Research on automated security incident management in public cloud environments*

Oksana Sapsai[1,†], Yevhenii Martseniuk[1,†], Andrii Partyka[1,†] and Oleh Harasymchuk[1,*,†]

[1] Lviv Polytechnic National University, 12 Stepana Bandery str., 79000 Lviv, Ukraine

Abstract

Modern organizations are increasingly integrating public cloud platforms such as AWS, Azure, and Google Cloud Platform into their infrastructure to enhance flexibility and scalability. However, multi-cloud environments introduce new cybersecurity challenges. The human factor and careless use of access parameters to cloud resources can lead to serious threats. In particular, if an attacker gains access to authorization keys, they can not only take control of existing resources but also create new ones for their own purposes, such as carrying out attacks, distributing malware, or mining cryptocurrencies. Such incidents can quickly lead to financial losses, undermine user trust, and impact the stability of critical services. This study examines the use of Splunk SOAR (Security Orchestration, Automation, and Response) as a tool for the automatic detection, analysis, and response to threats in public cloud environments. The primary focus is on integrating Splunk SOAR with cloud provider APIs for dynamically blocking compromised resources and implementing detailed playbooks that allow for isolating threats at the level of individual components (virtual machines, network policies, user accounts). The research also explores the integration of Splunk for anomaly detection through Palo Alto Prisma as a comprehensive anomaly scanner, the use of HashiCorp Vault for credential protection, the implementation of a quarantine mode for isolating compromised resources, and improving incident response processes. The study results show that automating security processes with Splunk SOAR significantly reduces response time, minimizes the impact of the human factor, and lowers the risk of cloud infrastructure compromise. The proposed approach enhances an organization's resilience to threats in multi-cloud environments, ensuring an optimal balance between security, availability, and operational efficiency. Keywords—component: Splunk SOAR, public cloud environments, automated incident response, resource blocking, multi-cloud infrastructure, human factor, anomaly monitoring, cloud provider APIs.

Keywords

cloud security, automation, DevOps, SOAR, remediation, incident management, security operations, threat intelligence

1. Introduction. The problem of incident response and remediation steps in multi-cloud infrastructure

The increasing adoption of public cloud platforms such as AWS, Azure, and Google Cloud Platform has significantly transformed modern IT infrastructure, providing organizations with flexibility, scalability, and cost efficiency. However, this transition also introduces new security challenges, especially in multi-cloud environments, where access management, threat monitoring, and incident response become increasingly complex. One of the most critical risks arises from human errors and improper handling of cloud access credentials. If attackers gain unauthorized access to authentication keys, they can exploit the cloud environment by creating and managing resources for malicious purposes, including data breaches, malware distribution, and cryptocurrency mining [1].

Traditional approaches to cloud security incident response often rely on manual intervention, which can lead to delayed reactions, ineffective threat containment, and high operational costs. Additionally, organizations face challenges such as false-positive security alerts, a lack of granular threat mitigation controls, and inefficient coordination between security teams. These limitations

* CSDP'2025: Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine

* Corresponding author.

† These authors contributed equally.

oksana.sapsai.kb.2022@ipnu.ua (O. Sapsai), yevhenii.v.martseniuk@lpnu.ua (Y. Martseniuk); andrijp14@gmail.com (A. Partyka); oleh.i.harasymchuk@lpnu.ua (O. Harasymchuk)

0009-0004-1472-7814 (O. Sapsai), 0009-0009-2289-0968 (Y. Martseniuk); 0000-0003-3037-8373 (A. Partyka); 0000-0002-8742-8872 (O. Harasymchuk)

highlight the need for an automated, scalable, and intelligent solution for real-time detection, analysis, and response to cloud security incidents.

This study explores the application of an automated SOAR (Security Orchestration, Automation, and Response) approach as a comprehensive solution for automating security incident management in public cloud environments. The research focuses on integrating Palo Alto Prisma with cloud provider APIs to detect and isolate compromised resources using automated scripts dynamically. Key components include:

1. Anomaly monitoring through Palo Alto Prisma for detecting suspicious activities in cloud environments.
2. Automated quarantine mechanisms (Quarantine Mode) to prevent security breaches with minimal operational disruptions.
3. Integration with HashiCorp Vault to protect access credentials and prevent unauthorized privilege escalation.
4. Granular resource blocking to mitigate threats without shutting down the entire cloud environment.
5. Post-mortem analysis workflows for continuous security improvement and adaptive incident response.

The results of this study show that automated incident response using SOAR automation significantly enhances cloud security by reducing response time, minimizing human intervention, and ensuring effective resource isolation. By implementing structured response mechanisms and leveraging automation, organizations can effectively mitigate threats while maintaining the resilience and availability of their cloud infrastructure [2].

The scientific novelty of this research lies in the development and practical implementation of a multi-level architecture for automated security incident response in public cloud environments. The proposed model integrates Splunk SOAR, Jenkins, and HashiCorp Vault, establishing a comprehensive incident management framework. For the first time, a dynamically triggered "RedButton" automation scenario is introduced for L2 SecOps teams, enabling real-time orchestration of resource isolation across AWS, Azure, and GCP. This approach balances rapid response, security, and operational continuity, while mitigating the risks of unauthorized access and delayed remediation [3–6].

Unlike traditional solutions where components operate in isolation, this model establishes a unified automated response framework that integrates:

1. threat detection tools (Prisma Cloud).
2. incident orchestration platforms (Splunk SOAR).
3. secure credential management systems (Vault).
4. infrastructure automation tools (Jenkins).

The aim of this research is to develop a comprehensive architecture for automated security incident response (SOAR) in multi-cloud environments that enables dynamic secrets management, controlled infrastructure intervention, and scalability to environments with over 400 cloud accounts without centralized administration. The research seeks to establish a formalized logic for transforming anomalies into actionable infrastructure changes with authorization verification at each stage, and to build a risk assessment model with quantitative impact metrics, including economic valuation. Additionally, the goal is to integrate Zero Trust principles, UEBA, and machine learning analytics into the decision-making process, and to implement a self-learning mechanism for adaptive response policy updates based on accumulated experience, eliminating the need for manual intervention [7].

In contrast to existing solutions that are limited to alert generation or executing predefined playbooks, the proposed model delivers a full response cycle—from threat detection to infrastructure

isolation—accompanied by self-documentation and audit reporting. This eliminates delays between detection and action, reduces human dependency, enables effective scaling across hundreds of cloud environments, and ensures compliance with security standards such as NIST 800-53, ISO 27001, and SOC 2. The implementation of this model lays the foundation for next-generation self-managed cloud security architectures operating in real-time with adaptive compliance capabilities.

Numerous studies have explored the challenges and solutions related to cloud security and automated incident response. Research such as [1] and [2] highlights the growing importance of automation in cybersecurity, especially in the context of dynamic and scalable cloud environments.

The concept of SOAR has evolved as a response to the need to reduce manual interventions and increase the efficiency of Security Operations Centers (SOC). According to Suram [8], automation of Identity and Access Management (IAM) plays a critical role in securing cloud platforms. Similarly, Thokala [9] emphasizes the role of scalable cloud deployment and orchestration in maintaining operational security in e-commerce systems.

Recent studies research [10, 11] analyze shadow IT risks and centralized secret management, pointing to the need for integrated orchestration tools like SOAR. These findings align with current practices in leading organizations where tools such as Splunk SOAR and Prisma Cloud are used to detect, classify, and respond to threats across public cloud environments.

Furthermore, Soldatenko and Vik [12] investigated the use of infrastructure-as-a-service (IaaS) and highlighted the operational benefits of automation in cloud infrastructure security. Other research works [13–15] examine the intersection of AI, cloud pipelines, and blockchain-enabled automation, pointing to promising directions for further enhancement of cloud security management systems.

2. Risk assessment and the role of SOAR in their mitigation

In the context of ensuring information security in public cloud environments, a critical task is the systematic identification and assessment of risks that may lead to data compromise or the disruption of infrastructure integrity. Given the complexity of multi-cloud environments and the high dynamics of change within them, the analysis of threats related to unauthorized access, weak authentication mechanisms, and insufficient environment segmentation becomes particularly relevant [11, 13].

This research employed the risk assessment methodology defined by the NIST SP 800-30 standard, which is based on qualitative analysis of threats using two key parameters: the likelihood of occurrence and the potential impact. This approach enabled the construction of a risk criticality matrix, presented in Table 1. The identified risks are ranked by their level of criticality, providing a foundation for developing an effective response strategy and designing robust security mechanisms within multi-cloud environments [16].

The SOAR solution plays a pivotal role in minimizing risks associated with the security of public cloud environments by enabling automated, rapid, and coordinated threat response. Its application significantly reduces the time between risk detection and the implementation of mitigation measures, which is critical in cases of unauthorized access or exploitation of vulnerabilities [12, 17]. Through integration with security monitoring systems, credential management platforms, and infrastructure automation tools, SOAR establishes a unified response framework capable of promptly neutralizing threats and isolating potentially compromised resources [1, 14].

