 Comparative Studies and Evaluation Frameworks

Despite the fact that there are a great number of works that are devoted to the analysis of individual monitoring tools or threat modeling methods, the comparative analysis of third-party SIEM solutions like Splunk and native cloud monitoring services is still insufficient. The lack of a direct comparison study is a research void that can generate knowledge that will be beneficial to organizations about the best way of improving their CSMS. Survey done by Tounsi and Rais (2018) titled Technical threat intelligence in the era of complex cyber threats may be relevant as it offers criteria to assess the efficacy of threat intelligence and monitoring solutions. Their work centered into the need to have accurate and timely threat intelligence as a means of dealing with contemporary cyber threats. The authors described a number of suggest the criteria for the comparison of threat intelligence platforms concerning the data quality, integration, and analytical depth.

The authors in Tounsi and Rais (2018) proposed a systematic framework for evaluating threat intelligence solutions; however, the work of the authors do not highlight a clear distinction of cloud native monitoring versus third-party monitoring toolkits. This limitation exposed the need for work that uses such approaches to assess the comparative efficacy of solutions such as Splunk to native cloud monitoring tools with regard to the security of cloud environments. An understanding of signed and implicitly trusted malicious code threats to compile a threat analysis framework, which is helpful in gaining knowledge on the effectiveness of monitoring solution in identifying advanced threats. Their strategy was based on the investigation of signs that might not be detected by other modern security systems. The authors described a four-step method of analyzing a program's source code, which included applying data and control flow analysis, as well as behavior observation to identify suspicious actions.

Although Larrea et al. (2015) framework was not proposed with cloud context of use in mind, their could be rather easily customized to the purpose of comparing Splunk with other AWS native monitoring tools in the scope of threat detection in cloud environment. Thus, the focus on behavioral analysis and the possibility of correlating many factors correspond to the nature of cloud security monitoring, during which threats can affect multiple services and resources. The study of Larrea et al. (2015) shows that modern solutions for security monitoring and analysis require aspects of advanced analytics and machine learning. This leads one to wonder whether other third-party SIEM tools like Splunk, which may be head and shoulders above native cloud monitoring for analytics, are better or whether the native cloud products will offer lower tail latency necessary for real time analysis.

2.5 AWS Native Monitoring Tools: CloudWatch and CloudTrail

Looking at the cloud security monitoring, AWS provides powerful native security tools that play a significant role in protecting cloud infrastructures. AWS's monitoring environment includes CloudWatch and CloudTrail: they are essential, as both allows tracking of cloud resource usage, performance of the applications, and activity log. According to Nikolai et al. (2014), AWS CloudWatch is a service of AWS that performs the monitoring of AWS resources and of applications running on AWS infrastructure in real time. The authors discuss about the usage of CloudWatch for getting the metrics of various services, owning logs and inserting alarms. This multi-dimensional approach enables organisations the visibility of the system and helps in detecting issues as well as addressing the changes in their operation in cloud environment.

While CloudWatch covers the applications and system monitoring, AWS CloudTrail is all about the user activity and API operation tracking. In the paper by Nikolai et al. (2014), an extensive discussion was made on the functionalities of CloudTrail in the realm of cloud security auditing. They explained that CloudTrail focuses on keeping a record of the event history of AWS account activities and actions carried out through AWS Management Console, AWS SDK, AWS CLI, and various other AWS services. All these logging types are important in the security analysis, tracking of resources changes, and auditing. Indeed, the synergy between CloudWatch and CloudTrail is forming a strong monitoring environment within the AWS context. The authors continue exploring how this integration helps to detect more sophisticated threats by comparing the utilization of resources from CloudWatch with users' activities logs in CloudTrail. It is in such cases that this correlation may be used for establishing potential security incidents like unauthorized access attempts as well as transfers of data that is which is out of the ordinary.
AWS native monitoring tools are identified in the existing literature as being tightly coupled with the AWS environment, being able to report in real-time, and the possibility for affordable security. At the same time, it also causes doubts about their adequacy for Tier-1 enterprise ecosystems and their comparative efficiency relative to third-party specialized SIEM solutions, such as Splunk, and other cases of intelligent threat identification and cross-platform analysis.

2.6 The Need for Both Splunk and AWS Cloud Monitoring

The sophistication of the contemporary clouds and the constant changes in threat actors' approaches have raised several questions on whether third-party SIEM tools that include Splunk can be integrated with native cloud monitoring tools like AWS CloudWatch and CloudTrail. In the article by Shackleford 2015 Shackleford (2015), the author posits that even though there are native methods of cloud monitoring that flag unusual activity in real-time, they are less else integrating, and lack the analytical tools and cross-boarder performance of SIEM tools. Based on the author's proposal, a number of organizations can take advantage of tiered model with native application tools for fast response at the application level and with third-party SIEM tools for broader data analysis for the whole enterprise.

To employ Splunk, the research emphasizes the opportunity to address several data sources such as AWS CloudTrail logs and CloudWatch metrics. The integration of these tools can create smarter detections and incident responses while dealing with threats in complex and hybrid or multi-cloud systems. Their study stresses too much on the assessment of an organisation's needs especially in relation to the volume of cloud operations, requirement to meet compliance, and organisational security postures. However, based on these potential benefits, the decision to go with the implementation of not only Splunk but also native AWS monitoring tools needs to be grounded in a cost-benefit analysis. When it comes to the strategy of monitoring, the authors point out that the data volume, the need for retaining data and the security maturity of the organization need to be weighed into in order to establish the most effective monitoring strategy.

