SCIENTIFIC OASIS

Decision Making: Applications in Management and Engineering

ISSN: 2560-6018, eISSN: 2620-0104

LEVERAGING CSPM FOR PROACTIVE CLOUD CONFIGURATION MANAGEMENT

G Sreenivasa Yadav
Research Scholar
Department of Computer Science and Engineering
Annamalai University
Annamalainagar – 608 002

Dr. G Karthick
Assistant Professor
Department of Computer Science and Engineering
Annamalai University
Annamalainagar – 608 002

Dr. C.H. Mukundha
Associate Professor
Department of Information Technology
Sreenidhi Institute of Science and Technology, Hyderabad
Telangana-501301.

Abstract – The widespread use of cloud computing has led to big and small organizations alike facing myriad and demanding security challenges. Cloud Security Posture Management (CSPM) tools have been developed to help organizations manage not just security configurations on cloud infrastructure but other associated problems. This research takes on the difficulty of accurately assessing and maintaining cloud security. Such failing often goes undetected because top-down assessments of cloud infrastructure and services are hard to accomplish. Hence in this research a new methodology was proposed namely Dynamic Cloud Security Assessments (DCSA), to continually evaluate the use of CSPM tools in a series of real-world, real-time, and virtual experiments. A public cloud platform that the authors were more than familiar with and appeared to offer what one would call real-time visibility was chosen, within its terms of service.

Amazon Web Services (AWS), Microsoft Azure, and the Google Cloud Platform (GCP) were the platforms under evaluation.

Keywords– CSPM, DSCA, Dynamic Cloud Security Assessments and Cloud Computing.

I. INTRODUCTION

The deployment and management of IT resources in organizations has been dramatically changed by cloud computing, as it allows incomparable scalability, flexibility, and cost-effectiveness [1-2][9]. However, the transition of cloud has brought new complexities and challenges about security. Protecting the cloud environment's security plays a critical role because misconfigurations, vulnerabilities, and compliance failures often result in a serious of data breaches and disruptive operations [3]. Therefore, Cloud Security Posture Management (CSPM), a suite of tools that provides automated mechanisms for monitoring, assessing, and identifying security misconfigurations in cloud environments, gained popularity as an essential solution that helps combating these security challenges [4].

While the potential of CSPM tools is clear, testing their effectiveness in real-life settings remains a key question. Our study investigates the Dynamic Cloud Security Assessment (DCSA) methodology, a new system for measuring the functionality of CSPM tools in a controlled yet practical cloud environment. With a heavy emphasis on dynamic monitoring, automated reaction to emergencies and ongoing compliance checks, the DCSA methodology employs cutting edge techniques to create a comprehensive testing framework.

PROBLEM STATEMENT

The changes occurring in IT infrastructures, due to the speed at which cloud computing is being taken up, are dramatic and offer distinct advantages such as cost and flexibility improvements through scalability. Nonetheless, cloud migration includes some severe challenges, none possibly more so than the security of the cloud. Traditional measures, policies and practices in this area do not easily apply to the distributed nature of the cloud, the continuous development and integration and the commonality of the multi-tenancy network architectural [5-6].

Managing security configurations for the rapidly changing and diverse cloud resources is one of the most urgent challenges in cloud security [7]. Misconfiguration is one of the pivotal reasons for cloud security incidents. This opens the door to data breaches and puts critical systems at risk. Open network ports, insecure storage permissions, weak identity and access management (IAM) policies, and lack of encryption are among the common misconfigurations. The dynamic and short-lived nature of cloud resources further complicates the issue [8-10]. In cloud deployments, configurations change so quickly that manual control is not practical and is prone to error.

The essential tools to address these challenges are Cloud Security Posture Management (CSPM) tools [11-13]. CSPM tools provide automated mechanisms for continuously monitoring public cloud environments, identifying cloud misconfigurations, vulnerabilities, and compliance

issues, and enforcing cloud security best practices [14]. Although CSPM tools expand their capabilities to emerging cloud service providers, many challenges still exist in real-world scenarios. In this research, we focus on evaluating the effectiveness of CSPM tools in enabling security operation teams to provide the security guarantee on elastic. Rather than this research studying on how CSPM tools improve cloud security, we focus on answering the following research questions:

RQ1: How effectively can CSPM tools adapt to the dynamic nature of cloud environments?

RQ2: How effectively can CSPM tools detect and mitigate security incidents in public cloud environments in real-time?

RQ3: How effectively can CSPM tools enforce regulatory compliance that involves privacy and residency constraints?

The main issue here is that we don't have a standardized, all-things-considered method for assessing how well CSPM tools work with realistic cloud environments [15-20]. Right now, the ways we typically gather information to evaluate them are missing a lot of important stuff.
A Dynamic Environment Simulation: Many evaluation techniques fail to fully simulate the dynamic and ever-evolving nature of cloud environments. They do not consider the continuous changes in configurations, the addition of new resources, and the operational updates that are standard in cloud environments [16-17]. This missing link makes it difficult to evaluate how an ongoing CSPM solution is able to accommodate the changes and sustain a comprehensive security model in place.

Real-world misconfigurations: One major missing piece is the lack of realistic testing scenarios, including the common misconfigurations and vulnerabilities found on the real cloud, without those scenarios [18], it is hard to evaluate the CSPM tool’s capability to detect and remediate the security issues that the organization actually face.

Continuous compliance verification is paramount in cloud security as regulatory standards and internal policies dictate. Nonetheless, none of the existing evaluation methods holistically evaluate the capability of CSPM tools to enforce continuous compliance, log audit trails, and generate thorough compliance reports [19].

Integration and Automation: Successful cloud security management depends on the seamless integration and automation of different security tools and processes [20-21]. Many evaluation methodologies overlook the integration of CSPM tools with additional security modules, such as intrusion detection systems (IDS) [15][18], security orchestration, automation, and response (SOAR) platforms, and log management systems. This oversight fails to understand how well CSPM tools can work within a larger security environment.

In order to address these gaps, a novel and comprehensive methodology is needed that provides a rigorous and realistic assessment of CSPM tools. To fill this void, the Dynamic Cloud

Security Assessment (DCSA) methodology is proposed. The DCSA methodology focuses on real-time monitoring, automated incident response, continuous compliance verification, and the introduction of intentional misconfigurations to develop a robust assessment framework.

Through the use of cutting-edge technologies such as Shuffle, Suricata, and the ELK stack (Elasticsearch, Logstash, and Kibana) to support the technique, the DCSA methodology achieves a near-replication of a real-world cloud environment. In addition to these systems, it integrates collected and processed data to automatically evaluate the efficiency and efficacy of the continuous process. Furthermore, the methodology conducts the continuous compliance check and provides the automated remediation process to verify the ability of CSPM tools in maintaining regulatory compliance and the improvement of the security posture as a whole.

MOTIVATION OF THIS RESEARCH

This research is motivated by the need to improve the security of cloud environments against rapidly increasing cyber threats and the inherent complexity of cloud infrastructures. As organizations migrate their businesses and processes to the cloud, they are confronted with various security challenges that the traditional security solutions have difficulty in adequately mitigating [22]. The CI/CD pipeline along with the enormous resources and multi-tenant architecture of cloud environments demand advanced and automated security solutions. In order to overcome these challenges, a powerful technology called CSPM has emerged [23-25]. CSPM solutions have tools that automate monitoring cloud environments, looking for misconfigurations, potential vulnerabilities and regulatory standard violations. Despite CSPM tools having these promising features, there is limited knowledge about the effectiveness of these tools in the real world or where they are most effective. These reasons are why this experiment was conducted, to find an optimal routine for configuring CSPM tools, to evaluate the tools effectiveness based off these configurations, and where CSPM tools are most effective [26-27].

