

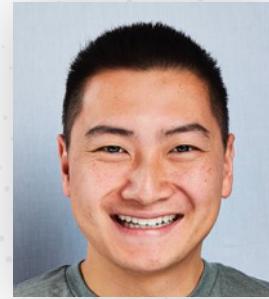


# Securing Microsoft 365 with Elastic

ElasticON Global 2021



# INTRODUCTION



**ERIC OOI**

**Director of Security & Research**  
[eooi@ironvine.com](mailto:eooi@ironvine.com)  
[@ericooi](https://twitter.com/ericooi)

# AGENDA

- Overview
- Why capture Microsoft 365 and Azure logs?
- M365 & Filebeat Setup
- Azure & Filebeat Setup
- Kibana Queries
- Kibana Visuals
- Custom Dashboards



# OVERVIEW

## CLOUD SECURITY IS A SHARED RESPONSIBILITY

Cloud provider → Cloud tenant

# WHY CAPTURE MICROSOFT 365 AND AZURE LOGS?



Security



Compliance



Centralize logs



Investigate alerts



Identify notable activity



Microsoft



Azure

# M365 SETUP



## CONFIGURE M365 LOGGING

1. Enable audit logging  
<https://compliance.microsoft.com>
2. Register Azure AD application
3. Note the following:
  - Application (Client) ID
  - Directory (Tenant) ID
  - Tenant Name
  - Client Secret



# FILEBEAT SETUP

## SET UP FILEBEAT TO CAPTURE LOGS

1. Enable the Filebeat M365 module  
*filebeat modules enable o365*
2. Setup Filebeat M365 assets  
*filebeat setup -e*
3. Edit M365 configuration file  
*/etc/filebeat/modules.d/o365.yml*
4. Restart Filebeat  
*sudo systemctl restart filebeat*

<https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-module-o365.html>



# AZURE SETUP

## CONFIGURE AZURE LOGGING

1. Create Azure Resource Group
2. Create Azure Event Hub
3. Create Blob Storage Account
4. Stream logs to Event Hub
5. Note the following:
  - [Event Hub](#)
  - [Connection String](#)
  - [Storage Account](#)
  - [Storage Account Key](#)



# FILEBEAT SETUP

## SET UP FILEBEAT TO CAPTURE LOGS

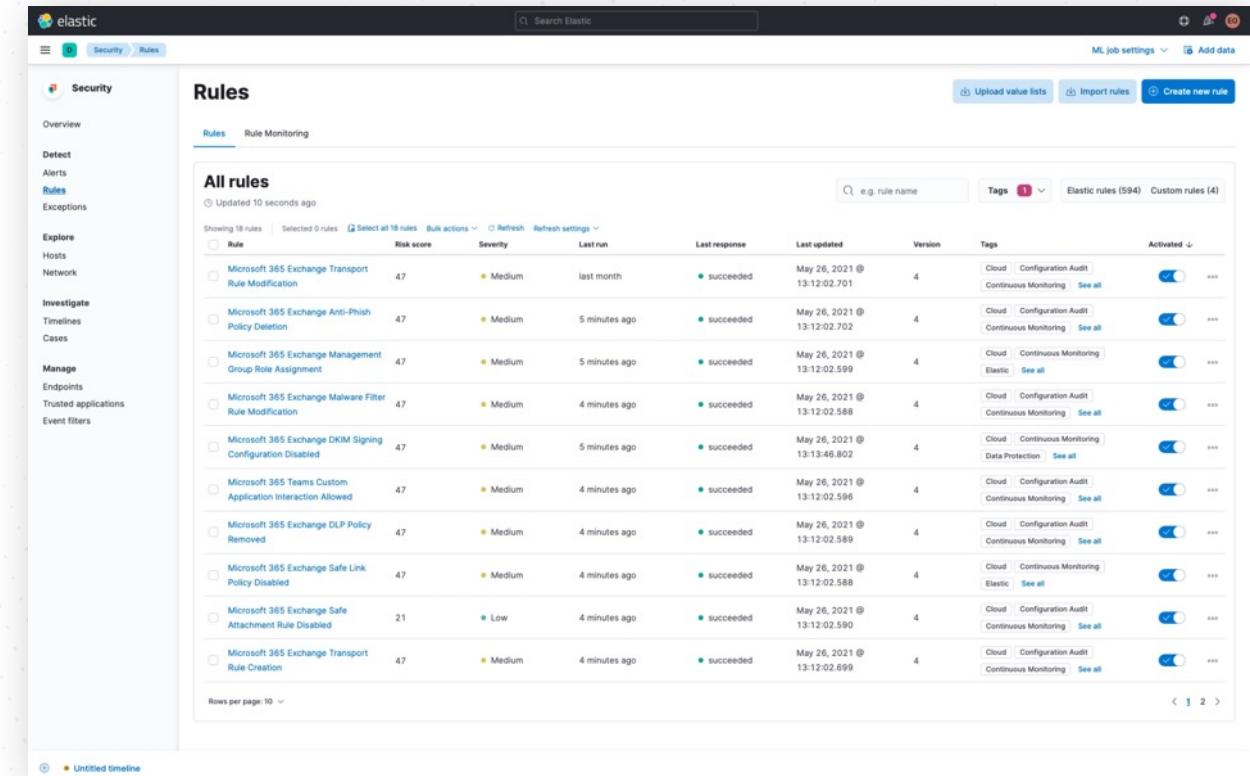
1. Enable the Filebeat Azure module  
*filebeat modules enable azure*
2. Setup Filebeat Azure assets  
*filebeat setup -e*
3. Edit Azure configuration file  
*/etc/filebeat/modules.d/azure.yml*
4. Restart Filebeat  
*sudo systemctl restart filebeat*

