■■ KQL + Microsoft Defender EDR 28■Day Analyst Lab (Weeks 1–3)

■ Week 1 — Baselines & Core KQL

Purpose: Learn Defender tables and establish what normal endpoint behavior looks like.

Day 1 – Process Telemetry Familiarization

Purpose: Understand raw process execution telemetry and early investigation techniques.

```
DeviceProcessEvents
| take 30

DeviceProcessEvents
| project Timestamp, DeviceName, FileName
| take 30
```

Day 2 – Time■Based Scoping

Purpose: Reduce noise by narrowing telemetry to relevant time windows.

```
DeviceProcessEvents
| where Timestamp > ago(24h)

DeviceProcessEvents
| where Timestamp > ago(1h)
```

Day 3 – Baseline: What Runs Normally

Purpose: Identify commonly executed processes across hosts.

```
DeviceProcessEvents
| summarize Count=count() by FileName
| order by Count desc

DeviceProcessEvents
| summarize Count=count() by DeviceName
```

Day 4 – Suspicious Process Awareness

Purpose: Spot high■risk binaries frequently abused by attackers.

```
DeviceProcessEvents
| where FileName == "powershell.exe"

DeviceProcessEvents
| where FileName == "cmd.exe"
```

Day 5 – Execution Context Matters

Purpose: Understand parent processes, users, and command■line context.

```
DeviceProcessEvents
| project Timestamp, DeviceName, FileName, ProcessCommandLine

DeviceProcessEvents
| project FileName, ParentProcessName, AccountName
```

Day 6 – Sorting for Signal

Purpose: Prioritize events during triage using time ordering.

```
DeviceProcessEvents
| order by Timestamp desc

DeviceProcessEvents
| order by Timestamp asc
```

Day 7 – Clean Host Baseline

Purpose: Establish known■good behavior on a clean Windows 10 system.

```
DeviceProcessEvents
| where DeviceName == "WIN10-CLEAN"
| summarize Count=count() by FileName
| order by Count desc

DeviceProcessEvents
| where DeviceName == "WIN10-CLEAN"
| project FileName, ProcessCommandLine
```

■ Week 2 — Deviations & Attacker Tradecraft

Purpose: Detect deviations from baseline and recognize attacker behaviors.

Day 8 – Command■Line Threat Indicators

Purpose: Identify malicious command■line patterns.

```
DeviceProcessEvents
| where ProcessCommandLine contains "http"

DeviceProcessEvents
| where ProcessCommandLine contains "-enc"
```

Day 9 – Keyword■Based Hunting

Purpose: Use keyword logic to detect PowerShell abuse.

```
DeviceProcessEvents
| where ProcessCommandLine has "Invoke-"

DeviceProcessEvents
| where ProcessCommandLine has "FromBase64String"
```

Day 10 – Script & Payload Detection

Purpose: Detect script■based execution.

```
DeviceProcessEvents
| where ProcessCommandLine endswith ".ps1"

DeviceProcessEvents
| where ProcessCommandLine endswith ".bat"
```

Day 11 – Parent / Child Abuse

Purpose: Identify malicious execution chains.

```
DeviceProcessEvents
| where ParentProcessName in~ ("winword.exe","excel.exe","outlook.exe")
```

```
| where FileName in~ ("powershell.exe","cmd.exe","wscript.exe","mshta.exe")

DeviceProcessEvents
| where FileName == "powershell.exe" and ProcessCommandLine contains "-enc"
```

Day 12 – Living■off■the■Land Binaries

Purpose: Detect abuse of legitimate system binaries.

```
DeviceProcessEvents
| where FileName in ("powershell.exe","mshta.exe","rundll32.exe","regsvr32.exe")

DeviceProcessEvents
| where FileName in ("wscript.exe","cscript.exe")
```

Day 13 – Rare Process Hunting

Purpose: Identify low■frequency executions.

```
DeviceProcessEvents
| summarize Hosts=dcount(DeviceName), Events=count() by FileName
| order by Hosts asc, Events asc

DeviceProcessEvents
| summarize count() by FileName
| order by count_ asc
```

Day 14 – User Behavior Deviations

Purpose: Detect unusual user activity patterns.

```
DeviceProcessEvents
| summarize count() by AccountName

DeviceProcessEvents
| summarize count() by AccountName, FileName
```

■ Week 3 — Correlation & Analyst Thinking

Purpose: Correlate telemetry across tables like a real threat hunter.

Day 15 – Network Telemetry Awareness

Purpose: Understand outbound network visibility.

```
DeviceNetworkEvents
| take 30

DeviceNetworkEvents
| project Timestamp, DeviceName, RemoteIP, RemotePort
```

Day 16 – Suspicious Egress Traffic

Purpose: Identify suspicious outbound connections.

```
DeviceNetworkEvents
| where RemoteIPType == "Public"

DeviceNetworkEvents
| summarize count() by RemotePort
```

Day 17 – File Drop Detection

Purpose: Detect payload staging.

```
DeviceFileEvents
| where ActionType == "FileCreated"
| where FolderPath has_any ("\\AppData","\\Temp","\\Users\\Public","\\ProgramData")

DeviceFileEvents
| summarize count() by FolderPath
```

Day 18 – Authentication Sanity Checks

Purpose: Identify suspicious authentication behavior.

```
DeviceLogonEvents
| summarize count() by DeviceName, AccountName, LogonType

DeviceLogonEvents
| where ActionType == "LogonFailed"
```

Day 19 – Time■Based Behavior Patterns

Purpose: Detect abnormal bursts of activity.

```
DeviceProcessEvents
| summarize count() by bin(Timestamp, 30m)

DeviceNetworkEvents
| summarize count() by bin(Timestamp, 1h)
```

Day 20 – Cross■Table Correlation

Purpose: Correlate process and network activity to confirm malicious behavior.

Day 21 – Analyst Confidence Day

Purpose: Independently hunt, optimize queries, and explain findings.