



Alliant Ransomware Supplemental Application

Email Security

1. Do you pre-screen emails for potentially malicious attachments and links?	<input type="checkbox"/> Y <input type="checkbox"/> N
2. Are external emails flagged?	<input type="checkbox"/> Y <input type="checkbox"/> N
3. Are macros automatically disabled?	<input type="checkbox"/> Y <input type="checkbox"/> N
4. Do you provide a quarantine service to your users?	<input type="checkbox"/> Y <input type="checkbox"/> 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?	<input type="checkbox"/> Y <input type="checkbox"/> N
6. Do you strictly enforce Sender Policy Framework (SPF) on incoming emails?	<input type="checkbox"/> Y <input type="checkbox"/> N
7. How often is phishing/cybersecurity training conducted to all staff?	<input type="checkbox"/> Never <input type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Annually <input type="checkbox"/> Ad Hoc
8. Can your users access email through a web app on a non-corporate device? <i>If Yes: do you require and enforce Multi-Factor Authentication?</i>	<input type="checkbox"/> Y <input type="checkbox"/> N <input type="checkbox"/> Y <input type="checkbox"/> N
9. Do you use Office 365 in your organization? <i>If Yes: do you use the o365 Advanced Threat Protection add-on?</i>	<input type="checkbox"/> Y <input type="checkbox"/> N <input type="checkbox"/> Y <input type="checkbox"/> 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	<input type="checkbox"/> Y <input type="checkbox"/> N
11. What email filtering is deployed? (select all that apply) <input type="checkbox"/> Gateway Based(Mimecast/Proofpoint) <input type="checkbox"/> Provider Based (O365/Gmail/IBM mail) <input type="checkbox"/> Machine Learning-Behavior Based <input type="checkbox"/> Supported by a User Reporting Program <input type="checkbox"/> None	

Internal Security

<p>12. Do you use an endpoint protection (EPP) product across your enterprises?</p> <p> <input type="checkbox"/> Microsoft <input type="checkbox"/> Crowdstrike <input type="checkbox"/> Symantec <input type="checkbox"/> TrendMicro <input type="checkbox"/> Sophos <input type="checkbox"/> ESET <input type="checkbox"/> McAfee <input type="checkbox"/> Kaspersky <input type="checkbox"/> Cylance <input type="checkbox"/> BitDefender <input type="checkbox"/> Carbon Black <input type="checkbox"/> Cisco <input type="checkbox"/> Panda Security <input type="checkbox"/> SentinelOne <input type="checkbox"/> F-Secure <input type="checkbox"/> Palo Alto Networks <input type="checkbox"/> Check Point Software Technologies <input type="checkbox"/> Fortinet <input type="checkbox"/> Malwarebytes <input type="checkbox"/> Other <input type="checkbox"/> Have No EPP Product </p>	
<p>13. Do you use an endpoint detection and response (EDR) product across your enterprise?</p> <p> <input type="checkbox"/> Crowdstrike Falcon Endpoint Protection <input type="checkbox"/> Cybereason Defense Platform <input type="checkbox"/> Cynet 360 <input type="checkbox"/> Malwarebytes Endpoint Protection and Response <input type="checkbox"/> Intercept X <input type="checkbox"/> SentinelOne <input type="checkbox"/> Symantec Endpoint Security (SES) Complete <input type="checkbox"/> Sophos Intercept X <input type="checkbox"/> Carbon Black Cloud <input type="checkbox"/> Cisco AMP <input type="checkbox"/> Symantec EDR <input type="checkbox"/> Endgame Endpoint Protection <input type="checkbox"/> Fireeye Endpoint Security <input type="checkbox"/> RSA Netwitness <input type="checkbox"/> McAfee MVision EDR <input type="checkbox"/> Fortinet FortiEDR <input type="checkbox"/> SolarWinds <input type="checkbox"/> RedCanary <input type="checkbox"/> BitDefender <input type="checkbox"/> Other <input type="checkbox"/> Have no EDR Product </p>	
<p>14. Do you require Multi-Factor Authentication for:</p> <p>a. Remote access to users?</p> <p>b. To protect Privileged User accounts?</p> <p>c. For all Cloud resources including Office365?</p> <p>d. For all Remote Desktop Protocol (RDP) and Virtual Desktop Instances (VDI)?</p>	<p><input type="checkbox"/> Y <input type="checkbox"/> N</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N</p> <p><input type="checkbox"/> Y <input type="checkbox"/> N</p>
<p>15. Is a hardened baseline configuration materially rolled out across servers, laptops, desktops and managed mobile devices?</p>	<p><input type="checkbox"/> Y <input type="checkbox"/> N</p> <p><input type="checkbox"/> Partial</p>
<p>16. What % of the enterprise is covered by your scheduled vulnerability scans?</p>	
<p>17. In what time frame do you install critical and high severity patches across your enterprise?</p> <p> <input type="checkbox"/> Within 2 weeks <input type="checkbox"/> Within 1 month <input type="checkbox"/> Within 2 months <input type="checkbox"/> Ad hoc </p>	
<p>18. Do you use Microsoft Active Directory?</p> <p>If Yes:</p> <ul style="list-style-type: none"> › 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? 	<p><input type="checkbox"/> Y <input type="checkbox"/> N</p>

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

32. Is remote access exposed to the internet (RDP, Telnet, SSH), without any controls such as IP whitelisting?	<input type="checkbox"/> Y <input type="checkbox"/> N
33. What elements exist on the segmented network? Select all that apply. <input type="checkbox"/> Demilitarized Zones (DMZs) <input type="checkbox"/> Security Network <input type="checkbox"/> Guest/Wireless Network <input type="checkbox"/> Sites (Office locations, Industrial Control Systems, etc.) <input type="checkbox"/> Server Network <input type="checkbox"/> IT Management Network <input type="checkbox"/> VoIP Network <input type="checkbox"/> N/A	

Detection & Response Assessment

34. What is the cadence of internal vulnerability scanning?	<input type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> N/A
35. What is the cadence of external vulnerability scanning?	<input type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> N/A
36. Is external penetration testing performed?	<input type="checkbox"/> Yes. Bi-Annually <input type="checkbox"/> Yes. Annually <input type="checkbox"/> No
37. How is the environment monitored? <input type="checkbox"/> Dedicated SOC/MSSP (internal/external staff – on call rotations 24x7) <input type="checkbox"/> Dedicated SOC/MSSP (internal/external staff – on call rotations 9x5) <input type="checkbox"/> Internal IT Staff Receives Email 24x7 <input type="checkbox"/> Internal IT Staff Receives Emails, Only Responding When on the Clock <input type="checkbox"/> No Monitoring	
38. Is there alerting to an encryption data event? <input type="checkbox"/> Get Alerts to All Encryption Events <input type="checkbox"/> Get Alerts to Server Encryption Events <input type="checkbox"/> No Alerts for Encryption Events	
39. Is there an incident response plan?	<input type="checkbox"/> Y <input type="checkbox"/> N
40. Does the incident response plan include a ransomware playbook?	<input type="checkbox"/> Y <input type="checkbox"/> N
41. Do you have a documented process to respond to phishing campaigns (whether targeted specifically at your or not)? <i>If yes: Please describe the principal steps to respond</i>	<input type="checkbox"/> Y <input type="checkbox"/> N

Back-Up & Recovery Policies

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

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

Signature: _____
Printed Name: _____
Title: _____
Company: _____
Date: _____