<https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-module-azure.html>

# ELASTIC SIEM



## PRE-BUILT MICROSOFT 365 RULES



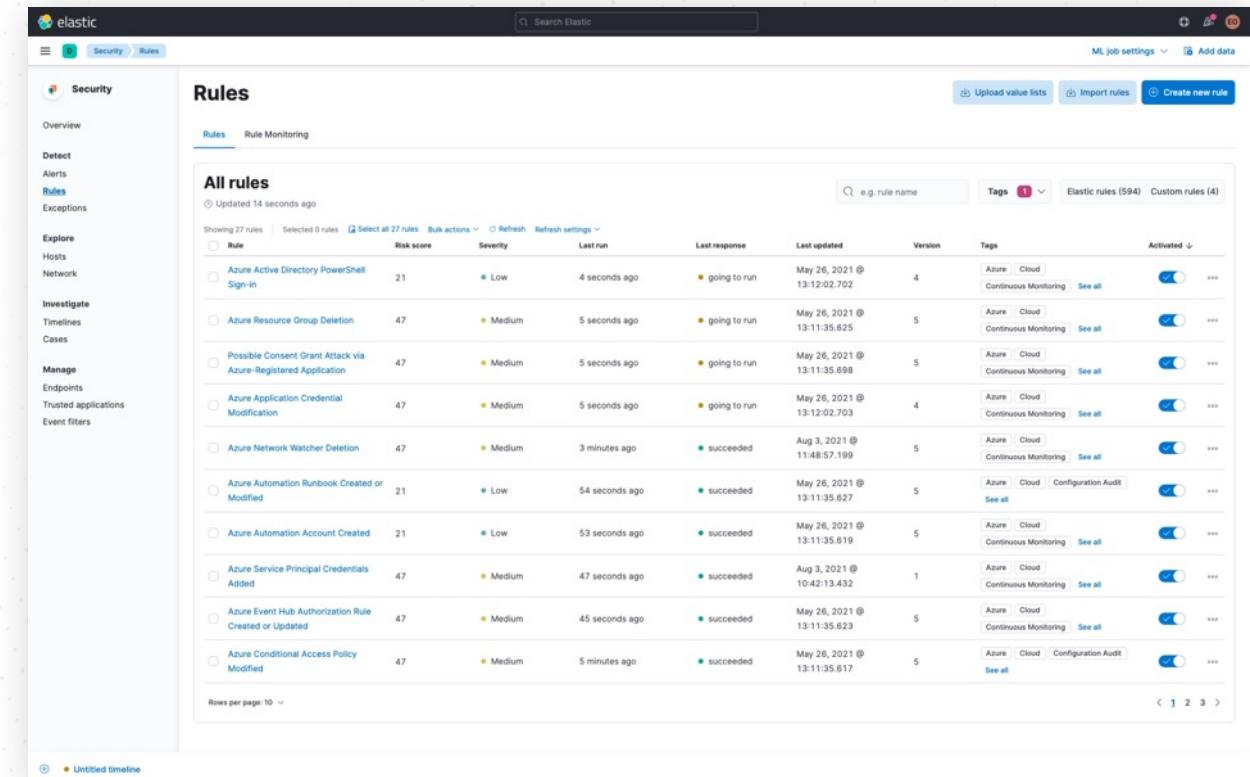
The screenshot shows the Elastic SIEM interface with the "Rules" section selected. The page displays a table of 18 pre-built rules for Microsoft 365, including Exchange Transport, Anti-Phish, Management, and DLP policies. Each rule is listed with its name, risk score (Medium), severity (Medium), last run (within the last month), last response (succeeded), last updated (May 26, 2021), version (4), and tags (Cloud, Configuration Audit, Continuous Monitoring). The "Activated" column shows that all rules are enabled. The interface includes navigation buttons for rows per page (10, 20, 50, 100) and a timeline selector.

