SECURITY INCIDENT REPORT

Incident ID:	INC-AD7CB9
Severity:	HIGH
Status:	OPEN
Detection Time:	2026-02-02 22:05:57 UTC
Endpoint:	EP-0049
Attack Type:	lateral_movement

Report Generated: 2026-02-02 22:06:03

EXECUTIVE SUMMARY

A security incident was detected on endpoint **EP-0049** at 2026-02-02 22:05:57 UTC. The anomaly detection system identified suspicious behavior with an ensemble confidence of **81.2%**.

The system detected **2** 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	1.000
Isolation Forest	0.498
LOF	0.888
Ensemble	**0.795**
Confidence	**81.2%**

MITRE ATT&CK; TECHNIQUES

T1110: Brute Force

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

T1021: Remote Services

Tactic: Lateral Movement
Confidence: 95.0%
Matched Features: auth_attempts
Description: Adversaries may use valid accounts to log into a service specifically designed to accept remote connections.

FEATURE ANALYSIS

Feature	Value	Baseline	Deviation	Contribution
Failed Logins	0.00	0.50	0.00x	26.1%
Auth Attempts	12.67	2.00	6.33x	21.1%
Network Out	11.17	80.00	0.14x	16.2%
Api Calls	17.03	100.00	0.17x	14.8%
Memory Usage	11.02	45.00	0.24x	12.1%
Dns Queries	33.88	30.00	1.13x	2.3%
Disk Write	74.44	100.00	0.74x	1.9%

AI EXPLANATION

Anomalous behavior detected:
• Failed Logins is significantly reduced (0.0x baseline, 26.1% contribution)
• Auth Attempts is significantly elevated (6.3x baseline, 21.1% contribution)
• Network Out is significantly reduced (0.1x baseline, 16.2% contribution)

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