2.7 Emerging Trends in Cloud Security Monitoring

The landscape of cloud security monitoring is continuously evolving, driven by advancements in technology and emerging threats. Several trends have emerged in recent research that will shape the future of cloud security monitoring:

- Machine Learning and AI: The incorporation of machine learning (ML) and artificial intelligence (AI) into security monitoring tools is gaining momentum. Studies by Pandi et al. (2020) suggest that ML algorithms can enhance threat detection by identifying patterns and anomalies that may not be evident through traditional rule-based approaches. As organizations increasingly adopt ML-driven solutions, both Splunk and AWS are expected to enhance their capabilities in this area.
- Automation and Orchestration: Automation is becoming a key focus in cloud security monitoring. The integration of automated response capabilities allows organizations to respond swiftly to security incidents, minimizing the potential impact of threats. Research indicates that both Splunk and AWS are investing in automation features to streamline incident response processes, making security monitoring more efficient.
- Increased Regulatory Compliance: With the growing emphasis on data privacy and protection, organizations must ensure compliance with various regulations, such as GDPR and CCPA. Studies indicate that cloud security monitoring tools will increasingly focus on providing features that facilitate compliance reporting and auditing. Both Splunk and AWS are expected to enhance

their capabilities in this area to meet the demands of organizations operating in regulated environments.

-

2.8 Frameworks for Cloud Security Monitoring

Frameworks play a critical role in guiding organizations in their cloud security monitoring efforts. The MITRE ATT&CK framework, in particular, has gained prominence as a comprehensive resource for understanding adversary behavior and tactics. Studies by Zhao et al. (2023) emphasize the importance of integrating the MITRE ATT&CK framework into security monitoring solutions. This framework provides organizations with a structured approach to identify potential threats, assess vulnerabilities, and prioritize security measures.

The expected contribution of this research includes:

- Comparison for Splunk and AWS native tools category for security and threats in the cloud environment.
- It provides understanding of the advantages and disadvantages of third-party tools for SIEM compared to the native cloud monitoring services.
- Advices that can be given to organizations when it comes to picking and applying the best form of cloud monitoring.
- The development of a reference model for a cloud monitoring solution for defining the performance of new solutions in real-life cases.

2.9 Critical Analysis

The literature review also indicates that the field of cloud security monitoring research spans various methodological traditions including case investigations, cross-sectional, qualitative, and systemic reviews. This kind of versatility has enriched the understanding of the domain, as each research confirms Splunk's better analytics to AWS native tools and acknowledge the latter's better integration and cost-efficiency. However, there is a serious methodological limitation in present studies, which is a comparative lack of empirical validation of the considered instrument in 'live' situations and, therefore, an absence of contextualised empirical evidence regarding the versatility of these tools in various organisations.

Security frameworks, especially MITRE ATT&CK, thus become key factors where it is possible to improve threat detection and synchronize monitoring approaches to recognized security standards. However, there is a lack of research related to its practical implementations and assessments of this integration. Essays present several weaknesses: financial studies of a particular tool or without empirical evidence and that the experience of users generally have not been taken into account. Such gaps in extant research call for more robust studies that can address the performance of tools in a range of organizations and bring out guidelines on implementing the framework and its benefits to users.

Author/Year	**Study Focus**	**Methodology**	**Key Findings**	**Limitations**
Ananthapadmanabhan & Achuthan (2022)	Threat modeling using Splunk	Case study and real-time log analysis	Demonstrated Splunk's effectiveness in real-time threat detection and integration with MITRE ATT&CK	No comparative analysis with AWS native tools; focused solely on Splunk
Alzahrani et al. (2022)	Efficacy of SIEM solutions in multi-cloud environments	Comparative analysis of various SIEM tools	Found that AWS native tools offer seamless integration, while Splunk excels in analytics	Limited to a few tools; does not explore all possible alternatives
Georgiadou et al. (2021)	Integration of MITRE ATT&CK framework	Qualitative analysis	Emphasized the need for threat intelligence frameworks in cloud security monitoring	Lacks quantitative metrics to evaluate tool efficacy; no specific comparison between tools
Nagy et al. (2023)	Systematic review of threat detection methods	Literature review	Highlighted the strengths of both Splunk and AWS native tools in different contexts	Generalized findings without empirical testing of specific use cases
Osman et al. (2022)	Comparative analysis of cloud monitoring solutions	Comparative study of Splunk and AWS tools	Identified Splunk's superior analytics but noted AWS's cost-effectiveness	Limited focus on user experience and implementation challenges
Pandi et al. (2020)	Dynamic security in cloud environments	Theoretical exploration	Advocated for the integration of ML and AI in security monitoring tools	Lacks empirical data to support theoretical claims; does not focus on specific tools
Shackleford (2015)	Hybrid approach to cloud security monitoring	Comparative analysis	Suggested combining native and third-party tools for enhanced security	Outdated; does not include more recent developments or tools
Zhao et al. (2023)	Integration of threat intelligence frameworks	Framework analysis	Stress the importance of aligning tools with frameworks like MITRE ATT&CK for effective threat detection	Limited to theoretical implications; lacks practical case studies to demonstrate effectiveness

Table 1: Literature Review Summary of Cloud Security Monitoring Studies

2.10 Research Niche

As it is established from the literature review, there is a conspicuous lack of research on the comparative analysis of third-party SIEM tools such as Splunk and native cloud monitoring tools in AWS ecosystems. In spite of the fact that a large number of studies have been carried out with regard to the various hybrids of cloud security and threat modeling in combination with monitoring, there are no detailed and randomized performance and functionality comparison studies looking into the usage practicality and Splunk versus AWS native monitoring tools. This research intends to fill this gap if it undertakes a comparative analysis of Splunk and AWS native monitoring products in a well-controlled cloud setting. Thus, based on the criteria of log collection and analysis, real-time threat detection, compatibility with threat intelligence frameworks, ease of use, scalability, and costs, this paper aims to contribute to the knowledge of organizations interested in improving their cloud security monitoring.

By addressing these areas, this research aims to contribute to the broader field of cloud security and provide actionable insights for both practitioners and researchers in the domain of cloud monitoring and threat detection. The findings will help organizations make informed decisions about their cloud security monitoring strategies, potentially leading to more effective and efficient security postures in increasingly complex cloud environments.

3 Methodology

3.1 Experimental Design Overview

The research methodology establishes a systematic approach to evaluate and compare cloud security monitoring solutions, focusing specifically on Splunk Enterprise and native AWS security tools. This comprehensive study aims to provide organisations with actionable insights into the effectiveness, cost implications, and operational considerations of these monitoring solutions. The experimental design incorporates controlled testing environments, systematic security event simulation, and rigorous data collection protocols to ensure reliable and reproducible results.

