🟢 WEEK 1 — BASELINES & CORE KQL

🗓️ Day 1 — Process Telemetry Familiarization 🔍

- **Endpoint Telemetry:** Data collected from endpoint devices such as processes, network connections, file activity, and logons.
- **Process Execution:** The act of a program or executable running on a system.

Technology Breakdown

- **MDE (Microsoft Defender for Endpoint):** Microsoft's EDR platform that continuously collects endpoint telemetry.
- Process execution data is stored in the **DeviceProcessEvents** table.

Why This Matters

- Threat hunting starts with understanding raw data before alerts ever exist.

🗓️ Day 2 — Time-Based Scoping ⏱️

- **Time Scoping:** Limiting telemetry to a defined time window.
- **Telemetry Noise:** High volumes of benign events that obscure threats.

Technology Breakdown

- MDE timestamps all events in UTC.
- **KQL (Kusto Query Language)** allows filtering events using relative time (for example, last hour vs last day).

Why This Matters

- Most investigations start with *when* something happened.

🗓️ Day 3 — Baseline: What Runs Normally 📊

- **Baseline:** A statistical picture of normal behavior in an environment.
- **Frequency Analysis:** Measuring how often an event occurs.

Technology Breakdown

- MDE logs *all* executions, not just malicious ones.
- Analysts use aggregation to identify what is common vs uncommon.

Why This Matters

- You can't label activity suspicious without knowing what normal looks like.

🗓️ Day 4 — Suspicious Process Awareness ⚠️

- **Scripting Engine:** A program that executes interpreted commands (example: PowerShell).
- **Dual-Use Tool:** Legitimate software commonly abused by attackers.

Technology Breakdown

- PowerShell and CMD are core Windows utilities heavily abused in attacks.
- MDE captures execution context even for trusted binaries.

Why This Matters

- Modern attackers rely on built-in tools to evade detection.

🗓️ Day 5 — Execution Context Matters 🧠

- **Command Line:** The full set of arguments used to start a process.
- **Parent Process:** The process that launched another process.

Technology Breakdown

- MDE tracks process lineage (parent → child relationships).
- Context often reveals malicious intent even when tools are legitimate.

Why This Matters

- The same process can be benign or malicious depending on how it was launched.

🗓️ Day 6 — Sorting for Signal 🧹

- **Triage:** Quickly prioritizing events for investigation.
- **Recency:** Giving priority to newer activity during active incidents.

Technology Breakdown

- Analysts sort data constantly to surface relevant events first.

Why This Matters

- SOC analysts rarely read logs sequentially — they prioritize.

🗓️ Day 7 — Clean Host Baseline 📏

- **Known-Good Host:** A system assumed to be clean and uncompromised.
- **Comparative Analysis:** Comparing one system's behavior to another.

Technology Breakdown

- Clean VMs act as control systems in cyber ranges.

Why This Matters

- Baselines reduce false positives in noisy environments.

🟡 WEEK 2 — DEVIATIONS & ATTACKER TRADECRAFT

🗓️ Day 8 — Command-Line Threat Indicators 🚩

- **Threat Indicator:** A pattern commonly associated with malicious behavior.
- **Obfuscation:** Hiding intent to evade detection.

Technology Breakdown

- Attackers often retrieve payloads via HTTP/S.
- Encoded commands are frequently used in PowerShell attacks.

Why This Matters

- Command lines often expose attacker intent directly.

🗓️ Day 9 — Keyword-Based Hunting 🧩

- **Keyword Matching:** Searching for strings strongly associated with attacks.

Technology Breakdown

- PowerShell attack frameworks reuse common functions and verbs.

Why This Matters

- Keyword hunting is a foundational SOC detection technique.

🗓️ Day 10 — Script & Payload Detection 📜

- **Script Execution:** Running interpreted code instead of compiled binaries.
- **Payload:** Malicious code delivered to a system.

Technology Breakdown

- Scripts are easy to modify and hard to signature-detect.

Why This Matters

- Script-based attacks dominate initial access techniques.

🗓️ Day 11 — Parent / Child Abuse 💉

- **Process Chain:** Sequence of processes spawned during execution.

Technology Breakdown

- Office applications should not spawn command shells.

Why This Matters

- Office-to-script execution is one of the highest-signal detections.

🗓️ Day 12 — Living-off-the-Land Binaries (LOLBins) 🧰

- **LOLBin:** Legitimate OS binary abused for malicious purposes.

Technology Breakdown

- LOLBins are trusted and digitally signed, making detection harder.

Why This Matters

- Attackers prefer abusing trusted tools over dropping malware.

🗓️ Day 13 — Rare Process Hunting 🎯

- **Outlier:** Activity that significantly deviates from the baseline.

Technology Breakdown

- Rare processes often indicate custom malware or misuse.

Why This Matters

- Rarity is one of the strongest hunting signals.

🗓️ Day 14 — User Behavior Deviations 🕵️‍♀️

- **Behavioral Deviation:** Activity inconsistent with a user's normal behavior.

Technology Breakdown

- MDE ties process execution to user identities.

Why This Matters

- Credential compromise often appears here first.

🟠 WEEK 3 — CORRELATION & ANALYST THINKING

🗓️ Day 15 — Network Telemetry Awareness 🌐

- **Egress Traffic:** Outbound network traffic from a device.

Technology Breakdown

- MDE logs per-process network connections.

Why This Matters

- Malware must communicate externally to operate.

🗓️ Day 16 — Suspicious Egress Traffic 🚨

- **Beaconing:** Periodic outbound connections to attacker infrastructure.

Technology Breakdown

- Public IP connections provide stronger investigation signals.

Why This Matters

- Network activity validates endpoint suspicions.

🗓️ Day 17 — File Drop Detection 📂

- **Payload Drop:** Writing malicious files to disk.

Technology Breakdown

- Common attacker directories include AppData and Temp.

Why This Matters

- Disk artifacts enable deeper forensics and remediation.

🗓️ Day 18 — Authentication Sanity Checks 🔐

- **Logon Type:** Method used to authenticate (interactive, service, remote).
- **Credential Abuse:** Unauthorized use of valid credentials.

Technology Breakdown

- MDE captures authentication activity across endpoints.

Why This Matters

- Identity is the new perimeter.

🗓️ Day 19 — Time-Based Behavior Patterns ⏳

- **Burst Activity:** Sudden spike in events over a short period.

Technology Breakdown

- Automated tools produce consistent, repetitive patterns.

Why This Matters

- Humans are inconsistent — malware is predictable.

🗓️ Day 20 — Cross-Table Correlation 🔗

- **Correlation:** Linking related events across multiple telemetry sources.

Technology Breakdown

- MDE allows process, network, file, and logon data to be joined.

Why This Matters

- Single events lie; correlated evidence doesn't.

🗓️ Day 21 — Analyst Confidence Day 🧠

- **Threat Hunt:** Proactive search for adversary activity without alerts.
- **Hypothesis-Driven Hunting:** Starting with a question or suspicion.

Technology Breakdown

- Mature SOCs hunt continuously, not just react to alerts.

Why This Matters

- This is where you stop running queries and start thinking like an analyst.

📌 Acronym Glossary (Used Throughout the Lab)

- **EDR:** Endpoint Detection and Response
- **MDE:** Microsoft Defender for Endpoint
- **KQL:** Kusto Query Language
- **SOC:** Security Operations Center
- **VM:** Virtual Machine
- **UTC:** Coordinated Universal Time
- **LOLBins:** Living-off-the-Land Binaries
- **HTTP/S:** Hypertext Transfer Protocol (Secure)