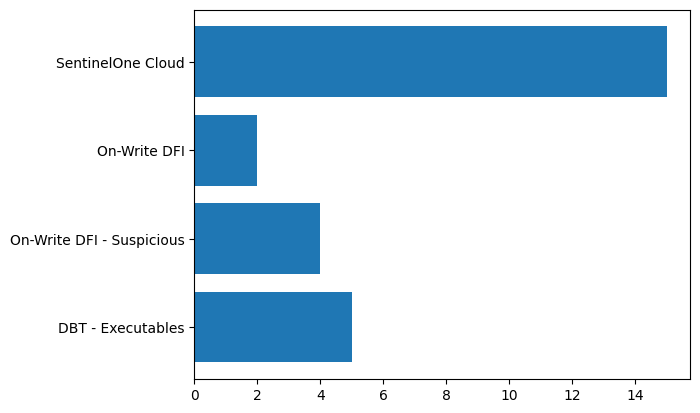
센티넬원 리포트

# 기간 : 2022-11-01 ~ 2022-12-19

## 1.기간별 전체 탐지 내역

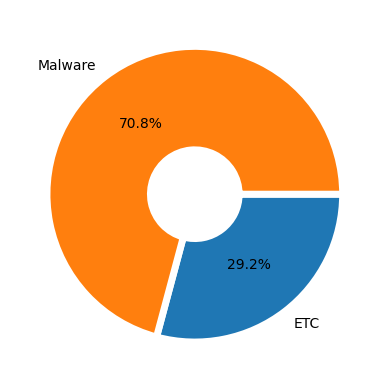
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| agent 명 | IP 주소 | 종류 | 처리 여부 | 위협 구분 | account>site>group |
| OLD\_PAYROLL | 192.168.100.33 | Generic.Heuristic | not\_mitigated | suspicious | Wonik>0-머트리얼즈>01.서버 |
| OLD\_PAYROLL | 192.168.100.33 | Generic.Heuristic | not\_mitigated | suspicious | Wonik>0-머트리얼즈>01.서버 |
| OLD\_PAYROLL | 192.168.100.33 | Generic.Heuristic | not\_mitigated | suspicious | Wonik>0-머트리얼즈>01.서버 |
| wimcopolicysvr | 169.254.176.44 | Malware | not\_mitigated | suspicious | Wonik>0-머트리얼즈>01.서버 |
| OLD\_PAYROLL | 192.168.100.33 | Generic.Heuristic | not\_mitigated | suspicious | Wonik>0-머트리얼즈>01.서버 |
| OLD\_PAYROLL | 192.168.100.33 | Generic.Heuristic | not\_mitigated | suspicious | Wonik>0-머트리얼즈>01.서버 |
| newmessvr | 192.168.20.155 | Malware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| newmessvr | 192.168.20.155 | Malware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Malware | not\_mitigated | suspicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Malware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Malware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Ransomware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Malware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Malware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Malware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Malware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Malware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Malware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Ransomware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Malware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Malware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Malware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Malware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |
| OC\_QA\_RTDB | 192.168.3.248 | Malware | mitigated | malicious | Wonik>0-머트리얼즈>01.서버 |

## 3. 엔진별 탐지



|  |  |
| --- | --- |
| 엔진명 | 탐지수 |
| DBT - Executables | 5 |
| On-Write DFI - Suspicious | 4 |
| On-Write DFI | 2 |
| SentinelOne Cloud | 15 |

## 2. 위협별 탐지



|  |  |
| --- | --- |
| 탐지내역 | 탐지수 |
| etc(Generic.Heuristic, Ransomware, ) | 7 |
| Malware | 17 |