

## CS457 SIEM Software Lab - Sample Answers - Andy, Cary, Chuck, Juno

### Lab Questions:

#### Question 1:

### Agents (1)

[Deploy new agent](#) [Refresh](#) [Export formatted](#) [More](#) [Settings](#)

☒ Show only outdated

[WQL](#)

<input type="checkbox"/>	ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
<input type="checkbox"/>	001	juno-laptop	127.0.0.1	default	Ubuntu 24.04.1 LTS	node01	v4.9.2	<span>●</span> <a href="#">Info</a>	<a href="#">View</a> <a href="#">More</a>

Rows per page: 10 [<](#) [1](#) [>](#)

#### Question 2:

[Filter by type](#) 0

Selected fields [v](#)

[\\_source](#)

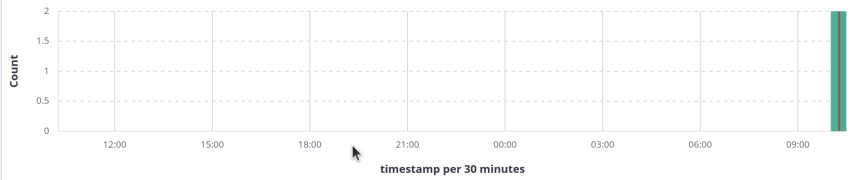
Available fields [v](#)

[Search](#) [DQL](#) [Last 24 hours](#) [Show dates](#) [Refresh](#)

[rule.groups: authentication\\_success](#) [+ Add filter](#)

2 hits

Nov 29, 2024 @ 10:16:03.261 - Nov 30, 2024 @ 10:16:03.261 per [Auto](#)



Time [v](#)

[\\_source](#)

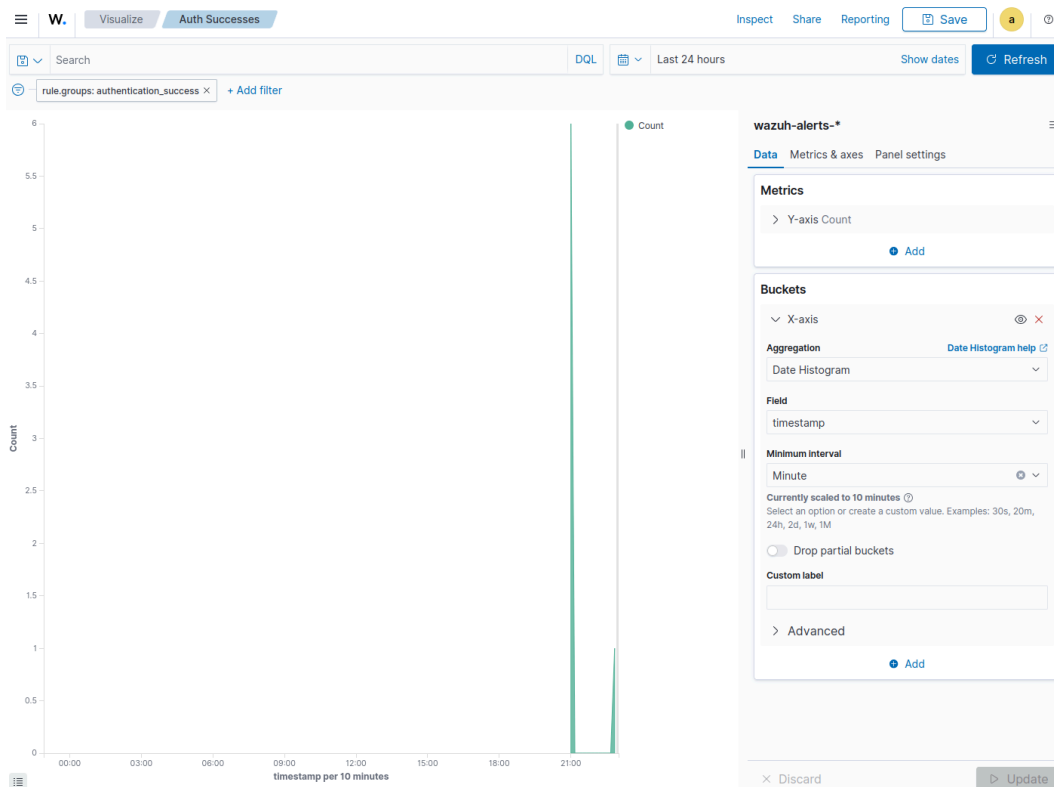
[Nov 30, 2024 @ 10:15](#) [+](#) [-](#)

```
predecoder.hostname: juno-laptop predecoder.program_name: su predecoder.timestamp: Nov 30 15:15:00 input.type: log agent.ip: 127.0.0.1 agent.name: juno-laptop agent.id: 001 manager.name: wazuh.manager data.srcuser: juno data.uid: 0 data.dstuser: root(uid=0) rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2, CC7.3 rule.description: PAM: Login session opened. rule.groups: pam, syslog, authentication_success
```