The difficulty of managing security configurations grows as cloud environments become more involved and larger. Manual attention doesn't suffice, and automated tools are necessary for organizations to maintain a secure posture [28]. Evaluating the performance of CSPM tools in accommodating the dynamic and large-scale nature of modern cloud infrastructures is crucial to ensuring a strong security posture. There is a high number of securitymisconfigurations.Misconfigurations continue to be a major contributing factor for security incidents in the cloud. This often leads to data breaches and unauthorized access [29]. Common issues such as open ports on networks, insecure storage permissions, and weak IAM (Identity and Access Management) policies are widespread [30-31]. We need to evaluate how efficiently and timely CSPM (Cloud Security Posture Management) tools can identify and correct these misconfigurations in a real-time sense thereby closing the door to a security breach.

Requirements for Regulatory Compliance: Adhering to several regulations like HIPAA, GDPR, and PCI-DSS is essential for businesses in regulated industries. However, guaranteeing that you remain compliant with these regulations in the ever-changing cloud environment all the

time is hard enough. CSPM tools, in addition to scoring security gaps, must enforce rules and produce detailed auditable documentation. Assessing the capacity of CSPM tools to maintain regulatory compliance is your primary responsibility to make sure you won't suffer regulatory penalties or litigation.

Integrating and Automating Security Tools: To adequately manage cloud security, different security tools and processes must effortlessly intertwine. Other elements, such as intrusion detection systems (IDS), security orchestration, automation, and response (SOAR) platforms, and log management systems, must work in harmony with CSPM tools. Fully understanding how well CSPM tools connect with these components and automate security workflows is vital for the full attainment of total cloud security. One of the main reasons why it is difficult to evaluate security products is the absence of standardized methodologies for evaluation. The current methods for evaluating CSPM tools are often non-standardized and do not sufficiently replicate the dynamic nature of the cloud environment, leading to a partial understanding of how these tools perform. It is of urgent importance to innovate and construct a comprehensive evaluation process that effectively simulates real-world cloud scenarios, which includes continuous monitoring, compliance validation and auto-remediation.This research aims to address these motivations by proposing Dynamic Cloud Security Assessment (DCSA) methodology, a strong framework for assessing CSPM tools in realistic cloud environments. By employing advanced technologies such as Shuffle (a SOAR tool), Suricata (an open-source network threat detection engine), and the ELK stack (Elasticsearch, Logstash, and Kibana), DCSA methodology creates an environment simulating the real-world cloud deployments very closely. Through this approach, DCSA methodology can ensure a rigorous evaluation of CSPM tools' capabilities in detecting and mitigating security threats, maintaining compliance, and integrating other security components.Ultimately, this research seeks to equip organizations with the intelligence and tools to strengthen their cloud security posture. It is by being cognizant of the strengths and limitations of CSPM solutions that organizations may select and optimize their cloud security strategies, thereby securing their assets and operations in the face of an ever more intricate and adversarial cybersecurity ecosystem.

The objective of this research is to create a realistic cloud environment that is ideal for running state-of-the-art CSPM tools. We need to artificially inject most common misconfigurations and threats so we can interpret how accurate and effective CSPM tools are. On top of that, we will include continuous compliance checks and automated remediation to validate CSPM tools are actually meeting the security and compliance standards.

Insights acquired from this research will allow the DCSA to better generate risk profiles of cloud service providers (CSPs) and comparative cyber security performance metrics of CSPs. Additionally, by leveraging privacy policy elements and CSP control implementations, the DCSA risk scoring algorithm will be modified to include levels of risk associated with data owners (consumers). As a result, the DCSA will be able to provide CSPs with measurable data points that

can be used to adjust their degree of cyber security alignment and cloud service delivery capabilities.

CONTRIBUTION IN THIS PAPER

- This paper presents DSCA, an original framework developed to evaluate CSPM in a real cloud system. DCSA introduces a holistic assessment approach, which covers real-time monitoring, continuous compliance verification and automated incident response. The novelty of the DCSA methodology lies in the integrated system of real-time CSPM tools evaluation, which provides a reliable quantifiable assessment of the effectiveness of CSPM tools, as well as in providing a testbed for CSPM benchmarking.
- Leveraging advanced technologies such as Shuffle, Suricata and ELK stack (Elasticsearch, Logstash, and Kibana), the research creates an automated and integrated evaluation environment. By integrating processes, it enables efficient data flow, immediate threat detection, and high analysis capabilities. Thus enabling a more accurate, more relevant assessment.
- By simulating dynamic operational changes and introducing intentional misconfigurations, the authors create an authentic testing environment that resembles real-world cloud deployments. This methodology allows the evaluators to fully assess the capability of the CSPM tools with respect to detecting and remedying the common security risks, and further ensure their practical applicability.
- Elaboration of assessment metrics plays a crucial role for the effectiveness of the proposed automated tool and represents the technical merit of the dissertation. The detection accuracy, response time, resource impact, and compliance enforcement are established to comprehensively evaluate the performance of the CSPM tools. These metrics together provide a panoramic view of the CSPM tools' performance, enabling organizations to understand the strengths and limitations of the CSPM tools at various aspects.

The organization of the paper is as follows: Section II constitutes a detailed examination of current scholarship on cloud security. It investigates the problems that traditional security measures face when applied to the cloud and the way in which new shared responsibility models are starting to resolve these issues. The core contribution of this research, the DCSA methodology, is introduced in Section III. There, we explain its technical depth and components and emphasize the integration of advanced technologies such as the Shuffle algorithm, Suricata, and the ELK stack. We also describe DCSA's real-time monitoring, continuous compliance verification, and automated incident response.In Section IV, several experiments are carried out. The first part of this section applies the DCSA process to carry out cloud security and privacy monitoring in a test environment. This includes the monitoring of real-time events, the accuracy of which will later be measured against CSPM tools. Finally, the paper ends in Section V, which provides a summary of the overall contribution of the work and a discussion of the implications and future research directions.

II. LITERATURE SURVEY

Cloud computing is one of the most successful technologies in this era. It is successful because of its many benefits like flexibility, cost-effectiveness, and the deployment ease etc. Among the many benefits mentioned above, security is undoubtedly the biggest concern facing Cloud computing. This is because Cloud-specific attacks which are not existent in the classic environment and many existing non Cloud-attacks are magnifying in Cloud environment. Every year it is observed that there is a significant rise in threats in the cloud environment and the new tools and techniques invented by threat actors. Any threat in the cloud environment can cause a significant service disruption. The major obstacle in the utilization of the cloud is cloud security, especially for the organizations dealing with the sensitive data. How to cope with these threats is our biggest challenge for different organizations. In order to remain ahead of these threats, providers have implemented different kinds of solutions. A proactive knowledge of safety threats can fix from environment to cloud grounds for cloud consumers. In this research discusses about security trends of cloud computing infrastructure and explains about cloud computing and its advantages. In addition includes security threats, impact of security threats, and an analysis of best practices and tools available to counter these threats. Also, this is support with a survey which enables to identify latest trends it question with active cloud users and professionals [5].

