REVIEW | PUBLIC-SOURCE TECHNICAL DOSSIER

CrowdStrike Cause and Remediation

DECISION QUESTION

Did the public evidence establish both the cause of the July 2024 outage and the remediation that followed?

EXECUTIVE POSITION

CrowdStrike's public technical record identifies a Rapid Response Content update as the trigger for the July 19, 2024 Windows crashes and later published a root-cause analysis with mitigations. That supports a strong account of the immediate mechanism and documented remediation steps. It does not, by itself, independently prove every long-term resilience claim or eliminate all future failure modes.

Product	REVIEW
Product purpose	Test the answer you already have. Challenge an existing narrative, report, model, assertion or conclusion before reliance.
Sector	Cybersecurity / software / resilience
Jurisdiction	United States / global
Status	CONTROLLED PUBLICATION CANDIDATE - HUMAN APPROVAL PENDING
Evidence cut-off	8 September 2026, 07:38 SAST
Issue	8 September 2026 | Version 2.0
Governing master	PHW Research AI v11.0 Approved Governing Master
Document code	APW-REV-260908-05

REALITY BEFORE RELIANCE | VERIFICATION BEFORE INTERPRETATION | EVIDENCE BEFORE NARRATIVE

Independent public-source case study - not a client engagement. No conclusion stronger than the available evidence. Final human approval remains pending.

Package control & evidence architecture

Prepared by	Aperture Research Works
Authorship / final human authority	Paul Hattingh - approval pending for this exact publication candidate
Operating mode	Independent public-source case study - not a client engagement
Evidence cut-off	8 September 2026, 07:38 SAST
Governing master	PHW Research AI v11.0 Approved Governing Master
Research readiness	95/100 - ready for controlled dossier construction with specified limitations
Evidence sources	12
Controlled propositions	18
Page count	30
Publication state	CONTROLLED PUBLICATION CANDIDATE - HUMAN APPROVAL PENDING
Professional boundary	No legal advice, engineering certification, audit opinion, actuarial opinion, investment advice or other reserved professional determination is provided.

Six-document package

Doc	Controlled document	Function
1	Principal Investigative Dossier	Decision answer, scope, findings, technical analysis, hypotheses, contradictions, gaps, risk and hand-off controls.
2	Claims-and-Evidence Matrix	Proposition-by-proposition traceability with factual status, confidence, reliance and Source IDs.
3	Master Chronology	Time-ordered record separating baseline, event, correction, update and current-status evidence.
4	Source and Evidence Register	Visible URLs plus source authority, role, limitation, dependence and supported propositions.
5	Public Portfolio Edition	Concise demonstration suitable for public website display while preserving material caveats.
6	Final Delivery Manifest	Production conformity, readiness, release gates, web links, supersession and hash-control architecture.

Reader workflow

- Start with the decision question and executive position.
- Test every material finding in Document 2 against its S-IDs.
- Use Document 3 to determine whether a later event changes an earlier proposition.
- Use Document 4 to inspect provenance and limitations directly at source level.
- Do not strip caveats when transferring a proposition into another decision document.
- Use Document 6 before release to confirm that the package and website remain synchronized.

DOCUMENT 1

Principal Investigative Dossier

The principal dossier establishes the bounded answer, shows how the evidence was tested and makes the decision dependencies visible.

How to use this document

- Read the executive answer first.
- Follow each material finding to its C-ID and S-ID.
- Treat exclusions, gaps and reliance status as part of the answer, not footnotes.
- Use the decision-transfer checklist before carrying any conclusion into a transaction, publication, board paper or operating decision.

Evidence-chain reading rule

Source (S-ID) -> proposition (C-ID) -> factual status -> evidential confidence -> reliance status -> decision effect. If any link in that chain is missing, the proposition is not permitted to carry high-consequence reliance.

1. Matter understanding and decision frame

Did the public evidence establish both the cause of the July 2024 outage and the remediation that followed?

CrowdStrike's public technical record identifies a Rapid Response Content update as the trigger for the July 19, 2024 Windows crashes and later published a root-cause analysis with mitigations. That supports a strong account of the immediate mechanism and documented remediation steps. It does not, by itself, independently prove every long-term resilience claim or eliminate all future failure modes.

Product outcome

Test the answer you already have. Challenge an existing narrative, report, model, assertion or conclusion before reliance.

In scope

- The July 19, 2024 CrowdStrike Windows outage mechanism described in the public technical record.
- The distinction between immediate cause, root cause, mitigation and long-term resilience claims.
- Evidence architecture for reviewing vendor post-incident statements.
- Residual reliance limits after remediation.

Explicit exclusions

- Penetration testing or independent source-code review.
- A warranty that the incident class cannot recur in another form.
- Cybersecurity legal advice or contractual interpretation.
- A complete assessment of all customer losses.

Jurisdictions and disciplines

Jurisdiction(s)	United States / global
Applicable disciplines	incident review; software assurance; operational resilience; litigation and regulatory status
Governing evidence date	8 September 2026, 07:38 SAST
Decision transfer	Orientation / diligence planning unless a proposition is separately cleared for stronger reliance

2. Executive findings and reliance effect

Finding 1

CrowdStrike's preliminary incident review identifies the affected window, Windows sensor versions and the

Claim linkage: C01. Read together with the cited sources and qualification in Document 2.

Finding 2

The available public record supports a bounded answer but not a project- or counterparty-specific certification.

Claim linkage: C02. Read together with the cited sources and qualification in Document 2.

Finding 3

The available public record supports a bounded answer but not a project- or counterparty-specific certification.

Claim linkage: C03. Read together with the cited sources and qualification in Document 2.

Finding 4

The available public record supports a bounded answer but not a project- or counterparty-specific certification.

Claim linkage: C04. Read together with the cited sources and qualification in Document 2.

Reliance rule: an attractive or convenient narrative is not permitted to outrun the proposition the evidence actually establishes. Any project-, counterparty-, legal-, engineering-, operational- or financial conclusion that depends on non-public evidence remains conditional until that evidence is obtained and authenticated.

3. Technical and operating analysis

3.1 Incident mechanism

CrowdStrike stated that a Rapid Response Content update for Channel File 291 caused crashes on Windows hosts. The later RCA described a mismatch between expected and supplied input fields that resulted in an out-of-bounds memory read. That is a materially specific causal account, but it is primarily company-originated evidence.

- Distinguish trigger from systemic contributing controls.
- Separate affected platform scope from unaffected systems.
- Record precise timestamps and release path.
- Do not convert a company RCA into independent assurance merely by repetition.

Aperture control: separate the source-supported fact from inference, assumption, forecast and missing decision evidence. Carry the C-ID/S-ID chain forward when this module is used in a decision.

3.2 Remediation evidence

Post-incident materials describe validation changes, deployment controls and other mitigations. The review question is whether those actions address the identified failure path and whether evidence exists for implementation, not merely intention.

- Map each root cause to a stated mitigation.
- Separate implemented, planned and independently reviewed controls.
- Look for technical evidence of rollback, canary or staged deployment mechanisms.
- Track whether subsequent incidents challenge the resilience claim.

Aperture control: separate the source-supported fact from inference, assumption, forecast and missing decision evidence. Carry the C-ID/S-ID chain forward when this module is used in a decision.

3.3 Causation versus resilience

A strong explanation of one incident does not establish that all related operational risks are eliminated. Long-term resilience depends on software change control, testing coverage, release safeguards, architectural containment and organisational learning.

- Treat “this exact scenario cannot recur” narrowly.

- Avoid extrapolating to every content-update failure mode.
- Use subsequent performance only with defined observation period.
- Seek third-party evidence where reliance is high.

Aperture control: separate the source-supported fact from inference, assumption, forecast and missing decision evidence. Carry the C-ID/S-ID chain forward when this module is used in a decision.

3.4 Decision use

For vendor risk, the appropriate conclusion is layered: immediate mechanism may be well-supported; remediation may be documented; future resilience remains a separate proposition. Procurement and concentration decisions should preserve that distinction.

- Record incident-cause confidence separately from resilience confidence.
- Map dependency concentration and recovery capability.
- Require business-continuity evidence for critical deployments.
- Refresh vendor risk after material platform changes.

Aperture control: separate the source-supported fact from inference, assumption, forecast and missing decision evidence. Carry the C-ID/S-ID chain forward when this module is used in a decision.

4. Evidence tests applied to the technical modules

Authority test

Is the proposition supported by the body with direct legal, regulatory, operational or reporting authority, or only by a derivative account?

Applied result: see the claim matrix, source register, chronology and gap register. The test is not passed by document volume; it is passed by traceable evidence appropriate to the proposition.