Furthermore, to enhance the effectiveness of automated incident management, it is advisable to integrate information classification and risk assessment mechanisms based on SOC 2 Type II [16, 18]. The use of models that consider the interaction of antagonistic agents in cybersecurity systems allows for more accurate prediction of potential threats and optimization of response scenarios [19]. Additionally, the “Security-as-Code” approach facilitates the standardization of security policies and reduces the time required to implement control measures across multi-cloud environments [1]. As a result, the SOAR system gains self-learning and adaptation capabilities to new attack types, thereby increasing the overall security posture of the infrastructure [20].

Table 1
Common Intrusion Scenarios in Public Cloud Environments and Their Coverage by the SOAR Model

#	Intrusion Scenario	Primary Vulnerability	Likelihood	Impact	Risk Level	SOAR Model Response
1	An attacker gains access to a developer's account through leaked credentials in a public repository	Absence of MFA; weak secret management	High	High	Critical	Detection of anomalous login; automatic account lockout; triggering secret rotation via Vault
2	Malicious actor creates new privileged resources (EC2, IAM policies) after user compromise	Lack of Zero Trust model; ineffective user activity controls	High	Medium	High	Monitoring resource changes; execution of playbooks to block and isolate created entities
3	After initial access, attacker moves laterally across VPCs/projects to expand privileges	No network segmentation; non-isolated roles; shared tokens	Medium	High	High	Traffic segmentation; region isolation; audit and restriction of access rights; automated SOAR response
4	Backdoor installed via access to functions (Lambda, GCF) or S3 buckets, followed by data exfiltration	Inadequate access policy; anonymous object access; unaudited APIs	Medium	High	High	Detection of API request spikes; access restriction; object quarantine; SecOps alerting
5	Resources (e.g., compute instances) are used for cryptomining or botnet participation	Unrestricted egress; weak activity monitoring	High	Medium	High	Detection of abnormal load; suspension of resources; Jenkins integration for rollback to baseline state

Moreover, SOAR reduces the influence of the human factor in the response process, thereby decreasing the likelihood of errors or delays in decision-making during incidents [10]. The incorporation of Zero Trust principles and User and Entity Behavior Analytics (UEBA) within SOAR enables proactive detection of anomalies and potentially malicious behavior before a threat escalates [15]. An additional advantage is the integration of machine learning mechanisms that ensure the system's self-learning capability based on prior incident experiences. This facilitates the continuous adaptation of defense scenarios to emerging threat types, enhancing protection effectiveness in a dynamic environment [9].

Thus, the implementation of SOAR contributes to the development of a proactive and adaptive information security system that not only reduces the probability of risk realization but also mitigates the impact of incidents when they occur, ensuring compliance with contemporary information protection standards [8, 21].

2.1. Vulnerabilities of Cloud Infrastructure in the absence of monitoring

The use of public cloud services without the implementation of proper monitoring tools and automated controls creates significant preconditions for violations of the core attributes of information security—confidentiality, integrity, and availability of data [8, 10] . The absence of continuous observation of anomalous activity, the inadequacy of security event correlation mechanisms, and weak control over authentication and authorization processes significantly increase the likelihood of prolonged undetected presence of adversaries in cloud environments (commonly referred to as dwell time) [13, 22].

This situation complicates the timely detection of incidents and rapid response, thereby increasing the risk not only of localized compromise of individual resources but also of access escalation, threat propagation, and potential cascading impact on adjacent information systems [11], [17]. Moreover, the lack of centralized monitoring limits an organization's ability to detect security policy violations, anomalous user behavior, and unauthorized API usage, all of which are critical in the context of multicloud infrastructure with complex topologies and multiple access points [12, 14].

2.2. Analysis of major security incidents in Public Cloud Environments (2023–2025)

Incident Analysis in Cloud Environments (2023–2025): The Impact of Absent Monitoring on the Emergence of Critical Threats.

In the context of the evolving digital ecosystem, particularly with the growth of multicloud architectures, the issue of timely detection of information security incidents and adequate response has become increasingly critical [2, 10] . The lack of integrated monitoring tools, automated analysis of security events, and real-time threat response capabilities creates conditions for large-scale compromises of information assets [11, 15].

Analysis of several high-profile incidents recorded between 2023 and 2025 reveals typical vulnerability patterns that enabled the execution of advanced and complex attacks [1, 14].

The most illustrative cases include:

- The 2023 compromise of the MOVEit platform, hosted on Azure Blob Storage, due to a SQL injection in the absence of API call monitoring [9]. The incident led to the data breach of over 500 organizations, including multinational corporations and U.S. government agencies.
- A targeted attack on Microsoft Exchange Online (2023) by the Storm-0558 group, which used a compromised signing key to forge OAuth tokens [13]. This resulted in unauthorized access to the email accounts of U.S. government entities.
- The 2024 Snowflake incident, which caused a data breach of AT&T users due to the absence of multi-factor authentication and inadequate monitoring of user sessions [23].
- The 2025 compromise of the Sisense environment, which occurred due to hardcoded secrets and the absence of inter-environment isolation [8], leading to the exposure of confidential data belonging to government and corporate clients.

Additional incidents recorded in 2025 further confirm the relevance of this issue:

- Zero-day vulnerability CVE-2025-53770 in Microsoft SharePoint Server, which enabled spoofing attacks and resulted in the compromise of at least 75 servers [12].
- The Azure Blob Storage exposure incident at TalentHook, which led to the disclosure of over 26 million resumes containing personal data, highlighting the criticality of configuration errors [11].

- A massive data breach stemming from an attack on Oracle Cloud authentication services (SSO/LDAP), which compromised over 6 million user accounts [2].
- The exploitation of CVE-2025-3928 in Commvault Metallic, which allowed unauthorized access to clients' Microsoft 365 environments and underscored the risks of relying on third-party SaaS solutions without sufficient monitoring [17].

An academically grounded summary of these cases is presented in Table 2.

Table 2
Consolidated Overview of Cloud Environment Compromises (2023–2025) and Assessment of Economic Losses

Year	Incident	Description of the Event	Exploited Vulnerability	Causes of Compromise	Consequences
2023	MOVEit	Compromise of Azure Blob-based file transfer platform	SQL injection	Lack of API monitoring, low transparency of calls	Data breach affecting 500+ organizations (BBC, Shell, BA)
2023	Storm-0558	Access to Exchange Online mailboxes	OAuth token forgery	Key compromise, lack of token control	Access to emails of 25 organizations, including the US government
2024	Snowflake / AT&T	Compromise of customer accounts	Lack of MFA	Poor session control, lack of UEBA	Compromise of data from 160+ organizations, metadata leak
2024	Snowflake FinSec	Access to banks' financial data	Privileged service accounts	No Zero Trust, weak access audit, lack of UEBA	Exfiltration of transactions from several banks
2025	SharePoint CVE-2025-53770	Zero-day attack on SharePoint Server	Zero-day / spoofing	Lack of verification, non-isolated traffic	Compromise of 75 servers, including government ones
2025	TalentHook / Azure Blob	Public container with 26 million résumés	Misconfiguration	Lack of access control, misconfiguration	Massive leak of personal data
2025	Oracle SSO / LDAP	Attack on authentication service	Authentication compromise	Lack of domain isolation, poor account security	Compromise of 6 million user accounts
2025	Commvault / Jupiter	Vulnerability in Commvault Metallic SaaS solution	Third-party SaaS vulnerability	Lack of monitoring, absence of behavioral analytics	Access to Microsoft 365 environments

All of the aforementioned cases highlight the limitations of traditional security approaches in the absence of adaptive monitoring, proper access management, and automated response mechanisms [10, 24]. As a result, threat actors remain undetected in the system for extended periods (dwell time), escalate attacks to interconnected components, and cause large-scale asset compromise [15].

The use of SOAR-type systems addresses these shortcomings by enabling:

- Real-time automated verification of access configuration parameters.
- Execution of immediate response scenarios through integrated playbooks.
- Isolation and disconnection of compromised infrastructure components.
- Formalized auditing of response actions, which ensures event traceability and compliance with regulatory requirements [18, 25].

Thus, the updated overview of threats observed in 2025 confirms the necessity of transitioning to a proactive, automated model for cloud security—one in which SOAR solutions play a critical role in risk mitigation and the enhancement of digital infrastructure resilience [14, 26].

2.3. Economic impact of Security incidents in Cloud Environments

Beyond the technical threat vectors associated with cloud infrastructure compromise, a critical rationale for implementing integrated monitoring and automated response systems lies in their economic viability. According to IBM Security's "Cost of a Data Breach Report 2024" [1], the average cost of a single data breach in a cloud environment is estimated at $5.17 million. In multi-cloud architectures with fragmented access control, these figures may rise significantly, elevating financial risk for organizations lacking sufficient automation in their security processes [9].

