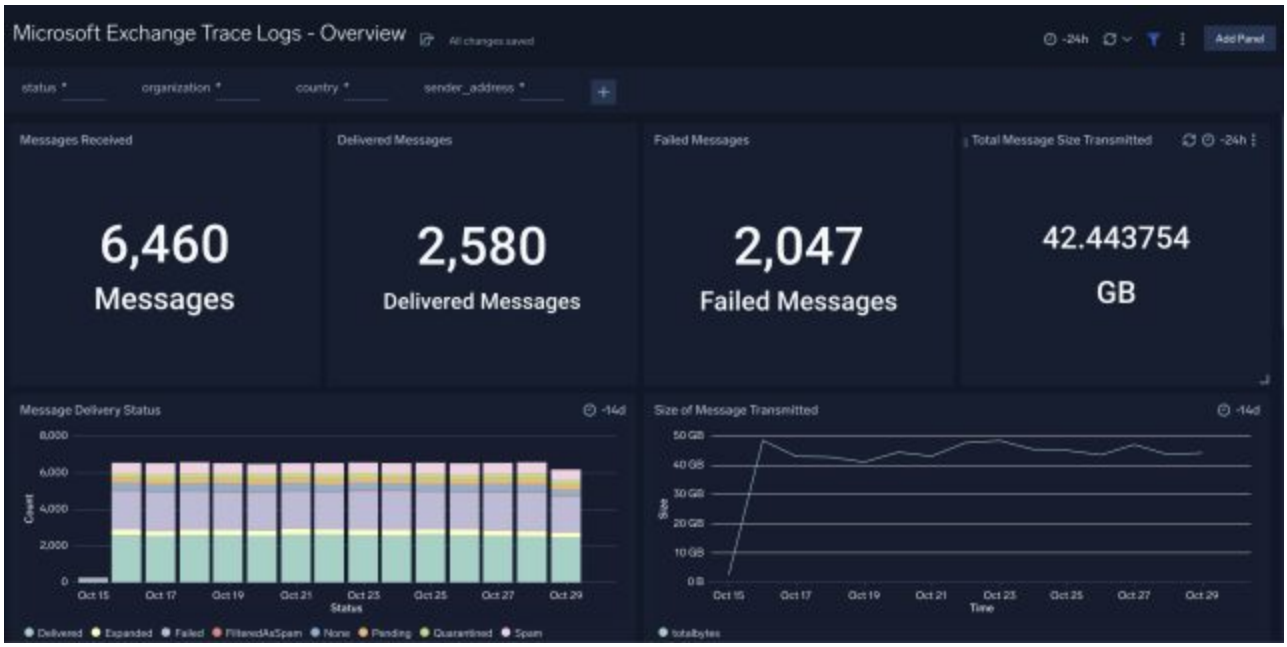
Analyzing Exchange Online Message Tracking Logs with Sumo Logic

dev.classmethod.jp/articles/exchange-online-sumo-logic-log-analysis

酒井剛

October 29, 2023



Many companies use Microsoft 365 as their office groupware, and in those cases, they probably use Exchange Online to send and receive emails on a daily basis.

The fundamental principle of email is that it can be freely sent to and received by anyone you want, and its flexibility has made email an indispensable medium for business and it is used daily.Due
to these characteristics, email is often used as a delivery route for cybersecurity attacks, making it a security measure that must be protected with a high priority.

Exchange Online has a feature called "Message Trace" that records email delivery history (logs) and allows you to search them in the Exchange Admin Center .

So what do you do with these "message tracking logs"? Have you ever thrown them away without analyzing them and letting them expire in Microsoft 365?

In such cases, you can analyze logs by importing them into a SIEM product to improve security.
Let's take a look at how this can be done with Sumo Logic, a SIEM product.

Collecting logs

Sumo Logic is a cloud-native SaaS product, and as such, it can collect logs from major SaaS services very easily and with minimal configuration by utilizing a Cloud-to-Cloud API integration method.

As described in the official documentation, all you need to do is register an application in the Azure portal and grant API execution permissions.
In Sumo Logic, you can start collecting logs by creating a source and registering the ID information and API secret you set on the Azure side.