Rule	Risk score	Severity	Last run	Last response	Last updated	Version	Tags	Activated
Microsoft 365 Exchange Transport Rule Modification	47	Medium	last month	succeeded	May 26, 2021 @ 13:12:02.701	4	Cloud Configuration Audit Continuous Monitoring See all	<input checked="" type="checkbox"/>
Microsoft 365 Exchange Anti-Phish Policy Deletion	47	Medium	5 minutes ago	succeeded	May 26, 2021 @ 13:12:02.702	4	Cloud Configuration Audit Continuous Monitoring See all	<input checked="" type="checkbox"/>
Microsoft 365 Exchange Management Group Role Assignment	47	Medium	5 minutes ago	succeeded	May 26, 2021 @ 13:12:02.599	4	Cloud Continuous Monitoring Elastic See all	<input checked="" type="checkbox"/>
Microsoft 365 Exchange Malware Filter Rule Modification	47	Medium	4 minutes ago	succeeded	May 26, 2021 @ 13:12:02.588	4	Cloud Configuration Audit Continuous Monitoring See all	<input checked="" type="checkbox"/>
Microsoft 365 Exchange DKIM Signing Configuration Disabled	47	Medium	5 minutes ago	succeeded	May 26, 2021 @ 13:13:46.802	4	Cloud Continuous Monitoring Data Protection See all	<input checked="" type="checkbox"/>
Microsoft 365 Teams Custom Application Interaction Allowed	47	Medium	4 minutes ago	succeeded	May 26, 2021 @ 13:12:02.596	4	Cloud Configuration Audit Continuous Monitoring See all	<input checked="" type="checkbox"/>
Microsoft 365 Exchange DLP Policy Removed	47	Medium	4 minutes ago	succeeded	May 26, 2021 @ 13:12:02.589	4	Cloud Configuration Audit Continuous Monitoring See all	<input checked="" type="checkbox"/>
Microsoft 365 Exchange Safe Link Policy Disabled	47	Medium	4 minutes ago	succeeded	May 26, 2021 @ 13:12:02.588	4	Cloud Continuous Monitoring Elastic See all	<input checked="" type="checkbox"/>
Microsoft 365 Exchange Safe Attachment Rule Disabled	21	Low	4 minutes ago	succeeded	May 26, 2021 @ 13:12:02.590	4	Cloud Configuration Audit Continuous Monitoring See all	<input checked="" type="checkbox"/>
Microsoft 365 Exchange Transport Rule Creation	47	Medium	4 minutes ago	succeeded	May 26, 2021 @ 13:12:02.699	4	Cloud Configuration Audit Continuous Monitoring See all	<input checked="" type="checkbox"/>

