

OpenSearch Dashboards Reports

Search

28 Sep, 2025 @ 21:03:44.95 → 29 Sep, 2025 @ 22:00:00.00

Threat Hunting (MARKDOWN)

Threat Hunting

Total Alerts Count

15,689

Total Alerts

Total Level 12 or Above Alerts

797

Level 12 Alerts or Above

Total Failed Login Events

1,800

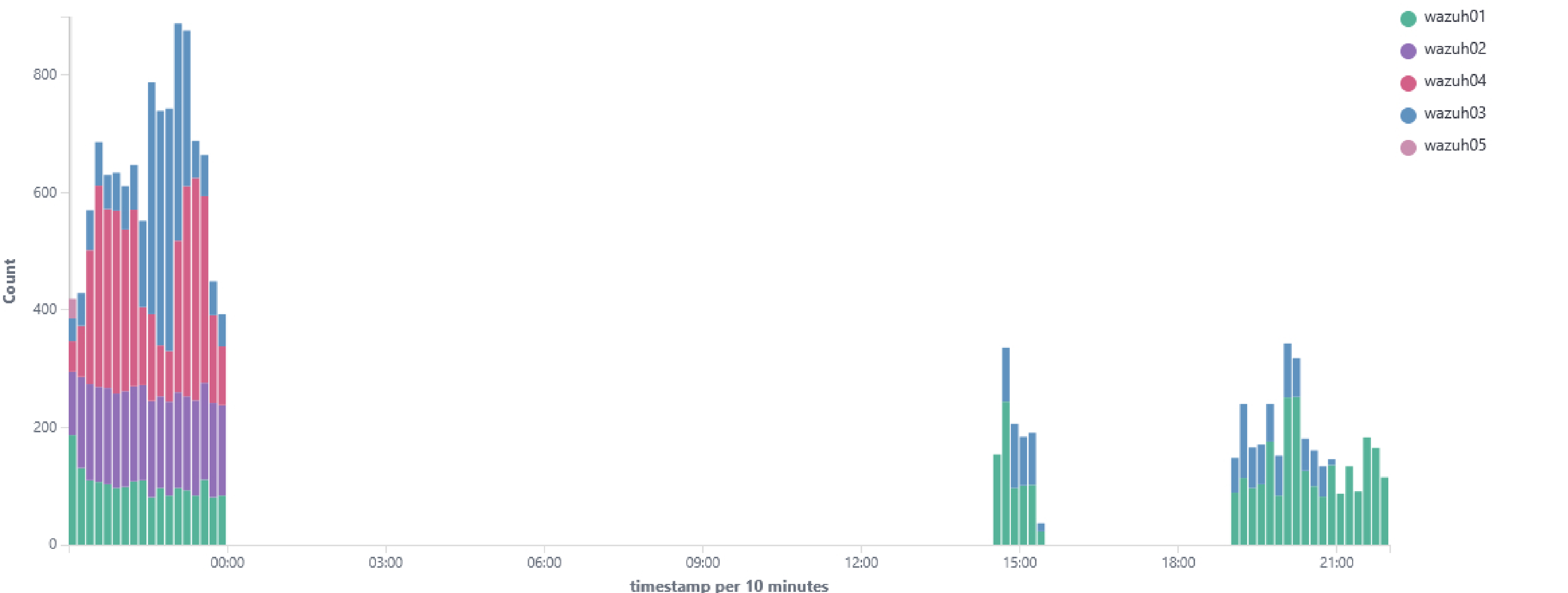
Failed Login Events

Total Successful Login Events

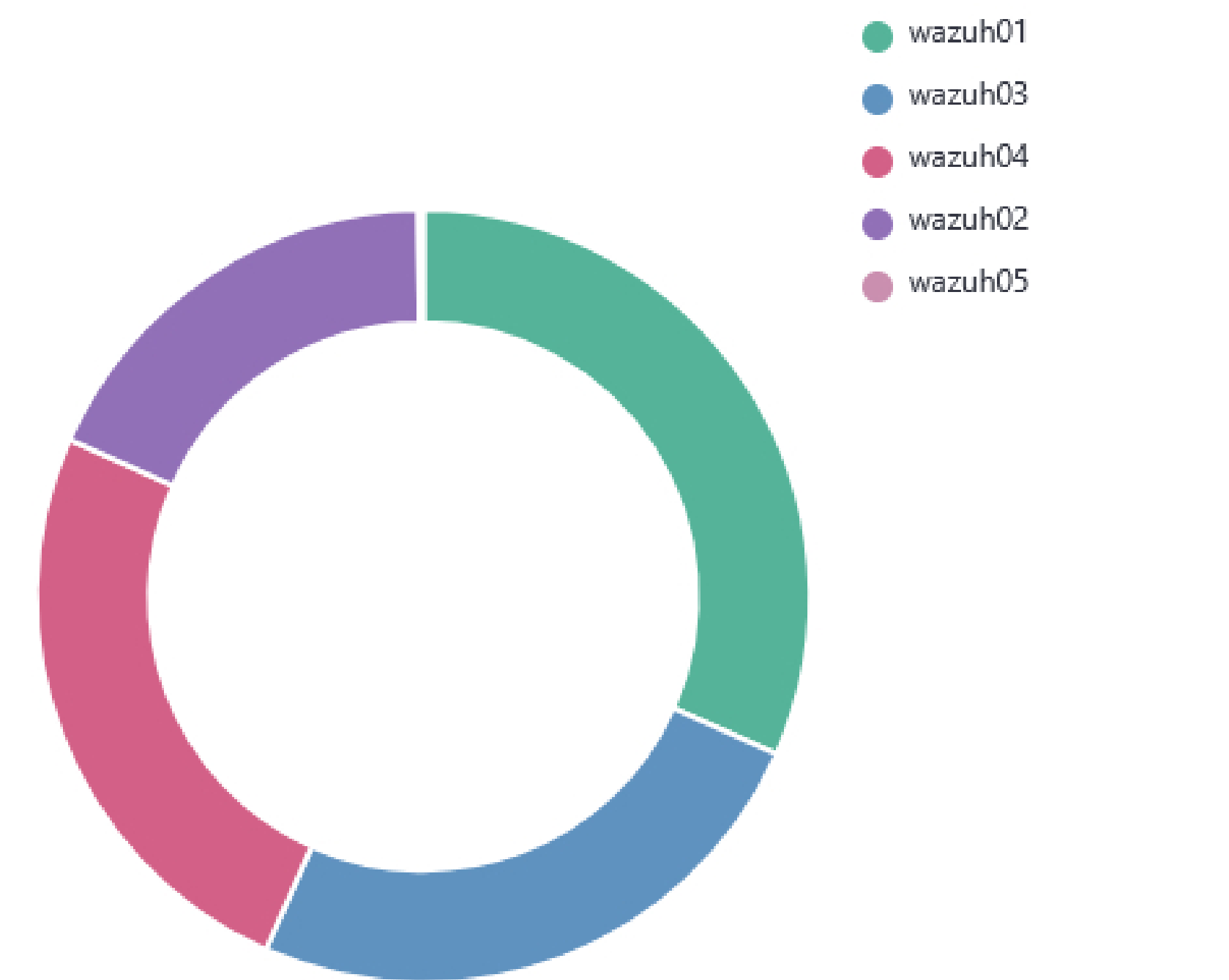
254

Successful Login Events

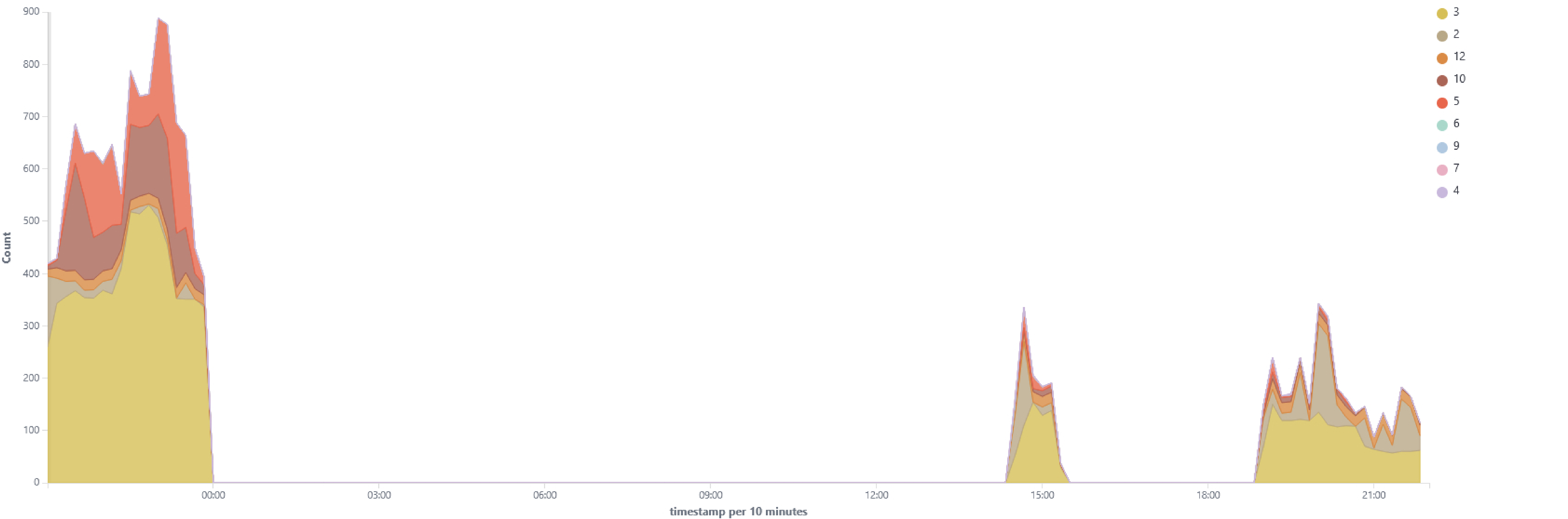
Top 5 Agents (Bar)



