ADOPTIUM

Improving Security Through Access Auditing

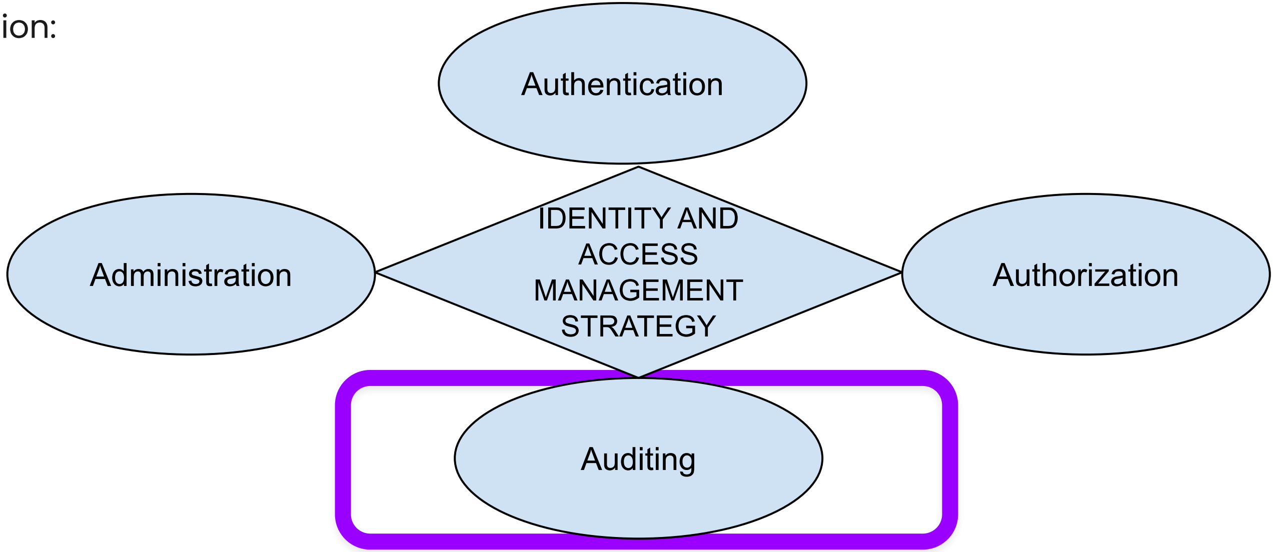
Agenda

- Introduction
- Identity & Access Management
- Tool Selection & Features
- Demonstration
- Questions

Introduction

Introduction & Background

- ❏ Who Am I ?
- ❏ What Is The Adoptium Project?
- ❏ Todays Feature Presentation:



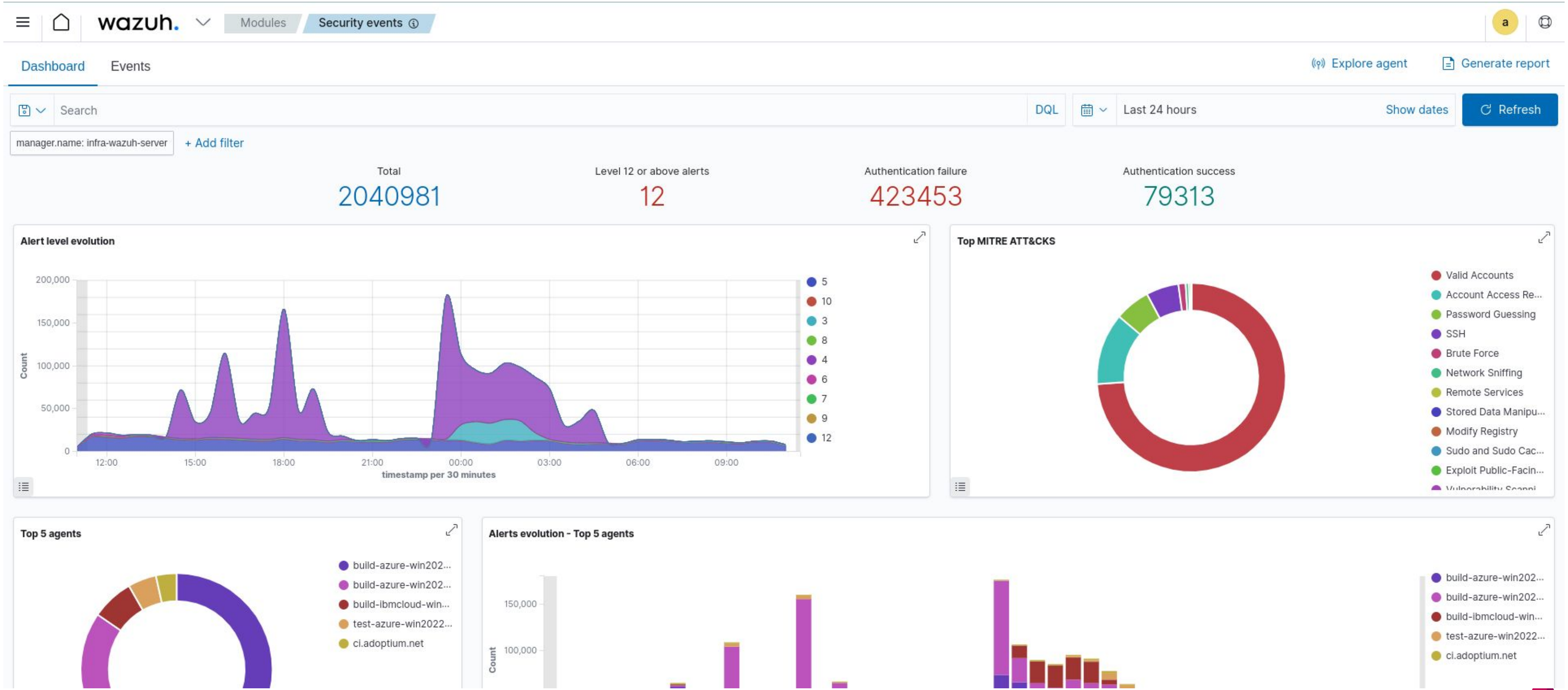
Tool Selection & Features

Tool Selection

- Identify Key Requirements
  - Access Auditing - All Logins & System Access Attempts Should Be Captured
  - Automated Response & Alerting
  - Analytics
  - Reporting
- Why Wazuh ?

