Password Guessing via Multi-Source Authentication Failure Correlation, Detection Strategy DET0551

Archived: 2026-04-05 18:06:26 UTC

AN1521

Series of authentication failures (Event ID 4625) targeting the same or similar user accounts over time from one or more remote IPs

Log Sources

Mutable Elements

Field	Description
TimeWindow	Defines the period in which multiple failed attempts are aggregated (e.g., 10 minutes)
UsernamePattern	Filter for common account naming conventions, e.g., service accounts or administrator variants
SourceIPThreshold	Limit on unique IPs trying to authenticate against a single account

AN1522

Repeated failed SSH login attempts followed by a possible success from the same remote host

Log Sources

Mutable Elements

Field	Description
PortScope	Can be tuned to non-standard ports if SSH is moved from default
UserScope	Filter high-value or restricted users (e.g., root, service)
AttemptThreshold	Number of consecutive failures before flagging (e.g., >5 in 2 minutes)

AN1523

Series of failed logins from loginwindow or sshd with repeated usernames or password prompts

Log Sources

Mutable Elements

Field	Description
AuthMechanism	Local console vs. SSH vs. remote Apple Admin tools
FailurePattern	Use regex to isolate brute force messages among other log noise

AN1524

Multiple failed sign-in attempts from external sources across many users followed by success from the same IP

Log Sources

Mutable Elements

Field	Description
GeoRiskScore	Elevate anomalies from uncommon geolocations
MFAStatus	Elevate logins missing MFA on high-value accounts

AN1525

Login attempt failures over SNMP, Telnet, or SSH interface, often reflected in logs or syslog events

Log Sources

Mutable Elements

Field	Description
InterfaceType	Specify monitoring of Telnet/SSH/SNMP for login activity
FailedAttemptThreshold	How many failures in short succession should trigger alerting

AN1526

Password guessing attempts against web-based apps (e.g., Dropbox, Google Workspace) reflected in API or sign-in logs

Log Sources

Mutable Elements

Field	Description
AppContext	Which SaaS apps should be monitored for brute force attempts
EmailPattern	Limit scope to enterprise domains or service accounts

---