INCIDENT FORENSIC REPORT

Incident ID: c0effc79...

Full ID: c0effc79-a6a0-46c3-972c-c5fc40194bba

Severity	State	Confidence	Processing Time
CRITICAL	CLOSED	95.0%	62 seconds

1. EXECUTIVE SUMMARY

False positive: No supporting evidence found for alleged data exfiltration campaign

FALSE POSITIVE - Auto-Dismissed

Swarm Analysis Metrics

Human Hours Saved	Parallel Agents	Tool Calls	Tokens Used
5 hrs	8	55	59,354

2. AGENT ANALYSIS

2.1 THE JURY - Verdict & Logic

Core analysis agents responsible for verdict.

TRIAGE | Confidence: 95% | Tokens: 735

This incident has a CRITICAL severity, which contributes a severity weight of 1.0 to the priority score. The high confidence in the detection, combined with the significant impact of a compromised admin account and data exfiltration from a critical file server, result in a very high priority score. The recency of the event also adds to the urgency. This incident requires immediate attention from the security team.

CORRELATOR | Confidence: 90% | Tokens: 11,166

The analysis of the pre-fetched data indicates that this is likely part of a coordinated campaign. The same IP address, user, and host are involved in multiple related incidents within a short timeframe, suggesting an ongoing attack. The shared entities and kill chain stages observed across the incidents point to a multi-stage campaign targeting this organization. While some of the individual incidents were initially marked as false positives, the broader context reveals a more concerning pattern of activity that requires further investigation and response.

ANALYST | Confidence: 95% | Tokens: 7,797

This alert lacks any corroborating evidence despite involving critical entities (admin user, file server, external IP). The complete absence of supporting logs across multiple data sources (SIEM, EDR, identity systems) over a 72-hour period strongly indicates a false positive. The IP address appears to be non-existent (no WHOIS data, failed reverse DNS), the user shows no activity, and the file server has no running processes. A genuine data exfiltration campaign would generate multiple observable artifacts. The DLP system likely triggered on benign activity or experienced a configuration error.

2.2 INTEL & ORIGIN - The Proof

Threat intelligence and forensic evidence.

DATAGUARD | Confidence: 80% | Tokens: 3,782

The event details indicate a potential data exfiltration attempt from a compromised admin account on a critical FILESERVER host. While the IP address does not have any known malicious reputation, the lack of enrichment data and the high-risk nature of the compromised admin account on a sensitive server suggest this is a credible threat that requires further investigation. Additional monitoring and analysis of user activity and data transfers from this host would be prudent to detect and prevent any actual data loss.

HUNTER | Confidence: 70% | Tokens: 6,102

The IP address 198.51.100.77 has a low reputation score in VirusTotal and no abuse reports in AbuseIPDB, which could indicate suspicious activity. Additionally, the hostname 'FILESERVER' could not be resolved, which may be an attempt to hide the true identity of the host. These findings warrant further investigation to determine if this is a legitimate activity or a potential threat.

INTEL | Confidence: 52% | Tokens: 5,061

The IP address 198.51.100.77 has a low VirusTotal reputation score of 0, indicating it is not currently associated with known malicious activity. AbuseIPDB also shows no abuse reports for this IP, further suggesting it is not a high-risk IP address. However, the lack of additional context from Shodan and GreyNoise means I cannot fully rule out the possibility of this IP being involved in suspicious activity. Additional investigation may be warranted.

FORENSICS | Confidence: 90% | Tokens: 1,920

Critical data exfiltration campaign requires comprehensive forensic collection. Priority evidence: 1) Memory capture from FILESERVER to preserve volatile artifacts including process memory, network connections, and encryption keys. 2) Full disk imaging to capture file system artifacts, deleted files, and timeline evidence. 3) Network capture targeting suspicious IP 198.51.100.77 to document exfiltration methods and data volumes. 4) Security logs preservation covering 4-hour window to establish attack timeline. Chain of custody initiated with forensics agent as primary collector, requiring secondary verification before analysis. All artifacts stored in incident-specific directory structure for legal admissibility.

BEHAVIORAL | Confidence: 80% | Tokens: 4,150

The IP address 198.51.100.77 has a low VirusTotal reputation score of 0 and an AbuseIPDB abuse score of 0, indicating it may be associated with malicious activity. This IP address was involved in an exfiltration event from the 'compromised_admin' user account on the 'FILESERVER' host. This suggests the user account may be compromised and being used for malicious data exfiltration. The combination of the low IP reputation, privileged user account, and exfiltration event results in a high confidence that this is a user account compromise incident.

2.3 RISK & COMPLIANCE - The Value

Regulatory and risk assessment.

COMPLIANCE | Confidence: 90% | Tokens: 1,393

This incident involves the potential exfiltration of sensitive data, including potentially protected health information (PHI) and personal data of EU residents. It represents a serious breach of multiple compliance frameworks, including HIPAA, SOC2, and GDPR. Immediate action is required to investigate, contain, and report the incident as per the applicable regulations.

LEGAL | Confidence: 85% | Tokens: 1,375

CRITICAL data exfiltration from FILESERVER via compromised admin account triggers multiple breach notification requirements across jurisdictions. Unknown scope of affected data types (PII/PHI/PCI) and individual count requires immediate legal counsel involvement to determine specific obligations, notification timing, and regulatory coordination. Evidence preservation is mandatory given potential litigation and regulatory investigation. Law enforcement notification recommended due to severity and criminal implications.

2.5 SPECIALISTS

Domain-specific agents.

SANDBOX | Confidence: 0% | Tokens: 1,605

This event appears to be a DLP (Data Loss Prevention) alert indicating data exfiltration activity involving user 'compromised_admin' on host 'FILESERVER' communicating with IP 198.51.100.77. However, no actual file sample was provided for dynamic analysis in the sandbox environment. The raw payload is empty, containing no executable content, documents, scripts, or other artifacts that could be detonated and analyzed for malicious behavior. To perform meaningful sandbox analysis, I would need the actual suspicious files, executables, or documents that were involved in this exfiltration event. The DLP system has detected the data movement, but without the specific files or malware samples involved, there is nothing for the sandbox to execute and analyze dynamically.

SENTINEL | Confidence: 70% | Tokens: 3,884

The IP address 198.51.100.77 has a low VirusTotal reputation score and a low number of AbuseIPDB reports, which is unusual compared to the expected baseline for this organization. This could indicate the IP is associated with malicious activity or is being used for unauthorized purposes. Further investigation is warranted to determine the nature of the activity originating from this IP address.

3. INVESTIGATION TIMELINE

Time	Agent	Action	Tokens
22:47:19	sandbox	FINDING	1605
22:47:19	sentinel	FINDING	3884
22:47:19	dataguard	FINDING	3782
22:47:19	compliance	COMPLIANCE	1393
22:47:19	hunter	FINDING	6102
22:47:19	intel	ENRICHMENT	5061
22:47:19	triage	TRIAGE	735
22:47:19	legal	LEGAL	1375
22:47:19	forensics	FORENSICS	1920
22:47:19	behavioral	FINDING	4150
22:47:19	correlator	CORRELATION	11166
22:47:39	analyst	VERDICT	7797

4. RECOMMENDATIONS

1. No immediate action required - incident determined to be a false positive.
2. Consider tuning detection rules to reduce similar false positives.
3. Review source alert configuration for sensitivity adjustments.
4. Document this false positive pattern for future reference.

This report was automatically generated by HORNET Autonomous SOC. All findings represent the consensus of 56 specialized AI agents working in parallel.