RFP Questions and Answers
Security Incident and Event Management (SIEM)
Solution and Professional Services for Implementation
Job # 05-21-IT
12-Feb-21

Information request as part of RFP question and answer process

Log Sources

Devices in Scope	Product Name	Quanity
Applications		
Anti-Virus / Enpoint Monitoring Number of Host Monitored	N/A	
Database Servers	SQL	14
Email Type and Number of mailboxes	O365/Cloud	1
Point of Sale	Windows Workstations with Card Readers	10
Proxy	N/A	0
Vulnerability Scanners	N/A	0
Web Server	Windows Server with a combination of IIS and/or Apache	25
Log Management Systems	Note - The SIEM will be replacing these	2
Operating Systems		
Apple OSX	N/A	
Cloud	N/A	
IBM iSeries	N/A	
Windows Servers	Windows Server (2012-2019)	149
Domain Controllers	Windows Server	5
Workstations	Windows 10	~800
LINUX Servers		10
Network Devices		
External Firewalls	4 Palo Alto, 1 Cisco	5
Internal Firewalls	N/A	
IDS / IPS	Note these are integrated NGFW, counted above	2

Load Balancers	Azure	2
Network Monitor	Solarwinds for now. This may be something else in the near future	1
Access Points	Cisco	140
Routers	Cisco	6
Switches	Cisco	150
Physical Security Systems	These are windows servers that run the security system	10
Cloud		
AWS	Amazon Web Services (Route 53 DNS Only)	
AZURE	Azure GOV. Note: The devices (Servers and Firewalls are included above)	
Google	N/A	
Email	N/A	
Office 365	Exchange, SharePoint, Office Suite	