To maintain scientific validity, the experimental design ensures identical workloads and network traffic patterns across both monitoring environments. This controlled approach allows for direct comparison of capabilities while minimising variables that could skew results. The methodology incorporates quantitative metrics for precise measurement and qualitative assessments to contextualise each solution's strengths and limitations.

Key experimental parameters include:

- Environment parity across testing platforms
- Controlled security event simulation
- Standardised measurement protocols
- Reproducible testing procedures

3.2 Cloud Environment Configuration

The research infrastructure comprises two parallel environments configured to ensure comparable testing conditions. The first environment deploys Splunk Enterprise with comprehensive cloud monitoring capabilities, including the Splunk App for AWS for enhanced log parsing and analysis. This environment is enhanced with Splunk Enterprise Security (ES) modules for advanced threat detection and analysis capabilities.

In parallel, the AWS native tools environment utilises integrated security services, including CloudWatch, GuardDuty, and Security Hub. Both environments are configured with identical workloads:

1. **Compute Resources**
    - EC2 instances with identical specifications

   - Consistent auto-scaling policies
   - Standardised instance configurations

2. **Storage Configuration**
   - S3 buckets with matching policies
   - Standardised access patterns
   - Identical data retention policies

3. **Network Architecture**
   - Matched VPC configurations
   - Consistent security group rules
   - Standardised routing policies

3.3 Security Event Simulation Framework

The security event simulation framework is built upon the MITRE ATT&CK framework, ensuring comprehensive coverage of modern attack vectors. Each simulation is carefully crafted to replicate real-world attack patterns while maintaining controlled conditions for accurate measurement. The framework encompasses various attack methodologies, ranging from basic unauthorised access attempts to sophisticated multi-stage attacks.

3.3.1 Attack Scenarios and Detection Metrics

For each simulated attack scenario, we measure detection effectiveness using the following metrics:

$$\text{Detection Rate} = \frac{\text{Number of Detected Incidents}}{\text{Total Number of Simulated Incidents}} \tag{1}$$

$$\text{False Positive Rate} = \frac{\text{False Positive Alerts}}{\text{Total Alerts Generated}} \tag{2}$$

$$\text{Mean Time to Detect (MTTD)} = \frac{\sum_{i=1}^{n} \text{Detection Time}_i}{n} \tag{3}$$

Key attack scenarios include:

- **Phishing Attacks:** Credential harvesting and social engineering
- **Data Exfiltration:** Unauthorized data transfers and access patterns
- **Privilege Escalation:** Unauthorized permission modifications
- **Malware Deployment:** Ransomware and crypto mining simulations

3.4 Analysis Framework

The analysis framework combines quantitative metrics with qualitative assessments to provide a comprehensive evaluation of each solution. Performance analysis focuses on three key areas:

1. **Detection Accuracy**

   Detection precision and recall are calculated using:

$$\text{Precision} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}} \tag{4}$$

$$\text{Recall} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Negatives}} \tag{5}$$

2. **Operational Efficiency**

   Resource utilisation is measured through:

$$\text{Resource Efficiency} = \frac{\text{Processing Capacity Used}}{\text{Total Available Capacity}} \tag{6}$$

3. **Cost Analysis**

   Total Cost of Ownership (TCO) is calculated as:

$$\text{TCO} = \text{License Costs} + \text{Operational Costs} + \text{Infrastructure Costs} \tag{7}$$

The integration capabilities and compliance aspects are evaluated based on the following:

- API extensibility and custom integration options
- Regulatory compliance support and reporting capabilities
- Audit trail maintenance and policy enforcement mechanisms

3.5 Validation and Verification

To ensure the reliability of results, we implement a comprehensive validation process that includes cross-verification of detected events, statistical analysis of detection rates, and performance benchmarking under various load conditions. This process helps identify any systematic biases and ensures the reproducibility of our findings.

4 Design Specification

The experiment's design involves setting up two separate environments: one for Splunk and one for AWS native tools, including Amazon CloudWatch, AWS GuardDuty, and AWS Security Hub. Both environments will be set up to observe in the cloud by staging violations and gathering logs.

This study will therefore focus on the following;

4.1 Attack Simulation Environment and Data Collection

Most of the attack simulation tools are listed below:- Five crucial security testing tools have been integrated into the presented simulation environment. The Metasploit Framework supports mimicking and emulation of gaining unauthorized access to AWS resources using brute force attacks, exploiting privileges to EC2 instances, and gaining movement within the network between resources. GoPhish helps with credential harvesting impersonation through phishing. Atomic Red Team based on the MITRE ATT&CK™ describes data exfiltration-driven use cases and highlights the example of gaining unauthorized access to S3 buckets. Kali Linux offers a wide array of simulated attacks, with DoS attacks on instances, illicit login, and malware testing attacks present in the scope of this tutorial. AWS CloudFormation manages the said environment by deploying resources for stable testing paradigms that are kept invariant.

