SECURITY INCIDENT REPORT

Incident ID:	INC-000005
Severity:	HIGH
Status:	OPEN
Detection Time:	2026-02-01 13:50:59 UTC
Endpoint:	EP-0011
Attack Type:	lateral_movement

Report Generated: 2026-02-01 13:54:29

EXECUTIVE SUMMARY

A security incident was detected on endpoint **EP-0011** at 2026-02-01 13:50:59 UTC. The anomaly detection system identified suspicious behavior with an ensemble confidence of **95.0%**.

The system detected **3** MITRE ATT&CK; technique(s) associated with this incident, with the primary technique being **Exploit Public-Facing Application**.

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

INCIDENT DETAILS

Model	Anomaly Score
Autoencoder	0.796
Isolation Forest	0.676
LOF	0.822
Ensemble	**0.765**
Confidence	**95.0%**

MITRE ATT&CK; TECHNIQUES

T1190: Exploit Public-Facing Application

Tactic: Initial Access
Confidence: 95.0%
Matched Features: process_creation
Description: Adversaries may attempt to exploit a weakness in an Internet-facing computer or program using software, data, or commands.

T1021: Remote Services

Tactic: Lateral Movement
Confidence: 89.3%
Matched Features: auth_attempts, process_creation, failed_logins
Description: Adversaries may use valid accounts to log into a service specifically designed to accept remote connections.

T1496: Resource Hijacking

Tactic: Impact
Confidence: 85.1%

Matched Features: process_creation
Description: Adversaries may leverage the resources of co-opted systems to solve resource intensive problems, which may impact system availability.

FEATURE ANALYSIS

Feature	Value	Baseline	Deviation	Contribution
Failed Logins	3.44	0.50	6.87x	22.7%
Auth Attempts	7.84	2.00	3.92x	16.3%
Process Creation	18.01	5.00	3.60x	15.3%
Dns Queries	67.93	30.00	2.26x	10.1%
Cpu Usage	39.81	25.00	1.59x	6.2%
Network In	237.41	150.00	1.58x	6.1%
Network Out	123.94	80.00	1.55x	5.8%

AI EXPLANATION

Anomalous behavior detected:
• Failed Logins is significantly elevated (6.9x baseline, 22.7% contribution)
• Auth Attempts is significantly elevated (3.9x baseline, 16.3% contribution)
• Process Creation is significantly elevated (3.6x baseline, 15.3% contribution)

■■ Possible brute force attack or credential stuffing attempt

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