Demonstration

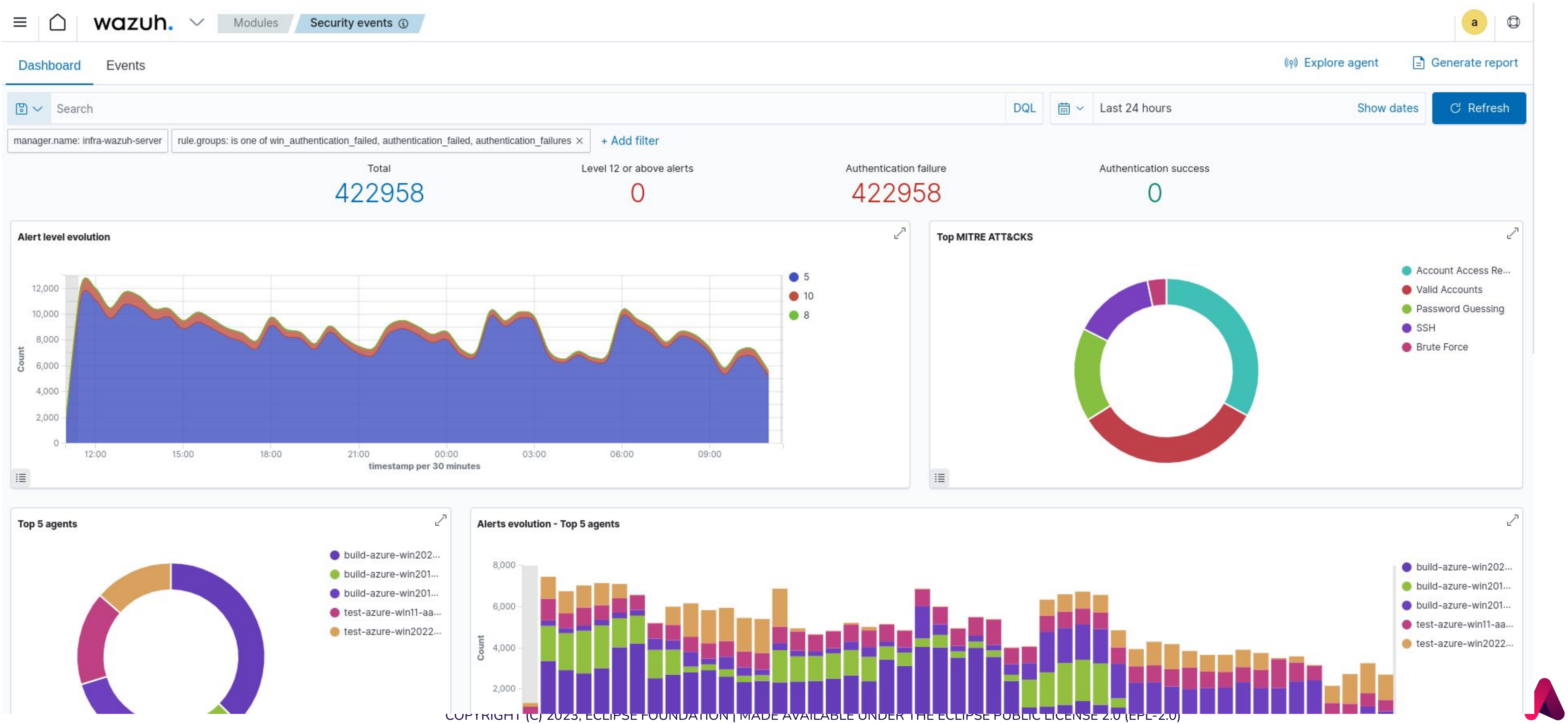
Security Overview



manager.name: infra-wazuh-server

Total	Level 12 or above alerts	Authentication failure	Authentication success
2040981	12	423453	79313