Entity test

Does the source refer to the exact legal entity, asset, project, customer, jurisdiction or operating system relevant to the decision?

Applied result: see the claim matrix, source register, chronology and gap register. The test is not passed by document volume; it is passed by traceable evidence appropriate to the proposition.

Time test

Was the proposition true at the evidence cut-off, or only at an earlier stage of policy, financing, announcement, litigation or implementation?

Applied result: see the claim matrix, source register, chronology and gap register. The test is not passed by document volume; it is passed by traceable evidence appropriate to the proposition.

Completion test

Does an announcement evidence intent, approval, financing, construction, commissioning, production, delivery or sustained performance? These are separate states.

Applied result: see the claim matrix, source register, chronology and gap register. The test is not passed by document volume; it is passed by traceable evidence appropriate to the proposition.

Quantification test

Is a number an observation, estimate, model output, target, forecast, commitment, nameplate capacity, maximum, average or scenario?

Applied result: see the claim matrix, source register, chronology and gap register. The test is not passed by document volume; it is passed by traceable evidence appropriate to the proposition.

Negative-evidence test

What expected authoritative evidence is absent? Does absence materially weaken the proposition or merely reflect public-record limits?

Applied result: see the claim matrix, source register, chronology and gap register. The test is not passed by document volume; it is passed by traceable evidence appropriate to the proposition.

Independence test

Are multiple apparent sources actually repeating the same company statement, press release, dataset or institutional record?

Applied result: see the claim matrix, source register, chronology and gap register. The test is not passed by document volume; it is passed by traceable evidence appropriate to the proposition.

Decision-materiality test

Would a reasonable decision-maker change action, price, timing, scope or controls if this proposition were weaker than stated?

Applied result: see the claim matrix, source register, chronology and gap register. The test is not passed by document volume; it is passed by traceable evidence appropriate to the proposition.

5. Competing hypotheses, steelman and falsification

ID	Hypothesis	Strengthening evidence	Falsification condition
H1	The July 2024 outage arose from a specific content-update validation/deployment failure.	Evidence that would materially strengthen it	Evidence that would falsify or materially weaken it
H2	CrowdStrike remediation reduced recurrence risk for the identified failure mode.	Evidence that would materially strengthen it	Evidence that would falsify or materially weaken it
H3	System-wide operational resilience cannot be inferred solely from company remediation claims.	Evidence that would materially strengthen it	Evidence that would falsify or materially weaken it
H4	Current litigation/regulatory records remain material to a full review.	Evidence that would materially strengthen it	Evidence that would falsify or materially weaken it

Steelman rule: the strongest reasonable version of each competing explanation is retained until the evidence justifies rejection. Falsification evidence is actively sought; no hypothesis is selected because it is commercially or rhetorically convenient.

6. Contradiction and evidence-gap register

ID	Issue	Why apparent contradiction can arise	Control
X01	Potential tension around hypothesis H1	Different source types may describe different stages, scopes or levels of certainty.	Do not force reconciliation. Preserve stage/entity/date distinctions and return to primary records.
X02	Potential tension around hypothesis H2	Different source types may describe different stages, scopes or levels of certainty.	Do not force reconciliation. Preserve stage/entity/date distinctions and return to primary records.
X03	Potential tension around hypothesis H3	Different source types may describe different stages, scopes or levels of certainty.	Do not force reconciliation. Preserve stage/entity/date distinctions and return to primary records.
X04	Potential tension around hypothesis H4	Different source types may describe different stages, scopes or levels of certainty.	Do not force reconciliation. Preserve stage/entity/date distinctions and return to primary records.

Gap	Type	Missing / excluded evidence	Decision effect	Required closure
G01	Scope-excluded evidence	Penetration testing or independent source-code review.	Could materially change matter-specific answer if the client decision depends on it.	Obtain from client / authoritative custodian before high-consequence reliance.
G02	Scope-excluded evidence	A warranty that the incident class cannot recur in another form.	Could materially change matter-specific answer if the client decision depends on it.	Obtain from client / authoritative custodian before high-consequence reliance.
G03	Scope-excluded evidence	Cybersecurity legal advice or contractual interpretation.	Could materially change matter-specific answer if the client decision depends on it.	Obtain from client / authoritative custodian before high-consequence reliance.

Gap	Type	Missing / excluded evidence	Decision effect	Required closure
G04	Scope-excluded evidence	A complete assessment of all customer losses.	Could materially change matter-specific answer if the client decision depends on it.	Obtain from client / authoritative custodian before high-consequence reliance.
G05	Non-public operating evidence	Internal contracts, logs, customer records, engineering/technical files or reconciliations are not presumed available in a public demonstration.	Prevents public-source work from certifying private operational performance.	Request and authenticate matter-specific evidence if commissioned.
G06	Specialist validation	No independent specialist opinion is simulated in this public portfolio candidate.	Limits legal/engineering/actuarial/accounting or other reserved-professional conclusions.	Route defined questions to an appropriately qualified specialist.
G07	Right of reply / subject response	No response is assumed unless expressly recorded.	Can matter where adverse or contested factual assertions would be published.	Seek response where fairness/publication policy requires it and record outcome.
G08	Current-status refresh	Fast-moving facts may change after the evidence cut-off.	Can stale otherwise correct findings.	Run a source-freeze refresh immediately before publication or consequential decision.

Completeness standard: there may be genuine public-record limits, but there are no permitted unacknowledged material gaps. Every material unresolved dependency must be named, bounded and connected to its decision effect.

7. Risk, failure mode and control register

Risk	Failure mode	Likelihood	Impact	Control
R01	Review Target Not Frozen	Medium	High	Tie the decision to C-IDs/S-IDs, preserve contrary evidence, enforce current-status checks and escalate when the decision requires evidence outside the public record.
R02	Management Narrative Treated As Fact	Medium	High	Tie the decision to C-IDs/S-IDs, preserve contrary evidence, enforce current-status checks and escalate when the decision requires evidence outside the public record.
R03	Contradictory Evidence Omitted	High	High	Tie the decision to C-IDs/S-IDs, preserve contrary evidence, enforce current-status checks and escalate when the decision requires evidence outside the public record.
R04	Later Corrective Record Missed	Medium	High	Tie the decision to C-IDs/S-IDs, preserve contrary evidence, enforce current-status checks and escalate when the decision requires evidence outside the public record.
R05	Cause Confused With Correlation	Medium	Medium to high	Tie the decision to C-IDs/S-IDs, preserve contrary evidence, enforce current-status checks and escalate when the decision requires evidence outside the public record.
R06	Remediation Claim Mistaken For Validated Resilience	Medium	High	Tie the decision to C-IDs/S-IDs, preserve contrary evidence, enforce current-status checks and escalate when the decision requires evidence outside the public record.
R07	Legal/Professional Conclusion Made Without Specialist Review	Medium	High	Tie the decision to C-IDs/S-IDs, preserve contrary evidence, enforce current-status checks and escalate when the decision requires evidence outside the public record.
R08	Source Hierarchy Collapsed	Low to medium	High	Tie the decision to C-IDs/S-IDs, preserve contrary evidence, enforce current-status checks and escalate when the decision requires evidence outside the public record.

8. Decision-transfer and hand-off checklist

- Freeze the exact proposition being relied upon and record its C-ID.
- Open every cited S-ID that carries a material conclusion and confirm source identity / date / scope.
- Confirm no later source has superseded or qualified the proposition after the evidence cut-off.

- Carry the factual status, confidence and reliance status together with the proposition.
- Resolve any G-ID whose decision effect is material to the intended use.
- Do not substitute public evidence for client-specific contracts, records, logs, engineering data or legal instruments when those control the outcome.
- Escalate reserved professional questions to the correct specialist.
- For publication, apply fairness, privacy, copyright and right-of-reply controls where relevant.
- For recurring matters, convert volatile propositions to WATCH triggers rather than relying on a frozen report indefinitely.
- Record the final human approval and exact file hash before release.

9. Research method, reproducibility and evidence discipline

Research is the process; responsible reliance is the product. Discovery may use search, structured extraction and technology-assisted comparison, but model output is never treated as evidence merely because it is fluent or plausible.

Primary-source-first does not mean primary sources are infallible. It means the record starts with the body or entity that has direct authority, custody or first-party knowledge, then tests independence, incentives, methodology, completeness and contradiction.

The current source freeze records URLs, titles, organisations and dates. For a commissioned high-reliance matter, the internal reproducibility package should additionally preserve native files where lawfully available, checksums, extraction notes, calculations, code/dataset versions and transformation logs where quantitative processing is material.

Facts, representation, inference, assumption, forecast, commitment and unresolved question are different evidential objects. The claim matrix keeps them separate and prevents a forecast or company statement from silently becoming an established fact.

