

Cyber Incident Executive Summary

Alerts to Answers Analyst Field Guide 08 - v21

Introduction

Use this guide to turn verified investigation findings into a concise executive summary that explains business impact, response status, residual risk, and the decision leadership needs to make. It extends the evidence record established during FG 07 triage into leadership reporting.

Chapter and Lab Alignment

Alignment	Placement
Primary chapter alignment	Chapter 7 - Digital Forensics and Incident Response
Supporting chapter alignment	Chapter 9 - Operating the Platform
Lab alignment	PL-08 capstone reporting and incident investigation write-ups
Recommended point of use	After initial triage and evidence validation; update as material facts or decisions change

Purpose and Scope

Purpose. Give leadership the verified facts needed to understand current business risk, decide, and allocate resources. Executives have limited bandwidth: signal, not noise. Order matters — Bottom Line Up Front. Target one-half page, ≤ 250 words, never more than one page.

“Two lines. One decision. Zero speculation.”

The two-line test: after reading only the first two lines, can the executive reader answer —

What happened? Is it controlled? What is the business risk? What decision or resource do you need from me (the executive), and by when?

Rules of the road

- **Not legal advice.** Legal and notification requirements change and differ by jurisdiction, sector, contract, and incident facts. Verify with authorized counsel and compliance before relying on any clock or obligation in this guide.
- **Executives read to decide.** End with the decision and its deadline — or say “No decision required.”
- **Facts are labeled.** Confirmed / Assessed / Suspected / Ruled out / Unknown for facts; low / moderate / high confidence for judgments.
- **Numbers beat adjectives.** “14 of 220 servers (6%)” not “a significant number.” Give ranges with confidence.
- **Bound every “no evidence” claim.** Name the telemetry, systems, and time range checked (§3).
- **Containment is proven, not inferred.** A drop in alerts is not containment; confirm attack path, persistence, and scope are addressed.
- **Absolute time only.** UTC plus local, ISO 8601. Never “earlier today.” Detection time starts most clocks.
- **Translate, then tag.** “Stolen VPN credentials were used (T1078)” — executives get the story, the SOC gets the ID.
- **Banned words:** possibly, believed to be, sophisticated, widely exploited, significant, advanced, breach. Replace with a labeled fact, number, or confidence. “Breach” is a legal conclusion: only counsel, after reviewing the facts against applicable statutes and contracts, declares one. Until then it is an incident.
- **No attribution in writing** until evidence supports it, it is qualified, and counsel approves.
- **Write it last; draft freely, then compress.** Cut any sentence that does not change understanding, risk, action, timing, or accountability. Raw indicators, logs, and full timelines go to the technical record; hyperlinks follow Supplement C.
- **Assume discovery.** Regulators, insurers, auditors, or opposing counsel may read this later. Timestamp, version, retain, control distribution; correct by new version, never overwrite.
- **The subject line does work.** “[TLP:AMBER] Incident 2026-017 — Contained — 2-min read — 1 decision by 1700.”

1. Fast Workflow

Step	Action
1 Verify	Confirm material facts, scope, evidence coverage, and response state before writing.
2 Translate	Convert technical findings into business impact, residual risk, and operational consequence.
3 Draft BLUF	Write the first two lines first. They must stand alone.
4 Assign	Every material action and decision gets an owner and a due time.
5 Challenge	Test every “no evidence,” “contained,” “recovered,” and attribution claim against the evidence boundary.
6 Release	Apply handling marking, check every link (Supplement C), preserve the version, verify distribution, state next update time or trigger.

Context line (first line of every summary)

Incident ID & name | Severity | Executive owner | Incident lead | Current as of <date, time, zone> | v# | TLP | Privileged: Y/N (only if counsel directs) | Next update

Example: Incident 2026-017 Contractor-VPN | Severity HIGH | Exec owner: CIO | Lead: J. Analyst x4421 | Current as of 2026-09-16 14:30 UTC (10:30 ET) | v3 | TLP:AMBER | Privileged: Y (per counsel) | Next update 16 Sep 22:00 UTC

