

Exam Objectives that do NOT Exist in Security+ SY0-401 but ARE in SY0-501

OBJ/Sub-OBJ

NEW in 501

3.0 Architecture and Design

3.2 Given a scenario, implement secure network architecture concepts.

- Zones/topologies
 - o DMZ 1.3 DMZ
- Segregation/segmentation/isolation **Main sub-obj. 4.5 for below**
 - o Physical **4.5** **NEW**
 - o Logical (VLAN) **4.5** **NEW**
 - o Virtualization **4.5** **NEW**
 - o Air gaps **NEW**
- Tunneling/VPN **New- 4.0 is Wireless only**
 - o Site-to-site **New- 4.0 is Wireless only**
 - o Remote access **New- 4.0 is Wireless only**
- Security device/technology placement
 - o SSL accelerators **NEW**
 - o Aggregation switches **NEW**
 - o Taps and port mirror **NEW**
- SDN **NEW**

3.3 Given a scenario, implement secure systems design.

- Hardware/firmware security
 - o FDE/SED **NEW**
 - o UEFI/BIOS **NEW**
 - o Supply chain **NEW**
 - o Hardware root of trust **NEW**
 - o EMI/EMP
- Appliance **NEW**
- Kiosk **NEW**
- Mobile OS
 - o Secure configurations **NEW**
- Peripherals
 - o Wireless keyboards **NEW**
 - o Wireless mice **NEW**
 - o Displays **NEW**
 - o WiFi-enabled MicroSD cards **NEW**
 - o Printers/MFDs **NEW**
 - o External storage devices **NEW**
 - o Digital cameras **NEW**

3.4 Explain the importance of secure staging deployment concepts.

- Integrity measurement

3.5 Explain the security implications of embedded systems.

- o Wearable technology **NEW**
- o Home automation
 - SoC **NEW**
 - RTOS **NEW**
 - Camera systems **NEW**
 - Special purpose **NEW**
- o Medical devices **NEW**
- o Aircraft/UAV **NEW**

3.6 Summarize secure application development and deployment concepts.

- Development life-cycle models **NEW**
 - o Waterfall vs. Agile **NEW**
- Secure DevOps **NEW**
 - o Security automation **NEW**
 - o Immutable systems **NEW**
 - o Infrastructure as code **NEW**
- Provisioning and deprovisioning **NEW**
- Secure coding techniques
 - o Normalization **NEW**
 - o Stored procedures **NEW**
 - o Obfuscation/camouflage **NEW**
 - o Memory management **NEW**
 - o Use of third-party libraries and SDKs **NEW**
 - o Data exposure **NEW**
- Code quality and testing
 - o Stress testing **NEW**
 - o Model verification **NEW**
- Compiled vs. runtime code **NEW**

3.7 Summarize cloud and virtualization concepts.

- VM sprawl avoidance **NEW**
- VM escape protection **NEW**
- VDI/VDE **NEW**
- Cloud access security broker **NEW**

3.8 Explain how resiliency and automation strategies reduce risk.

- Automation/scripting
 - o Automated courses of action **NEW**
- Templates **NEW**
- Master image **NEW**
- Non-persistence **NEW**
 - o Snapshots **NEW**
 - o Revert to known state **NEW**
 - o Rollback to known configuratic **NEW**

o Live boot media	NEW
· Scalability	NEW
· Distributive allocation	NEW

3.9 Explain the importance of physical security controls.

· Airgap	NEW
· Faraday cage	NEW
· Screen filters	NEW ?