Microsoft Sentinel Threat Hunting

When hunting for threats in Microsoft Sentinel, it's crucial to focus on detecting anomalous behaviors, suspicious activities, and potential indicators of compromise (IOCs) that could signify a security breach or ongoing attack. Below are some key areas to focus on, along with specific recommendations for what to hunt and what to look out for:

1. Unusual Logon Activities

Hunt for:

- ✓ Multiple Failed Logon Attempts: Indicative of brute force attacks.

```
SecurityEvent
| where EventID == 4625  // Failed logon event
| summarize FailedAttempts = count() by Account, IpAddress, bin(TimeGenerated, 1h)
| where FailedAttempts > 10  // More than 10 failed attempts within an hour
| sort by FailedAttempts desc
```

- ✓ Logons from Unusual Locations: Logins from unexpected geographic locations could signal compromised accounts.

```
SecurityEvent
| where EventID == 4624  // Successful logon event
| summarize LatestLogon = max(TimeGenerated) by Account, IpAddress
| join kind=inner (
   Geolocation
   | summarize Locations = count() by Account, Country
) on Account
| where Country != "ExpectedCountry"  // Replace with expected country
```

- ✓ Impossible Travel: Logons from different locations within a timeframe that's physically impossible.

```
SecurityEvent
| where EventID == 4624  // Successful logon event
| project Account, IpAddress, TimeGenerated
| sort by Account, TimeGenerated
| extend PreviousTime = prev(TimeGenerated), PreviousIP = prev(IpAddress)
| extend TimeDiff = datetime_diff('minute', TimeGenerated, PreviousTime)
| where TimeDiff > 0 and TimeDiff < 60  // Logons within 60 minutes
| where IpAddress != PreviousIP
```

- ✓ Logon at Unusual Hours: Users logging in at odd hours, especially outside their regular patterns.

```
SecurityEvent
| where EventID == 4624  // Successful logon event
| extend Hour = datetime_part("hour", TimeGenerated)
| where Hour < 6 or Hour > 18  // Logons outside of business hours (e.g., 6 AM - 6 PM)
| summarize LogonCount = count() by Account, Hour
| sort by LogonCount desc
```

Look Out for:

- ✓ Account lockouts.
- ✓ Repeated failed logon attempts followed by a successful logon.
- ✓ Logons using service accounts or privileged accounts outside of maintenance windows.

2. Process Creation and Execution

Hunt for:

- ✓ Execution of Suspicious Processes: Look for processes associated with known malicious activities (e.g., powershell.exe, cmd.exe spawning unusual processes).

```
SecurityEvent
| where EventID == 4688  // Process creation event
| where ProcessName in ("powershell.exe", "cmd.exe", "wmic.exe", "psexec.exe")
| project TimeGenerated, Account, ProcessName, CommandLine, ParentProcessName
| sort by TimeGenerated desc
```

- ✓ Processes Running from Unexpected Locations: Executables running from temp folders or user profiles.

```
SecurityEvent
| where EventID == 4688  // Process creation event
| where ProcessName endswith ".exe" and not(ExecutablePath startswith "C:\\Program Files" or
ExecutablePath startswith "C:\\Windows")
| project TimeGenerated, Account, ExecutablePath, ProcessName, CommandLine
```

- ✓ Newly Installed Applications or Scripts: Especially those that are unsigned or not commonly used within the environment.

```
SecurityEvent
| where EventID == 4688  // Process creation event
| where ProcessName endswith ".exe" or ProcessName endswith ".ps1" or ProcessName endswith ".bat"
| where ProcessName !contains "Signed"  // Look for unsigned executables or scripts
| project TimeGenerated, Account, ProcessName, CommandLine, ParentProcessName
| sort by TimeGenerated desc
```

Look Out for:

- ✓ High privilege process executions (e.g., wmic.exe, psexec.exe).
- ✓ Processes initiating network connections, especially to uncommon or suspicious destinations.
- ✓ Unauthorized use of remote execution tools (e.g., PsExec, PowerShell remoting).

