You are an expert threat hunter and Microsoft Sentinel analyst.

Given the cybersecurity threat intelligence report below, perform the following:

Extract key attack phases, TTPs, and IOCs (domains, IPs, file hashes, emails, malware names).

Create detailed SIEM Security Use Cases describing what to detect, triggers (logs/events), and map to MITRE ATT&CK techniques.

For each IOC category and use case, generate multiple actionable Microsoft Sentinel KQL queries that:

Match specific IOCs

Detect anomalous or suspicious behavior related to the threat

Use multiple Microsoft Sentinel tables/log sources (SigninLogs, AuditLogs, AADNonInteractiveUserSignInLogs, AADServicePrincipalSignInLogs, SecurityAlert, SecurityIncident, DeviceEvents, DeviceNetworkEvents, DeviceFileEvents, DeviceProcessEvents, DeviceRegistryEvents, DeviceImageLoadEvents, DeviceLogonEvents, CommonSecurityLog, Syslog, DnsEvents, VMConnection, OfficeActivity, EmailEvents, EmailUrlInfo, EmailAttachmentInfo, AzureActivity, AzureDiagnostics, AppTraces, AppRequests, AppDependencies, Heartbeat, Perf, Update, WireData, etc.)

Include threshold-based or time-windowed detections (e.g., multiple failed logins or DNS queries within short time)

Correlate different event types or IOC categories where relevant

Detect living-off-the-land or stealth techniques (e.g., SSH enabling, reverse shell, abnormal process execution)

Only include queries that are directly runnable in Microsoft Sentinel. If a category has no IOCs, return "null" for that category.

Format the output as:

SIEM Security Use Cases:

[Use Case Name]

Description: ...

Trigger: ...

MITRE: ...

KQL Queries

Domains/URLs:

<query 1>

<query 2>

...

IP Addresses:

<query 1>

<query 2>

...

File Hashes (SHA256):

<query 1>

...

Email Addresses:

...

Malware/Exploits:

...

Here is the threat intelligence: {{ $json.cleaned\_text }}