2. Executive Summary Order and Word Budget

Section	Budget	What Leadership Needs
1 Bottom Line Up Front	≤ 40 words	What happened, to what, is it over; Business consequence; decision required Y/N; Incident type: phishing, stolen credentials, web exploit, ransomware, insider, third party, unknown;
2 Executive Risk Statement	1 sentence	[MOST IMPORTANT] Why this matters now; Lead with Severity on the defined scale (§4);
3 Current Status	1–2 lines	Investigation, containment, eradication, recovery, residual risk — each stated (§3); What changed since the prior version;
4 Detection and Timeline	≤ 30 words	First activity (if known); detected when, how, by whom; declared when; Dwell time; Absolute timestamps with zone;
5 Scope and Impact	≤ 50 words	Confirmed vs. potentially affected; counts with denominators (42 of 318 hosts); Data with evidence label and what was checked; Operational, financial, legal, privacy, customer, safety, reputational impact; Ratings: Functional Information Recoverability;
6 Threat Activity	≤ 40 words	Observed behavior in plain English — entry, persistence, movement — ATT&CK/CVE in parentheses; Confidence; if root cause unconfirmed, leading hypothesis and validation date; No attribution unless evidence-supported, qualified, counsel-approved;
7 Response and Recovery	≤ 40 words	Containment, eradication, evidence preservation, restoration, validation — timestamped and owned; States: DONE IN PROGRESS PLANNED BLOCKED VALIDATED; Recovery is complete only when the business owner accepts it;
8 Known Unknowns	≤ 3 bullets	What cannot yet be said, why it matters, when the answer is expected;
9 Decisions and Next Steps	≤ 50 words	Decision Owner Deadline Options/tradeoff Cost of delay Recommendation — or “No decision required”; Immediate actions (24–48 h) with owner and date; Clocks: regulatory, contractual, insurance, customer; notifications made; Post-incident review date;

3. Status and Evidence Discipline

3.1 Status dimensions

Status is multidimensional. Report every dimension; never collapse it to one word. An incident can be contained while eradication is in progress and recovery has not started.

Dimension	Vocabulary	Question Answered
Investigation (DETECT)	Active Monitoring Closed	Are facts and scope still being established?
Containment (RESPOND)	Not contained Partial Contained	Has spread or further harm been stopped?
Eradication (RESPOND)	Not started In progress Complete Validated	Are access, persistence, and enabling conditions removed?
Recovery (RECOVER)	Not started In progress Restored Validated	Are services restored and accepted by the business owner?
Residual risk (GOVERN / IDENTIFY)	Critical High Moderate Low	What exposure remains after current controls? State it even when Low.

Dimensions follow the NIST SP 800-61r3 lifecycle mapped to CSF 2.0 Functions: Detect DE.AE; Respond RS.MI containment and eradication; Recover RC.RP; Govern / Identify GV.RM, ID.RA residual risk.

3.2 Evidence and confidence labels

Label	Meaning
Confirmed	Supported by validated evidence.
Assessed	Most likely explanation on current evidence; state confidence (low / moderate / high).
Suspected	Plausible, not sufficiently validated.
Ruled out	Excluded within a stated scope and visibility; name what was checked.
Unknown	Evidence unavailable or analysis incomplete; say when it will be known.

Source: adapted from ODNI ICD 203, Analytic Standards (separate information from judgment; express confidence as low / moderate / high) and NIST SP 800-61 Rev. 2 §3.2.7 (incident records distinguish confirmed from suspected). The five-label set is a Kalos convention built on those standards.

“No evidence” statements — state the visibility boundary

A visibility boundary is the edge of what you actually looked at: which data sources, which systems, which time window. Inside it you can say what you did and did not find; outside it you know nothing, so a claim that reaches past it is a guess dressed as a finding. Plain terms: “I checked every room on the second floor between 8 and 10 pm and saw no one” is bounded; “nobody was in the house” claims rooms and hours you never checked.

Statement	Verdict	Why
“No data was stolen.”	Not defensible	Claims a fact about everything, everywhere, at all times. You checked some sources for some period; the sentence promises more than the evidence covers.
“No evidence of exfiltration was found.”	Not defensible	Unbounded — found where? for when? The reader assumes you looked everywhere.
“No evidence of exfiltration was identified in 30 days of egress NetFlow and EDR telemetry from the 3 affected hosts.”	Defensible	Names the sources (NetFlow, EDR), the systems (3 affected hosts), and the window (30 days). Anything outside that is explicitly still unknown and can be listed under Known Unknowns.