Top 5 Agents (Pie)



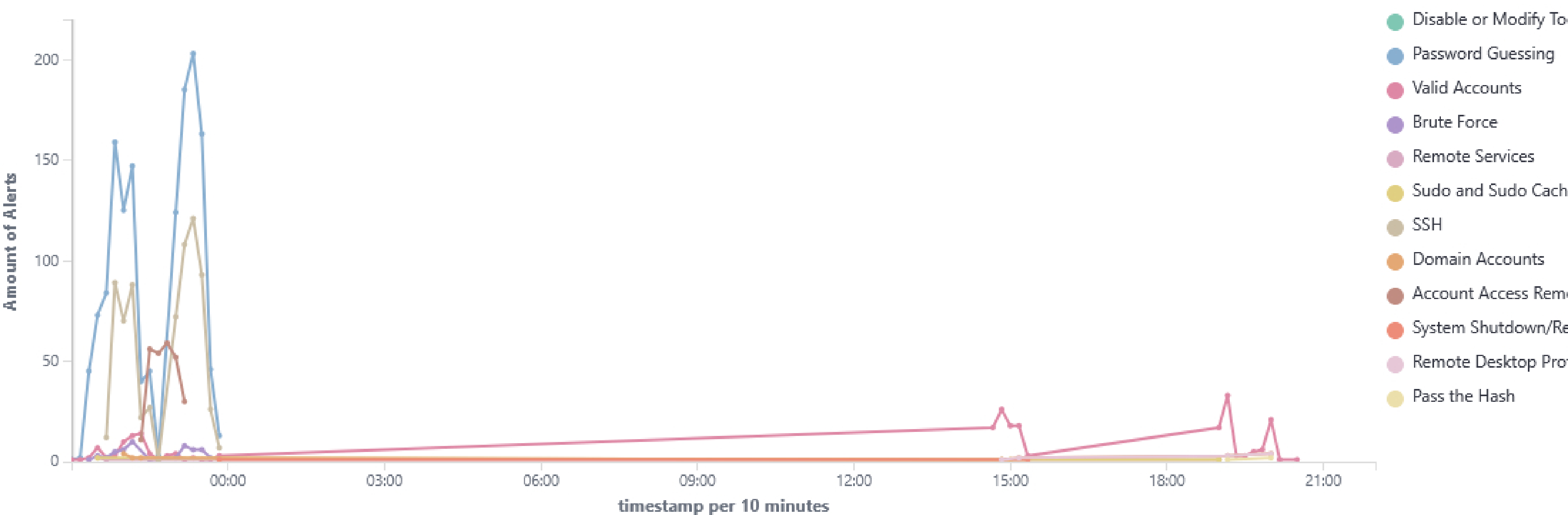
Top 10 Alert Level Evolution



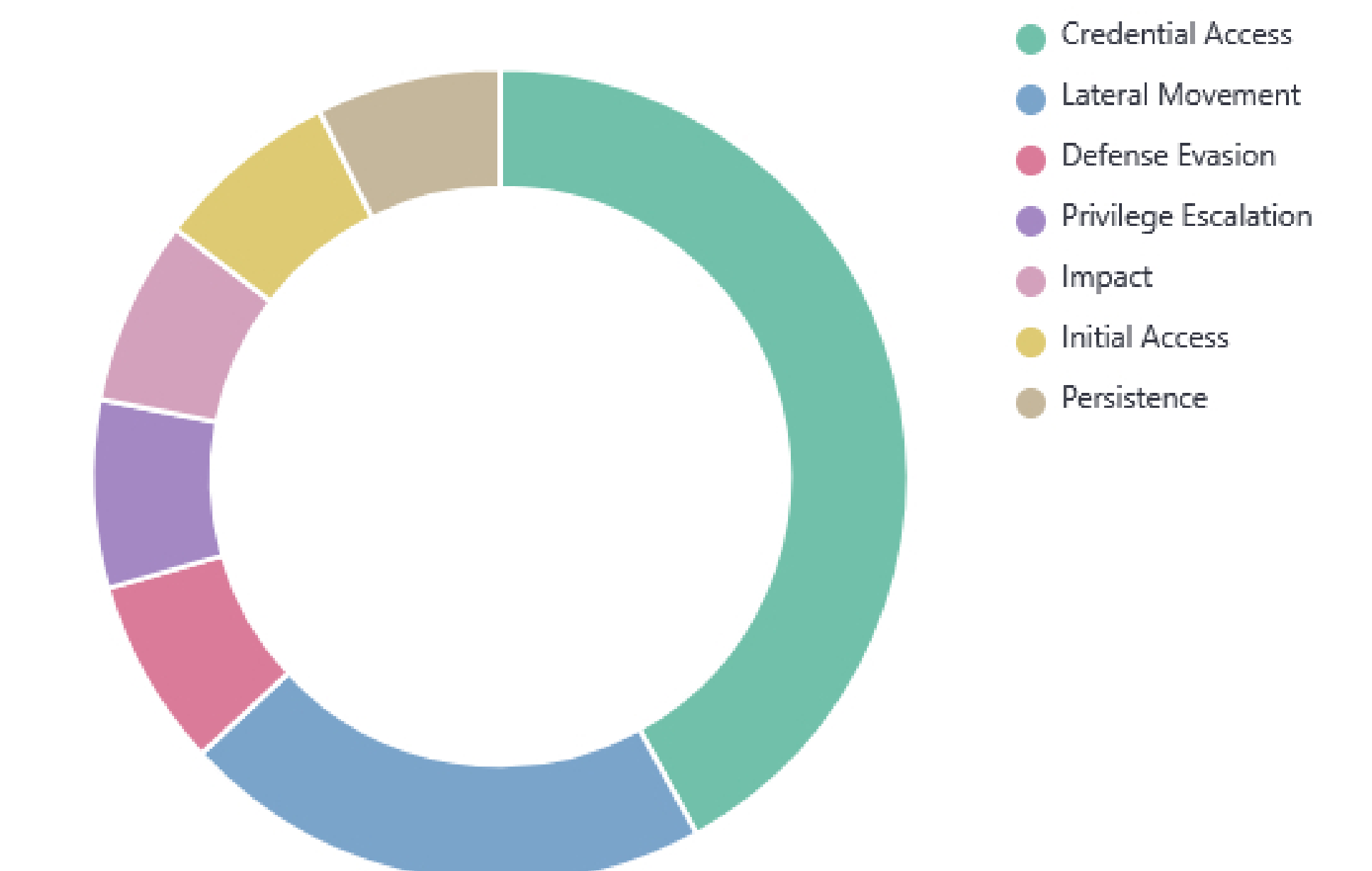
MITRE ATT&CK (MARKDOWN)

