Ogden City Corporation
Request for Proposal
SIEM & SOC Services
Q & A

---

1. I see that you are using Sophos on your endpoints can you be specific to which product (i.e. Intercept X, Central, etc.)? **Device Encryption, Intercept X Advanced, Mobile Advanced, Intercept X Advanced for Server**
2. How many domain controllers are currently being utilized by Ogden and can you provide a rough user count if different from your overall end user count? **3 Domain Controller and about 1,000 users**
3. Regarding the Data collectors at central location, What are those data collectors? Syslog or something else? **Syslog**
4. For the replacement SIEM, does the City of Ogden want to own it or have it fully managed in the cloud? **Either way, but cloud is preferred.**
5. Does the city know their Gig/day? **20 Gig**
6. Do they have defined policies and appropriate data to detect those violations? **Yes**
7. Can references be provided after down-selection & MNDA? **No, we are scoring off of references**
8. Does the City have a preferred replacement SIEM solution or SIEM type (cloud, on-premise, hybrid)? **Cloud**
9. Is the city open to a service with everything included (SIEM they do not own)? **Yes**
10. Are the different locations segmented or can they backhaul logs to a central location? **Backhaul to a central location**
11. Does the city have existing use-cases, playbooks or runbooks that will need to be cut over from the current SIEM? If so, how many? **No**

12. Would Ogden City consider a 1-week extension for RFP response? **No**
13. We wanted to know if you could provide an estimate of the number of GBs of logs that will be ingested per day. **20 Gig**
14. Could you define a period of time that you would like logs to be retained in storage? **120 Days**