The MOVEit platform incident (2023) exemplifies both the scale and cost of impact mitigation. Independent audit reports estimate total losses due to unauthorized access to Azure Blob Storage at over $410 million [8]. This figure encompasses costs related to breach containment, regulatory fines (GDPR, HIPAA), litigation from affected parties, and investments in reputational recovery.

Similarly, the leak of 26 million résumés caused by a misconfiguration of Azure Blob Storage by TalentHook (2025) demonstrated that even non-malicious errors can result in severe economic consequences [10]. Direct damages in this case amounted to several million dollars, with a significant portion attributed to reputational harm, increased cyber insurance premiums, and forensic analysis expenses (see Table 3) [12].

The 2025 compromise of Oracle Cloud's authentication infrastructure, resulting in the theft of over 6 million user accounts, highlighted the economic vulnerability of centralized access systems such as SSO and LDAP. Due to lateral movement, attackers escalated privileges and compromised adjacent services. Cumulative losses for Oracle and its partners are estimated between $4.5 million and $20 million, depending on industry sector, regulatory exposure, and the depth of the breach [2, 11].

According to the same IBM report, organizations without SOAR-class solutions take, on average, 76 days longer to detect and contain a breach [1]. Increased dwell time directly correlates with breach severity and financial impact, while complicating compliance audits for SOC 2, ISO/IEC 27001, and PCI DSS standards [14].

Thus, the implementation of automated security systems—especially those based on SOAR, Zero Trust, and UEBA concepts—not only enhances technical resilience but also optimizes incident response expenditures. Public ROI evaluation models in cybersecurity indicate that deploying a full-fledged SOAR solution can reduce economic losses from incidents by at least 25–50% compared to traditional reactive security models [13, 15].

3. Threat detection tools and automated response systems as the foundation of cloud security strategy

An effective strategy for ensuring information security in public cloud environments requires the integration of two key components: Threat Detection Tools and Security Orchestration, Automation, and Response (SOAR) systems. This dual approach enables not only comprehensive real-time monitoring of the cloud infrastructure's state but also the generation of adaptive responses to a wide range of threats, taking into account their nature, criticality, and potential impact on organizational assets [2, 9].

Table 3
Estimated economic impact of cloud security incidents (2023–2025)

#	Incident	Platform / Component	Vulnerability Type	Key Consequences	Estimated Financial Loss (USD)
1	MOVEit (2023)	Azure Blob Storage	SQL injection, lack of API monitoring	Data breach affecting 500+ organizations (BBC, Shell, etc.)	~410 M
2	Storm-0558 (2023)	Microsoft Exchange Online	Key compromise, OAuth token forgery	Compromise of government email accounts	up to 20 M
3	Snowflake / AT&T (2024)	Snowflake (multi-cloud)	Missing MFA, weak monitoring	Leakage of telecom metadata	5–8 M
4	Sisense compromise (2025)	Snowflake / Sisense	Lack of isolation, secrets stored insecurely	Breach of government and corporate customer data	10–15 M
5	SharePoint CVE-2025-53770	Microsoft SharePoint Server	Zero-day (spoofing), lack of lateral movement control	Compromise of 75+ servers	3–6 M
6	TalentHook Azure Blob leak (2025)	Azure Blob Storage	Misconfiguration	Exposure of 26 million résumés	5–7 M
7	Oracle SSO/LDAP breach (2025)	Oracle Cloud	Credential theft, SSO compromise	Leakage of 6 million user accounts	4.5–20 M
8	Commvault CVE-2025-3928 (2025)	Commvault Metallic (Azure SaaS)	Third-party SaaS vulnerability	Access to Microsoft 365 customer resources	8–12 M

Threat detection systems perform deep inspection of cloud environment telemetry using behavioral pattern analysis, anomaly detection, event correlation, and threat intelligence feeds [10]. Their role is to identify potential attack vectors, policy violations, and atypical usage patterns that may indicate a security threat [8, 13].

SOAR systems, on the other hand, function as strategic tools for automating the response to detected incidents. They standardize response procedures, enable centralized coordination between various security tools, and significantly reduce Mean Time to Respond (MTTR) [11, 14]. Integrating these components into a unified security perimeter minimizes dependence on the human factor—a critical concern in highly dynamic multi-cloud infrastructures—and ensures compliance with international security standards such as NIST SP 800-53, ISO/IEC 27001, and SOC 2 [1, 15].

Thus, the synergy between threat detection tools and SOAR platforms forms the backbone of a modern cloud security strategy, capable of not only swiftly identifying and mitigating threats but also enhancing infrastructure resilience against complex, multi-vector attacks [12].

3.1. Threat detection systems as the basis of proactive Cloud Security

The functional capabilities of threat detection systems extend far beyond merely identifying intrusions or breaches. These systems perform deep inspection of user behavior, services, and

network connections by applying analytics based on security policies, signature-based methods, heuristics, and behavioral models [9, 11]. This approach enables not only the detection of overt incidents but also the proactive identification of latent threats that have not yet manifested as active attacks—such as lateral movement, privilege escalation attempts, or the abuse of legitimate tools for unauthorized actions (commonly referred to as Living off the Land, or LotL) [12, 14].

A key advantage of these systems is their ability to classify identified incidents by criticality level, which allows for the optimization of security resource allocation and the prioritization of response actions. This is particularly important in environments with limited human resources within Security Operations Centers (SOCs) and high levels of informational noise in the form of false positives [15]. Threat detection systems act as a filtering layer that not only suppresses insignificant events but also enriches incident data with contextual information—such as user identity, affected resource, geographic location, and threat type [8].

Strategically, threat detection systems also serve as a feedback mechanism for improving security policies, forming threat intelligence feeds, and adapting defensive strategies in response to changes in the threat landscape [2, 10]. Without this functionality, SOAR solutions cannot operate effectively, as the structured and high-quality output from threat detection systems acts as the primary trigger for initiating automated response playbooks [13].

3.1.1. Market leaders in proactive Threat Detection

In the context of the increasing complexity of multicloud environments, the selection of threat detection tools becomes a strategically critical step in building an effective security system. The quality and functional capabilities of these tools determine the organization's ability not only to timely identify potential attacks or vulnerabilities, but also to provide the necessary context for subsequent response activities [2, 22]. This is especially relevant in scenarios where incident management is tightly integrated with security automation systems (SOAR), which require high precision and completeness of data to support effective decision-making [14].

Accordingly, this study presents a comparative analysis of leading threat detection platforms in cloud environments, including Prisma Cloud, AWS GuardDuty, Microsoft Defender for Cloud, Google Security Command Center, Orca Security, and Lacework. This analysis serves as the foundation for selecting the most appropriate tool to meet multicloud security requirements, ensuring not only comprehensive threat detection, but also efficient integration with SOAR platforms for building a cohesive cloud infrastructure protection strategy [15, 27].

3.1.1.1. Commercial and open solutions for Threat Detection

Prisma Cloud is a comprehensive platform combining Cloud Security Posture Management (CSPM), Cloud Workload Protection Platform (CWPP), and integrated capabilities for threat and anomaly detection at the levels of resources, network traffic, configurations, and identity data [13, 15]. A key advantage is its integration with the Cortex XSOAR ecosystem, enabling a seamless transition from threat detection to automated response [9]. The platform supports all three major cloud providers—AWS, Azure, and GCP—without coverage limitations, which is critical for multicloud strategies.

AWS GuardDuty is a native security service designed for the AWS environment. It performs monitoring and threat detection based on log flows, VPC traffic, CloudTrail data, and DNS queries [14]. Its primary limitation is its exclusive applicability within AWS, without support for other cloud providers. Furthermore, GuardDuty focuses mostly on anomaly detection and lacks in-depth configuration analysis or workload protection.

Microsoft Defender for Cloud (formerly Azure Defender) offers a broad set of security features for Azure, including CSPM, CWPP, and threat detection capabilities [17]. Although the product supports integration with AWS and GCP, such support is partial and does not offer functional parity with its Azure-native features. Its tight integration with the Microsoft Security Stack makes it a strong option for organizations based primarily on Azure.

Google Security Command Center (SCC) provides a centralized security monitoring platform for GCP, including vulnerability detection, misconfiguration analysis, and indicators of compromise [18]. However, SCC is restricted to Google Cloud, which reduces its effectiveness in multicloud environments. While its CSPM features are competitive, the lack of integration with third-party SOAR solutions creates a gap between detection and response.

Orca Security offers an agentless architecture for in-depth scanning of AWS, Azure, and GCP environments [24]. The platform detects vulnerabilities, policy violations, and threats without the need to install agents on individual resources. Its main strengths are rapid deployment and minimal performance overhead. However, Orca does not include its own SOAR system, requiring integration with external solutions.

Lacework focuses on behavioral analytics and activity monitoring across cloud workloads [27]. The platform excels at detecting anomalies and potentially malicious activity using machine learning algorithms. While it supports multicloud environments, it has a more limited CSPM feature set compared to Prisma Cloud and does not offer equally deep integration with automation platforms.

The comparative Table 4 below outlines the key characteristics of leading threat detection platforms in cloud environments across several critical parameters relevant for integration into a comprehensive cloud security strategy.