Cloud computing allows multi users and organizations to exchange, store, and retrieve data at any moment and from any place. Securing the cloud-based infrastructure has significant challenges due to a lack of change management and misconfigurations, as well as different techniques and policies with shortcomings from multiple providers. Because of the existence of privacy and sensitive data, protection is a crucial fraction of cloud computing. Protecting the sensitive and crucial data transferred by multiple companies and users in the cloud is significant. The nervousness of the cloud's secrecy is appreciated.

This research analyses information security, performance, and management issues in cloud computing. It presents the cloud security performance and management paradigm that includes different factors of cloud computing, like security, performance, and management. The evolution of the proposed Cloud Security Posture Management (CSPM) is also discussed in this paper. The CSPM model outlines factors and levels, and data management and time performance are discussed during the implementation phase of this research project [4].

As multi-cloud environments become more widespread, so does the need for CSPM. The emphasis is now on not just visualizing and monitoring security postures, but also automating tasks with minimum disruption. NIST and MITRE Corporation have put in tremendous effort to collect, categorize and publish Vulnerability Incidents as CVE (Common Vulnerabilities and Exposures) datasets. They also publish CWE (Common Weakness Enumerations) data on a year after year basis, strengthening Vulnerability Classification by including new Weakness Enumerations.

In real-time contexts such as CSPM, the use of fast-turnaround intelligence from the wealth of information readily available in the CVE/CWE advisories database requires vulnerability

classifiers to respond to the real-time signals/alerts/poses. Although many research efforts exploit the databases of CWE/CVE for vulnerability classification these methods do not provide a single method that uses real-time alerts/signals as the input to the classifier.

The research paper by [3] included here leverages the CVE and CWE databases for classifying cloud error logs and identifying vulnerability in real-time. Cloud error logs are real-time indicators of the system health, and classifying vulnerability based on cloud error logs can greatly help automate CSPM.

The framework both maps cloud error logs to vulnerability classes and calculates a CVS score (Common Vulnerabilities Severity Score) on every error log that suggests the severity of threats, thus providing cardinal information for the subsequent CSPM. To establish ML models that get trained on Cloud error logs as well as CVE explanations, Deep Learning techniques adorned with CNN, LSTM, and Transformers are employed by this framework. Cloud migration has been seen in the recent days in various companies (AWS, GCP, and Azure). Companies prefer cloud infrastructure over and above on premise servers, because of its easy setup, scalable nature, cheap cost, and very limited maintenance in compared to on premise servers against existing business requirements. The problem of Cloud security settings from misconfigurations on cloud resources when shared, mistakes can arise for the violation of a compliance. This work addresses the problem related to cloud security settings when violate the compliance rules from misconfigurations on cloud resources when shared. Their work adds new rules to improve the effectiveness of the organization as well as to protect the environment in cloud by implementing new rules by using CSPM tool (Scout suite) [1].

Dickinson *et al*.,(2021) presents a federated resource allocation scheme driven by joint performance and security for data-intensive scientific applications. Because of no standardized formalization method, considering end–to–end security requirements across multiple domains is often realized as an afterthought, leading to inter-conflicts between application security and performance requirements caused by diverse domain resource and security policies. In response, SSpecs for Data-Intensive Application Security Specifications (DSA-Spec) is defined and characterized, an alignment technique inspired by Portunes Algebra is described to homogenize domain resource policies (RSpecs) along the application's workflow lifecycle stages and beyond. Based on this formalization and alignment, we propose a near–optimal cost–aware joint QSpecs-SSpecs-driven, RSpecs-compliant resource allocation algorithm for multi-cloud computing resource domain/location selection and network path selection. This scheme is implemented by a framework called "OnTimeURB" and validated in a multi-cloud environment by exemplary data-intensive application workflows involving Distributed Computing and Remote Instrumentation use cases with different performance and security demands [2].

Awaysheh et al. [6] implemented Big Data (BD) operations in cloud deployment architectures (CDAs) where they enormously scale, incorporate flexibility and low-cost potentials in Virtual Machine (VM) features. In CDAs, the cloud service provider (CSP) accepted the

responsibility of managing and maintaining the infrastructure for BD operations. Nevertheless, this architecture means that data are no longer directly controlled by the user. Therefore, traditional models of the physical control of artifacts are no longer applicable in CDAs. Coming up with a complete security strategy would be difficult, except on the basis of an informative up front-analysis that certifies a practical secure setup, and addresses area-specific susceptibilities [7]. A new pioneering security-by-design framework for BD frameworks' deployment over cloud computing (BigCloud) is presented in this article. The presented framework relies on a systematic security analysis methodology and a full automated security assessment framework that aid in architecting a meticulous secured design for BD frameworks deployment in the cloud. The framework has facilitated the mapping of the BigCloud security domain knowledge to best practices in the design phase. The validation of the proposed framework has been carried out by implementing an Apache Hadoop stack use case. The findings of the study demonstrate its effectiveness in increasing the security aspects awareness and reducing the security design time. The strengths and limitations of the proposed framework have been further evaluated, and the main existing and open challenges in the BigCloud-related field have been presented.

III. DYNAMIC CLOUD SECURITY ASSESSMENTS (DCSA)

Dynamic Cloud Security Assessment (DCSA) methodology was developed to evaluate the efficiency in maintaining robust security configurations, vulnerability identification, and best practices in modern rapid-deployment cloud environments.

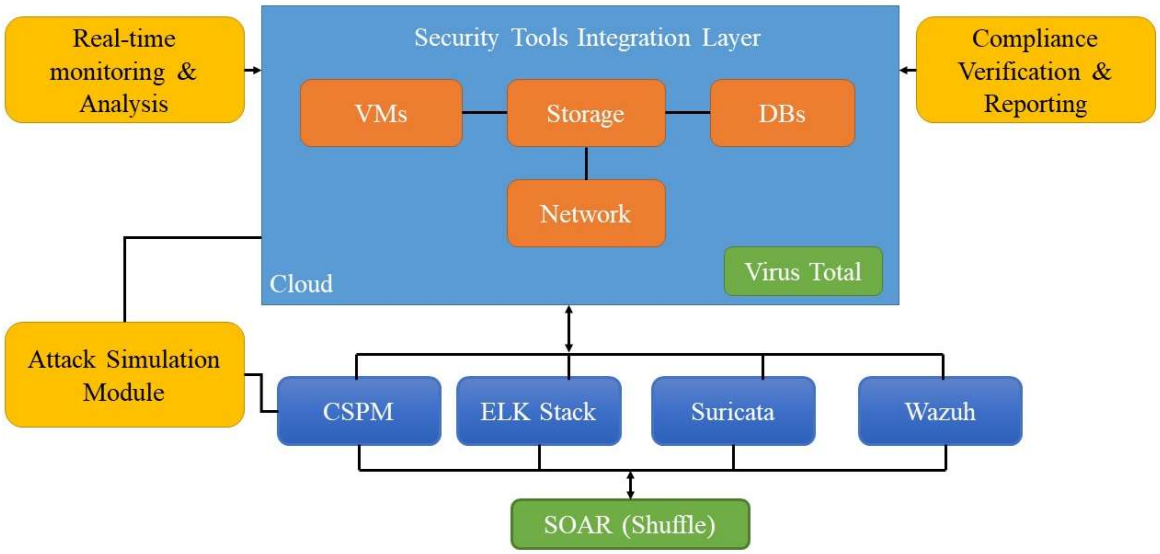

Figure.1. Architecture of DSCA

It does so by applying a variety of real-time, real-world experiments and actions to simulate a "diverse and dynamic" cloud service environment. DCSA can offer a comprehensive understanding of how a Cloud Security Posture Management (CSPM) tool actually performs in a live, multi-function cloud computing environment.

