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

- How many of the following network devices will the SIEM and SOC monitor on the network, and what type are in scope?
    - Routers – 10 approx.
    - Firewall – 4x Sophos XG series
    - Switches – 100
- How many servers will the SIEM and SOC monitor on the network that are in scope?
    - 150-200
- How many workstations will the SIEM and SOC monitor that are in scope?
    - 600-700
- How many of all other end points will the SIEM and SOC monitor that are in scope?
    - 50-100
- What is the total number of business locations in scope?
    - 3 Major locations, and 40+ minor locations throughout. (No Datacenters)
- Are all hardware and operating systems in the IT infrastructure still within the manufacturer's support window?
    - Most is yes, with some exceptions.
- Do you currently have a SIEM solution in place? Can you provide the name of this solution?
    - Yes, we do. Name will not be disclosed at this time.
- What types of environments are in scope (e.g., IT, OT, VOIP)?
    - All, IT, Voip, O365, SNMP, Sophos Endpoint and Firewalls, Alcatel Lucent Switches/routers, Vmware, Avigilon ACM and ACC and more.
- Would Ogden accept an electronic submission of this proposal response, such as an email submission?

  - No, we will not accept emailed or electronic responses. Since the City currently does not have a secured on-line bid/proposal submittal platform, we require sealed hard copy submittals.
- Will Ogden accept services from a Security Operations Center based in Canada?
  - No.
- How are offices / data centers connected? Do they have network connectivity to each other?
  - They are networked together.
- Is there a virtualization infrastructure in place? Please describe.
  - Vmware
- Where are server resources located?
  - Multiple city-owned locations
- Is there any server/infrastructure management solution in place? (E.g.: Microsoft SCOM, Microsoft SCCM). If so, what is the name, vendor and version.
  - No.
- Are you a Microsoft 365 customer? If so, what O365/M365 licenses are in place, and quantities?
  - Gov Office 365
- Do you operate a hybrid Microsoft Exchange organization?
  - No, office 365 only mail
- Is Azure AD Connect configured?
  - Yes
- What identity products are being used? Active Directory, Azure AD, Okta, etc.
  - AD only
- Is there any endpoint management solution in place? (E.g.: Microsoft SCCM)
  - PDQ
- Are all laptops/desktops running Windows 10 as operating system?
  - Most are, but not all.
- What Antivirus/EDR is currently in place?

  - Sophos Endpoint
- Is there a Security Awareness solution in place? (KnowB4, GoSecure, Etc)
  - The Current SIEM may get replaced, if chosen.
- What make/brand/model of network switches and routers are in place?
  - Alcatel Lucent, various models
- Does the city of Ogden expect the provider to provide a replacement SIEM or looking for the provider to manage an existing SIEM platform rather than replace? If it's the management of an existing SIEM if you could clarify your position on SIEM management.
  - Ogden City is looking for provider to provide a replacement SIEM management solution.
- Does Ogden have any data residency requirements?
  - Yes, City-owned data (logs) will only be stored in U.S. locations (datacenters).
- You stated that there are 3 Major locations, and 40+ minor locations. Our solution requires that an appliance be implemented at each in-scope location. Are the 40+ minor locations going to be in-scope, thus requiring a separate SIEM appliance?
  - The minor locations probably do not need a SIEM appliance, They are all accessible and directly connected either via fiber, wireless or in some smaller cases a Site to Site VPN, those likely will not need a SIEM as it only serves things like burglar alarms or cameras. I would like an SNMP trap on the switches out at these locations however so not sure if your solution requires a separate appliance that just that.