SECURITY INCIDENT REPORT

Incident ID:	INC-000009
Severity:	HIGH
Status:	OPEN
Detection Time:	2026-02-01 13:59:00 UTC
Endpoint:	EP-0031
Attack Type:	data_exfiltration

Report Generated: 2026-02-01 14:00:08

EXECUTIVE SUMMARY

A security incident was detected on endpoint **EP-0031** at 2026-02-01 13:59:00 UTC. The anomaly detection system identified suspicious behavior with an ensemble confidence of **90.1%**.

The system detected **3** MITRE ATT&CK; technique(s) associated with this incident, with the primary technique being **Brute Force**.

Current Status: **OPEN**
Severity Classification: **HIGH**

INCIDENT DETAILS

Model	Anomaly Score
Autoencoder	0.986
Isolation Forest	0.654
LOF	0.695
Ensemble	**0.778**
Confidence	**90.1%**

MITRE ATT&CK; TECHNIQUES

T1110: Brute Force

Tactic: Credential Access
Confidence: 95.0%
Matched Features: network_out
Description: Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained.

T1496: Resource Hijacking

Tactic: Impact
Confidence: 71.4%
Matched Features: network_out
Description: Adversaries may leverage the resources of co-opted systems to solve resource intensive problems, which may impact system availability.

T1071: Application Layer Protocol

Tactic: Command and Control
Confidence: 71.4%

Matched Features: network_out
Description: Adversaries may communicate using application layer protocols to avoid detection/network filtering.

FEATURE ANALYSIS

Feature	Value	Baseline	Deviation	Contribution
Disk Read	958.78	200.00	4.79x	21.1%
Network Out	266.20	80.00	3.33x	16.3%
Failed Logins	0.13	0.50	0.26x	13.6%
Dns Queries	59.97	30.00	2.00x	9.8%
Auth Attempts	3.58	2.00	1.79x	8.4%
File Access	85.99	50.00	1.72x	7.9%
Memory Usage	72.85	45.00	1.62x	7.2%

AI EXPLANATION

Anomalous behavior detected:
• Disk Read is significantly elevated (4.8x baseline, 21.1% contribution)
• Network Out is significantly elevated (3.3x baseline, 16.3% contribution)
• Failed Logins is significantly reduced (0.3x baseline, 13.6% contribution)

■■ Large data transfer detected - possible data exfiltration

RECOMMENDED ACTIONS

1. Isolate the affected endpoint from the network immediately
2. Conduct a forensic analysis of the endpoint
3. Review and analyze related logs for the affected timeframe
4. Check for lateral movement to other systems
5. Update detection rules based on this incident
6. Implement recommended MITRE ATT&CK; mitigations