COMPONENTS OF DCSA

A. Environmental Setup

Cloud security assessment is an essential part of the secure setup of cloud computing. It starts with the selection of the cloud platform that the enterprise is going to work with. This choice is an important one; it affects every aspect of an enterprise that has any part of itself in the cloud. Once the decision has been made, and the cloud has been deployed, the cloud environment must be properly implemented. This is the "getting started" part of the cloud security assessment. What must be done here is straightforward (although how to do it might not be quite so straightforward). The cloud must be configured to use best practices so that the chance of a breach is minimized.

B. Real-time Monitoring and Analysis

The Dynamic Cloud Security Assessment (DCSA) methodology relies on real-time monitoring and analysis as core components. This phase is pivotal when evaluating how effectively a Cloud Security Posture Management (CSPM) tool operates in a continuously effective manner. The set-up of a strong monitoring framework is done in this phase to seize and analyze real-time data on the security posture, configurations changes, and compliance status in cloud environments.

Continuous Monitoring

The continuous monitoring framework was built to deliver ongoing visibility into the cloud environment. This is done by integrating CSPM tools with the cloud platforms (AWS, Azure, and Google Cloud) to collect and analyze real-time data. A typical monitoring setup looks as below,

Cloud Resource Inventory: CSPM tools continuously discover cloud resources such as virtual machines, storage buckets, databases, network components, etc. This inventory gives a complete overview of the assets within the cloud environment.

Configuration State Monitoring: Resources in the configuration states are continuously monitored in real-time. These states will cover things like security group settings, encryption settings, IAM roles, and much more. Any changes to these states will be instantly identified and observed.

Event Logging and Analysis: Every important event such as logging in, changing a policy, accessing data, etc., will be logged. The logs will then be further analyzed in order to detect behaviors that could be linked to a security threat or policy violation.

C. Automated Alerts and Reports

Generating automated alerts and detailed reports is a core requirement of real-time monitoring. CSPM solutions are configured to trigger alerts based on pre-defined security rules and policies. These alerts are designed to keep administrators informed of potential security problems as soon as they occur.Alerts that are generated when variations from security baseline

standards set by service account (open/misconfigured network ports, unencrypted storage, overly open access controls) are found by CSPM (cloud security posture management) tools.

Detecting Anomalies

CSPM tools leverage machine learning and behavior analysis to discover abnormal activities that potentially signify security incidents, like multiple failed login attempts or accessing sensitive data from an unknown IP address. Also, non-compliant actions are also identified, such as not complying with GDPR, HIPAA, or PCI-DSS requirements.The alerts come with extensive reports that give full details of the problems, including what resources are affected, what went wrong or what the threat is, and what steps to take to recover. These reports are crucial to help the admins rapidly comprehend and repair the vulnerabilities.

Real-time Data Collection and Analysis

CSPM tools depend a lot on their ability to aggregate and normalize data in real-time, through activities such as: Telemetry Data where User specifies the telemetry data sources, from amongst various cloud resources, such as, Performance metrics, access logs, configuration data etc. Data from these sources is continuously streamed to the CSPM platform.

Correlation and Contextualization: User sets the correlation policies in terms of what events within the specified data sources may have to be correlated and/or how to provide contextual understanding of a security event. For instance, data from an access log would be correlated with an event stream coming from a misconfigured cloud resource to determine if the misconfiguration is being exploited.

Trend Analysis: User sets the trend policies and visualizations, which help analyze the trends and patterns emerging from the specified data sources over time. Examples of such policies could be continuous misconfigurations of a particular type of resource and/or making sure that cloud resources should only be accessed from specific IP addresses, etc.

D. Evaluation of CSPM Tools

DCSA's other data pointing and analysis real time facet aims to evaluate the fidelity and the effectiveness of CSPM tools. It focuses on several key dimensions namely i) Detection Accuracy: The tools ability to accurately detect security issues is measured. Precision (that is, minimizing false positives) and recall (maximizing real issue detection) are key metrics. ii) Response Time: how quickly do the CSPM tools generate alerts and reports? When a security issue is detected. Fast response time is a key to attempt at threat mitigation before it causes severe damage. iii) Remediation Support: Are the CSPM tools providing good remediation guidance? A decent tool in this space not only identifies an issue, but also tells the user how to fix the issue.iv) Resource Impact: What is the impact of CSPM tools on cloud environment resource utilization? Resource consumption of monitored instances should not be (unreasonably) degraded by the tools.

Operational Integration

Lastly, an effective integration with an organization's operational workflows is needed for real-time monitoring and analysis. CSPM tools must be integrated with incident response processes to make sure alerts result in timely and effective remediation actions. Intuitive dashboards with high UI/UX for Administrators to monitor the security posture of the cloud environment. This helps the admins to dissect the issues. Also these Insights gained from real-time monitoring drive continuous improvement in security policies and practices. This includes updating configuration baselines, refining alert rules, and enhancing compliance checks.

E. Evaluation Metrics

Within the methodology of Dynamic Cloud Security Assessment (DCSA), evaluation metrics have a vital role to play. These systematic approaches evaluate the effectiveness and efficiency of Cloud Security Posture Management (CSPM) tools. Evaluation metrics perform a quantitative and qualitative evaluation of the device's ability to describe, act upon and eliminate security problems within cloud environments. The following provides a details assessment of the principal evaluation metrics used in DCSA.

Detection Accuracy

Detection accuracy is a basic metric that evaluates to what extent CSPM tools properly detect vulnerabilities and security misconfigurations. It refers to two prime elements:

Precision measures the part of the security issues which are appropriately recognized out of the entire issues which the CSPM tools have surged for. A high precision sense the tool generates less in count false positives thus setting an assurance on meaningful and serviceable alerts. For example, if a CSPM tool surges 100 security issues flags, among this 90 are vulnerabilities and only 10 are the cases of rational, thus the precision will be 90%.

Recall: This metric quantifies the rate at which security issues are detected by the CSPM tools in a test. It means how many of the true security issues can be found out of all, it ensures that the developed CSPM tool is wide and deep enough to cover all the possible vulnerabilities. If there are 100 security issues in the cloud environment, and the CSPM tool can find 90 out of them, the recall will be around 90%. For analyzing the effectiveness of CSPM, assessing the specificity and sensitivity is vital, because the approach maintains the equilibrium between lowering any superfluous alerts and increasing the overall vulnerability coverage.

Remediation Effectiveness

There are a few criteria by which you can evaluate the effectiveness of the remediations that are suggested or proposed by CSPM tools. First of all, you can look for the clarity of the recommendations. This has to do with whether, in fact, the CSPM tool provides clear, understandable and actionable steps for the administrator, for you, to fix the problem. Some of these tools, or some of the assessments have very little guidance there and some have very detailed advice about exactly what settings should be changed in what components of what service in what

cloud in what way, in order to fix the particular problem. A second interesting characteristic you could look for is automated remediation. Some of these CSPM tools have the capability to automatically remediate or fix well defined, well understood, certain classes of misconfigurations or vulnerabilities. Again, this is a lovely feature in the sense that 99% of the time if you like, it's right, it's done. And at 1% of the time someone has to look at what the tool has done and either say, thank you, that was indeed what I would have recommended, or, I'm sorry there's a change here or there because my application is different from whatever it is the tool assumed or that's actually not what I want to do here or blah, blah, blah, or even worse, it's simply not correct, which can happen.Another interesting criterion is simply the success rate of these remediation. So, somebody runs a CSPM tool assessment, it's identified a certain number of issues, we can then do an objective experiment and measure exactly the number and proportion of those issues that are successfully resolved by following the tool's recommendations. That's an interesting metric because it goes backwards and gives me some insight into exactly how much any of these tools are going to improve my security posture if I actually use them.

