```
_id timestamp rule agent manager full_log predecoder decoder data location 1716373074.2782
2024-05-22T16:17:54.546+0600 {'level': 3, 'description': 'PAM: Login session opened.', 'id':
'5501', 'mitre': {'id': ['T1078'], 'tactic': ['Defense Evasion', 'Persistence', 'Privilege Escalation',
'Initial Access'], 'technique': ['Valid Accounts']}, 'firedtimes': 1, 'mail': False, 'groups': ['pam',
'syslog', 'authentication_success'], 'pci_dss': ['10.2.5'], 'gpg13': ['7.8', '7.9'], 'gdpr': ['IV_32.2'],
'hipaa': ['164.312.b'], 'nist_800_53': ['AU.14', 'AC.7'], 'tsc': ['CC6.8', 'CC7.2', 'CC7.3']} {'id': '000',
'name': 'mmetroooo'} {'name': 'mmetroooo'} May 22 15:17:54 mmetroooo su:
pam_unix(su:session): session opened for user aomer(uid=1000) by aomer(uid=0)
{'program_name': 'su', 'timestamp': 'May 22 15:17:54', 'hostname': 'mmetroooo'} {'parent': 'pam',
'name': 'pam'} {'srcuser': 'aomer', 'dstuser': 'aomer(uid=1000)', 'uid': '0'} /var/log/auth.log
```