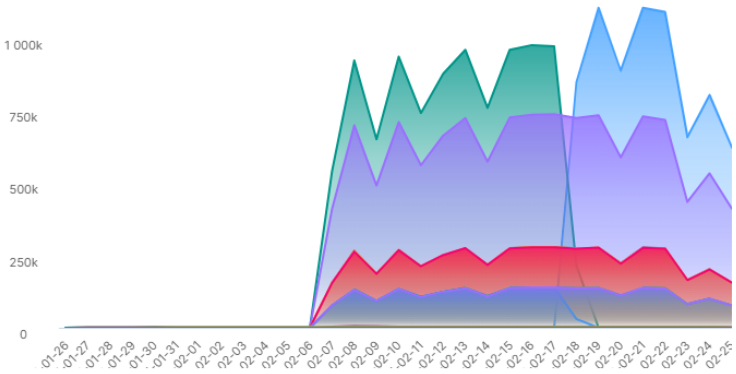
Exabeam - Log Monitoring

Count by Product Last 30 Days



Count by Activity Type 24 hours

ACTIVITY TYPE	COUNT
alert-trigger	934,546
network-traffic	267,344
vpn-login	267,072
network-notification	266,908
endpoint-login	266,126
http-session	222,182
N/A	177,631
ssh-traffic	134,006
http-traffic	133,498
rdp-traffic	133,306

Events by Count 24 hours

VENDOR	EVENT CODE	EVENT NAME	EVENT CATEGORY	CATEGORY
Cisco	N/A	N/A	N/A	N/A
Ivanti	N/A	N/A	N/A	N/A
Symantec	N/A	N/A	N/A	js
Unix	ssh	N/A	N/A	N/A
Cisco	605005	N/A	N/A	N/A
Microsoft	4624	An account was successfully logged on	N/A	N/A
Cisco	106015	Deny TCP (no connection)	N/A	N/A
Cisco	302001	N/A	N/A	N/A

Count by Parser Name 24 hours

MSG TYPE	COUNT
exabeam-aa-kv-alert-trigger-exaanalyticsmaster	667,755
cisco-asa-str-network-notification-success	266,914
symantec-wss-cef-http-session-proxysg	266,539
unix-unix-mix-ssh-traffic-success-ssh2accepted	134,008
cisco-asa-cef-network-traffic-fail-106023	133,947
cisco-fp-kv-alert-trigger-success-ipsimpact	133,669
cisco-asa-str-vpn-login-success-713184	133,571
juniper-ps-str-vpn-login-success-sessionstarted	133,501
cisco-asa-str-http-traffic-304001	133,498
cisco-asa-str-network-traffic-fail-106015	133,399

Log Volume Count 7 Days

19,659,166

Parsed vs. Unparsed

PARSED	COUNT
Yes	2,982,187
No	133,275

Collector Name/Type 24 hours

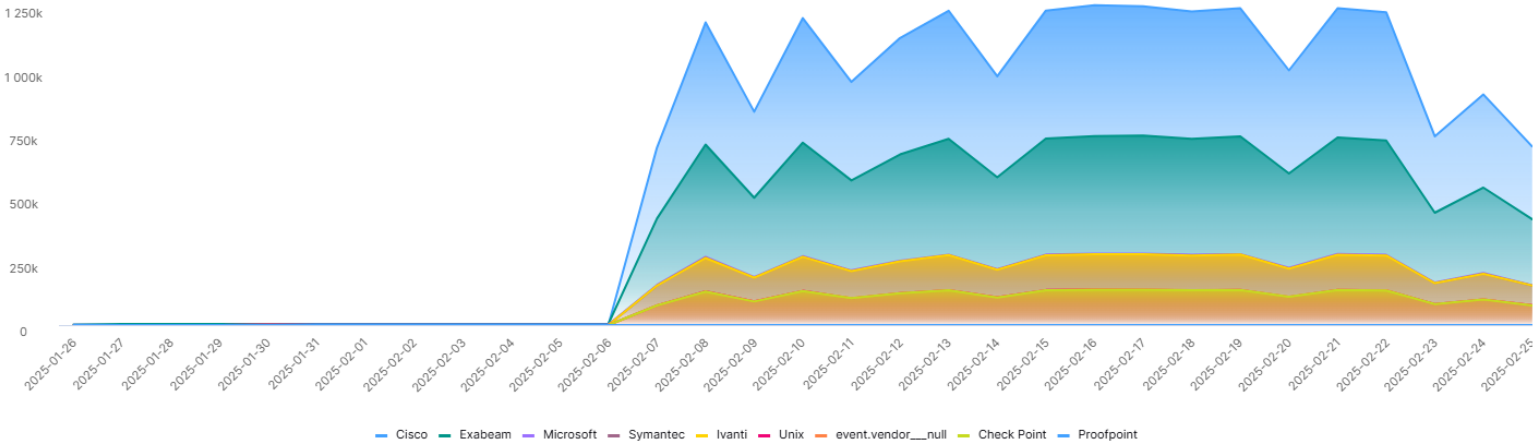
M COLLECTOR NAME	M COLLECTOR TYPE	COUNT
Test_Silent_Log_Source_Monitoring	Webhook	1,056