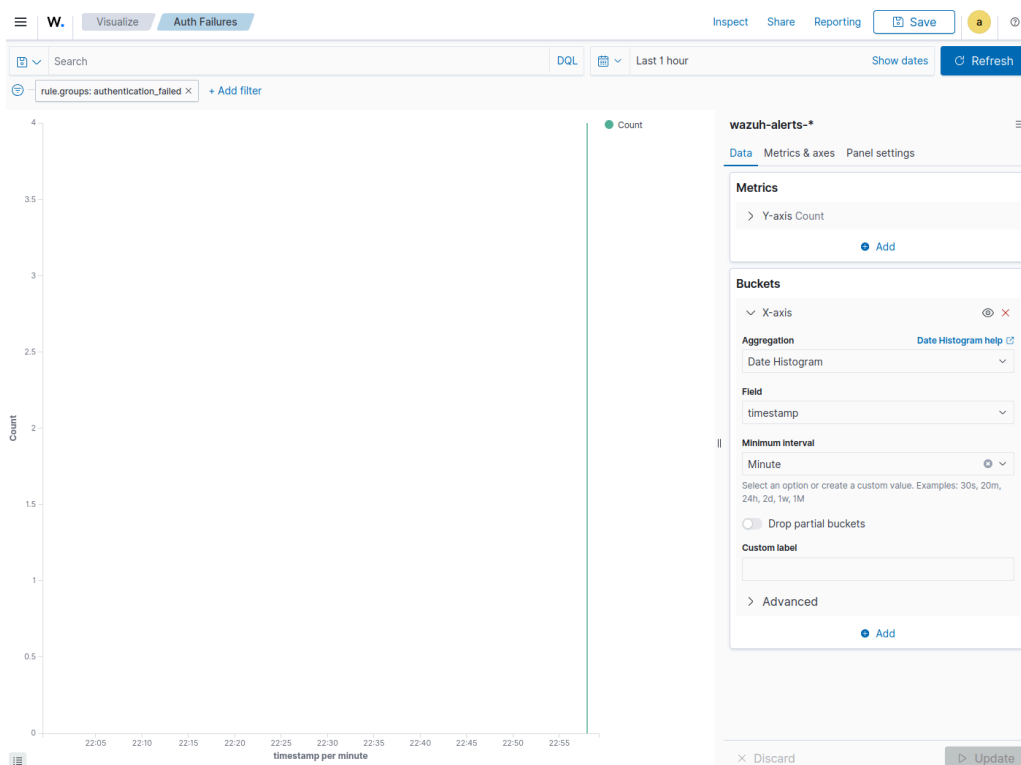
[Nov 30, 2024 @ 10:15](#) [+](#) [-](#)

```
predecoder.hostname: juno-laptop predecoder.program_name: sudo predecoder.timestamp: Nov 30 15:15:00 input.type: log agent.ip: 127.0.0.1 agent.name: juno-laptop agent.id: 001 manager.name: wazuh.manager data.srcuser: juno data.uid: 1000 data.dstuser: root(uid=0) rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2, CC7.3 rule.description: PAM: Login session opened. rule.groups: pam, syslog, authentication_success
```

