Data Ingestion and Health

Time is in the last 1 month Log Type is not null

Ingested Events Count

215 M

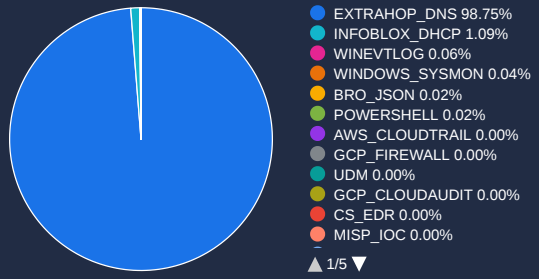
▼ -41,426 K

Ingestion Error Count

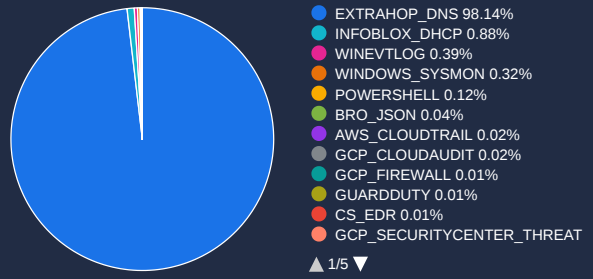
18 M

▼ -1,175,614.9 K

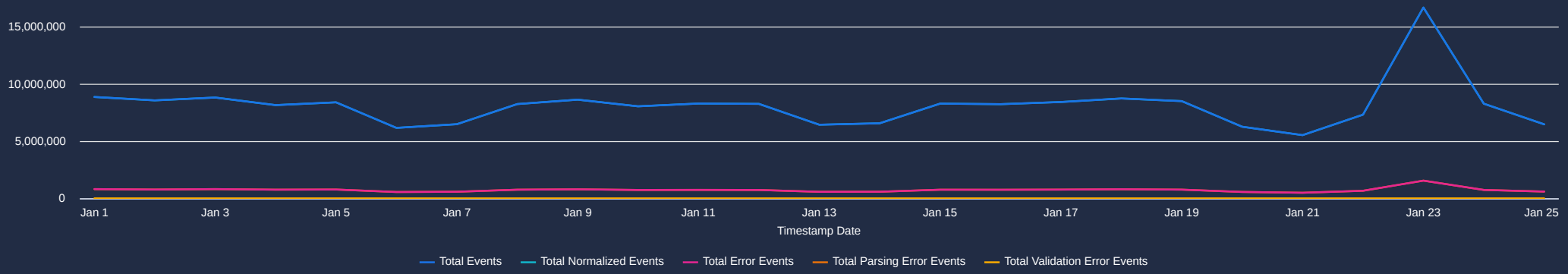
Log Type Distribution by Events Count



Log Type Distribution by Throughput



Ingestion - Events by Status



Ingestion - Events by Log Type

Log Type	Ingested Throughput	Ingested Events	Normalized Events	Errors	Parsing Errors	Validation Errors
EXTRAHOP_DNS	50,660,848,148	200,026,989	200,026,989	18,388,045	18,388,045	0
INFOBLOX_DHCP	455,848,734	2,322,914	2,322,914	0	0	0
WINEVTLOG	202,398,528	117,950	117,950	0	0	0
WINDOWS_SYSMON	165,726,789	80,482	80,482	0	0	0
POWERSHELL	59,527,587	41,707	41,707	0	0	0
BRO_JSON	22,739,231	47,871	47,871	0	0	0
AWS_CLOUDTRAIL	12,810,460	9,186	9,186	0	0	0
GCP_CLOUDAUDIT	9,506,864	3,716	3,716	25	25	0
GCP_FIREWALL	5,232,640	4,590	4,590	0	0	0
GUARDDUTY	4,111,459	1,701	1,701	0	0	0

Please note that the dashboards below have timelines that are pre-selected and the “Time” filter doesn’t apply to them

