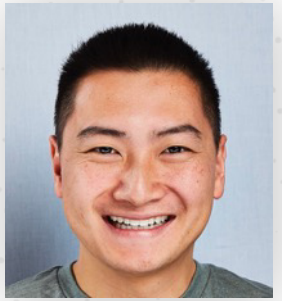
IRON VINE SECURITY

Securing Microsoft 365 with Elastic

ElasticON Global 2021

INTRODUCTION



ERIC OOI

Director of Security & Research

eooi@ironvine.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

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

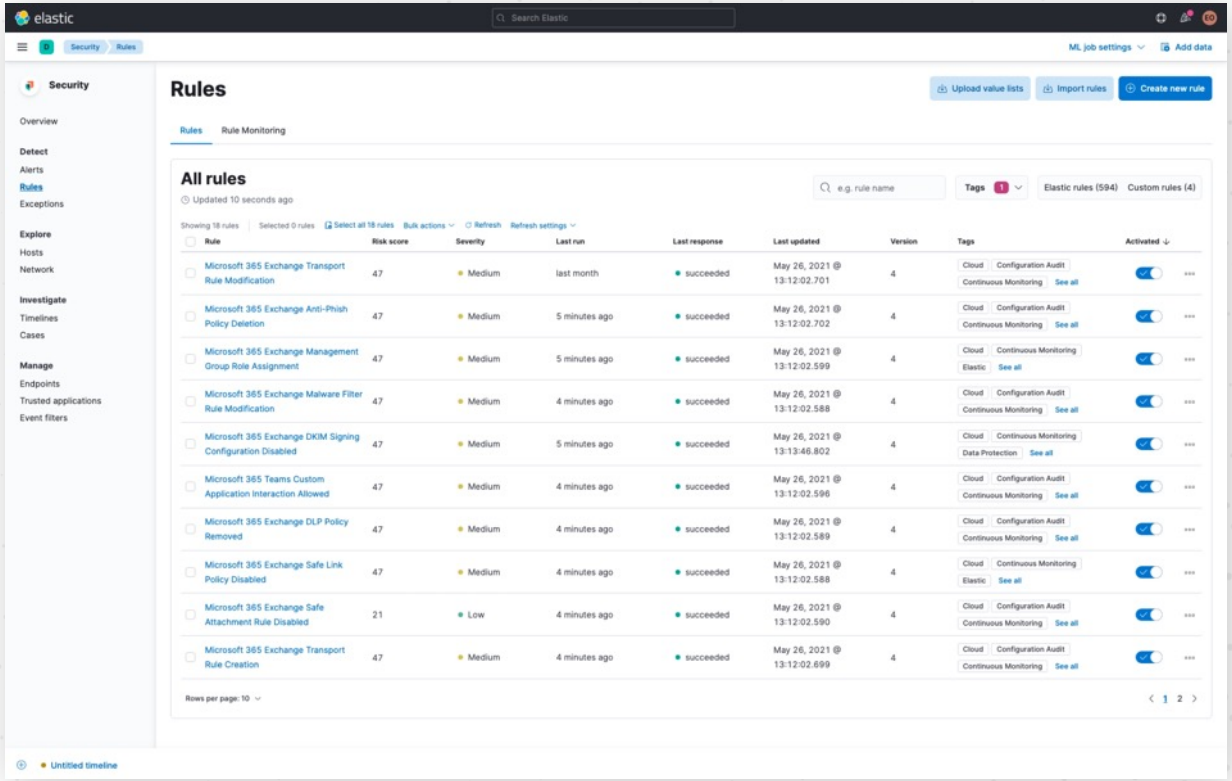
SET UP FILEBEAT TO CAPTURE LOGS

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