Performance Impact

When measuring the performance impact of CSPM tools, one of the key aspects to examiner is how the operational aspects of the CSPM tools affect the overall performance and resource utilization of the cloud environment. Analyzing the overhead of Resource Utilization that CSPM tools place on cloud resources such as CPU, Memory, and Network Bandwidth is also very crucial. Consequently, adequately designed CSPM tools should make efforts to minimize the resource overhead they cause to avoid causing degradation in the performance of monitored resources. Additionally, We evaluate any otherwise totally avoidable delays that CSPM tools introduce when they process and respond to configuration changes as well as security events. Real-time monitoring, something CSPM tools must accomplish if they are to be considered effective, must be efficient to ensure timely identification then fixes to any security issue that might arise from these cloud environments.

F. Compliance Verification

The DCSA approach relies on Compliance Verification to determine how well Cloud Security Posture Management (CSPM) tools help organizations maintain and enforce compliance with a variety of industry standards and regulatory requirements. In verifying compliance, CSPM tools have a key role to play in that these solutions continually enforce security policies and standards. These policies commonly originate from compliance frameworks such as GDPR, HIPAA, PCI-DSS, as well as internal organizational security policies. These tools continuously inspect the cloud environment to ensure that all configurations and operations follow these policies that have already been defined. This includes: Policy checks are automated: CSPM tools are set up to perform automated checks against a complete set of compliance requirements. These are executed continuously or at planned intervals to guarantee ongoing compliance. For example, a CSPM tool may check that all data storage is encrypted, enforce that multi-factor authentication is used, and that access controls adhere to the principle of least privilege.

Alerts for Non-compliance in Real-time

When the CSPM tools notice any deviation from the enshrined policies, they shoot off an alert. These alerts notify the administrators of the exact non-compliance, affected resources, and the risks of non-compliance. This real-time feedback mechanism makes sure that the non-compliance can be fixed right away, giving a better chance to lower the vulnerability window.

To conduct successful compliance verification, a range of logging and reporting capabilities is required. CSPM tools will maintain exhaustive, access-restricted audit logs of all security-related events and configuration modifications within the cloud infrastructure. These audit logs are vital for:Tools Like (CSPM Tools) Maintain a Continuous Audit Trail of All Activities and Changes in the Cloud Environment. This Includes User Actions, Configuration Modifications, Access Attempts, Policy Enforcement Actions, Etc. Regular reports on compliance are automatically issued by CSPM tools. These reports depict the present status of the cloud environment in terms of compliance. They normally contain data on the observation of compliance regulations, violations discovered, actions took for remediation, and changing patterns over time. For internal review and external audits, it is critical to have compliance reports so that the organization's resolution to follow compliance is obvious. Assessing compliance verification includes trying to determine how well CSPM tools help support constant compliance with sector standards and regulations. It comprises of the following: Policy Enforcement: This refers to the ability of CSPM tools to consistently impose industry and security policies along with compliance requirements, including but not limited, to GDPR, HIPAA and PCI-DSS. Efficient tools automatically ensure regulatory compliance and notify admins about compliance policy deviations.

Audit Logs and Reporting: Refers to the comprehensiveness along with the understandability of security audit logs along with compliance reports(customized/built-in) for CSPM tools. Audit logs capture evidence that security events(permissions to access cloud API's, AWS service requests, etc.) have occurred in the environment and what actions are being done when. These logs are pivotal to addressing cloud security risks, facilitating audits and regulatory reviews against companies or other relational safeguards.

Frequency of Compliance Checks: provides the assurance of compliance by silhouette occurrences of performance checks on standards by CSPM tools which helps maintain the posture and acknowledging of change in Cloud-directive atmospheres.

Compliance Frameworks and Standards

The tools included in this category are designed to support multiple compliance frameworks and standards, which enables organizations to meet multiple regulatory requirements. The Key frameworks include: GDPR where the personal data is processed and stored in compliance with GDPR requirements such as data minimization, purpose limitation, and ensuring data subject rights. HIPAA which helps in protecting health information by enforcing strict access controls, encrypting data both at rest and in transit, and monitoring and auditing access. PCI-DSS

which helps in protecting payment card information through the use of stringent access controls, data encryption, and regular monitoring and auditing.

Real-time Compliance Checks

Maintaining continuous compliance with regulatory standards in the cloud requires performing real-time compliance checks. CSPM solutions achieve this using a variety of techniques:

Baselines for Configuration Management : Establishing configuration baselines that define the desired state of compliance. CSPM solutions constantly compare the current state of cloud resources to these baselines, looking for deviations.

Anomaly Detection : Employing machine learning and enhanced analytics to spot patterns and anomalies that suggest violations of compliance. For example, strange access patterns or sudden changes in configurations might indicate a compliance violation and generate a compliant alert.

Act Remediating : In the event of a compliance violation, CSPM solutions do not only notify administrators what has occurred. The solutions also allow them to fix the issue and provide the steps they need to remediate. These measures might entail returning configurations to compliant states, imposing additional access controls, or triggering the activated scripts to recover.

Integrating Compliance checks with Incident Response

Compliance verification engages closely with an organization's incident response processes. When compliance violations are detected by CSPM tools, the following general steps are typically taken:

Alert Routing

Compliance alerts are channelled to the relevant incident response teams. These alerts generally provide specific information about the violation(s), the resources affected, and potential impact.

Incident Management

The incident response teams will use the information supplied by CSPM tools to help ascertain the severity of the compliance violation and dictate subsequent response actions. These actions might involve immediate remediation, further inquiry, and ultimately, escalation to superiors.

Post-incident Review

After compliance incidents have been resolved, a formal post-incident review is performed to analyze the root cause, how effectively the response to the incident was, and where there is room to advance. The CSPM tools provide the data and insights essential to these reviews.

G. Ongoing Improvement and Adaptation

The requirements for compliance as well as policies pertaining to security are not static, but they are always changing as new regulations, threats, and organizational shifts occur. Anything that continuously supports the malleability and improvement is the CSPM tool and it includes: Policy Updates where the said compliance policies and benchmarks are updated regularly and that includes the varied CSPM tools. This step must be taken for the variation of various regulatory requirements and best practices.

CONTINUOUS TRAINING AND SUPPORT

The CSPM vendors would also double down by providing continuous training as well as support which would help the organizations to use their respective tools properly. With this, they can also be kept well abreast of the new compliance requirements at all times. This further includes the documentation, webinars, and the customer support services.

A. Feedback Loops

The feedback from not just any compliance audits but security assessments and real-time monitoring also proves to be quintessential in the improvement of their compliance posture. While that's where all various CSPM tools also serve as they provide the businesses with actionable insights along with the recommendations grounded in the trends and patterns that have been observed.

POLICY ENFORCEMENT

Operational integration metrics evaluate the extent to which CSPM tools combine with the business' current operational workflows and security practices. This encompasses:

A. Incident Response Integration

The usefulness of integrating CSPM tools with incident response processes. This is determined by how alerts from CSPM tools are directed to the relevant response teams and how such teams utilize the tools' recommendations in their workflows.