The first criterion is multicloud support, assessing the platform's ability to operate across multiple cloud providers—AWS, Azure, and GCP. This is vital for organizations adopting multicloud architectures that require centralized security oversight.

The second aspect is the presence of Cloud Security Posture Management (CSPM), which identifies and remediates misconfigured cloud resources that can create vulnerabilities. CSPM ensures continuous configuration assessment and policy compliance.

The third criterion, Cloud Workload Protection Platform (CWPP), covers the protection of workloads such as virtual machines, containers, and serverless functions, which is particularly relevant in cloud and hybrid environments.

The fourth parameter is integration with SOAR platforms, indicating the ability to not only detect threats but also automate incident response. A lack of such integration limits the capacity for swift mitigation without operator intervention.

The final criterion is the approach to threat detection, characterizing the platform's methodolog—whether through log analysis, API request monitoring, configuration scanning, behavioral analytics, or machine learning–based anomaly detection.

The conducted analysis demonstrates that Prisma Cloud stands out with the highest level of functional completeness among the reviewed solutions [13, 15, 24], giving it a strategic advantage within multicloud architectures. The platform integrates both Cloud Security Posture Management (CSPM) capabilities—responsible for continuous auditing of cloud infrastructure configurations for compliance with security policies and standards—and Cloud Workload Protection Platform (CWPP) features, focused on protecting workloads ranging from virtual machines to containerized applications and serverless functions. This combination ensures strategic configuration control and tactical protection of dynamic workloads.

Additionally, Prisma Cloud features native integration with the Cortex XSOAR platform [9], establishing a direct connection between threat detection and automated response. This allows not only for timely identification of risks but also for immediate initiation of orchestrated response scenarios, which is critical in the highly dynamic threat landscape of cloud environments.

In contrast, other solutions such as AWS GuardDuty and Google Security Command Center (SCC), while effective within their native ecosystems, remain limited in a multicloud context [14], [21] due to the absence of a unified approach to CSPM and CWPP and a lack of—or limited—integration with SOAR platforms. This reduces their adaptability and effectiveness in heterogeneous infrastructures, where maintaining a unified standard for security management and incident response across cloud providers is essential.

Table 4
Comparative characteristics of threat detection systems for soar integration

Product	Multi-Cloud Support	CSPM	CWPP	SOAR Integration	Threat Detection Approach
Prisma Cloud	AWS, Azure, GCP	Yes	Yes	Yes	Configuration, traffic, API, behavior
AWS GuardDuty	AWS only	No	No	No	Logs, traffic, API
Microsoft Defender for Cloud	Azure (full), AWS/GCP (partial)	Yes	Yes	Native tools	Logs, configurations, integration with Sentinel
Google SCC	GCP only	Yes	No	No	Vulnerabilities, events
Orca Security	AWS, Azure, GCP	Yes	No	Partial	Agentless scanning
Lacework	AWS, Azure, GCP	Partial	No	Partial	Behavioral analytics (ML-based)

Thus, Prisma Cloud's multidimensional approach—combining comprehensive configuration control, workload protection, and an uninterrupted chain of detection and response—positions it as the optimal solution for organizations seeking to ensure cyber resilience within complex multicloud ecosystems.

3.2. The role of SOAR systems in security Incident Management strategy

SOAR (Security Orchestration, Automation, and Response) systems represent a critical component of modern cybersecurity, enabling automation, coordination, and standardization of threat detection, analysis, and incident response processes [9, 12]. Their implementation significantly reduces the mean time to detect (MTTD) and mean time to respond (MTTR), alleviates the workload on SOC analysts, and minimizes human-factor-related risks [14].

The relevance of SOAR increases markedly in multicloud environments, where the volume of security events requiring processing often exceeds the capacity of traditional response teams [11]. SOAR systems can integrate with a broad range of cloud security components—including cloud platform APIs (AWS, Azure, GCP), SIEM systems (such as Splunk), vulnerability management tools, identity and access management services (like HashiCorp Vault), and service desk tools [27].

Key capabilities of SOAR systems include:

- Automated detection of anomalous events based on data from monitoring systems (e.g., Prisma Cloud, GuardDuty, Splunk) [13].
- Execution of standardized response playbooks, including actions such as account locking, VM isolation, firewall policy modification, and alert generation in SIEM platforms [9].
- Orchestration of workflows across infrastructure components—from CMDB and EDR to incident management platforms like Jira and ServiceNow [12].
- Generation of auditable activity logs in compliance with standards such as NIST SP 800-61, ISO/IEC 27035, SOC 2, HIPAA, and others [28].

A typical SOAR use case involves automated response to the creation of cloud objects in atypical regions, unauthorized API access, or out-of-hours use of privileged accounts. In these scenarios, the system triggers appropriate actions—revoking access keys, isolating assets, and notifying the responsible teams [18].

A crucial aspect of SOAR integration is its interaction with secrets management systems like HashiCorp Vault, which enable Just-In-Time Access and eliminate the need for persistent credentials [29].

In conclusion, SOAR systems provide the technical and organizational foundation for building scalable, standards-compliant, and adaptive security strategies in cloud environments. Their adoption significantly reduces attacker dwell time, improves response transparency, and enhances the overall cyber resilience of the organization [1, 9].

3.2.1. Technical implementation of Automated response based on SOAR

The technological implementation of SOAR (Security Orchestration, Automation, and Response) solutions involves the creation of an integrated infrastructure for security incident management, enabling automation of critical stages—from anomaly detection to threat neutralization [9, 12]. In public and multicloud environments, where the volume of events and data sources significantly increases, SOAR becomes a foundational element for ensuring scalability, action consistency, and compliance with regulatory requirements [14, 27].

Architecturally, a SOAR platform functions as an orchestration node that interacts with the following classes of components:

- Telemetry and event sources: SIEM systems (such as Splunk, Chronicle), cloud monitoring and protection services (e.g., Prisma Cloud, AWS GuardDuty), vulnerability management systems, and authentication/identity services (Azure AD, Okta) [11, 28].
- Response orchestrator: the SOAR engine that correlates events, makes decisions, and triggers response playbooks—often implemented as a dedicated software solution (e.g., Cortex XSOAR, Splunk SOAR) [9].
- Integration gateways: tools for executing automated actions in cloud environments (AWS IAM, Azure Resource Manager), interfacing with incident management services (ServiceNow, Jira), secrets management systems (HashiCorp Vault), and DevOps automation tools (Ansible, Terraform) [29].

A typical automated response scenario proceeds as follows:

1. Prisma Cloud detects potentially anomalous activity (e.g., access to a container from an unusual region), which is classified as a high-risk event [1].
2. The event is forwarded to the SIEM platform (e.g., Splunk), where predefined correlation rules trigger an alert [11].
3. The SOAR platform receives the alert from the SIEM and activates the corresponding response playbook [13].
4. The playbook executes a sequence of actions:
    - Temporarily suspends credentials via integration with Vault [29].
    - Isolates the suspicious virtual instance.
    - Creates an incident in ServiceNow or Jira with relevant event attributes.
    - Automatically notifies the responsible analyst or response team [9, 21].

A key advantage of modern SOAR solutions is the ability to develop customized response playbooks, formalized as machine-readable structures (YAML, JSON), with comprehensive logging in accordance with audit trail principles. This ensures transparency and traceability, which are essential for compliance with standards such as ISO/IEC 27035, NIST SP 800-61, SOC 2, and PCI DSS [21].

SOAR integration with secrets management systems (e.g., HashiCorp Vault) enables the implementation of dynamic access control models such as Just-In-Time Access, where critical

privileges are granted only at the moment of execution. This significantly reduces the risk of exploiting vulnerabilities associated with persistently stored credentials [28].

Thus, the implementation of SOAR in cloud infrastructure establishes a technical and organizational foundation for proactive security, minimizes mean time to respond (MTTR), and optimizes coordination among subsystems within the cybersecurity architecture [9, 12].

3.2.2. Common Security Challenges in Cloud Infrastructure and the Role of SOAR in Their Mitigation

In the process of building multi-layered cloud architectures, organizations encounter a number of systemic vulnerabilities that lower the overall level of security. These include fragmented access control mechanisms, the absence of centralized oversight for inter-cloud interactions, the human factor in response processes, and the lack of formalized incident management procedures [12, 14]. These challenges are critical for modern multi-cloud environments and require technological solutions that enable scalable, standardized, and automated threat response. In this context, SOAR (Security Orchestration, Automation, and Response) systems play a pivotal role by enabling effective orchestration of detection, analysis, and incident response processes [9, 27].

