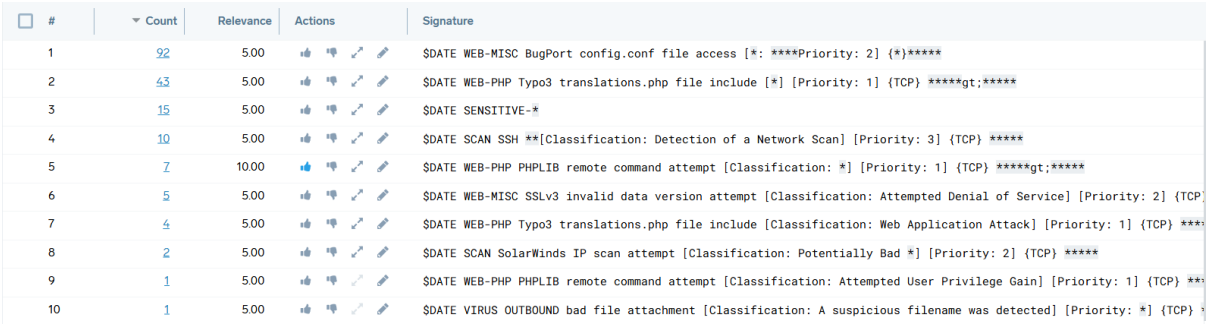
The Logreduce operator uses an algorithm to group messages together based on string and pattern similarity. It is a powerful tool, especially useful when dealing with a huge number of logs in a SOC environment. To be effective, the algorithm uses machine learning to group similar log lines. Variable parts like IP addresses or user IDs are being replaced with wildcards. This operator helps analysts to focus on unique behaviour, not the repeated messages.

Using logreduce helps analysts find log patterns that don't match normal behaviour. Using them on a category *prod/auth/* can highlight failed authentication attempts from an unknown IP range or unexpected user activity.

Another case would be using logreduce on a */network/firewall* log source. Analysts might discover a rare protocol usage, port scans, or malware comeback attempts, which could improve threat hunting altogether.

We will use logreduce on logs coming from Snort, which is an IDS/IPS software. To see the results, run the following query.

Query - _sourceCategory=labs/snort
| logreduce



#	Count	Relevance	Actions	Signature
1	92	5.00		$DATE WEB-MISC BugPort config.conf file access [*: ****Priority: 2] {*}*****
2	43	5.00		$DATE WEB-PHP Typo3 translations.php file include [*] [Priority: 1] {TCP} *****gt;*****
3	15	5.00		$DATE SENSITIVE-*
4	10	5.00		$DATE SCAN SSH **[Classification: Detection of a Network Scan] [Priority: 3] {TCP} *****
5	7	10.00		$DATE WEB-PHP PHPLIB remote command attempt [Classification: *] [Priority: 1] {TCP} *****gt;*****
6	5	5.00		$DATE WEB-MISC SSLv3 invalid data version attempt [Classification: Attempted Denial of Service] [Priority: 2] {TCP
7	4	5.00		$DATE WEB-PHP Typo3 translations.php file include [Classification: Web Application Attack] [Priority: 1] {TCP} ***
8	2	5.00		$DATE SCAN SolarWinds IP scan attempt [Classification: Potentially Bad *] [Priority: 2] {TCP} *****
9	1	5.00		$DATE WEB-PHP PHPLIB remote command attempt [Classification: Attempted User Privilege Gain] [Priority: 1] {TCP} ***
10	1	5.00		$DATE VIRUS OUTBOUND bad file attachment [Classification: A suspicious filename was detected] [Priority: *] {TCP}