# SECURITY INCIDENT REPORT

| | |
|---|---|
| **Incident ID:** | INC-934183 |
| **Severity:** | MEDIUM |
| **Status:** | OPEN |
| **Detection Time:** | 2026-02-03 21:33:51 UTC |
| **Endpoint:** | EP-0050 |
| **Attack Type:** | lateral_movement |

*Report Generated: 2026-02-03 21:33:53*

# EXECUTIVE SUMMARY

A security incident was detected on endpoint **EP-0050** at 2026-02-03 21:33:51 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 **Exploitation for Privilege Escalation**.

Current Status: **OPEN**
Severity Classification: **MEDIUM**

# INCIDENT DETAILS

| Model | Anomaly Score |
|---|---|
| Autoencoder | 0.786 |
| Isolation Forest | 0.623 |
| LOF | 0.560 |
| | |
| **Ensemble** | **0.657** |
| **Confidence** | **95.0%** |

# MITRE ATT&CK; TECHNIQUES

### *T1068: Exploitation for Privilege Escalation*

**Tactic:** Privilege Escalation
**Confidence:** 45.7%
**Matched Features:** failed_logins
**Description:** Adversaries may exploit software vulnerabilities in an attempt to elevate privileges.

### *T1190: Exploit Public-Facing Application*

**Tactic:** Initial Access
**Confidence:** 39.2%
**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:** 36.5%
**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.

## FEATURE ANALYSIS

| Feature | Value | Baseline | Deviation | Contribution |
|---|---|---|---|---|
| Failed Logins | 1.41 | 0.50 | 2.81x | 22.4% |
| Auth Attempts | 5.63 | 2.00 | 2.81x | 22.4% |
| Process Creation | 12.08 | 5.00 | 2.42x | 19.3% |
| Disk Write | 149.99 | 100.00 | 1.50x | 9.8% |
| Network In | 214.80 | 150.00 | 1.43x | 8.9% |
| Cpu Usage | 32.56 | 25.00 | 1.30x | 7.1% |
| Disk Read | 140.45 | 200.00 | 0.70x | 4.6% |

## AI EXPLANATION

Anomalous behavior detected:
• Failed Logins is significantly elevated (2.8x baseline, 22.4% contribution)
• Auth Attempts is significantly elevated (2.8x baseline, 22.4% contribution)
• Process Creation is significantly elevated (2.4x baseline, 19.3% 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