Tenant response worksheet

One record per tenant. Times in UTC. Leave unknowns explicit.

Tenant name / tenant ID

Owner / team

Opened (UTC)

Last updated (UTC)

Case / ticket reference

01 Local app containment evidence

Application ID

Local service-principal object ID

Connection / app name

Disabled status and time (UTC) / evidence reference

02 Evidence coverage

Use distinct states: Records available / No matching events / Not collected or expired

Record source	Earliest / latest (UTC)	State / known gap
Service-principal sign-ins		
Directory audit		
Microsoft Graph activity		
Purview / resource logs		

03 Findings

Actor / app	Operation / target	Result	Event / correlation ID

Tenant response worksheet

One record per tenant. Times in UTC. Leave unknowns explicit.

Tenant name / tenant ID

Owner / updated (UTC)

04 Access cleanup: use a continuation sheet for additional entries

Credential keyId / thumbprint

Target app / object ID

Approved change? Basis / approver

Use-search result / evidence reference

Authorized removal / time (UTC) / operator

05 Change review status: record status, evidence reference, and owner

Roles

App owners

Consents

Policies

Mailboxes

Unresolved findings

06 Recovery and reconnection

Workload	Last recovery point (UTC)	Restore available? / interim plan	Owner

Next review (UTC) / owner

Reconnection authority / decision

Verified test job / result / time (UTC)