

## ZT Assessment Questions

- 1 Data
  - 1.1 Where does the organization store sensitive data?
    - 1.1.1 On-premises
    - 1.1.2 Cloud
    - 1.1.3 Hybrid
  - 1.2 What kind of sensitive digital assets does your business need to protect? (Select all that apply)
    - 1.2.1 Consumer data
    - 1.2.2 IoT
    - 1.2.3 SCADA
    - 1.2.4 APIs
    - 1.2.5 Banking data
    - 1.2.6 Customer data
    - 1.2.7 Medical data
    - 1.2.8 Card data
  - 1.3 Do you continuously scan for sensitive data in the environment?
    - 1.3.1 Yes
    - 1.3.2 No
    - 1.3.3 Not consistently
  - 1.4 Do you have the ability to label data for sensitivity and other context (metadata)?
    - 1.4.1 Using regex
    - 1.4.2 Using ML models
    - 1.4.3 Manually
    - 1.4.4 Other
  - 1.5 Do you maintain an inventory of data sources for the business and the applications that depend on them?
    - 1.5.1 Yes
    - 1.5.2 No
    - 1.5.3 Not consistently
  - 1.6 Within your organization, do you understand the relationships between upstream data sources or data producers and downstream data consumers?
    - 1.6.1 Yes
    - 1.6.2 No
    - 1.6.3 Not consistently
- 2 Workloads
  - 2.1 Does your organization create bespoke software systems?
    - 2.1.1 For ourselves
    - 2.1.2 For others
    - 2.1.3 No
  - 2.2 Do your developers write their own components for data protection?
    - 2.2.1 Always
    - 2.2.2 Sometimes
    - 2.2.3 Never
  - 2.3 Can your applications respond defensively to a change in risk level?
    - 2.3.1 Yes
    - 2.3.2 No
    - 2.3.3 Not consistently
- 3 Identity
  - 3.1 Where is your authoritative source of identity in the organization?
    - 3.1.1 On-premises

- 3.1.2 Cloud
- 3.1.3 Hybrid
- 3.2 Do you monitor identities for changes in risk level? (UEBA)
  - 3.2.1 Yes
  - 3.2.2 No
  - 3.2.3 Not consistently
- 3.3 Can you dynamically assess an identity's authorization to access specific resources before each attempt?
  - 3.3.1 Yes
  - 3.3.2 No
  - 3.3.3 Not consistently

#### 4 Devices

- 4.1 Is there a strong associate between devices and identities?
  - 4.1.1 Yes
  - 4.1.2 No
  - 4.1.3 Not consistently
- 4.2 Do you monitor devices for changes in risk level? (UEBA)
  - 4.2.1 Yes
  - 4.2.2 No
  - 4.2.3 Not consistently
- 4.3 Can you dynamically assess an entity's authorization to access specific resources before each attempt?
  - 4.3.1 Yes
  - 4.3.2 No
  - 4.3.3 Not consistently