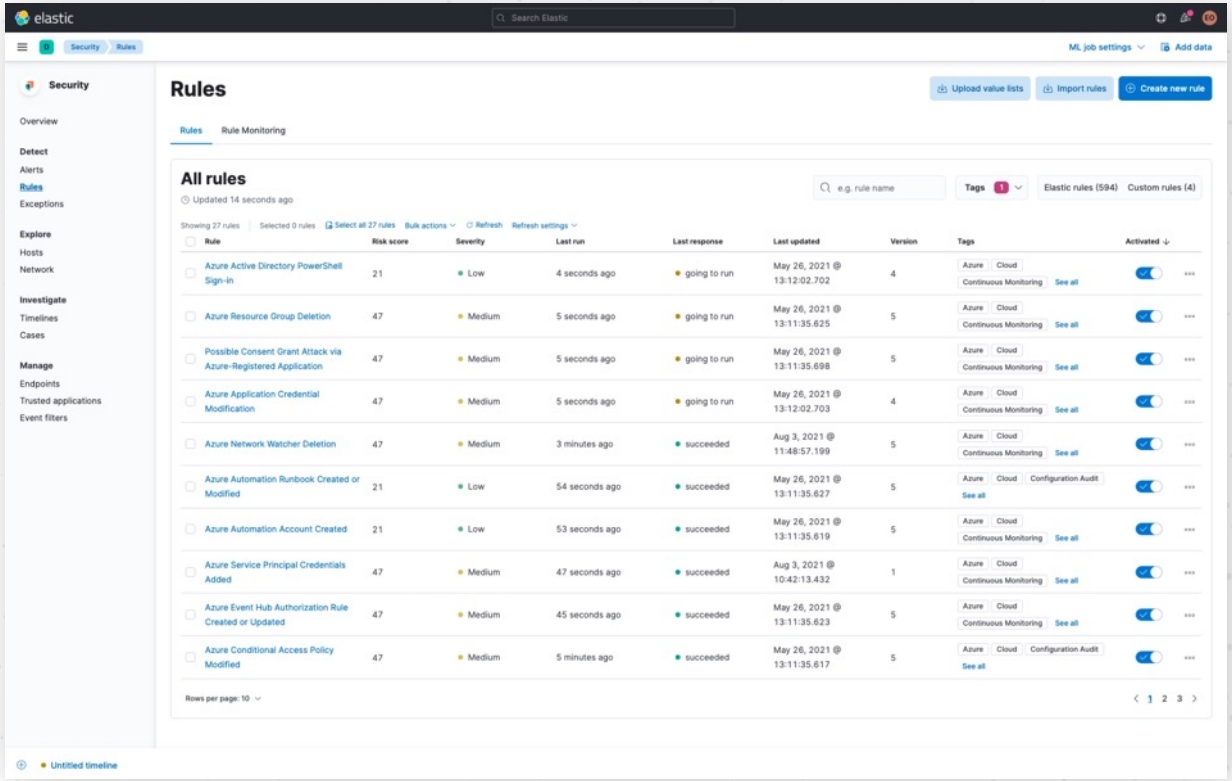
ELASTIC SIEM

PRE-BUILT MICROSOFT 365 RULES



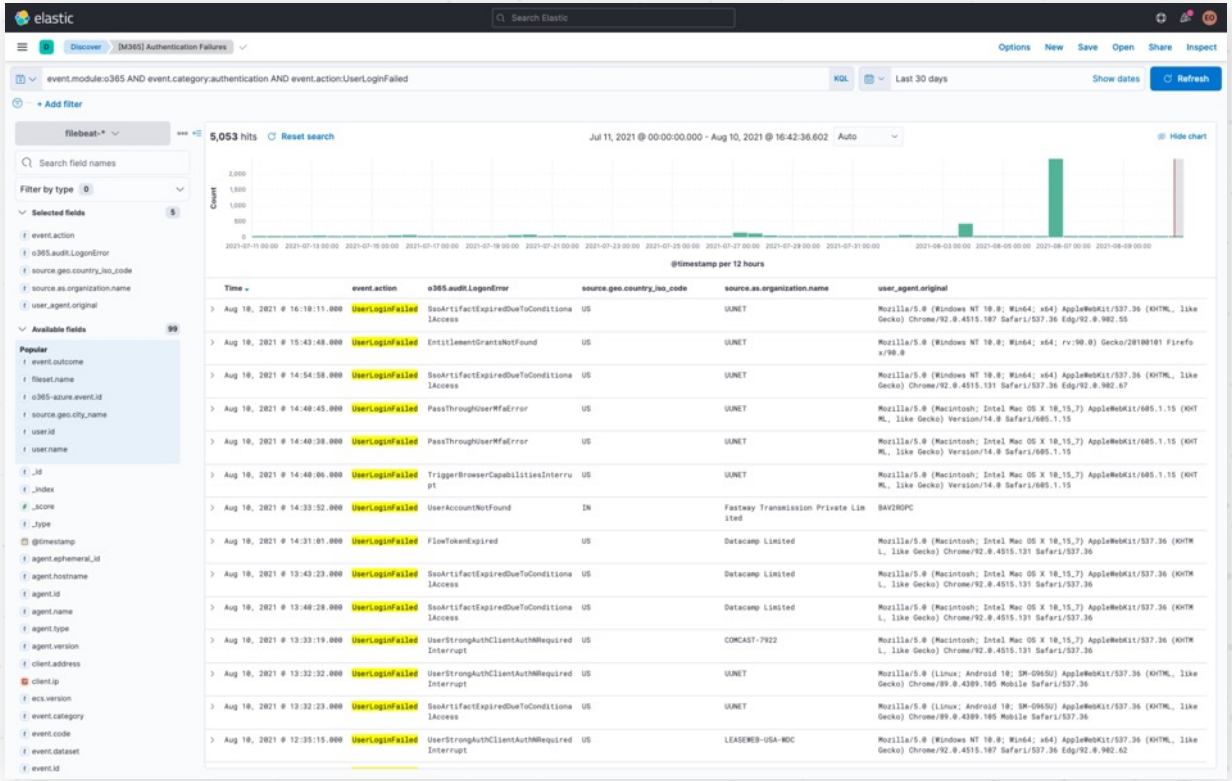
ELASTIC SIEM

PRE-BUILT AZURE RULES



KIBANA QUERIES

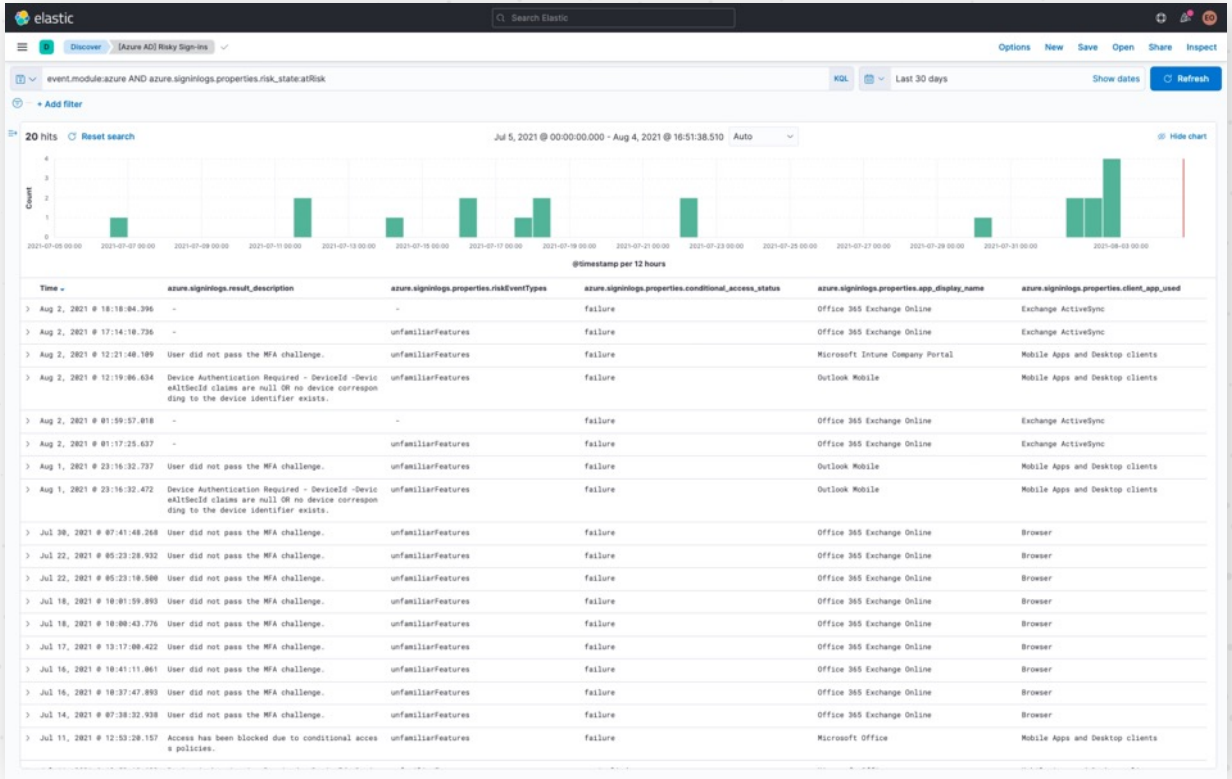