Below is an overview of the most common security issues in cloud infrastructures and the mechanisms for their mitigation through SOAR solutions:

1. Fragmented Access in Multi-Cloud Environments
   When multiple cloud providers (e.g., AWS, Azure, GCP) are used simultaneously, it becomes increasingly difficult to manage access rights and audit user actions. SOAR provides centralized aggregation of access logs and events, allowing for the detection of anomalous cross-environment movements (lateral movement) and the implementation of dynamic Zero Trust policies [15, 24].
2. Lack of Standardized Response Procedures
   Manual response, which depends on the subjective perception of SOC analysts, often leads to delays or erroneous decisions. SOAR employs predefined playbooks that automate the resolution of common scenarios—such as isolating resources, revoking access keys, or creating incidents in service desk systems [9, 11].
3. Human Factor and Limited SOC Resources
   A significant portion of incidents is not escalated in a timely manner due to the overload of first-line security analysts or insufficient qualifications. SOAR enables the delegation of routine tasks to automated mechanisms—such as creating and updating CMDB records, processing SIEM events, or interacting with Vault to restrict access rights [13, 29].
4. Lack of Transparency and Auditability in Response
   In many cases, organizations fail to ensure an audit trail of actions taken during incident response, making it impossible to achieve compliance certifications (SOC 2, ISO/IEC 27001, PCI DSS). SOAR formalizes and logs every step taken within a playbook, indicating the timestamp, initiator, and consequences of each action [28].
5. High Dwell Time of Threat Actors
   Due to the absence of automated anomaly analysis, threats may remain undetected for several weeks. SOAR, in combination with UEBA modules or SIEM systems (e.g., Splunk, Sentinel), can initiate detection based on behavioral patterns, promptly escalate incidents, and trigger containment measures [16, 26].

Thus, common security issues in cloud environments can be effectively mitigated through the implementation of SOAR as a systemic component. Its ability to integrate with cloud APIs, manage access via Vault, automate response playbooks, and retain a complete event log makes it an indispensable tool for achieving both technological and regulatory maturity in cybersecurity [9, 29].

3.3. Comparison of SOAR systems and justification of selection

As part of this study, a comparative analysis was conducted on leading Security Orchestration, Automation and Response (SOAR) solutions in order to justify the selection of tools for automating security incident management in multi-cloud environments. The analysis covered four of the most widely used platforms: Palo Alto Cortex XSOAR, Splunk SOAR, IBM QRadar SOAR, and Microsoft Sentinel [9, 22]. The evaluation was based on the following criteria:

- level of integration support for cloud providers (AWS, Azure, GCP).
- flexibility and manageability of automation playbooks.
- availability and capabilities for working with threat intelligence sources.
- scalability across large distributed infrastructures.
- compliance with international information security standards (NIST SP 800-53, ISO/IEC 27001, SOC 2, etc.) [24, 28].

The results of the comparison are presented in Table 5.

Table 5
Comparative characteristics of SOAR solutions

Platform	Cloud Integration	Playbooks	Threat Intelligence	Scalability	Usage Comment
Cortex XSOAR	AWS, Azure, GCP	Visual, flexible	Integrated Threat Intel	High	Full compatibility with Prisma Cloud
Splunk SOAR	AWS, Azure, GCP	YAML + UI	External sources	High	Best integration with Splunk SIEM
IBM QRadar SOAR	Limited (via add-ons)	Partially restricted	Built-in intelligence	Medium	Challenges in multi-cloud support
Microsoft Sentinel	Mainly Azure	LogicApps (Playbooks)	Built-in	High	Tightly coupled with Azure ecosystem

The conducted analysis has demonstrated that the most optimal configuration for the research objectives is the combination of: Prisma Cloud (for anomaly detection and incident identification), Splunk SOAR (for centralized response automation), HashiCorp Vault (for secure secrets management), and Jenkins (as an execution tool for environment changes) [12, 13, 30]. This selection is justified by the high degree of interoperability between the components, compliance with industry standards, and the ability to scale across heterogeneous cloud environments.

The proposed model also stands out by integrating preventive, detection, and response components into a unified managed system. The use of SOAR significantly reduces the time between incident detection and response (Mean Time to Detect / Mean Time to Respond), limits adversary dwell time, and minimizes the impact of human error in response processes [10, 15].

The scientific novelty of the proposed approach lies in constructing a holistic model of automated incident response in a multi-cloud environment, taking into account the principles of Zero Trust, least privilege, and automated protection of secret access through Vault. Unlike conventional SOAR implementations, which often limit themselves to event logging and manual intervention, this model demonstrates deep integration across monitoring, response, and automated threat remediation [14, 29].

4. Methodology for automation of security incident management in public cloud environments using PaloAlto Prisma

4.1. Security standards as a foundation for Incident Response automation

Automation of detection, classification, and response processes to incidents in cloud environments must align with the requirements of international information security standards. These standards not only formalize the expected behavior of an organization during a security incident but also define criteria for evaluating the effectiveness of technical and organizational protective measures [19, 28]. The deployment of SOAR solutions within multi-cloud infrastructure should rely on normative frameworks such as SOC 2, NIST SP 800-53, ISO/IEC 27001, ISO/IEC 27035, PCI DSS, and HIPAA [15].

The ISO/IEC 27001 standard mandates the implementation of procedures for detecting, logging, and responding to information security events. Together with ISO/IEC 27035, which elaborates on incident management processes, these standards form the foundation for designing SOAR playbooks. Specifically, the standard requires the formalization of incident classification criteria, limitations on response time, and maintenance of audit trails—all of which can be operationalized through automated response scenarios [11].

The NIST SP 800-53 recommendations define a comprehensive set of control requirements for information systems, including the IR (Incident Response) family, which mandates:

- Mechanisms for event detection (IR-4).
- Real-time response capabilities (IR-5).
- Methods to limit the impact of incidents (IR-6).
- Effectiveness analysis of response measures (IR-8) [30].

Within a SOAR platform, these requirements can be fulfilled through automated incident creation based on SIEM triggers, execution of response playbooks, action logging, and report generation [27].

SOC 2 focuses on building trust in cloud services based on five principles: security, availability, processing integrity, confidentiality, and privacy. In this context, SOAR ensures continuous monitoring and verification of access, reduces the impact of incidents on service availability, and enables centralized retention of forensic evidence [10].

In the financial services and e-commerce sectors, the PCI DSS standard is widely adopted, mandating event logging (Req. 10), regular monitoring (Req. 11), and clearly defined response procedures (Req. 12.10) [32]. The use of SOAR facilitates the automation of these processes, ensuring audit transparency [12].

Regarding the protection of medical data, the HIPAA standard requires implementation of technical safeguards for access control, intrusion detection, and user notification about unauthorized access attempts. The integration of cloud logs with SOAR enables fulfillment of these requirements through systematic access event processing, incident isolation, and subsequent analysis [13].

Thus, compliance with international standards is not only a matter of audit readiness but also a critical factor in building an effective, scalable, and regulatory-aligned architecture for automated security in the cloud. Leveraging SOAR as a mechanism for implementing these standards ensures a structured, controlled, and transparent threat response process [15].

4.2. Implementation of an Automated model in a multi-cloud environment

Within the proposed architecture for automated incident response in information security, a central role is played by the integration of the Palo Alto Prisma platform into the public cloud infrastructure. In the context of multi-cloud deployments—particularly across Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)—the processes of monitoring, threat

detection, and response become increasingly complex due to differences in access mechanisms, authentication standards, and network isolation capabilities [14]. Traditional methods that rely on manual intervention prove ineffective under such conditions, as they are unable to ensure timely response and are prone to delays, thereby increasing the risk of asset compromise [18].

The introduction of automated approaches based on Jenkins enables the construction of response logic that orchestrates security actions according to predefined scenarios. This is achieved through the use of automated playbooks, enrichment of threat intelligence by analytical modules, and continuous real-time incident monitoring [17]. Such mechanisms allow for the isolation of infrastructure resources prior to the involvement of SecOps personnel, significantly reducing dwell time and mitigating the risk of lateral movement and escalation [27].

Orchestration via Jenkins is implemented through ready-to-use connectors and APIs that enable unified interaction across different cloud service providers. This facilitates the enforcement of consistent response standards across heterogeneous clouds without the need to develop separate manual procedures for each platform [26]. A key advantage lies in enabling interoperability between security tools, which collectively function as a coordinated system. This simplifies incident management, unifies event sources, response actions, and reporting within a centralized platform [25].

Leveraging the expertise of Palo Alto and the analytical capabilities of Prisma allows for the detection of emerging attack vectors based on anomalous behavior and the immediate application of appropriate security policies [11]. These data are subsequently forwarded to Security Operations Centers (SOC) for analysis, enabling not only a timely response but also knowledge accumulation for the continual enhancement of response mechanisms [23].

Thus, the implementation of an automated model in a multi-cloud environment using Prisma, Jenkins, and SOAR ensures scalable, efficient, and standardized incident response in alignment with the requirements of modern dynamic infrastructures [24].

4.3. Scenario of automated incident response

The presented security automation architecture for public cloud environments utilizes integrated solutions to detect threats, analyze them, and execute automated responses. This process involves a step-by-step execution of actions aimed at isolating threats with minimal human intervention.

