УДК 004.056

Martseniuk Y., postgraduate student
Lviv Polytechnic National University

BUILDING A SERVICE CATALOGUE FOR CLOUD SECURITY. HOW TO SET UP CLOUD SECURITY SERVICES: ACCESS PROVISIONING, AUTOMATED IR, CSPM/DSPM, DATA CLASSIFICATION, ENCRYPTION-AS-A-SERVICE

Abstract

The rapid growth of public and hybrid cloud infrastructures is reshaping information security approaches. As organizations migrate sensitive data and critical workloads to the cloud, risks caused by misconfigurations, inconsistent access control, and limited visibility increase. Traditional security methods are insufficient, creating a need for standardized and automated controls.

A cloud security service catalogue provides a unified framework that defines core security services, their scope, responsibilities, and automation workflows. This paper examines key catalogue components - access provisioning, automated incident response, CSPM/DSPM, data classification, and encryption-as-a-service - and shows how they collectively strengthen cloud security by enabling consistency, automation, and integrated risk management.

Keywords: Service Catalogue, Access Provisioning, Automated Incident Response, CSPM/DSPM, Data Classification, Encryption-as-a-Service

1. Introduction

1.1. Service catalog in cloud security

The growing complexity of cloud infrastructures requires a systematic approach to security management. A security services catalogue is a standardised repository of cloud security services that describes their structure, automation, monitoring, and control. It defines clear rules for how services work: scope, roles, responsibilities, workflows, service levels, and necessary tools. This unification reduces fragmentation, improves configuration consistency, simplifies integration with DevOps/DevSecOps, and provides better visibility and scalability of security practices.

1.2. Problem statement, hypothesis, and research objective

Problem statement

Cloud environments often lack unified management: access, data protection, encryption, and incident response are implemented differently across different teams. This leads to misconfigurations, loss of visibility,

automation complexity, and increased risks. The lack of a service catalogue makes it impossible to standardise and predict security controls.

Hypothesis

If a clearly defined and standardized cloud security services catalogue (access, automated response, CSPM/DSPM, data classification, encryption) is implemented, security processes will become consistent, automated and measurable. This will reduce incidents due to misconfigurations, improve risk detection, and increase control over cloud environments.

Research objective

Create a structured model for developing a cloud security services catalogue that defines the roles, automation level, and operational processes of key security services. The goal is to show how such a catalogue improves management, supports compliance with standards, strengthens risk management, and integrates with DevSecOps in dynamic clouds.

2. Methodological basis for building the catalogue

The cloud security service catalog is built on principles, standards, and operational models that define how security services are delivered and automated. Its methodology ensures both a clear structure and compliance with security requirements, corporate policies, and international standards.

2.1. Basic principles of catalogue construction

Table 1. Basic principles of catalogue construction

Zero trust principle	The service catalogue is built based on the zero trust concept, which assumes no trust in any user or resource by default. All services must provide for identity, context, and policy compliance verification.
Least privilege and separation of duties	Each service in the catalogue must take into account the principle of least privilege and separation of duties. This is especially important for access provisioning, DSPM, and cryptographic services.
Policy-as-code	Cloud security services must be described by policies that can be executed automatically (Terraform, Open Policy Agent, AWS SCP). This ensures repeatability, verification, and control.
Automation and orchestration	The catalogue should be geared towards full or partial automation of security processes: from problem detection to response. This is the basis for automated IR, CSPM, and DSPM.

2.2. Shared responsibility model

The catalogue reflects the shared responsibility model, defining which security aspects the cloud provider handles and which are the organisation's responsibility. The provider secures physical infrastructure, hypervisors, and networks, while the customer manages cloud configurations, access, data

classification, and encryption. The catalogue formalises these boundaries and covers gaps on the customer side.

2.3. The role of international standards

When compiling the catalogue, it is necessary to focus on the requirements and recommendations of global standards, such as:

- NIST SP 800-53 - control measures for information systems.
- ISO/IEC 27001 - requirements for information security management systems.
- CIS Benchmarks - best practices for configuring cloud resources.
- GDPR / HIPAA / PCI-DSS - regulatory requirements for data processing.

The catalogue should include services that ensure compliance with these requirements (e.g., data classification or encryption-as-a-service for GDPR).

2.4. DevSecOps as an operational model

The catalogue integrates with DevSecOps, becoming part of the CI/CD pipeline. It enables automatic IaC verification, configuration checks via CSPM, continuous access monitoring, and incident response through SOAR, ensuring security before deployment.

2.5. Risk-based approach

The security catalogue is built taking into account the criticality levels of data and environments. For example:

Table 2. Critical levels of data and environments

Dev	minimum requirements (no sensitive data)
Prod	maximum protection, DSPM + CSPM + EaaS

This allows services to be adapted to the level of risk without complicating processes where it is not necessary.

3. Description of key cloud security services in the service catalog

This section defines the core security services included in the cloud security service catalog. Each service describes a standardized security function that supports consistent protection, automation, and governance across cloud environments.

3.1. Access provisioning

Access provisioning aims to eliminate excessive permissions, prevent orphaned accounts, and standardise access in the cloud. The service provides controlled access based on the principles of least privilege and zero trust, automatically grants and revokes access to users, service accounts, and

workloads, verifies policies as code, and integrates with key and secret management systems.

