### ENT#4274 CEF 파서 출력 필드 정규화

CEF 파서의 출력 필드에 대해 정규화된 필드 이름과 타입을 적용하였습니다.

사용자 정의 라벨에 공백이 들어간 경우 공백을 underscore(\_)로 치환하여 필드명으로 지정합니다.

파서 생성시 버전을 2로 설정하면 파싱 결과가 정규화된 필드로 출력됩니다. 버전을 설정하지 않고 생성하거나 기존 배포 버전에서 생성한 파서는 정규화가 적용되지 않은 필드가 출력됩니다.



변경되는 필드들은 다음과 같습니다.

|  |  |  |
| --- | --- | --- |
| 변경전 | 변경후 | 타입 |
| src | src\_ip | IP |
| spt | src\_port | INT |
| dst | dst\_ip | IP |
| dpt | dst\_port | INT |
| sourceTranslatedAddress | nat\_src\_ip | IP |
| sourceTranslatedPort | nat\_src\_port | INT |
| destinationTranslatedAddress | nat\_dst\_ip | IP |
| destinationTranslatedPort | nat\_dst\_port | INT |
| dvc | device\_ip | IP |
| dvchost | device\_host | STRING |
| dvcmac | device\_mac | STRING |
| dvcpid | device\_pid | LONG |
| sourceDnsDomain | src\_domain | STRING |
| sourceServiceName | src\_service | STRING |
| destinationDnsDomain | dst\_domain | STRING |
| destinationServiceName | dst\_service | STRING |
| shost | src\_host | STRING |
| smac | src\_mac | STRING |
| dhost | dst\_host | STRING |
| dmac | dst\_mac | STRING |
| suid | src\_user\_id | STRING |
| suser | src\_user | STRING |
| duid | dst\_user\_id | STRING |
| duser | dst\_user | STRING |
| spid | src\_pid | LONG |
| sproc | src\_process | STRING |
| dpid | dst\_pid | LONG |
| dproc | dst\_process | STRING |
| fileCreateTime | file\_ctime | DATE |
| fileModificationTime | file\_mtime | DATE |
| fname | file\_name | STRING |
| filePath | file\_path | STRING |
| fileType | file\_type | STRING |
| fsize | file\_size | LONG |
| fileHash | file\_hash | STRING |
| in | rcvd\_bytes | LONG |
| out | sent\_bytes | LONG |
| proto | protocol | STRING |
| app | app | STRING |
| act | action | STRING |
| cat | category | STRING |
| cnt | event\_count | INT |
| requestMethod | method | STRING |
| requestClientApplication | user\_agent | STRING |