Forensisches Playbook – Microsoft Defender for Endpoint

Vorbedingungen / Verantwortlichkeiten

- Berechtigungen im MDE-Portal sicherstellen (Security Reader/Responder/Contributor).
- Rechtliche Rahmenbedingungen vorab klären (Legal Hold, Datenschutz).
- Zugriff auf security.microsoft.com, PowerShell, Hash-Tools sicherstellen.
- Untersuchungsprotokoll mit Case-ID und Zeitstempeln (UTC) sofort starten.

Schritt 0 — Sofortmaßnahmen

- Gerät isolieren (Defender > Geräteseite > 'Gerät isolieren').
- Jeden Schritt mit Zeitstempel ins Untersuchungsprotokoll eintragen.
- Kommunikation: SOC, IT, Legal informieren.

Teil 1 — Incident-Dashboard

- Portal öffnen (https://security.microsoft.com) → Vorfälle.
- Attack Story sichern (Screenshot/PDF, alle Knoten aufklappen).
- Assets & Evidence sichern (CSV/JSON exportieren, Screenshots optional).

Teil 2 — Geräte-Timeline

- Zeitraum definieren (z.B. 24h vor/nach erstem Alarm).
- Filter nutzen (ProcessCreated, NetworkConnection, FileCreated etc.).
- Timeline exportieren (CSV/JSON), Hashwert berechnen und dokumentieren.

Teil 3 — Investigation Package

- Investigation Package im Portal anfordern (mit Begründung).
- ZIP herunterladen, sinnvoll benennen, SHA256 berechnen.
- Paket enthält Prefetch, Amcache, Prozesse, Netzwerke, Logs etc.

Teil 4 — Advanced Hunting

- IOCs identifizieren (Hash, Domain, IP, CommandLine).
- KQL-Abfragen in Advanced Hunting ausführen.
- Ergebnisse als CSV exportieren, Hash berechnen, dokumentieren.

Chain-of-Custody

- Jede Datei mit Case-ID, Hash, Quelle, Speicherort und Verantwortlichem dokumentieren.
- Originale schreibgeschützt aufbewahren, Arbeitskopien separat halten.

Abschlussbericht

- Executive Summary, Methodik, Timeline, IOCs, Beweisverzeichnis, Empfehlungen.
- Anhänge: CSVs, Screenshots, Queries, Chain-of-Custody-Protokoll.

Quick Checklist

Aktion	Erledigt (✓/✗)	Bemerkung
Gerät isoliert		
Untersuchungsprotokoll gestartet		
Attack Story gesichert		
Timeline exportiert & gehasht		
Investigation Package gesammelt & gehasht		
Advanced Hunting Queries ausgeführt & exportiert		
Chain-of-Custody dokumentiert		
Abschlussbericht erstellt		