ALERTING:  
  
index=main sourcetype=python\_app

| rex "^(?<ts>\S+\s+\S+),\s\*(?<level>\S+)\s+(?<message>.\*)"

| search level="ERROR"  
  
A close-up of a computer screen

AI-generated content may be incorrect.  
  
  
A screenshot of a computer

AI-generated content may be incorrect.  
  
  
A screenshot of a computer

AI-generated content may be incorrect.  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
**Nginx Overview**

**Requests per Minute**

index=main sourcetype=nginx\_access

| rex "(?<clientip>\d+\.\d+\.\d+\.\d+) - - \[(?<ts>[^\]]+)\] \"(?<method>\S+) (?<uri>\S+)\S\*\" (?<status>\d{3}) (?<bytes>\d+)"

| timechart span=1m count AS requests

**Error Rate (%)**

index=main sourcetype=nginx\_access

| rex "\"(?<method>\S+) (?<uri>\S+)\S\*\" (?<status>\d{3})"

| eval is5xx=if(status>=500,1,0)

| stats count AS total sum(is5xx) AS errors

| eval error\_rate=round((errors/total)\*100,2)

**Windows Security**

**Failed Logons (Top 5)**

index=main sourcetype=windows\_security

| rex "Account Name: (?<account>[^,]+)(?:, Source IP: (?<src\_ip>\d+\.\d+\.\d+\.\d+))?"

| stats count BY account

| sort -count

| head 5

**Successful Logons**

index=main sourcetype=windows\_security

| search "successfully logged on"

| stats count AS success\_logons

**Docker Logs**

**Error Trend**

index=main sourcetype=docker\_logs

| rex "^(?<ts>\S+)\s+(?<container>\S+)\s+(?<level>INFO|WARN|ERROR|DEBUG)\s+(?<message>.\*)"

| timechart span=5m count(eval(level="ERROR")) AS errors

**Recent Errors**

index=main sourcetype=docker\_logs

| rex "^(?<ts>\S+)\s+(?<container>\S+)\s+(?<level>\S+)\s+(?<message>.\*)"

| search level="ERROR"

| table \_time container message

| sort -\_time

| head 10

**Firewall Traffic**

**ACCEPT vs DROP**

index=main sourcetype=firewall

| rex "(?<action>(?:ACCEPT|DROP))"

| timechart span=5m count BY action

**Top Source IPs (Blocked)**

index=main sourcetype=firewall

| rex "(?<action>DROP)\s+(?<proto>\S+)\s+(?<src\_ip>\d+\.\d+\.\d+\.\d+)"

| stats count BY src\_ip

| sort -count

| head 5

**Python App**

**Log Levels Over Time**

index=main sourcetype=python\_app

| rex "^(?<ts>\S+\s+\S+),\s\*(?<level>\S+)\s+(?<message>.\*)"

| timechart span=5m count BY level

**Latest Errors**

index=main sourcetype=python\_app

| rex "^(?<ts>\S+\s+\S+),\s\*(?<level>\S+)\s+(?<message>.\*)"

| search level="ERROR"

| table \_time message

| sort -\_time

| head 10