Negative evidence is treated cautiously. Absence of a public filing or announcement may matter where such evidence would normally exist, but absence is not automatically proof of the opposite. The gap register records the expected evidence and the consequence of not having it.

Current-status control is mandatory. A proposition that was correct at source date can become stale. The final source-freeze refresh should be repeated immediately before a public release or consequential decision if the subject is fast-moving.

10. Entity and relationship register

ID	Entity / organisation	Evidence role	Established relationship	Boundary
E01	CrowdStrike	Organisation / evidence origin	Relationship to matter established only to the extent shown by the cited source record.	Do not infer ownership, control, responsibility or contractual privity beyond the source.
E02	Microsoft	Organisation / evidence origin	Relationship to matter established only to the extent shown by the cited source record.	Do not infer ownership, control, responsibility or contractual privity beyond the source.
E03	CrowdStrike / SEC	Authoritative / regulatory custodian	Relationship to matter established only to the extent shown by the cited source record.	Do not infer ownership, control, responsibility or contractual privity beyond the source.
E04	Cybersecurity and Infrastructure Security Agency	Authoritative / regulatory custodian	Relationship to matter established only to the extent shown by the cited source record.	Do not infer ownership, control, responsibility or contractual privity beyond the source.
E05	U.S. Securities and Exchange Commission	Authoritative / regulatory custodian	Relationship to matter established only to the extent shown by the cited source record.	Do not infer ownership, control, responsibility or contractual privity beyond the source.

11. Quantitative, metric and calculation register

Metric	Claim	Number / metric proposition	Calculation status	Control
M01	C08	The cited record supports this bounded proposition: Independent ecosystem evidence estimating approximately 8.5 million Windows devices affected.	Source-reported unless an explicit calculation is separately stated.	Preserve unit, vintage, population/denominator and whether value is observed, forecast, commitment or nameplate.
M02	C11	The cited record supports this bounded proposition: Independent platform-vendor operational record concerning remediation of the outage on Windows devices.	Source-reported unless an explicit calculation is separately stated.	Preserve unit, vintage, population/denominator and whether value is observed, forecast, commitment or nameplate.

Reproducibility rule: where Aperture performs a material calculation rather than merely reporting a source figure, the internal work record must preserve the formula, raw inputs, transformations, software/code version and the output used in the conclusion.

12. Evidence acquisition and authentication plan

Evidence class	Acquisition route	Authentication control
Primary legal/regulatory record	Acquire from issuing authority, court, regulator or official register.	Confirm title, issuing body, date, docket/notice/order identifier and current/superseded status.
Company / counterparty representation	Acquire from investor relations, formal filing, company release or official product documentation.	Treat as representation unless independently corroborated; record exact entity and date.
Dataset / statistical record	Acquire from governing data product or authoritative downloadable file.	Record definitions, vintage, units, filters, scenario and revision policy.
Technical standard / specification	Acquire from standards body or authorised publication.	Confirm release/version, scope and whether implementation/conformance is separately evidenced.
Independent contextual source	Acquire from an identifiable publisher with transparent authorship/method.	Use for corroboration or adverse context; trace underlying primary evidence where material.
Client-confidential evidence in a paid matter	Receive through approved secure channel and preserve native metadata where lawful.	Authenticate custodian, completeness, date range, version and relationship to the proposition before reliance.

13. Fairness, privacy, copyright, right-of-reply and specialist controls

Fairness / adverse attribution

Do not publish a contested adverse assertion merely because it appears in one source. Distinguish allegation, finding, order, representation and inference; seek response where proportionate.

Privacy / personal data

Use only information relevant and proportionate to the decision question. Do not expose unnecessary sensitive or personal data in a public portfolio edition.

Copyright

Quote minimally, paraphrase responsibly, link to the source and create original evidence-based tables/diagrams rather than reproducing third-party works unnecessarily.

Right of reply

Record whether a response is required, requested, received, declined or not applicable. Silence is not treated as admission.

Specialist boundary

Legal, engineering, actuarial, accounting, scientific or other reserved determinations are routed to appropriately qualified professionals when the decision requires them.

Information security

A public demonstration contains public-source material only. Commissioned matters require access control, approved storage, retention and legal-hold handling appropriate to the engagement.

14. Current-status, monitoring and change-control plan

Trigger	Monitored custodian	Baseline source	Change condition	Required action
T01	CrowdStrike	Falcon Content Update Preliminary Post Incident Report	New order / filing / dataset revision / policy change / operational update materially affecting a C-ID.	Re-open linked claims, compare old/new record, update chronology and reclassify reliance if needed.
T02	CrowdStrike	Channel File 291 Incident: Root Cause Analysis is Available	New order / filing / dataset revision / policy change / operational update materially affecting a C-ID.	Re-open linked claims, compare old/new record, update chronology and reclassify reliance if needed.
T03	CrowdStrike	Executive Summary: Root Cause Analysis - Channel File 291	New order / filing / dataset revision / policy change / operational update materially affecting a C-ID.	Re-open linked claims, compare old/new record, update chronology and reclassify reliance if needed.
T04	Microsoft	Helping customers through the CrowdStrike outage	New order / filing / dataset revision / policy change / operational update materially affecting a C-ID.	Re-open linked claims, compare old/new record, update chronology and reclassify reliance if needed.
T05	CrowdStrike / SEC	CrowdStrike FY2025 Form 10-K	New order / filing / dataset revision / policy change / operational update materially affecting a C-ID.	Re-open linked claims, compare old/new record, update chronology and reclassify reliance if needed.
T06	CrowdStrike / SEC	CrowdStrike 2026 quarterly SEC filing	New order / filing / dataset revision / policy change / operational update materially affecting a C-ID.	Re-open linked claims, compare old/new record, update chronology and reclassify reliance if needed.
T07	Microsoft	Windows release health - resolved issues	New order / filing / dataset revision / policy change / operational update materially affecting a C-ID.	Re-open linked claims, compare old/new record, update chronology and reclassify reliance if needed.
T08	Cybersecurity and Infrastructure Security Agency	CISA alert - CrowdStrike Falcon content update for Windows hosts	New order / filing / dataset revision / policy change / operational update materially affecting a C-ID.	Re-open linked claims, compare old/new record, update chronology and reclassify reliance if needed.

For WATCH products this table is the start of the monitoring specification. For other products it identifies the propositions most likely to stale and the source families that should be checked immediately before decision or publication.

15. Finding-to-decision map

Finding	Claim	Evidence answer	Decision sensitivity	Next step
F1	C01	CrowdStrike's preliminary incident review identifies the affected window, Windows sensor versions and the	If weaker than stated, reassess scope, timing, value, control or reliance before proceeding.	Resolve linked gaps and inspect all cited S-IDs.
F2	C02	The available public record supports a bounded answer but not a project- or counterparty-specific certification.	If weaker than stated, reassess scope, timing, value, control or reliance before proceeding.	Resolve linked gaps and inspect all cited S-IDs.
F3	C03	The available public record supports a bounded answer but not a project- or counterparty-specific certification.	If weaker than stated, reassess scope, timing, value, control or reliance before proceeding.	Resolve linked gaps and inspect all cited S-IDs.
F4	C04	The available public record supports a bounded answer but not a project- or counterparty-specific certification.	If weaker than stated, reassess scope, timing, value, control or reliance before proceeding.	Resolve linked gaps and inspect all cited S-IDs.

16. Commissioned-matter extension specification

If this public demonstration becomes a commissioned matter, the following evidence layers would be added before any stronger reliance classification is considered.

Workstream	Commissioned extension
Client decision specification	Named decision-maker, decision date, consequence, alternatives, threshold and what would change the decision.
Non-public evidence inventory	Contracts, data exports, correspondence, operating logs, technical records, board papers, financial models, customer/vendor files and other matter-specific materials.
Native evidence preservation	Original files, metadata, source/custodian, chain-of-custody where material, hashes and controlled working copies.
Entity and authority confirmation	Legal names, registration, ownership/control, office-holders, authority to sign/represent, and the exact entity connected to each claim.
Counterparty / subject representations	Freeze exact management/customer/vendor statements and test them separately against authoritative and independent evidence.

Workstream	Commissioned extension
Specialist workstreams	Defined legal, engineering, actuarial, accounting, scientific, technical or forensic questions routed to qualified reviewers where needed.
Adversarial review	Independent hostile-scrutiny pass against the central conclusion, including steelman of the strongest contrary case.
Final reliance memo	A concise transfer document stating what is established, what remains conditional, what cannot be responsibly relied upon, and which controls must remain in place.

DOCUMENT 2

Claims-and-Evidence Matrix

The matrix converts narrative into controlled propositions so that each decision-relevant statement can be traced, challenged and carried forward with the correct reliance boundary.

