23.5. Logging and Alerting in Public Cloud

Objective

23.5.1. Security-related events are recorded from across an agency's public cloud platforms and are able to be analysed for timely notification of potential threats or incidents.

Context

Scope

23.5.2. This section describes the requirements for capturing security-related information from public cloud services by examining electronic logs for indications that unauthorised security-related activities have been attempted or performed.

23.5.3. Reference to other chapters and sections in this document is essential. In particular:

- Section 7.1 – Detecting information security incidents
- Section 16.6 – Event logging and auditing

Logging

23.5.4. Appropriate ongoing logging is vital for detecting threat actor activity occurring within agency public cloud environments.

23.5.5. Public cloud introduces particular aspects of logging that agencies must consider, including:

- Responsibility for logging and detecting anomalies is shared between the agency and its cloud service provider.
- Cloud services may introduce differences in what information is able to be logged, where it can be logged, and in what format the log messages are constructed. It may not be possible for the consuming agency to customise logging parameters.
- Key security components used by cloud services may be sourced from multiple providers (e.g., identity federation or SaaS integration). Effective log monitoring and incident investigation requires these logs to be accessible and be able to be correlated with each other.
- Some components of the environment where logs are traditionally collected may not be available in cloud environments (e.g., network traffic or boundary devices), or the information may need to be collected in different ways.
- Only a subset of log information may be able to be exported from a cloud environment due to technical or cost implications.

23.5.6. Agencies running across multiple clouds or running a hybrid of public cloud and on premise infrastructure must also balance the advantages of platform-specific capabilities against the need for centralised visibility. Centralised visibility does not necessarily require centralised log aggregation, but agencies must be able to track and correlate activity across all the log sources available to them.

Alerting

23.5.7. While logging is vital for detecting threat actor activity occurring across agency public cloud systems, in isolation it does not provide a detection capability and must be paired with appropriate analysis and alerting tools.

References

23.5.8. Further references can be found at:

Reference	Title	Publisher	Source
	CSA Security Guidance for Critical Areas of Focus in Cloud Computing	CSA	CSA Security Guidance for Cloud Computing | CSA (cloudsecurityalliance.org)

PSR References

23.5.9. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR mandatory requirements	GOV2 - Take a risk-based approach GOV5 - Manage risks when working with others GOV6 - Manage security incidents INFOSEC1 - Understand what you need to protect INFOSEC2 - Design your information security INFOSEC3 - Validate your security measures INFOSEC4 - Keep your security up to date	Mandatory requirements | Protective Security Requirements
PSR protocol for information security	Management protocol for information security	Management protocol for information security | Protective Security Requirements

Rationale & Controls

Logging public cloud events

23.5.10.R.01. **Rationale**

Logging capabilities and shared responsibility models for log collection, storage, and retention differ between public cloud providers. The division of responsibility may also vary across different deployment models and the individual services within a cloud platform.

23.5.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7494]

Agencies MUST understand the range of logging capabilities provided by their cloud service providers and determine whether they are sufficient for agency needs.

Logging requirements

23.5.11.R.01. **Rationale**

It may not be possible, or desirable, to centralise all public cloud log information into a single protected repository. However it is vital that log information is still collected and maintained to meet legislative, regulatory and incident response requirements (see 16.6.8 - Logging requirements).

23.5.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7496]

Agencies MUST ensure that logs associated with public cloud services are collected, protected, and that their integrity can be confirmed in accordance with the agency's documented logging requirements.

Detecting information security incidents in public cloud

23.5.12.R.01. **Rationale**

Specialised tools and procedures may be required to detect security incidents that occur within public cloud environments (See 7.1.7 - Preventing and detecting information security incidents).

23.5.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7498]

Agencies MUST ensure that cloud service provider logs are incorporated into overall enterprise logging and alerting systems or procedures in a timely manner to detect information security incidents.

23.5.12.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7499]

Agencies SHOULD ensure that tools and procedures used to detect potential information security incidents account for the public cloud services being consumed by the agency.