SECURITY ANALYST CHEATSHEET

QUERY	SYNTAX
HOST/AGENT INFO	
Hostname	`AgentName`
OS	`AgentOS`
Version of Agent	`AgentVersion`
Domain name	`DNSRequest`
Site ID	`SiteId`
Site name	`SiteName`
Account ID	`AccountId`
Account Name	`AccountName`

QUERY	SYNTAX
FILE/REGISTRY INTEGRITY	
File ID	`FileID`
File Name	`FileFullName`
Date and time of file creation	`FileCreatedAt`
MD5	`FileMD5`
Date and time of file change	`FileModifyAt`
SHA1 signature	`FileSHA1`
SHA256 signature	`FileSHA256`
SHA1 of file before it was changed	`OldFileSHA1`
Name of file before rename	`OldFileName`
Identity of file signer	`Publisher`
Signature Status	`Signed Status`
Verification Status	`Verified status`
Why not verified	`Why not verified`
Registry Key Unique ID	`RegistryID`
Full path location of the Registry Key entry	`RegistryPath`

QUERY	SYNTAX
NETWORK DATA	
String: GET, POST, PUT, DELETE	`NetworkMethod`
URL	`NetworkUrl`
DNS response data	`DNSResponse`
IP address of the destination	`DstIP`
Port number of destination	`DstPort`
IP address of traffic source	`SrcIP`
Port number of traffic source	`SrcPort`
Browser type	`Source`

QUERY	SYNTAX
PROCESS TREE	
Process ID	`PID`
PID of the parent process	`ParentPID`
Parent Process	`ParentProcessName`
Time parent process started to run	`ParentProcessStartTime`
Unique ID of parent process	`ParentProcessUniqueKey`
Process command line	`ProcessCmd`
Display name of process	`ProcessDisplayName`
Generated ID of the group of processes, from first parent to last generation (SentinelOne Patent)	`ProcessGroupId`
Pathname of running process	`ProcessImagePath`
SHA1 signature of running process	`ProcessImageSha1Hash`
String: SYSTEM (operating system processes), HIGH (administrators), MEDIUM (non-administrators), LOW (temporary Internet files), UNTRUSTED	`ProcessIntegrityLevel`
Process Name	`ProcessName`
ID of the terminal session of a process	`ProcessSessionId`
Process start time	`ProcessStartTime`
String: SYS_WIN32, SYS_WSL, SUBSYSTEM_UNKNOWN	`ProcessSubSystem`
Unique ID of process	`ProcessUniqueKey`
PID after relinked	`Rpid`
Thread ID	`Tid`
ID of all objects associated with a detection	`TrueContext`
Username	`User`

QUERY	SYNTAX
SCHEDULED TASKS	
Name of a scheduled task	`TaskName`
Full path location of a scheduled task	`TaskPath`
The file who has been executed	`executable file`

HUNTING QUERIES

QUERY	SYNTAX
Net User Add User	ProcessCmd RegExp "net\s+user(?:(?!\s+/add)(?:.|\n))*\s+/add"
Enable SMBv1	processCmd = "REG ADD HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v SMB1 /t REG_DWORD /d 1 /f"
Unusual Schedule Task Created	ProcessCmd ContainsCIS "schtasks" AND processName != "Manages scheduled tasks"
Powershell with Net connections	DstIP Is Not Empty AND ProcessName ContainsCIS "powershell"
Shell Process Creating File	(ProcessName ContainsCIS "windows command processor" OR ProcessName ContainsCIS "powershell") AND FileModifyAt > "Mar 26, 2017 00:00:39"
Shell Process Modify or File	(ProcessName ContainsCIS "windows command processor" OR ProcessName ContainsCIS "powershell") AND (FileModifyAt > "Mar 26, 2017 00:00:10" OR FileCreatedAt > "Mar 26, 2017 00:00:31")
Registry Alteration via Command line	ProcessCmd RegExp "reg\s+add" OR ProcessCmd RegExp "reg\s+del"
svchost.exe running in a unusual user context	processImagePath = "C:\Windows\System32\svchost.exe" AND User != "NT AUTHORITY\SYSTEM" AND User != "NT AUTHORITY\LOCAL SERVICE" AND User != "NT AUTHORITY\NETWORK SERVICE"
Powershell runnning as system user	ProcessName ContainsCIS "powershell" AND User ContainsCIS "SYSTEM"
Powershell Scheduled Tasks Created	ParentProcessName = "Windows PowerShell" AND ProcessName = "Task Scheduler Configuration Tool"
Executable Created	FileCreatedAt > "Apr 2, 2017 00:00:03" AND ProcessName ContainsCIS ".exe"
Suspicious Parent Process svchost.exe	ProcessName ContainsCIS "Host Process for Windows Services" AND ParentProcessName != "Host Process for Windows Services" AND ParentProcessName != "Services and Controller app"
Vulnerable App launching shell	ParentProcessName = "Insert Vulnerable Application name from Applications Tab" AND (ProcessName ContainsCIS "Windows Command Processor" OR ProcessName ContainsCIS "Powershell")
Excel Running Shell or Python	ParentProcessName ContainsCIS "excel" AND (ProcessName ContainsCIS "sh" OR ProcessName ContainsCIS "python")
Whoami	ProcessCmd ContainsCIS "whoami"
Powershell Get Clipboard Entry	processCmd RegExp "powershell\.exe\s+echo\s+Get\-Process\s+|\s+clip"
Powershell Get Running Processes	processCmd ContainsCIS "powershell.exe echo Get-Process"
Powershell Search for Doc Files	processCmd ContainsCIS "powershell Get-ChildItem -Recurse -Include *.doc"
Find string	processCmd ContainsCIS "findstr"
Windows 10 Get Network Adaptor Details	ProcessCmd ContainsCIS "wmic nic"
Execute File in Appdata folder	processCmd ContainsCIS "/FILE" AND ProcessCmd ContainsCIS "Appdata"
Nslookup	ProcessCmd ContainsCIS "nslookup"
Net User Delete User	ProcessCmd RegExp "net\s+user(?:(?!\s+/delete)(?:.|\n))*\s+/delete"
Net User Domain	ProcessCmd RegExp "net\s+user(?:(?!\s+/domain)(?:.|\n))*\s+/domain"
Add user to AD	ProcessCmd ContainsCIS "dsadd user"
Powershell add local user	ProcessCmd ContainsCIS "powershell.exe New-LocalUser"
Powershell upload or download methods	ProcessCmd ContainsCIS "(New-Object Net.Webclient)"
Suspicious - List all SPNs in a Domain	ProcessCmd ContainsCIS "setspn" AND ProcessCmd RegExp "-t" AND ProcessCmd RegExp "-q */*"
list vssadmin shadows	ProcessCmd ContainsCIS "vssadmin.exe list shadows"
Add user or Query local admin group	ProcessCmd ContainsCIS "net localgroup administrators"
Change firewall profile settings	ProcessCmd ContainsCIS "netsh advfirewall"

