EDR

EDR (　　　　)

EDR

(　　)

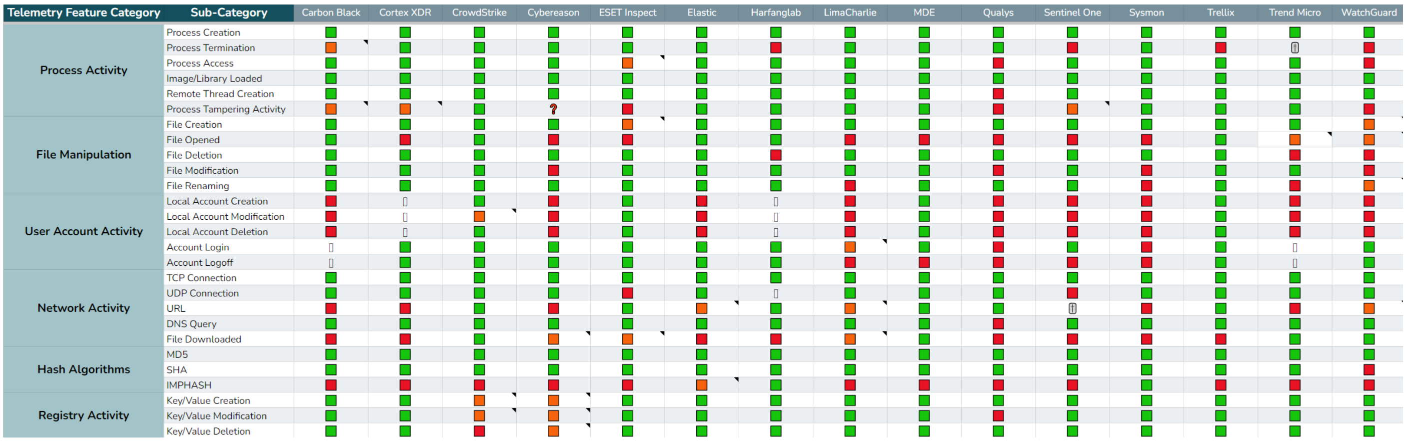
API

EDR

EDR Agent

Agent

Agent https://github.com/tsale/EDR-Telemetry URL) 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	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟩
	Process Tampering Activity	🟧	🟧	🟩	?	🟥	🟩	🟩	🟩	🟩	🟥	🟧	🟩	🟩	🟩	🟥
File Manipulation	File Creation	🟩	🟩	🟩	🟩	🟧	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟧
	File Opened	🟩	🟥	🟩	🟥	🟥	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟩	🟧	🟧
	File Deletion	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥
	File Modification	🟩	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟩	🟥	🟩	🟥	🟩	🟩	🟥
	File Renaming	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟩	🟥	🟩	🟥	🟧
User Account Activity	Local Account Creation	🟥	▯	🟩	🟥	🟩	🟥	▯	🟥	🟩	🟥	🟥	🟥	🟩	🟥	🟥
	Local Account Modification	🟥	▯	🟧	🟥	🟩	🟥	▯	🟥	🟩	🟥	🟥	🟥	🟩	🟥	🟥
	Local Account Deletion	🟥	▯	🟩	🟥	🟩	🟥	▯	🟥	🟩	🟥	🟥	🟥	🟩	🟥	🟥
	Account Login	▯	🟩	🟩	🟩	🟩	🟩	🟩	🟧	🟩	🟥	🟩	🟥	🟩	▯	🟩
	Account Logoff	▯	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟩	▯	🟩
Network Activity	TCP Connection	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	UDP Connection	🟩	🟩	🟩	🟩	🟥	🟩	▯	🟩	🟩	🟩	🟥	🟩	🟩	🟩	🟩
	URL	🟥	🟥	🟩	🟥	🟩	🟧	🟩	🟧	🟩	🟩	▯	🟥	🟩	🟥	🟧
	DNS Query	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟩
	File Downloaded	🟥	🟥	🟩	🟧	🟧	🟥	🟥	🟧	🟩	🟥	🟥	🟥	🟥	🟩	🟩
Hash Algorithms	MD5	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	SHA	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥
	IMPHASH	🟥	🟥	🟥	🟥	🟥	🟧	🟩	🟥	🟥	🟥	🟥	🟩	🟥	🟥	🟥
Registry Activity	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

lsass EDR LSASS

EDR

Revision #5
Created 1 June 2023 03:05:22 by
Updated 24 March 2024 15:17:35 by unknown