# Rapid Security Questionnaire

This checklist is designed to give you an understanding of the key tasks you need to address for thorough cybersecurity. Please note, this list is not exhaustive. Additional steps may need to be taken for complete and effective protection.

## A. Email Security

### 1. Phishing

- ☐ Are you filtering content delivered via email?
- ☐ Are you able to detect and protect against email spoofing of your domain?
- ☐ Do you leverage transport layer encryption for email?
- ☐ Do you have an ephemeral virtualized sandboxing environment for high-risk activities?

### 2. Security Awareness

- ☐ Do you have a security awareness program in place to educate users on primary threats (phishing, malware, etc.)?

## B. Identity & Access Management

### 1. Privileged Access Management

- ☐ Do you leverage the principle of least privilege across your estate?
- ☐ Do you have an enterprise password vault?
- ☐ Do you restrict the usage of local administrator accounts?
- ☐ Do you segment your network and restrict access to assets based on contextual user data?

### 2. MFA

- ☐ Do you leverage enterprise-level multi-factor authentication?
- ☐ Are you able to dynamically trigger MFA based on contextual user data (e.g., UEBA)?

### 3. Single-Sign On

- ☐ Do you leverage best practice SSO integration technologies (e.g., SAML2)?
- ☐ Do you abide by industry best practices for signing and encrypting authentication requests?

### 4. Identity Governance

- ☐ Do you have an identity governance program that includes recurring attestations of privileged users?
- ☐ Do you automate onboarding and offboarding processes?

### 5. Unified IAM

- ☐ Do you have a single source of truth in your

environment for identities?

- ☐ Do you have a scalable way to extend your corporate identities to a new application (e.g., SSO via IDaaS)?
- ☐ Do you have a single location to enforce security policies surrounding identities (e.g., password complexity, MFA, password history, trusted locations, etc.)?

## C. Endpoint Security

### 1. MDM

### 2. Workstations & Servers

- ☐ Are you able to centrally manage and globally limit execution to approved programs on workstations and servers?
- ☐ Do you allow corporate devices direct internet connectivity?
- ☐ Do you have a modern AV deployed?
- ☐ Do you follow and enforce a hardening process for your servers?
- ☐ Do you follow and enforce a hardening process for your operating systems?
- ☐ Do your endpoint controls have behavioral and reputational based capabilities?
- ☐ Are you able to restrict the use of removal storage and connected devices?
- ☐ Do you have a process for keeping your AV up to date with latest signatures and vendor updates?
- ☐ Do you have an ephemeral virtualized sandboxing environment for high-risk activities?
- ☐ Do you have host-based IDS/IPS capabilities deployed to your organization's endpoints?
- ☐ Do you leverage endpoint application firewalls for restricting unauthorized ingress traffic?
- ☐ Do you leverage endpoint application firewalls for restricting unauthorized egress traffic?
- ☐ Are you able to centrally manage and restrict MS Office Macros from executing?
- ☐ Do you centrally harden user applications (e.g., browsers, PDF viewers)?
- ☐ Do you have an Endpoint Detection & Response (EDR) solution deployed and centrally managed in your environment?

## D. Threat & Vulnerability Management

### 1. Patch Management

- ☐ Are you able to patch applications effectively across the enterprise estate?
- ☐ Are you able to patch operation system effectively across the estate?

### 2. Threat Management

- ☐ Are you able to capture and review ingress/egress network traffic to and from corporate computers?
- ☐ Do you leverage an enterprise threat intelligence model for threat/incident hunting?
- ☐ Are you able to centralize and normalize all

available threat intelligence for the enterprise to leverage within your security controls?

- ☐ Do you perform log and alert monitoring?

## E. Cloud Security

### 1. IaaS/PaaS/Serverless

- ☐ Do you standardize deployments via infrastructure as code (e.g., terraform, ansible, puppet, chef)?
- ☐ Do you architect your solutions with availability in mind (e.g., three, four, or five 9's)?
- ☐ Do you follow CSP best practices when storing private keys and secrets?
- ☐ Do you have clearly understood and tested system recovery capabilities?
- ☐ Are you leveraging and periodically testing daily backups in your organization?
- ☐ Have you established and tested business continuity and disaster recovery plans?

### 2. SaaS

- ☐ Do you restrict the use of cloud storage services and scan for sensitive organizational data via outbound emails?
- ☐ Do you integrate SaaS applications into your IAM architecture and identity lifecycle via standard technologies when possible (e.g., SAML-based SSO)?
- ☐ Do you restrict access to company owned network addresses whenever possible?
- ☐ Do you have a reliable process or scoring system to assess the security risk of your vendors?

### 3. Containerization

- ☐ Do you scan your container image repositories for vulnerabilities?
- ☐ Do you have policies in place to prevent container images with critical or high vulnerabilities from being deployed to your production environment?
- ☐ Do you have the ability to detect containers running in production environments with critical/high vulnerabilities?

### 4. CSPM (Cloud Security Posture Management)

- ☐ Do you have a centralized and scalable way of measuring the posture of your cloud infrastructure against known security frameworks?

### 5. CWPP (Cloud Workload Protection Platform)

- ☐ Do you have a centralized and scalable way of protecting cloud workloads during runtime?
- ☐ Do you have a centralized and scalable way of managing the operations of your cloud workloads?
- ☐ Do you leverage a network-based IDS/IPS?

## F. Data Loss Prevention

### 1. Data Classification

- ☐ Are you able to label documents that contain

sensitive information?

### 2. DLP

- ☐ Are you able to set granular policies based upon previously classified information for egress network traffic?
- ☐ Are you able to set granular policies based upon previously classified information for outbound email?
- ☐ Are you able to restrict the use of removal storage and connected devices?

## G. Application Security

### 1. Asset Catalog

- ☐ Have you established an asset catalog to determine your mission critical applications and related systems?

### 2. Continuous Integration/Continuous Deployment

- ☐ Do you have a centralized and standard process for your software builds?
- ☐ Do you require unit tests to be developed and serve as a prerequisite for build success?
- ☐ Do you have security toll gates in place to ensure the integrity of the software as it moves through your application delivery lifecycle?
- ☐ Has your organization established and communicated security policies?

### 3. SAST

- ☐ Do you scan your code base for known vulnerabilities and defects?
- ☐ Do you scan your code repositories for known vulnerabilities and defects?

### 4. DAST

- ☐ Do you scan your software for behavioral inconsistencies and defects before deploying to a production environment?

### 5. Penetration Testing

- ☐ Do you periodically coordinate penetration tests for critical and internet facing applications?

### 6. PKI

- ☐ Do you leverage a trusted commercial certificate authority for the provisioning of TLS certs for your internet facing sites?
- ☐ Do you prevent the use of wildcard certificates for your externally facing applications?
- ☐ Do you have a scalable certificate governance and provisioning program for your internet facing applications?