MITRE ATT&CK

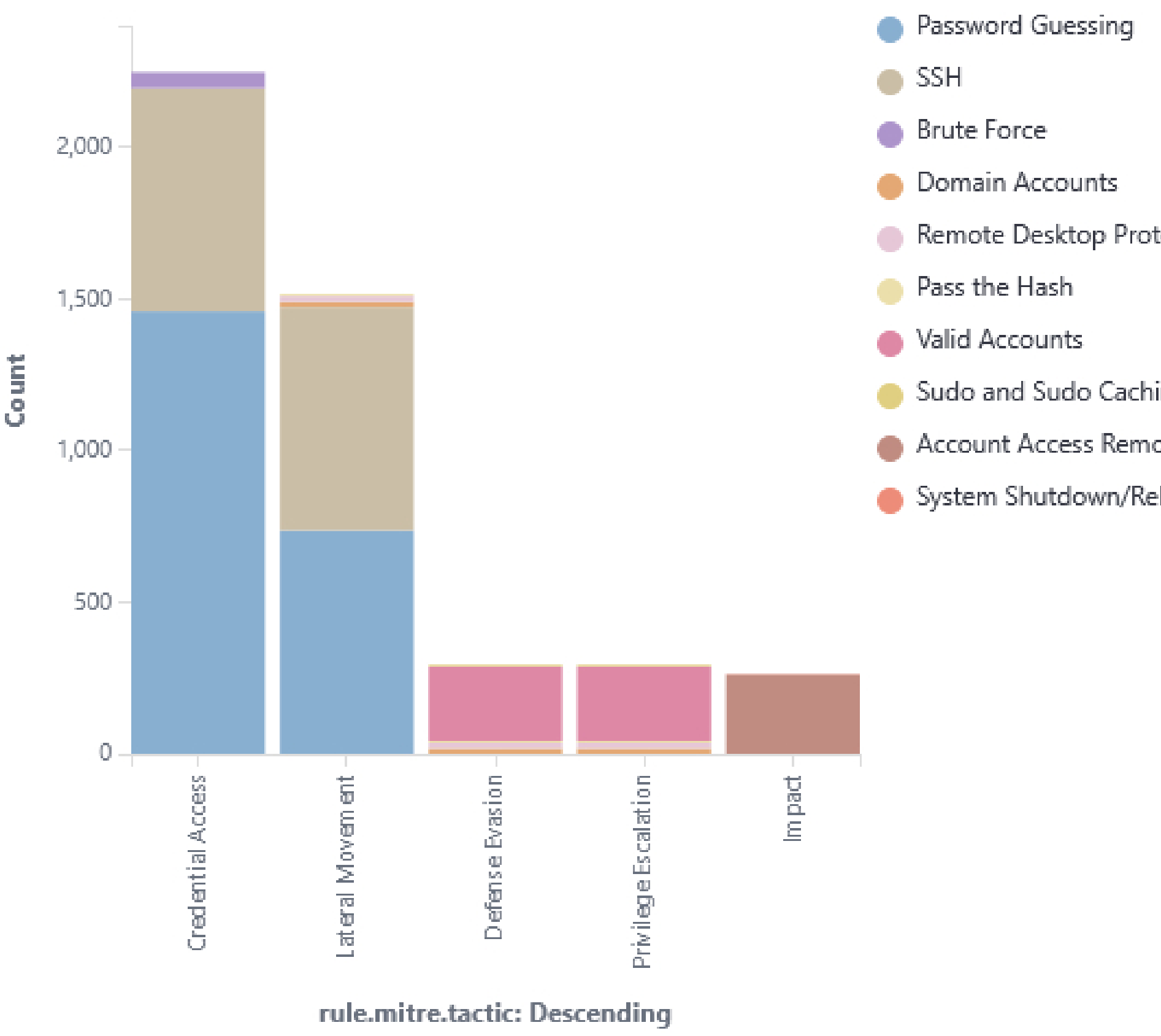
Alerts Evolution Over Time



