Carbon Black Queries for Threat Hunting and Incident Response

1. Suspicious Process Execution

Query: process_name:svchost.exe AND -parent_name:services.exe

Description: This query looks for suspicious instances of svchost.exe being executed without services.exe as the parent. Svchost.exe is commonly used by malware to masquerade as legitimate processes.

2. Unusual Network Connections

Query: netconn_ipv4:<destination_ip> AND -process_name:browser.exe

Description: This query helps identify unusual network connections by processes that typically shouldn't be making network requests. Excluding browser processes helps reduce noise.

3. PowerShell Execution

Query: process_name:powershell.exe AND cmdline:*

Description: PowerShell is frequently abused in attacks. This query looks for PowerShell execution along with the command line to identify potentially malicious scripts.

4. Persistence Mechanisms

Query: regmod_name:HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Description: This query checks for registry modifications where persistence mechanisms could be established. Attackers often add startup items in these locations.

5. In-Memory Injection

Query: modload_name:ntdll.dll AND process_name:notepad.exe

Description: This query searches for DLL injection attempts where malicious code is loaded into legitimate processes like Notepad, which shouldn't normally load ntdll.dll.

6. Suspicious Child Processes

Query: parent_name:explorer.exe AND process_name:cmd.exe

Description: This query looks for cmd.exe being spawned by explorer.exe, which is uncommon and often a sign of exploitation or user action triggering a shell.

7. Malicious File Downloads

Query: netconn_domain:<known_malicious_domain> AND filemod_name:C:*\Downloads*

Description: This query checks for file modifications in the Downloads directory that correspond to network connections with known malicious domains.

8. Uncommon Parent-Child Relationships

Query: process_name:svchost.exe AND -parent_name:services.exe

Description: Looks for processes like svchost.exe being started by an unusual parent process, which could indicate process hollowing or privilege escalation.

9. Known Malware Hashes

Query: filemod_sha256:<malicious_hash>

Description: This query checks if files with known malicious hashes have been observed on the system, allowing quick identification of known threats.

10. Suspicious Script Execution

Query: process_name:python.exe OR process_name:perl.exe

Description: This query looks for scripting languages like Python or Perl that are often used in exploitation or lateral movement attempts.