

Kill-Chain Gap Overlay

IR Packet

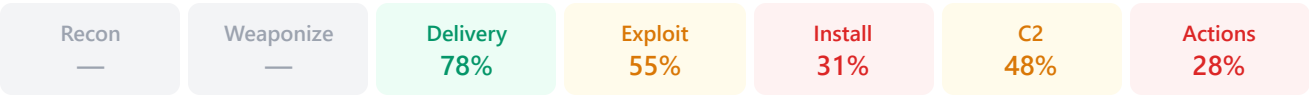
Client Company — observed incident techniques mapped against assessed control coverage

Generated: 2026-08-25 (sample scenario) Scenario: Ransomware intrusion — 8 techniques entered

Framework: CIS Controls v8.1

Coverage across the kill chain

Each phase shows how well the organization's assessed controls cover the entered techniques that land in that phase. Low coverage explains where the attacker likely progressed unopposed.



Lockheed Martin Cyber Kill Chain® phases · MITRE ATT&CK® technique positioning · — = no entered techniques in phase

Coverage disclosure: 7 of the 8 entered techniques have control mappings in CIS v8.1. One (T1657 — Financial Theft) has no mapped controls in this framework and is excluded from all percentages above. Percentages describe mapped techniques only.

Technique-by-technique

TECHNIQUE	PHASE	YOUR COVERAGE	READING
T1566.001 Spearphishing Attachment Defended by: 9.2, 9.6, 14.2 (best score 3/4)	Delivery	Strong	Mail filtering and awareness training are in place; delivery likely required user action to succeed.

T1204.002 User Execution: Malicious File Defended by: 2.5, 2.7, 10.1 (best score 4/4)	Exploitation	Strong	Anti-malware scored full marks; expect EDR telemetry for the execution event — pull it.
T1078 Valid Accounts Defended by: 5.3, 6.3, 6.5 (best score 2/4 on admin MFA)	Exploitation	Partial	Admin MFA gap (6.5 at 2/4) makes credentialed access plausible. Review privileged sign-ins first.
T1021.001 Remote Services: RDP Defended by: 4.6, 12.2 (best score 2/4)	Installation	Gap	Flat network and weak remote-service hardening — lateral movement over RDP was likely unimpeded.
T1003.001 OS Credential Dumping: LSASS Defended by: 10.7 (best score 3/4)	Installation	Partial	Behavioral EDR may have alerted; check EDR history for LSASS access events.
T1071.001 Application Layer Protocol: Web Defended by: 13.3, 13.8 (best score 2/4)	Command & Control	Partial	Limited network monitoring; C2 detection depends on firewall egress logs — preserve them now.
T1490 Inhibit System Recovery Defended by: 11.4 (best score 2/4)	Actions on Objectives	Gap	Backup isolation incomplete — assume shadow copies and reachable backups were targeted. Verify offline copies before recovery planning.
T1486 Data Encrypted for Impact Defended by: 11.1, 11.2 (best score 3/4)	Actions on Objectives	Partial	Recovery capability exists on paper; restore testing is stale (11.5 at 1/4). Recovery timeline is uncertain.

T1657 Financial Theft
No mapped controls in
CIS v8.1

Actions on
Objectives

Unmapped

Not scored — coverage unknown, not covered. Treat business-process controls (payment verification) as out of framework scope.

Containment actions, sorted by what you can actually execute

Executable now — capability confirmed by assessment

- Isolate affected hosts via the EDR console (Malware Defenses in place).
- Disable compromised accounts and revoke sessions in Entra ID (identity platform known and managed).
- Scope affected assets from the maintained inventory (Control 1 in place).
- Block delivery-stage indicators in M365 mail filtering.

Assumes capability the assessment says is missing or weak

- "Review 90 days of centralized logs" — retention beyond ~30 days not assured (8.10/8.11 low). Collect endpoint-local logs instead.
- "Restore from offline backups" — isolation incomplete, restores untested for over a year (11.4/11.5). Validate a clean copy first.
- "Contain to the affected VLAN" — no meaningful segmentation exists (12.2/12.8). Plan containment host-by-host.

Coverage reflects the organization's self-assessed control maturity, not observed defensive performance in this incident. Techniques without mappings in the selected framework are excluded from percentages and flagged, never silently dropped.

Sample uses a representative ransomware technique set. In the shipped feature, responders enter observed technique IDs (or pick a threat-actor profile) and this overlay is computed on demand against the organization's current assessment.