Mail server data

Email remains the primary form of formal communication in most organizations. As such, mail server databases and logs are some of the most important business records. Due to their size and tendency to grow without bounds, email data management typically requires both data retention and archival policies so that only important records are held and inactive data is moved to low cost storage.

Mail server transaction and error logs also are essential debugging tools for IT problem resolution and also may be used for usage-based billing. Mail server data can help identify malicious attachments, malicious domain links and redirects, emails from known malicious domains, and emails from unknown domains. It can also be used to identify emails with abnormal or excessive message sizes, and abnormal email activities times. In the Common Information Model, mail server data is typically mapped to the Email data model.

Application

When your Splunk deployment is ingesting mail server data, you can use it to accomplish security and compliance and IT ops use cases.

- Managing known phishing email addresses
- Managing O365 workloads

Sources

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). In addition, these Splunk Add-Ons and Apps are helpful for working with mail server data.

- Splunk App for Microsoft Exchange
- Microsoft O365 Add-on for Splunk