Count by Vendor and Product 24 hours

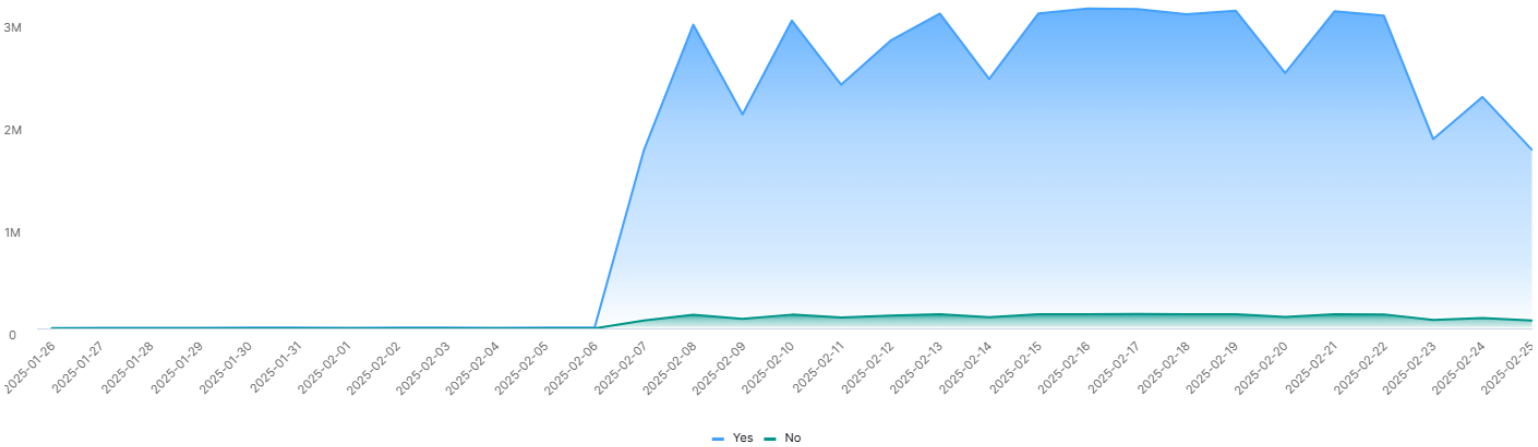
VENDOR	PRODUCT	COUNT
Cisco	Cisco Network Security	1,068,306
Exabeam	Advanced Analytics	705,476
Microsoft	Event Viewer - Security	266,779
Ivanti	Ivanti Pulse Secure	266,757
Symantec	Symantec Web Security Service	266,539

Cisco	Cisco ISE	133,073
Exabeam	Audit Log	3,896
Microsoft	Event Viewer - System	1,261
Exabeam	Search	1,135
Exabeam	PS Solutions	1,056
Microsoft	Event Viewer - Application	556
Exabeam	Correlation Rule	236

Count by Vendor, Last 30 Days



Parsed vs. Unparsed 30 days



Unparsed Raw Logs 24 hours

EVENT RAW LOGS

<190>Feb 24 19:17:03 localhost {"@timestamp": "02/24/2025 07:17:03 PM","beat":{"hostname":"10.10.2.147","name":"10.10.2.147","version":"5.4.1"},"bytes_in":78,"bytes_out":288,"client_ip":"10.10.1.116","client_port":342,"client_proc":"","client_server":"","direction":"out","http":{"request":{"headers":{"content-length":0},"params":""},"response":{"code":200,"headers":{"content-length":19,"content-type":"text/plain"},"phrase":"OK"}},"ip":"10.10.1.116","method":"PUT","path":"/latest/meta-data/instance-id","port":342,"proc":"","query":"GET http://prpops.com/smile/compare/green/occur.aspx","responsetime":0,"server":"","status":"OK","type":"http"}

<190>Feb 24 19:17:07 localhost {"@timestamp": "02/24/2025 07:17:03 PM","beat":{"hostname":"192.168.2.231","name":"192.168.2.231","version":"5.4.1"},"bytes_in":8669,"bytes_out":175,"client_ip":"10.10.3.234","client_port":5,"client_proc":"","client_server":"","direction":"out","http":{"request":{"headers":{"content-length":0},"params":""},"response":{"code":200,"headers":{"content-length":19,"content-type":"text/plain"},"phrase":"OK"}},"ip":"10.10.3.234","method":"POST","path":"/latest/meta-data/instance-id","port":5,"proc":"","query":"GET http://enet.com.cn/friend.html","responsetime":0,"server":"","status":"OK","type":"http"}

