Safe Mode OFF
↳ labs after review ON
automatic Deployment
↳ Incognito (Guest apply)

Malware Analysis → Diff workstation. (IR panel)
① Alert ⑥ Persist
② Containm. ⑦ Close
③ Acquisition
④ C&C ⑤ Lateral mov.
→ ② Containment before acquisition

① Alert → Crowdstrike → Suspicious Process → abcd.exe
② Alert details → Parent Process → Powershell.
First Indicator
② File → Hash → Certutil.exe (MD5)
④ Virus total → security flags →
⑤ which type of malware.
⑥ Sand box → to open a file → ext. → hex editor → File
header (MZ) (exe
⑦ Header → Base64 → Decode
⑧ → Nature of Malware type (Ransomware, RAT?) → what type
↳ C&C, latera
Persistence
⑨ Device → forensic acquisitions
① Snapshot of sys → full image acquisition
② Metadata collection → memory → (Page file?)
some artifact.
③ Disk acquisition
↳ Reg files
Sys32 files
Prefetch → Files executed in sys → entry in sys
Mft → Master file table. → MAC B (time
USN journal → File modification data
copy of