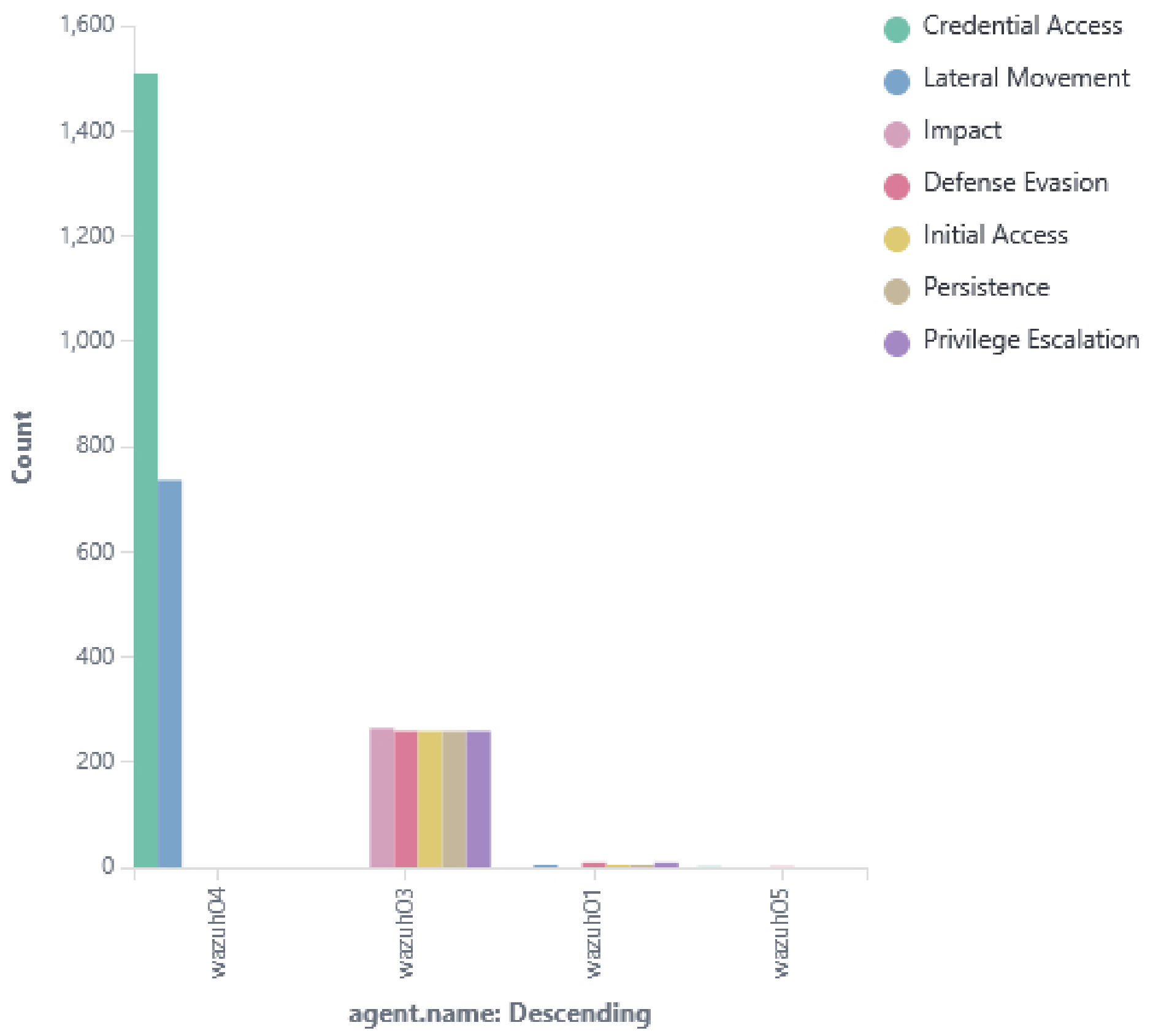
Top Tactics



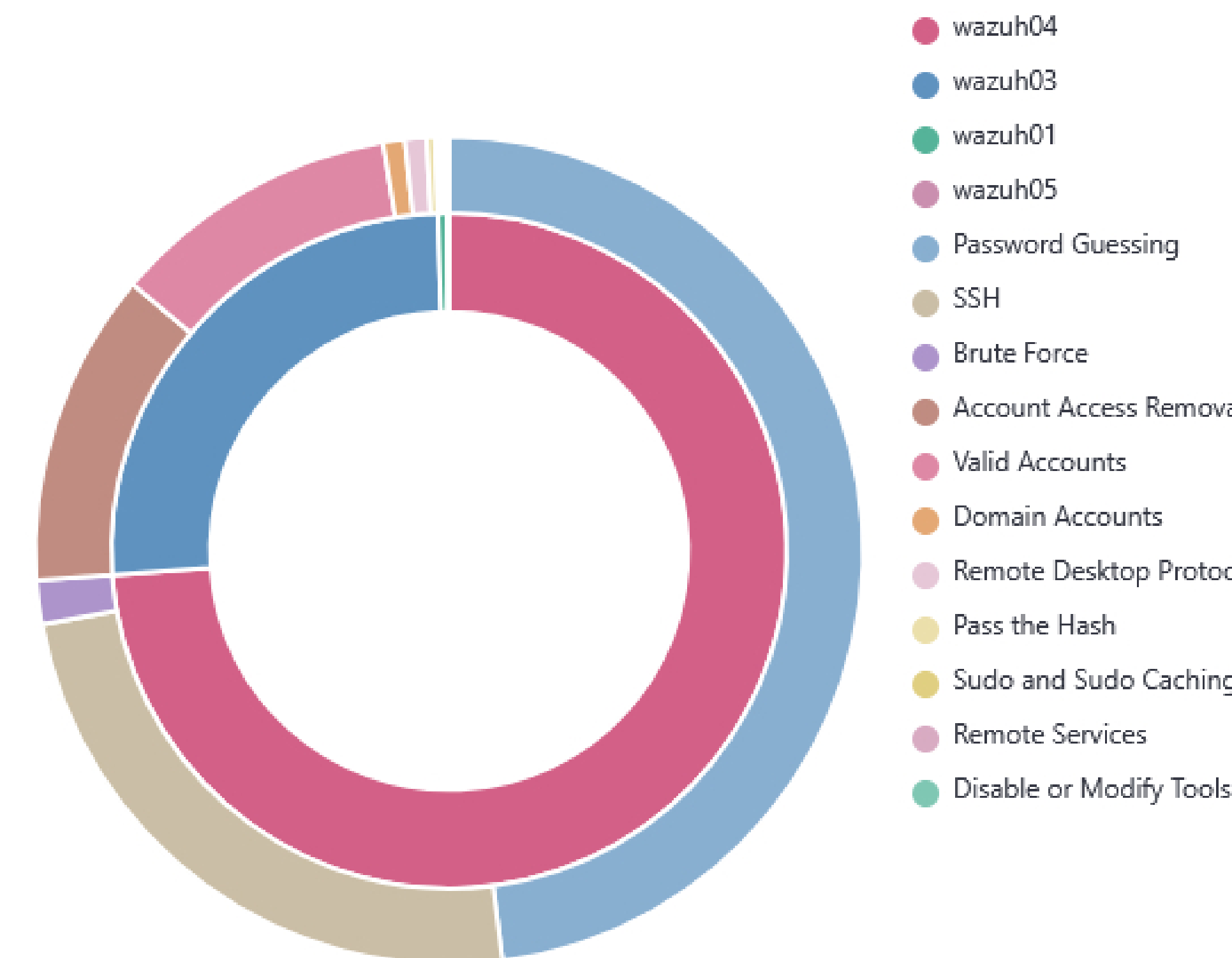
Attacks by Technique



Top Tactics by Agent



MITRE Techniques by Agent



Vulnerability Detection (MARKDOWN)

