RAW Logs directly to EventHub to Splunk

Custom Azure Policy - DINE Diag Azure Activity to EH

AzureActivity

customer.onmicrosoft.com

SQLSecurityAuditEvents

AuditEvent

Network Security Groups (Flow Logs)

Custom Azure Policy - DINE NSG Flow to Storage - East US

Custom Azure Policy - DINE NSG Flow to Storage - West US

Azure Raw Logs - Event Hub - Auto Inflate

Splunk Add-on for Microsoft Cloud Services

AddOn+

logstash

Analysis

https://www.rubydoc.info/gems/~l/44

Storage (Azure)

Storage (Azure)