3. Lateral Movement

Hunt for:

- ✓ Unauthorized RDP Sessions: Look for lateral movement using Remote Desktop Protocol (RDP).

```
SecurityEvent
| where EventID == 4624  // Successful logon event
| where LogonType == 10  // RDP logon
| summarize RDPLogons = count() by Account, IpAddress, bin(TimeGenerated, 1h)
| where RDPLogons > 5  // More than 5 RDP logons within an hour
```

- ✓ Pass-the-Hash and Pass-the-Ticket Attacks: Identify patterns indicating credential theft and reuse.

```
SecurityEvent
| where EventID in (4624, 4672)  // Logon and special privileges assigned
| where AuthenticationPackageName in ("NTLM", "Kerberos")
| extend LogonTime = TimeGenerated, TargetAccount = Account
| project LogonTime, TargetAccount, AuthenticationPackageName, IpAddress, LogonType
| join kind=inner (
   SecurityEvent
   | where EventID == 4672  // Special privileges assigned
   | project PrivilegeTime = TimeGenerated, Account, Privileges
) on $left.TargetAccount == $right.Account
| where PrivilegeTime between (LogonTime .. LogonTime + 10m)
// Privileges assigned within 10 minutes of logon
| sort by LogonTime desc
```

- ✓ WMI or SMB-Based Lateral Movement: Detect suspicious use of Windows Management Instrumentation (WMI) or Server Message Block (SMB) for lateral movement.

```
SecurityEvent
| where EventID == 4688  // Process creation event
| where ProcessName in ("wmiprvse.exe", "wmic.exe", "svchost.exe")
| project TimeGenerated, Account, ProcessName, CommandLine, TargetMachine
| join kind=inner (
   SecurityEvent
   | where EventID == 5140  // Network share object accessed (SMB traffic)
   | project SMBTime = TimeGenerated, Account, ShareName, IpAddress
) on $left.Account == $right.Account and TargetMachine == IpAddress
| where SMBTime between (TimeGenerated .. TimeGenerated + 5m)
| sort by TimeGenerated desc
```

Look Out for:

- ✓ Use of admin shares (e.g., C$, ADMIN$) for file copying.
- ✓ Accounts logging into multiple machines in a short timeframe.
- ✓ High volume of network traffic between servers not typically communicating.

4. Privilege Escalation

Hunt for:

- ✓ Newly Added Users to Privileged Groups: Monitor changes to Active Directory groups, especially those granting administrative privileges.

```
SecurityEvent
| where EventID == 4728 or EventID == 4732  // User added to privileged group
| project TimeGenerated, TargetUserName, MemberName, GroupName
| where GroupName contains "Admins"  // Look for admin groups
```

- ✓ Use of Built-in Administrator Accounts: Especially if not commonly used in daily operations.

```
SecurityEvent
| where EventID == 4624  // Successful logon event
| where Account in ("Administrator", "Admin")
| project TimeGenerated, Account, IpAddress, LogonType
| sort by TimeGenerated desc
```

- ✓ Attempts to Disable Security Controls: Actions like disabling antivirus, tampering with security settings, or stopping security services.

```
SecurityEvent
| where EventID == 4688  // Process creation event
| where ProcessName in ("msconfig.exe", "sc.exe", "powershell.exe")
| where CommandLine contains "disable" or CommandLine contains "stop" or CommandLine contains "uninstall"
| project TimeGenerated, Account, ProcessName, CommandLine
| sort by TimeGenerated desc
```

Look Out for:

- ✓ Execution of commands like net localgroup administrators.
- ✓ Unusual modifications to Group Policy Objects (GPOs) or security policies.
- ✓ Sudden elevation of privileges for non-admin accounts.

