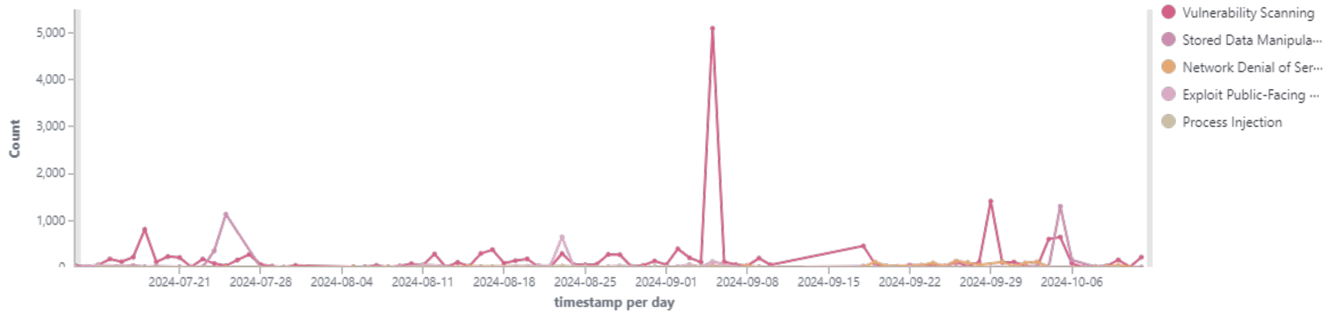
MITRE ATT&CK report

Security events from the knowledge base of adversary tactics and techniques based on real-world observations

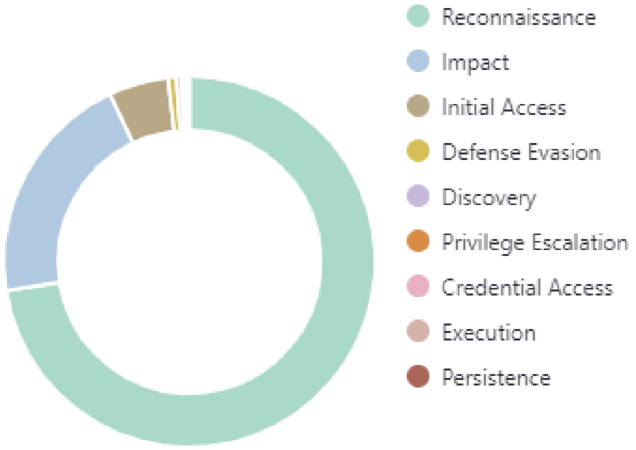
2024-07-12T11:28:39 to 2024-10-12T11:28:39

manager.name: soc AND rule.mitre.id: * AND rule.level: 7-null

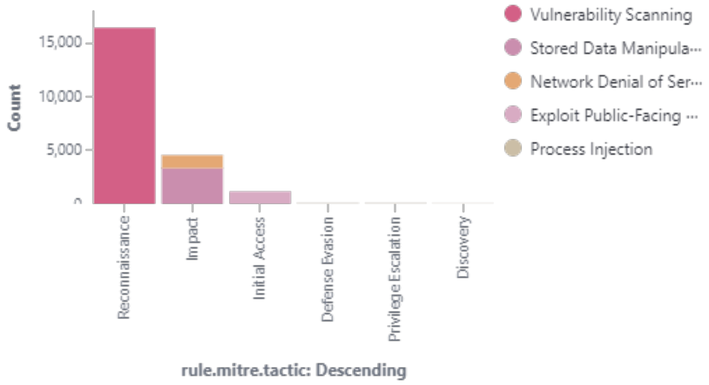
Alerts evolution over time



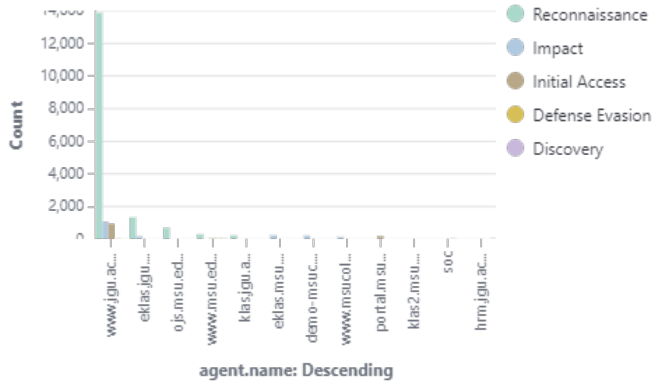
Top tactics



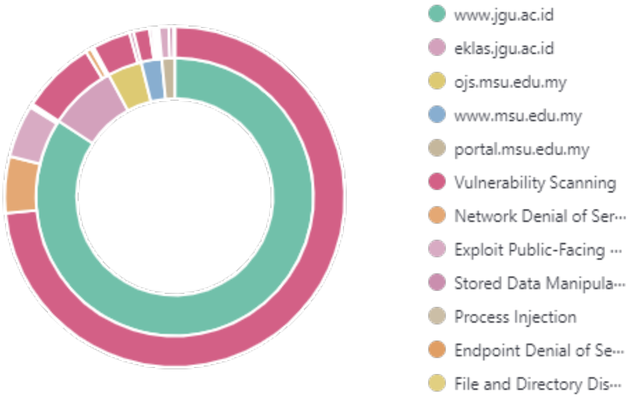
Attacks by technique



Top tactics by agent



Mitre techniques by agent



Alerts summary

Rule ID	Description	Level	Count
31151	Multiple web server 400 error codes from same source ip.	10	16401
550	Integrity checksum changed.	7	3359
31533	High amount of POST requests in a small period of time (likely bot).	10	1181
31103	SQL injection attempt.	7	1173
553	File deleted.	7	70
31153	Multiple common web attacks from same source ip.	10	51
5104	Interface entered in promiscuous(sniffing) mode.	8	51
31152	Multiple SQL injection attempts from same source ip.	10	25
521	Possible kernel level rootkit	11	17
31154	Multiple XSS (Cross Site Scripting) attempts from same source ip.	10	8
31163	Multiple web server 503 error code (Service unavailable).	10	7
2502	syslog: User missed the password more than one time	10	3
5902	New user added to the system.	8	3
5108	System running out of memory. Availability of the system is in risk.	12	2
5758	Maximum authentication attempts exceeded.	8	2
60204	Multiple Windows logon failures.	10	2
2833	Root's crontab entry changed.	8	1
30316	Apache: Multiple Invalid URI requests from same source.	10	1
40112	Multiple authentication failures followed by a success.	12	1
5712	sshd: brute force trying to get access to the system. Non existent user.	10	1
5904	Information from the user was changed.	8	1