<190>Feb 24 19:17:07 localhost {"@timestamp": "02/24/2025 07:17:04 PM","beat":{"hostname":"10.10.1.0","name":"10.10.1.0","version":"5.4.1"},"bytes_in":666,"bytes_out":25,"client_ip":"192.168.2.178","client_port":18,"client_proc":"","client_server":"","direction":"out","http":{"request":{"headers":{"content-length":0},"params":""},"response":{"code":200,"headers":{"content-length":19,"content-type":"text/plain"},"phrase":"OK"}},"ip":"192.168.2.178","method":"DELETE","path":"/latest/meta-data/instance-id","port":18,"proc":"","query":"GET https://udemy.com/area/planet.aspx","responsetime":0,"server":"","status":"OK","type":"http"}

<190>Feb 24 19:17:07 localhost {"@timestamp": "02/24/2025 07:17:04 PM","beat":{"hostname":"10.10.1.240","name":"10.10.1.240","version":"5.4.1"},"bytes_in":665,"bytes_out":29,"client_ip":"10.10.1.6","client_port":66,"client_proc":"","client_server":"","direction":"out","http":{"request":{"headers":{"content-length":0},"params":""},"response":{"code":200,"headers":{"content-length":19,"content-type":"text/plain"},"phrase":"OK"}},"ip":"10.10.1.6","method":"PUT","path":"/latest/meta-data/instance-id","port":66,"proc":"","query":"GET https://slideshare.net","responsetime":0,"server":"","status":"OK","type":"http"}

<190>Feb 24 19:17:07 localhost {"@timestamp": "02/24/2025 07:17:04 PM","beat":{"hostname":"10.10.3.118","name":"10.10.3.118","version":"5.4.1"},"bytes_in":97,"bytes_out":2496,"client_ip":"10.10.0.47","client_port":872,"client_proc":"","client_server":"","direction":"out","http":{"request":{"headers":{"content-length":0},"params":""},"response":{"code":200,"headers":{"content-length":19,"content-type":"text/plain"},"phrase":"OK"}},"ip":"10.10.0.47","method":"GET","path":"/latest/meta-data/instance-id","port":872,"proc":"","query":"GET https://delta.com/since/contain/melody/lone/","responsetime":0,"server":"","status":"OK","type":"http"}

<190>Feb 24 19:17:07 localhost {"@timestamp": "02/24/2025 07:17:04 PM","beat":{"hostname":"192.168.2.166","name":"192.168.2.166","version":"5.4.1"},"bytes_in":24,"bytes_out":486,"client_ip":"10.10.0.212","client_port":42,"client_proc":"","client_server":"","direction":"out","http":{"request":{"headers":{"content-length":0},"params":""},"response":{"code":200,"headers":{"content-length":19,"content-type":"text/plain"},"phrase":"OK"}},"ip":"10.10.0.212","method":"PUT","path":"/latest/meta-data/instance-id","port":42,"proc":"","query":"GET https://sahibinden.com/arrive/sugar/lead/well.js","responsetime":0,"server":"","status":"OK","type":"http"}

<190>Feb 24 19:17:07 localhost {"@timestamp": "02/24/2025 07:17:05 PM","beat":{"hostname":"10.10.3.160","name":"10.10.3.160","version":"5.4.1"},"bytes_in":276,"bytes_out":9849,"client_ip":"192.168.2.193","client_port":136,"client_proc":"","client_server":"","direction":"out","http":{"request":{"headers":{"content-length":0},"params":""},"response":{"code":200,"headers":{"content-length":19,"content-type":"text/plain"},"phrase":"OK"}},"ip":"192.168.2.193","method":"POST","path":"/latest/meta-data/instance-id","port":136,"proc":"","query":"GET http://tube8.com/opposite/hit/human/melody.htm","responsetime":0,"server":"","status":"OK","type":"http"}