3.2. Automated incident response

Automated incident response reduces MTTR and standardises incident response through automated scripts. The service automatically corrects misconfigurations, isolates suspicious resources, forces key rotation, quarantines anomalous activity, and integrates with SIEM, CSPM, DSPM, and SOAR pipelines.

3.3. CSPM / DSPM

CSPM/DSPM provide comprehensive visibility into risks at the infrastructure and data levels.

- CSPM continuously checks cloud configurations, detects errors, scans IaC, compares parameters with CIS, NIST, and ISO 27001, and supports automatic remediation.
- DSPM locates data, classifies sensitive information, analyses access patterns and exposure risks.

Together, they provide context: DSPM finds sensitive data → CSPM identifies its dangerous exposure → automated IR responds.

3.4. Data classification

Data classification ensures that data sensitivity is correctly identified and appropriate controls are applied. The service performs automatic content analysis (ML, patterns, context), assigns tags, integrates with DLP/DSPM, correlates data types with GDPR, HIPAA, PCI-DSS requirements, and applies access, storage, and encryption policies.

3.5. Encryption-as-a-service

Encryption-as-a-service ensures consistent and correct application of encryption across all cloud environments. It centralises key management (KMS, HSM), automates rotation, provides encryption of storage, databases, traffic and backups, and provides auditing of cryptographic operations.

4. Integrated model of service interaction in the cloud security catalog

The cloud security service catalogue operates as an integrated system where services reinforce each other and form an automated security perimeter: access control, data protection, configuration monitoring, and response.

4.1. Inter-service interaction

The services interact in a logical sequence:

- Access provisioning sets permissions and least privilege principles.
- DSPM assesses how these permissions affect access to sensitive data.

- CSPM correlates data risks with configuration errors.
- Automated IR performs automated remediation based on DSPM/CSPM signals.

This creates a continuous risk management flow: identity → data → configurations → response.

4.2. Automated security cycle

The model operates cyclically, minimising manual work and unifying control across different environments.:

1. **Detection**: DSPM identifies sensitive data and suspicious access.
2. **Classification**: data is tagged (PII, PHI, financial, etc.).
3. **Risk assessment**: CSPM checks resource compliance with policies.
4. **Response**: automated IR isolates resources, restricts access, updates keys, and corrects configurations.

To ensure coordinated operation of the cycle, the services have the following dependencies:

- DSPM transmits sensitivity metadata to CSPM and IR;
- CSPM uses access policies from Access Provisioning;
- Automated IR applies standardised playbooks linked to DSPM/CSPM results;
- Events (unauthorised access, data exposure, configuration errors) automatically trigger appropriate actions.

These dependencies create a unified, predictable, and scalable security model that aligns identity, data, configuration, and incident workflows into a single operational framework.

5. Practical challenges and issues

Table 3. Practical challenges and issues

Multicloud and API diversity	Different cloud platforms have their own APIs, access models, and log formats. This complicates the unification of CSPM/DSPM, automation configuration, and maintenance of consistent security policies.
Inconsistent policies across teams	Teams take different approaches to access, tagging, and configurations. Without a policy catalogue, policies remain fragmented, creating the risk of excessive privileges and non-compliance with standards.
Data quality issues for classification	Incomplete or missing tags, duplicate data, and lack of structure all reduce the accuracy of automatic classification and DSPM analysis.

False positives in CSPM/DSPM	A large number of false or low-priority alerts leads to 'alert fatigue.' Rule configuration and contextual correlation are essential for reducing noise.
Automation risks in production	Automated actions (resource isolation, key rotation, IAM policy changes) can cause production failures if they do not include validation or rollback mechanisms.

6. Conclusions

The expansion of cloud environments demands a standardized rather than fragmented approach to security. A cloud security service catalogue provides this structure by unifying core services, defining consistent workflows, and centralizing the enforcement of security policies. Although practical challenges remain - such as multicloud complexity and automation risks - the catalogue offers a predictable and scalable operational model to address them.

The analysis confirms that a well-designed catalogue improves visibility, strengthens risk management, and supports automation across modern cloud environments. As data volumes and infrastructure complexity continue to grow, the role of CSPM/DSPM and automated workflows will become increasingly fundamental for resilient cloud security.

References

1. James, Liam. (2026). Zero Trust Architecture Integration with NIST CSF for Resilient and AI-Augmented Critical Infrastructure Defense.

2. James, Liam. (2026). Adaptive Zero Trust Architecture for Critical Infrastructure Protection Using AI-Powered Threat Detection and NIST-Compliant Governance Models.

3. Ilochonwu, Ifeanyi. (2024). Information Technology Governance in Cloud Computing: A Framework of Risk Management and Compliance. Volume 11. pp:591-602.

4. ISO/IEC 27001:2022. (n.d.). ISO. https://www.iso.org/standard/27001

5. Jimmy, FNU. (2023). Cloud security posture management: tools and techniques. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online). 2. 10.60087/jklst.vol2.n3.p622

6. AWS Security Reference Architecture (AWS SRA) – core architecture - AWS Prescriptive Guidance. (n.d.). https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/introduction.html