REMI Incident Response | Analysis

04 Synthetic enterprise incident - email endpoint cloud SIEM

Analysis summary

Observed reuse of the contractor maintenance token is the first supported access event in the operation. The associated remote session led to execution of the maintenance process and its coordinator child on the AI-worker server.

Workers were placed before activation across six destinations. Matching hashes connect placed files to later starts, and process identities link active workers to archive creation.

An internal administrative session widened application permissions, enabled two outside destinations and disabled the transfer alert. The associated change record shows that security and data-owner approvals had yet to be submitted.

Eight archives contained 192 distinct documents. Five matching committed receipts account for 120 distinct documents outside approved recipient scope, including at least one record from Active investigation files.

Responders revoked sessions, isolated the AI-worker server and terminated three processes. The county worker still completed a model exchange after those actions, so activity remained on that branch.

The material questions concern initial token acquisition, the administrative account operator and the duration of remaining activity.

USDF-G-AI-WORKERS-01

24 Aug UTC: token reuse at 13:00:01 and first execution at 13:03:00.

analysis-tables.xlsx > Evidence sheet > rows 11-12, 14-15.

USDF-G-HQ-01

27 Aug UTC: permission and monitoring changes from 14:30 to 14:33.

analysis-tables.xlsx > Evidence sheet > rows 153-157.

Five committed archive receipts on 28 Aug.

analysis-tables.xlsx > Evidence sheet > rows 9, 149, 153, 180, 185, 190, 195, 200, 208, 216, 224, 229, 236, 247, 254, 261.

USDF-G-PARTNER-COUNTY-02

28 Aug, 17:36 UTC: worker exchange after response.

analysis-tables.xlsx > Evidence sheet > rows 278-283, 285.

REMI Incident Response | Analysis

04 Synthetic enterprise incident - email endpoint cloud SIEM

Remote access leads to execution

The contractor maintenance account appears in the token-reuse record and the remote session. Server records use the same session ID for remote-maintenance-host.exe and identify that process as the parent of TelemetryCoordinator.exe.

Why it matters

This establishes the first supported route to execution inside the environment. The token acquisition method and operator remain unresolved.

USDF-G-CONTRACTOR-DMZ-01

Remote session started 24 Aug at 13:01:00 UTC.

analysis-tables.xlsx > Evidence sheet > rows 12.

USDF-G-AI-WORKERS-01

Token reuse was observed at 13:00:01 UTC. First execution at 13:03:00 UTC followed token reuse by 2 minutes 59 seconds and remote session start by 2 minutes. The coordinator started at 13:05 UTC.

analysis-tables.xlsx > Evidence sheet > rows 11-12, 14-15.

Programs are staged before activation

The Windows and Linux worker files were present about 22.5 hours to two days before their recorded starts. Inventory snapshots recorded zero running instances between placement and activation. The file hashes match the later executions.

Why it matters

The snapshots and execution records separate preparation from observed activation. Matching startup records explain how the files became running workers.

USDF-G-REGION-EAST-01

Placed 24 Aug at 13:20 UTC and ran 26 Aug at 13:00 UTC.

analysis-tables.xlsx > Evidence sheet > rows 23-24, 34, 39.

USDF-G-LAB-02

Placed 24 Aug at 13:32 UTC and ran 26 Aug at 13:10 UTC.

analysis-tables.xlsx > Evidence sheet > rows 32-33, 35, 46.

USDF-G-HQ-01

Headquarters, western office, private cloud and county partner files were placed 26 Aug and ran 27 Aug.

analysis-tables.xlsx > Evidence sheet > rows 57-58, 66-67, 75-76, 84-89, 98, 107, 115, 123.

REMI Incident Response | Analysis

04 Synthetic enterprise incident - email endpoint cloud SIEM

Execution reaches six destinations

The coordinator created the eastern office and laboratory workers. The eastern worker branched to headquarters and private cloud, and the laboratory worker branched to the western office and county partner.

Why it matters

Matching job IDs, destination hosts and hashes establish a connected seven-system execution chain including the coordinator. The process IDs also link the workers to later archive creation.

USDF-G-AI-WORKERS-01

Coordinator and first two worker branches.

analysis-tables.xlsx > Evidence sheet > rows 15-16, 20, 29, 39, 46.