AUTHENTICATION FAILURES



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

KIBANA QUERIES

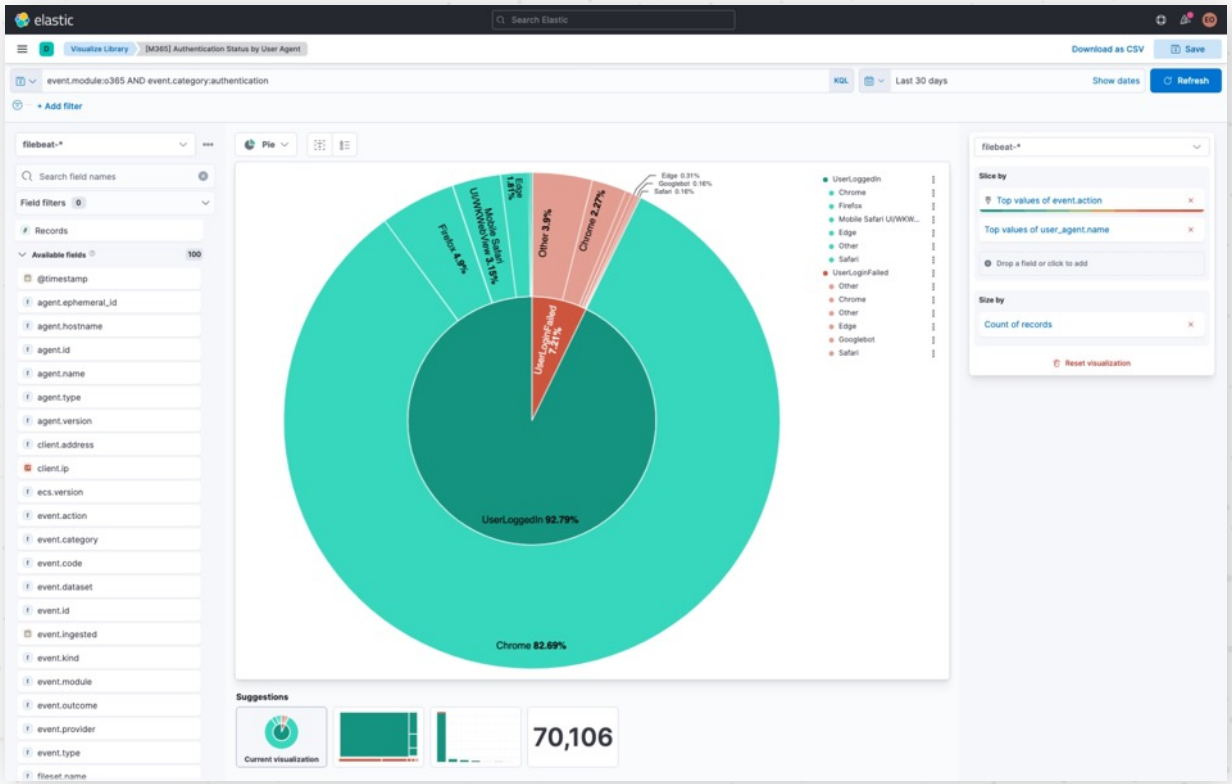
RISKY SIGN-INS



event.module:azure AND azure.signinlogs.properties.risk_state:atRisk