Vulnerability Detection

Low Severity Vulnerabilities Count

102

Total Low Severities

Medium Severity Vulnerabilities Count

442

Total Medium Severities

High Severity Vulnerabilities Count

3,085

Total High Severities

Critical Severity Vulnerabilities Count

9

Total Critical Severities

Pending Evaluation

2,2...

Pending Evaluation

Top 5 OS

Top 5 OS	Count
Ubuntu 24.04.3 LTS (Noble Numbat)	2,982
Microsoft Windows Server 2025 Datacenter Azure Ed	103

Top 5 Packages

Top 5 Packages	Count
linux-azure	2,706
Microsoft Windows Server 2025 Datacenter Azure	103
cryptography	12
Jinja2	10
binutils	9

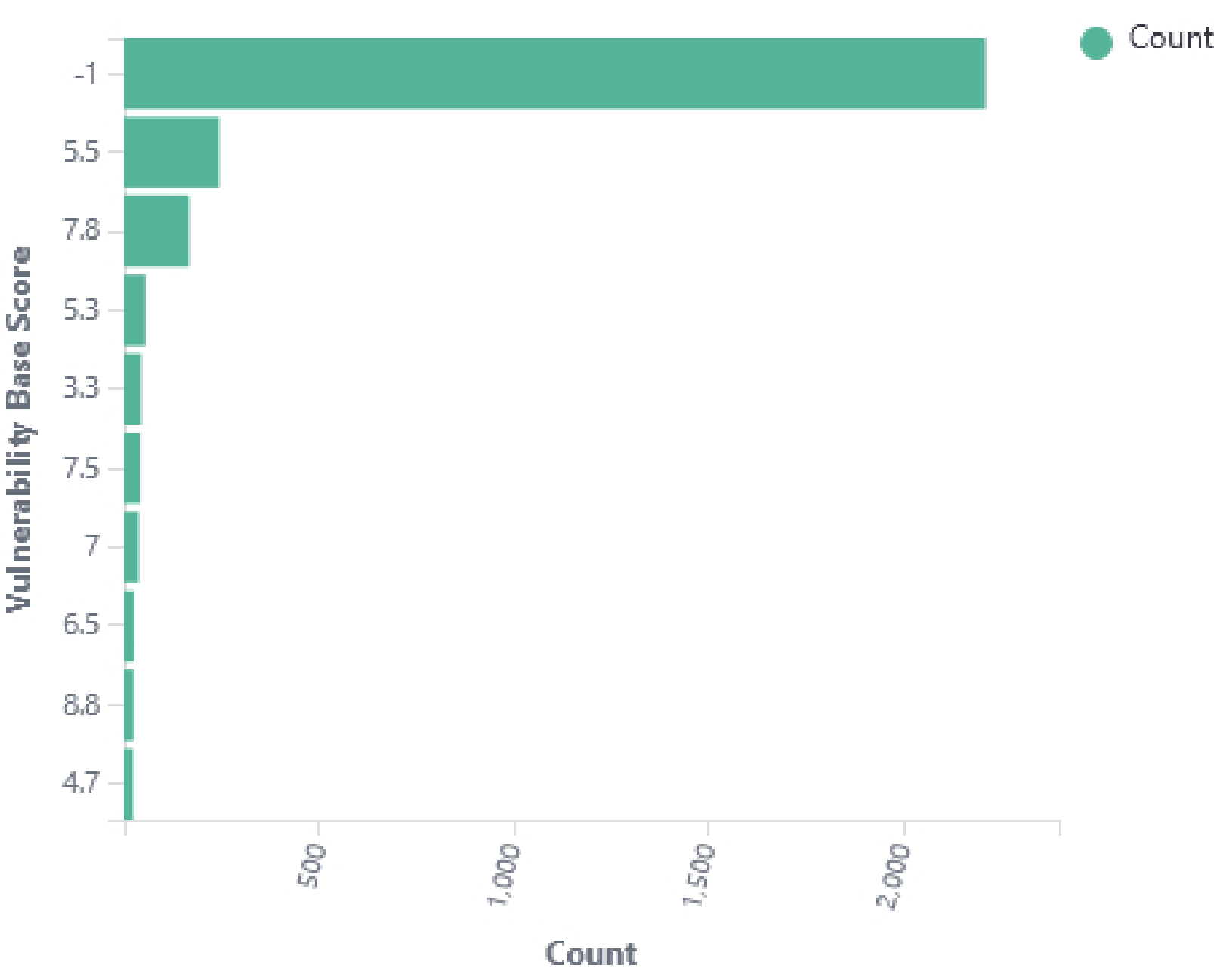
Top 5 Vulnerabilities

Top 5 Vulnerabilities	Count
CVE-2022-3219	22
CVE-2017-13716	8
CVE-2025-1147	8
CVE-2025-1148	8
CVE-2025-3198	8