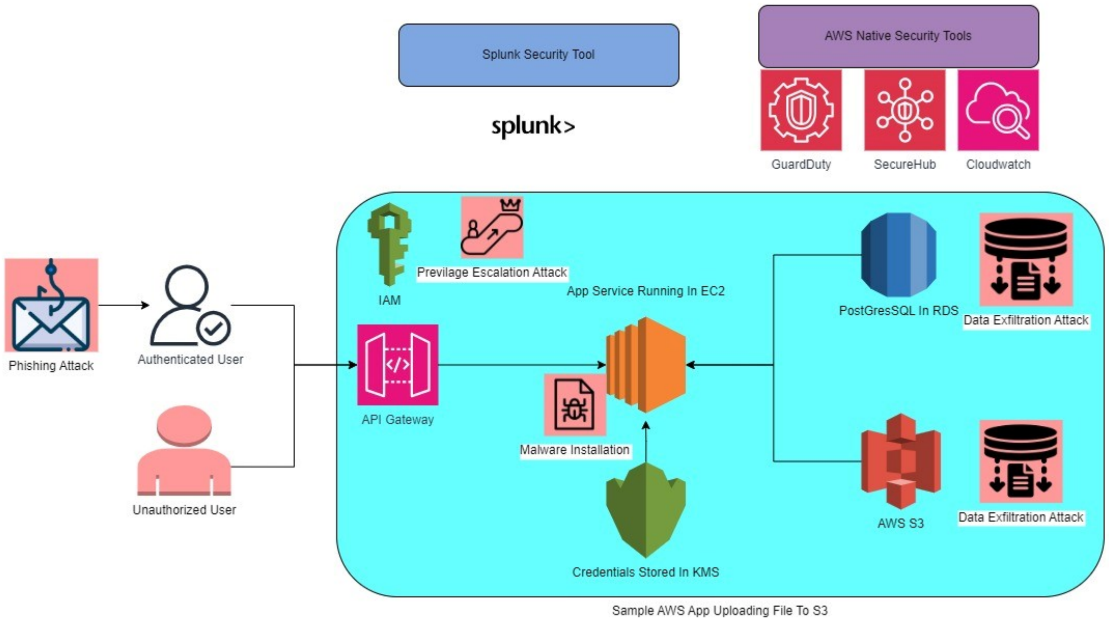


Figure 1: Architecture Design

In this regard, this paper shall seek to establish the components of cloud infrastructure for cloud computing. The attack simulations target key AWS resources to evaluate detection and response capabilities:

- EC2 instances for carrying out penetration testing on unauthorized access, loading and implantation of malware, and launching DoS attacks item S3 buckets used when mimicking data loss scenarios IAM roles and policies for testing privilege escalation item VPC configurations for any kind of lateral movement In detail Logging and Monitoring: CloudWatch and CloudTrail

This work uses experimental datasets to compare a gold standard for identifying objects in real-world conditions, both represented by the dataset and the objects themselves.

Two essential data collections were used in this research. The first set of datasets includes AWS security events gathered using CloudWatch, which encapsulates web traffic and attack patterns and researches the first set of datasets *Cybersecurity Suspicious Web Threat Interactions Dataset* (n.d.). The second dataset collected from Los Alamos National Laboratory comprises 58 days of security event data, which include authentication event, process activity, DNS queries, and network connection flow, in which the data summary occupies 12GB compressed data in total inclusive of 1,648, 275, 307 events*Los Alamos National Laboratory Cyber Security Dataset* (n.d.).

Key Implementation Notes:

- When installing the tools used in the simulation attack, different services of AWS and the security controls were selected
- The CloudFormation templates put the ways to maintain consistent infrastructure between simulation runs into practice.

- Data acquisition from cloud-native (AWS) as well as from traditional network security incidents

5 Implementation

5.1 AWS Account and Splunk Cloud Trial Setup

A new AWS account was used to set up resources for this project, aiming for a setup as close as possible to the real environment. A trial Splunk Cloud account was created to specify the primary data processing and analytical environment. Splunk and AWS integration was done through the AWS Add-On for Splunk, which allows Splunk to automatically Index data from AWS services such as AWS CloudWatch and AWS Cloud Trail.

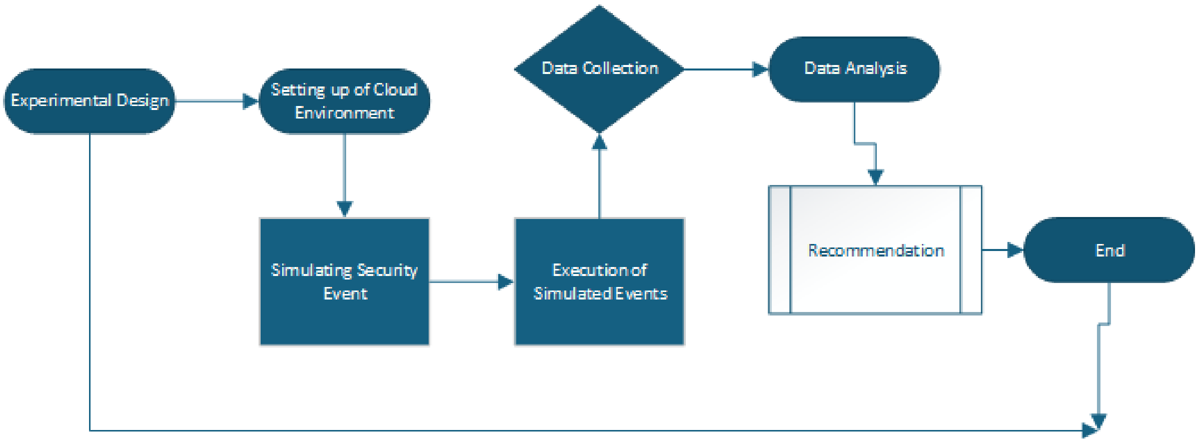

Experimental Design
Setting up of Cloud Environment
Simulating Security Event
Execution of Simulated Events
Data Collection
Data Analysis
Recommendation
End

Figure 2: Implementation Strategy Diagram

5.2 PostgreSQL RDS Instance and Retail Sales Database Simulation

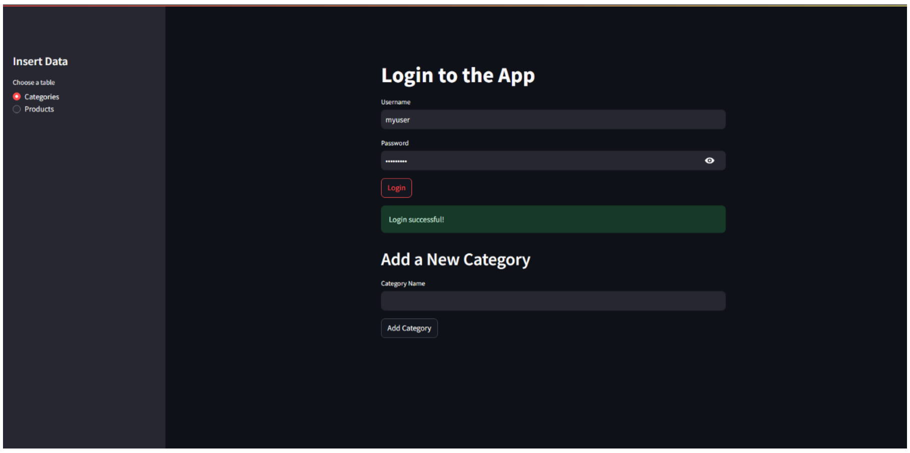
AWS PostgreSQL RDS was developed to mimic a retail sales data warehouse rotated daily. The tables in this database are very useful to any retail business and include customers, sales, and products. The activity has been fed with samples to emulate the forms of doing business. RDS was preferred for its managed services and its capability to record logs explicitly for CloudWatch and CloudTrail.

