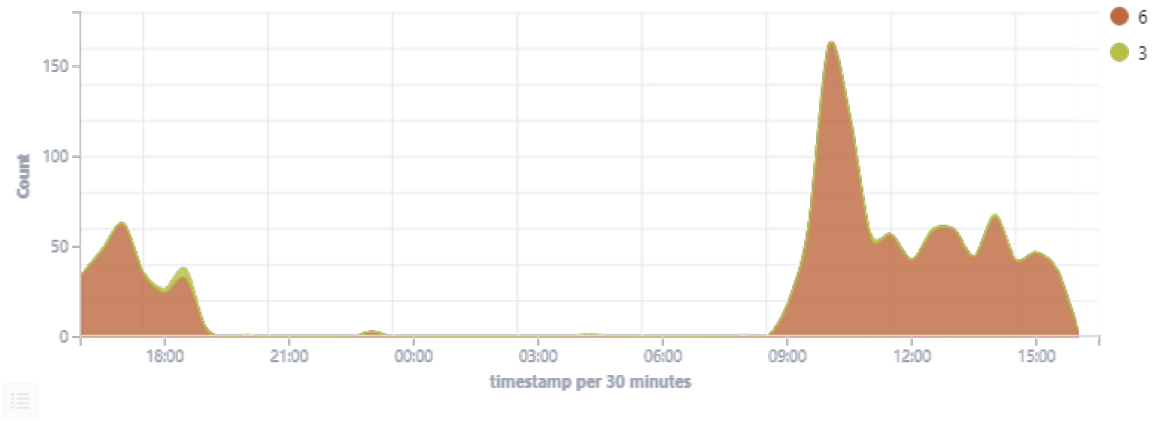
Security events report

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

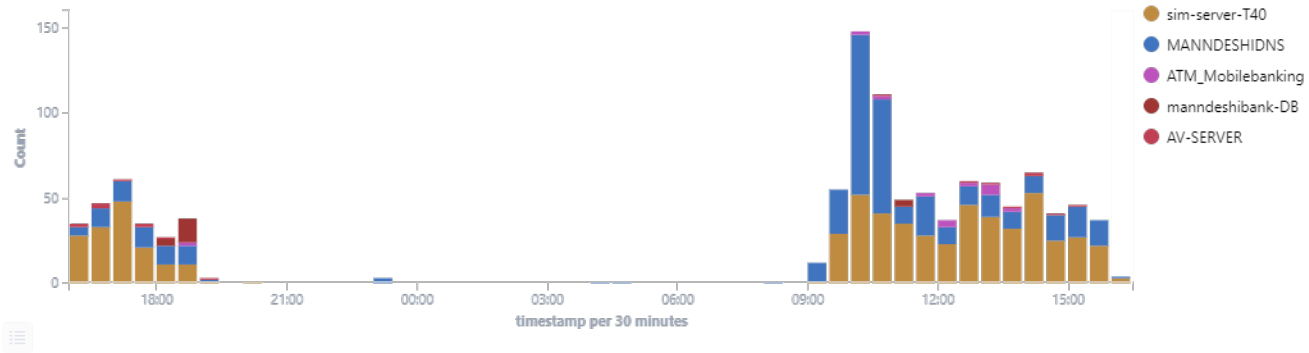
2024-01-01T16:00:52 to 2024-01-02T16:00:52

manager.name: sim-server-T40 AND (remote)