At the initial stage, anomalies in cloud infrastructure behavior are detected using Prisma Cloud (Step 1 in Figure 1). These anomalies, which may indicate potential security incidents, are transmitted to Splunk for further processing (Step 2). In Splunk, the data is analyzed to determine the criticality of events, after which a list of “notable events” requiring response is generated [2, 14].

The decision on further actions is made by the Level 2 (L2) SecOps team (Step 3), which receives notifications about critical events through Splunk (Step 4). SecOps waits for a response from the end user within 15 minutes, after which blocking procedures are executed through automation. If the threat is confirmed, the team activates an automated SOAR action known as “RedButton” (Step 5). This action triggers an automation script in Splunk SOAR, which initiates the Jenkins automation node (Step 6).

Jenkins functions as a coordination node, obtaining the necessary credentials for accessing public cloud platforms (AWS, Azure, Google Cloud Platform) from HashiCorp Vault. (Step 7) [15, 22]. This ensures the secure use of credentials for executing blocking actions in the cloud infrastructure.

Next, Jenkins applies the appropriate isolation policies defined in preconfigured playbooks (Step 8). In Google Cloud Platform, this may include blocking access via Cloud IAM or modifying virtual network (VPC) settings. In AWS, it involves disabling compromised IAM accounts, changing security group rules, or restricting access through VPC. In Microsoft Azure, isolation is enforced by modifying Azure IAM or restricting virtual networks. It is important to note that resources remain operational, preventing a complete shutdown of infrastructure operations (Step 9) [24].

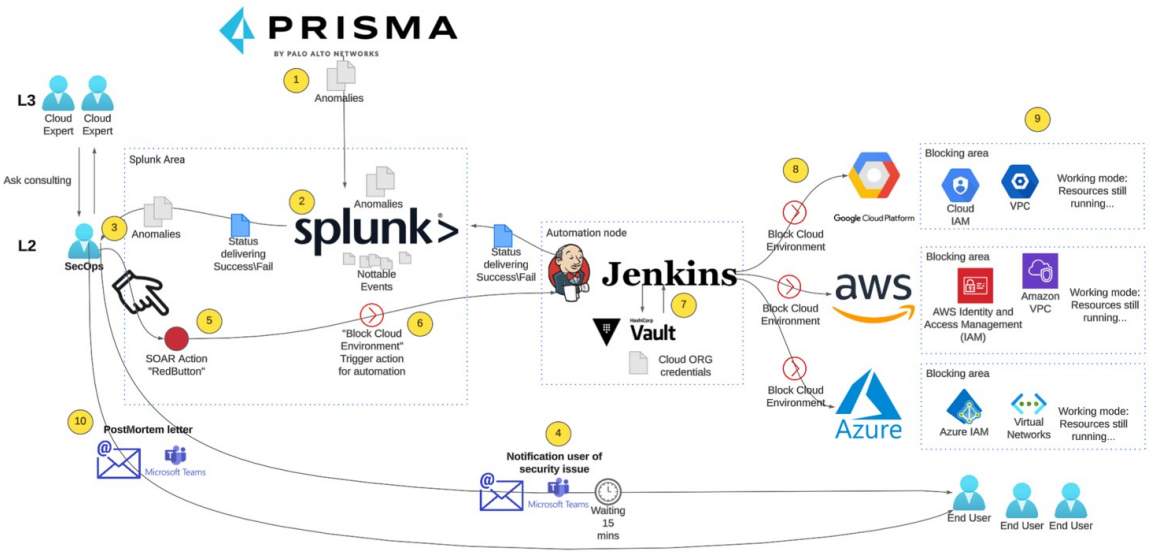

Figure 1: Automated security incident response process

After executing the actions, end users and administrators receive incident notifications via email or Microsoft Teams. These notifications contain detailed information about the nature of the threat, the measures taken, and further recommendations [15, 17].

The final stage is the creation of a post-mortem report, which includes an analysis of the incident's causes, its consequences, the actions performed, and recommendations to prevent similar situations in the future. This report aims to improve response processes and enhance the overall effectiveness of the security system (Step 10) [12].

4.4. Technical and Organizational Risks of Deploying Automated Solutions in Multi-Cloud Environments

Despite the economic and operational feasibility of implementing SOAR systems, a number of risks must be considered that may limit their effectiveness or complicate their deployment:

1. Limited integration compatibility with private and on-premises infrastructures.
   A significant portion of local systems lacks support for standard interfaces (such as REST API and Webhooks), which makes it impossible to fully automate incident response within such environments [13].
2. Absence of unified API standards among cloud providers.
   The heterogeneity of event log formats, authentication protocols, and access structures complicates the implementation of unified response scenarios across different platforms [27].
3. Possibility of errors in automated scenarios.
   Insufficiently validated or improperly configured playbooks may cause service availability disruptions, accidental blocking of legitimate traffic, or other operational failures [15].
4. High dependency on third-party components.
   The operation of a SOAR system assumes stable functioning of the integrated platforms (SIEM, Vault, CI/CD, log services). A failure in any one component can disrupt the entire response chain [18].
5. Scalability and complexity management.
   As infrastructure scales, there arises a need for expanded computational resources, increased throughput of logical links, and support for more complex response scenarios [22].
6. Organizational barriers.
   A low level of personnel awareness, lack of coordinated response procedures, and a shortage of qualified specialists may significantly reduce the effectiveness of the implementation [32].

To mitigate the above-mentioned risks, a phased implementation strategy is recommended. This strategy should include pilot environment testing, gradual scaling, playbook revision, establishment of fallback manual response mechanisms, and alignment with international incident response standards (such as NIST SP 800-61 and ISO/IEC 27035) [2].

4.5. Empirical testing of the implemented solution's effectiveness

To validate the effectiveness of the proposed model, experimental testing was conducted within a controlled demonstration environment simulating the multi-cloud architecture of a mid-sized enterprise. The evaluation focused on key operational metrics—Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), false positive rate, risk level, and SOC team workload [14].

The test environment included: AWS (3 accounts), Azure (2), and GCP (1); integrated with Prisma Cloud, Jenkins, Vault, and Splunk SOAR. Typical simulated incidents involved suspicious account activity, unauthorized API calls, and unauthorized modifications to security policies. The control group operated without automated response.

Table 7
Results of comparative analysis

Metric	Without Automation (2025 estimate)	With Automated Response	Improvement (%)
Mean Time to Detect (MTTD / hours)	2.5	0.15	93
Mean Time to Respond (MTTR / hours)	5.5	1	81
False Positive Incident Rate (%)	14	5	64
SOC Analyst Workload (%)	100	40	60
Direct Loss per Incident (USD)	1700	320	81
Potential Impact (Risk Score, out of 10)	8	2	75

A comparison of the obtained results with analytical reports—particularly the IBM Cost of a Data Breach Report 2023—confirms alignment with industry trends: on average, MTTR without automation exceeds six hours, and direct losses surpass $4.45 million [12]. Thus, implementation of the developed model demonstrates high effectiveness and strong potential for scalability within organizations operating dynamic multi-cloud architectures [27].

It should be noted that the model's effectiveness is limited in cases of fragmented event logging or incidents requiring deep contextual analysis, which is not achievable with current systems. This highlights the need for further evolution of the solution through the integration of ML/AI technologies, behavioral analytics, and UEBA mechanisms [33].

4.6. Implementation results and future development directions

The proposed model of automated incident management in public cloud environments has been implemented through the integration of modern tools for detection, analysis, and response. The core components include: Prisma Cloud by Palo Alto Networks as the primary risk detection platform [21], Splunk SOAR as the orchestration and response automation system [14], Jenkins as an execution mechanism for infrastructure-level changes [15], and HashiCorp Vault for secure credential management [22]. All elements are interconnected within a closed-loop automated response cycle (detect → analyze → respond → document), operating in real time without manual operator intervention [17].

The model is adapted to multi-cloud infrastructures comprising more than 400 cloud accounts across AWS, Azure, and GCP, accounting for typical characteristics such as asset distribution, dynamic scaling, and heterogeneous authentication and access control policies [27]. The architecture follows the principles of Zero Trust, ensuring isolation of environments, real-time verification of every access request, and dynamic privilege management.

From a practical standpoint, the system enables a timely response to incidents such as:

1. Credential compromise due to leaked secrets or unauthorized access [11].
2. Detection of geographic or session behavioral anomalies [13].
3. Unauthorized infrastructure modification or policy violations.
4. Execution of suspicious API requests or privilege escalation attempts [24].

When an incident occurs, the system automatically detects the risk using Prisma Cloud, generates an event in Splunk, which is then transformed via a playbook into an infrastructure-level response action (e.g., VPC or IAM blocking), initiates secure retrieval of temporary credentials via Vault, and executes the action using Jenkins. All stages are logged, and a post-incident report is generated upon completion [14, 15, 22].

