

Index	Type	Sourcetype	Interesting Fields
web	Online sales	access_combined	action , bytes , categoryId , clientip , itemId , JSESSIONID , price , productId , product_name , referer , referer_domain , sale_price , status , user , useragent
security	Active Directory	winauthentication_security	LogName , SourceName , EventCode , EventType , User
	Badge reader	history_access	Address_Description , Department , Device , Email , Event_Description , First_Name , last_Name , Rfid , Username
	Web server	linux_secure	action , app , dest , process , src_ip , src_port , user , vendor_action
sales	Business Intelligence server	sales_entries	AcctCode , CustomerID , TransactionID
	Retail sales	vendor_sales	AcctID , categoryId , product_name , productId , sale_price , Vendor , VendorCity , VendorCountry , VendorID , VendorStateProvince
network	Email security data	cisco_es	dcid , icid , mailfrom , mailto , mid
	Web security appliance data	cisco_wsa_squid	action , cs_method , cs_mime_type , cs_url , cs_username , sc_bytes , sc_http_status , sc_result_code , severity , src_ip , status , url , usage , x_mcafee_virus_name , x_wbrs_score , x_webcat_code_abbrev
	Firewall data	cisco_firewall	bcg_ip , dept , Duration , f name , IP , lname , location , rfid , splunk_role , splunk_server , Username

games	Game logs	SimCubeBeta	<code>date_hour, date_mday, date_minute, date_month, date_second, date_wday, data_year, date_zone, eventtype, index, linecount, punct, splunk_server, timeendpos, timestartpos</code>
-------	-----------	-------------	---