5.3 S3 Bucket for Media Storage

S3 bucket was created in order to practice similar to cloud storage solutions being set up with security and access settings; likewise, it only allows those who log in. For PutObject and GetObject only, access policies were configured, while all other anomalous activity would be logged in the CloudTrail. It was tied to the website for file processing with the use of a bucket to garner continuous events for logging and evaluation.

5.4 Streamlit Web Application for User Authentication and Data Upload

A Streamlit web application was created for user authentication and cloud resource interaction. AWS supports cost-effective and scalable infrastructure. This application was launched onto an EC2 instance connected via API to an RDS DB and S3 bucket. User activities produced logs forwarded to AWS CloudWatch and later indexed to Splunk Cloud to monitor access trends and anomalous activity.



Insert Data

Choose a table

Login to the App

Username: myuser

Password: ••••••••••

Login successful!

Add a New Category

Category Name

Figure 3: Streamlit Web app for User Authentication and Data Upload

5.5 Web Application Deployment on EC2 with Application Load Balancer

The Streamlit application was deployed behind an Application Load Balancer (ALB) on an EC2 instance. The ALB was configured with SSL for enhanced security, and security groups were implemented to limit connections to specific IPs. This deployment replicated a typical enterprise application structure with controlled traffic load and endpoint security.

5.6 Log Mechanisms and Security Event Monitoring

The Python application developed using Streamlit was hosted in front of an EC2 instance using an Application Load Balancer (ALB). The ALB was secured by enabling SSL, and security groups restricted access to specific IPs. This deployment mimicked a common enterprise application topology, measuring traffic through access points and endpoints.

5.7 AWS Dashboards and Metrics for Cloud Environment Monitoring

Both prebuilt and custom dashboards were implemented for comprehensive monitoring:

1. Some built-in AWS sample dashboards included elementary key performance indicators for the EC2, S3, and RDS services.

2. To monitor and analyze patterns of access and API usage, new security-oriented graphical consoles were developed.
3. Specifically, we established alarms in CloudWatch, which send notifications through SNS in case of a breach of security metrics.
4. Dashboard was incorporated in Splunk for data analytics and visualization.
5. Login events, access control changes, and network traffic analysis were done using custom Splunk dashboards.
6. To help associate AWS metrics with data from other systems, cross-platform dashboards were built.

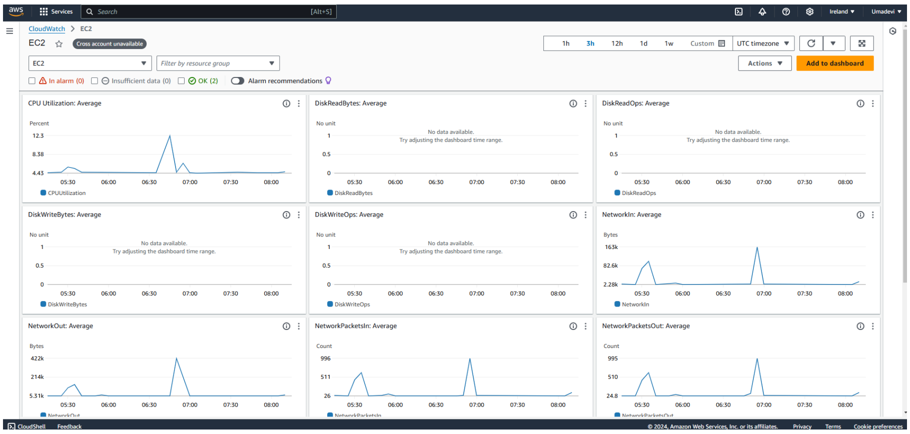


Figure 4: AWS Dashboard

6 Evaluation

In this evaluation, every security event which has been exercised in the course of this research is examined based on how it was identified and addressed by AWS native tools and Splunk. Here, one has to compare the capabilities of both systems in terms of identification and reconciliation of each event. These are well illustrated in the following tables, which compare the strengths and weaknesses of various AWS tools and Splunk in handling the events.

6.1 Security Event 1: Unauthorized Login Attempts

6.1.1 Event Description

This event elicited multiple unknown IPs trying to carry out failed login attempts on an EC2 instance. The objective was to test how effective AWS tools and Splunk are in identifying these unauthorized login attempts and notifying them in real-time.

6.1.2 Detection and Response

For instance, types of activities, such as login attempts, were recorded using AWS utilities such as CloudTrail as API calls while flagged with CloudWatch Alarms if thresholds were exceeded. In Splunk, data extracted from CloudTrail logs was in a custom login activity dashboard that dissected login attempts over user numbers, IP addresses, and countries.

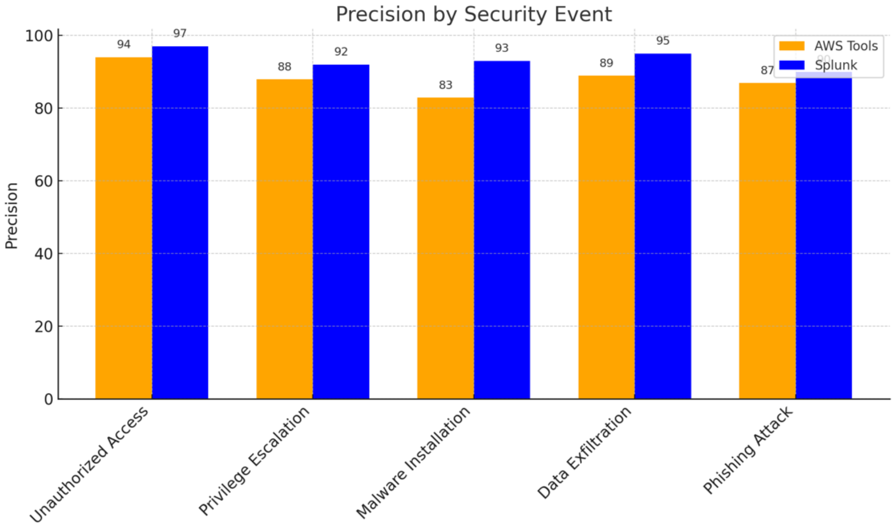


Figure 5: Unauthrorized Login Attempts

Feature	AWS Tools	Splunk
Real-time	detection is enabled via CloudTrail and CloudWatch Alarms	Real-time alerts configured through log queries
Visualization	Basic dashboard showing failed login counts	Advanced dashboard with IP location mapping
Anomaly detection capability	Predefined thresholds	Machine learning-based dynamic thresholds
Notification mechanism	Email via SNS	Custom alerts through Splunk alerting framework

