

[Redacted]

[Redacted]

E

(0-3, with 3 being the perfect score)

Q e i 3

D e c a d a i i a d d a e !? h e c b g e f e c i D e c i b e e c i e d

e A

D e c i b e h d d e a e h i

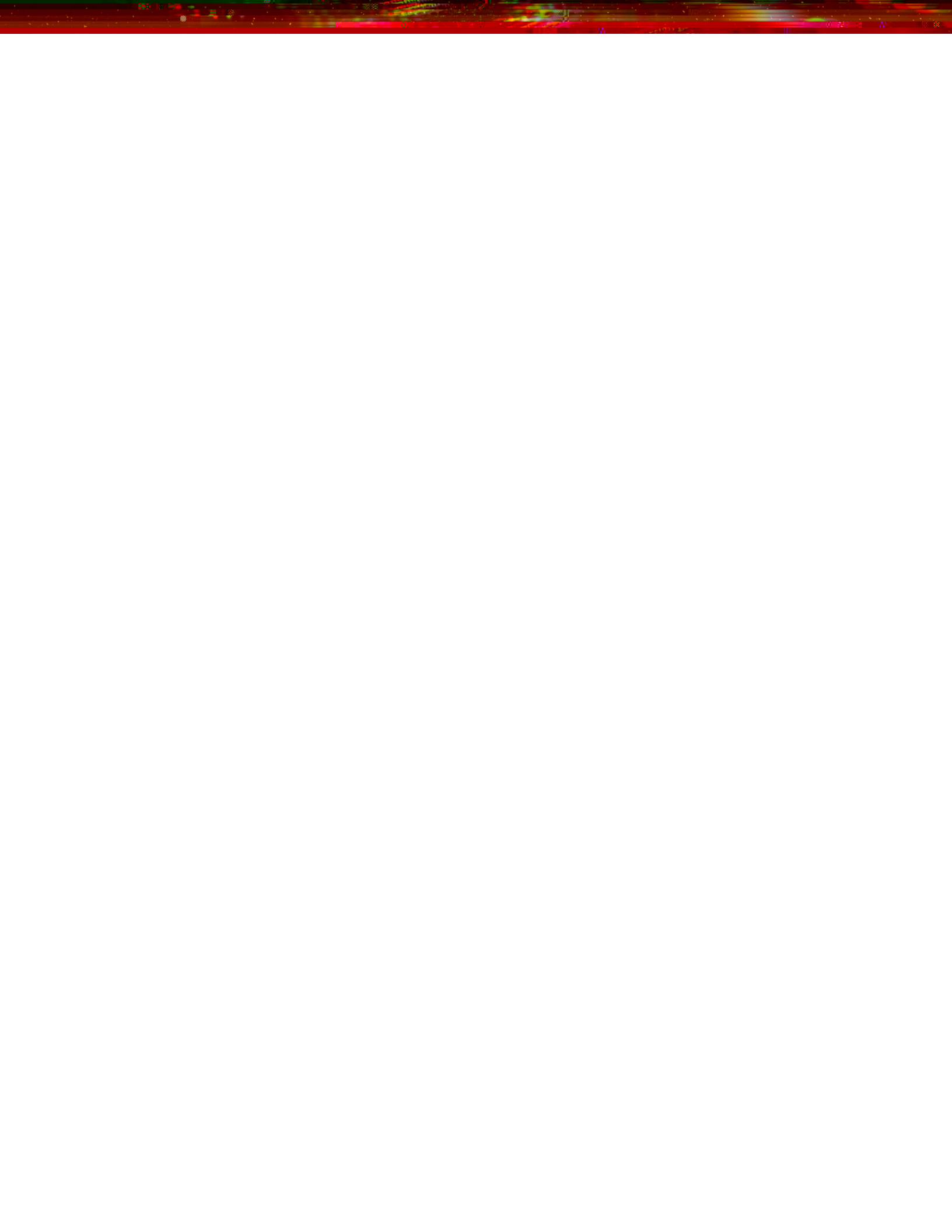
W h h i a e

S e

Your data has to be secure, both in motion and at rest. Some people charge extra for encrypting your historical data. Know your options.