B. User Interface and Dashboards

The ease and clarity of the CSPM tools' dashboards and interfaces. Effective software should present simple, easily-interpreted insights via user-centric dashboards, so that administrators can quickly assess the security posture and investigate any issues further.

C. Training and Support

The degree of assistance and training provided by the CSPM tool vendors. This factor takes into account the availability of documentation, training sessions, and customer support options to assist organisations in using and integrating the tools into their security operations.

IV. EXPERIMENTAL RESULTS

EXPERIMENTAL SETUP

The experimental configuration for the Dynamic Cloud Security Assessment (DCSA) has been designed to comprehensively evaluate the capabilities of Cloud Security Posture Management (CSPM) tools in a controlled and automated environment. This configuration makes use of Shuffle – Security Orchestration, Automation, and Response (SOAR), integrated with Suricata and the ELK stack for intrusion and anomaly detection.

To coordinate and automate the various pieces of the experimental set up, we use Shuffle. It allows the different security tools to be seamlessly integrated and communicate with each other thus, making it possible to collect, process and respond to the data efficiently. Shuffle automates the workflows that handle the flow of data between Suricata, the ELK stack and the CSPM tools, including packeting network traffic data, logging the data and analyzing it as well as generating the alerts and reports. Furthermore, it automates the IR actions, basically, when an event or alarm is recognized, Shuffle will take predefined IR actions according to the rules and conditions, to have the appropriate actions taken or to the right instances alerted when the anomaly/intrusion occurs in the network. Moreover, Shuffle provides a facility to let Suricata, ELK and CSPM tools communicate with each other by integrations with a variety of APIs and services.

To observe suspicious behavior in network traffic, Suricata is a network threat detection engine that is customizable. It enforces real-time intrusion detection (IDS) and intrusion prevention (IPS), network security monitoring (NSM), and network visibility with Suricata configured. Our Suricata configuration contains an extensive set of IDS/IPS rules to identify various threats, which are continually revised to represent the most recent threat intelligence. When implemented within the cloud network, Suricata intercepts traffic in real-time which enables it to either parry or warn any threats it finds. Data indicating a detection by Suricata is formatted to the ELK stack for examination and representation.

The ELK stack (Elasticsearch, Logstash, and Kibana) is used to process and analyze the log data generated by Suricata, as well as other components of the cloud architecture. The first phase of the process is the collection and process of the Suricata log data using Logstash. Logstash collects log data from Suricata as well as other sources. Logstash filters, parses, and enhances the log data before forwarding it to Elasticsearch which is the third phase. Filters include the normalization of the structured log data formats, selection of interesting fields, and introduction of derived transformations. Elasticsearch is the storage mechanism for the log data. The indexed and searchable store is optimized for fast querying. The platform provides superior efficiency in the storage and retrieval of big volumes of log data. Kibana stores the visual and interactive platform through which the logs can be accessed. The Kibana dashboard provides configurable, real-time analysis, and views of trends and metrics along with Suricata alerts as visual aids for the monitoring of network security incidents.

A typical production-like arrangement is shown in this assessment's cloud setting. Virtual machines, storage buckets, databases, and network components, among other usual cloud resources and services, have all been set into create a cloud environment. The initial security settings for all cloud resources are created to help with detect misconfigurations and protected from breaking security rules. From our research on the cloud in terms of CSPM-tools there are some non-conformance that we introduce intentionally. For instance, open network ports, unsecured storage permissions which were given and weak IAM policiesush.

The setup incorporates CSPM tools which facilitate in real time monitoring and assessment of the security positioning of the cloud environment to constantly scan and report misconfigurations, vulnerabilities and compliance issues. The integration encompasses CSPM tools configured to collect data from cloud environment, Suricata, ELK stack, which encapsulates configuration states, security events, and network traffic logs. Within CSPM tools security and compliance policies are enforced to measure the security positioning and to generate alerts in case of any violations observed. Respective CSPM tools are also afforded functionalities to perform automatic remediation of few misconfigurations and vulnerabilities based on predefined rules and conditions.

The last part of the experiment setup is analyzing and evaluating the CSPM tools' performance. The analysis is done by using different metrics such as detection accuracy, which evaluates the CSPM tools' precision and recall while identifying security issues and compliance violations; response time, which evaluates the time the CSPM tools take to detect issues and generate alerts or remediation actions with various number of issues; resource impact, which measures the CSPM tools' impact on the cloud environment's performance including CPU, memory, and network utilization; and compliance verification, which respects to the CSPM tools' ability to continuously enforce the compliance with regulatory standards and internal policies.

ATTACK SIMULATIONS

A. Intentional Misconfiguration

Intentional misconfigurations are the integral part of the DCSAas it assesses the ability of CSPM tools to identify and resolve real-world security problems. Certain misconfigurations of security are purposefully inserted, only one of which is open network ports, insecure storage privileges, and bad identification and access management (IAM) at times. They are carefully managed to reliably represent the fundamental security lapses that we may consider in cloud environments. Moreover, configurations are regularly updated the same way operational situation and cloud situations in the real world do not seem to be quite constant. It safeguards that the evaluation is nowadays very real and tests the capacity of CSPM technologies for ongoing security management.

First of all, we deliberately introduce common security misconfigurations to the cloud environment. These security misconfigurations are chosen according to their prevalence and potential impact in the real world. Here are some examples:

B. Open Network Ports

Opening of unnecessary network ports can lead to unauthorized access and attacks against the cloud environment. By introducing this misconfiguration, we assess if CSPM tools can detect open ports and alert administrators timely.

C. Insecure Storage Permissions

Setting of excessively permissive access controls on the storage services can result in unauthorized data access and potential data breaches. We assess if CSPM tools can identify storage resources with insecure permissions and suggest corrective actions.

D. Weak Identity and Access Management (IAM) Policies

Weak IAM policies such as granting excessive privileges or neglecting to enforce Multi-Factor Authentication (MFA) pose serious security risks. We introduce these vulnerabilities to see if the CSPM tools can red flag and fix weak IAM configurations.

E. Controlled Misconfigurations

These configurations have been very carefully done in order to reflect real-world security mistakes inside fair frameworks of the cloud. By producing these exposure areas deliberately, we're generating the foundation of testing the detection algorithms of the CSPMs. Control is the hallmark of these tests and shows the precision of our configurations and correctness our valuation.Aside from being able to verify static misconfigurations, various dynamic changes are propagated over the configurations. That is, the environment is changed to imitate the ongoing operational changes and updates that actually occur in deployed cloud, in real-time. Scaling Resources, such as upscaling or downscaling the number of virtual machines or storage volumes to test the efficiency of CSPM tools with scaling operations.

Updating Software: By deploying updates to applications and operating systems, we will evaluate our tools' effectiveness in monitoring and securing the environment during the patching process.

Modifying Network Configurations: Modifying network routes, firewalls, and security groups to replicate typical administrative operations to analyzerealtime monitoring and response attributes of High Time Cloud Security Configuration (HTCSC) tools.

