Detection summary

Remote-access traffic was flagged at the contractor gateway. Other flags identify new application identities, scheduled program starts, file archiving and cloud uploads across Windows and Linux computers. Network, identity, endpoint and cloud records provide the evidence for those flags.

The headquarters server has the widest variety of flags, including an email-linked execution alert and access changes. Email protection also identified six phishing messages that were blocked. Other click and external-storage records have no confirmed computer assignment.

Why these flags matter

These flags draw attention to activity that can provide access, start software automatically, or package and move files. Endpoint process records support the scheduled starts and the headquarters email alert. Storage records distinguish completed uploads from partial receipts, while the email records preserve the blocked outcome of the phishing messages.

Scope

- **Computers:** 8 named computers with device-specific flags.
- **Device findings:** 18 grouped findings across those computers.
- **Source groups:** 3 groups without a confirmed asset assignment.
- **Source set:** The same 35 files and 2,928 imported records.

Time order

Computers and their flags appear in order of the recorded source events. All displayed times are in UTC.

Computers in observed-time order

Computer: USDF-G-CONTRACTOR-DMZ-01
24 Aug 2026 13:02:00 UTC | 1 finding
10.71.14.21 | Windows Server 2022

Computer: USDF-G-AI-WORKERS-01
24 Aug 2026 13:20:12 UTC | 1 finding
10.71.15.21 | Windows Server 2022

Computer: USDF-G-REGION-EAST-01
24 Aug 2026 13:20:31 UTC | 3 findings
10.71.11.21 | Windows Server 2022

Computer: USDF-G-HQ-01
26 Aug 2026 14:00:31 UTC | 5 findings
10.71.10.21 | Windows Server 2022

Computer: USDF-G-CLOUD-PRIVATE-01
26 Aug 2026 14:30:31 UTC | 3 findings
10.71.16.21 | Windows Server 2022

Computer: USDF-G-LAB-02
28 Aug 2026 12:40:06 UTC | 2 findings
10.71.13.22 | Linux

Computer: USDF-G-REGION-WEST-02
28 Aug 2026 13:00:06 UTC | 2 findings
10.71.12.22 | Linux

Computer: USDF-G-PARTNER-COUNTY-02
28 Aug 2026 13:20:06 UTC | 1 finding
10.71.17.22 | Linux

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

USDF-G-CONTRACTOR-DMZ-01

Windows Server 2022 | 10.71.14.21 | 1 grouped finding

Computer: USDF-G-CONTRACTOR-DMZ-01

Remote-access traffic flagged

A network rule flagged a successful flow from the contractor zone into the AI-worker zone. The flow uses the same session recorded by the contractor gateway.

Why it matters: This is activity crossing from a remote-access area into an internal system, so the session and destination are relevant to the flag.

24 Aug 2026 13:02:00 UTC
Flow: 10.71.14.200 to 10.71.15.21.
Sources: network flow and contractor VPN.
detection-tables.xlsx > Evidence sheet > rows 4-6.

USDF-G-AI-WORKERS-01

Windows Server 2022 | 10.71.15.21 | 1 grouped finding

Computer: USDF-G-AI-WORKERS-01

New application identities

Identity records flag six application identities created using the contractor maintenance account. Each creation is recorded against this computer.

Why it matters: Application identities can give software its own access. Their creation is significant because it adds identities that can be used independently of an interactive sign-in.

24 Aug 13:20:12 to 26 Aug 14:45:12.
6 application identities; creation recorded as successful.
Source: identity application audit.
detection-tables.xlsx > Evidence sheet > rows 14, 23, 48, 57, 66, 75.

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

USDF-G-REGION-EAST-01

Windows Server 2022 | 10.71.11.21 | 3 grouped findings

Computer: USDF-G-REGION-EAST-01

Scheduled program start

An enabled scheduled task was created for TelemetrySync.exe. A later process record carries the matching task identifier and file hash.

Why it matters: The task provides a way to start the program automatically; the matching process record shows it ran.

Task created: 24 Aug 13:20:31.
Matching start: 26 Aug 13:00:05.
Source: Windows endpoint records.
detection-tables.xlsx > Evidence sheet > rows 17, 32.

Archive creation

The endpoint records flag creation of 2 archives in the telemetry-cache folder. Both creation events are recorded as successful.