<190>Feb 24 19:17:07 localhost CEF: 0|Blue Coat|Proxy SG||TCP_DENIED|TCP_DENIED|Medium| eventId=137708360 app=http in=1641 out=33 categorySignificance=/Informational categoryBehavior=/Execute/Response categoryDeviceGroup=/Proxy catdt=Firewall categoryOutcome=/Success categoryObject=/Host/Resource/File art=1484078357261 cat=Security Compromised Websites deviceSeverity=304 act=TCP_DENIED rt=02/24/2025 07:17:04 PM shost=10.10.3.248 src=10.10.0.234 sourceZoneURI=/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255 suser=bdover dhost=http://mediawhirl.net/oil/ dst=10.10.3.189 destinationZoneURI=/All Zones/ArcSight System/Public Address Space Zones/ARIN/96.0.0.0-99.255.255.255 (ARIN) dpt=443 request=https://liputan6.com requestMethod=TCP_TERMINATE requestContext=https://liputan6.com

requestClientApplication=Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36 cs1=text/javascript;%20charset\=utf-8 cs4=js cs5=none cs6=none cn1=304 cn2=65 cs1Label=Content Type cs2Label=Exception ID cs3Label=Virus ID cs4Label=Extension cs5Label=BC Application Name cs6Label=BC Application Operation cn1Label=HTTP Status Code cn2Label=Time Taken ahost=10.10.0.218 agt=10.135.162.116 agentZoneURI=/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255 av=7.0.7.7279.0 atz=CST6CDT aid=3t8JFD1ABABCAAYIz1SGBRg\=\= at=syslog dvchost=10.10.0.218 dvc=10.10.0.218 deviceZoneURI=/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255 dtz=CST6CDT requestProtocol=https requestUrlAuthority=https://liputan6.com:80 requestUrlHost=https://liputan6.com requestUrlPort=80 requestUrlFileName=say requestUrlQuery=corner deviceZoneName=RFC1918: 10.0.0.0-10.255.255.255 sourceZoneName=RFC1918: 10.0.0.0-10.255.255.255 destinationZoneName=96.0.0.0-99.255.255.255 (ARIN) agentZoneName=RFC1918: 10.0.0.0-10.255.255.255 _cefVer=0.10|Blue Coat|Proxy SG||DELETE|DELETE|Medium| eventId=137708360 app=http in=1641 out=33 categorySignificance=/Informational categoryBehavior=/Execute/Response categoryDeviceGroup=/Proxy catdt=Firewall categoryOutcome=/Success categoryObject=/Host/Resource/File art=1484078357261 cat=Security Compromised Websites deviceSeverity=304 act=TCP_DENIED rt=1484099955000 shost=txbx-0000047.prod-am.ameritrade.com src=10.134.34.212 sourceZoneURI=/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255 suser=LEW225 dhost=http://india.com/night/ready.php.com dst=96.16.7.42 destinationZoneURI=/All Zones/ArcSight System/Public Address Space Zones/ARIN/96.0.0.0-99.255.255.255 (ARIN) dpt=80 request=https://liputan6.com requestMethod=GET requestContext=https://liputan6.com requestClientApplication=chrome/Windows cs1=Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36 cs4=js cs5=none cs6=none cn1=0xe cn2=65 cs1Label=Content Type cs2Label=Exception ID cs3Label=Virus ID cs4Label=Extension cs5Label=BC Application Name cs6Label=BC Application Operation cn1Label=HTTP Status Code cn2Label=Time Taken ahost=10.10.0.218 agt=10.10.3.189 agentZoneURI=/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255 av=7.0.7.7279.0 atz=CST6CDT aid=3t8JFD1ABABCAAYIz1SGBRg\=\= at=syslog dvchost=10.10.0.218 dvc=10.10.3.189 deviceZoneURI=/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255 dtz=CST6CDT requestProtocol=http requestUrlAuthority=https://liputan6.com:80 requestUrlHost=https://liputan6.com requestUrlPort=80 requestUrlFileName=https://liputan6.com requestUrlQuery=corner deviceZoneName=RFC1918: 10.0.0.0-10.255.255.255 sourceZoneName=RFC1918: 10.0.0.0-10.255.255.255 destinationZoneName=96.0.0.0-99.255.255.255 (ARIN) agentZoneName=RFC1918: 10.0.0.0-10.255.255.255 _cefVer=0.1

<190>Feb 24 19:17:33 localhost {"@timestamp": "02/24/2025 07:17:07 PM","beat":
{"hostname":"10.10.0.68","name":"10.10.0.68","version":"5.4.1"},"bytes_in":66,"bytes_out":712,"client_ip":"10.10.1.75","client_port":241,"client_proc":"","client_server":"","direction":"out","http":{"request":{"headers":{"content-length":0},"params":""},"response":{"code":200,"headers":{"content-length":19,"content-type":"text/plain"},"phrase":"OK"}},"ip":"10.10.1.75","method":"POST","path":"/latest/meta-data/instance-id","port":241,"proc":"","query":"GET http://subscene.com","responsetime":0,"server":"","status":"OK","type":"http"}

<190>Feb 24 19:17:33 localhost {"@timestamp": "02/24/2025 07:17:08 PM","beat":