Alliant Ransomware Supplemental Application

Email Security

1. **Do you pre-screen emails for potentially malicious attachments and links?**	☐ Y ☐ N
2. **Are external emails flagged?**	☐ Y ☐ N
3. **Are macros automatically disabled?**	☐ Y ☐ N
4. **Do you provide a quarantine service to your users?**	☐ Y ☐ N
5. **Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if malicious prior to delivery to the end user?**	☐ Y ☐ N
6. **Do you strictly enforce Sender Policy Framework (SPF) on incoming emails?**	☐ Y ☐ N
7. **How often is phishing/cybersecurity training conducted to all staff?**	☐Never ☐Monthly ☐Quarterly ☐Annually ☐Ad Hoc
8. **Can your users access email through a web app on a non-corporate device?** *If Yes: do you require and enforce Multi-Factor Authentication?*	☐ Y ☐ N ☐ Y ☐ N
9. **Do you use Office 365 in your organization?** *If Yes: do you use the o365 Advanced Threat Protection add-on?*	☐ Y ☐ N ☐ Y ☐ N
10. **Do you implement PowerShell best practices as outlined in the Environment Recommendations by Microsoft?** https://docs.microsoft.com/en-us/mem/configmgr/apps/deploy-use/learn-script-security	☐ Y ☐ N

11. **What email filtering is deployed? (select all that apply)**

☐ Gateway Based(Mimecast/Proofpoint) ☐ Provider Based (O365/Gmail/IBM mail)
☐ Machine Learning-Behavior Based ☐ Supported by a User Reporting Program ☐ None

Internal Security

12. **Do you use an endpoint protection (EPP) product across your enterprises?**

☐ Microsoft ☐ Crowdstrike ☐ Symantec ☐ TrendMicro ☐ Sophos ☐ ESET
☐ McAfee ☐ Kaspersky ☐ Cylance ☐ BitDefender ☐ Carbon Black ☐ Cisco
☐ Panda Security ☐ SentinelOne ☐ F-Secure ☐ Palo Alto Networks
☐ Check Point Software Technologies ☐ Fortinet ☐ Malwarebytes ☐ Other
☐ Have No EPP Product

13. **Do you use an endpoint detection and response (EDR) product across your enterprise?**

☐ Crowdstrike Falcon Endpoint Protection ☐ Cybereason Defense Platform ☐ Cynet 360
☐ Malwarebytes Endpoint Protection and Response ☐ Intercept X ☐ SentinelOne
☐ Symantec Endpoint Security (SES) Complete ☐ Sophos Intercept X ☐ Carbon Black Cloud
☐ Cisco AMP ☐ Symantec EDR ☐ Endgame Endpoint Protection ☐ Fireeye Endpoint Security ☐ RSA Netwitness ☐ McAfee MVision EDR ☐ Fortinet FortiEDR ☐ SolarWinds
☐ RedCanary ☐ BitDefender ☐ Other ☐ Have no EDR Product

14. **Do you require Multi-Factor Authentication for:**	
a. *Remote access to users?*	☐ Y ☐ N
b. *To protect Privileged User accounts?*	☐ Y ☐ N
c. *For all Cloud resources including Office365?*	☐ Y ☐ N
d. *For all Remote Desktop Protocol (RDP) and Virtual Desktop Instances (VDI)?*	☐ Y ☐ N
15. **Is a hardened baseline configuration materially rolled out across servers, laptops, desktops and managed mobile devices?**	☐ Y ☐ N ☐ Partial
16. **What % of the enterprise is covered by your scheduled vulnerability scans?**	

17. **In what time frame do you install critical and high severity patches across your enterprise?**

☐ Within 2 weeks ☐ Within 1 month ☐ Within 2 months ☐ Ad hoc

18. **Do you use Microsoft Active Directory?**	☐ Y ☐ N
If Yes:	
› *Number of user accounts in the Domain Administrators Group (include service accounts, if any)*	
› *Number of service accounts in the Domain Administrators Group*	
› *What are the service accounts used for and why do they require domain admin entitlements?*	
› *What are the footprints of these service accounts? If the account interacts with critical assets such as domain controllers, can it also interact with workstations, servers etc.? Essentially, can a service account get used across multiple solutions, or by both users and applications?*	
› *What Windows log-on types are the accounts using? (Interactive, Network etc.)*	
› *What steps are you taking to mitigate any exposure the service accounts' configuration creates which could result in credential harvesting etc?*	

