
🔎 Using logreduce in Sumo Logic

Query Example:

```
_sourceCategory=labs/snort

| logreduce
```

✅ What logreduce Does

- logreduce groups together **similar log messages** by identifying their patterns.
- Instead of showing thousands of repetitive logs, it creates **summarized signatures** (templates) that highlight only what's different (variables such as IPs, usernames, ports, etc.).
- This allows analysts to quickly **separate common noise from unique or suspicious events**.

💡 Why It's Beneficial

- **Faster Analysis:** Instead of reading through thousands of nearly identical Snort alerts, you see just a handful of patterns.
- **Noise Reduction:** Helps filter out routine/expected logs and spot unusual patterns more clearly.
- **Efficient Triage:** Security teams can prioritize unique or rare events (possible attacks) over repetitive ones.
- **Better Visualization:** Makes it easier to understand what's happening across the environment at a glance.

📌 Example

Imagine Snort is generating **10,000 intrusion alerts** in one hour.

- Without logreduce: You'd see all 10,000 logs, with minor differences like IP addresses or timestamps.
- With logreduce: Those 10,000 logs may collapse into **just 10–20 patterns**, such as:
  - ET SCAN Potential SSH Scan from <IP>
  - ET POLICY Suspicious DNS Query for <domain>
  - ET WEB_SERVER Possible Apache Struts Exploit Attempt

Now, instead of drowning in data, you instantly understand **what types of threats are happening** and can act faster.
