Security Questions Deep-Dive

1 **Do you have a SIEM (Security Incident & Event Management) and / or SOC (Security Operations Center) in place today?**

Who is responding to the alerts? Outsourced SOC or Internal?

2 **Are you currently leveraging any Next Gen AV or Endpoint Detection and Response (EDR) solutions?**

If not, what are you doing for your endpoints to secure them?

3 **Do you train your end users for Phishing attempts? What Security Awareness tools do you use?**

4 **Are you current firewalls being centrally managed and updated to current level of firmware?**

Have you enabled IDS, IPS and Content Filtering

5 **Have you implemented 2FA (Two Factor Authentication) or MFA (Multi Factor Authentication)?**

What applications are you protecting?

6 **Have you implemented Single Sign on?**

7 **How are you currently keeping your servers and endpoints patched?**

Are you patching 3rd party applications regularly? If so by what method?

8 **Do you perform regular vulnerability scans?**

Who is analyzing the scans and remediating the findings?

9 **If you have workloads in the cloud, are you providing the same level of security of them as you are in your on-premises workloads?**

10 **How are you protecting your users from email born security threats?**

If you have your email in the cloud (ie. Office 365), are you backing it up?