QUERY	SYNTAX
Clear Windows Event Logs Powershell or Wevtutil	ProcessCmd ContainsCIS "wevtutil cl system" OR ProcessCmd ContainsCIS "Clear-EventLog"
netsh disable firewall	ProcessCmd ContainsCIS "netsh firewall" AND ProcessCmd ContainsCIS "disable"
Query logged in Users	ProcessCmd ContainsCIS "quser"
Qwinsta - Display information Terminal Sessions	ProcessCmd ContainsCIS "qwinsta"
Current Running Processes	ProcessCmd ContainsCIS "tasklist"
Net User - Query a User	ProcessCmd ContainsCIS "net user"
Query Network Shares	ProcessCmd ContainsCIS "net share"
Query Account & Password Policy	ProcessCmd ContainsCIS "net accounts"
Net Config - Query Workstation Current Settings	ProcessCmd ContainsCIS "net config workstation"
Query AD	ProcessCmd ContainsCIS "dsquery"
WMIC user account list	ProcessCmd ContainsCIS "wmic useraccount get" OR ProcessCmd RegExp "wmic useraccount list"
WMIC NT Domain Object Query	ProcessCmd ContainsCIS "wmic ntdomain"
WMIC Group List on Local System	ProcessCmd ContainsCIS "wmic group list"
WMIC List built in System Accounts	ProcessCmd ContainsCIS "wmic sysaccount list"
Reg Query - last 10 files accessed or executed by explorer	ProcessCmd ContainsCIS "RecentDocs" AND ProcessCmd ContainsCIS "REG QUERY" AND ProcessCmd ContainsCIS "explorer"
Reg Query - RunOnce	ProcessCmd ContainsCIS "Runonce" AND ProcessCmd ContainsCIS "REG QUERY"
Reg Query - Check Patterns for Virtual Machines	ProcessCmd ContainsCIS "Reg Query" AND ProcessCmd ContainsCIS "Disk" AND ProcessCmd ContainsCIS "Enum"
Query Group Policy RSOP Data	ProcessCmd ContainsCIS "gpresult"
System Info - windows	ProcessCmd ContainsCIS "systeminfo"
System Info and Network data gathering	ProcessCmd ContainsCIS "systeminfo" OR ProcessCmd RegExp "ver >" OR ProcessCmd RegExp "type\s+%APPDATA%" OR ProcessCmd RegExp "ipconfig" OR ProcessCmd RegExp "net\s+view" OR ProcessCmd RegExp "arp -a" OR ProcessCmd RegExp "netstat"
WMIC Process Get - Process data and sub commands	ProcessCmd RegExp "wmic\s+process\s+get"
WMIC qfe - Gather Windows Patch Data	ProcessCmd ContainsCIS "wmic qfe"
Powershell suspicious commands	ProcessName ContainsCIS "powershell" AND (ProcessCmd ContainsCIS "Invoke-Expression" OR ProcessCmd ContainsCIS "-encodedcommand" OR ProcessCmd ContainsCIS "hidden" OR ProcessCmd ContainsCIS "write-host" OR ProcessCmd ContainsCIS "Get-NetIPConfiguration")
echo command	ProcessCmd ContainsCIS "echo"
regsvr32 and scrobj.dll register-unregister dll	ProcessCmd ContainsCIS "regsvr32" AND ProcessCmd ContainsCIS "scrobj.dll"
regsvr32 suspicious downloads	processName = "Microsoft(C) Register Server" AND DstIP Is Not Empty
regsvr32 suspicious file modification	processName = "Microsoft(C) Register Server" AND FileModifyAt > "Mar 1, 2019 00:00:45"
regsvr32 Persistence	ProcessCmd ContainsCIS "regsvr32" AND (RegistryPath ContainsCIS "machine\software\classes" OR ProcessCmd ContainsCIS "schtasks\s+/create")
Bitsadmin suspicious commands	ProcessCmd ContainsCIS "bitsadmin" AND (ProcessCmd ContainsCIS "transfer" OR ProcessCmd ContainsCIS "download" OR ProcessCmd ContainsCIS ".ps1" OR ProcessCmd ContainsCIS "powershell")
Registry Persistence	ProcessCmd ContainsCIS "reg add" AND (ProcessCmd ContainsCIS "Run" OR ProcessCmd ContainsCIS "Null")
Copy commands	ProcessCmd ContainsCIS "copy" OR ProcessCmd ContainsCIS "xcopy"