4.6.1. Implementation results

The practical value of this model lies in its ability to provide centralized incident management across an environment with over 400 cloud accounts. According to IBM's Cost of a Data Breach Report 2023, the average cost of a cloud data breach is $4.45 million [29], and the dwell time (i.e., time an attacker remains undetected in a system) may exceed 20–30 days [32]. The implemented model reduces dwell time to a few hours, shortens Mean Time to Detect (MTTD) to minutes, and decreases Mean Time to Respond (MTTR) to hours, collectively reducing financial risk by more than 80% compared to manual incident handling [28].

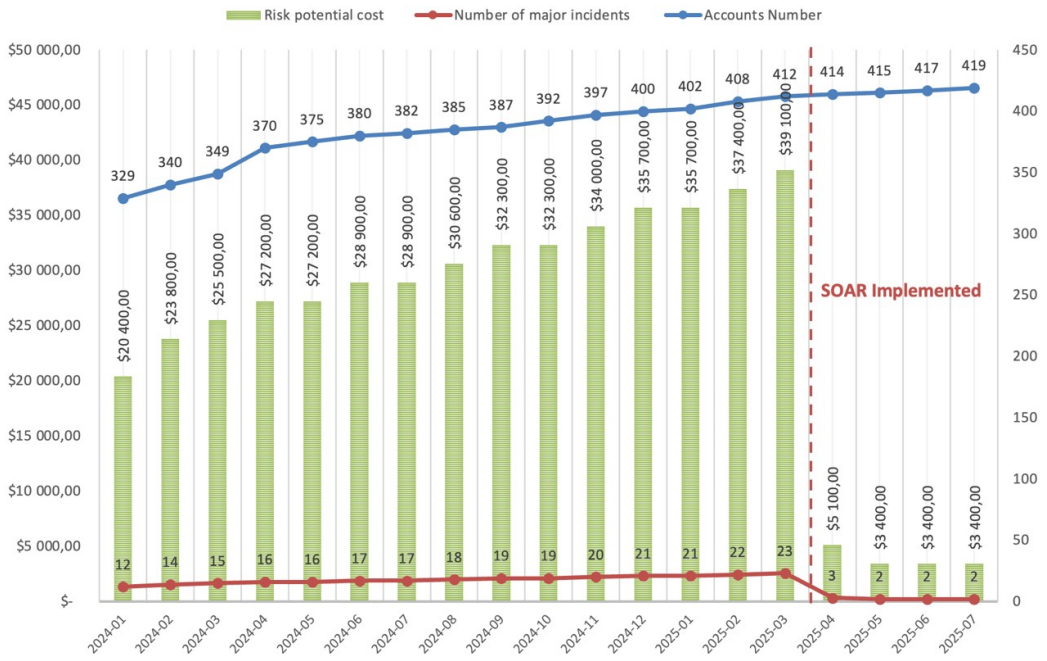

Figure 2: Reducing the Cost of risks after SOAR implementation

The proposed solution was deployed within a complex multi-cloud environment encompassing three major public cloud platforms—Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)—with the total number of active accounts reaching 419 by mid-2025. This environment was specifically chosen to mirror the scale and operational diversity of real-world enterprise infrastructures, providing a representative foundation for a 19-month empirical evaluation of the performance, adaptability, and scalability of the automated incident response model based on SOAR principles.

Prior to the implementation of the solution in March 2025, the security operations center (SOC) was predominantly reliant on manual incident processing. During this period, the average monthly

exposure to cloud-related risks fluctuated between $20,000 and $39,000, driven by a persistent stream of 12 to 23 major incidents each month. These incidents were primarily associated with unauthorized access attempts, leakage of sensitive secrets, misconfigurations of cloud-native services, and the absence of real-time detection mechanisms. The lack of standardization, automation, and cross-cloud visibility not only delayed the response process but also imposed a significant cognitive load on first-line analysts. As a result, the estimated annual potential financial impact exceeded $370,000.

To address these operational inefficiencies, an integrated incident response model leveraging Prisma Cloud for threat detection and Splunk SOAR for orchestration and automation was implemented in March 2025. This architecture enabled the real-time ingestion and correlation of telemetry data from heterogeneous cloud environments, execution of automated playbooks for critical incident types, validation of user actions against security policies, and escalation-free handling of common security scenarios. The transformation from a reactive to a semi-autonomous response workflow significantly accelerated decision-making and reduced false-positive rates.

Within just four months following deployment, the number of major incidents dropped dramatically to 2–3 per month, and the estimated financial exposure decreased to a range of $3,400–$5,100 monthly (see Figure 2). This sharp decline in both operational noise and financial risk clearly demonstrates the practical effectiveness of the solution in mitigating high-frequency, high-impact threats. Based on historical expenditure trends, the total savings achieved during this initial post-deployment phase exceeded $130,000, despite the relatively short observation window. These results affirm the economic viability and strategic value of integrating automated response mechanisms into large-scale, dynamic cloud environments, particularly in organizations facing increasing demands for compliance, visibility, and operational resilience.

4.6.2. Economic feasibility of implementing an automated response model in a multi-cloud environment

The deployment of the proposed architecture for automated incident response in a multi-cloud environment has demonstrated not only technical viability, but also a high level of economic efficiency. The real-world deployment scenario encompassed three major public cloud platforms—AWS, Azure, and GCP—with an overall scale of 419 cloud accounts, which reflects typical enterprise-level complexity and variability.

To validate the financial soundness of the implemented SOAR-based model, a comprehensive cost–benefit analysis was performed covering a 12-month period before and after implementation. The assessment incorporated both direct costs (such as SOC analyst salaries, incident-related damages, and downtime) and indirect costs (including service unavailability, loss of productivity, and system recovery efforts). Capital and operational investments associated with software and automation tools—such as Prisma Cloud, Splunk SOAR, Jenkins, and Vault—were categorized according to CAPEX and OPEX accounting standards.

Table 6
Comparative evaluation of economic efficiency before and after SOAR implementation

Indicator	Before SOAR Implementation (2025)	After SOAR Implementation	Change %
Number of major incidents (per month)	23	2	91.3
Risk potential cost (USD year)	370000	50000	83.3
Total annual incident-related losses (USD millions/ year)	6.9	0.55	92
Annual cots of SOC analyst expenses (USD year)	720000	540000	25
Investment in SOAR solution (USD)	—	380000 (one-time)	—

As shown in Table 6, the average number of major monthly incidents decreased from 23 to just 2, a 91.3% reduction. The annual risk potential cost dropped from $370,000 to $50,000, representing an 83.3% decrease. Total estimated annual losses fell dramatically from $6.9 million to $550,000 (a 92% reduction), largely due to faster containment, improved detection accuracy, and lower false positive rates enabled by the new automated response framework.

Additionally, the annual operational costs associated with SOC analyst teams were reduced by 25%, from $720,000 to $540,000, due to decreased workload and automation of standard incident response scenarios. The one-time investment in the SOAR solution amounted to $380,000.

Taken together, these results indicate that the total cost savings achieved in the first year of operation exceeded $6 million, yielding a full return on investment (ROI) in under three months. This clearly demonstrates the financial feasibility of scaling the SOAR-based automated response model across large-scale multi-cloud environments. These findings reinforce the strategic importance of integrating automation into cloud security operations for both risk mitigation and operational efficiency.

4.6.3. Future development directions

Future development of the model is expected along the following strategic directions:

1. Integration of AI/ML analytics. The use of machine learning algorithms will improve incident prioritization, reduce false positives, and enable dynamic adaptation of response strategies based on behavioral patterns, time of day, and access level [26].
2. UEBA (User and Entity Behavior Analytics). Implementing behavioral analysis of users and services will help detect covert attacks, lateral movement, use of dormant accounts, and non-obvious anomalies that traditional signature-based systems may miss [25].
3. Deepening the Zero Trust model. The system will be enhanced to incorporate dynamic access control, conditional authorization, micro-segmentation of cloud infrastructure, and strict inter-region traffic controls [8].
4. Post-incident automation and self-analysis. Mechanisms for automatic post-mortem analysis of incidents will be developed to not only record events but also build causal graphs, offer security policy improvement suggestions, and dynamically update playbooks [16].
5. Audit and metrics-based control. Advanced reporting systems and dashboards monitoring key security metrics (MTTD, MTTR, dwell time, alert fatigue level, compliance coverage rate) will allow organizations to transparently track system effectiveness, ensure regulatory compliance (SOC 2, ISO/IEC 27001, NIST 800-53), and prepare for external audits [10, 33].
6. Extending playbook adaptability. Leveraging branching mechanisms and contextual response capabilities in Splunk SOAR, dynamic response scenarios can be implemented, automatically considering resource type, event context, data sensitivity, and business process criticality [14].

The proposed model not only meets modern requirements for response agility, process automation, and regulatory compliance, but also lays the foundation for an evolving, intelligent, self-learning cloud security architecture based on the principles of Data-Driven Security and Continuous Adaptive Risk and Trust Assessment [1].