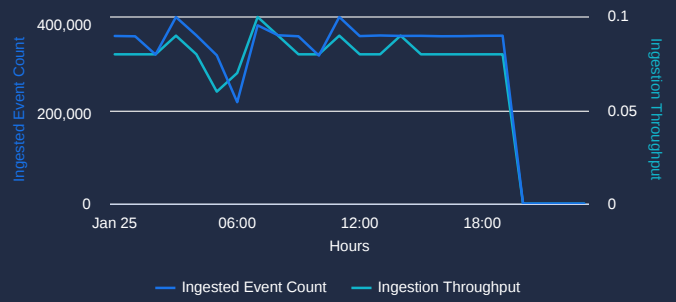
Recently Ingested Events

Log Type	Timestamp
EXTRAHOP_DNS	2024-01-25 20:04:32
INFOBLOX_DHCP	2024-01-25 19:59:32
EXTRAHOP_DNS	2024-01-25 19:59:32
INFOBLOX_DHCP	2024-01-25 19:54:32
EXTRAHOP_DNS	2024-01-25 19:49:32
INFOBLOX_DHCP	2024-01-25 19:44:32
EXTRAHOP_DNS	2024-01-25 19:44:32
INFOBLOX_DHCP	2024-01-25 19:39:32
EXTRAHOP_DNS	2024-01-25 19:39:32
EXTRAHOP_DNS	2024-01-25 19:29:32

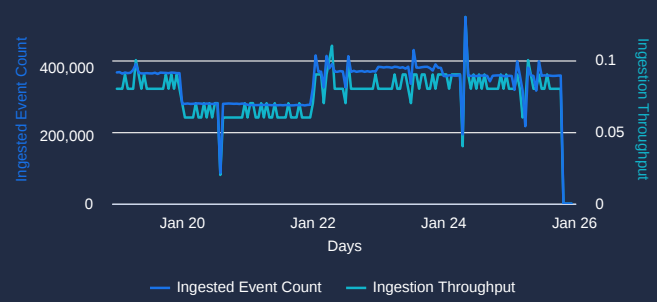
Daily Log Information

Log Type	Timestamp Date	Total Entry Number
ZSCALER_WEBPROXY	2024-01-25	32
GCP_BIGQUERY_CONTEXT	2024-01-25	1
SQUID_WEBPROXY	2024-01-25	3
WINDOWS_SYSMON	2024-01-25	9,136
WORKSPACE_ACTIVITY	2024-01-25	50
GCP_CLOUDAUDIT	2024-01-25	197
MICROSOFT_DEFENDER_ENDPOINT	2024-01-25	2
GCP_DLP_CONTEXT	2024-01-25	5
AZURE_AD	2024-01-25	15
OKTA	2024-01-25	40

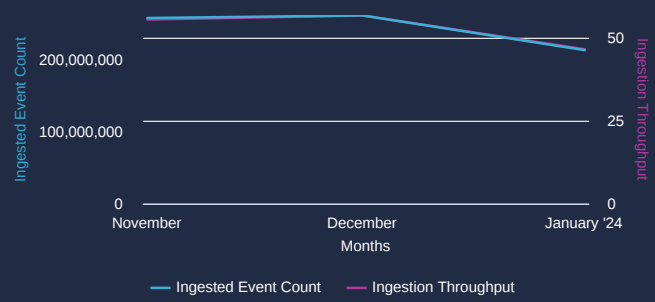
Event Count vs Size (Last 24 hours)



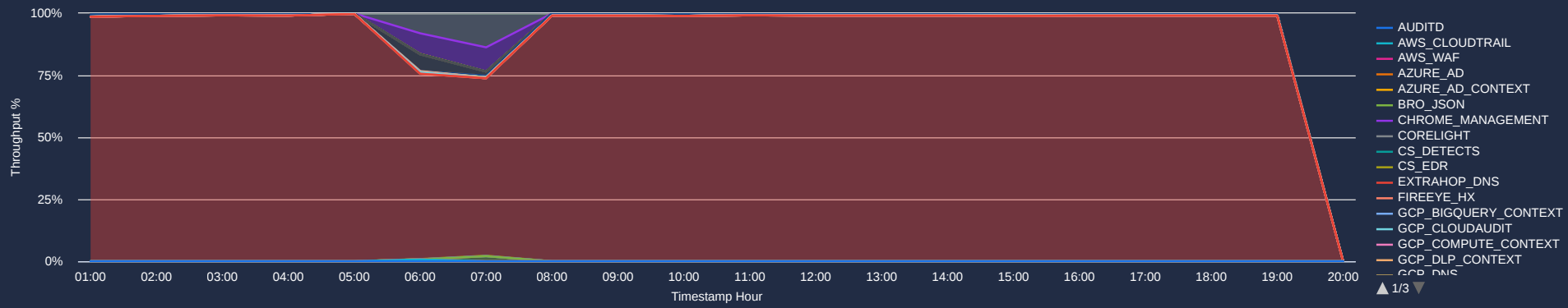
Event Count vs Size (Last 1 week)