# ELASTIC SIEM



## PRE-BUILT AZURE RULES



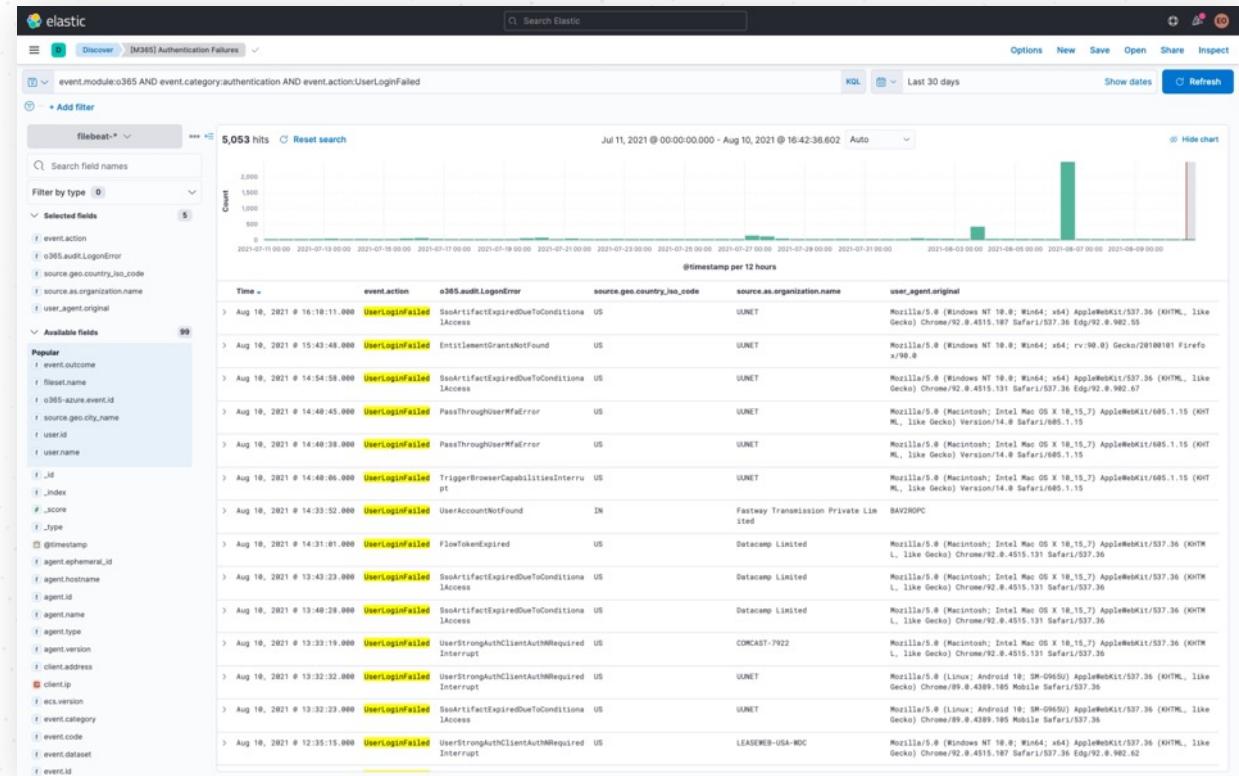
The screenshot shows the Elastic SIEM interface under the 'Security' tab, specifically the 'Rules' section. The left sidebar includes categories like Overview, Detect, Alerts, Rules (which is selected), Exceptions, Explore, and Manage. The main area displays a table titled 'All rules' with 27 entries. Each entry includes details such as the rule name, risk score, severity, last run, last response, last updated, version, tags, and activation status. The table also features filters for rule name, tags, and type (Elastic rules vs. Custom rules). A search bar at the top right allows for searching by rule name or tags.

