charliemac Exabeam
06-03-2025

LogRhythm UEBA Control Center | Grafana Dashboard

TLDR; It's a UEBA dashboard. Grafana JSON below, you need SQL & ES Datasources and to potentially open a port. Screenshots etc below.

As you are likely aware there has been some huge cyber attacks in the UK of the past couple of months, this highlights the need for some additional UEBA capacity within the SIEM. Alarms are critical, but as we have seen sometimes it's not that simple, we have to baseline behaviours and have more complex aggregate calculations for these to really highlight anomalies. This post gives you a means to do that via a dashboard like the below;

As part of the subscription services team it's common that we have to build custom Grafana dashboards and integrations to elevate/customize reporting within the product. Please see below an example of this that I wanted to share with the community - If this is something you are interested in having assistance with then I would encourage you to reach out to us and consider our subscription services offering, please see following links;

Want to learn more about our services? - **SAM+Unlimited Upgrades** | **Analytic Co-Pilot** | **TAM**

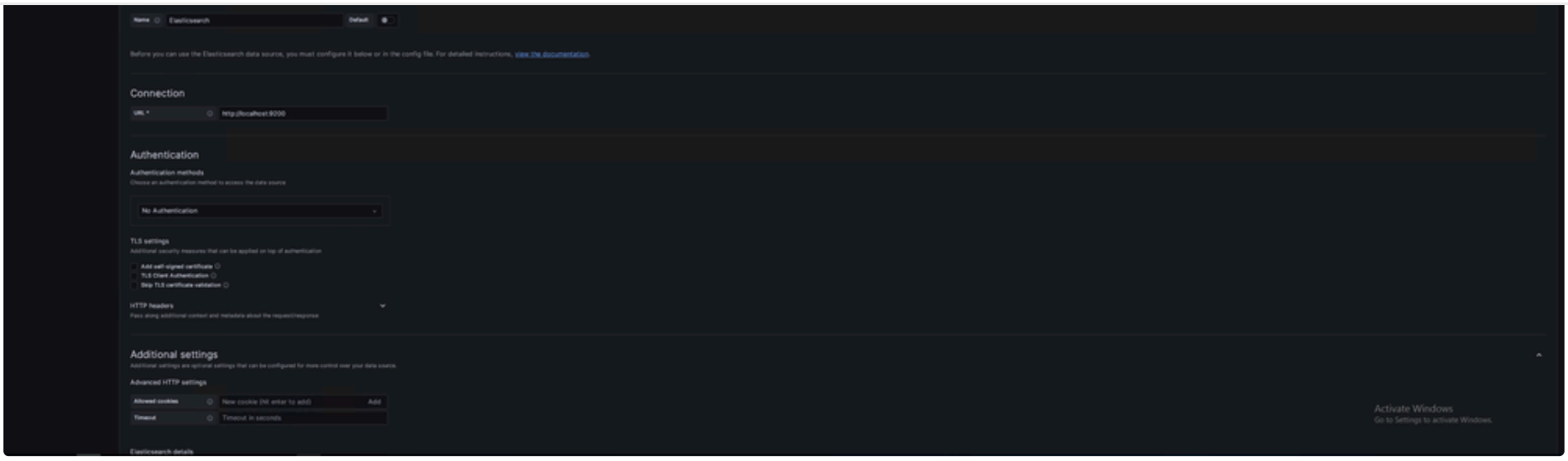
Purpose: We need a high level aggregated view of all the data in the SIEM, to aid in threat hunting. The dashboard makes it easy to pick out suspicious activity, see which regions, processes and activities have been flagged as high risk. etc. This allows you to search back further in time than the web console, it lets you have widgets that are both SQL/Events and DX/Live Data and it lets you group by risk score across any meta data field.

- In quick succession, M&S, Co-Op, and now Harrods have suffered major cyber incidents.
- M&S is still recovering, suggesting a full rebuild instead of paying ransom. With ransomware events now triggering legal and regulatory scrutiny, keeping such incidents quiet is increasingly impossible — leading to broader fallout from media, class actions, and regulators. Once it’s visible, paying ransom is not an option – but as we can see from the press, rebuild is very costly time consuming and painful.
- The group behind these attacks is Scattered Spider, an English-speaking, financially motivated crew known for cloud-native intrusion, social engineering, and endpoint-evasive methods. Microsoft labelled them “one of the most dangerous financial cybercriminal groups”.
- Scattered Spider first emerged in 2022 and was 2023’s most queried threat group, indicating they’ve been active for longer than publicly reported — and many incidents may have gone unobserved due to their stealth and the limitations of traditional security tooling.

