

# EDR

EDR ( )

EDR

( )

API

EDR

EDR Agent

Agent

Agent <https://github.com/tsale/EDR-Telemetry> EDR Github (

| Telemetry Feature Category | Sub-Category               | Carbon Black | Cortex XDR | CrowdStrike | Cybereason | ESET Inspect | Elastic | HarfangLab | LimaCharlie | MDE | Qualys | Sentinel One | Sysmon | Trellix | Trend Micro | WatchGuard |
|----------------------------|----------------------------|--------------|------------|-------------|------------|--------------|---------|------------|-------------|-----|--------|--------------|--------|---------|-------------|------------|
| Process Activity           | Process Creation           | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | Process Termination        | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | Process Access             | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | Image/Library Loaded       | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | Remote Thread Creation     | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
| File Manipulation          | Process Tampering Activity | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | File Creation              | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | File Opened                | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | File Deletion              | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | File Modification          | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
| User Account Activity      | File Renaming              | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | Local Account Creation     | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | Local Account Modification | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | Local Account Deletion     | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | Account Login              | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
| Network Activity           | Account Logoff             | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | TCP Connection             | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | UDP Connection             | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | URL                        | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | DNS Query                  | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
| Hash Algorithms            | File Downloaded            | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | MD5                        | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | SHA                        | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
| Registry Activity          | IMPHASH                    | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | Key/Value Creation         | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | Key/Value Modification     | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |
|                            | Key/Value Deletion         | █            | █          | █           | █          | █            | █       | █          | █           | █   | █      | █            | █      | █       | █           | █          |

EDR EDR

API

API NTAPI ( NtAllocateVirtualMemory) EDR Hooking

Windows PsSetCreateProcessNot

```
NTSTATUS PsSetCreateProcessNotifyRoutineEx(
    [ in] PCREATE_PROCESS_NOTIFY_ROUTINE_EX NotifyRoutine,
    [ in] BOOLEAN Remove
);
```

ETW

Windows (ETW) ETW Agent

Isass EDR LSASS

## EDR

---

Revision #5

Created 1 June 2023 03:05:22 by

Updated 24 March 2024 15:17:35 by unknown