### Question 3:



### Question 4:



## Question 5:

W. Visualize Auth Successes By User

Inspect Share Reporting Save a

Search DQL Last 1 hour Show dates Refresh

rule.groups: authentication\_success X + Add filter

User	Count
juno	1

wazuh-alerts-\*

Data Options

Metrics

> Metric Count

Add

Buckets

Split rows

Aggregation Terms help

Field data.srcuser

Order by Metric: Count

Order Descending Size 10

☐ Group other values in separate bucket

☐ Show missing values

Custom label User

> Advanced

Add

< 1 > Discard Update

## Question 6:

W. Visualize Failed Auth Attempts By User

Inspect Share Reporting Save a

Search DQL Last 1 hour Show dates Refresh

rule.groups: authentication\_failed X + Add filter

User	Failed Login Attempts
juno	2

wazuh-alerts-\*

Data Options

Aggregation Count help

Custom label Failed Login Attempts

Add

Buckets

Split rows

Aggregation Terms help

Field data.srcuser

Order by Metric: Failed Login Attempts

Order Descending Size 10

☐ Group other values in separate bucket

☐ Show missing values

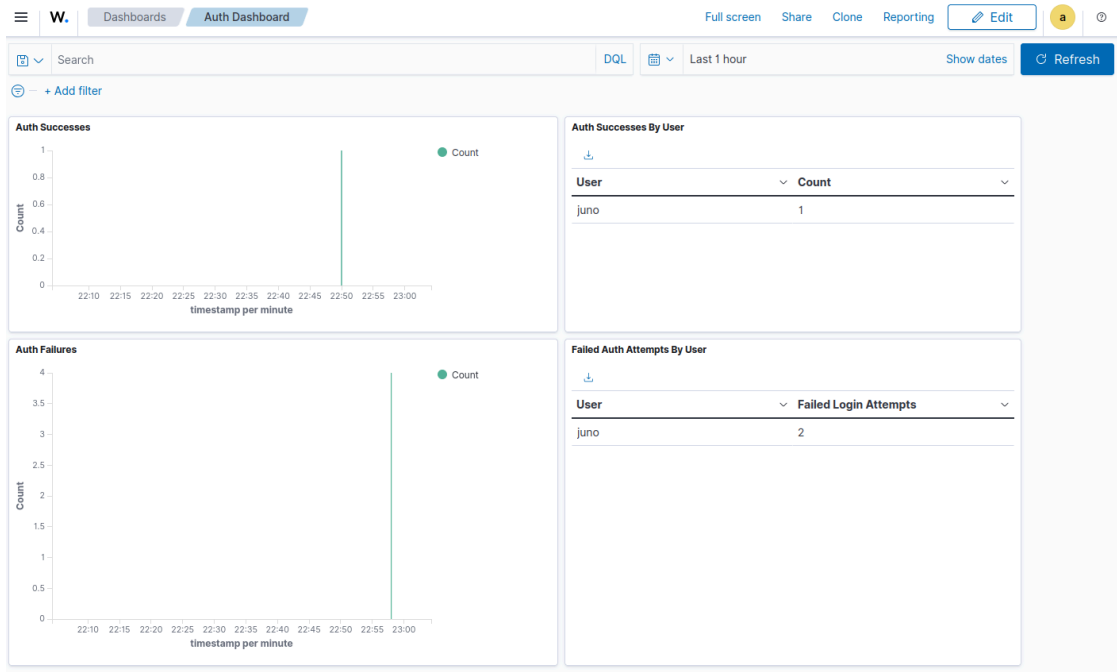
Custom label User

> Advanced

