info@wazuh.com
https://wazuh.com

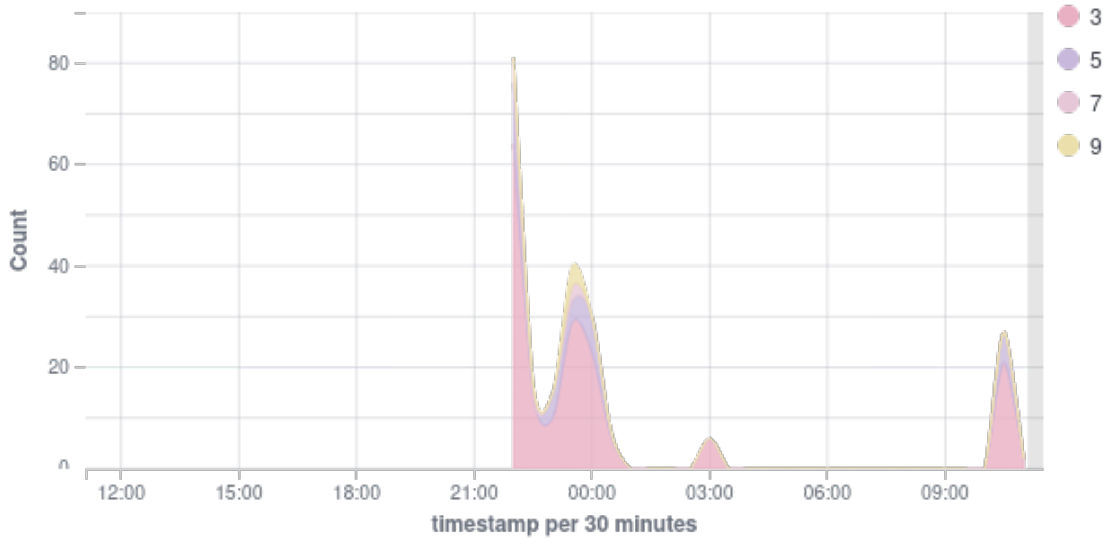
Threat hunting report

Browse through your security alerts, identifying issues and threats in your environment.

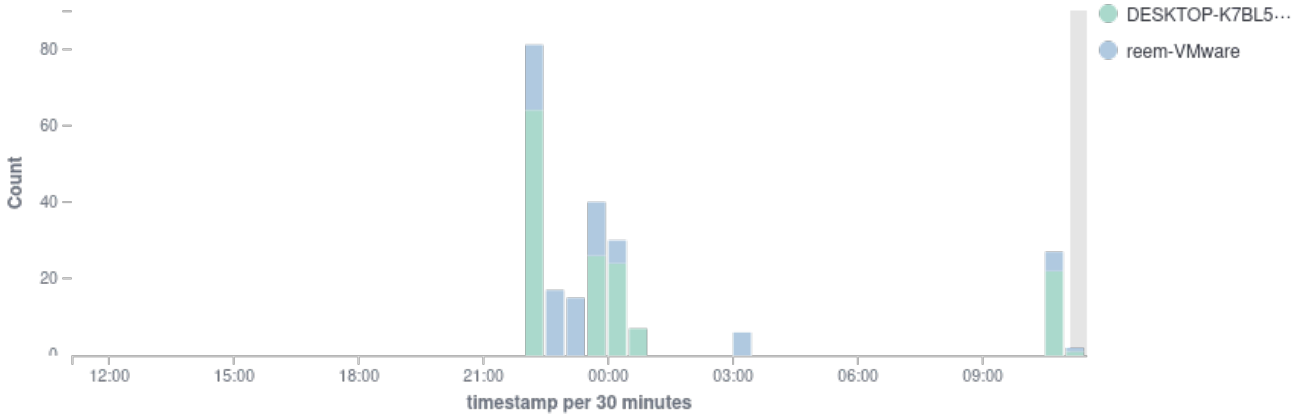
2024-10-19T11:05:43 to 2024-10-20T11:05:43