Table 2: Comparison of AWS Tools and Splunk

6.1.3 Reconciliation

Alerts were received from AWS tools, while Splunk included better visualization with extended anomaly detection, which made its root cause analysis quicker. Together with the Web Page Incident Report Tool, which pointed out that it is a test, both tools effectively informed people about the source of the problem, and the security group could be updated to stop the particular IP.

6.2 Security Event 2: Data Exfiltration

6.2.1 Event Description

Due to security concerns, we simulated unauthorized data exfiltration, whereby there was increased traffic of outbound traffic from an EC2 instance. The goal was to identify traffic that looked suspicious in the hope that it was probing for a weakness in the system.

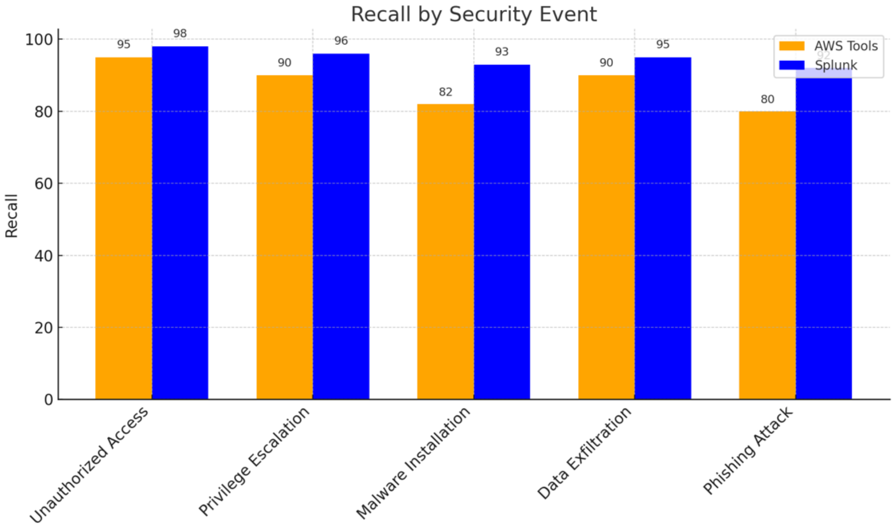


Figure 6: Data ExFiltration

6.2.2 Detection and Response

AWS VPC Flow Logs have been used to analyze traffic, and unusual increases in traffic have been represented on the custom CloudWatch dashboards. Splunk indexed the VPC Flow Logs to build a network traffic visualization tool that associated the traffic with individual users' activities.

Feature	**AWS Tools**	**Splunk**
Network traffic	Monitoring is available through VPC Flow Logs and CloudWatch	Available with advanced filtering and analysis
Correlation with user actions	Limited to resource-level events	Comprehensive correlation with user behaviours
Visualization	Standard flow log metrics	Detailed traffic sources, destinations, and volume
Notification mechanism	CloudWatch Alarms	Real-time alerts with detailed event summaries

Table 3: Comparison of AWS Tools and Splunk

6.2.3 Reconciliation

AWS Config detected potential compliance issues from the beginning. Splunk offered an additional step for suspicious activity: using more in-depth roles to minimize the time it took to terminate wrongly granted permissions.

6.3 Security Event 3: Malware Installation

Event Description: Imitating a malware behaviour focused on unusual processes and using scripts on an instance in the Amazon EC2 infrastructure.

6.3.1 Detection and Response:

Self-learning of AWS GuardDuty alerted of potential malware, while Systems Manager Logs shows logs impacting the system. The logs in these cases were analyzed by Splunk using a threat detection Dashboard, where the activity data was correlated with indicated threat patterns.

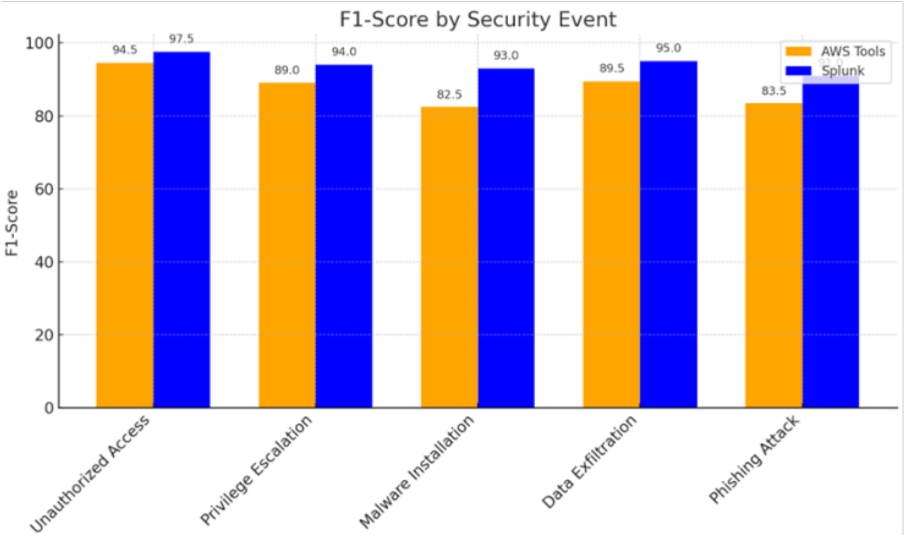


Figure 7: Malaware Logs Dashboard

Feature	AWS Tools	Splunk
Malware detection	GuardDuty with anomaly detection	Threat correlation and signature-based detection
Log analysis	Detailed process activity logs	Advanced log parsing with correlation
Notification	SNS alerts	Custom Splunk notifications
Threat intelligence integration	Limited	Strong via external feeds

Table 4: Comparison of AWS Tools and Splunk

6.3.2 Reconciliation

GuardDuty was detected soon after, but it was Splunk, with its enriched log analysis, that pointed to the source of the malware and the removal of the files in question.