How to use this document

- Use this matrix to test proposition-by-proposition support.
- A claim with Conditional reliance must travel with its qualification.
- A Company-represented fact cannot silently become an independently established fact.
- Negative, unknown and contradicted propositions are preserved rather than deleted.

Evidence-chain reading rule

Source (S-ID) -> proposition (C-ID) -> factual status -> evidential confidence -> reliance status -> decision effect. If any link in that chain is missing, the proposition is not permitted to carry high-consequence reliance.

Matrix control summary

Controlled propositions	18
Evidence sources	12
Claims without Source IDs	0
Negative / boundary propositions	Preserved explicitly
Three-axis classification	Factual Status | Evidential Confidence | Reliance Status
Rule	No proposition may be upgraded because it is repeated in derivative sources.

Interpretation guide

Axis	Meaning
Factual status	What kind of proposition is this? Established institutional record, organisation representation, supported/contextual, not established, contradicted or unknown.
Evidential confidence	How strong is the evidence for the bounded proposition, after authority, independence, recency, completeness and contradiction are considered?
Reliance status	What may the intended user responsibly do with it? Direct within scope, conditional, orientation only, or do not rely.
Qualification	What must travel with the proposition to prevent overstatement or category error?

ID	Proposition	Factual status	Confidence	Reliance	Source IDs	Qualification
C01	CrowdStrike's preliminary incident review identifies the affected window, Windows sensor versions and the	Supported by current record	High	Conditional - carry stated scope and qualifications	S01, S02, S03	Matter-specific non-public evidence may be required before transaction/operating reliance.
C02	The available public record supports a bounded answer but not a project- or counterparty-specific certification.	Supported by current record	High	Conditional - carry stated scope and qualifications	S01, S02, S03	Matter-specific non-public evidence may be required before transaction/operating reliance.

ID	Proposition	Factual status	Confidence	Reliance	Source IDs	Qualification
C03	The available public record supports a bounded answer but not a project- or counterparty-specific certification.	Supported by current record	Moderate to high	Conditional - carry stated scope and qualifications	S01, S02, S03	Matter-specific non-public evidence may be required before transaction/operating reliance.
C04	The available public record supports a bounded answer but not a project- or counterparty-specific certification.	Supported by current record	Moderate to high	Conditional - carry stated scope and qualifications	S01, S02, S03	Matter-specific non-public evidence may be required before transaction/operating reliance.
C05	The cited record supports this bounded proposition: Incident timing, affected systems and initial causal explanation	Organisation-represented	Moderate to high	Conditional; corroborate for high-consequence reliance	S01	Company-primary source
C06	The cited record supports this bounded proposition: Root-cause analysis publication and remediation framing	Organisation-represented	Moderate to high	Conditional; corroborate for high-consequence reliance	S02	Company-primary source
C07	The cited record supports this bounded proposition: Technical root-cause and mitigation summary	Organisation-represented	Moderate to high	Conditional; corroborate for high-consequence reliance	S03	Company-primary technical report
C08	The cited record supports this bounded proposition: Independent ecosystem evidence estimating approximately 8.5 million Windows devices affected.	Supported / contextual	Moderate	Conditional	S04	Microsoft estimate is not a complete count of every affected endpoint or economic loss.
C09	The cited record supports this bounded proposition: Regulatory filing recording material litigation, business impacts, risk disclosures and financial context after the incident.	Established in cited institutional record	High	Direct within stated scope	S05	Issuer filings contain management representations and litigation remain subject to change.
C10	The cited record supports this bounded proposition: Current regulatory filing updating litigation and government inquiry status, including appellate and Delta-related developments.	Established in cited institutional record	High	Direct within stated scope	S06	Pending litigation and inquiries are unresolved and must not be treated adjudicated liability.
C11	The cited record supports this bounded proposition: Independent platform-vendor operational record concerning remediation of the outage on Windows devices.	Supported / contextual	Moderate	Conditional	S07	Resolution of the incident does not certify CrowdStrike architecture or future release processes.
C12	The cited record supports this bounded proposition: U.S. government incident alert and remediation context.	Established in cited institutional record	High	Direct within stated scope	S08	Alert is operational guidance, not a complete root-cause investigation.
C13	The cited record supports this bounded proposition: Regulatory index for current and historical issuer filings used to refresh litigation/risk status.	Established in cited institutional record	High	Direct within stated scope	S09	Filing index is a navigation record; individual filings contain the substan evidence.
C14	The cited record supports this bounded proposition: Independent platform-vendor remediation tooling and recovery evidence.	Supported / contextual	Moderate	Conditional	S10	Recovery tool does not validate CrowdStrike future controls.
C15	The cited record supports this bounded proposition: Company-primary description of changes following the incident.	Organisation-represented	Moderate to high	Conditional; corroborate for high-consequence reliance	S11	Self-reported remediation is not independent assurance of control effectiveness.
C16	The cited record supports this bounded proposition: Independent ecosystem context on lessons and recovery after the incident.	Supported / contextual	Moderate	Conditional	S12	Vendor commentary is not an audit CrowdStrike.
C17	The existence of a corrective narrative does not by itself prove the reviewed system or process is now universally resilient.	Not established / boundary control	High	Do not rely beyond stated boundary	S01, S02, S03, S04	This negative proposition protects against overclaiming and defines th reliance boundary.
C18	The review does not convert unresolved legal, technical or specialist questions into established facts.	Not established / boundary control	High	Do not rely beyond stated boundary	S01, S02, S03, S04	This negative proposition protects against overclaiming and defines th reliance boundary.

Traceability test

- Every C-ID has at least one S-ID.
- Every material finding on the executive pages maps to a C-ID.
- Every S-ID states what it supports and what it does not prove.
- Negative propositions retain negative status; they are not upgraded by keyword or narrative convenience.
- Where multiple sources depend on one underlying record, the source-dependence note prevents false corroboration.

Proposition evidence cards

The matrix above is compact. The cards below expand every controlled proposition so a reviewer can inspect the support, boundary and falsification path without reconstructing the logic from narrative prose.

C01 - Controlled proposition

CrowdStrike's preliminary incident review identifies the affected window, Windows sensor versions and the

Factual status	Supported by current record
Evidential confidence	High
Reliance status	Conditional - carry stated scope and qualifications
Supporting sources	S01 - Falcon Content Update Preliminary Post Incident Report; S02 - Channel File 291 Incident: Root Cause Analysis is Available; S03 - Executive Summary: Root Cause Analysis - Channel File 291
Qualification / boundary	Matter-specific non-public evidence may be required before transaction/operating reliance.

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C02 - Controlled proposition

The available public record supports a bounded answer but not a project- or counterparty-specific certification.

Factual status	Supported by current record
Evidential confidence	High
Reliance status	Conditional - carry stated scope and qualifications
Supporting sources	S01 - Falcon Content Update Preliminary Post Incident Report; S02 - Channel File 291 Incident: Root Cause Analysis is Available; S03 - Executive Summary: Root Cause Analysis - Channel File 291
Qualification / boundary	Matter-specific non-public evidence may be required before transaction/operating reliance.

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C03 - Controlled proposition

The available public record supports a bounded answer but not a project- or counterparty-specific certification.

Factual status	Supported by current record
Evidential confidence	Moderate to high
Reliance status	Conditional - carry stated scope and qualifications
Supporting sources	S01 - Falcon Content Update Preliminary Post Incident Report; S02 - Channel File 291 Incident: Root Cause Analysis is Available; S03 - Executive Summary: Root Cause Analysis - Channel File 291
Qualification / boundary	Matter-specific non-public evidence may be required before transaction/operating reliance.

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C04 - Controlled proposition

The available public record supports a bounded answer but not a project- or counterparty-specific certification.

Factual status	Supported by current record
Evidential confidence	Moderate to high
Reliance status	Conditional - carry stated scope and qualifications

Supporting sources	S01 - Falcon Content Update Preliminary Post Incident Report; S02 - Channel File 291 Incident: Root Cause Analysis is Available; S03 - Executive Summary: Root Cause Analysis - Channel File 291
Qualification / boundary	Matter-specific non-public evidence may be required before transaction/operating reliance.

