PIC011/2020: Questions and answers

1. How many internal facing IPs are in scope for the solution? Approx. 1300 live IP addresses

2. Are all the internal IPs in scope accessible from a single location on the network? I.e. are there separate networks and/or branches or locations that need to be catered for that cannot be scanned centrally?

   The following are the in- scope locations
   - PIC Head Office at Menlyn Maine (Pretoria)
   - PIC Disaster Recovery Site (Sandton)
   - PIC Infrastructure as-a Service (to be Hosted at Vodacom… Currently In project mode)
   - Microsoft Azure

3. Please provide further detail on your cloud infrastructure e.g.
   a. Which Cloud providers do you utilise? Microsoft Azure
   b. Is there public cloud infrastructure in scope?
      i. If so what is the number of IPs in scope? Microsoft Azure, approx. 15 IP addresses
   c. Is there private cloud infrastructure in scope?
      i. If so what is the number of IPs in scope? IaaS to be hosted at Vodacom (estimated 250 IPs)
      ii. How are these IPs reachable for scanning e.g. from internal network, via a jump server, etc.? (migration to private cloud still in project mode, Bidder can propose solution for scanning the IaaS cloud environment)
4. With regard to the Business requirements listed in section 4.1 of the RFP:

RFP Requirement (Section 4.1)	**Clarification Question**
4.1.22 Ability to integrate with any vulnerability scanning tools and existing security tools to aggregate, normalize, prioritize, correlate and improve all of the vulnerability data.	Could you provide a list of existing tools that must be integrated? Microsoft Defender ATP Threat & Vulnerability Management (in O365)
4.1.23 Automated vulnerability remediation response workflows.	Can you elaborate on the level of remediation response workflows required? E.g. Assigning remediation tasks to teams/users, or going further and initiating and automating remediation tasks (e.g. patches) to systems? Assigning remediation tasks to teams/users

4.1.24 Provide capability to integrate with various incident logging solution.	Could you provide the incident logging solutions that must be integrated? Microsoft Service Manager
4.1.32 The solution is expected to operate on all platforms	Does this refer to the types of platforms that can be scanned for vulnerabilities, or the platform that the vulnerability software is installed on? This refers to the platforms that can be scanned for vulnerabilities
4.1.35 The solution must be able to integrate with all and future PIC solutions including the SIEM solution.	Can you provide the current SIEM solution that must be integrated with? QRadar SIEM Microsoft Sentinel