manager.name: reem-VMware

Top 10 Alert level evolution



Alerts evolution - Top 5 agents



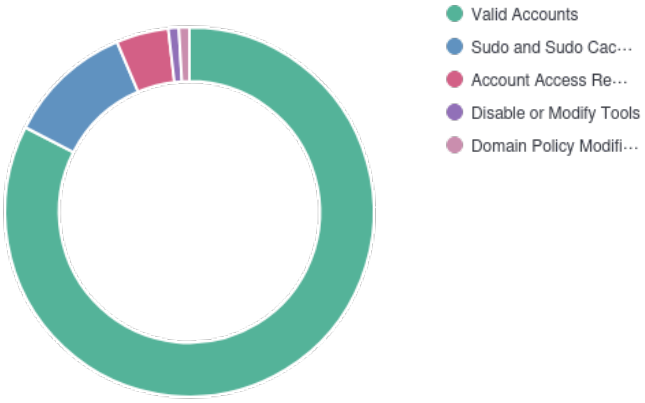
225
- Total -

0
- Level 12 or above alerts -

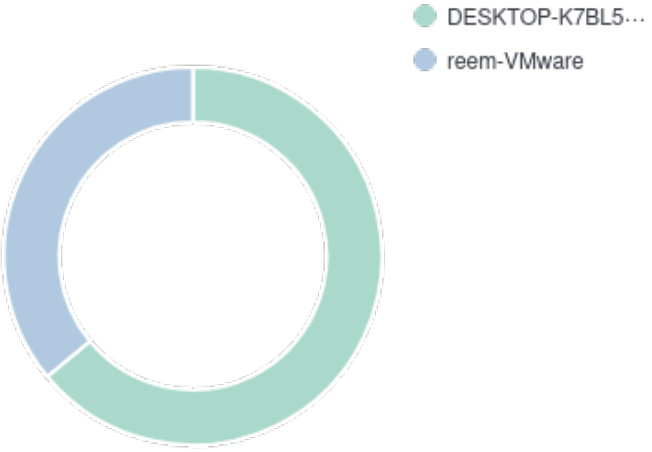
5
- Authentication failure -

90
- Authentication success -

Top 10 MITRE ATT&CKS



Top 5 agents



Alerts summary

Rule ID	Description	Level	Count
60106	Windows Logon Success	3	73
52002	Apparmor DENIED	3	16
5501	PAM: Login session opened.	3	15
5502	PAM: Login session closed.	3	14
5402	Successful sudo to ROOT executed.	3	12
60642	Software protection service scheduled successfully.	3	10
61104	Service startup type was changed	3	10
61109	Name resolution for the name wpad timed out	5	9
510	Host-based anomaly detection event (rootcheck).	7	8
2834	Crontab opened for editing.	5	6
60122	Logon Failure - Unknown user or bad password	5	5
502	Wazuh server started.	3	4
52000	Apparmor messages grouped.	3	4
60646	License activation (slui.exe) failed.	5	3
19004	SCA summary: CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Score less than 50% (32)	7	2
503	Wazuh agent started.	3	2
60118	Windows Workstation Logon Success	3	2
60132	System time changed	5	2
60808	The database engine is replaying log file C:\Winnt\system32\wins\j50.log.	3	2
67023	Non service account logged off.	3	2
19013	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Account lockout duration' is set to '15 or more minute(s)'.: Status changed from failed to 'not applicable'	5	1
19013	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Enforce password history' is set to '24 or more password(s)'.: Status changed from failed to 'not applicable'	5	1
19013	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Minimum password age' is set to '1 or more day(s)'.: Status changed from failed to 'not applicable'	5	1
19013	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Minimum password length' is set to '14 or more character(s)'.: Status changed from failed to 'not applicable'	5	1
19014	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Account lockout duration' is set to '15 or more minute(s)'.: Status changed from 'not applicable' to failed	9	1
19014	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Enforce password history' is set to '24 or more password(s)'.: Status changed from 'not applicable' to failed	9	1
19014	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Minimum password age' is set to '1 or more day(s)'.: Status changed from 'not applicable' to failed	9	1
19014	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Minimum password length' is set to '14 or more character(s)'.: Status changed from 'not applicable' to failed	9	1
19012	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'.: Status changed from passed to 'not applicable'	5	1
19012	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'.: Status changed from passed to 'not applicable'	5	1
19008	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'.	3	1

Rule ID	Description	Level	Count
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'.	3	1
19015	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'.: Status changed from 'not applicable' to passed	3	1
2832	Crontab entry changed.	5	1
40704	Systemd: Service exited due to a failure.	5	1
504	Wazuh agent disconnected.	3	1
60668	The Windows search service started.	3	1
60702	The VSS service is shutting down due to idle timeout.	5	1
60798	The database engine attached a database.	3	1
60805	The database engine is starting a new instance.	3	1
60807	The database engine is initiating recovery steps.	3	1
60809	The database engine has completed recovery steps.	3	1
61102	Windows System error event	5	1
67028	Special privileges assigned to new logon.	3	1