STUDENT USE ONLY

Student:

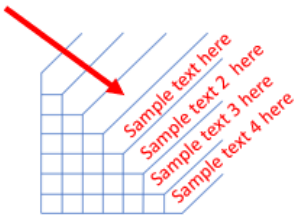
(LastName)_____(FirstName)_____

Class_____Section_____Semester:_____

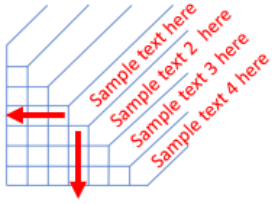
Week:_____Project:_____

Instructions:

1. Place property (or subject) between 45-degree angle:



2. Identify adjoining similarities:



3. Mark associations using:

For identifying SIEM/Security products:

Identify and rank 10 components (data sets or logs) that can be imported to a SIEM - rank them upon, do this with 2 separate SIEM products (LogRythm, Splunk, QRadar, ArcSight, AlienVault, NuSiem, Dell SecureWorks, Rapid 7) Rank according to Application Programming Interface (API):

API rating "0" - Data integration is not possible with non-proprietary data sets
API rating "1" - manual retrieval of information
API rating "2" - We can produce API
API rating "3" - Community will produce API
API rating "4" - Organization will produce and deploy API
API rating "5" - Existing API produced and backed by Vendor

For Cost Associations (Highest cost to Lowest cost):

1 – _____ to _____ (example over $50,000)
2 – _____ to _____ (example $40,000 to $49,999)
3 – _____ to _____ (example $25,000 to $39,999)
4 – _____ to _____ (example $10,000 to $24,999)
5 – _____ to _____ (example under $9,999)

For Identifying Indicators of Compromise (IoC):

Rank according to:

1 – No association (validated or confirmed)
2 – Suspected not association
3 – Association unknown (status unknown)
4 – Suspected association
5 – Association confirmed (validated or confirmed)