USDF-G-REGION-EAST-01

Eastern office to headquarters and private cloud.

analysis-tables.xlsx > Evidence sheet > rows 54, 72, 98, 115.

USDF-G-LAB-02

Laboratory to western office and county partner.

analysis-tables.xlsx > Evidence sheet > rows 63, 81, 107, 123.

Archive creation records tied to the worker processes.

analysis-tables.xlsx > Evidence sheet > rows 179, 184, 189, 194, 199, 207.

Email leads to a separate execution sequence

A delivered message and click share a message ID. The clicked URL matches the headquarters download. The file hash and device match the subsequent start of RecordsConnectorUpdate.exe, and its process identifier matches the outbound connection.

Why it matters

The chain establishes another route to execution. Its relationship to the contractor access and later permission changes remains unresolved.

USDF-G-HQ-01

27 Aug UTC: delivered 13:40, clicked 13:44:05, downloaded 13:44:11, executed 13:47 and connected at 13:47:10.

analysis-tables.xlsx > Evidence sheet > rows 131, 133-134, 136, 139-140.

REMI Incident Response | Analysis

04 Synthetic enterprise incident - email endpoint cloud SIEM

Collection and confirmed exposure

Manifests identify 192 distinct documents across eight archives. Five committed receipts match their source archives by identity, file hash and byte count. Those archives contain 120 distinct documents and reached tenants outside the approved recipient scope.

Why it matters

The delivered documents include at least one record from Active investigation files. The permission grant covered six categories. The workbook establishes delivery for one category.

Approved-recipient policy and five committed archives.

analysis-tables.xlsx > Evidence sheet > rows 9, 179-180, 184-185, 189-190, 194-195, 199-200.

Matching destination receipts.

analysis-tables.xlsx > Evidence sheet > rows 229, 236, 247, 254, 261.

USDF-G-HQ-01

Category link for G-DOC-0001 and the six-category permission grant.

analysis-tables.xlsx > Evidence sheet > rows 149, 153, 180, 229.

Other outcomes: county upload failed, eastern archive was partially received and uncommitted, laboratory archive remained staged in the supplied records.

analysis-tables.xlsx > Evidence sheet > rows 207-208, 215-216, 223-224, 269, 276-277.

A blocked upload succeeds after rerouting

The first headquarters request for G-ARCH-03 was blocked. The failure record was supplied to a model request. The returned instruction changed the destination, and a dispatched command led to a matching upload and committed receipt.

Why it matters

The initial block interrupted one route. The later receipt completes the same archive already included in the five confirmed deliveries.

USDF-G-HQ-01

28 Aug UTC: original request blocked at 15:13:00, revised destination returned at 15:20:02, command dispatched at 15:20:03 and receipt committed at 15:20:15.

analysis-tables.xlsx > Evidence sheet > rows 189-190, 241-245, 247.

REMI Incident Response | Analysis

04 Synthetic enterprise incident - email endpoint cloud SIEM

Access expands while monitoring is reduced

The headquarters session under dana.mercer@usdf.example granted access to six worker accounts, enabled two outside storage tenants and disabled the transfer-monitoring rule. The matching change record lists security and data-owner approvals as not submitted.

Why it matters

These actions widened access and transfer options and reduced monitoring. The records identify the account and session used; the operator remains unresolved.

USDF-G-HQ-01

27 Aug UTC: grant at 14:30, storage changes at 14:32 and rule disabled at 14:33. Session G-EMP-SESSION and change G-CHANGE-417.

analysis-tables.xlsx > Evidence sheet > rows 151-157.

Response and remaining activity

The response records show one session-revocation action, one device isolation and three process terminations. The county worker sent a successful request and received a response after the recorded interventions.

Why it matters

The later exchange shows that the county branch remained active. Complete containment remains unresolved, and these events establish a model exchange.

USDF-G-HQ-01

Response started 28 Aug at 17:20 UTC. The AI-worker server was isolated at 17:21 UTC. Three terminations were recorded at 17:23 UTC.

analysis-tables.xlsx > Evidence sheet > rows 278-282.

USDF-G-PARTNER-COUNTY-02

Existing worker job G-JOB-2407 exchanged messages at 17:36:00 and 17:36:02 UTC.

analysis-tables.xlsx > Evidence sheet > rows 123, 283, 285.