SECURITY INCIDENT · CONCEPT SAMPLE

Incident S-0932

Account takeover followed by data staging · user j.sample · correlated from four sources, 25 Sep 2026, 03:05 EAT

FINAL STATUS	RESPONSE	POLICY	APPROVAL	ATTACK WINDOW
Contained	Session disabled	P-07 v3	1 of 1 · Lead B	4 events · 51 min

PART A **Response outcome**
Plain English, for the security lead and auditors

Summary

OUTCOME IN BRIEF

Between 02:14 and 03:05 on 25 September, four events touched the identity **j.sample**: **23 repeated MFA prompts** (identity), a session from a **new network route** (network), an **admin role added** on laptop wks-221 (endpoint) and a **bulk read of 1,842 objects** from customer storage (cloud). Each stayed below its own tool's alert threshold. Shield put them on one timeline, **correlated them into an attack path** and raised incident S-0932. The **security copilot** explained the path as an account takeover followed by data staging and suggested disabling the session; it took no action. **Policy P-07 v3** met all three conditions and covered "disable session" with **one approver**. Analyst A requested the response; a request to delete the user account was **blocked because no policy covers it**. **Lead B approved**, and the session was disabled at 03:14:55 under P-07 v3.

4 events · 4 sources · 51 min | Copilot suggestion · advisory only | P-07 v3 · 3 of 3 conditions | Uncovered request blocked | Approved by a second person | Session disabled

Key facts

WHAT THE INCIDENT CONNECTS

IDENTITY	CORRELATED	RAISED → CONTAINED	REQUESTER ≠ APPROVER
j.sample	4 events · 4 sources	03:05:50 → 03:14:55	Enforced

AI assists, policy decides

THE DETERMINISM BOUNDARY

Advisory: correlation and copilot

Shield correlated the four events and the copilot explained the likely attack path and suggested a response. Neither can disable a session, isolate a host, revoke a key or block an address, approve a response or change a policy.

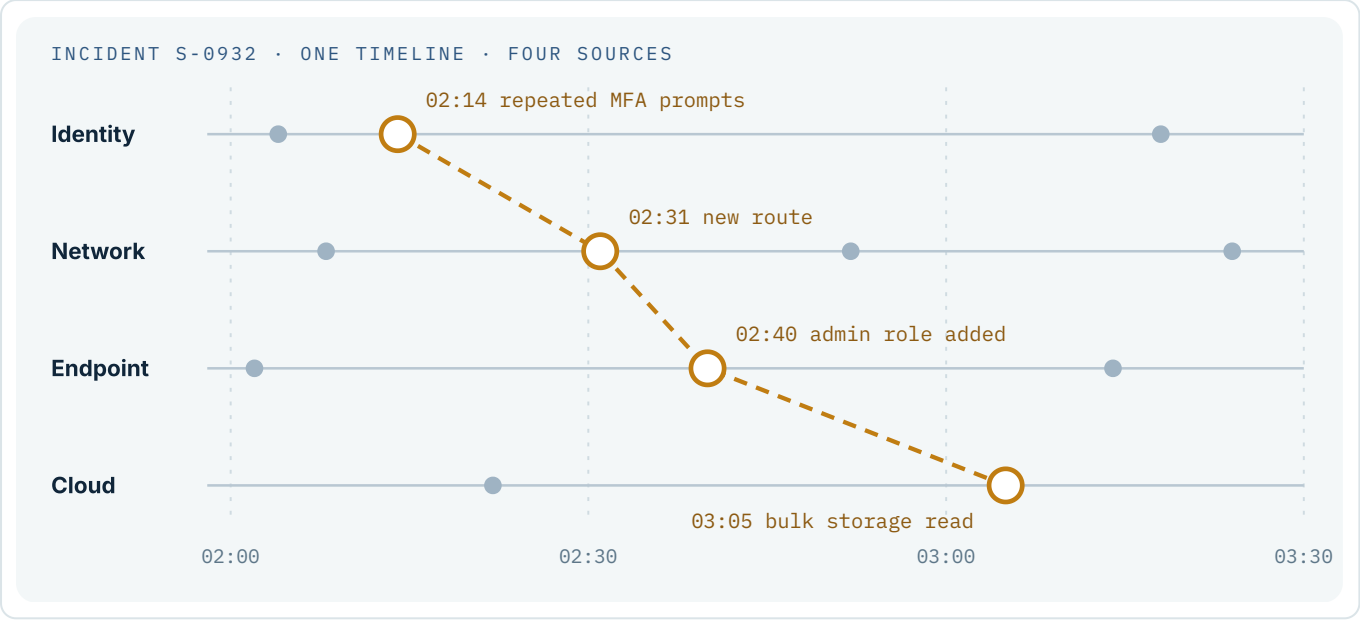
DETERMINISM BOUNDARY

Deterministic: governed policy

Whether a response may run came from policy P-07 v3, a versioned policy with an owner and an approver. The same input always gives the same result. The response ran only after a person other than the requester approved it.

