SECURITY INCIDENT REPORT

Incident ID:	INC-102C93
Severity:	CRITICAL
Status:	OPEN
Detection Time:	2026-02-02 22:10:24 UTC
Endpoint:	EP-0032
Attack Type:	lateral_movement

Report Generated: 2026-02-02 22:10:25

EXECUTIVE SUMMARY

A security incident was detected on endpoint **EP-0032** at 2026-02-02 22:10:24 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 **Remote Services**.

Current Status: **OPEN**
Severity Classification: **CRITICAL**

INCIDENT DETAILS

Model	Anomaly Score
Autoencoder	0.999
Isolation Forest	0.769
LOF	0.899
Ensemble	**0.889**
Confidence	**95.0%**

MITRE ATT&CK; TECHNIQUES

T1021: Remote Services

Tactic: Lateral Movement
Confidence: 95.0%
Matched Features: 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: 91.4%
Matched Features: process_creation
Description: Adversaries may leverage the resources of co-opted systems to solve resource intensive problems, which may impact system availability.

T1110: Brute Force

Tactic: Credential Access
Confidence: 89.1%

Matched Features: failed_logins, network_in
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
File Access	0.00	50.00	0.00x	19.2%
Auth Attempts	0.00	2.00	0.00x	19.2%
Failed Logins	3.01	0.50	6.01x	15.1%
Process Creation	18.64	5.00	3.73x	11.2%
Api Calls	301.20	100.00	3.01x	9.5%
Network In	293.39	150.00	1.96x	6.0%
Cpu Usage	9.80	25.00	0.39x	5.9%

AI EXPLANATION

Anomalous behavior detected:
• File Access is significantly reduced (0.0x baseline, 19.2% contribution)
• Auth Attempts is significantly reduced (0.0x baseline, 19.2% contribution)
• Failed Logins is significantly elevated (6.0x baseline, 15.1% 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