Rule: absence of evidence inside a stated boundary is a finding; absence of evidence with no boundary is an assumption.

3.3 Composite status shorthand

A composite status is one phrase that says where the incident sits in the lifecycle — for the subject line, status board, or first words of the status line. It introduces the 3.1 dimensions; it never replaces them: “Contained – Monitoring: investigation active; contained; eradication in progress; recovery not started; residual risk Moderate.” Each state also tells leadership what to focus on.

Composite Status	Typical Dimensions	Leadership Focus
Ongoing – Active Threat	Investigation active; not or partially contained	Decide: isolation, shutdown, external forensics, counsel or IR retainer.
Contained – Monitoring	Contained; eradication and recovery incomplete	Risk persists; recovery timeline uncertain.
Eradicated – Recovering	Eradication complete; recovery in progress	Recovery progress, residual data risk, business-owner validation.
Resolved – Post-Incident	Investigation closed; recovery validated	Root cause, lessons learned, control improvements, risk register.

Source: the four states follow the NIST SP 800-61 Rev. 2 lifecycle (Detection and Analysis; Containment, Eradication, and Recovery; Post-Incident Activity) as carried into Rev. 3 and the CSF 2.0 Respond and Recover Functions. State names and the Leadership Focus column are Kalos conventions; use the IR plan’s approved terms where defined.

4. Severity and Impact Scale

Axis	Levels
Functional	None · Low (minor efficiency loss) · Medium (critical service lost for some users) · High (critical service lost for all users)
Information	None · Privacy breach (PII) · Proprietary breach · Integrity loss (data altered or destroyed)
Recoverability	Regular (existing resources) · Supplemented (added resources) · Extended (outside help, unpredictable) · Not recoverable
Overall Severity	High / Medium / Low — the worst of the three axes; or CISA NCISS when federal partners are involved

Default scale: NIST SP 800-61 Rev. 2 §3.2.6 (Tables 3-2 to 3-4). Pick one scale, define it in the IR plan, and use it on every incident so incidents are comparable across quarters.

5. Governance and Disclosure Checkpoints

Question	Record
Crosses a board or executive escalation threshold?	Yes / No / Under review
Regulatory disclosure status (SEC 8-K Item 1.05, GDPR Art. 33, HIPAA, state law, sector rule)?	Determined / In progress / Ruled out
Any statutory, contractual, insurance, or customer notification clock running?	Trigger event, owner, deadline, approval authority
Counsel engaged? Work directed by counsel?	Privilege only when counsel directs the work — not because counsel was copied
Handling marking correct?	TLP governs sharing; it is not privilege or classification
Legal, privacy, compliance, insurer, public affairs, law enforcement, third parties notified?	Date each
Risk register update or accountability gap? Post-incident review scheduled?	Yes / No; date and owner

6. Pre-Send Checklist

Incident ID: _____ Version: ____ Analyst: _____ Date/time (UTC): _____

Done	Requirement
☐	Context line complete: ID, severity, owners, as-of time with zone, version, TLP, privilege, next update
☐	Two-line test passes; incident type named
☐	Severity on the defined scale; risk statement is one sentence
☐	Investigation, containment, eradication, recovery, residual risk stated separately; change since last version named
☐	Every fact labeled; every judgment has a confidence; every “no evidence” claim is bounded
☐	Counts have denominators or say why the total is unknown
☐	No banned words (including “breach” unless counsel has declared one), unsupported attribution, or unexplained acronyms
☐	Actions timestamped and owned; DONE vs. IN PROGRESS separated; evidence preserved
☐	Known unknowns state why they matter and when resolved
☐	Decision has owner, deadline, options, cost of delay — or “none”
☐	Regulatory, contractual, insurance, and customer clocks reviewed with the authorized owner
☐	≤ 1 page; raw indicators in appendix; prior version retained
☐	Links: no active links to indicators, malware, or untrusted sites; malicious URLs defanged; link text descriptive (Supplement C)
☐	Distribution list and handling marking verified before sending

Approved for distribution by: _____ Time (UTC): _____

Supplement A. Executive Summary Outline (copy and fill)

Strip everything else away. Fill each block in order, stay inside the budget, delete any block that has nothing material and write "None." Total ≤ 250 words, one page.