19. **Which systems are patched with the above cadence?**	☐ Internal Servers ☐ Perimeter Systems ☐ Workstations ☐ None
20. **If you have any end of life or end of support software, is it segregated from the rest of the network?**	☐ Y ☐ N ☐ Partial ☐ N/A
21. **Have you configured host-based and network firewalls to disallow inbound connections by default?**	☐ Y ☐ N ☐ Partial
22. **Do you use a protective DNS service (e.g. Quad9, OpenDNS, or the public sector PDNS)?**	☐ Y ☐ N
23. **Do you use an endpoint application isolation and containment technology?** ☐ Menlo Security Isolation Platform ☐ Authentic8 Silo ☐ Symantec Web Security Service – Web Isolation ☐ CylanceProtect ☐ Puffin Secure Browser ☐Apozy ☐ Bitdefender Browser Isolation ☐ Cigloo Remote Browsing ☐ Cyberinc Isla ☐ Passages by Ntrepid ☐ WEBGAP Remote Browser ☐ Curose Internet Isolation ☐ Cyberwall ☐ Garrison SAVI ☐ Light Point Web ☐ Morphisec Endpoint Threat Prevention – Browser Based ☐Randed AGU ☐ Other ☐ No such Product	
24. **Do your users have local admin rights on their laptop / desktop?**	☐ Y ☐ N
25. **Do users who have admin rights have separate privileged accounts for daily tasks?** *If Yes: How are those accounts controlled?* ☐ By an Identity Access Manager (IAM) Solution ☐ By Technical Policies and Automatically Logged Off ☐ By Administrative Policies ☐ No Policy/Control over Privileged Accounts	☐ Y ☐ N
26. **How is the principle of least privilege enforced in the environment?** ☐ Least privilege on All Data ☐ Least privilege on All Sensitive Data ☐ Least privilege on Some Sensitive Data ☐ All User have Same Access	
27. **Can users run MS Office Macro enabled documents on their systems by default?**	☐ Y ☐ N ☐ Partial
28. **Do you provide your users with a password manager software?**	☐ Y ☐ N
29. **Do you manage privileged accounts using tooling? E.g. CyberArk**	☐ Y ☐ N ☐ Partial
30. **Do you have a security operations center established, either in-house or outsourced?**	☐ Y ☐ N ☐ Partial
31. **Is SMBv1 in use on the network?**	☐ Y ☐ N

32. **Is remote access exposed to the internet (RDP, Telnet, SSH), without any controls such as IP whitelisting?**	☐ Y ☐ N

33. **What elements exist on the segmented network? Select all that apply.**

☐ Demilitarized Zones (DMZs) ☐ Security Network ☐ Guest/Wireless Network
☐ Sites (Office locations, Industrial Control Systems, etc.) ☐ Server Network
☐ IT Management Network ☐ VoIP Network ☐ N/A

Detection & Response Assessment

34. **What is the cadence of internal vulnerability scanning?**	☐ Monthly ☐ Quarterly ☐ N/A
35. **What is the cadence of external vulnerability scanning?**	☐ Monthly ☐ Quarterly ☐ N/A
36. **Is external penetration testing performed?**	☐ Yes. Bi-Annually ☐ Yes. Annually ☐ No

37. **How is the environment monitored?**

☐ Dedicated SOC/MSSP (internal/external staff – on call rotations 24x7)
☐ Dedicated SOC/MSSP (internal/external staff – on call rotations 9x5)
☐ Internal IT Staff Receives Email 24x7
☐ Internal IT Staff Receives Emails, Only Responding When on the Clock
☐ No Monitoring

38. **Is there alerting to an encryption data event?**

☐ Get Alerts to All Encryption Events
☐ Get Alerts to Server Encryption Events
☐ No Alerts for Encryption Events

39. **Is there an incident response plan?**	☐ Y ☐ N
40. **Does the incident response plan include a ransomware playbook?**	☐ Y ☐ N
41. **Do you have a documented process to respond to phishing campaigns (whether targeted specifically at your or not)?** *If yes: Please describe the principal steps to respond*	☐ Y ☐ N

Back-Up & Recovery Policies

42. **Are your backups encrypted?**	☐ Y ☐ N ☐ Partial
43. **Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose?**	☐ Yes-Full Online ☐ Yes-Cloud Service ☐ Yes-Partially Offline ☐ No
44. **Do you use a Cloud synching service (e.g. Dropbox, OneDrive, SharePoint, Google Drive) for backups?**	☐ Y ☐ N
45. **Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months?**	☐ Y ☐ N ☐ Partial
46. **Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware?**	☐ Y ☐ N ☐ Partial
47. **What is the average time to triage and contain security incidents of workstations year to date?** ☐ Do not know/do not track ☐ Less than 30 minutes ☐ 30 minutes – 2 hours ☐ 2-8 hours ☐ Greater than 8 hours	

Please sign below and return this form to your Alliant representative:

Signature:	
Printed Name:	
Title:	
Company:	
Date:	

Alliant