Authentication Failures

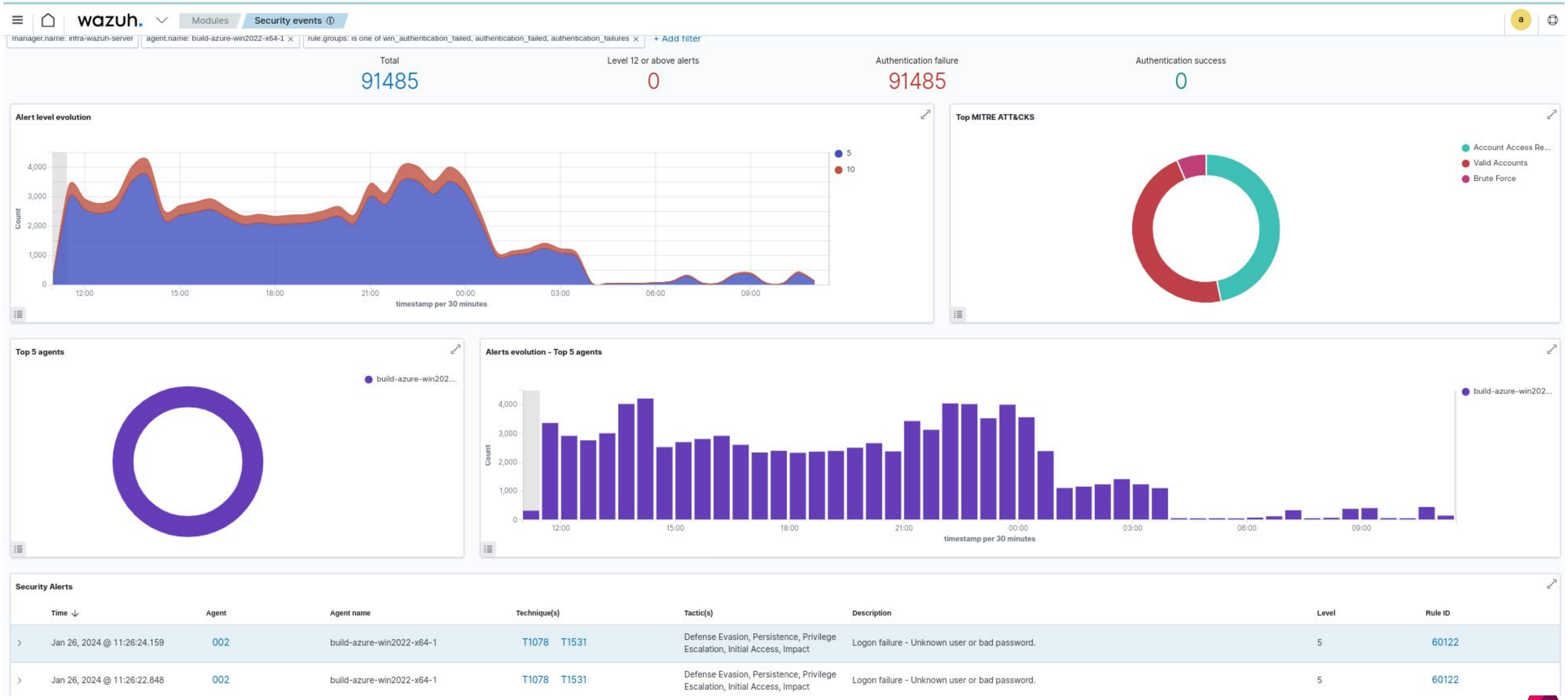


manager.name: infra-wazuh-server

rule.groups: is one of win_authentication_failed, authentication_failed, authentication_failures

Total	Level 12 or above alerts	Authentication failure	Authentication success
422958	0	422958	0

Failures On A Single Host



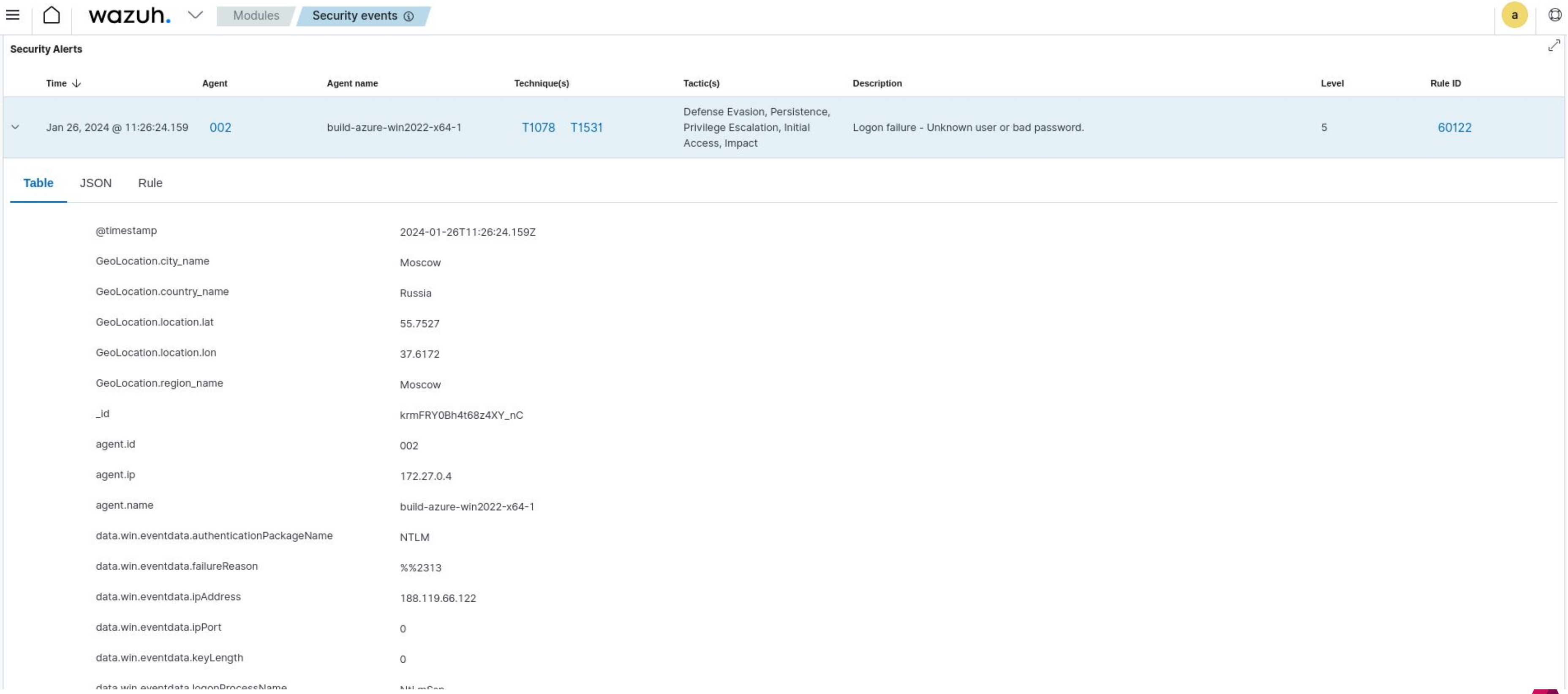
manager.name: infra-wazuh-server | agent.name: build-azure-win2022-x64-1 × | rule.groups: is one of win_authentication_failed, authentication_failed, authentication_failures × | + Add filter

