

Domino Log Analysis - Examples

Please find below several examples for the Domino Log Sensor

Detection of Semaphoring Events

New

Domino Log Analysis Sensor

help ?

Configuration

Targets

Schedule

0 Action(s)

Sensor Name

Semaphore Analysis

Status

✓

Enabled

▼ Search String

Search Mode

Multiple phrases, search exact phrase

▼

Search String

WAITING FOR SEM;Task table entry semaphore

Separator for multiple phrases is ';' (semicolon)

other examples (screenshots take from the old UI)

Detection of SMTP attacks ?

Search String

Search Mode

Single phrase, search exact phrase

▼

Search String

SMTP Server: Authentication failed

Detection for certain events

Search Mode

Multiple phrases, search exact phrase

▼

Search String

operation did not complete in a reasonable

Detection if a task/event terminated abnormally

Search String	
Search Mode	Single phrase, search exact phrase ▼
Search String	has terminated abnormally

Detection if Passthru happens

Search Mode	Single phrase, search exact phrase ▼
Search String	Established passthru session

Detection of SMTP attacks ?

Search String	
Search Mode	Multiple phrases, search exact phrase ▼
Search String	disconnected. 0 message[s] received; rejected by DNS blacklist filter; Recipient could not be found in the Domino Directory

Detection if users have issues with Internet Passwords

Settings	Targets	Actions	Schedule
Search String			
Search Mode	Single phrase, search exact phrase ▼		
Search String	authentication failure using internet password		

Detection if Policies are involved 😊

Search Mode	Multiple phrases, search exact phrase ▼
Search String	disconnected. 0 message[s] received;rejected for policy reasons