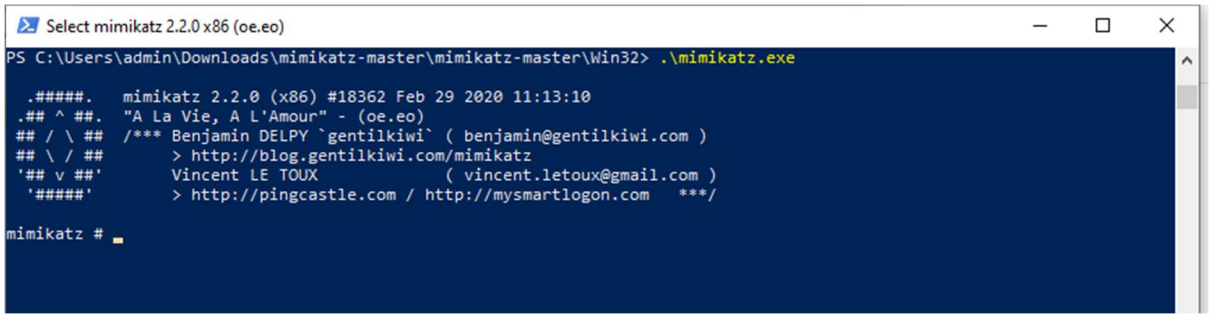

Figure 2. Screenshot of Mimikatzexecution as the part of simulation

In Figure 2, we can see a snapshot of the execution of Mimikatz, as part of a cloud instances security assessment. Mimikatz is one of the most powerful post-exploitation tools out there. It is generally utilised to extract credentials, tokens and other sensitive information from memory. The screenshot above shows Mimikatz executing within the cloud infrastructure. The goal of this specific attacking scenario was to demonstrate the ease by which cloud instances can be attacked for the purpose of credential theft and unauthorized access. By emulating such an attack scenario organizations can ascertain the robustness of their security environment and understand what if any vulnerabilities remain. By understanding our weaknesses we can mitigate, at the very least, the likelihood of unauthorized access and data breaches.

F. Realistic Assessment

The dynamic nature of the provisioning of intentional misconfigurations is ensuring that the testing is realistic and comprehensive. By delivering evolving changes to the CSPM tools, the DCSA methodology is testing the ability of these tools' operationalize and hold the security posture through the introduction of a changing environment. This testing will challenge the CSPM tools to not only identify and flag the initial introduction of those misconfigurations, but to also understand and manage the ongoing changes. Failure to validate this component will indicate that the CSPM tool being evaluated will be unsuccessful in providing continuous security management.

In the end, the introduction of those intentional misconfigurations under the DCSA framework does provide a sufficient testing ground for CSPM tools to prove validity and robustness. The complexities and dynamics of this replication of a real-world cloud environment permit CSPM tools to be measured against a security issue that is present, detectable, manageable, and remediable on a continuous base. This will determine the operational value for the purpose of a secure cloud infrastructure.

In Figure 3, integration between different components in security orchestration, automation, and response (SOAR) automation is illustrated. It is integrated with different security tools such as Cloud Security Posture Management (CSPM), Wazuh, Virustotal, and ELK stack. Using this integration, different components of security seamlessly communicate with each other. By using SOAR automation as central orchestrator, organizations can automate the process of incident response and centralize them across their security infrastructure. There are a numerous repetitive tasks,SOAR automation provides services to automate those redundant tasks, fulfilling requirement. This helps organizations to respond security incidents in real time by managing security in most effectively.

Figure 3. SOAR automation configured to work aligned with the CSPM & Other security tools like Wazuh, Virustotal, ELK etc.

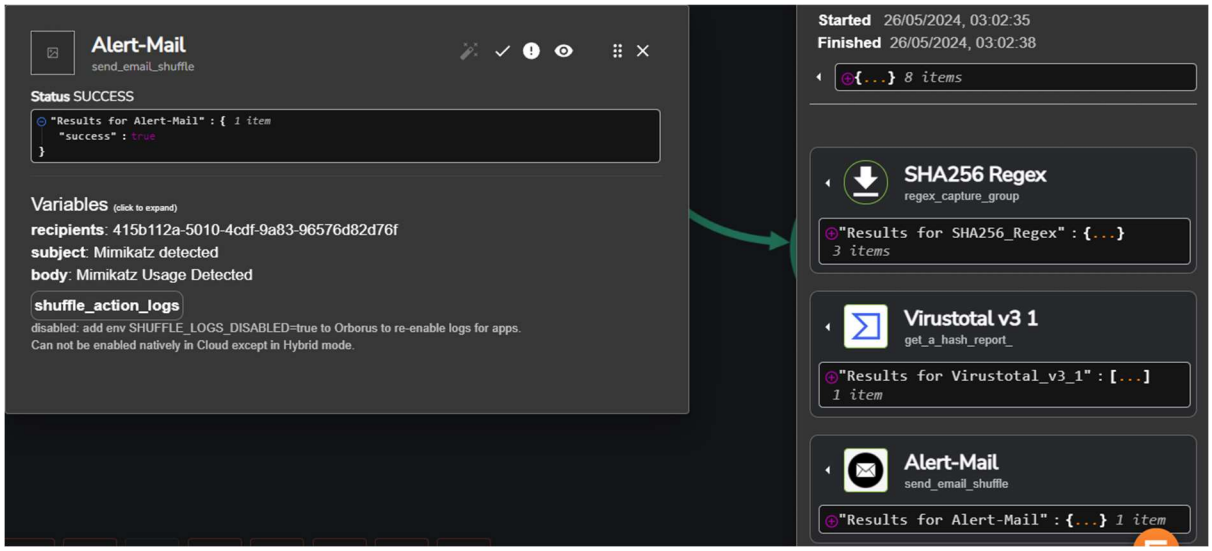

Figure 4. Alert module configuration

The email alert module is one of the most important part of security notification system, which is shown in Figure 4. When the security incident or anomaly occurs, this module is responsible for timely alerting the relevant stakeholders. In the event of any interesting activity, such as security breach or policy violation, the email alert module will generate an alert notification and dispatch it to specific recipients via email. The alert notification includes essential information about the event, such as its nature, severity level, affected resources, and recommended actions to mitigate the effect. By using this email alert module, organization can ensure that the people who

are responsible for the security will be informed of security events as soon as possible. Because of this reason, they can rapidly response and mitigate the security incidents to prevent the attacker to rollout the integrity and confidentiality of systems and data.

V. CONCLUSION

In this paper, we have presented an innovative method for the assessment of Cloud Security Posture Management (CSPM) tools by employing the Dynamic Cloud Security Assessment (DCSA) framework. By overcoming the existing assessment frameworks' limitations, our DCSA framework offers a holistic and pragmatic evaluation on the CSPM tools' efficacy in confining cloud environments. By integrating advanced technologies such as Shuffle, Suricata, and ELK stack, the methodology is capable of achieving real-time monitoring, continuous compliance verification, and automated incident response. Experimental results show that DCSA is practically applicable and effective in simulating real-world cloud scenarios and evaluating the performance of CSPM tools. Additionally, the inclusion of attack simulations, like running Mimikatz, emphasizes the need for preventive security tactics in removing the dangers associated with password pilfering and not allowed admittance. On the whole, this research aids in raising security measures in cloud computing by delivering organizations with a wealth of detailed information about how secure their systems are and how best to pursue a security program to thwart newly emerging dangers.

