CYBERSECURITY AND IT QUESTIONNAIRE

Client Name:

Main Location or Corporate HQ Address:

1. How many locations?
   - Can you provide a list including site inventory?
2. How many full-time company employees and contractors?
3. How big is the IT team supporting these users?
   - Open head count and how many openings?
4. Please provide an assessment of your IT Team's capabilities today including strengths and weaknesses:
5. Can you provide a list of projects and goals your team is currently engaged, and can you share a 12-24 month roadmap?
   - Do you have remote users and how are they being secured today?
   - Other applications that are critical to your organization – please explain how they are set up?
6. Do you have any primary concerns around your Cybersecurity posture? (data leakage, downtime, legal/regulatory/compliance, reputation, improve posture)
7. What industry or customer concerns do you have around compliance?
   - If so, please explain?
8. Do you need source code or anything proprietary reviewed?
   - If so, can you explain.
9. Is there an existing "baseline" or any known standard for security framework that you are aligned to?
   - Controls Framework you align to:
10. Do you have compliance, regulations, or insurance requirements you need to adhere to and if so, can you explain that?
    - How often are you audited?
    - Which vendors do you use for this?
11. Have you recently had a breach?
    - If so, please explain what you have done and how did it impact your business.
12. Do you have any written Security Polices or Run Books
    - How often do you review them and update them?
13. Do you have written IT Policies or Run Books?
    - How often do you review them and update them?
14. Who makes the company's security decisions and sets policies?
15. Do you need help with policies?
    - If so, how?
16. What is your current email protection and how is this managed today?
    - Do you feel it is effective or are there any improvements that you would like to investigate with other solutions?
17. What is your current End Point Protection and how is this managed today?
    - Do you feel it is effective or are there any improvements that you would like to investigate with other solutions?
18. Can you explain what is in place today in terms of how you monitor, respond, and remediate alerts and suspicious activity?
19. Do you have any SIEM in place?
20. Who manages and what does your SOC look like?
21. Do you have a 360-degree view with your environment today?
22. Do you currently have a security awareness/training program in place and if so can you explain what that looks like?
23. Are there any users who routinely experience phishing attempts?
24. Could a lost laptop or device result in a potential unauthorized data disclosure issue?
25. How do you determine if vulnerabilities have been properly addressed and are under control?
26. What do you do for vulnerability management today?

27. When was the last time you ran a vulnerability scan?
    - How many IP's?
    - Were you given a report and was there anything actionable?
    - If so, can you share the results?
    - Who performed that and how often are you performing the scan?
28. How do you perform patch management today and how is this maintained?
29. What are you doing to have visibility of potentially anomalous behavior and/or threats to servers and Network devices in your environment?
30. How are you handling data loss prevention, and do you have any DLP solutions in place today?
31. Other Security Solutions you have implemented (MFA, ID Mgt, PAM, Zero Trust, ZTNA, SASE)?
    - Please list the vendor and solution and if they meet your needs.
32. When was the last time you ran a penetration scan?
    1. How many IP's?
    2. Were you given a report and was there anything actionable? If so what.
    3. Are you able to share the findings?
    4. Who performed that and how often are you performing the scan?
33. What "continuity of operations" or "incident response" plan, policies or 3rd party support structure do you currently have in place in the event of an attack or outbreak? Please explain:
34. What is your DR strategy and how is this managed?
    - Have you tested your DR strategy?
35. What is your backup strategy and how is this managed?
    - Do you have an RPO and RTO for your backup?
36. Are there any Cybersecurity solutions or topics that you want to learn more about or investigate and why?
37. Please list any other pertinent information you feel will be helpful to assist our understanding of your environment:

NOTES