Rule	Risk score	Severity	Last run	Last response	Last updated	Version	Tags	Activated
Azure Active Directory PowerShell Sign-in	21	Low	4 seconds ago	going to run	May 26, 2021 @ 13:12:02.702	4	Azure Cloud Continuous Monitoring	See all
Azure Resource Group Deletion	47	Medium	5 seconds ago	going to run	May 26, 2021 @ 13:11:35.625	5	Azure Cloud Continuous Monitoring	See all
Possible Consent Grant Attack via Azure-Registered Application	47	Medium	5 seconds ago	going to run	May 26, 2021 @ 13:11:35.698	5	Azure Cloud Continuous Monitoring	See all
Azure Application Credential Modification	47	Medium	5 seconds ago	going to run	May 26, 2021 @ 13:12:02.703	4	Azure Cloud Continuous Monitoring	See all
Azure Network Watcher Deletion	47	Medium	3 minutes ago	succeeded	Aug 3, 2021 @ 11:48:57.199	5	Azure Cloud Continuous Monitoring	See all
Azure Automation Runbook Created or Modified	21	Low	54 seconds ago	succeeded	May 26, 2021 @ 13:11:35.627	5	Azure Cloud Configuration Audit	See all
Azure Automation Account Created	21	Low	53 seconds ago	succeeded	May 26, 2021 @ 13:11:35.619	5	Azure Cloud Continuous Monitoring	See all
Azure Service Principal Credentials Added	47	Medium	47 seconds ago	succeeded	Aug 3, 2021 @ 10:42:13.432	1	Azure Cloud Continuous Monitoring	See all
Azure Event Hub Authorization Rule Created or Updated	47	Medium	45 seconds ago	succeeded	May 26, 2021 @ 13:11:35.623	5	Azure Cloud Continuous Monitoring	See all
Azure Conditional Access Policy Modified	47	Medium	5 minutes ago	succeeded	May 26, 2021 @ 13:11:35.617	5	Azure Cloud Configuration Audit	See all

