CHECKLIST

VULNERABILITY

- [ ] How do you remediate the vulnerability?
- [ ] What information should be provided about the vulnerability?
- [ ] Is a vulnerability assessment program expensive?
- [ ] How does a given vulnerability impact your own network?
- [ ] How to standardize sla for data recovery vulnerability?
- [ ] What is the level of effort required to address the vulnerability in its entirety?
- [ ] Does the cloud provider conduct regular vulnerability assessments and penetration tests?
- [ ] What should a solutions architect do to remediate the vulnerability?
- [ ] How did you find the vulnerability?
- [ ] How should vulnerability be measured?
- [ ] Does the nature of the vulnerability make it difficult to exploit?
- [ ] Is the vulnerability actually being exploited?
- [ ] What is vulnerability scanning and how can it be leveraged?
- [ ] Are vulnerability patches publicly visible long before disclosure?
- [ ] How important are the applications impacted by the vulnerability?
- [ ] How is vulnerability remediation prioritized?
- [ ] What measures would reduce the vulnerability of elements/groups?
- [ ] How much time do you spend working with other teams on vulnerability remediation, from scan to fix?
- [ ] Is there a capability maturity model for threat and vulnerability management?
- [ ] What categories of information assets are included in your vulnerability assessment and remediation program?
- [ ] What specific vulnerability checks should be present in your database assessment product?
- [ ] Did it involve performing some form of vulnerability scanning?

CHECKLIST

- [ ] Who owns the responsibility to remediate the vulnerability of a solution, SaaS infrastructure or corporate system?
- [ ] What domains or URLs are associated with delivering exploits for a vulnerability?
- [ ] Are vulnerability tests conducted on a quarterly basis?
- [ ] Does the solution provide an approval work flow for vulnerability exceptions?
- [ ] Are vulnerability reporting rates declining?
- [ ] Are vulnerability scores used consistently?
- [ ] What is different about database vulnerability assessment?
- [ ] Can the common vulnerability scoring system be trusted?
- [ ] Can the solution perform discovery, vulnerability, and configuration assessments in a single unified scan?
- [ ] What malicious files are known to exploit a vulnerability?
- [ ] Which is your vulnerability scanner configured to scan?
- [ ] How is the age of each vulnerability calculated?
- [ ] What is the actual severity of the vulnerability?
- [ ] When should a vulnerability assessment be used?
- [ ] What exactly is vulnerability assessment, and how does it differ from penetration testing?
- [ ] How much time on average does your development team spend remediating each vulnerability found in development?
- [ ] What kind of vulnerability scanning do you do?
- [ ] Do you believe your vulnerability remediation program is mature?
- [ ] How much could be lost if the module has a vulnerability introduced?
- [ ] Are vulnerability scanning tools run on the incident management systems and networks?
- [ ] How should active vulnerability scans be managed for environments sensitive to denial of service impacts?
- [ ] Which remediation actions should the analyst take to implement a vulnerability management process?
- [ ] How do you risk prioritize your vulnerability remediation efforts?

CHECKLIST

- [ ] How are you securing new technology adoption and managing vulnerability with your legacy technology?
- [ ] Does your vulnerability scanner perform authenticated scans?
- [ ] Do you need to create a vulnerability management policy or update it?
- [ ] How are vulnerable items and vulnerability groups assigned to remediation teams?
- [ ] How much time on average does your development team spend remediating each vulnerability found in production?
- [ ] What vulnerability checks are tested?
- [ ] When did you find the vulnerability?
- [ ] How often do you run vulnerability scans?
- [ ] What policy levers do you have for reducing vulnerability?
- [ ] How long is long enough to respond to a vulnerability?
- [ ] NOTES: