Validate Forwarder Versions and TLS Settings

Ensure that the forwarders that are deployed are to the best possible version available based on the OS that they are installed on. Older versions of Universal Forwarders have been found to be exploitable and can lead to potential data compromise.

Splunk Search to validate the versions deployed:

<fill in search later>

Normalize High Volume Sources

Apply the Common Information Model to high volume sources to allow the data sources to be searched across multiple indexes easier, as well as prepare them for inclusion into Data Models. A lot of organizations hit hiccups when taking large volumes of data (Firewalls/Crowdstrike), by not leveraging the Data Models to perform accelerated searches against the datasets.

Set KPIs: Errors and Growth Monitoring

As new data sources come on board, there needs to be monitoring in place to highlight potential issues taking place. An often-overlooked metric that should be monitored is search concurrency as the hardware only has enough headroom to operate searches at a given time. This is usually brought onto an error of “Maximum number of searches reached for a given time period”.

Another important KPI to set and monitor would be for license utilization. Whether the organization is an ingest based license or workload, it is important to monitor and understand sudden spikes in growth and adjust as needed.

Rationalize Top 10 Alerts

Periodic review of the most active top ten alerts is a critical path for maturity as well as a strong starting point for review. Are these alerts generating alert fatigue, wasting too much time to work the same alerts over and over with low true positive rates? These are simple steps to enforce a review of the content as well as identify problem errors for SOC personnel.

Index=notable earliest=-30d@d | stats count by source | sort – limit=10