Australian Government
Australian Taxation Office

Digital Service Provider (DSP) Operational Framework Review

Fraud Detection & Monitoring Focus Group – Session 2

Presented by Diana Porter

7th April 2021

Recap - What are we trying to achieve?

To improve information security documentation relating to fraud detection and monitoring controls

1 Expanding Security Monitoring

Explore benefits in expanding scope of security monitoring control to all DSP controlled cloud environments.

2 Preservation and Retention of Log Data

Improved guidance on:

- Protection and preservation of audit logs.
- Retention periods that align to legislative requirements.
- Accessing information to share in the case of a security incident.

3 Breach Notification Guidance

Improve process and guidance to assist DSPs:

- Respond to breaches.
- Notify and report a security breach.
- With incident response and fraud investigations.
- With supporting information for clients.

1 Expanding Security Monitoring

1 Expanding Security Monitoring

REVIEW CONSIDERATIONS

Commercial impacts to be considered for smaller DSPs.

Uplift is 'good for industry'.

ATO to establish the baseline controls.

CURRENT ENVIRONMENT – APPLICATION AND SUPPORTING GUIDANCE

DSP Operational Framework Requirements to utilise ATO digital services (pg. 21-22)

DSP controlled environments with less than 10,000 client records and consuming low risk APIs do not require security monitoring.

Security monitoring practices

This requirement seeks to detect and respond to cyber-attacks, channel misuse and business threats. Monitoring is a joint responsibility between the ATO and you as the DSP. Where relevant you need to be able to demonstrate that you scan your environment for threats and that you take appropriate action where you detect anomalies.

Evidence required
Network / infrastructure layer - relevant combinations of:

- Screen shots of an intrusion detection system or firewall that generates alerts.
- Photos of your Security information and event management dashboard.
- If leveraging off a cloud provider you can provide either an invoice or screenshot from within the environment showing the type of monitoring captured.

Application layer – relevant combinations of:

Screen shots of the function page in the application, and reports from the backend system.

Transaction (data) layer – relevant combinations of:

Reports from the backend system and screenshots of an anomaly detection system.

1 Expanding Security Monitoring

REVIEW CONSIDERATIONS

Commercial impacts to be considered for smaller DSPs.

Uplift is 'good for industry'.

ATO to establish the baseline controls.

UPDATE TO APPLICATION & SCOPE OF CONTROL

DPO will uplift this control to all DSP controlled environments.

UPDATE TO SUPPORTING GUIDANCE

Security Monitoring

This requirement seeks to minimise the risk and impact of cyber incidents by having controls in place to detect, prevent and respond to cyber-attacks.

You must demonstrate appropriate monitoring of networks, applications and transactions is in place.

Evidence requirements

- Screenshot of an intrusion detection system such as a firewall that generates alerts.
- Approach to detect anomalies or a screenshot of a security event and incident management dashboard.
- Intrusion prevention system which protects end points and scans the DSP environment to prevent malicious events.

2 Preservation and Retention of Log Data

2 Improved Guidance on Retention and Preservation of Audit Logs

REVIEW CONSIDERATIONS

Specific guidance on expectations of log preservation

Mapping to industry standards will improve guidance and assist DSPs make risk based decisions

ATO to establish the baseline controls

CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg. 14)

This requirement seeks to ensure traceability of access and actions.

Audit logging should include both application level (access logs) and event based actions. Audit logs are not required to be submitted to the ATO on a regular or ongoing basis. You will need to be able to access or supply the logs on the occurrence of a security event where further investigation of the data is required.

You should consider your environment and what logging should be implemented and ensure that the logging records include the following where applicable:

- Date and time of the event
- Relevant user or process
- Event description
- Success or failure of the event
- Event source e.g. application name
- ICT equipment location and identification
- Data identifiers (product ID, Tax File Number (TFN)).

Evidence required

- Sample of a dummy audit log in CSV format.
- A data dictionary that describes the data attributes and maps against key audit log components.

2 Improved Guidance on Retention and Preservation of Audit Logs

REVIEW CONSIDERATIONS

Specific guidance on expectations of log preservation

Mapping to industry standards will improve guidance and assist DSPs make risk based decisions

ATO to establish the baseline controls

UPDATE TO SUPPORTING GUIDANCE

This requirement seeks to ensure traceability of access and actions within software which can be used for detection of anomalies or to support investigation of a security incident.

You must at a minimum capture authentication and authorisation events, privilege escalations events and events within your software which will ensure an end-to-end audit trail. Each individual user will need to be identifiable through audit logs.

At a minimum the logs will need to capture all of the below fields:

- Date and time of the event
- User or process
- Success or failure of the event
- Event description
- ICT equipment location and identification

In DSP controlled environments DSPs must ensure logs are reviewed regularly and where possible sensitive information from audit logs to be removed and DSP staff are trained on how to access logs.

We recommend DSPs adopt a risk based approach in implementing controls from the Australian Cyber Security Centre guidelines for system monitoring or an industry standard or equivalent such as the NIST - Guide to Computer Security Log Management.

Evidence required

- Audit logging policy
- Dummy authentication/authorisation, privilege escalations and event logs.
- Data dictionary that describes data attributes and maps against key audit log components.

3 Breach Notification Guidance

3 Breach Notification Guidance

REVIEW CONSIDERATIONS

The timeframe to report should align to an industry standard

Guidance on risk thresholds for reporting breaches

Clarification on actions taken by ATO

CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg. 24-25)
DSP Operational Framework terms and conditions (pg. 30)
DSP de-whitelisting process major and moderate security incident (pg. 5-6)

What's the process?

DSPs to raise a ticket through online services for DSPs, notify account manager or through DPO@ato.gov.au.

What is required?

Information to provide includes:

- Appropriate contact person (specialist IT security/fraud representative)
- Nature of the incident
- Number of affected records
- Date and timestamp
- Session ID reference
- Host Services (Internet Service Provider)/IP address
- Device ID (ESID) if available
- TFN information
- Non-TFN information (name/address/biographical information)
- Product name and type (desktop or cloud)
- What format the data was in (e.g. CSV or encrypted)

3 Breach Notification Guidance

REVIEW CONSIDERATIONS

The timeframe to report should align to an industry standard

Guidance on risk thresholds for reporting breaches

Clarification on actions taken by ATO

UPDATES

Streamlined process to report a security breach ticket in online services for DSPs

- Removal of duplicated fields.
- Removal of fields which have not been used in the past 12 months.
- Modification of fields to provide clarity of requested information.

Changes to Breach notification guidance

- Updates to documentation to include when, timeframe & how to notify the ATO and what action ATO will take.
- Additional content to be added into the Knowledge base of Online Services for DSPs to assist in developing a data breach response plan with industry references i.e. OAIC - Data breach preparation and response and ISO 31000.

NEW - Breach reporting matrix

- The matrix will establish a tiered approach for timeframe to report breaches.
- Provide clarity on when a DSP is required to notify of a security incident.
- Provide factors and examples to assist DSPs determine timeframe to report i.e. breach of TFN or bank account.

Open Discussion & Thankyou

Actions & support for working group

- Do the changes meet the overarching aim of the intent to improve information security documentation relating to fraud detection and monitoring controls?
- Will changes address specific outcomes relating to:
  - Expanding security monitoring
  - Preservation and retention of audit logs
  - Breach notification guidance
- Are there any other concerns or gaps we haven't been able to address?
- Closure of Fraud Detection & Monitoring Focus Group?

Next steps

1. Incorporate feedback and finalise changes within the draft requirements documentation.
2. DPO will provide draft requirement documentation for review by the Operational Framework Review working group.