Simulado – Certificação TI Safe CASE (*Certified Automation Security Engineer*)

1) Qual dos itens a seguir NÃO é um benefício da detecção cibernética em sistemas SCADA?
   (a) A detecção acelera a resposta e limita os problemas em ataques com sucesso.
   (b) A detecção pode identificar alterações em sistemas de segurança cibernética.
   (c) A detecção pode identificar ataques ainda na fase de reconhecimento.
   (d) A detecção pode automaticamente bloquear alguns tipos de ataques.
   (e) Ferramentas de detecção podem ser atualizadas para identificar novas vulnerabilidades.

2) Qual das seguintes diretivas de grupo (GPOs) está disponível no Active Directory?
   (a) Comportamento na remoção de Smart Cards.
   (b) Banner de Login.
   (c) Política de senhas.
   (d) Tempo sem uso.
   (e) Todas as alternativas anteriores estão corretas.

3) Selecione a alternativa FALSA a respeito dos agentes de IDS e IPS:
   (a) Os agentes dos IDS e IPS de Host são intrusivos e sempre reescrevem ou modificam a pilha TCP-IP.
   (b) Os agentes dos IDS e IPS de Host podem incluir tanto assinaturas quanto detecções de anormalidades.
   (c) Os agentes dos IDS e IPS de Host podem provocar a parada de um computador em processos de emergências.
   (d) Os agentes dos IDS e IPS de Host identificam ataques que estejam ocorrendo na rede.
   (e) Os agentes dos IDS e IPS de Host devem ser certificados pelo fabricante do aplicativo SCADA antes de serem implementados.

4) Verdadeiro ou Falso: Um Firewall pode ter mais de uma DMZ.
   (a) Verdadeiro.
   (b) Falso.

5) O primeiro sistema operacional a vir com o Active Directory foi:
   (a) Windows NT.
   (b) Windows 95.
   (c) Windows 98.
   (d) Windows 2000.
   (e) Linux.

6) Selecione a resposta que NÃO é uma vantagem em usar um firewall em *appliance* ao invés de usar um firewall instalado em um servidor genérico?
   (a) Melhor rastreamento de estados e melhores funcionalidades de filtragem de pacotes.
   (b) Um sistema operacional reduzido e com customizações de segurança (*hardening*).
   (c) Sistema operacional pré-instalado e software do firewall tornam a instalação mais fácil.
   (d) Uma GUI para configurar o firewall em appliance elimina a necessidade de conhecer o sistema operacional.
   (e) Ter um mesmo fabricante para o suporte do hardware e software do firewall.

7) Selecione a dispositivo que NÃO é comumente encontrada em dispositivos de campo SCADA:
   (a) RTU.
   (b) CLP.
   (c) IED.
   (d) Servidor de dados históricos.

8) O item “Usuários devem selecionar uma senha difícil de ser adivinhada” é um exemplo de:
   (a) Um item de um guia de segurança.
   (b) Um item de um procedimento de segurança.
   (c) Um item de um padrão de segurança.
   (d) Um item de uma política de segurança.

9) Verdadeiro ou Falso: Caso um *smart card* de autenticação de um usuário seja perdido em um esquema de autenticação por duplo fator, a segurança do sistema estará comprometida.
   (a) Verdadeiro.
   (b) Falso.

10) O Acesso remoto à rede SCADA confiável:
   (a) Deveria ser permitido para controle remoto de processos em situações de emergência.
   (b) Nunca deveria ser permitido.
   (c) Deveria ser permitido para evitar o firewall.
   (d) Deveria ser limitado à manutenções de emergência e tarefas administrativas.

GABARITO

1. (d) A detecção pode automaticamente bloquear alguns tipos de ataques.
2. (e) Todas as alternativas anteriores estão corretas.
3. (d) Os agentes dos IDS e IPS de Host identificam ataques que estejam ocorrendo na rede.
4. (a) Verdadeiro.
5. (d) Windows 2000.
6. (a) Melhor rastreamento de estados e melhores funcionalidades de filtragem de pacotes.
7. (d) Servidor de dados históricos.
8. (d) Um item de uma política de segurança.
9. (b) Falso.
10. (a) Deveria ser permitido para controle remoto de processos em situações de emergência.