# KIBANA QUERIES



## AUTHENTICATION FAILURES

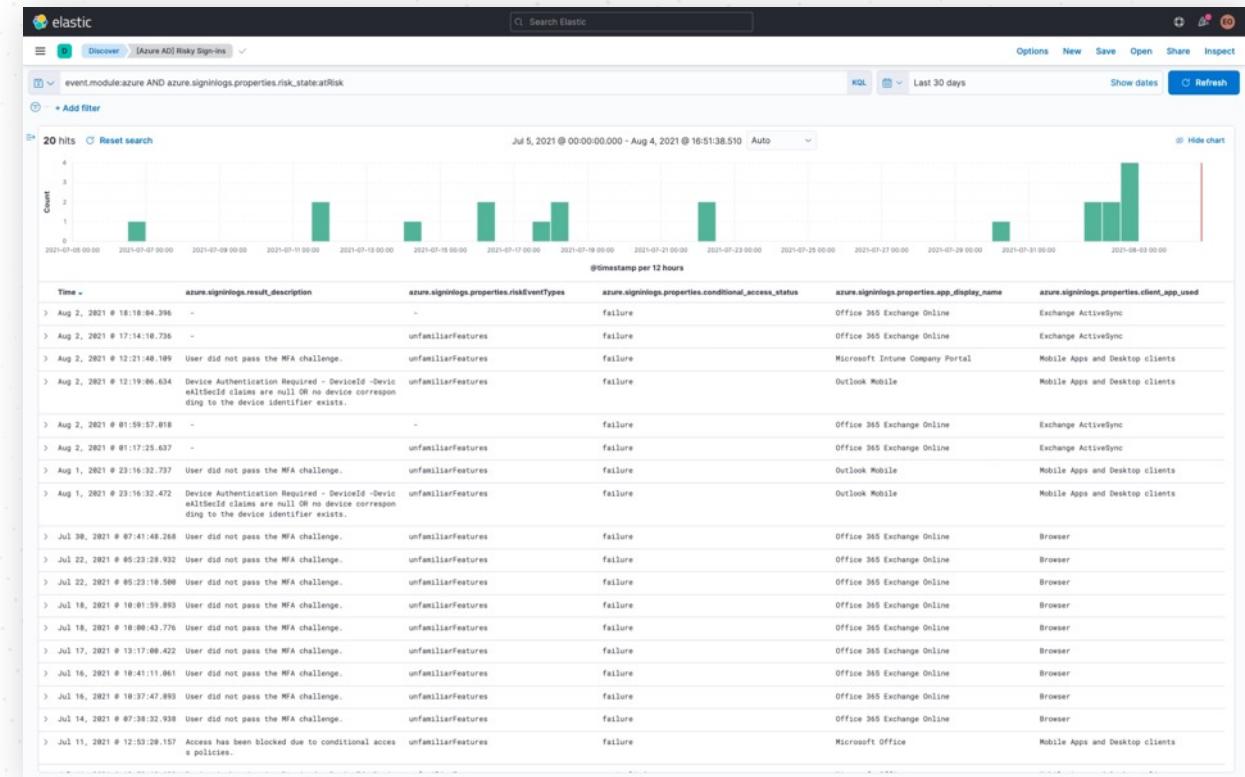


event.module:o365 AND event.category:authentication  
AND event.action:UserLoginFailed