Block	Content to complete
Context line	Incident ID & name: _____ Severity: _____ Exec owner: _____ Incident lead / contact: _____ Current as of: ____-____-____:____ UTC (____:____ local) v____ TLP: _____ Privileged: Y / N Next update: _____
1 BLUF (≤ 40 words)	What happened: _____ To what / whom: _____ Is it over: Yes / No / Partly Business consequence: _____ Decision required: Yes / No Incident type: phishing / stolen credentials / web exploit / ransomware / insider / third party / unknown
2 Executive Risk (1 sentence)	Severity: HIGH / MEDIUM / LOW — Why it matters now: _____
3 Current Status (1–2 lines)	Composite: Ongoing–Active / Contained–Monitoring / Eradicated–Recovering / Resolved Investigation: _____ Containment: _____ Eradication: _____ Recovery: _____ Residual risk: _____ Changed since v____: _____
4 Detection & Timeline (≤ 30 words)	Detected: ____-____-____:____ UTC by _____ (source) / _____ (team) Earliest activity: ____-____-____:____ Dwell time: ____ days Declared: ____-____-____:____ UTC
5 Scope & Impact (≤ 50 words)	Systems: ____ of ____ (____%) Accounts: ____ of ____ Records: _____ Data: _____ — Confirmed / Suspected / Ruled out / Unknown — checked via: _____ Impact: operational _____ financial _____ legal/privacy _____ customer _____ Functional: _____ Information: _____ Recoverability: _____
6 Threat Activity (≤ 40 words)	Observed behavior (plain English): _____ (ATT&CK _____ / CVE _____) Confidence: Low / Moderate / High Root cause: Confirmed / Hypothesis: _____ validate by _____ Attribution: None
7 Response & Recovery (≤ 40 words)	DONE: ____:____ (owner) ____:____ (owner) IN PROGRESS / PLANNED / BLOCKED: _____ (owner, ETA _____) Evidence preserved: Yes / No Monitoring: _____
8 Known Unknowns (≤ 3)	(1) _____ — why it matters: _____ — expected: _____ (2) _____ — why it matters: _____ — expected: _____
9 Decisions & Next Steps (≤ 50 words)	Decision: _____ Owner: _____ Deadline: _____ Options: _____ Cost of delay: _____ Recommend: _____ — or — No decision required. Immediate actions (24–48 h): _____ (owner, date) Clocks: regulatory _____ contractual _____ insurance _____ customer _____ Notified: _____ Post-incident review: _____

Supplement B. Worked Example (fictional, annotated)

Block	Executive Summary Content
Context line	Incident 2026-017 Contractor-VPN Severity HIGH Exec owner: CIO Lead: J. Analyst x4421 Current as of 2026-09-16 14:30 UTC (10:30 ET) v3 TLP:AMBER Privileged: Y (per counsel) Next update 16 Sep 22:00 UTC
BLUF	An attacker used a stolen contractor VPN credential to access three Engineering file servers and copied ~4 GB of design documents to an external cloud account. Access is cut off; no customer or employee PII is involved; one decision is required by 17 Sep 12:00 UTC.
Executive Risk	Severity HIGH (Information: proprietary breach; Recoverability: supplemented). Primary risk is IP loss and contractual notification to two customers whose designs were in scope.
Status	Contained – Monitoring. Investigation active; contained; eradication in progress; recovery not required (nothing destroyed). Residual risk Moderate: six related contractor accounts under review. Changed since v2: PII ruled out.
Detection	15 Sep 02:10 UTC, EDR alert (SOC). Earliest attacker login 11 Sep — dwell time 4 days. Declared 15 Sep 03:30 UTC.
Scope & Impact	3 of 41 file servers (7%). 1 account Confirmed; 6 Unknown (review by 22:00). Engineering drawings: Confirmed. Customer PII: Ruled out (DLP + share ACL review). Functional Low Information Proprietary Recoverability Supplemented.
Threat Activity	Valid-account VPN login (T1078); file discovery and transfer to cloud storage (T1567.002). Volume Assessed, moderate confidence. No attribution.
Response	DONE — 15 Sep 02:40 credential disabled, session killed (SOC); 03:15 hosts isolated (EDR); disk and log images preserved. IN PROGRESS — contractor account rotation (IAM, ETA 16 Sep 22:00); enhanced egress monitoring 14 days.
Known Unknowns	(1) Exact file list — expected 17 Sep. (2) Use of the 6 remaining accounts — expected 16 Sep 22:00.
Decisions & Next Steps	(1) Approve customer notification draft by 17 Sep 12:00 UTC (Legal); delay risks contract breach. (2) Approve MFA enforcement for contractor VPN, est. 2 days disruption for 40 contractors (CIO). Regulatory clock: none. Contractual clock: 5 business days from confirmation. Insurer notified 15 Sep. Post-incident review 30 Sep.