One timeline, four sources

02:00–03:30 EAT · IDENTITY, NETWORK, ENDPOINT, CLOUD



Correlated attack path ○ Correlated event ● Routine event, not linked

Correlated events

EACH BELOW ITS OWN TOOL'S ALERT THRESHOLD

TIME	SOURCE	EVENT	ENTITY
02:14	Identity	**Repeated MFA prompts** 23 push prompts in 6 minutes; the 23rd was approved at 02:19. Usual sign-in needs one prompt.	`j.sample`
02:31	Network	**New network route** Session moved to 203.0.113.58, a route and provider never seen for this user in 90 days.	`203.0.113.58`
02:40	Endpoint	**Admin role added** Local administrator role granted to j.sample on laptop wks-221 from the new session. No change ticket.	`wks-221`
03:05	Cloud	**Bulk storage read** 1,842 objects (6.3 GB) read from bucket cust-records-demo in 9 minutes. Daily average: 12 objects.	`cust-records-demo`

Eight routine events in the same window (sign-ins, keep-alives, a DNS failover, patch checks, a backup job) stayed on the timeline for context and were not linked. The link is the identity j.sample and the order of the four events: access, move, escalate, collect.

Attack path

CORRELATED EVENTS IN ORDER · 51 MINUTES

STEP 1 · IDENTITY
MFA fatigue on user j.sample
02:14 · j.sample

→

STEP 2 · NETWORK
Session from new network route
02:31 · 203.0.113.58

→

STEP 3 · ENDPOINT
Privilege escalation to admin
02:40 · wks-221

→

STEP 4 · CLOUD
Bulk read of customer storage
03:05 · cust-records-demo

Copilot explanation

ADVISORY · CANNOT TAKE ACTION

Security copilot

ADVISORY · CANNOT TAKE ACTION

Four events in 51 minutes that no single tool would flag on its own.

At 02:14 j.sample received 23 MFA prompts in six minutes and approved the last one. At 02:31 the session moved to a network route never seen for this user, at 02:40 an admin role was added on their laptop, and at 03:05 the same identity read 1,842 objects from customer storage.

Together they match an account takeover followed by data staging. **Suggested response: disable session.**

EVIDENCE CITED

- MFA prompt log, 02:14–02:19
- Session route change to 203.0.113.58 at 02:31
- Admin role grant on wks-221 at 02:40
- Storage read of 1,842 objects from 03:05

SUGGESTED CHECKS

- Call j.sample on a known number to confirm they did not approve the prompt
- Check whether data left the network after 03:05
- Review other identities that used 203.0.113.58

i **Action request declined at 03:12:00.** Asked to “disable the session now”, the copilot declined: it can read signals, correlate them, explain the attack path and suggest a response, but it has no permission to disable sessions, isolate hosts, revoke keys or block addresses, to request or approve a response, to dismiss an incident, or to change a policy. The request and the refusal are in the audit log.

Copilot permissions

FIXED · NO SETTING GRANTS AN ACTION

PERMISSION	STATUS
Read identity, network, endpoint and cloud signals	ALLOWED
Correlate events and draft an explanation	ALLOWED
Suggest a response for an analyst	ALLOWED
Disable sessions, isolate hosts, revoke keys or block addresses	NOT PERMITTED
Request or approve a response · dismiss an incident	NOT PERMITTED
Change a policy, condition or approver count	NOT PERMITTED

Policy gate

DETERMINISTIC · POLICY SET PS-2026.09

POLICY	VER.	ACTION	CONDITION	REQUIRED	OBSERVED	APPROVERS	RESULT
P-07 Disable a compromised session	v3	Disable session	Correlated events on one identity	≥ 3	4	1	MET
			Privilege change in the attack path	Yes	Yes		MET
			Activity covered by an approved change ticket	No	No		MET
P-07 v3 covers disable session · 3 of 3 conditions met · requires 1 approver, not the requester							
P-11 Isolate a host showing ransomware precursors	v5	Isolate host	Ransomware precursor indicators on the host	≥ 2	0	1 2 for production	NOT MET
			Hosts contacted by lateral movement	≥ 1	0		NOT MET
			Activity covered by an approved change ticket	No	No		MET
P-11 v5 does not cover isolate host · 1 of 3 conditions met							
P-14 Revoke a cloud access key used abnormally	v2	Revoke access key	Key used from a region never seen for it	Yes	Not observed	1	NOT MET
			API calls with the key in 15 minutes	≥ 100	Not observed		NOT MET
P-14 v2 does not cover revoke access key · 0 of 2 conditions met							
P-19 Block a hostile source address	v4	Block IP	Source address on the threat-intelligence list	Yes	No	1	NOT MET
			Connections from the address in one hour	≥ 20	14		NOT MET
P-19 v4 does not cover block IP · 0 of 2 conditions met							

✓ **Result: P-07 v3 covers the suggested response, disable session, with one approver other than the requester.** Every policy in the live set is evaluated in the same order for every incident, and a policy covers its action only when all of its conditions are met. Evaluation fingerprint `pg-feefc6f7`: re-running with the same input gives the same result. A sandbox test of a higher correlated-events threshold was run and not applied; a real change would be a new version (P-07 v4) with an approver.

