Correlation summary

The records connect a reused contractor account to a remote session and program execution on the AI-worker server. Matching session and parent-process identifiers show how that access reached the program that coordinated the later activity.

From that server, worker-creation records branch to the eastern office and laboratory. Those workers created further branches to headquarters, the western office, private cloud and county partner. Matching parent and child jobs, destination computers and file identities connect the controller and six executing workers.

The worker files were placed before they ran. Later process records connect those same workers to archive creation and uploads, and matching destination receipts confirm that five archives reached two outside storage services. The other archives have failed, partial or staged-only outcomes.

A separately evidenced email sequence reaches headquarters through a delivered message, a click, a downloaded file and program execution. Its connection to the earlier remote access is unresolved. Later account changes connect permissions and storage settings through their own session and change record.

The records also follow a failed headquarters upload to a revised destination and a completed receipt for the same archive. After response actions began, the county worker still exchanged messages under its existing process and job identifiers.

Why the connections matter: The matching identifiers connect access, execution and received archives into a supported sequence. They also show where a separate branch or an incomplete transfer must remain separate.

From: USDF-G-CONTRACTOR-DMZ-01
To: USDF-G-AI-WORKERS-01
- 24 Aug: account/session access to program execution.

From: USDF-G-AI-WORKERS-01
To: USDF-G-REGION-EAST-01
To: USDF-G-LAB-02
- 24 Aug: first worker branches; active 26 Aug.

From: USDF-G-REGION-EAST-01
To: USDF-G-HQ-01
To: USDF-G-CLOUD-PRIVATE-01
- 26 Aug: onward branches; active 27 Aug.

From: USDF-G-LAB-02
To: USDF-G-REGION-WEST-02
To: USDF-G-PARTNER-COUNTY-02
- 26 Aug: onward branches; active 27 Aug.

From: Email source
To: USDF-G-HQ-01
- 27 Aug: separate message-to-program sequence.

Receiving storage: vault-a.sync-exchange.example
Receiving storage: vault-b.archive-relay.example
- 28 Aug: five distinct committed archives.

Times: 2026 UTC. References name the existing workbook, worksheet and Excel rows.

Access reaches the coordinator

The identity record places the reused token in the same session later recorded by the contractor gateway and the AI-worker server. The server then records a maintenance process starting the coordinator as its child process.

Why it matters: This establishes a path from remote access to execution inside the environment. The supplied records do not establish how the original token was obtained or who operated it.

From: USDF-G-CONTRACTOR-DMZ-01
To: USDF-G-AI-WORKERS-01

- 24 Aug 13:00:01: token reuse; 13:01:00: remote session.
- 13:03:00: maintenance process; 13:05:00: coordinator.
- Account: svc-federated-maint@contractor.usdf.example.
- Matching session: G-SESSION-7002.

correlation-proof.xlsx > Evidence sheet > rows 11-12, 14-15.

Staged programs become connected workers

The coordinator first created workers for the eastern office and laboratory. Those workers later created branches to headquarters, the western office, private cloud and county partner.

Each worker-creation record identifies a destination and child job. The file placed there has the same hash as the later running program. Inventory checks between placement and activation recorded no running instance. The programs are TelemetrySync.exe on Windows and telemetry-sync on Linux.

Why it matters: These links distinguish files placed on a computer from programs that later ran there. The parent and child job records explain how the activity reached seven executing systems, rather than treating every imported device as involved.

From: USDF-G-AI-WORKERS-01
To: USDF-G-REGION-EAST-01

- Placed 24 Aug 13:20; ran 26 Aug 13:00.

correlation-proof.xlsx > Evidence sheet > rows 20, 23, 34, 39.

From: USDF-G-AI-WORKERS-01
To: USDF-G-LAB-02

- Placed 24 Aug 13:32; ran 26 Aug 13:10.

correlation-proof.xlsx > Evidence sheet > rows 29, 32, 35, 46.