Setup Summary: To get this up and running you will need to configure the following things. They are all fairly straightforward and will require standard administrators details like the SA password for SQL, admin rights on the XM/PM server so you can edit some configuration files and general remote access etc. If you are running a standalon

- You will need to configure two required data sources, to be able to monitor/query/alert correctly;

ElasticSearch Data Source (Steps below).



You will likely need to open a hole on the host firewall of the DX, if you are running a standalone DX cluster e.g. not an XM all in once box. It would have to be done on the specific node you're going to connect tom you can use any node for this.

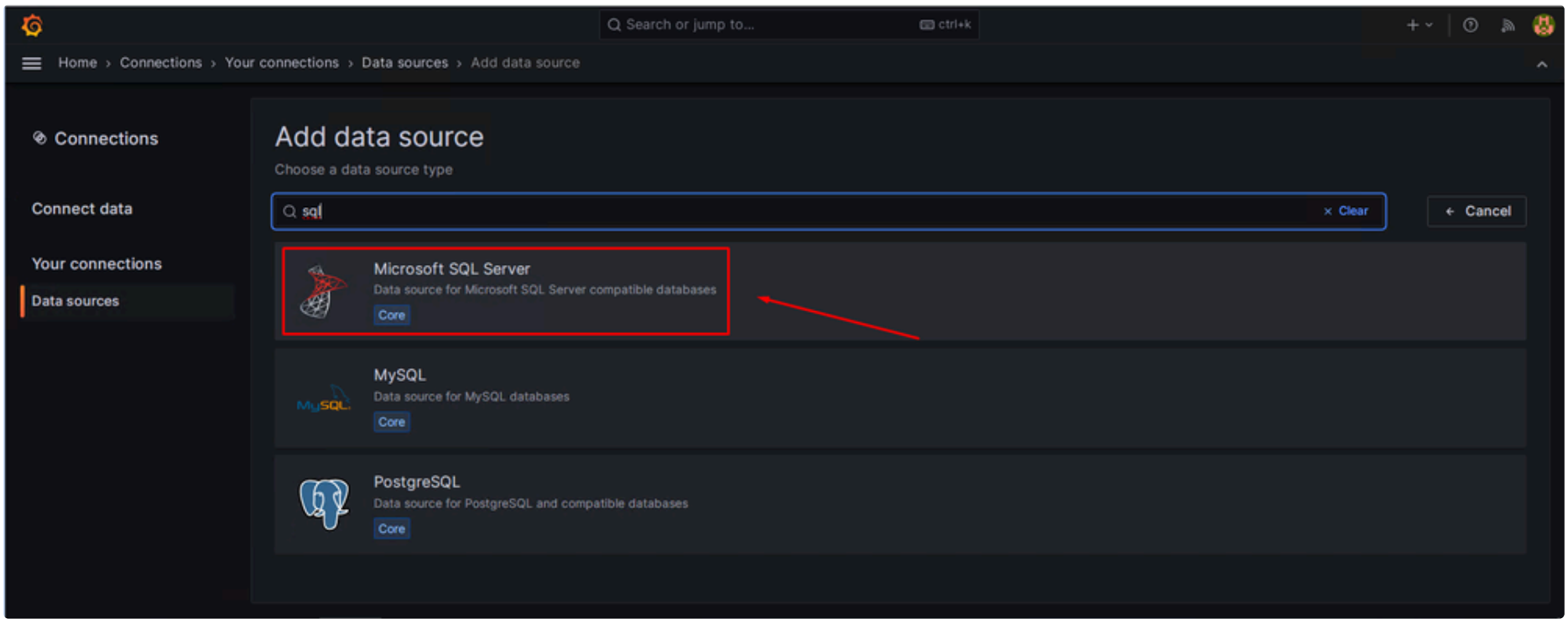
sudo firewall-cmd --zone=public --permanent --add-rich-rule='rule family="ipv4" port port="9200" protocol="tcp" source address="<replace_this_with_Grafana_IP>/32" accept'
sudo firewall-cmd --reload