5. Suspicious Network Traffic

Hunt for:

- ✓ Data Exfiltration: Look for large outbound data transfers, especially to uncommon destinations.

```
AzureDiagnostics
| where ResourceType == "NETWORKSECURITYGROUPS"
| where Direction == "Outbound" and Action == "Allow"
| summarize TotalBytes = sum(TotalBytesTransferred) by DestinationIP, bin(TimeGenerated, 1h)
| where TotalBytes > 1000000000  // More than 1 GB transferred within an hour
| sort by TotalBytes desc
```

- ✓ Unusual DNS Queries: DNS requests to suspicious or rarely used domains, or domains known for phishing/malware.

```
DnsEvents
| where QueryType == "A"  // DNS A record lookup
| where QueryName endswith ".xyz" or QueryName contains "maliciousdomain"
| project TimeGenerated, QueryName, ClientIP
| sort by TimeGenerated desc
```

- ✓ Internal Reconnaissance: Traffic patterns suggesting internal network scanning or probing.

```
AzureDiagnostics
| where ResourceType == "NETWORKSECURITYGROUPS"
| where Direction == "Inbound" and Action == "Allow"
| summarize Probes = count() by SourceIP, DestinationIP, DestinationPort, bin(TimeGenerated, 1m)
| where Probes > 10  // More than 10 connections within a minute
| sort by Probes desc
```

Look Out for:

- ✓ Outbound traffic to known malicious IPs or domains.
- ✓ Unencrypted sensitive data being sent over the network.
- ✓ Lateral movement attempts via unusual ports or protocols.

6. Suspicious File Activities

Hunt for:

- ✓ File Access by Unauthorized Users: Monitor critical file shares or sensitive data access by non-privileged users.

```
FileAuditLogs
| where EventID == 4663  // File access event
| where ObjectName contains "sensitive" or ObjectName contains "confidential"
| project TimeGenerated, Account, ObjectName, Accesses
| sort by TimeGenerated desc
```

- ✓ Creation of New Executables in Unusual Locations: Especially in system directories or user profiles.

```
SecurityEvent
| where EventID == 4688  // Process creation event
| where ProcessName endswith ".exe"
| where not(ExecutablePath startswith "C:\\Program Files" or ExecutablePath startswith "C:\\Windows")
| project TimeGenerated, Account, ExecutablePath, ProcessName, CommandLine
| sort by TimeGenerated desc
```

- ✓ Mass File Deletion or Modification: Could indicate ransomware activity.

```
SecurityEvent
| where EventID == 4660  // File deleted
| summarize Deletions = count() by Account, bin(TimeGenerated, 1h)
| where Deletions > 100  // More than 100 deletions within an hour
| sort by Deletions desc
```

Look Out for:

- ✓ Files being accessed or modified outside of business hours.
- ✓ Unexpected encryption or compression of large volumes of files.
- ✓ Sudden surge in file write operations on critical systems.

7. Persistence Mechanisms

Hunt for:

- ✓ Registry Modifications: Look for changes in autostart locations in the Windows Registry (e.g., HKLM\Software\Microsoft\Windows\CurrentVersion\Run).

```
SecurityEvent
| where EventID == 4657  // Registry value change
| where ObjectName startswith "HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run"
| project TimeGenerated, Account, ObjectName, NewValue
| sort by TimeGenerated desc
```

- ✓ Scheduled Tasks or Services: Newly created or modified scheduled tasks or services that may be used for persistence.

```
SecurityEvent
| where EventID == 4698 or EventID == 7045  // Scheduled task created or service installed
| project TimeGenerated, Account, ServiceName, TaskName, CommandLine
| sort by TimeGenerated desc
```

- ✓ Startup Folder Modifications: Files placed in startup folders to ensure execution on boot.

```
SecurityEvent
| where EventID == 4663  // File accessed
| where ObjectName contains "C:\\Users\\" and ObjectName contains "\\Startup\\"
| project TimeGenerated, Account, ObjectName, Accesses
| sort by TimeGenerated desc
```

Look Out for:

- ✓ Creation of hidden tasks or services.
- ✓ Backdoor creation or use of DLL hijacking for persistence.
- ✓ Modifications to system files or drivers.