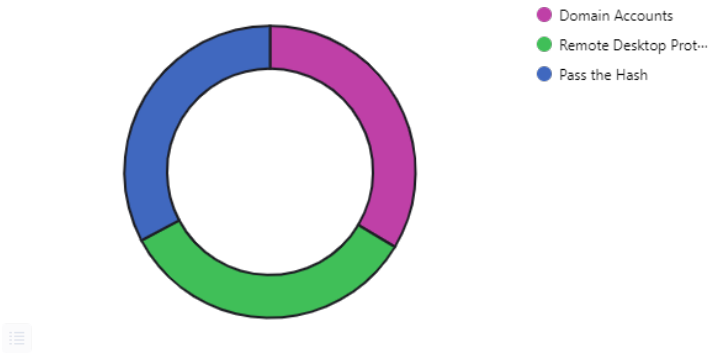
Alert level evolution



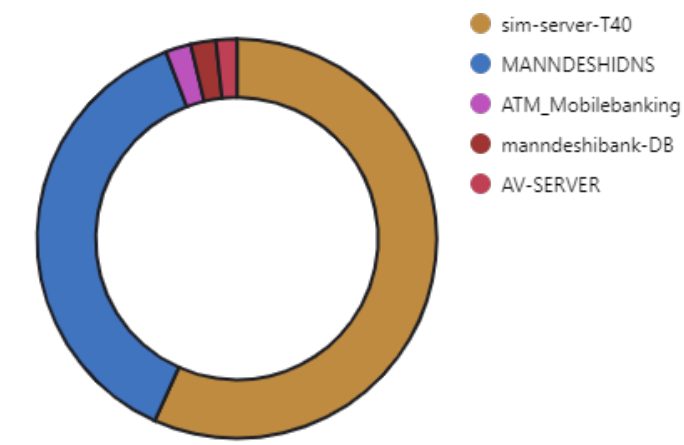
Alerts evolution Top 5 agents



Alerts



Top 5 agents



Alerts summary

Rule ID	Description	Level	Count
81644	Fortigate: Blocked URL belongs to a denied category in policy.	6	610
92657	Successful Remote Logon Detected - User:\KSS - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-HO-221 is allowed to perform RDP connections	6	24
92657	Successful Remote Logon Detected - User:\bank_admin - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that PAM-SARVER-46 is allowed to perform RDP connections	6	23
92657	Successful Remote Logon Detected - User:\MMSBNK_PRINTER$ - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK_PRINTER is allowed to perform RDP connections	6	20
92657	Successful Remote Logon Detected - User:\RSK - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-07-21 is allowed to perform RDP connections	6	17
92657	Successful Remote Logon Detected - User:\PAA - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-HO-151 is allowed to perform RDP connections	6	14
92657	Successful Remote Logon Detected - User:\JMU - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-HO-247 is allowed to perform RDP connections	6	11
92657	Successful Remote Logon Detected - User:\SAB - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-06-207 is allowed to perform RDP connections	6	11
92657	Successful Remote Logon Detected - User:\MAY - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-05-199 is allowed to perform RDP connections	6	10
92657	Successful Remote Logon Detected - User:\admin1 - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that NAS-MDMSBANK is allowed to perform RDP connections	6	10
92657	Successful Remote Logon Detected - User:\DVM - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-02-207 is allowed to perform RDP connections	6	9
92657	Successful Remote Logon Detected - User:\BSS - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-05-202 is allowed to perform RDP connections	6	8
92657	Successful Remote Logon Detected - User:\Administrator - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MDF-IT-210 is allowed to perform RDP connections	6	6
92657	Successful Remote Logon Detected - User:\Administrator - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-HO-247 is allowed to perform RDP connections	6	6
92657	Successful Remote Logon Detected - User:\CDM - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-02-203 is allowed to perform RDP connections	6	6
92657	Successful Remote Logon Detected - User:\JMU - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-HO-55 is allowed to perform RDP connections	6	6
92657	Successful Remote Logon Detected - User:\NMA - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-07-20 is allowed to perform RDP connections	6	6
92657	Successful Remote Logon Detected - User:\PMP - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-06-150 is allowed to perform RDP connections	6	6
92657	Successful Remote Logon Detected - User:\SCS - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-HO-150 is allowed to perform RDP connections	6	6
92657	Successful Remote Logon Detected - User:\DRB - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-07-019 is allowed to perform RDP connections	6	5
92657	Successful Remote Logon Detected - User:\DSB01 - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that MMSBNK-01-IT is allowed to perform RDP connections	6	5
92653	User: MANNDESHIBANK\Administrator logged using Remote Desktop Connection (RDP) from ip:192.168.71.243.	3	4
92653	User: MANNDESHIBANK\repluser logged using Remote Desktop Connection (RDP) from ip:192.168.71.46.	3	4
92653	User: MANNDESHIBANK\Administrator logged using Remote Desktop Connection (RDP) from ip:192.168.71.210.	3	3
92653	User: MANNDESHIBANK\repluser logged using Remote Desktop Connection (RDP) from ip:192.168.206.167.	3	2