Ransomware Incident Response Playbook: LockBit 3.0 Kill Chain

Objective: To provide comprehensive, validated detection coverage and a structured, multi-stage response procedure for a full ransomware kill chain (Initial Access through Impact).

Adversary Campaign: LockBit 3.0 Style (as simulated in the lab report)

1. Detection and Triage Stages

This table outlines the high-priority detection queries that trigger an alert and the immediate steps to validate the threat.

Stage	MITRE Tactic	High-Fidelity Detection Trigger (Based on Lab Queries)	Triage Action
1. Initial Access / RAT Install	T1219, T1547.001	New process creation (DeviceProcessEvents) for known remote access tools like **AnyDesk.exe** or **TeamViewer.exe**, OR associated Registry Persistence (DeviceRegistryEvents).	**Isolate the Source Host** immediately and confirm if the account (CORP\bob, CORP\alice) authorized the installation.
2. Reconnaissance	T1059.001	Excessive execution of discovery commands (net view, whoami, ipconfig, Get-LocalUser) by the same process	Check for follow-up Lateral Movement attempts (Stage 3). If isolated, proceed to forensically image.

		or account in a short time frame.	
3. Lateral Movement	T1569.002, T1047	**Network Logon (Type 3)** to critical servers (DC/SQL) from a previously unauthenticated host, especially when initiated by tools like **PsExec.exe** or **wmiprvse.exe** over SMB ports (445/139).	**Disable the Compromised User Account** (CORP\svc-backup) and **isolate the source host** (e.g., ENG-VM03).
4. Data Staging	T1119	Creation of large archive files (.zip, .7z, .rar) on shared UNC paths (FilePath has @"\\") by non-backup service accounts.	Monitor network traffic from the source host (Stage 5 trigger) and check the contents of the archive if possible.
5. Exfiltration	T1041	Large volume of HTTP POST traffic (DeviceNetworkEvents) to known C2/file-sharing domains (**transfer.sh, dropbox.com**) originating from a suspicious process (e.g., AnyDesk.exe).	**Block the destination IP/URL** at the firewall/proxy immediately to halt data theft.
6. Impact / Ransomware	T1486	Mass file renaming (thousands of files suddenly ending with **.locked** or **.encrypted**) or execution of	**Power Off/Hard Quarantine the Encryption Host(s)** immediately to stop the payload.

		commands to delete Volume Shadow Copies (vssadmin.exe delete shadows).	

2. Immediate Containment Procedure (Phase B)

If *any* stage alert (2-6) is validated as malicious, the following steps must be executed immediately, focusing on limiting the attacker's blast radius:

1. **Stop Propagation:** Block all C2 domains/IPs (transfer.sh, etc.) at the perimeter firewall/proxy.
2. **Isolate & Quarantine:** Isolate the current **Source Host** and **Target Host** (if applicable) using EDR tools.
3. **Disable Account: Disable the Compromised User Account** (e.g., CORP\svc-backup) that is actively engaging in lateral movement or staging.
4. **Preserve Image:** Create a snapshot or forensically image the initially compromised host (Stage 1) for later root cause analysis.

3. Eradication and Investigation Procedure (Phase C)

Once containment is confirmed, the team moves to remove the threat and confirm the extent of the damage.

1. **Full Path Tracing:** Review logs to map out the entire intrusion path (the "blast radius")—every device, account, and resource touched by the compromised credentials/hosts.
2. **Clean Persistence:** Check all affected hosts for hidden persistence mechanisms (Registry Run Keys, Scheduled Tasks, new services - T1543.003), and remove them.
3. **Mandatory Credential Reset:** Force a password reset for *all* user and service accounts that authenticated to any compromised host during the intrusion window.
4. **System Rebuild:** Do **NOT** clean and redeploy the compromised hosts; **Reimage** them completely from a trusted gold image.
5. **Data Validation:** Confirm backup integrity and restoration capabilities.
6. **Post-Mortem:** Document all findings, actions taken, and the **Recommendations & Next Steps** from the lab report (e.g., Enable PowerShell & Sysmon logging, Automate response with Logic Apps).