8. Suspicious Email Activity

Hunt for:

- ✓ Phishing Emails: Identify emails with suspicious attachments, links, or unusual sender domains.

```
OfficeActivity
| where Operation == "Send" and ItemType == "Phishing"
| project TimeGenerated, Sender, Recipient, Subject, Url
| sort by TimeGenerated desc
```

- ✓ Email Forwarding Rules: Automatic forwarding of emails to external domains could indicate account compromise.

```
OfficeActivity
| where Operation == "Set-MailboxAutoReplyConfiguration" or Operation == "Set-InboxRule"
| project TimeGenerated, UserId, ForwardingSmtpAddress, AutoReplyState
| where ForwardingSmtpAddress != "" or AutoReplyState == "Enabled"
```

- ✓ Mass Mailing: Outbound emails sent in bulk by compromised accounts.

```
OfficeActivity
| where Operation == "Send" and ItemType == "Message"
| summarize SentEmails = count() by UserId, bin(TimeGenerated, 1h)
| where SentEmails > 100  // More than 100 emails sent within an hour
| sort by SentEmails desc
```

Look Out for:

- ✓ Sudden surge in email activity from a single user.
- ✓ Emails containing executables, macros, or other potentially malicious content.
- ✓ External communication with known phishing domains.

9. Security Solution Evasion

Hunt for:

- ✓ Disabling or Uninstalling Security Tools: Monitor for actions that attempt to disable antivirus, firewalls, or endpoint detection and response (EDR) solutions.

```
SecurityEvent
| where EventID == 4688  // Process creation event
| where ProcessName in ("msconfig.exe", "sc.exe", "powershell.exe")
| where CommandLine contains "disable" or CommandLine contains "uninstall"
| project TimeGenerated, Account, ProcessName, CommandLine
| sort by TimeGenerated desc
```

- ✓ Tampering with Logs: Look for attempts to clear or manipulate security event logs.

```
SecurityEvent
| where EventID == 1102  // Security log cleared
| project TimeGenerated, Account
| sort by TimeGenerated desc
```

- ✓ Bypassing Multi-Factor Authentication (MFA): Monitor for MFA bypass attempts or anomalous MFA prompts.

```
SigninLogs
| where ResultDescription == "MFA denied" or AuthenticationRequirement == "MFARequired" and Status has "Success"
| project TimeGenerated, UserPrincipalName, Status, AuthenticationRequirement, AuthenticationMethod, ConditionalAccessPolicies
| sort by TimeGenerated desc
```

Look Out for:

- ✓ Unusual changes to security configurations or policies.
- ✓ Gaps in security logging or sudden absence of expected log entries.
- ✓ Repeated login attempts without the expected MFA challenge.

10. Suspicious PowerShell or Scripting Activities

Hunt for:

- ✓ PowerShell Executions: Monitor for execution of PowerShell scripts, especially those involving base64 encoded commands or downloading files from the internet.

```
SecurityEvent
| where EventID == 4688  // Process creation event
| where ProcessName == "powershell.exe"
| where CommandLine contains "Invoke-WebRequest" or CommandLine contains "IEX"
| project TimeGenerated, Account, CommandLine
| sort by TimeGenerated desc
```

- ✓ Batch Scripts: Unusual usage of batch scripts (.bat files) for system changes or network access.

```
SecurityEvent
| where EventID == 4688  // Process creation event
| where ProcessName endswith ".bat"
| project TimeGenerated, Account, ProcessName, CommandLine, ParentProcessName
| sort by TimeGenerated desc
```

- ✓ Scripting Languages: Use of Python, Perl, or other scripting languages in environments where they are not common.

```
SecurityEvent
| where EventID == 4688  // Process creation event
| where ProcessName in ("python.exe", "perl.exe", "ruby.exe")
| project TimeGenerated, Account, ProcessName, CommandLine, ParentProcessName
| sort by TimeGenerated desc
```

Look Out for:

- ✓ PowerShell commands involving Invoke-WebRequest, Invoke-Expression, or IEX.
- ✓ Scripts attempting to connect to external IP addresses.
- ✓ Use of scripting tools by non-developers or users without a clear business need.