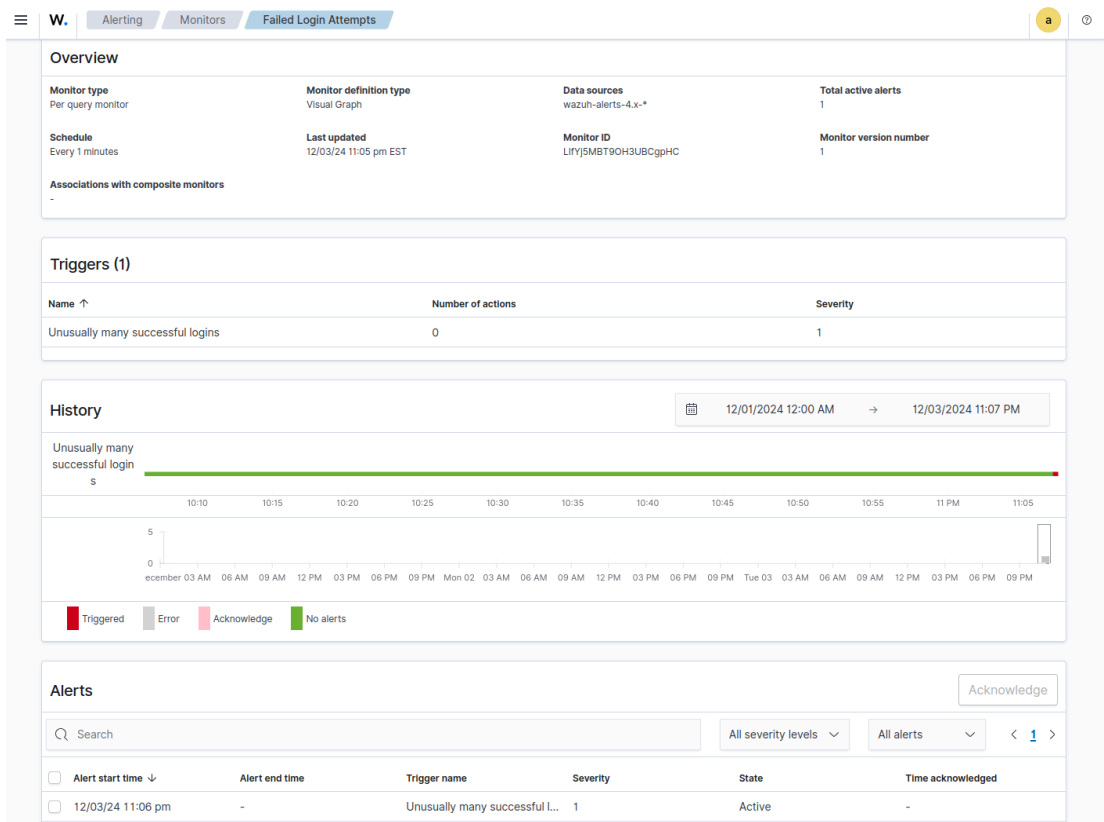
Add

< 1 > Discard Update

Question 7:



Question 8:



## **Reflection Questions:**

### **Question 1:**

Responses should name an event generated while the computer is running. There is enough variety that most should include some bit of info that they haven't thought of. False positive can be a yes/no (maybe a login attempt flagged as suspicious or the like).

### **Question 2:**

Responses should describe a feature in the visualizations tool (ie a different type of graph/chart/etc) and another potential use case (ie creating a graph of users on a system using the most resources, etc)

### **Question 3:**

Responses should describe a common computer security threat (ie remote logins, suspicious processes running, users being given admin privileges, etc) and how the SIEM software responds to it (ie alerting in response). The second half of the question depends on if the writer intends to pursue a career in computer security (could be something like "Yes, I want to manage critical systems at an engineering firm and SIEM software could help monitor and keep them secure."