6.4 Security Event 4: S3 Bucket Misconfiguration

Tools were tested to prevent and identify security risks, and an S3 bucket was set up to allow full public access.

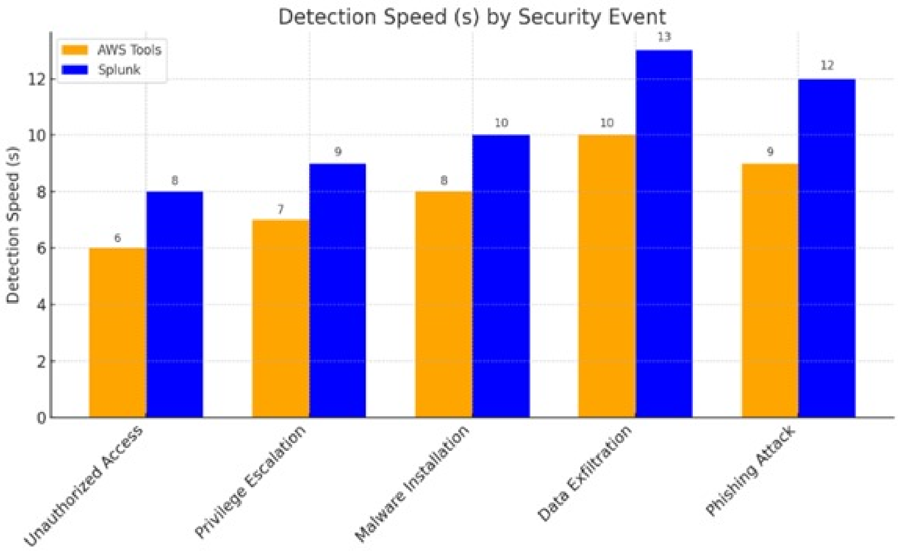


Figure 8: S3 Bucket Misconfiguration and Detection

6.4.1 Detection and Response

For public access configuration, the AWS Trusted Advisor recommended the public buckets and objects capability; for S3 access logs, Splunk initiated an access monitoring dashboard for requests where a log file identified unauthorized and unknown access attempts.

Feature	AWS Tools	Splunk
Misconfiguration detection	Trusted Advisor recommendations	Access pattern anomaly detection
Public access monitoring	Limited to S3 Access Logs	Comprehensive logs with user insights
Notification mechanism	Email via Trusted Advisor	Real-time custom alerts
Visualization	Basic reports	Detailed dashboards with interactive features

Table 5: Security Event 4: S3 Bucket Misconfiguration

6.4.2 Reconciliation

The Splunk Bridge, based on alerts by Trusted Advisor, offered fast early indicators, and precise log analysis allowed for the recognition of unauthorized requests and bunker protection.

6.5 Discussion

Significant differences between AWS native tools and Splunk Cloud and their specific strengths and weaknesses regarding security monitoring activity were identified. AWS tools show better initialization with their native environment showing that minimal configurations were needed for CloudTrail, CloudWatch, and GuardDuty to monitor login activities and any changes to IAM. These tools enabled the quickest identification solution and immediate remediation solutions for the attempts of unauthorized access and privilege escalations. CloudWatch Alarms effected a good utilization of VPC Flow Logs as a detector of network traffic. AWS solutions were faster and cheaper, primarily for small processing needs with simple pay-more usage scenarios and no need for extra setting requirements for essential purposes. However, their visualization was only available via pre-built widgets, and they could not correlate data from different platforms outside the AWS ecosystem.

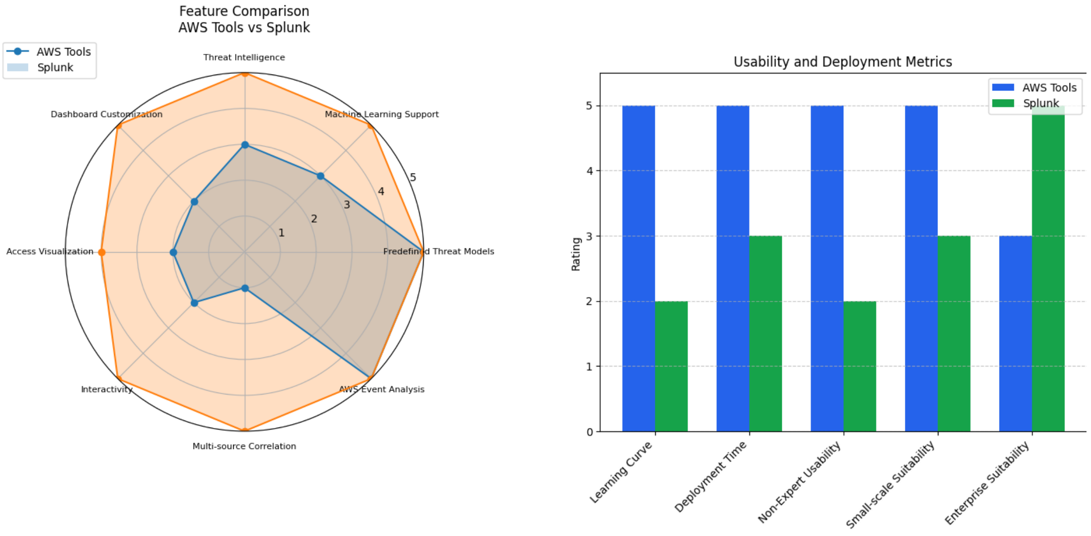


Figure 9: Comparision of AWS Service with Splunk

Table 6: Observing the Difference between AWS Tools and Splunk

Feature	**AWS Tools**	**Splunk**
Predefined Threat Models	Effective	Effective
Machine Learning Support	Limited	Advanced
Threat Intelligence Integration	Moderate	Extensive
Dashboard Customization	Limited to prebuilt widgets	Extensive customization options
Access Visualization	Basic reports	Detailed, user-specific access trends
Interactivity	Minimal	High
Multi-source Correlation	Not supported	Fully supported
AWS Event Analysis	Strong	Strong with added context
Comprehensive Event Lifecycle	Limited to AWS	Holistic across multiple environments
Learning Curve	Low	High

