Brute Force Authentication Failures with Multi-Platform Log Correlation, Detection Strategy DET0463

Archived: 2026-04-05 14:47:13 UTC

AN1275

High volume of failed logon attempts followed by a successful one from a suspicious user, host, or timeframe

Log Sources

Mutable Elements

Field	Description
TimeWindow	Adjustable window to correlate failed logons, e.g., 5-10 minutes
UserContext	Define scope of monitored users (e.g., service accounts, admins)
FailureThreshold	Count of failed logons before raising an alert (e.g., 10-15)

AN1276

Multiple authentication failures for valid or invalid users followed by success from same IP/user

Log Sources

Mutable Elements

Field	Description
TimeWindow	Period of brute force activity correlation (e.g., 5 mins)
IPWhitelist	Exclude known monitoring IPs or jump boxes
LoginSource	Filter SSH vs. local logins

AN1277

Password spraying or brute force attempts across user pool within short time intervals

Log Sources

Mutable Elements

Field	Description
UsernameSprayThreshold	Max number of accounts targeted from a single IP
GeoAnomaly	Mismatch between user location and request location

AN1278

Multiple failed authentications in unified logs (e.g., loginwindow or sshd)

Log Sources

Mutable Elements

Field	Description
TimeWindow	Scope of authentication failures (e.g., 10-15 mins)
TargetUser	Filter known service or decoy accounts

AN1279

Excessive login attempts followed by success from SaaS apps like O365, Dropbox, etc.

Log Sources

Mutable Elements

Field	Description
AppName	Detect brute force attempts targeting specific apps
UserGroup	Limit alert scope to high-value user groups