Installing apps

Sumo Logic provides an app called "out-of-the-box" that provides ready-made dashboards that do not require any customization. There is an app called
Microsoft Exchange Trace Logs , so we will install this.

The app can be set up with just one click, just by setting the source category.

Let's analyze

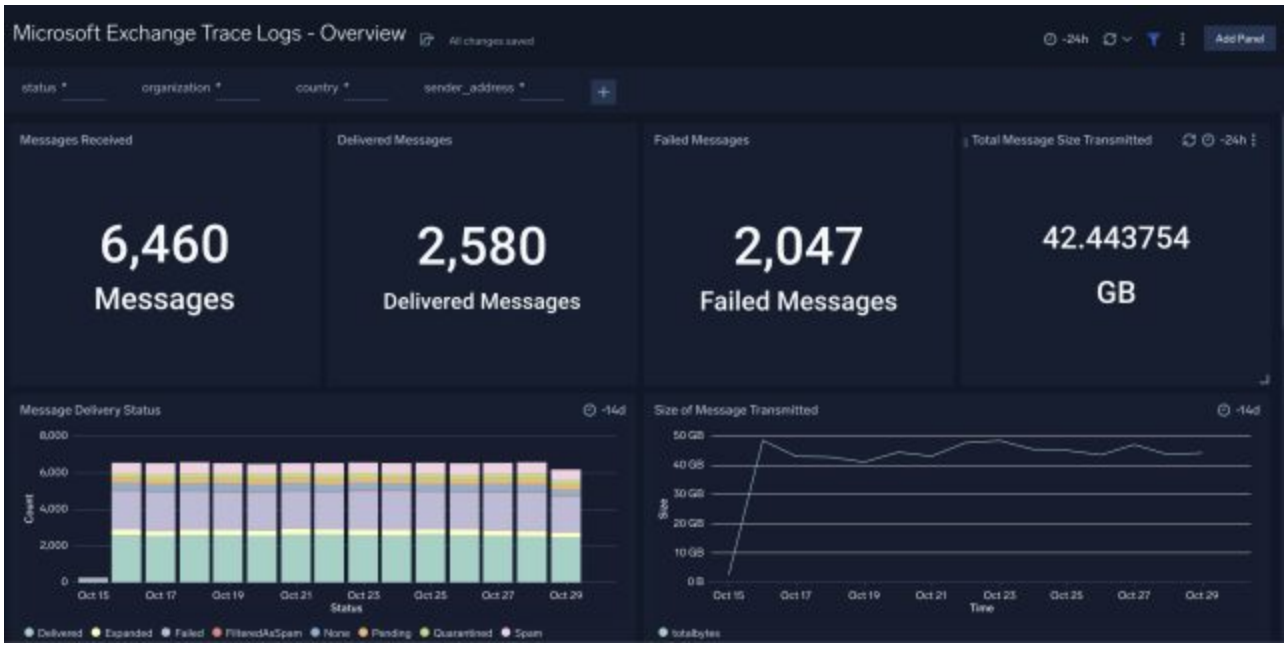
Here is a brief summary of the points to consider when analyzing email logs.

- Is there a sudden increase in emails identified as spam or phishing?
- Is the sender's domain or IP address outside of Japan?
- Are you receiving a large number of messages with similar titles?
- Are there any large messages with attachments, or are they occurring repeatedly?
- Are there any suspicious user email activities detected by other security products (such as endpoint security)?