# KIBANA QUERIES



## RISKY SIGN-INS

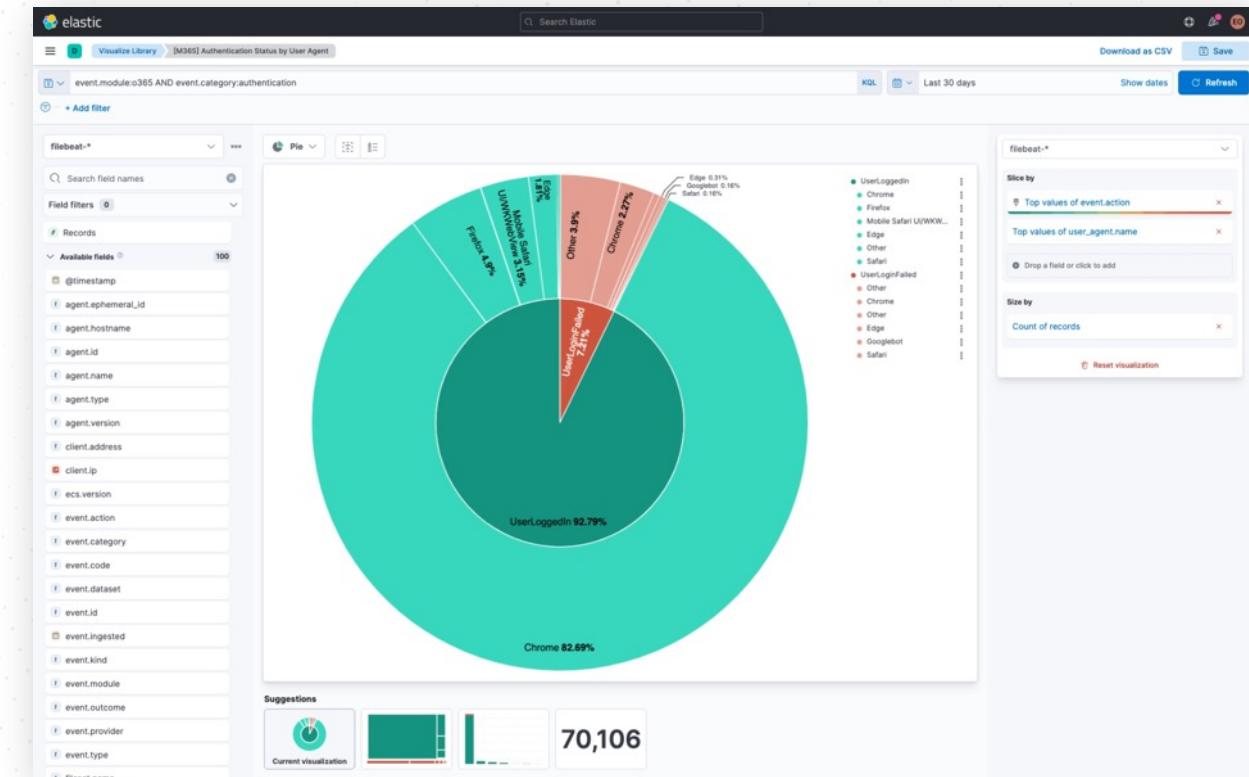


**event.module:azure AND  
azure.signinlogs.properties.risk\_state:atRisk**

# KIBANA VISUALS



## AUTHENTICATION STATUS

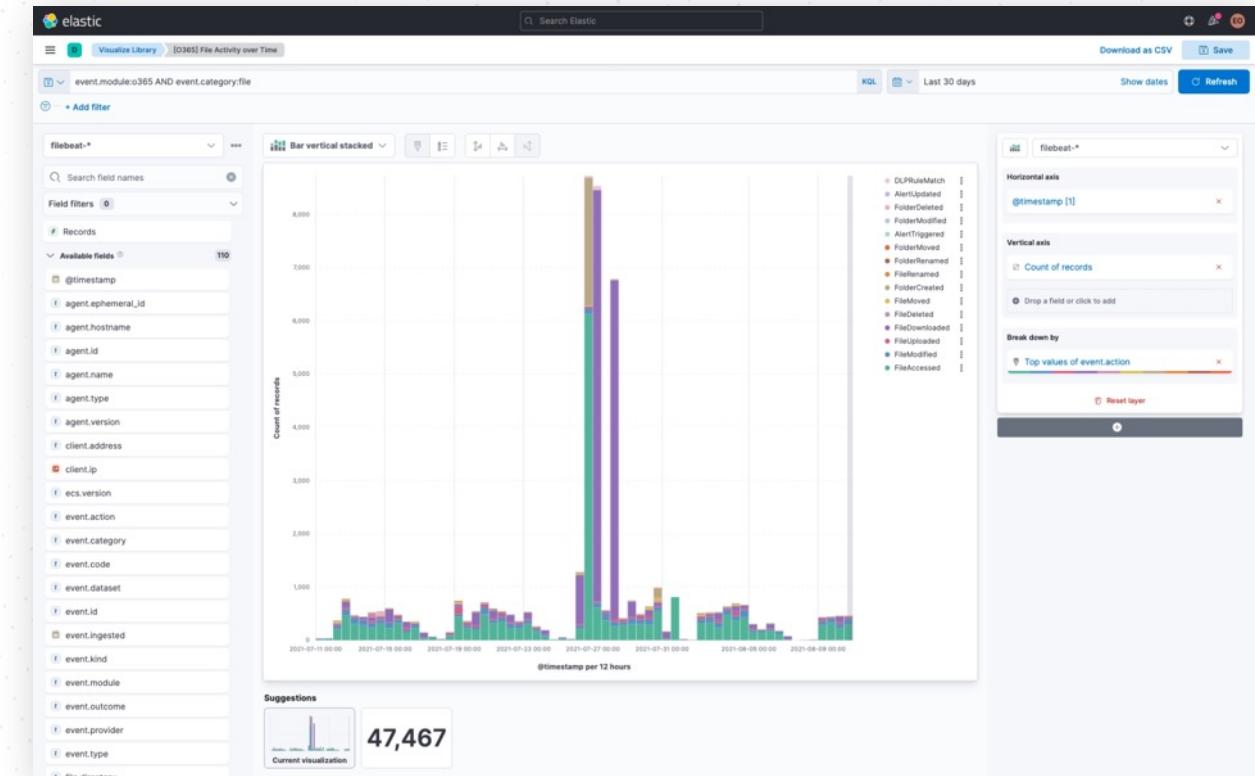


event.module:o365 AND event.category:authentication

# KIBANA VISUALS



## FILE ACTIVITY OVER TIME



event.module:o365 AND event.category:file



# CUSTOM DASHBOARDS

## GOING BEYOND

- Turn repeat queries into saved searches and visualizations
- Use these to build useful dashboards
  - Where in the world are users logging in from?
  - Who invited or added a guest user?
  - What files are users sharing internally and externally and with who?
  - What users does Azure AD consider to be risky and why?
  - Are there suspicious user agents attempting to login?
  - Which users receive the most suspicious mail?

[github.com/ironvine/elastic-m365](https://github.com/ironvine/elastic-m365)



# THANK YOU

[ironvine.com](http://ironvine.com)

@ivsec

[github.com/ironvine](https://github.com/ironvine)