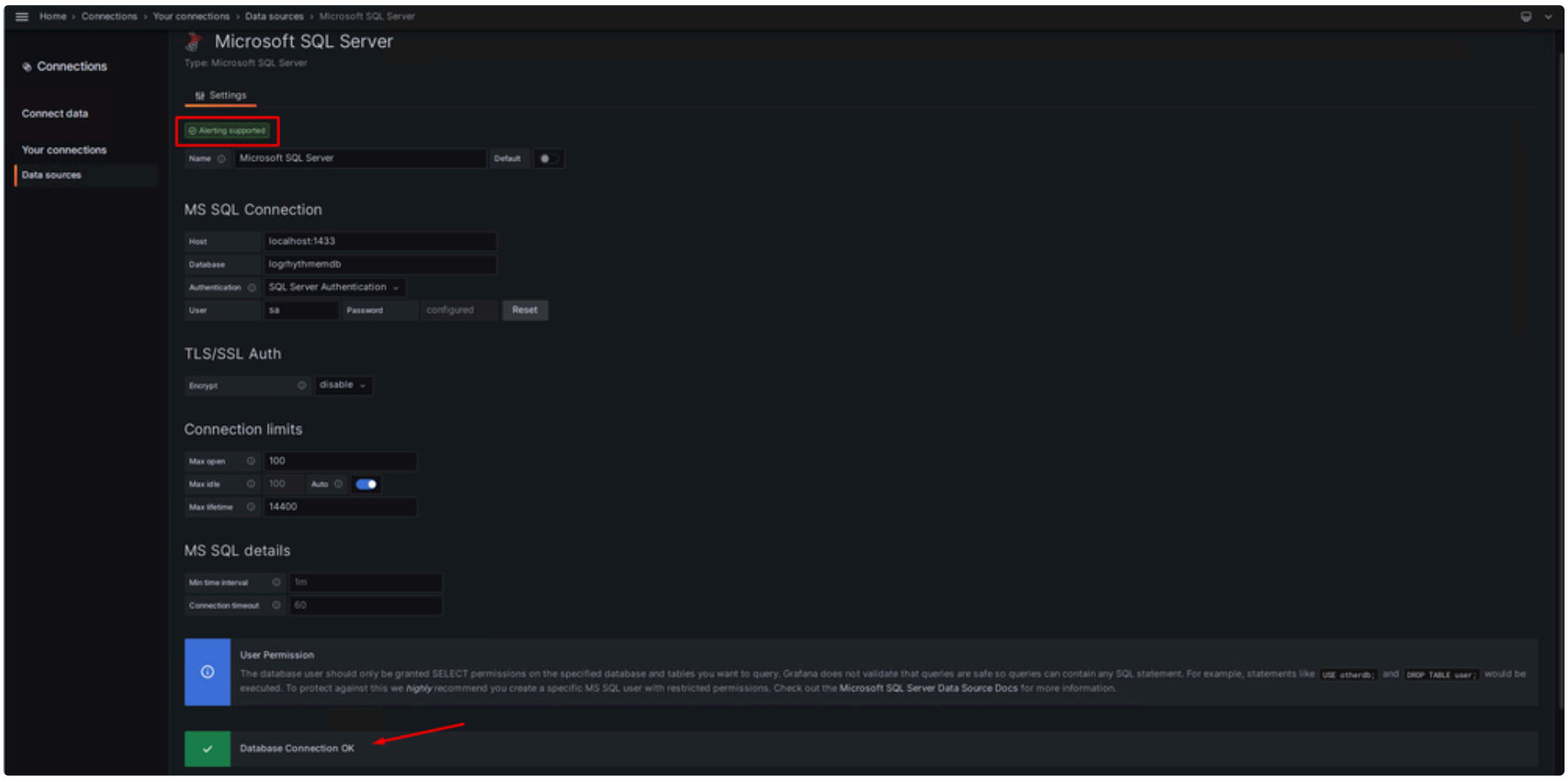
Verify if it has been added & loaded successfully.
sudo firewall-cmd --zone=public --list-rich-rules

After adding this, you can try a browser on the Grafana box & query the cluster health, if the connection works you should see the usual cluster health output:

http://x.x.x.x:9200/_cluster/health?pretty

SQL Data Source (Steps Below)





If you have any questions on how to set this up or around Grafana in general please do not hesitate to reach out.

Your Friendly Neighbourhood TAM,
Charlie MacArthur

UEBAGrafanaDashboard-CharlieMac.json
114 KB

+ TAG

1 Reply