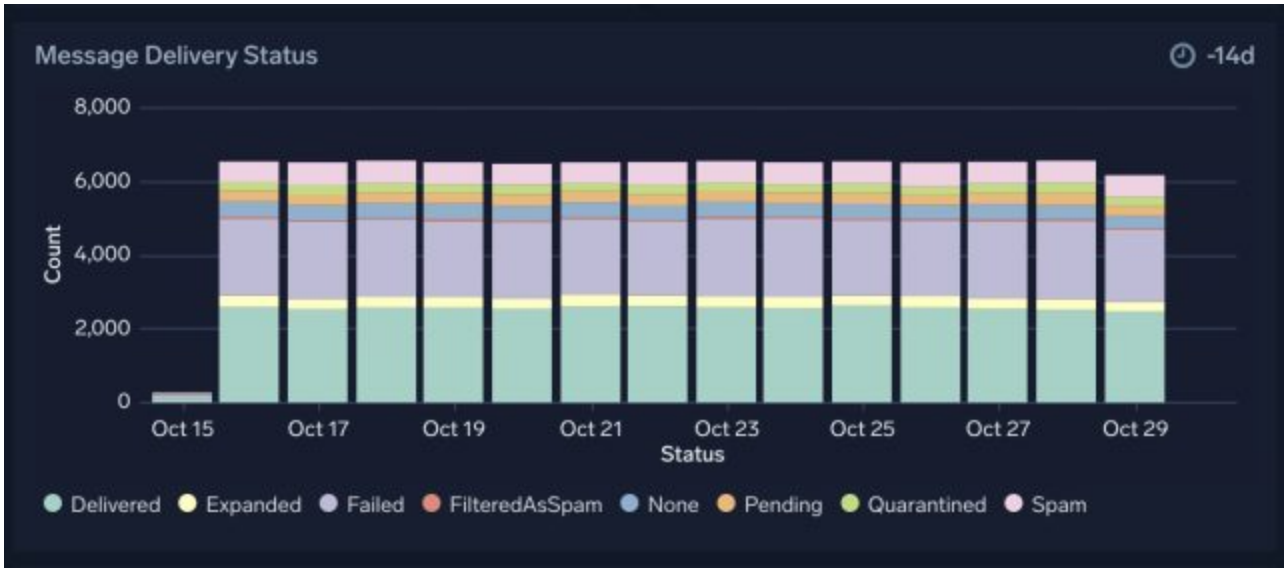
Now let's take a look at the app and analyze it.

Microsoft Exchange Trace Logs - Overview Dashboard

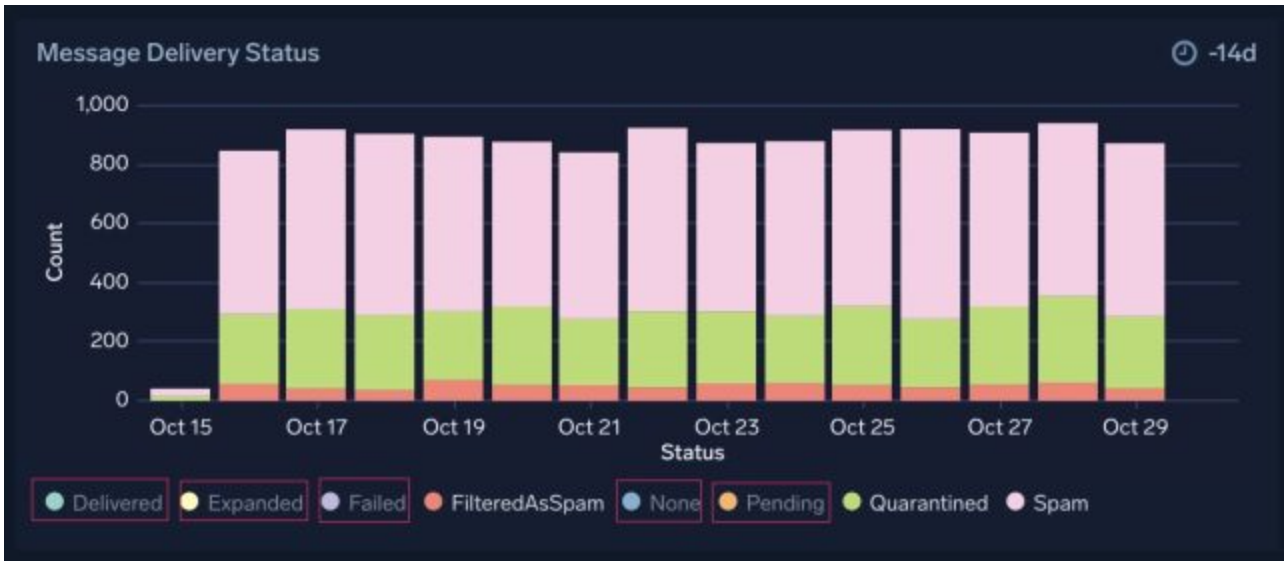
Let's take a look at the "Microsoft Exchange Trace Logs - Overview" dashboard.