Why it matters: Packaging files into an archive is relevant to a collection or transfer review. Archive creation by itself does not establish that the files left this computer.

28 Aug 12:30:06 to 28 Aug 13:30:06.
2 archives created.
Source: Windows EDR.
detection-tables.xlsx > Evidence sheet > rows 172, 208.

Cloud upload activity

Cloud records flag an upload associated with this computer. The destination record reports a completed commit. A separate archive has only a partial receipt, and a repeated acknowledgment belongs to the already completed upload.

Why it matters: The destination records show that archive data reached storage. A completed commit identifies a received object; a partial receipt identifies only part of an upload.

28 Aug 14:40:15 - one completed archive.
28 Aug 16:40:15 - separate partial receipt.
Repeated acknowledgment counted once.
Source: destination storage records.
detection-tables.xlsx > Evidence sheet > rows 223, 225, 272.

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

USDF-G-HQ-01

Windows Server 2022 | 10.71.10.21 | 5 grouped findings

Computer: USDF-G-HQ-01

Scheduled program start

An enabled scheduled task was created for TelemetrySync.exe. A later process record carries the matching task identifier and file hash.

Why it matters: The task provides a way to start the program automatically; the matching process record shows it ran.

> Task created: 26 Aug 14:00:31.
> Matching start: 27 Aug 12:45:05.
> Source: Windows endpoint records.
> detection-tables.xlsx > Evidence sheet > rows 51, 91.

Email-linked execution alert

Sentinel reports an email-linked execution alert for this computer. Email and endpoint records support the click, download, program start and outbound connection described by the alert.

Why it matters: The alert has device-level activity behind it, beyond delivery of a message or a click alone.

> Observed: 27 Aug 13:40:00 to 13:47:10.
> Program: RecordsConnectorUpdate.exe.
> Sources: Sentinel, email and Defender endpoint logs.
> detection-tables.xlsx > Evidence sheet > rows 124-125, 127, 129, 132-133, 286.

Access and storage changes

A source-referenced SIEM alert identifies an application permission change. Cloud records also flag an outside storage destination being enabled. The same account appears in the associated transfer-alert configuration change.

Why it matters: These changes affect what applications can access and where transfers can go. The records identify the account used, without identifying the person operating it.

> Observed: 27 Aug 14:30:00 to 14:33:00.
> Account: dana.mercer@usdf.example.
> Sources: Entra, Azure and Sentinel audits.
> detection-tables.xlsx > Evidence sheet > rows 146, 148-150, 284.

Archive creation

The endpoint records flag creation of an archive in the telemetry-cache folder.

Why it matters: Packaging files into an archive is relevant to a collection or transfer review. Archive creation by itself does not establish that the files left this computer.

> 28 Aug 12:50:06.
> 1 archive created.
> Source: Windows EDR.
> detection-tables.xlsx > Evidence sheet > row 182.

Cloud upload activity

Cloud records flag an upload associated with this computer. The destination record reports a completed commit.

Why it matters: The destination records show that archive data reached storage. A completed commit identifies a received object; a partial receipt identifies only part of an upload.

> 28 Aug 15:20:15.
> Destination: vault-b.archive-relay.example.
> Source: destination storage records.
> detection-tables.xlsx > Evidence sheet > rows 241-242.

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

USDF-G-CLOUD-PRIVATE-01

Windows Server 2022 | 10.71.16.21 | 3 grouped findings

Computer: USDF-G-CLOUD-PRIVATE-01

Scheduled program start

An enabled scheduled task was created for TelemetrySync.exe. A later process record carries the matching task identifier and file hash.

Why it matters: The task provides a way to start the program automatically; the matching process record shows it ran.

Task created: 26 Aug 14:30:31.
Matching start: 27 Aug 13:05:05.
Source: Windows endpoint records.
detection-tables.xlsx > Evidence sheet > rows 69, 108.

Archive creation

The endpoint records flag creation of an archive in the telemetry-cache folder.

Why it matters: Packaging files into an archive is relevant to a collection or transfer review. Archive creation by itself does not establish that the files left this computer.

28 Aug 13:10:06.
1 archive created.
Source: Windows EDR.
detection-tables.xlsx > Evidence sheet > row 192.

Cloud upload activity

Cloud records flag an upload associated with this computer. The destination record reports a completed commit.

Why it matters: The destination records show that archive data reached storage. A completed commit identifies a received object; a partial receipt identifies only part of an upload.

28 Aug 16:00:15.
Destination: vault-b.archive-relay.example.
Source: destination storage records.
detection-tables.xlsx > Evidence sheet > rows 255-256.

USDF-G-LAB-02

Linux | 10.71.13.22 | 2 grouped findings

Computer: USDF-G-LAB-02

Archive creation

The endpoint records flag creation of 2 archives in the telemetry-cache folder. Both creation events are recorded as successful.

Why it matters: Packaging files into an archive is relevant to a collection or transfer review. Archive creation by itself does not establish that the files left this computer.

28 Aug 12:40:06 to 28 Aug 13:40:06.
2 archives created.
Source: Linux audit.
detection-tables.xlsx > Evidence sheet > rows 177, 216.

Cloud upload activity

Cloud records flag an upload associated with this computer. The destination record reports a completed commit.

Why it matters: The destination records show that archive data reached storage. A completed commit identifies a received object; a partial receipt identifies only part of an upload.

28 Aug 15:00:15.
Destination: vault-a.sync-exchange.example.
Source: destination storage records.
detection-tables.xlsx > Evidence sheet > row 231.

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

USDF-G-REGION-WEST-02

Linux | 10.71.12.22 | 2 grouped findings

Computer: USDF-G-REGION-WEST-02

Archive creation

The endpoint records flag creation of an archive in the telemetry-cache folder.

Why it matters: Packaging files into an archive is relevant to a collection or transfer review. Archive creation by itself does not establish that the files left this computer.

28 Aug 13:00:06.
1 archive created.
Source: Linux audit.
detection-tables.xlsx > Evidence sheet > row 187.

Cloud upload activity

Cloud records flag an upload associated with this computer. The destination record reports a completed commit.

Why it matters: The destination records show that archive data reached storage. A completed commit identifies a received object; a partial receipt identifies only part of an upload.

28 Aug 15:40:15.
Destination: vault-b.archive-relay.example.
Source: destination storage records.
detection-tables.xlsx > Evidence sheet > rows 248-249.

USDF-G-PARTNER-COUNTY-02

Linux | 10.71.17.22 | 1 grouped finding

Computer: USDF-G-PARTNER-COUNTY-02

Archive creation

The endpoint records flag creation of an archive in the telemetry-cache folder.

Why it matters: Packaging files into an archive is relevant to a collection or transfer review. Archive creation by itself does not establish that the files left this computer.

28 Aug 13:20:06.
1 archive created.
Source: Linux audit.
detection-tables.xlsx > Evidence sheet > row 200.

Source records without a confirmed computer

Email click flags without a confirmed device

Nineteen other allowed-click records matched the email rule. Their threat-classification fields are blank, and the available records do not assign these clicks to a confirmed computer. These remain unresolved source matches, rather than established device findings.

Why it matters: A rule match and a successful click are not enough to label a computer infected or join it to the endpoint alert.

Source: Email source
27 Aug 12:11:40 to 27 Aug 14:12:56.
19 click records; device not established.
Source: Microsoft 365 URL click records.
detection-tables.xlsx > Evidence sheet > rows 83-84, 143.
See the workbook for the full group.

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

Source records without a confirmed computer

Phishing messages blocked

The email system identifies six messages as phishing through impersonation detection and records that all six were blocked into quarantine. No endpoint device is identified for these messages.

Why it matters: These are detected email attempts with a recorded blocked outcome. They do not establish delivery or execution on a computer.

Source: Email source
27 Aug 13:46:40 to 27 Aug 13:54:15.
6 messages; all blocked.
Source: Microsoft 365 email records.
detection-tables.xlsx > Evidence sheet > rows 131, 134-136, 138-139.

Source records without a confirmed computer

External object-access records

Destination storage records flag five object reads under the label EXTERNAL-REVIEW. That label is not a device in the supplied asset inventory, so the activity remains attributed to the source rather than assigned to a guessed computer.

Why it matters: The records show access to stored objects. They do not identify the physical device or person behind the source label.

Source: EXTERNAL-REVIEW
28 Aug 14:40:25 to 28 Aug 16:00:25.
5 object-read records; reported as successful.
Source: external storage operator records.
detection-tables.xlsx > Evidence sheet > rows 224, 232, 243, 250, 257.

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