# Central Log Request Form

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Requestor: | (Name) | (Title) | (email) | (phone) |
| Department: | (Name) | (Business Unit) |  |  |
| Service: | (Service Name) |  |  |  |
| Business Impact: | (high-med-low) | (Front-end service, Back-end service, internal service) |  |  |

## List of systems:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Hostname | common name | IP | service owner | OS | Application | Role |
| (us-splunk-sh01) | Search Head 01 | x.x.x.x | John Smith | RedHat Linux | Splunk | UI & job scheduling |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## Service & Systems Architecture Diagrams

\*\*\*Please attached a visio and/or a pdf of the network diagram & the service diagram so that all parties have an understanding of how the service works & how to best design alerts & monitoring conditions.\*\*\*

## Log Details

### List of desired logs to monitor:

|  |  |  |  |
| --- | --- | --- | --- |
| Log | type | Location | Format |
| Splunkd.log | Core application log | /opt/splunk/var/log/splunk/splunkd.log | Non-standard log format |
| Messages | OS log | /var/log/messages | Linux OS log format |
| Verdict Log | Custom App | /data/scanner/log/verdict.json | Multi-line json |

For each non-OS log, answer the following:

* Daily rate (log size mb/day or entries/day) average observed or estimated
* Link to vendor/internal documentation on event-codes & message definition
* OR: Event Code summary

Event Code Summary Table

|  |  |  |  |
| --- | --- | --- | --- |
| Event-Code | Normality | Impact | Definition |
| http 500 | Abnormal | High | Page Failed |
| http 401 | Abnormal at high rates | Medium | Login failure |

\*\*\*For each non-OS log, please head & tail the log and attach to request as a txt file.\*\*\*

### Desired prebuilt metrics & alerts:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item (priority & number) | Description | data source | Audience | Action |
| P1-1 | Splunk crash | Splunkd.log | Splunk Admins | Alert Email |
| P2-1 | Failed Logins | Splunkd.log | Splunk Admins, SOC | Alert Email |
| P2-1 | Verdict Failed | Verdict Log | SOC, IR | Rate Metric |

## Standard Questionnaire

|  |  |
| --- | --- |
| Desired Retention Period: |  |
| Desired completion Date: |  |
| Business Justification: |  |

Will your team need any of the following services:

|  |  |
| --- | --- |
| User Training: | (Y/N) |
| Power User Training: | (Y/N) |
| Power User Access: | (Y/N) |
| Dashboard Building: | (Y/N) |
| Report Building: | (Y/N) |
| Alert Building: | (Y/N) |

Any Additional Requested Services?

|  |
| --- |
|  |