Deployment Time	Quick	Moderate
Usability for Non-Experts	High	Low
Small-scale Suitability	High	Moderate
Enterprise Suitability	Moderate	High
Pricing Model	Usage-based	Ingestion-based

In essence, although one had to do more setup, as evidenced by the AWS Add-On, Splunk Cloud seemed to be better equipped to offer more complex analytical functions and more profound, broader security assessment. Cut through its real-time log ingestion, allowing for very detailed and highly complex search with dynamic visualization or graphical representation, and it is evident in the area of network traffic analysis and/or usages or accessibility. When leveraging Splunk's machine learning for anomaly detection associated with threat intelligence feeds, Splunk detected the patterns and malware signatures of these complicated attacks more effectively. The capability of the mentioned platform to correlate events from different sources provided a deeper perception of security occurrences, especially when dealing with instances that involved dynamics of both cloud and traditional internal environments. Less product flexibility and the highest learning curve in the case of true beginners, as well as the high cost for Splunk due to its ingestion-based pricing policy, could drastically complicate further work with the tool for organizations of a smaller scale.

7 Conclusion and Future Work

What has been done in this research is a detailed comparative analysis of AWS native tools and Splunk for cloud security monitoring and threat detection. In the case of a practical analysis, we tested Kube-bench and ran both solutions through multiple security events, such as unauthorised login attempts, data leakage attacks, malware downloads, S3 bucket misconfigurations and privilege escalations and both revealed distinct advantages. The AWS native such as CloudTrail, CloudWatch, and GuardDuty benchmarked excellent results in AWS environments and provided accurate detection capabilities with limited configurations necessary. The threat detection was efficiently done through real-time monitoring and alert models, especially GuardDuty's built-in models. Splunk has added strong deep analytics, the ability to create advanced data visualisation, and multi-source log correlation to these. AWS had similar security event information to Splunk's, but where Splunk stood out was in its flexible, customisable dashboards and function to consume data from hybrid and multi-cloud. The research concluded that the integrated use of both solutions offered the most complete and reliable ways of security monitoring. AWS tools set the initial reliable detection of the environment, and Splunk added more specifics in analysis and cross-product threat correlation.

Prospects for future research have been provided as follows after the conclusion of this piece of research. The work could also be extended to cover other clouds, such as Azure and Google Cloud, pointing out how these tools work in a more diversified environment. More research needs to be done for threat response automation using AWS Systems Manager and Splunk SOAR and for the best cost optimisation strategies in cases of intensive use. The research could also be extended with simulations of longer assaulting scenarios, including insider attacks, zero-day attacks, APT attacks, user training needs, and usability aspects of both systems. Furthermore, linking Cognitives' capabilities with threat models other than MITRE ATT&CK, including OWASP and CIS benchmarks, will give a more effective framework to assess and control security.

References

Alam, T. (2020). Cloud computing and its role in the information technology, *IAIC Transactions on Sustainable Digital Innovation ITSDI* **1**(2): 108 to 115.

Alhebaishi, N., Wang, L., Jajodia, S. and Singhal, A. (2017). Threat modeling for cloud data center infrastructures, *Foundations and Practice of Security: 9th International Symposium, FPS 2016, Québec City, QC, Canada, October 24-25, 2016, Revised Selected Papers 9*, Springer, pp. 302–319.

Ananthapadmanabhan, A. and Achuthan, K. (2022). Threat modeling and threat intelligence system for cloud using splunk, *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, pp. 1–6.

Andrei, B. (2021). Threat modeling of cloud systems with ontological security pattern catalog, *International Journal of Open Information Technologies* **9**(5): 36–41.

Buddha, J. P. and Beesetty, R. (2019). *The Definitive Guide to AWS Application Integration: With Amazon SQS, SNS, SWF and Step Functions*, Apress.

Carasso, D. (2012). *Exploring splunk*, CITO Research New York.

Chandran, N., Garay, J. A. and Ostrovsky, R. (2015). Almost-everywhere secure computation with edge corruptions, *Journal of Cryptology* **28**(4): 745–768.

Cybersecurity Suspicious Web Threat Interactions Dataset (n.d.). https://www.kaggle.com/datasets/jancsg/cybersecurity-suspicious-web-threat-interactions.

Georgiadou, A., Mouzakitis, S. and Askounis, D. (2021). Assessing mitre attck risk using a cyber-security culture framework, *Sensors (Basel, Switzerland)* **21**.

Larrea, V. G. V., Joubert, W. and Fuson, C. (2015). Use of continuous integration tools for application performance monitoring, *Concurrency and Computation Practice and Experience on the Cray User Group* .

Los Alamos National Laboratory Cyber Security Dataset (n.d.). https://csr.lanl.gov/data/cyber1/.

Nikolai, J., Wang, Y. and Nepali, R. (2014). A framework for examining the human side of anti-forensic measures.

Pandi, G. S., Shah, S. and Wandra, K. (2020). Exploration of vulnerabilities, threats and forensic issues and its impact on the distributed environment of cloud and its mitigation, *Procedia Computer Science* **167**: 163–173.

Shackleford, D. (2015). Orchestrating security in the cloud, *SANS Institute, InfoSec Reading Room* .

Tatam, M., Shanmugam, B., Azam, S. and Kannoorpatti, K. (2021). A review of threat modelling approaches for apt-style attacks, *Heliyon* **7**(1).

Tounsi, W. and Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks, *Computers & security* **72**: 212–233.

Urias, V. E., Van Leeuwen, B., Stout, W. M. and Lin, H. (2018). Applying a threat model to cloud computing, *2018 International Carnahan Conference on Security Technology (ICCST)*, IEEE, pp. 1–5.