

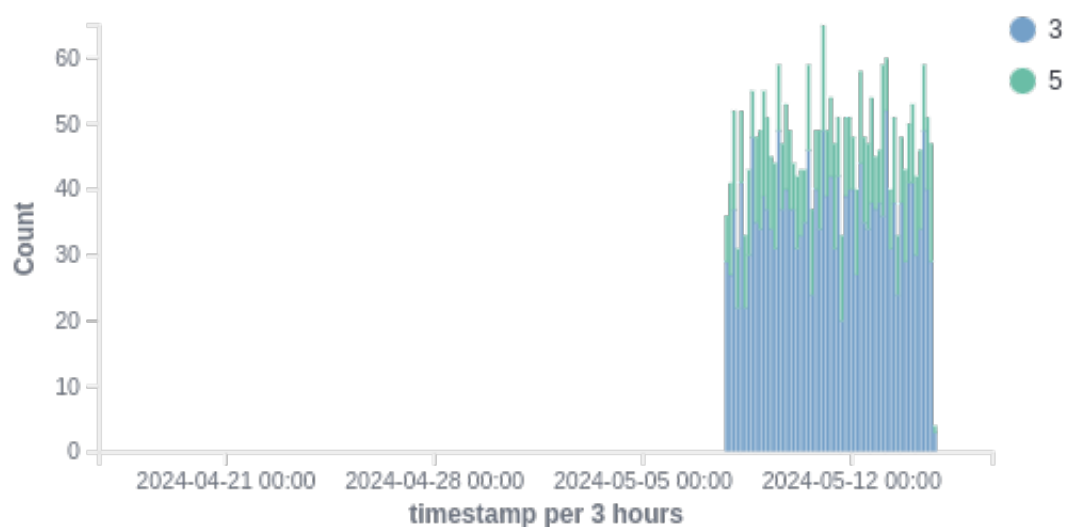
## Office 365 report

Security events related to your Office 365 services.

🕒 2024-04-16T17:52:09 to 2024-05-16T17:52:09

🔍 rule.groups: office365 AND cluster.name: wazuh

### Events by severity over time



### Geolocation map



5

- Max Rule Level -

0

- Suspicious Downloads -

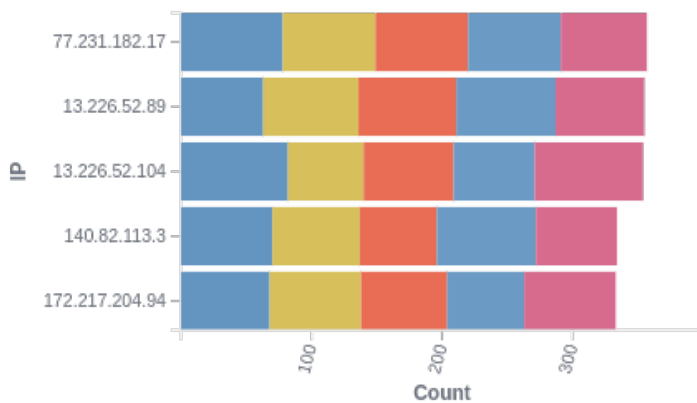
0

- Full Access Permissions -

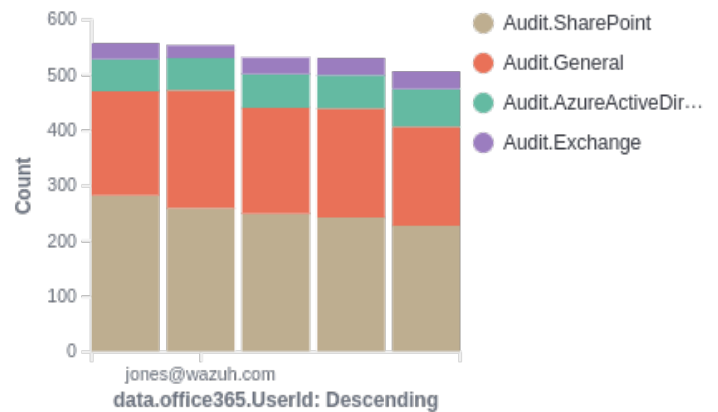
0

- Phishing and Malware -

## IP address by Users



## Top Users By Subscription

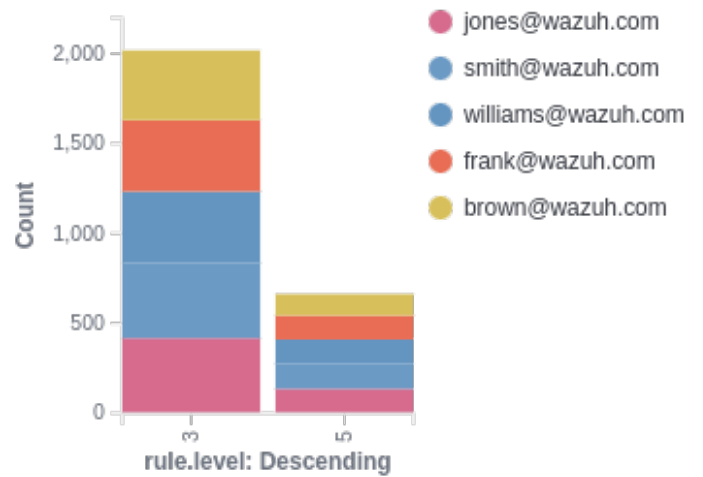


## Users by Operation Result

Operation	User	Result Status	Count
ClientViewSignaled	brown@wazuh.com	Failed	12
ClientViewSignaled	brown@wazuh.com	Succeeded	11
ClientViewSignaled	brown@wazuh.com	PartiallySucceeded	6
ClientViewSignaled	frank@wazuh.com	Succeeded	9
ClientViewSignaled	frank@wazuh.com	Failed	8

< 1 2 3 4 5 ... 30 >

## Severity by user



## Rule Description by Level

Rule Description	Rule Level	Count
Office 365: Admin actions f	5	663
Office 365: SharePoint eve	3	468
Office 365: SharePoint file	3	404
Office 365: Data Insights R	3	305
Office 365: SharePoint sha	3	240

< 1 2 >

## Alerts summary

Rule ID	Description	Level	Count
91548	Office 365: Admin actions from the Security and Compliance Center.	5	663
91536	Office 365: SharePoint events.	3	468
91537	Office 365: SharePoint file operation events.	3	404
91580	Office 365: Data Insights REST API events.	3	305
91544	Office 365: SharePoint sharing events.	3	240
91539	Office 365: Azure Active Directory events.	3	226
91564	Office 365: SharePoint List events.	3	152
91534	Office 365: Events from an Exchange mailbox audit log for actions that are performed on a single item, such as creating or receiving an email message.	3	145
91545	Office 365: Secure Token Service (STS) logon events in Azure Active Directory.	3	79