KIBANA VISUALS

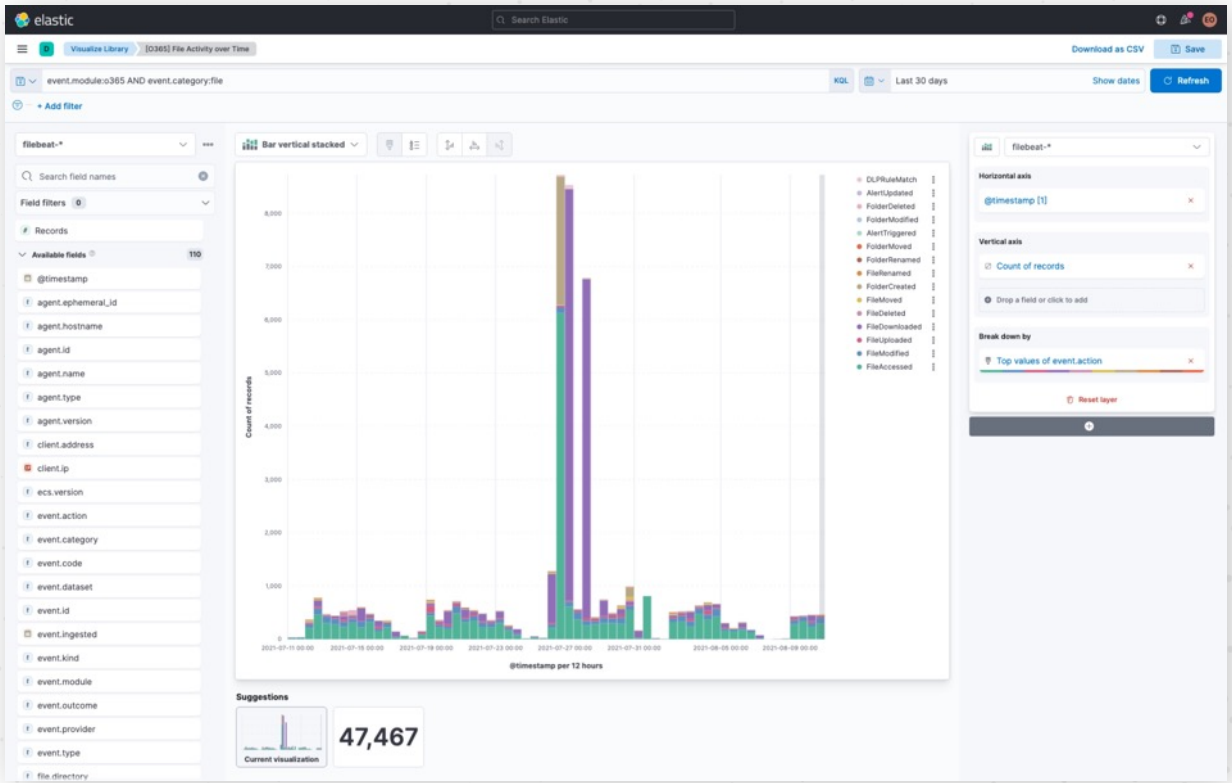
AUTHENTICATION STATUS



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

THANK YOU

ironvine.com
@ivsec
github.com/ironvine