By visualizing the delivery status of messages on a daily basis, you can analyze the increase or decrease in the number of emails with certain statuses.
Important statuses to look out for include sudden increases in "Quarantined," "FilteredAsSpam," and "Spam."

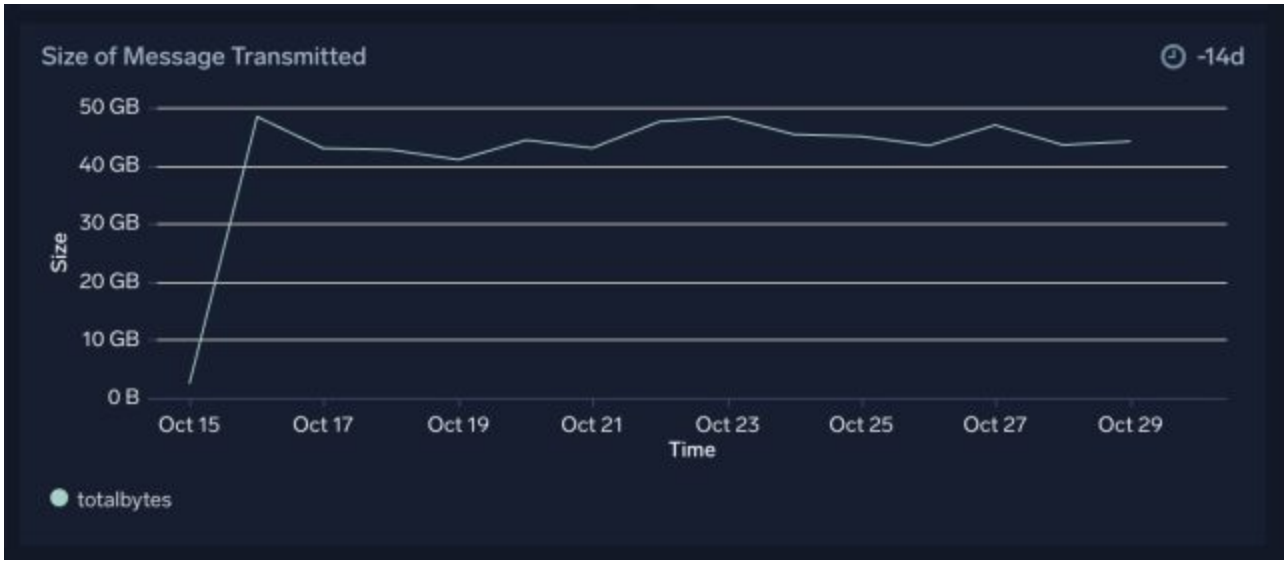


If you can discern a trend and want to see any increases or decreases more clearly, you can narrow down your analysis to a specific status by holding down Shift on your keyboard and selecting the red-framed area in the image below.

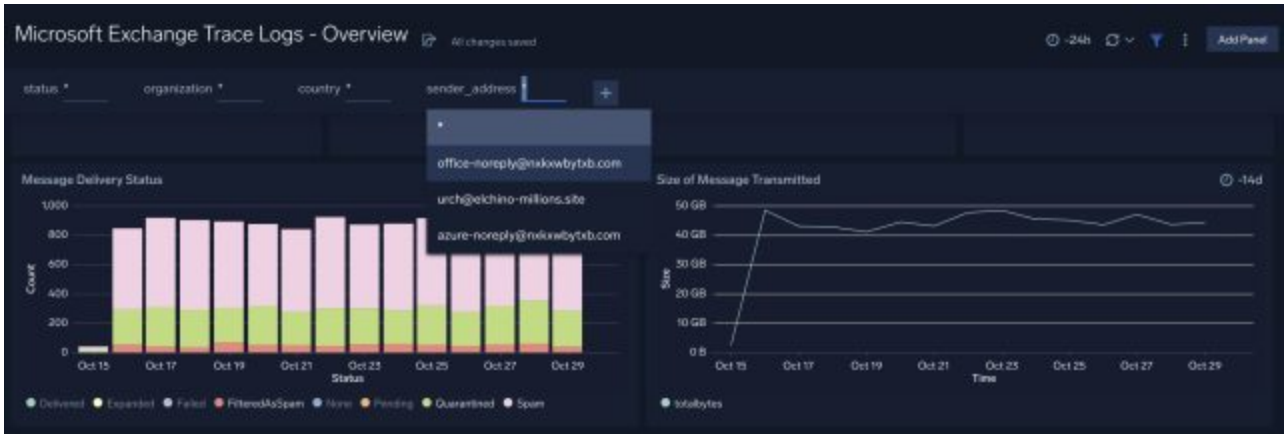


By visualizing the statistics of message sending data size, you can see the daily data sending trends.