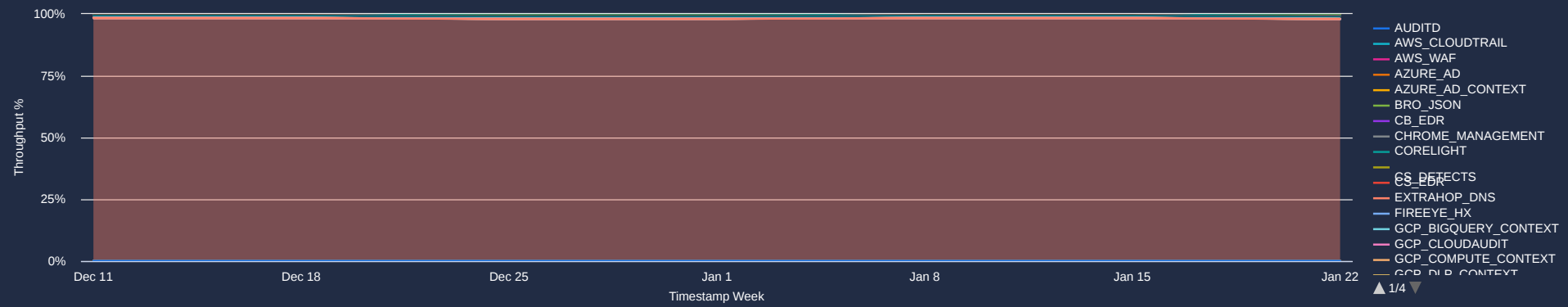
Event Count vs Size (Last 3 months)



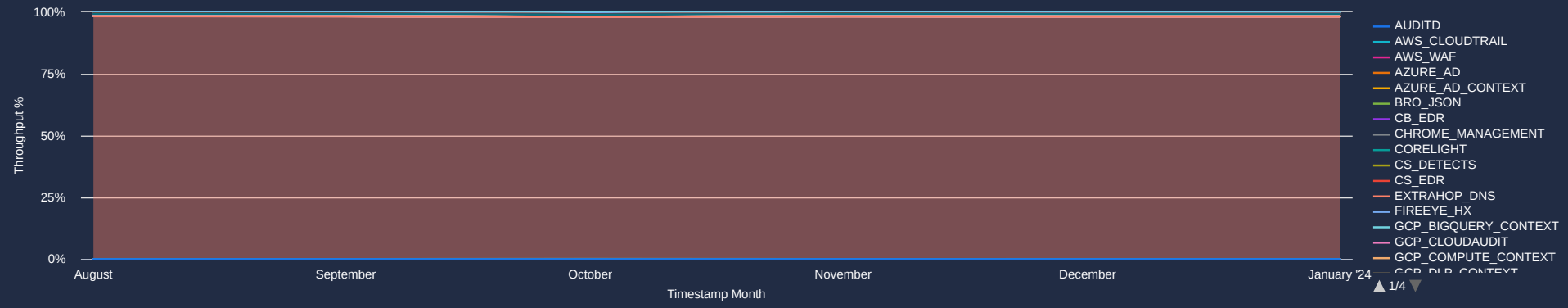
Ingestion - Throughput Hourly



Ingestion - Throughput Weekly



Ingestion - Throughput(Last 6 Months)



Ingestion - Throughput(All Time)