REFERENCES

[1]. B. Jeya Suriya, B. K. Amarnath, A. R. Raghuraman and C. Arumugam, "Cloud Security: Upgradation in CSPM Configuration Setting," *2024 4th International Conference on Data Engineering and Communication Systems (ICDECS)*, Bangalore, India, 2024, pp. 1-4

[2]. M. Dickinson *et al*., "Multi-Cloud Performance and Security Driven Federated Workflow Management," in *IEEE Transactions on Cloud Computing*, vol. 9, no. 1, pp. 240-257, 1 Jan.-March 2021

[3]. O. Jois, R. G, R. Baisak and S. R. Upadhyaya, "Logs2Vul: Vulnerability Detection from Logs for CSPM," *2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, Bhilai, India, 2024, pp. 1-7

[4]. G. SAWHNEY, G. KAUR and R. Deorari, "CSPM: A secure Cloud Computing Performance Management Model," *2022 International Conference on Cyber Resilience (ICCR)*, Dubai, United Arab Emirates, 2022, pp. 1-5

[5]. D. Ahir and N. Shaikh, "A Systematic Survey on Cloud Security Threats, Impacts and Remediation," *2023 IEEE Engineering Informatics*, Melbourne, Australia, 2023, pp. 1-9

[6]. F. M. Awaysheh, M. N. Aladwan, M. Alazab, S. Alawadi, J. C. Cabaleiro and T. F. Pena, "Security by Design for Big Data Frameworks Over Cloud Computing," in *IEEE Transactions on Engineering Management*, vol. 69, no. 6, pp. 3676-3693, Dec. 2022

[7]. S. An, A. Leung, J. B. Hong, T. Eom and J. S. Park, "Toward Automated Security Analysis and Enforcement for Cloud Computing Using Graphical Models for Security," in *IEEE Access*, vol. 10, pp. 75117-75134, 2022

[8]. S. Majumdar *et al*., "ProSAS: Proactive Security Auditing System for Clouds," in *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 4, pp. 2517-2534, 1 July-Aug. 2022

[9]. Akshay T, S. Sibi Chakkaravarthy , D. Sangeetha, M. Venkata Rathnam, V. Vaidehi,"Role Based Policy to Maintain Privacy of Patient Health Records in Cloud", Journal of Super Computing, Vol.75, Issue 9, June 2019, pp.5866–5881, Springer.

[10]. J. Li, H. Yan and Y. Zhang, "Efficient Identity-Based Provable Multi-Copy Data Possession in Multi-Cloud Storage," in *IEEE Transactions on Cloud Computing*, vol. 10, no. 1, pp. 356-365, 1 Jan.-March 2022

[11]. Dedipyaman Das, S.SibiChakkaravarthy, Suresh Chandra Satapathy, "A Decentralized Open Web Cryptographic Standard", Computers and Electrical Engineering, Elsevier, Vol. 99, 107751, April, 2022.

[12]. K. Muniasamy, R. Chadha, P. Calyam and M. Sethumadhavan, "Analyzing Component Composability of Cloud Security Configurations," in *IEEE Access*, vol. 11, pp. 139935-139951, 2023

[13]. Devi Priya V S, Sibi Chakkaravarthy Sethuraman, "Containerized cloud-based honeypot deception for tracking attackers", Scientific Reports, Nature, 2023.

[14]. J. Zhang, T. Li, Z. Ying and J. Ma, "Trust-Based Secure Multi-Cloud Collaboration Framework in Cloud-Fog-Assisted IoT," in *IEEE Transactions on Cloud Computing*, vol. 11, no. 2, pp. 1546-1561, 1 April-June 2023

[15]. S. Sibi Chakkaravarthy, V. Vaidehi and Steven Walczak, "Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles", Journal of Medical Systems, Vol.44, Article 29, Springer.

[16]. K. K. Singamaneni, G. Muhammad and Z. Ali, "A Novel Multi-Qubit Quantum Key Distribution Ciphertext-Policy Attribute-Based Encryption Model to Improve Cloud Security for Consumers," in *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1092-1101, Feb. 2024

[17]. K. Zhang, Z. Jiang, J. Ning and X. Huang, "Subversion-Resistant and Consistent Attribute-Based Keyword Search for Secure Cloud Storage," in *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1771-1784, 2022.

[18]. Sibi Chakkaravarthy Sethuraman, Devi Priya VS, Tarun Reddi, Mulka Sai Tharun Reddy, Muhammad Khurram Khan, "A Comprehensive Examination of Email Spoofing: Issues and Prospects for Email Security", Computers & Security, Elsevier, vol. 137, 103600, 2023.

[19]. G. Xu, S. Xu, J. Ma, J. Ning and X. Huang, "An Adaptively Secure and Efficient Data Sharing System for Dynamic User Groups in Cloud," in *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 5171-5185, 2023

[20]. S. Sibi Chakkaravarthy, D. Sangeetha and V. Vaidehi,“A Survey on malware analysis and mitigation techniques”, Computer Science Review, Vol. 32, pp 1 - 23, May 2019, Elsevier.

[21]. Q. Wang, Z. Wang and W. Wang, "Research on Secure Cloud Networking Plan Based on Industry-Specific Cloud Platform," in *IEEE Access*, vol. 11, pp. 51848-51860, 2023

[22]. A. Wu, A. Yang, W. Luo and J. Wen, "Enabling Traceable and Verifiable Multi-User Forward Secure Searchable Encryption in Hybrid Cloud," in *IEEE Transactions on Cloud Computing*, vol. 11, no. 2, pp. 1886-1898, 1 April-June 2023

[23]. X. Li, S. Liu, R. Lu, M. K. Khan, K. Gu and X. Zhang, "An Efficient Privacy-Preserving Public Auditing Protocol for Cloud-Based Medical Storage System," in *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 2020-2031, May 2022

[24]. Sibi Chakkaravarthy Sethuraman, Devi Priya, Saraju P Mohanty, “Flow based containerized honeypot approach for network traffic analysis: An empirical study", Computer Science Review, Elsevier, vol. 50, 100600, 2023.

[25]. H. Ma, R. Zhang, S. Sun, Z. Song and G. Tan, "Server-Aided Fine-Grained Access Control Mechanism with Robust Revocation in Cloud Computing," in *IEEE Transactions on Services Computing*, vol. 15, no. 1, pp. 164-173, 1 Jan.-Feb. 2022

[26]. J. Li, J. Ma, Y. Miao, R. Yang, X. Liu and K. -K. R. Choo, "Practical Multi-Keyword Ranked Search With Access Control Over Encrypted Cloud Data," in *IEEE Transactions on Cloud Computing*, vol. 10, no. 3, pp. 2005-2019, 1 July-Sept. 2022

[27]. Devi Priya, Sibi Chakkaravarthy Sethuraman, Muhammad Khurram Khan, “Container Security: Precaution levels, Mitigation Strategies, and Research Perspectives", Computers & Security, Elsevier, vol. 135, 103490, 2023.

[28]. L. Wang, Y. Lin, T. Yao, H. Xiong and K. Liang, "FABRIC: Fast and Secure Unbounded Cross-System Encrypted Data Sharing in Cloud Computing," in *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 6, pp. 5130-5142, Nov.-Dec. 2023

[29]. R. Bi, J. Xiong, Y. Tian, Q. Li and X. Liu, "Edge-Cooperative Privacy-Preserving Object Detection Over Random Point Cloud Shares for Connected Autonomous Vehicles," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 23

[30]. Gopinath M, Sibi Chakkaravarthy Sethuraman, “A comprehensive survey on deep learning based malware detection techniques”, Computer Science Review, Vol. 47, February 2023, Elsevier.

[31]. Sibi Chakkaravarthy Sethuraman, Aditya Mitra, Kuan-Ching Li, Anisha Ghosh, M Gopinath, Nitin Sukhija, "Loki: A Physical Security Key Compatible IoT Based Lock for Protecting Physical Assets", Vol. 10, Pages. 112721-112730, IEEE Access, 2023.