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C05 - Controlled proposition

The cited record supports this bounded proposition: Incident timing, affected systems and initial causal explanation

Factual status	Organisation-represented
Evidential confidence	Moderate to high
Reliance status	Conditional; corroborate for high-consequence reliance
Supporting sources	S01 - Falcon Content Update Preliminary Post Incident Report
Qualification / boundary	Company-primary source

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C06 - Controlled proposition

The cited record supports this bounded proposition: Root-cause analysis publication and remediation framing

Factual status	Organisation-represented
Evidential confidence	Moderate to high
Reliance status	Conditional; corroborate for high-consequence reliance
Supporting sources	S02 - Channel File 291 Incident: Root Cause Analysis is Available
Qualification / boundary	Company-primary source

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C07 - Controlled proposition

The cited record supports this bounded proposition: Technical root-cause and mitigation summary

Factual status	Organisation-represented
Evidential confidence	Moderate to high
Reliance status	Conditional; corroborate for high-consequence reliance
Supporting sources	S03 - Executive Summary: Root Cause Analysis - Channel File 291
Qualification / boundary	Company-primary technical report

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C08 - Controlled proposition

The cited record supports this bounded proposition: Independent ecosystem evidence estimating approximately 8.5 million Windows devices affected.

Factual status	Supported / contextual
Evidential confidence	Moderate
Reliance status	Conditional

Supporting sources	S04 - Helping customers through the CrowdStrike outage
Qualification / boundary	Microsoft estimate is not a complete count of every affected endpoint or economic loss.

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C09 - Controlled proposition

The cited record supports this bounded proposition: Regulatory filing recording material litigation, business impacts, risk disclosures and financial context after the incident.

Factual status	Established in cited institutional record
Evidential confidence	High
Reliance status	Direct within stated scope
Supporting sources	S05 - CrowdStrike FY2025 Form 10-K
Qualification / boundary	Issuer filings contain management representations and litigation remains subject to change.

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C10 - Controlled proposition

The cited record supports this bounded proposition: Current regulatory filing updating litigation and government inquiry status, including appellate and Delta-related developments.

Factual status	Established in cited institutional record
Evidential confidence	High
Reliance status	Direct within stated scope
Supporting sources	S06 - CrowdStrike 2026 quarterly SEC filing
Qualification / boundary	Pending litigation and inquiries are unresolved and must not be treated as adjudicated liability.

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C11 - Controlled proposition

The cited record supports this bounded proposition: Independent platform-vendor operational record concerning remediation of the outage on Windows devices.

Factual status	Supported / contextual
Evidential confidence	Moderate
Reliance status	Conditional
Supporting sources	S07 - Windows release health - resolved issues
Qualification / boundary	Resolution of the incident does not certify CrowdStrike architecture or future release processes.

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C12 - Controlled proposition

The cited record supports this bounded proposition: U.S. government incident alert and remediation context.

Factual status	Established in cited institutional record
Evidential confidence	High

Reliance status	Direct within stated scope
Supporting sources	S08 - CISA alert - CrowdStrike Falcon content update for Windows hosts
Qualification / boundary	Alert is operational guidance, not a complete root-cause investigation.

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C13 - Controlled proposition

The cited record supports this bounded proposition: Regulatory index for current and historical issuer filings used to refresh litigation/risk status.

Factual status	Established in cited institutional record
Evidential confidence	High
Reliance status	Direct within stated scope
Supporting sources	S09 - CrowdStrike SEC filings index
Qualification / boundary	Filing index is a navigation record; individual filings contain the substantive evidence.

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C14 - Controlled proposition

The cited record supports this bounded proposition: Independent platform-vendor remediation tooling and recovery evidence.

Factual status	Supported / contextual
Evidential confidence	Moderate
Reliance status	Conditional
Supporting sources	S10 - Microsoft recovery tool for CrowdStrike issue
Qualification / boundary	Recovery tool does not validate CrowdStrike future controls.

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C15 - Controlled proposition

The cited record supports this bounded proposition: Company-primary description of changes following the incident.

Factual status	Organisation-represented
Evidential confidence	Moderate to high
Reliance status	Conditional; corroborate for high-consequence reliance
Supporting sources	S11 - CrowdStrike remediation and resilience overview
Qualification / boundary	Self-reported remediation is not independent assurance of control effectiveness.

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C16 - Controlled proposition

The cited record supports this bounded proposition: Independent ecosystem context on lessons and recovery after the incident.

Factual status	Supported / contextual
Evidential confidence	Moderate

Reliance status	Conditional
Supporting sources	S12 - Windows ecosystem security and resilience blog
Qualification / boundary	Vendor commentary is not an audit of CrowdStrike.

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C17 - Controlled proposition

The existence of a corrective narrative does not by itself prove the reviewed system or process is now universally resilient.

Factual status	Not established / boundary control
Evidential confidence	High
Reliance status	Do not rely beyond stated boundary
Supporting sources	S01 - Falcon Content Update Preliminary Post Incident Report; S02 - Channel File 291 Incident: Root Cause Analysis is Available; S03 - Executive Summary: Root Cause Analysis - Channel File 291; S04 - Helping customers through the CrowdStrike outage
Qualification / boundary	This negative proposition protects against overclaiming and defines the reliance boundary.

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

C18 - Controlled proposition

The review does not convert unresolved legal, technical or specialist questions into established facts.

Factual status	Not established / boundary control
Evidential confidence	High
Reliance status	Do not rely beyond stated boundary
Supporting sources	S01 - Falcon Content Update Preliminary Post Incident Report; S02 - Channel File 291 Incident: Root Cause Analysis is Available; S03 - Executive Summary: Root Cause Analysis - Channel File 291; S04 - Helping customers through the CrowdStrike outage
Qualification / boundary	This negative proposition protects against overclaiming and defines the reliance boundary.

Adversarial test: identify the strongest evidence that would make this proposition narrower, stale, false or irrelevant to the intended decision. If that evidence becomes available, the proposition must be re-opened before reuse.

DOCUMENT 3

Master Chronology

Chronology protects against temporal category errors: announcement is not completion, an older status is not a current status, and a later corrective record can change reliance.

How to use this document

- Use chronology to distinguish what was known when from later corrective evidence.
- Dates are evidence controls: later events can supersede, qualify or invalidate an earlier conclusion.
- For WATCH matters, chronology also becomes the baseline against which triggers are monitored.

Evidence-chain reading rule

Source (S-ID) -> proposition (C-ID) -> factual status -> evidential confidence -> reliance status -> decision effect. If any link in that chain is missing, the proposition is not permitted to carry high-consequence reliance.

Chronology construction rule

Dates below derive from the controlled source register. Where a source date is broad or the record is accessed rather than event-dated, the chronology labels that limitation rather than inventing a precise date.

Date / vintage	Source	Event / record	Why it matters	Class
19 Jul 2024	S08	CISA alert - CrowdStrike Falcon content update for Windows hosts	U.S. government incident alert and remediation context.	Baseline / event / update
20 Jul 2024	S04	Helping customers through the CrowdStrike outage	Independent ecosystem evidence estimating approximately 8.5 million Windows devices affected.	Baseline / event / update
2024	S01	Falcon Content Update Preliminary Post Incident Report	Incident timing, affected systems and initial causal explanation	Baseline / event / update
2024	S03	Executive Summary: Root Cause Analysis - Channel File 291	Technical root-cause and mitigation summary	Baseline / event / update
2024	S10	Microsoft recovery tool for CrowdStrike issue	Independent platform-vendor remediation tooling and recovery evidence.	Baseline / event / update
2024	S12	Windows ecosystem security and resilience blog	Independent ecosystem context on lessons and recovery after the incident.	Baseline / event / update
6 Aug 2024	S02	Channel File 291 Incident: Root Cause Analysis is Available	Root-cause analysis publication and remediation framing	Baseline / event / update
FY ended 31 Jan 2025	S05	CrowdStrike FY2025 Form 10-K	Regulatory filing recording material litigation, business impacts, risk disclosures and financial context after the incident.	Baseline / event / update
Current / accessed 8 Sep 2026	S07	Windows release health - resolved issues	Independent platform-vendor operational record concerning remediation of the outage on Windows devices.	Baseline / event / update
Quarter ended 31 Jul 2026	S06	CrowdStrike 2026 quarterly SEC filing	Current regulatory filing updating litigation and government inquiry status, including appellate and Delta-related developments.	Baseline / event / update
Current	S09	CrowdStrike SEC filings index	Regulatory index for current and historical issuer filings used to refresh litigation/risk status.	Baseline / event / update
Post-incident	S11	CrowdStrike remediation and resilience overview	Company-primary description of changes following the incident.	Baseline / event / update

Chronology evidence notes

19 Jul 2024 | S08 | CISA alert - CrowdStrike Falcon content update for Windows hosts

U.S. government incident alert and remediation context.

Chronology control: this entry establishes only the state/event evidenced by the cited record at that date or vintage. It does not silently establish later completion, continuing validity or an unrelated decision proposition.

20 Jul 2024 | S04 | Helping customers through the CrowdStrike outage

Independent ecosystem evidence estimating approximately 8.5 million Windows devices affected.

