Exam Report: 3.9.3 Practice Questions

Date: 1/16/2020 5:22:07 pm
Time Spent: 8:30

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 80%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Match each Interoperability Agreement document on the left with the appropriate description on the right. Each document may be used once, more than once, or not at all.

Specifies exactly which services will be performed by each party

SLA

Creates an agreement with a vendor to provide services on an ongoing basis

BPO

Summarizes which party is responsible for performing specific tasks

MOU

Documents how the networks will be connected

ISA

Defines how disputes will be managed

SLA

Specifies a preset discounted pricing structure

BPO

Explanation

There are several key documents that may be included within an Interoperability Agreement (IA) that you should be familiar with:

- A Service Level Agreement (SLA) specifies exactly which services will be performed by the third party and what level of performance they guarantee. An SLA may also provide warranties, specify disaster recovery procedures, define how disputes will be managed, and specify when the agreement will be terminated.
- A Blanket Purchase Order (BPO) is an agreement with a third-party vendor to provide services on an ongoing basis. BPOs are typically negotiated to take advantage of a preset discounted pricing structure.
- A Memorandum of Understanding (MOU) is a very important document that provides a brief summary of which party in the relationship is responsible for performing specific tasks. In essence, the MOU specifies who is going to do what and when.
- An Interconnection Security Agreement (ISA) documents how the information systems of each party in the relationship will be connected and share data.

References

LabSim for Security Pro, Section 3.9.
[All Questions SecPro2017_v6.exm THIRD_PARTY_01]

Question 2: Correct

Your organization entered into an Interoperability Agreement (IA) with another organization a year ago. As a part of this agreement, a federated trust was established between your domain and the partner domain.

The partnership has been in the ongoing operations phase for almost nine months now. As a security administrator, which tasks should you complete during this phase? (Select two.)

- [x] Conduct periodic vulnerability assessments
- [ ] Draft an MOU document
- [x] Verify compliance with the IA documents
- [ ] Negotiate the BPO agreement
- [ ] Disable user and groups accounts used by the partner organization to access your organization's data

Explanation

During the ongoing operations phase of the relationship, you should:

- Regularly verify compliance with the IA documents
- Conduct periodic vulnerability assessments to verify that the network interconnections created by the relationship have not exposed or created security weaknesses

During the onboarding phase of the relationship, you should attend to BPO and draft the MOU. Disabling user and group accounts should take place during the off-boarding phase.

References

LabSim for Security Pro, Section 3.9.
[All Questions SecPro2017_v6.exm THIRD_PARTY_02]

Question 3: Correct

Your organization is in the process of negotiating an Interoperability Agreement (IA) with another organization. As a part of this agreement, the partner organization proposes that a federated trust be established between your domain and their domain. This configuration will allow users in their domain to access resources in your domain and vice versa.

As a security administrator, which tasks should you complete during this phase? (Select two.)

- [ ] Conduct security audits on the partner organization.
- [ ] Verify compliance with the IA documents.
- [ ] Reset all passwords used by the third party to access data or applications on your network.
- [x] Identify how data ownership will be determined.
- [x] Identify how data will be shared.

Explanation

During the onboarding phase of a third-party relationship, you need to formulate a plan that addresses several issues, including:

- How data ownership will be determined
- How data will be shared

Security and compliance audits should be conducted during the ongoing operations phase of the relationship. Partner passwords should be reset during the off-boarding phase.

References

LabSim for Security Pro, Section 3.9.
[All Questions SecPro2017_v6.exm THIRD_PARTY_03]

Question 4: Correct

Match each third-party integration phase on the left with the tasks that need to be completed during that phase on the right. Each phase may be used once, more than once, or not at all.

Communicate vulnerability assessment findings with the other party

✔ Ongoing operations

Disable VPN configurations that allow partner access to your network

✔ Off-boarding

Compare your organization's security policies with the partner's policies

✔ Onboarding

Disable the domain trust relationship between networks

✔ Off-boarding

Identify how privacy will be protected

✔ Onboarding

Draft an ISA

✔ Onboarding

Conduct regular security audits

✔ Ongoing operations

Explanation

During the onboarding phase of a relationship, you should take steps to ensure that the integration process maintains the security of each party's network by completing tasks, such as:

- Comparing your organization's security policies and infrastructure against each partner organization's policies and infrastructure
- Identifying how privacy will be protected
- Drafting an ISA to document how the information systems of each party in the relationship will be connected and share data

During the ongoing operations phase of the relationship, you need to verify that all parties are abiding by the Interoperability Agreement documents. To accomplish this goal, you should:

- Conduct regular security audits to ensure that each party in the relationship follows the security-related aspects of the IA documents
- Communicate vulnerability assessment and security audit findings with all of the parties in the relationship to maintain risk awareness

When the relationship with the third party ends, you need to ensure that all of the doors that were opened between organizations during the onboarding phase are closed by completing tasks, such as:

- Disabling any VPN, firewall, router, or switch configurations that allowed access to your network from the third-party network
- Disabling any domain trust relationships that were established between the organizations

References

LabSim for Security Pro, Section 3.9.
[All Questions SecPro2017_v6.exm THIRD_PARTY_04]

Question 5: Incorrect

Your company is preparing to enter into a partner relationship with another organization. It will be necessary for the information systems used by each organization to connect and integrate with each other.

Which of the following is of primary importance as you take steps to enter into this partner relationship?

- Ensure that all aspects of the relationship are agreed upon in writing
- ~~Identify how data ownership will be determined~~
- Ensure that both organizations have similar incident response procedures
- Ensure that the integration process maintains the security of each organization's network

Explanation

The most important step to take as the two parties enter into this partner relationship is to ensure that the integration process maintains the security of each organization's network.

Identifying how data ownership will be determined, ensuring that all aspects of the relationship are agreed upon in writing, and finding out if both organizations have similar incident response procedures are just a few of the steps that are taken to make sure that the security of each organization's network is maintained.

References

LabSim for Security Pro, Section 3.9.
[All Questions SecPro2017_v6.exm THIRD_PARTY_05]