Conclusions

Within the scope of the study, an architectural model for automated security incident management in public cloud environments was developed based on the integration of Prisma Cloud, Splunk SOAR, Jenkins, and HashiCorp Vault. The proposed model enables end-to-end automation of the incident response cycle—from anomaly detection to execution of corrective infrastructure actions—without operator intervention. This approach significantly reduces response time (MTTR),

minimizes human factor influence, and mitigates the risks associated with prolonged attacker presence in the environment.

The analysis of real-world cloud compromise cases revealed that the main pain points include the lack of effective monitoring, weak authentication controls, absence of event correlation, and inability to respond to incidents promptly. The proposed solution addresses these vulnerabilities through flexible playbook-based logic, integration with threat intelligence sources, and activity control enabled by a Zero Trust model.

The scientific novelty of the research lies in the synthesis of SOAR principles, Zero Trust, ML analytics, and UEBA into a unified architecture adapted to a multi-cloud infrastructure comprising over 400 cloud accounts. The developed model not only automates incident response but also enables scalable security policy enforcement without losing control, which is critical for modern enterprises managing large numbers of cloud assets.

From a practical perspective, the implementation of the described solution allows organizations to reduce the risk of financial losses related to cloud environment compromises. Based on the applied risk assessment model, it is estimated that the absence of automated incident management may result in annual losses reaching hundreds of thousands of dollars due to response delays, data leakage, and system downtime.

Future research directions include enhancing behavioral incident analysis mechanisms using machine learning methods, expanding platform support through dynamic API integration, and implementing self-learning capabilities based on historical response scenarios. Additionally, a formalized approach to regulatory compliance (NIST, ISO, SOC 2) via automated auditing and policy enforcement control is recommended.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] O. Vakhula, I. Opirskyy, O. Mykhaylova, Research on Security Challenges in Cloud Environments and Solutions based on the "Security-as-code" Approach, in: Cybersecurity Providing in Information and Telecommunication Systems, 3550, 2023, 55–69.

[2] S. Vasylyshyn, V. Susukailo, I. Opirskyy, Y. Kurii, I. Tyshyk, A Model of Decoy System based on Dynamic Attributes for Cybercrime Investigation, Eastern-European J. Enterp. Technol., 1.9(121) (2023) 6–20. doi:10.15587/1729-4061.2023.273363

[3] Y. Kostiuk, et al., A System for Assessing the Interdependencies of Information System Agents in Information Security Risk Management using Cognitive Maps, in: 3rd Int. Conf. on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN), Kyiv, Ukraine, vol. 3925, 2025, 249–264.

[4] Y. Kostiuk, et al., Models and Algorithms for Analyzing Information Risks during the Security Audit of Personal Data Information System, in: 3rd Int. Conf. on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN), Kyiv, Ukraine, vol. 3925, 2025, 155–171.

[5] S. Shevchenko, et al., Information Security Risk Management using Cognitive Modeling, in: Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II, vol. 3550 (2023) 297–305.

[6] S. Shevchenko, et al., Protection of Information in Telecommunication Medical Systems based on a Risk-Oriented Approach, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 158–167.

[7] I. Hanhalo, et al., Adaptive Approach to Ensuring the Functional Stability of Corporate Educational Platforms under Dynamic Cyber Threats, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3991 (2025) 481–491.
[8] K. Suram, Innovations in Infrastructure Automation: Advancing IAM in Cloud Security, Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., 11 (2025) 255–263. doi:10.32628/CSEIT25111223
[9] Y. Martseniuk, A. Partyka, O. Harasymchuk, S. Shevchenko, Universal Centralized Secret Data Management for Automated Public Cloud Provisioning, in: Cybersecurity Providing in Information and Telecommunication Systems II, 3826, 2024, 72–81.
[10] Y. Martseniuk, A. Partyka, O. Harasymchuk, E. Nyemkova, M. Karpinski, Shadow IT Risk Analysis in Public Cloud Infrastructure, in: Cyber Security and Data Protection, 3800, 2024, 22–31.
[11] V. S. Thokala, Scalable Cloud Deployment and Automation for e-Commerce Platforms using AWS, Heroku, and Ruby on Rails, Int. J. Adv. Res. Sci. Commun. Technol. (2023) 349–362. doi:10.48175/IJARSCT-13555A
[12] D. Soldatenko, Study of Efficiency of using IT-Infrastructure-as-a-Service for Cloud computing, System Technol., 2 (2022) 68–76. doi:10.34185/1562-9945-2-139-2022-07
[13] D. Narayanasamy, Transforming Healthcare with Secure Cloud Infrastructure, Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., 11 (2025) 633–644. doi:10.32628/CSEIT25111271
[14] P. Narayanan, Engineering Data Pipelines using Google Cloud Platform, 2024. doi:10.1007/979-8-8688-0602-5_16
[15] A. Sreerangapuri, Blockchain-enabled AI Governance for Scalable Cloud Security Automation, Int. J. Comput. Eng. Technol., 15 (2024) 947–959. doi:10.5281/zenodo.13962366
[16] O. Deineka, O. Harasymchuk, A. Partyka, A. Obshta, Application of LLM for Assessing the Effectiveness and Potential Risks of the Information Classification System According to SOC 2 Type II, in: Cybersecurity Providing in Information and Telecommunication Systems, 3991, 2025, 215–232.
[17] J. Ramya, Data-Driven Framework for Cloud Storage Security Optimization: Leveraging Predictive Analytics and Machine Learning to Enhance Threat Detection and Incident Response, J. Electr. Syst., 20 (2024) 6646–6653. doi:10.52783/jes.6721
[18] O. Harasymchuk, O. Deineka, A. Partyka, V. Kozachok, Information Classification Framework According to SOC 2 Type II, in: Cybersecurity Providing in Information and Telecommunication Systems II, 3826, 2024, 182–189.
[19] O. Milov, et al., Development of Methodology for Modeling the Interaction of Antagonistic Agents in Cybersecurity Systems, Eastern-European J. Enterp. Technol., 2.9(98) (2019) 56–66. doi:10.15587/1729-4061.2019.164730
[20] D. Shevchuk, O. Harasymchuk, A. Partyka, N. Korshun, Designing Secured Services for Authentication, Authorization, and Accounting of Users, in: Cybersecurity Providing in Information and Telecommunication Systems II, 3550, 2023, 217–225.
[21] K. Torkura, M. I. H. Sukmana, F. Cheng, C. Meinel, Continuous Auditing & Threat Detection in Multi-Cloud Infrastructure, TechRxiv, 2020. doi:10.36227/techrxiv.13108313
[22] Y. Martseniuk, A. Partyka, O. Harasymchuk, V. Cherevyk, N. Dovzhenko, Research of the Centralized Configuration Repository Efficiency for Secure Cloud Service Infrastructure Management, in: Cybersecurity Providing in Information and Telecommunication Systems, 3991, 2025, 260–274.
[23] J. Christian, L. Paulino, A. Sá, A Low-Cost and Cloud Native Solution for Security Orchestration, Automation, and Response, 2022. doi:10.1007/978-3-031-21280-2_7
[24] H. Rehan, Zero-Trust Architecture for Securing Multi-Cloud Environments, (2022) 236–273.
[25] J. Smith, E. Johnson, R. Patel, G. Christopher, Enhancing Cloud Security Incident Response with AI and Big Data Integration, 2023.
[26] P. Varadaraj, Multi-Cloud and Hybrid Infrastructure: Addressing Consistency Challenges Across Cloud Providers, Int. J. Adv. Res. Sci. Commun. Technol. (2025) 520–526. doi:10.48175/IJARSCT-24465

[27] M. Abbas, J. Iqbal, Autonomous Threat Response Systems: A New Paradigm for Intelligent Cloud Security Automation, 2025. doi:10.13140/RG.2.2.13750.20800

[28] A. Mahida, Real-Time Incident Response and Remediation—A Review Paper, J. Artif. Intell. Cloud Comput. (2023) 1–3. doi:10.47363/JAICC/2023(2)247

[29] V. Jangampet, S. Pulyala, A. Desetty, The Impact of Security Orchestration, Automation, and Response (SOAR) on Security Operations Center (SOC) Efficiency: A Comprehensive Analysis, Turk. J. Comput. Math. Educ., 10 (2019) 1545–1549. doi:10.61841/turcomat.v10i3.14323

[30] R. Vast, S. Sawant, A. Thorbole, V. Badgujar, Artificial Intelligence based Security Orchestration, Automation and Response System, (2021) 1–5. doi:10.1109/I2CT51068.2021.9418109

[31] Ismail, R. Kurnia, Z. Brata, G. Nelistiani, S. Heo, H. Kim, H. Kim, Toward Robust Security Orchestration and Automated Response in Security Operations Centers with a Hyper-Automation Approach using Agentic Artificial Intelligence, Information, 16 (2025) 365. doi:10.3390/info16050365

[32] O. Mercy, Holistic Security Solutions for Complex Multi-Cloud Ecosystems, Int. J. Novel Res. Dev. (2023).

[33] H. Pitkar, Cloud Security Automation through Symmetry: Threat Detection and Response, Symmetry, 17 (2025) 859. doi:10.3390/sym17060859