Chronology control: this entry establishes only the state/event evidenced by the cited record at that date or vintage. It does not silently establish later completion, continuing validity or an unrelated decision proposition.

2024 | S01 | Falcon Content Update Preliminary Post Incident Report

Incident timing, affected systems and initial causal explanation

Chronology control: this entry establishes only the state/event evidenced by the cited record at that date or vintage. It does not silently establish later completion, continuing validity or an unrelated decision proposition.

2024 | S03 | Executive Summary: Root Cause Analysis - Channel File 291

Technical root-cause and mitigation summary

Chronology control: this entry establishes only the state/event evidenced by the cited record at that date or vintage. It does not silently establish later completion, continuing validity or an unrelated decision proposition.

2024 | S10 | Microsoft recovery tool for CrowdStrike issue

Independent platform-vendor remediation tooling and recovery evidence.

Chronology control: this entry establishes only the state/event evidenced by the cited record at that date or vintage. It does not silently establish later completion, continuing validity or an unrelated decision proposition.

2024 | S12 | Windows ecosystem security and resilience blog

Independent ecosystem context on lessons and recovery after the incident.

Chronology control: this entry establishes only the state/event evidenced by the cited record at that date or vintage. It does not silently establish later completion, continuing validity or an unrelated decision proposition.

6 Aug 2024 | S02 | Channel File 291 Incident: Root Cause Analysis is Available

Root-cause analysis publication and remediation framing

Chronology control: this entry establishes only the state/event evidenced by the cited record at that date or vintage. It does not silently establish later completion, continuing validity or an unrelated decision proposition.

FY ended 31 Jan 2025 | S05 | CrowdStrike FY2025 Form 10-K

Regulatory filing recording material litigation, business impacts, risk disclosures and financial context after the incident.

Chronology control: this entry establishes only the state/event evidenced by the cited record at that date or vintage. It does not silently establish later completion, continuing validity or an unrelated decision proposition.

Current / accessed 8 Sep 2026 | S07 | Windows release health - resolved issues

Independent platform-vendor operational record concerning remediation of the outage on Windows devices.

Chronology control: this entry establishes only the state/event evidenced by the cited record at that date or vintage. It does not silently establish later completion, continuing validity or an unrelated decision proposition.

Quarter ended 31 Jul 2026 | S06 | CrowdStrike 2026 quarterly SEC filing

Current regulatory filing updating litigation and government inquiry status, including appellate and Delta-related developments.

Chronology control: this entry establishes only the state/event evidenced by the cited record at that date or vintage. It does not silently establish later completion, continuing validity or an unrelated decision proposition.

Current | S09 | CrowdStrike SEC filings index

Regulatory index for current and historical issuer filings used to refresh litigation/risk status.

Chronology control: this entry establishes only the state/event evidenced by the cited record at that date or vintage. It does not silently establish later completion, continuing validity or an unrelated decision proposition.

Post-incident | S11 | CrowdStrike remediation and resilience overview

Company-primary description of changes following the incident.

Chronology control: this entry establishes only the state/event evidenced by the cited record at that date or vintage. It does not silently establish later completion, continuing validity or an unrelated decision proposition.

Temporal reliance controls

- Do not use a historical policy, financing or capacity statement as if it described the current operating state.
- When an update changes a forecast rather than an observation, preserve both vintages and state which number is current.
- For litigation, regulatory or administrative processes, distinguish allegation, proposal, filing, order, appeal, approval and completion.
- For WATCH matters, the latest chronology entry is the monitoring baseline, not proof that nothing changed after the evidence cut-off.

DOCUMENT 4

Source and Evidence Register

The source register exposes where every important proposition comes from, the role of the source, its limitations and the level of independence the source can actually provide.

How to use this document

- Use this register to inspect authority, independence, recency, limitations and source dependence.
- Every material source has a visible URL and a source role.
- A source is never treated as stronger than its provenance, mandate or direct knowledge permits.

Evidence-chain reading rule

Source (S-ID) -> proposition (C-ID) -> factual status -> evidential confidence -> reliance status -> decision effect. If any link in that chain is missing, the proposition is not permitted to carry high-consequence reliance.

Source-control principles

- Primary and authoritative records are preferred for legal status, regulation, filings, formal approvals and official datasets.
- Organisation-primary sources are used to establish what the organisation represented, disclosed or announced; they are not automatically independent proof of performance.
- Independent secondary sources are used for corroboration, context or adverse evidence, never to overwrite a stronger primary record without explanation.
- URLs are shown in full and made clickable. Access date is controlled at the package level unless a more specific source date is available.
- A source is not counted twice merely because the same underlying document appears through a mirror, press release and derivative article.

Source-dependence register

Domain / custodian	Source IDs	Dependence control
www.crowdstrike.com	S01, S02, S03, S11	Same-domain records checked for distinct document/event scope; not treated as independent corroboration merely because multiple URLs exist.
blogs.microsoft.com	S04	Same-domain records checked for distinct document/event scope; not treated as independent corroboration merely because multiple URLs exist.
www.sec.gov	S05, S06, S09	Same-domain records checked for distinct document/event scope; not treated as independent corroboration merely because multiple URLs exist.
learn.microsoft.com	S07	Same-domain records checked for distinct document/event scope; not treated as independent corroboration merely because multiple URLs exist.
www.cisa.gov	S08	Same-domain records checked for distinct document/event scope; not treated as independent corroboration merely because multiple URLs exist.
techcommunity.microsoft.com	S10	Same-domain records checked for distinct document/event scope; not treated as independent corroboration merely because multiple URLs exist.
blogs.windows.com	S12	Same-domain records checked for distinct document/event scope; not treated as independent corroboration merely because multiple URLs exist.

Evidence quality assessment

Source	Authority	Independence	Authenticity control	Recency	Quality	Reliance note
S01	Medium-high	Low - source is subject/issuer	URL/custodian recorded	Historical - retained for chronology	Moderate	Use only for the bounded proposition stated in the register.
S02	Medium-high	Low - source is subject/issuer	URL/custodian recorded	Historical - retained for chronology	Moderate	Use only for the bounded proposition stated in the register.
S03	Medium-high	Low - source is subject/issuer	URL/custodian recorded	Historical - retained for chronology	Moderate	Use only for the bounded proposition stated in the register.
S04	Medium	Independent / contextual	URL/custodian recorded	Historical - retained for chronology	Moderate	Use only for the bounded proposition stated in the register.
S05	High	Institutional / direct	URL/custodian recorded	Historical - retained for chronology	High	Use only for the bounded proposition stated in the register.
S06	High	Institutional / direct	URL/custodian recorded	Current / controlled vintage	High	Use only for the bounded proposition stated in the register.
S07	Medium	Independent / contextual	URL/custodian recorded	Current / controlled vintage	Moderate	Use only for the bounded proposition stated in the register.
S08	High	Institutional / direct	URL/custodian recorded	Historical - retained for chronology	High	Use only for the bounded proposition stated in the register.
S09	High	Institutional / direct	URL/custodian recorded	Current / controlled vintage	High	Use only for the bounded proposition stated in the register.
S10	Medium	Independent / contextual	URL/custodian recorded	Historical - retained for chronology	Moderate	Use only for the bounded proposition stated in the register.
S11	Medium-high	Low - source is subject/issuer	URL/custodian recorded	Historical - retained for chronology	Moderate	Use only for the bounded proposition stated in the register.
S12	Medium	Independent / contextual	URL/custodian recorded	Historical - retained for chronology	Moderate	Use only for the bounded proposition stated in the register.

