Security - Assessment Questions

Whiteboard Session

Question	Why we ask?	How to score/rate? (1 lowest - 5 highest)	Weight?	What data can we pull to quantify?
Who is most likely to pose a potential threat?	It’s important to consider who is likely to attempt to abuse this application. Is it anonymous users on the Internet? Your customers? Internal users?			
What kind of data are you trying to protect?	Determining the type of data you are looking to protect as well, the sensitivity of that data, and the location of that data will help prioritize security efforts.			
What does your application's attack surface look like?	Defining the trust boundaries and attack surface you are exposing, to both untrusted and trusted users, is important.			
Where have you struggled with application-related security issues in the past?	This might point you in the direction of potential areas of concern. What application security incidents have taken place in the past if any?			
What Security Assessment and Testing services are in place ?				
Which security-related items need to be implemented and tested before other testing occurs?				
Does your organization have a formal system development lifecycle policy that includes application development and security testing?				
Do you know what you need to know about Security Assessment and Testing?				
What types of functional tests are performed on the software during its development (e.g., spot checking, component-level testing, security testing, integrated testing)?				
Who are your key stakeholders who need to sign off?				
What would be important requirements for an approach to test the security of a web application?				
Describe the design of the pilot and what tests were conducted, if any?				
What key stakeholder process output measure(s) does Security Assessment and Testing leverage and how?				
Has the Security Assessment and Testing work been fairly and/or equitably divided and delegated among team members who are qualified and capable to perform the work?				
Do you have a procedure for notifying authorities in the case of a disaster or Application security incident?				
How many systems are under the scope of Vulnerability Management and Penetration Testing?				
How does the team verify that corrective actions were were tracked and resolved?				
What are your key Security Assessment and Testing indicators that you will measure, analyze and track?				
What particular quality tools did the team find helpful in establishing measurements?				
What are the different categories of penetration testing your organization performs?				
How do you ensure that overall security is analyzed by your SAST tool?				

How do you know that Security Assessment and Testing analysis is complete and comprehensive?				
Is Process Variation Displayed/Communicated?				
Ids/ips traffic pattern analysis can often detect or block attacks such as a denial-of-service attack or a network scan. However, in some cases this is legitimate traffic (such as using cloud infrastructure for load testing or security testing). Does the cloud provider have a documented exception process for allowing legitimate traffic that the ids/ips flags as an attack pattern?				
How is the Security Assessment and Testing Value Stream Mapping managed?				
What Security Assessment and Testing metrics are outputs of the process?				
Are your outputs consistent?				
How do you measure the operational performance of your key work systems and processes, including productivity, cycle time, and other appropriate measures of process effectiveness, efficiency, and innovation?				
What practices helps your organization to develop its capacity to recognize security threats and patterns?				
How are the Security Assessment and Testing's objectives aligned to the group's overall stakeholder strategy?				
When a Security Assessment and Testing manager recognizes a problem, what options are available?				
For your Security Assessment and Testing project, identify and describe the business environment, is there more than one layer to the business environment?				
Does the team Secure OS, ‘hardening the OS,’ trim all unnecessary modules and files, and keep up with latest security patches				
What access controls will help ensure that unauthorised images or system updates are prevented.				
Does the security scan check for containers Vulnerability in all registries				
How you make sure that Containers are Digitally signed or do you have any specific integrity checks on container images				
Do you have policy for Tear down and clean up unused containers				
What Measures or Configurations are in place to avoid container attack				