Policy provenance

WHO OWNS AND APPROVED THE POLICY THAT ACTED

POLICY	OWNER	APPROVED BY	EFFECTIVE
P-07 v3	Security operations	CISO (fictional)	01 Sep 2026

History. v2 · 12 Jun 2026 · privilege-change condition added. v3 · 01 Sep 2026 · approved change tickets excluded.

Request blocked at the gate

NO POLICY, NO RESPONSE

TIME (EAT)	REQUESTED RESPONSE	REQUESTED BY	GATE RESULT
03:12:50	**Delete user account** Target j.sample	Analyst A	BLOCKED No policy in PS-2026.09 covers this action · nothing executed

Shield can only run responses that a versioned policy covers. There is no override and the copilot cannot add one; a new kind of response needs a new policy, with an owner and an approver, before it can ever run.

Request & approval

ZERO TRUST · LEAST PRIVILEGE · FOUR-EYES

Rule applied: a response runs only under a covering policy, after the approvers it names; the requester can never approve.

01

AA **Analyst A · request** Disable session · j.sample 25 Sep 2026 · 03:13:40

Four linked events on j.sample: MFA fatigue, new route, admin role, bulk read. Requesting P-07 disable session to stop the bulk read while we contact the user.

02

PG **Policy gate · request covered** 25 Sep 2026 · 03:14:05

P-07 v3 · 3 of 3 conditions met · 1 approver required, not the requester. Analyst A was blocked from approving their own request.

03

LB **Lead B · approval 1 of 1** Approved 25 Sep 2026 · 03:14:30

Checked the MFA log and the storage read. The session is still active and reading. Approved.

✓ **Response executed: disable session · j.sample · active session**

Run by Shield at 03:14:55 EAT under P-07 v3, after Lead B approved. Least privilege: the policy ends the one session; the account itself stays for investigation. The audit row is sealed.

Decision path

FROM SIGNALS TO A CONTAINED INCIDENT

STAGE	OUTCOME	BY	TIME (EAT)
Correlate	Incident S-0932 raised · 4 events in 51 minutes	Shield correlation	03:05:50
Explain	Explanation drafted; action request declined	Copilot (advisory)	03:12:00
Blocked	Delete user account · no policy covers it	Policy gate	03:13:15
Request	Disable session requested	Analyst A	03:13:40
Approve	Approved (1 of 1)	Lead B	03:14:30
Respond	Session disabled under P-07 v3	Shield	03:14:55

Audit log

16 EVENTS · OLDEST FIRST · EAT (UTC+3)

TIME	ACTOR	EVENT / DETAIL
25 Sep · 02:19:04	Identity provider	**MFA prompt burst** · j.sample · 23 prompts in 6 min · last one approved
25 Sep · 02:31:12	Network sensor	**New route for identity** · 203.0.113.58 · not seen in 90 days
25 Sep · 02:40:33	Endpoint agent	**Local admin role granted** · j.sample on wks-221 · no change ticket
25 Sep · 03:05:48	Cloud audit trail	**Bulk read started** · cust-records-demo · 1,842 objects in 9 min
25 Sep · 03:05:50	Shield correlation	**Incident raised** · S-0932 · 4 events, 4 sources, 51 min
25 Sep · 03:05:51	Policy engine	**Policies evaluated** · P-07 v3 covers disable session (3 of 3)
25 Sep · 03:05:52	Copilot (advisory)	**Explanation drafted** · Suggested response: disable session
25 Sep · 03:05:52	Shield	**Routed to SOC queue** · No response taken yet
25 Sep · 03:12:00	Copilot (advisory)	**Action request declined** · "Disable the session now" · no action permissions
25 Sep · 03:12:25	Analyst A	**Policy sandbox used (not applied)** · P-07 threshold tested · live policy unchanged
25 Sep · 03:12:50	Analyst A	**Response requested** · Delete user account · j.sample
25 Sep · 03:13:15	Policy gate	**Response blocked by policy gate** · No policy covers this action · nothing executed
25 Sep · 03:13:40	Analyst A	**Response requested** · Disable session · j.sample · active session
25 Sep · 03:14:05	Policy gate	**Request covered by policy** · P-07 v3 · 1 approver, not the requester
25 Sep · 03:14:30	Lead B	**Response approved (1 of 1)** · P-07 v3 · session still active and reading
25 Sep · 03:14:55	Shield	**Response executed under policy** · Session disabled · Analyst A → Lead B

About this report

HOW TO READ IT

- **Concept sample.** Saolix Shield is in development: an early access-control prototype exists, but the threat-response design in this report is not yet built. This report shows the planned format of a Shield incident response report.
- **Deterministic policy.** Every incident is evaluated against the same versioned policies, in the same order. The table on page 4 is the complete reason the response was allowed to run.
- **Advisory AI.** Correlation and the copilot explanation help an analyst understand an incident. They cannot take, request or approve a response.
- **People approve, every action is recorded.** Each request and approval carries a person, a note and a time; the requester can never approve their own request.
- **Fictitious data.** Incident S-0932, user j.sample, laptop wks-221, bucket cust-records-demo, the documentation-range address 203.0.113.58 and every other record here are fictitious.