S1QL CHEATSHEET FOR SECURITY ANALYSIS

QUERY SUBJECT	SYNTAX
HOST/AGENT INFO	
Hostname	AgentName
OS	AgentOS
Version of agent	AgentVersion
Domain name	DNSRequest
Site token	SiteId
Site name	SiteName
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	Signer
Registry key unique ID	RegistryID
Full path location of the Registry Key entry	RegistryPath
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

QUERY SUBJECT	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
SCHEDULED TASKS	
Name of a scheduled task	TaskName
Full path location of a scheduled task	TaskPath

S1QL CHEATSHEET FOR SECURITY ANALYSIS

QUERY SUBJECT	SYNTAX
HOST/AGENT INFO	
Hostname	AgentName
OS	AgentOS
Version of agent	AgentVersion
Domain name	DNSRequest
Site token	SiteId
Site name	SiteName
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	Signer
Registry key unique ID	RegistryID
Full path location of the Registry Key entry	RegistryPath
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

QUERY SUBJECT	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
SCHEDULED TASKS	
Name of a scheduled task	TaskName
Full path location of a scheduled task	TaskPath

WATCHLIST NAME	QUERY
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 RegExp “schtasks” AND processName != “Manages scheduled tasks”
Powershell with Net connections	DstIP Is Not Empty AND ProcessName RegExp “powershell”
Shell Process Creating File	(ProcessName RegExp “windows command processor” OR ProcessName RegExp “powershell”) AND FileModifyAt > “Mar 26, 2017 00:00:39”
Shell Process Modify or File	(ProcessName RegExp “windows command processor” OR ProcessName RegExp “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 RegExp “powershell” AND User RegExp “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 RegExp “.exe”
Suspicious Parent Process svchost.exe	ProcessName RegExp “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 RegExp “Windows Command Processor” OR ProcessName RegExp “Powershell”)
Excel Running Shell or Python	ParentProcessName RegExp “excel” AND (ProcessName RegExp “sh” OR ProcessName RegExp “python”)
Whoami	ProcessCmd RegExp “whoami”
Powershell Get Clipboard Entry	processCmd RegExp “powershell\.exe\s+echo\s+Get\-Process\s+|\s+clip”
Powershell Get Running Processes	processCmd RegExp “powershell.exe echo Get-Process”
Powershell Search for Doc Files	processCmd Contains “powershell Get-ChildItem -Recurse -Include *.doc”
Find string	processCmd Contains “findstr”

WATCHLIST NAME	QUERY
Windows 10 Get Network Adaptor Details	ProcessCmd RegExp “wmic nic”
Execute File in Appdata folder	processCmd RegExp “/FILE” AND ProcessCmd RegExp “Appdata”
Nslookup	ProcessCmd RegExp “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 Contains “dsadd user”
Powershell add local user	ProcessCmd RegExp “powershell.exe New-LocalUser”
Powershell upload or download methods	ProcessCmd RegExp “(New-Object Net.Webclient)”
Suspicious - List all SPNs in a Domain	ProcessCmd RegExp “setspn” AND ProcessCmd RegExp “-t” AND ProcessCmd RegExp “-q */*”
list vssadmin shadows	ProcessCmd RegExp “vssadmin.exe list shadows”
Add user or Query local admin group	ProcessCmd RegExp “net localgroup administrators”
Change firewall profile settings	ProcessCmd RegExp “netsh advfirewall”
Clear Windows Event Logs Powershell or Wevtutil	ProcessCmd RegExp “wevtutil cl system” OR ProcessCmd RegExp “Clear-EventLog”
Netsh disable firewall	ProcessCmd RegExp “netsh firewall” AND ProcessCmd RegExp “disable”
Query logged in Users	ProcessCmd RegExp “quser”
Qwinsta - Display information Terminal Sessions	ProcessCmd RegExp “qwinsta”
Current Running Processes	ProcessCmd RegExp “tasklist”
Net User - Query a User	ProcessCmd RegExp “net user”
Query Network Shares	ProcessCmd RegExp “net share”
Query Account & Password Policy	ProcessCmd RegExp “net accounts”
Net Config - Query Workstation Current Settings	ProcessCmd RegExp “net config workstation”
Query AD	ProcessCmd RegExp “dsquery”
WMIC user account list	ProcessCmd RegExp “wmic useraccount get” OR ProcessCmd RegExp “wmic useraccount list”
WMIC NT Domain Object Query	ProcessCmd RegExp “wmic ntdomain”

WATCHLIST NAME	QUERY
WMIC Group List on Local System	ProcessCmd RegExp “wmic group list”
WMIC List built in System Accounts	ProcessCmd RegExp “wmic sysaccount list”
Reg Query - last 10 files accessed or executed by explorer	ProcessCmd RegExp “RecentDocs” AND ProcessCmd RegExp “REG QUERY” AND ProcessCmd RegExp “explorer”
Reg Query - RunOnce	ProcessCmd RegExp “Runonce” AND ProcessCmd RegExp “REG QUERY”
Reg Query - Check Patterns for Virtual Machines	ProcessCmd RegExp “Reg Query” AND ProcessCmd RegExp “Disk” AND ProcessCmd RegExp “Enum”
Query Group Policy RSOP Data	ProcessCmd RegExp “gpresult”
System Info - windows	ProcessCmd RegExp “systeminfo”
System Info and Network data gathering	ProcessCmd RegExp “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 RegExp “wmic qfe”
Powershell suspicious commands	ProcessName RegExp “powershell” AND (ProcessCmd RegExp “Invoke-Expression” OR ProcessCmd RegExp “-encodedcommand” OR ProcessCmd RegExp “hidden” OR ProcessCmd RegExp “write-host” OR ProcessCmd RegExp “Get-NetIPConfiguration”)
echo command	ProcessCmd RegExp “echo”
regsvr32 and scrobj.dll register-unregister dll	ProcessCmd RegExp “regsvr32” AND ProcessCmd RegExp “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 RegExp “regsvr32” AND (RegistryPath Contains “machine\software\classes” OR ProcessCmd RegExp “schtasks\s+/create”)
Bitsadmin suspicious commands	ProcessCmd RegExp “bitsadmin” AND (ProcessCmd RegExp “transfer” OR ProcessCmd RegExp “download” OR ProcessCmd RegExp “.ps1” OR ProcessCmd RegExp “powershell”)
Registry Persistence	ProcessCmd RegExp “reg add» AND (ProcessCmd RegExp “Run” OR ProcessCmd RegExp “Null”)
Copy commands	ProcessCmd RegExp “copy” OR ProcessCmd RegExp “xcopy”