From: USDF-G-REGION-EAST-01
To: USDF-G-HQ-01

- Placed 26 Aug 14:00; ran 27 Aug 12:45.

correlation-proof.xlsx > Evidence sheet > rows 54, 57, 86, 98.

From: USDF-G-LAB-02
To: USDF-G-REGION-WEST-02

- Placed 26 Aug 14:15; ran 27 Aug 12:55.

correlation-proof.xlsx > Evidence sheet > rows 63, 66, 87, 107.

From: USDF-G-REGION-EAST-01
To: USDF-G-CLOUD-PRIVATE-01

- Placed 26 Aug 14:30; ran 27 Aug 13:05.

correlation-proof.xlsx > Evidence sheet > rows 72, 75, 88, 115.

From: USDF-G-LAB-02
To: USDF-G-PARTNER-COUNTY-02

- Placed 26 Aug 14:45; ran 27 Aug 13:15.

correlation-proof.xlsx > Evidence sheet > rows 81, 84, 89, 123.

Times: 2026 UTC. References name the existing workbook, worksheet and Excel rows.

A separate email path reaches headquarters

The delivered message and click share a message identifier and recipient. The clicked URL matches the headquarters download. The downloaded file and the new process share a device and file hash, and that process is identified in the outbound connection.

The Sentinel alert names the same message, device and endpoint records. It supports this sequence without creating another independent incident. The evidence does not connect this email to the earlier token reuse or prove it caused the later permission changes.

Why it matters: This supports an additional route to execution on headquarters while keeping its relationship to the earlier access unresolved.

From: Email source
To: USDF-G-HQ-01

- Recipient: dana.mercer@usdf.example.
- 27 Aug 13:40:00: delivered; 13:44:05: clicked.
- 13:44:11: download; 13:47:00: program start.
- 13:47:10: connection to relay.partner-support.example.
- Program: RecordsConnectorUpdate.exe.

correlation-proof.xlsx > Evidence sheet > rows 131-132, 134, 136, 139-140.

One session connects the access changes

An administrative session at headquarters links an application permission assignment, two outside storage destinations being enabled and a transfer-monitoring alert being disabled. The same session and change identifier appear across those records.

The permission assignment names the six worker accounts, and the storage changes list those accounts as allowed applications. The SIEM permission alert refers directly to the original assignment record.

Why it matters: The records connect the workers to expanded access and the configured receiving destinations. They identify the account used for the changes, without establishing who controlled it or linking the changes causally to the email.

Recorded computer: USDF-G-HQ-01

- Account: dana.mercer@usdf.example.
- 27 Aug 14:30:00: six worker accounts granted access.
- 14:32:00: two outside destinations enabled.
- 14:33:00: transfer-monitoring alert disabled.
- Session: G-EMP-SESSION; change: G-CHANGE-417.

correlation-proof.xlsx > Evidence sheet > rows 153, 155-157, 289.

Enabled destination: vault-a.sync-exchange.example
Enabled destination: vault-b.archive-relay.example

- The enabled destinations match the later receiving services.

Times: 2026 UTC. References name the existing workbook, worksheet and Excel rows.

Archives connect workers to receiving storage

Five workers created archives that can be followed to completed receipts at outside storage. The process identifiers connect archive creation to those workers; archive identifiers, file hashes and byte counts connect the source objects, outbound requests and committed destination receipts.

The eastern office and laboratory delivered one archive each to the first service. Headquarters, the western office and private cloud delivered one each to the second. The recorded recipient tenants are outside the supplied approved-recipient list.

Three other archive outcomes remain different: the county upload failed, a further eastern archive has only a partial receipt, and a further laboratory archive has no matching receipt in the supplied records. A repeated acknowledgment of the first eastern upload is counted once.

Why it matters: Matching source and destination evidence establishes which archives arrived. Failed requests, partial data and files staged on a computer do not become additional completed deliveries.

From: USDF-G-REGION-EAST-01
To: vault-a.sync-exchange.example
- 28 Aug 14:40:15: G-ARCH-01 committed.

correlation-proof.xlsx > Evidence sheet > rows 9, 179-180, 228-229, 231.