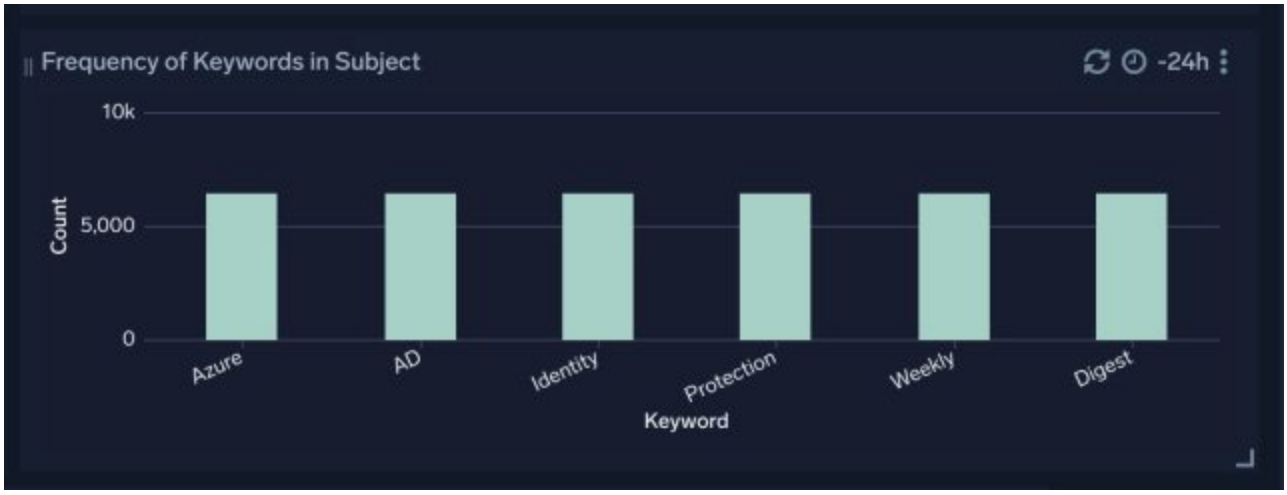
You can check if there are any particularly large days or if a specific sender is sending a lot of data.



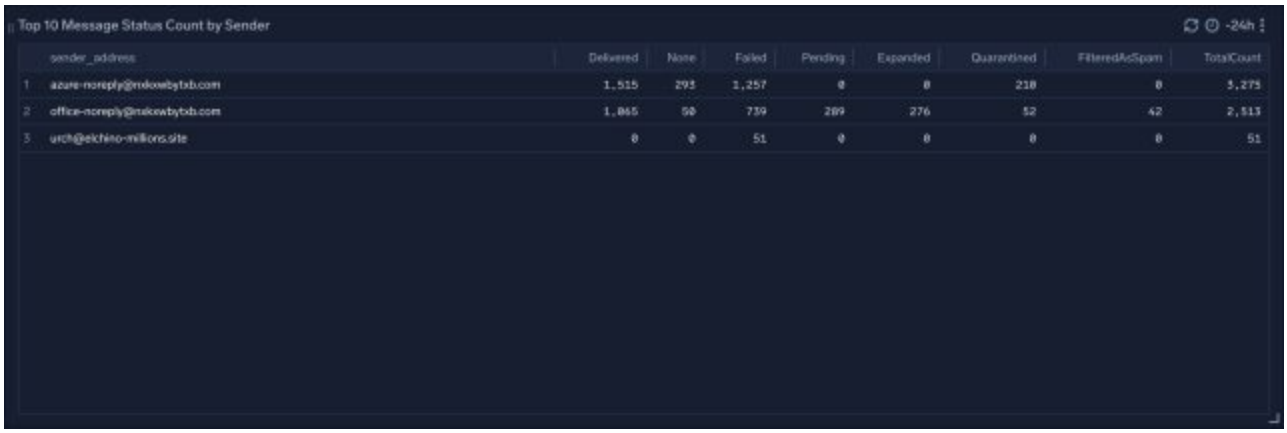
If you want to narrow down the data to a specific sender, use the filter function to perform the analysis.



