SECURITY INCIDENT REPORT

Incident ID:	INC-00AFD4
Severity:	HIGH
Status:	OPEN
Detection Time:	2026-02-03 21:33:45 UTC
Endpoint:	EP-0006
Attack Type:	lateral_movement

Report Generated: 2026-02-03 21:33:47

EXECUTIVE SUMMARY

A security incident was detected on endpoint **EP-0006** at 2026-02-03 21:33:45 UTC. The anomaly detection system identified suspicious behavior with an ensemble confidence of **86.6%**.

The system detected **2** MITRE ATT&CK; technique(s) associated with this incident, with the primary technique being **Remote Services**.

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

INCIDENT DETAILS

Model	Anomaly Score
Autoencoder	0.999
Isolation Forest	0.569
LOF	0.785
Ensemble	**0.784**
Confidence	**86.6%**

MITRE ATT&CK; TECHNIQUES

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.

T1110: Brute Force

Tactic: Credential Access
Confidence: 73.9%
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.

FEATURE ANALYSIS

Feature	Value	Baseline	Deviation	Contribution
Failed Logins	0.00	0.50	0.00x	27.5%
Process Creation	0.00	5.00	0.00x	27.5%
Auth Attempts	10.14	2.00	5.07x	19.6%
File Access	80.25	50.00	1.60x	6.4%
Network In	218.93	150.00	1.46x	5.3%
Dns Queries	37.46	30.00	1.25x	3.6%
Network Out	55.63	80.00	0.70x	2.7%

AI EXPLANATION

Anomalous behavior detected:
• Failed Logins is significantly reduced (0.0x baseline, 27.5% contribution)
• Process Creation is significantly reduced (0.0x baseline, 27.5% contribution)
• Auth Attempts is significantly elevated (5.1x baseline, 19.6% 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