Threat Hunting Report

Summary:

During proactive threat hunting, multiple failed login attempts were identified from external IP address 185.220.101.45. This pattern indicates potential malicious activity targeting user accounts.

Findings:

- 10 failed login attempts within a short time period
- External IP address detected
- Behavior consistent with brute force attack

Conclusion:

The activity represents a brute force attempt against a user account and should be considered a security incident.

Recommendations:

- Block the malicious IP address
- Implement account lockout policy
- Continue monitoring authentication logs