Total	Level 12 or above alerts	Authentication failure	Authentication success
91485	0	91485	0

Security Alerts

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jan 26, 2024 @ 11:26:24.159	002	build-azure-win2022-x64-1	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
Jan 26, 2024 @ 11:26:22.848	002	build-azure-win2022-x64-1	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122

Sample Details



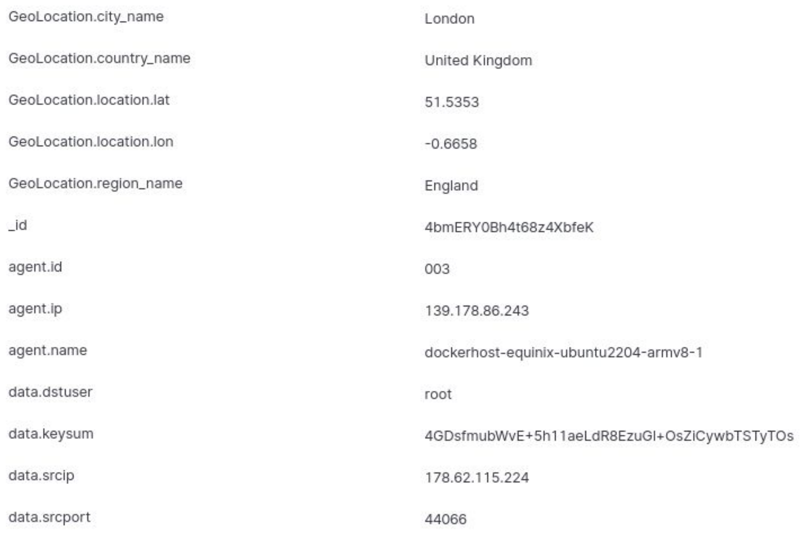
Security Alerts

	Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
⌄	Jan 26, 2024 @ 11:26:24.159	002	build-azure-win2022-x64-1	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122

Table JSON Rule

@timestamp	2024-01-26T11:26:24.159Z
GeoLocation.city_name	Moscow
GeoLocation.country_name	Russia
GeoLocation.location.lat	55.7527
GeoLocation.location.lon	37.6172
GeoLocation.region_name	Moscow
_id	krmFRY0Bh4t68z4XY_nC
agent.id	002
agent.ip	172.27.0.4
agent.name	build-azure-win2022-x64-1
data.win.eventdata.authenticationPackageName	NTLM
data.win.eventdata.failureReason	%%2313
data.win.eventdata.ipAddress	188.119.66.122
data.win.eventdata.ipPort	0
data.win.eventdata.keyLength	0
data.win.eventdata.logonProcessName	NtLmSsp

Extended Audit Information



GeoLocation.city_name	London
GeoLocation.country_name	United Kingdom
GeoLocation.location.lat	51.5353
GeoLocation.location.lon	-0.6658
GeoLocation.region_name	England
_id	4bmERY0Bh4t68z4XbfeK
agent.id	003
agent.ip	139.178.86.243
agent.name	dockerhost-equinix-ubuntu2204-armv8-1
data.dstuser	root
data.keysum	4GDsfmubWvE+5h11aeLdR8EzuGl+OsZiCywbTSTyTOs
data.srcip	178.62.115.224
data.srcport	44066

Thank you!

https://adoptium.net/

Join our Slack channel (adoptium.slack.com)

Twitter: @adoptium

LinkedIn: /adoptium