Why it works: the first two lines carry attack, assets, data consequence, and containment state; every scope claim has a number or evidence boundary; IDs support the narrative; actions are timestamped and owned; unknowns have dates; leadership gets two decisions with deadlines and cost of delay.

Deliberately excluded: IP addresses, hashes, alert names, screenshots, commands, full chronology, unverified actor claims — those live in the technical record unless one changes an executive decision.

Supplement C. Handling Links in Reports

Links support the report.

They are never the only location of critical evidence, and a link must never be the thing that causes the next incident.

Pragmatic rules

- **Standard stakeholder reports:** active links are acceptable for trusted, supplementary references (vendor documentation, CVE databases, NIST publications).
- **Sensitive forensic and executive reports:** limit active links to trusted, **personally validated** authoritative sources. When in doubt, plain-text citation.
- **High-risk indicators: ALWAYS defanged and non-clickable.** No exceptions, in any report, to any audience.
- **High-security environments:** plain-text citations or a non-clickable references appendix only.

Poor professional judgment

- An active link that points to a malicious or untrusted URL, replaces essential written content, or is delivered to an audience where one click could trigger a security incident.
- Unverified active links of any kind — unnecessary risk, and it reads as careless.
- Active links to malware, exploit repositories, suspicious domains, or live indicators.

1. Defang sensitive or malicious URLs

- Any URL pointing to attacker infrastructure, a threat actor, or an untrusted site is rendered inert: `hxxp://` for `http://`, `hxxps://` for the dot — e.g., `hxxps://evil-domain[.]example/payload`.
- Show the organization and domain in the visible text; strip URL shorteners and redirects so the true destination is readable.

2. Prioritize content over links

- Vulnerability mechanics, impact, and remediation steps exist as plain text in the document. If every link dies, the report is still actionable.
- Preserve critical source material separately (PDF, screenshot, archived copy); a link can change or disappear.

3. Use descriptive link text

- No raw URLs, no “click here.” Say where the link goes: “See the OWASP SQL Injection Prevention Cheat Sheet,” not “<https://owasp.org/...>”.

4. Contextualize references — help them help themselves

- A raw link dump (scanner output) adds nothing. Add one sentence on why the reference matters to this environment or finding.

Executive summary rule: the one-page summary carries no active links at all. Anything worth linking belongs in the technical report or this appendix.

References

Cybersecurity and Infrastructure Security Agency. (n.d.). CISA National Cyber Incident Scoring System (NCISS). U.S. Department of Homeland Security. <https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss>

Cybersecurity and Infrastructure Security Agency. (n.d.). Federal incident notification guidelines. U.S. Department of Homeland Security. <https://www.cisa.gov/federal-incident-notification-guidelines>

Forum of Incident Response and Security Teams. (2022). Traffic Light Protocol (TLP) 2.0. <https://www.first.org/tlp/>

MITRE. (n.d.). MITRE ATT&CK: Enterprise matrix. <https://attack.mitre.org/>

National Institute of Standards and Technology. (2012). Computer security incident handling guide (NIST Special Publication 800-61 Rev. 2). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-61r2>

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>

National Institute of Standards and Technology. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST Special Publication 800-61 Rev. 3). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-61r3>

Office of the Director of National Intelligence. (2015). Intelligence Community Directive 203: Analytic standards. <https://www.dni.gov/>

U.S. Department of the Army. (2020). Preparing and managing correspondence (Army Regulation 25-50). <https://armypubs.army.mil/>

Reporting clocks referenced in this guide (SEC Form 8-K Item 1.05; GDPR Article 33; CIRCIA; HIPAA Breach Notification Rule; NYDFS 23 NYCRR 500; DFARS 252.204-7012) are statutory and regulatory instruments; verify current text with counsel before use.