By visualizing frequently used keywords in email titles, you can check whether large-scale campaign emails such as Emotet are being sent.

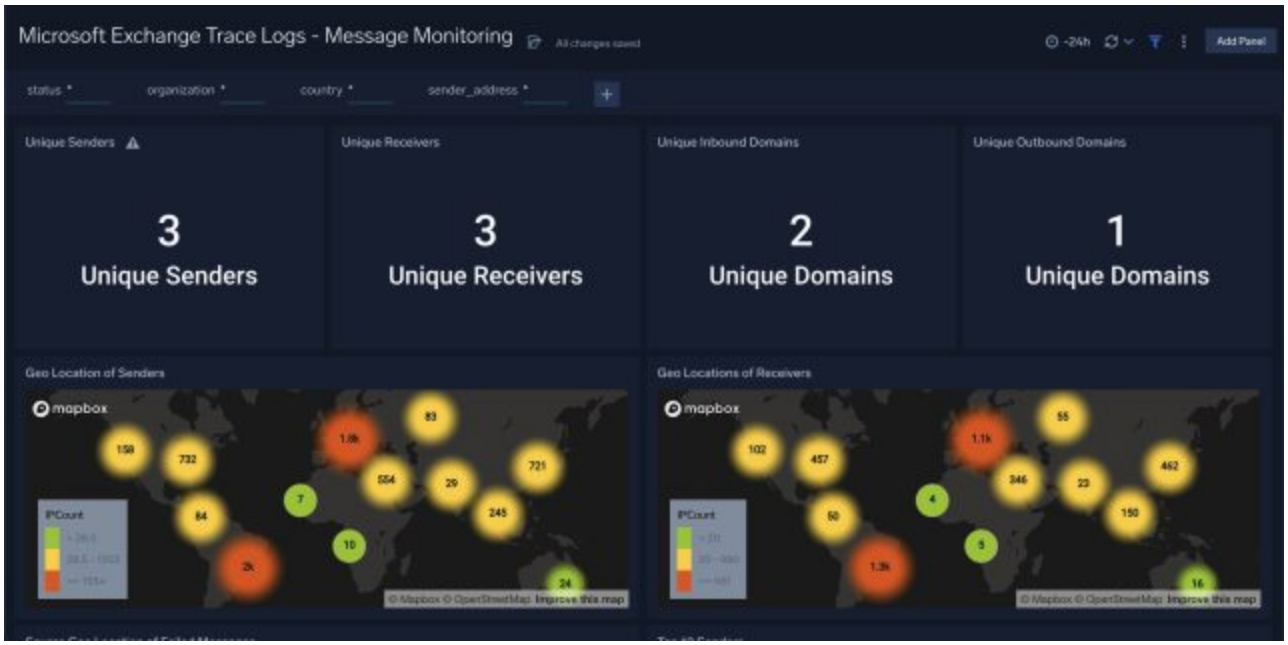


This visualizes statistics on email delivery status by sender.
You can analyze various things, such as whether there are any infected accounts that are acting as stepping stones, or understand trends as a summary.