1 2 0 3





Q e i 6

H d li e i a i f a g e d a e ?

e A

De c i b e h d t b e a e h i

W h h i a e

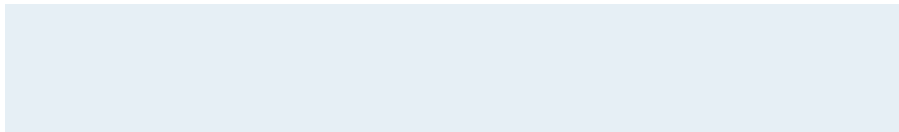
S e

You need to be able to query targeted data and large data sets. Make sure your solution can handle both types of queries with performance expectations.

1 2 0 3

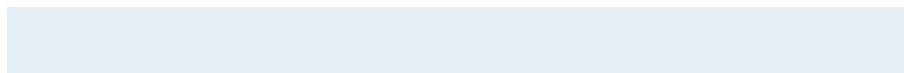
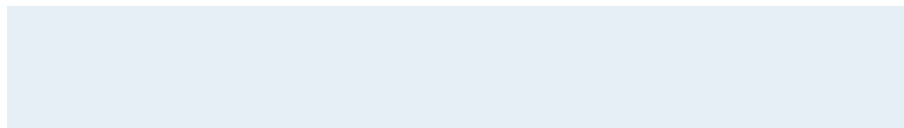
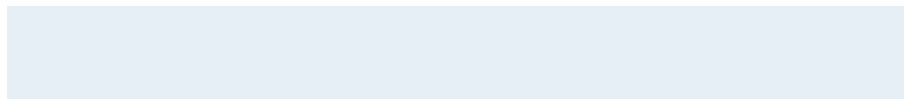
Q e i 7

P a l e d e c i b e h e a a i g e d a (a d



a 

c



We all have too much alert fatigue - how does this solution mitigate it?

Exclusions can drastically reduce alerts.

Grouping alerts can reduce alert fatigue and incidents.

UEBA can be a critical method for detecting threats like stolen creds. Understand if it is included and how it is priced.

(

Not all UEBA is created equal. Some UEBA models rely on a specific data source or format to function. Understand the limitations of the UEBA models.

Since UEBA relies on AI and models, you have to understand what it takes to get data into the model, train it, and tune it.

Category

()

Question 1

Describe the decision automation and machine learning capabilities of your SOAR.

Answer

Describe how you would demonstrate this to us

Why this matters

Score

Are

Question 4

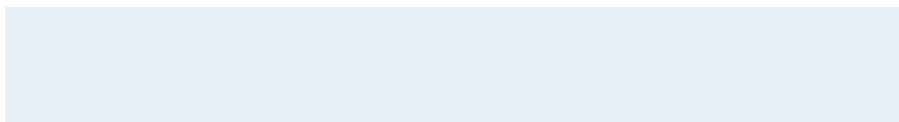
What is included in your SOAR implementation?

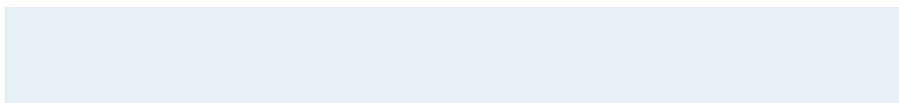
Answer

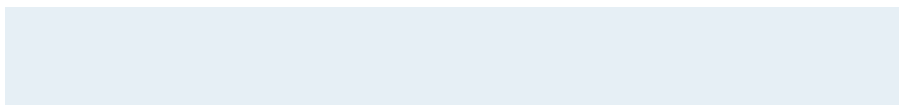
Describe how you would demonstrate this to us

Why this matters

Score







Category



Question 1

How does the solution automatically investigate events?

Answer

Describe how you would demonstrate this to us

Why this matters

Score

Question 4

How does your solution include hunting for threats (including zero-day threats) within our environment?

Answer

Describe how you would demonstrate this to us

Why this matters

Alerts can only detect known threats. You need a solution that is equally effective at hunting and finding unknown and emerging threats. Understand what the solution brings to the table in this area.

Score

0 1 2 3

Question 5

Is there any special software we need to deploy to support this hunting?

Answer

Describe how you would demonstrate this to us

Why this matters

If threat hunting requires 3rd party software or solutions, be aware of everything you need and what the process is for using the entire stack.

Score

0 1 2 3 4 5

Question 6

Does your hunting methodology map to any security frameworks e.g. MITRE? Please explain.

Answer

Describe how you would demonstrate this to us

Why this matters

Score

[Empty text box for answer]