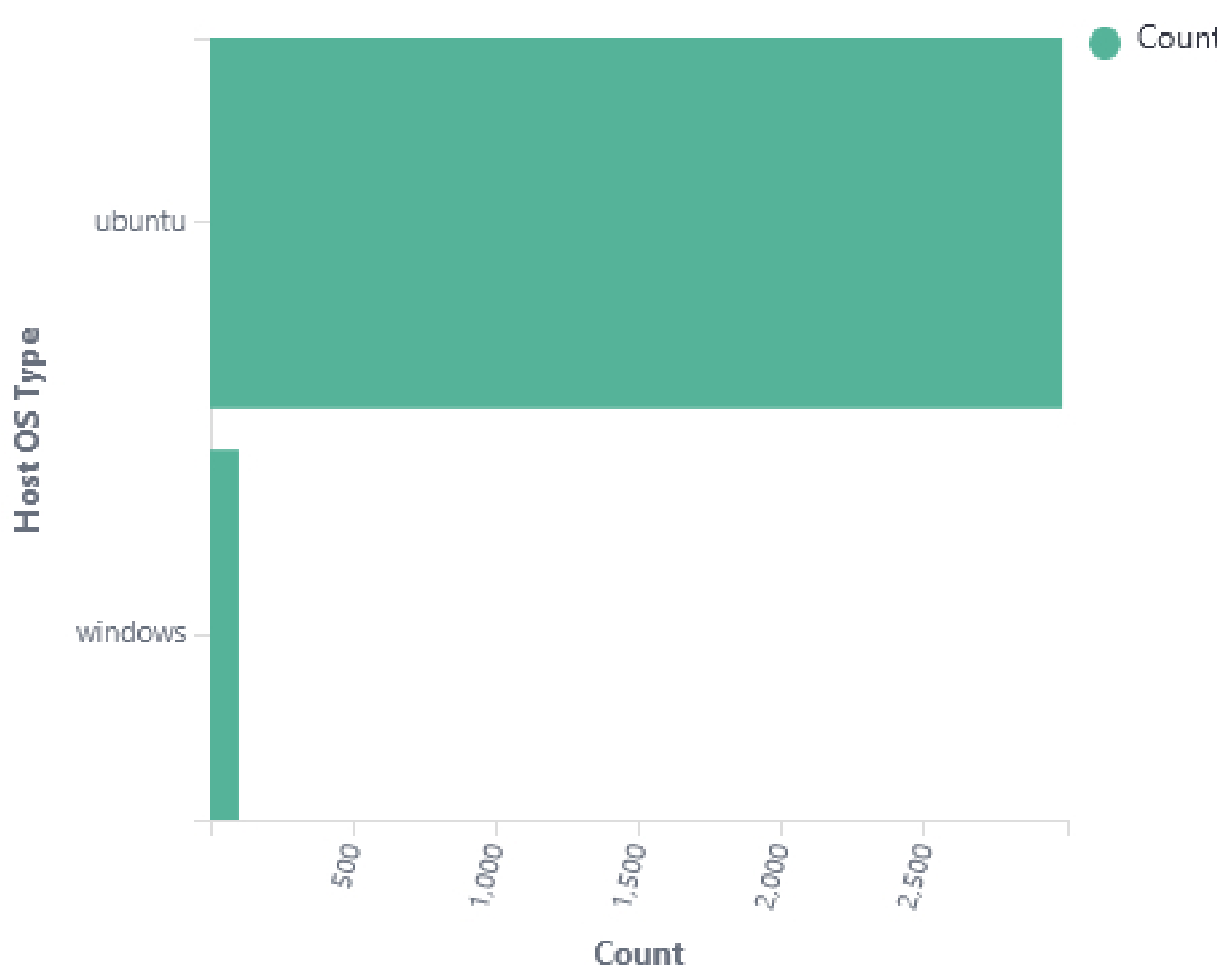
Top 5 Agents

Top 5 Agents	Count
wazuh04	1,523
wazuh02	1,459
wazuh03	103

Vulnerability Base Score



Most Vulnerable OS Families



Vulnerabilities by Year of Publication