Detailed evidence register

S01 - Falcon Content Update Preliminary Post Incident Report

Organisation / custodian	CrowdStrike
Date / vintage	2024
Source class	Organisation-primary / representation
Authority / confidence	Moderate to high
Evidence use	Incident timing, affected systems and initial causal explanation
Material limitation	Company-primary source
Accessed	8 September 2026
Supported C-IDs	C01, C02, C03, C04, C05, C17, C18

Visible source URL
https://www.crowdstrike.com/en-us/blog/falcon-content-update-preliminary-post-incident-report/

S02 - Channel File 291 Incident: Root Cause Analysis is Available

Organisation / custodian	CrowdStrike
Date / vintage	6 Aug 2024
Source class	Organisation-primary / representation
Authority / confidence	Moderate to high
Evidence use	Root-cause analysis publication and remediation framing
Material limitation	Company-primary source
Accessed	8 September 2026
Supported C-IDs	C01, C02, C03, C04, C06, C17, C18

Visible source URL
https://www.crowdstrike.com/en-us/blog/channel-file-291-rca-available/

S03 - Executive Summary: Root Cause Analysis - Channel File 291

Organisation / custodian	CrowdStrike
Date / vintage	2024
Source class	Organisation-primary / representation
Authority / confidence	Moderate to high
Evidence use	Technical root-cause and mitigation summary
Material limitation	Company-primary technical report
Accessed	8 September 2026
Supported C-IDs	C01, C02, C03, C04, C07, C17, C18

Visible source URL
https://www.crowdstrike.com/wp-content/uploads/2024/08/Executive-Summary_Root-Cause-Analysis_Channel-File-291.pdf

S04 - Helping customers through the CrowdStrike outage

Organisation / custodian	Microsoft
Date / vintage	20 Jul 2024
Source class	Independent / contextual
Authority / confidence	Moderate
Evidence use	Independent ecosystem evidence estimating approximately 8.5 million Windows devices affected.
Material limitation	Microsoft estimate is not a complete count of every affected endpoint or economic loss.
Accessed	8 September 2026
Supported C-IDs	C08, C17, C18

Visible source URL
https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/

S05 - CrowdStrike FY2025 Form 10-K

Organisation / custodian	CrowdStrike / SEC
Date / vintage	FY ended 31 Jan 2025
Source class	Authoritative / institutional primary
Authority / confidence	High
Evidence use	Regulatory filing recording material litigation, business impacts, risk disclosures and financial context after the incident.
Material limitation	Issuer filings contain management representations and litigation remains subject to change.
Accessed	8 September 2026
Supported C-IDs	C09

Visible source URL
https://www.sec.gov/Archives/edgar/data/1535527/000153552725000009/crwd-20250131.htm

S06 - CrowdStrike 2026 quarterly SEC filing

Organisation / custodian	CrowdStrike / SEC
Date / vintage	Quarter ended 31 Jul 2026
Source class	Authoritative / institutional primary
Authority / confidence	High
Evidence use	Current regulatory filing updating litigation and government inquiry status, including appellate and Delta-related developments.
Material limitation	Pending litigation and inquiries are unresolved and must not be treated as adjudicated liability.
Accessed	8 September 2026
Supported C-IDs	C10

Visible source URL
https://www.sec.gov/Archives/edgar/data/1535527/000153552726000031/crwd-20260731.htm

S07 - Windows release health - resolved issues

Organisation / custodian	Microsoft
Date / vintage	Current / accessed 8 Sep 2026
Source class	Independent / contextual
Authority / confidence	Moderate
Evidence use	Independent platform-vendor operational record concerning remediation of the outage on Windows devices.
Material limitation	Resolution of the incident does not certify CrowdStrike architecture or future release processes.
Accessed	8 September 2026
Supported C-IDs	C11

Visible source URL
https://learn.microsoft.com/en-us/windows/release-health/resolved-issues-windows-11-23H2

S08 - CISA alert - CrowdStrike Falcon content update for Windows hosts

Organisation / custodian	Cybersecurity and Infrastructure Security Agency
Date / vintage	19 Jul 2024
Source class	Authoritative / institutional primary
Authority / confidence	High
Evidence use	U.S. government incident alert and remediation context.
Material limitation	Alert is operational guidance, not a complete root-cause investigation.
Accessed	8 September 2026
Supported C-IDs	C12

Visible source URL
https://www.cisa.gov/news-events/alerts/2024/07/19/crowdstrike-falcon-content-update-windows-hosts

S09 - CrowdStrike SEC filings index

Organisation / custodian	U.S. Securities and Exchange Commission
Date / vintage	Current
Source class	Authoritative / institutional primary
Authority / confidence	High
Evidence use	Regulatory index for current and historical issuer filings used to refresh litigation/risk status.
Material limitation	Filing index is a navigation record; individual filings contain the substantive evidence.
Accessed	8 September 2026
Supported C-IDs	C13

Visible source URL
https://www.sec.gov/edgar/browse/?CIK=1535527&owner=exclude

S10 - Microsoft recovery tool for CrowdStrike issue

Organisation / custodian	Microsoft
Date / vintage	2024
Source class	Independent / contextual
Authority / confidence	Moderate
Evidence use	Independent platform-vendor remediation tooling and recovery evidence.
Material limitation	Recovery tool does not validate CrowdStrike future controls.
Accessed	8 September 2026
Supported C-IDs	C14

Visible source URL
https://techcommunity.microsoft.com/blog/windows-itpro-blog/new-recovery-tool-to-help-with-crowdstrike-issue-impacting-windows-endpoints/4196959

S11 - CrowdStrike remediation and resilience overview

Organisation / custodian	CrowdStrike
Date / vintage	Post-incident
Source class	Organisation-primary / representation
Authority / confidence	Moderate to high
Evidence use	Company-primary description of changes following the incident.
Material limitation	Self-reported remediation is not independent assurance of control effectiveness.
Accessed	8 September 2026
Supported C-IDs	C15

Visible source URL
https://www.crowdstrike.com/en-us/blog/technical-details-on-todays-outage/

S12 - Windows ecosystem security and resilience blog

Organisation / custodian	Microsoft
Date / vintage	2024
Source class	Independent / contextual
Authority / confidence	Moderate
Evidence use	Independent ecosystem context on lessons and recovery after the incident.
Material limitation	Vendor commentary is not an audit of CrowdStrike.
Accessed	8 September 2026
Supported C-IDs	C16

Visible source URL
https://blogs.windows.com/windowsexperience/2024/07/22/windows-security-best-practices-for-integrating-and-managing-security-tools/

Linked Aperture methodology references

Methodology
https://www.apertureforensic.com/methodology.html
Evidence standards
https://www.apertureforensic.com/evidence-standards.html
Evidence lineage
https://www.apertureforensic.com/evidence-lineage.html
Reliance boundary
https://www.apertureforensic.com/reliance-boundary.html
Selected Work
https://www.apertureforensic.com/selected-work.html
Search
https://www.apertureforensic.com/search.html
Languages
https://www.apertureforensic.com/languages.html
Enquiry
https://www.apertureforensic.com/enquiry.html
LinkedIn
https://www.linkedin.com/in/paul-hattingh-79568729

DOCUMENT 5

Public Portfolio Edition

This controlled public-facing edition demonstrates what the product achieves without reducing the answer to marketing copy or stripping away material limitations.

How to use this document

- This is the concise public-facing version of the evidence answer.
- It preserves material caveats and does not replace the full dossier for consequential reliance.
- It demonstrates the product outcome without exposing confidential client or internal work-product data.

Evidence-chain reading rule

Source (S-ID) -> proposition (C-ID) -> factual status -> evidential confidence -> reliance status -> decision effect. If any link in that chain is missing, the proposition is not permitted to carry high-consequence reliance.

CrowdStrike Cause and Remediation

Test the answer you already have. Challenge an existing narrative, report, model, assertion or conclusion before reliance.

Question

Did the public evidence establish both the cause of the July 2024 outage and the remediation that followed?

Answer supported by the public record

CrowdStrike's public technical record identifies a Rapid Response Content update as the trigger for the July 19, 2024 Windows crashes and later published a root-cause analysis with mitigations. That supports a strong account of the immediate mechanism and documented remediation steps. It does not, by itself, independently prove every long-term resilience claim or eliminate all future failure modes.

What is established or supported

- CrowdStrike's preliminary incident review identifies the affected window, Windows sensor versions and the
- The available public record supports a bounded answer but not a project- or counterparty-specific certification.
- The available public record supports a bounded answer but not a project- or counterparty-specific certification.
- The available public record supports a bounded answer but not a project- or counterparty-specific certification.

What remains conditional

- G01 - Penetration testing or independent source-code review. Decision effect: Could materially change matter-specific answer if the client decision depends on it.
- G02 - A warranty that the incident class cannot recur in another form. Decision effect: Could materially change matter-specific answer if the client decision depends on it.
- G03 - Cybersecurity legal advice or contractual interpretation. Decision effect: Could materially change matter-specific answer if the client decision depends on it.
- G04 - A complete assessment of all customer losses. Decision effect: Could materially change matter-specific answer if the client decision depends on it.
- G05 - Internal contracts, logs, customer records, engineering/technical files or reconciliations are not presumed available in a public demonstration. Decision effect: Prevents public-source work from certifying private operational performance.

Why this matters to a buyer / decision-maker

The value is independent challenge. The reviewed answer is decomposed into propositions so that evidence stronger, weaker or different from the original narrative changes reliance rather than being buried.