From: USDF-G-LAB-02
To: vault-a.sync-exchange.example
- 28 Aug 15:00:15: G-ARCH-02 committed.

correlation-proof.xlsx > Evidence sheet > rows 184-185, 235-236.

From: USDF-G-HQ-01
To: vault-b.archive-relay.example
- 28 Aug 15:20:15: G-ARCH-03 committed.

correlation-proof.xlsx > Evidence sheet > rows 189-190, 245, 247.

From: USDF-G-REGION-WEST-02
To: vault-b.archive-relay.example
- 28 Aug 15:40:15: G-ARCH-04 committed.

correlation-proof.xlsx > Evidence sheet > rows 194-195, 252, 254.

From: USDF-G-CLOUD-PRIVATE-01
To: vault-b.archive-relay.example
- 28 Aug 16:00:15: G-ARCH-05 committed.

correlation-proof.xlsx > Evidence sheet > rows 199-200, 259, 261.

Other outcome: USDF-G-PARTNER-COUNTY-02
- 28 Aug 16:20:07: G-ARCH-06 failed (HTTP 403).

correlation-proof.xlsx > Evidence sheet > rows 207, 269.

Other outcome: USDF-G-REGION-EAST-01
- 28 Aug 16:40:15: G-ARCH-07 partial; not committed.

correlation-proof.xlsx > Evidence sheet > rows 215, 276-277.

Other outcome: USDF-G-LAB-02
- 28 Aug 13:40:06: G-ARCH-08 created; no matched receipt.

correlation-proof.xlsx > Evidence sheet > rows 223-224.

Times: 2026 UTC. References name the existing workbook, worksheet and Excel rows.

A blocked upload changes destination

The first headquarters attempt to send its archive was blocked. That failed record was supplied to a model request. The returned instruction named a different storage destination, and the dispatched command, new upload and committed receipt retain the same archive identity.

The revised request and receipt also share the archive hash and byte count. This is the headquarters delivery already included among the five completed archives.

Why it matters: The linked failure, revised instruction and receipt show one transfer changing route and then arriving. Counting the retry as a new archive would overstate the completed deliveries.

From: USDF-G-HQ-01
First destination: vault-a.sync-exchange.example
- 28 Aug 15:13:00: blocked request; HTTP 403.
- Archive: G-ARCH-03.

correlation-proof.xlsx > Evidence sheet > row 241.

Same computer: USDF-G-HQ-01
Revised destination: vault-b.archive-relay.example
- 15:20:00: failed record submitted for revised instructions.
- 15:20:02: new destination; 15:20:03: command dispatched.
- 15:20:07: new upload; 15:20:15: committed receipt.
- Elapsed from first attempt to receipt: 7 minutes 15 seconds.

correlation-proof.xlsx > Evidence sheet > rows 242-245, 247.

The county connection continues after response

Response records show the contractor account sessions being revoked and the AI-worker server isolated. Sixteen minutes after the first of those actions, the county worker sent another request and received a response.

Its process and job identifiers match the worker previously started on the county computer. The request and response share their own exchange identifier.

Why it matters: The matching identities show that this branch continued after the recorded actions. This exchange does not establish a new archive delivery or determine the outcome for every other system.

Response recorded at: USDF-G-HQ-01
Isolation target: USDF-G-AI-WORKERS-01
- 28 Aug 17:20:00: contractor account sessions revoked.
- 17:21:00: AI-worker server isolation recorded.

correlation-proof.xlsx > Evidence sheet > rows 278-279.

Continued branch: USDF-G-PARTNER-COUNTY-02
Service: control.model-relay.example
- 17:36:00: request; 17:36:02: response.
- Same worker job: G-JOB-2407.

correlation-proof.xlsx > Evidence sheet > rows 123, 283, 285.

Times: 2026 UTC. References name the existing workbook, worksheet and Excel rows.