Windows

Telemetry	attack-pattern	Telemetry Type
Process monitoring	136	Endpoint
Process command-line parameters	76	Endpoint
File monitoring	68	Endpoint
API monitoring	39	Endpoint
Process use of network	36	Endpoint
Windows Registry	34	Endpoint
Packet capture	32	Network
Authentication logs	24	Endpoint
Netflow/Enclave netflow	24	Network
Windows event logs	19	Endpoint
Network protocol analysis	18	Network
DLL monitoring	17	Endpoint
Binary file metadata	16	Endpoint
Loaded DLLs	12	Endpoint
Malware reverse engineering	8	Endpoint
SSL/TLS inspection	8	Network
Network intrusion detection system	7	Network
Anti-virus	7	Endpoint
System calls	6	Endpoint
Data loss prevention	6	Endpoint-Nerwork
Application logs	5	Endpoint
Host network interface	4	Endpoint
Network device logs	4	Endpoint
Web proxy	4	Network
Windows Error Reporting	4	Endpoint
Kernel drivers	4	Endpoint
Email gateway	4	Network
Third-party application logs	3	Endpoint
Services	3	Endpoint
User interface	3	Endpoint
MBR	2	Endpoint
Web logs	2	Endpoint
BIOS	2	Endpoint
Detonation chamber	2	Endpoint
Mail server	2	Network
Access tokens	1	Endpoint
VBR	1	Endpoint
Browser extensions	1	Endpoint
Disk forensics	1	Endpoint
Component firmware	1	Endpoint
PowerShell logs	1	Endpoint
Web application firewall logs	1	Network
Asset management	1	Network
Sensor health and status	1	Endpoint
Digital certificate logs	1	Endpoint

Environment variable	1	Endpoint
Named Pipes	1	Endpoint
DNS records	1	Network
EFI	1	Endpoint
WMI Objects	1	Endpoint

Endpoint	548
Network	102
Endpoint-Nerwork	6