Decision-use summary

- C01: CrowdStrike's preliminary incident review identifies the affected window, Windows sensor versions and the [Conditional - carry stated scope and qualifications]
- C02: The available public record supports a bounded answer but not a project- or counterparty-specific certification. [Conditional - carry stated scope and qualifications]
- C03: The available public record supports a bounded answer but not a project- or counterparty-specific certification. [Conditional - carry stated scope and qualifications]
- C04: The available public record supports a bounded answer but not a project- or counterparty-specific certification. [Conditional - carry stated scope and qualifications]
- C05: The cited record supports this bounded proposition: Incident timing, affected systems and initial causal explanation [Conditional; corroborate for high-consequence reliance]
- C06: The cited record supports this bounded proposition: Root-cause analysis publication and remediation framing [Conditional; corroborate for high-consequence reliance]
- C07: The cited record supports this bounded proposition: Technical root-cause and mitigation summary [Conditional; corroborate for high-consequence reliance]
- C08: The cited record supports this bounded proposition: Independent ecosystem evidence estimating approximately 8.5 million Windows devices affected. [Conditional]

Public-source evidence base

12 controlled source records are listed in Document 4. The full URLs are visible and clickable. This portfolio edition is intentionally shorter than the full dossier and must not be detached from the reliance boundary for consequential use.

Aperture pathway

Product page

https://www.apertureforensic.com/review.html

Selected Work

https://www.apertureforensic.com/selected-work.html

Discuss a Matter

https://www.apertureforensic.com/enquiry.html

Search

https://www.apertureforensic.com/search.html

LinkedIn

https://www.linkedin.com/in/paul-hattingh-79568729

DOCUMENT 6

Final Delivery Manifest & Conformity Record

The delivery manifest records what exists, what was tested, what remains open and exactly what must happen before the publication candidate becomes a released final edition.

How to use this document

- Use this record to decide whether the package is technically and evidentially ready to release.
- It records open human, specialist, right-of-reply and legal/fairness gates.
- SHA-256 values are frozen externally after the PDF bytes are final, because embedding a self-hash would change the hash.

Evidence-chain reading rule

Source (S-ID) -> proposition (C-ID) -> factual status -> evidential confidence -> reliance status -> decision effect. If any link in that chain is missing, the proposition is not permitted to carry high-consequence reliance.

Delivery manifest

Matter	CrowdStrike Cause and Remediation
Product	REVIEW
Document code	APW-REV-260908-05
Filename	05_REVIEW_CrowdStrike_Cause_and_Remediation.pdf
Version	2.0 publication candidate
Governing master	PHW Research AI v11.0 Approved Governing Master
Evidence cut-off	8 September 2026, 07:38 SAST
Research readiness	95/100
Sources	12
Controlled claims	18
Pages	30
Visual identity	Aperture Research Works logo; navy #16233A; orange #FF7A00; cyan #00B8D9; secondary blue #4F81BD; product accent applied
Typography	Carlito / Carlito Bold headings; Liberation Sans / Liberation Sans Bold body, tables and footer
Public release	Pending final human approval of the frozen files
External hash	Recorded in V168_FINAL_PUBLICATION_MANIFEST.json after final byte freeze

Masjien conformity record

Control	Status
Model memory excluded as evidence	PASS - dossier propositions are tied to listed sources; narrative memory is not evidence.
Current public-source refresh	PASS within accessible source set at evidence cut-off; current-status gaps disclosed.
Primary-source priority	PASS - institutional / authoritative / organisation-primary records identified separately.
Claim-to-source register	PASS - every C-ID has S-ID support.
Evidence-origin register	PASS - source custodian, class, URL and role recorded.
Chronology register	PASS - source/event vintages retained.
Contradiction register	PASS - tensions preserved and controlled.
Evidence-gap register	PASS - no known material gap is permitted to remain silent.
Competing hypotheses / falsification	PASS - Document 1.
Three-axis classification	PASS - factual status, confidence, reliance.
Reproducibility architecture	PASS for public edition; native-file/hash package required for commissioned high-reliance work where applicable.
Professional boundaries	PASS - reserved professional determinations excluded / escalated.
Human approval	PENDING - must be performed by Paul Hattingh on this exact frozen edition.
Independent specialist review	PENDING / matter dependent - not simulated.
Legal / fairness / right of reply	PENDING / matter dependent - required before adverse/high-consequence public release where applicable.

Change register

Version / stage	Date	Change	Control status	
0.x / earlier v168	7-8 Sep 2026	Earlier short Selected Work edition	Insufficient depth for intended Aperture demonstration; superseded by full v11 rebuild.	Superseded Version 2.0.

Version / stage	Date	Change	Control status	
2.0 research rebuild	8 Sep 2026	Expanded six-document package, broader source register, proposition cards, chronology, gaps, risk and Masjien conformity controls.	Current publication candidate.	
2.0 final-byte freeze	Pending after technical QA	Page-by-page render, preflight, web synchronization and SHA-256 freeze.	Must occur before ZIP.	
2.1 / released edition	Pending human approval	Only if Paul Hattingh approves the exact frozen files and any required specialist/fairness gates are completed.	Not yet authorised.	

Technical publication preflight specification

Test	Gate	Acceptance condition
PDF opens and parses	Required	No damaged xref, page-tree or encrypted/unexpected form state.
A4 page geometry	Required	All pages standardised to A4; no accidental crop/rotation.
Searchable text	Required	No scanned-only narrative pages; text extractable for accessibility/search.
Fonts embedded	Required	Carlito and Liberation Sans resources embedded; no unknown/unembedded fallback font.
Hyperlinks	Required	Evidence URLs and Aperture navigation links preserved and clickable.
Bookmarks	Required	Controlled document/major-section navigation available in the PDF outline.
Visual render	Required	Every page rendered and checked for clipping, overlap, blank/sparse artefacts, dark blocks and broken glyphs.
Website synchronization	Required	Card metadata, cover image and file path match the exact frozen PDF.
Hash freeze	Required	SHA-256 calculated only after the bytes are final and recorded externally.
Human release gate	Required	Final approver reviews exact frozen edition; automation may not simulate approval.

Website synchronization checklist

- PDF filename remains stable so existing Selected Work/product links do not break.
- Rendered cover image is regenerated from page 1 of this exact PDF.
- Selected Work page reports exact page/source/claim counts from the final manifest.
- Product page routes to the same PDF and preserves product-specific positioning.
- Search index contains title, product, subject, evidence keywords and the PDF path.
- Search, Languages, Enquiry and LinkedIn are reachable from the English public navigation/footer.
- Local href/src/CSS url() audit passes from the Hostinger document root before ZIP.

Release gate

- Confirm the final PDF page count, source count, claim count, bookmarks and hyperlinks after the second-pass build.
- Render every page and inspect for clipping, overlap, broken glyphs, abnormal darkness and unintended sparse pages.
- Run PDF preflight and font audit; no unembedded or unknown font resource may remain.
- Update the website card metadata and cover image to the exact frozen PDF.
- Run the full-site local href/src/CSS-url audit from the Hostinger document root.
- Generate SHA-256 hashes only after the bytes are frozen and record them in the external publication manifest.
- Human approver reviews the frozen candidate and records approval. No automated process may simulate this gate.
- Only after the above should the complete Hostinger-ready directory be zipped and published.

Supersession control

This Version 2.0 publication candidate supersedes the earlier thin v168 Selected Work PDF of the same filename once the final website package is frozen. Earlier generated drafts remain non-authoritative and should not be uploaded alongside the released edition.

Contact and navigation

Website
https://www.apertureforensic.com/
Email
mailto:info@apertureforensic.com
LinkedIn
https://www.linkedin.com/in/paul-hattingh-79568729
Selected Work
https://www.apertureforensic.com/selected-work.html
Discuss a Matter
https://www.apertureforensic.com/enquiry.html

Final release-control panel

This panel is part of the controlled evidence product. It tells the final approver exactly what must remain attached to the conclusion when the dossier is transferred, updated or published.

Decision question	Retain the exact bounded question stated on the cover; do not broaden the conclusion after delivery.
Evidence chain	Any proposition reused outside this PDF must retain its C-ID, relevant S-ID(s), factual status, confidence and reliance qualification.
Open dependencies	Gaps, specialist boundaries, right-of-reply requirements and current-status triggers remain operative until separately closed.
Update rule	If a material source, status, event or governing rule changes after the evidence cut-off, re-open the affected proposition before reuse.
Release rule	Publish or circulate as a final Aperture product only after the exact frozen bytes, website metadata and external SHA-256 record are confirmed and human-approved.

Decision-transfer safeguard

- Do not detach the executive answer from the evidence cut-off and reliance boundary.
- Do not convert an organisation-primary representation into an independently established fact without corroboration.
- Do not treat an absence of contrary public evidence as proof that no contrary evidence exists.
- Where the decision becomes higher consequence than the public demonstration, commission the missing matter-specific evidence and specialist review before reliance.

END OF CONTROLLED PUBLICATION CANDIDATE