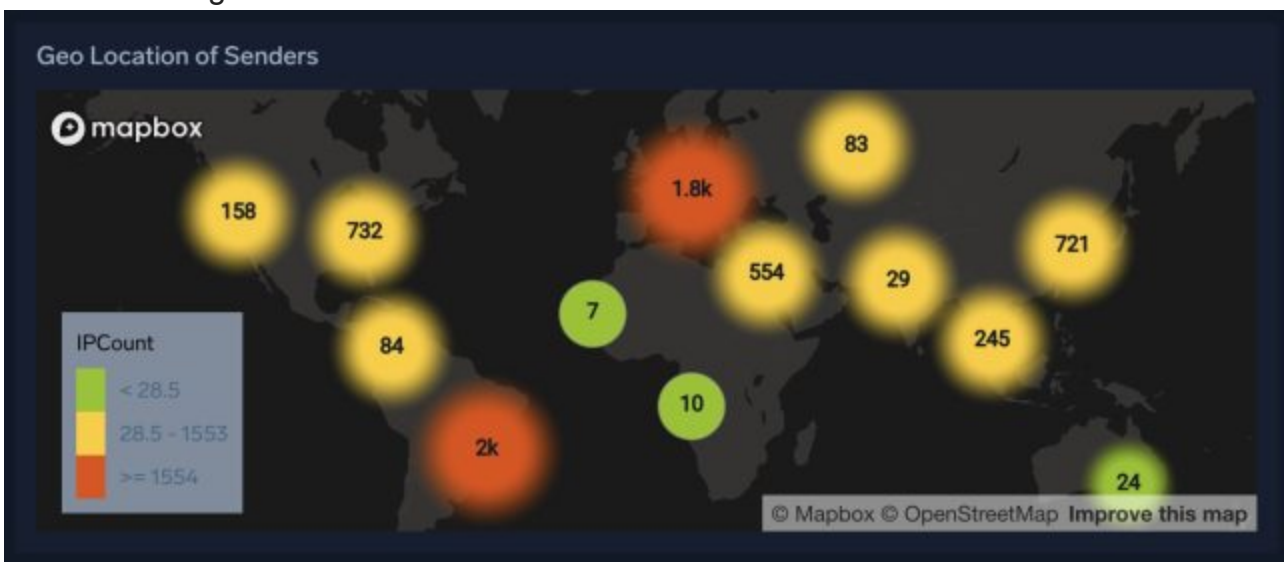


Microsoft Exchange Trace Logs - Message Monitoring Dashboard

Let's take a look at the "Microsoft Exchange Trace Logs - Message Monitoring" dashboard.



This allows you to visualize the country from which the IP address of an email message is coming. This
can be used to analyze messages sent from overseas, or to analyze whether an email account is being used overseas.

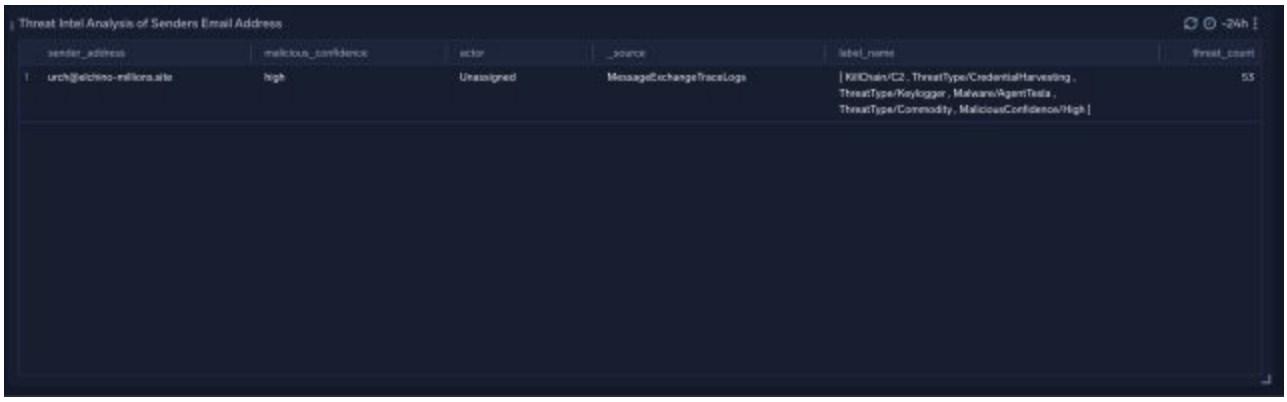


This visualizes the destination IP address of email messages and the country they are sent to. This
allows you to analyze whether emails are being sent overseas unintentionally, or whether

email accounts are being used overseas.

These panels can identify the sender address for further analysis.

Sender addresses can be analyzed to see if there is any data that matches CrowdStrike threat intelligence.



We recommend setting an alert on this query and investigating further if there is any output.

summary

Email is a security tool with a very high potential as an attack vector.
This time, we introduced how to analyze Exchange Online logs, but the analysis perspective is similar even for other email solutions.
We recommend actively importing email logs into a SIEM for analysis, so that you don't just acquire and store them without analyzing them.