* 1. **Malware Playbook**

|  |  |  |
| --- | --- | --- |
| Sl.No | Phases | Task |
| 1 | Preparation | 1 - Identify the Malware Infected System 2 - Collect and Preserve the Standard Evidences |
| 2 | Identification (Detect/Analyze) | 1 - Analyze affected system and account 2 - Analyze network for malware activity & Identify other Infected System 3 - Review Anti-Virus Venture and check status in AV database. 4 - add all logs and details. 5 - Update the Internal management team assessment |
| 3 | Containment | 1 - Select and Execute initial Containment Process/strategy 2 - Disconnect or isolate Compromised system (with IR approval) 3 - Capture the accurate time stamp for Containment of Incident |
| 4 | Eradicate (Respond) | 1 - Execute an appropriate eradication or Recovery process/strategy 2 - Confirm completion of malware Remediation 3 - Implement network Countermeasures |
| 5 | Recover | 1 - Remove temporary containment measures 2 - notify internal management Chain (resolution) 3 - Harden / patch all Vulnerable system |
| 6 | Learn | 1 - Improvement of Playbook or use case 2 - Update Policies, Procedures and Guidelines |

* 1. **Data Loss Playbook**

|  |  |  |
| --- | --- | --- |
| Sl.No | Phases | Task |
| 1 | Preparation | 1 - Determine the Characterization of Data 2 - Identify the Malware Infected System 3 - Collect and Preserve the Standard Evidences |
| 2 | Identification (Detect/Analyze) | 1 - Capture and Conduct analysis on appropriate Log files 2 - Determine data at-Risk based on known element of the incident 3 - outline the proposed recovery plan, risk assessment 4 - add all logs and details. |
| 3 | Containment | 1 - Select and Execute initial Containment Process/strategy 2 - Disconnect or isolate Compromised system (with IR approval) |
| 4 | Eradicate (Respond) | 1 - Execute an appropriate eradication or Recovery process/strategy 2 - Confirm completion of malware Remediation 3 - Implement network Countermeasures |
| 5 | Recover | 1 - Remove temporary containment measures 2 - notify internal management Chain (resolution) 3 - Harden / patch all Vulnerable system |
| 6 | Learn | 1 - Improvement of Playbook or use case 2 - Update Policies, Procedures and Guidelines |

* 1. **Phishing Playbook**

|  |  |  |
| --- | --- | --- |
| Sl.No | Phases | Task |
| 1 | Preparation | 1 - Determine the Characterization of Data 2 - Identify the Malware Infected System 3 - Collect and Preserve the Standard Evidences |
| 2 | Identification (Detect/Analyze) | 1 - Analyze header of suspected email message 2 - determine the techniques used for engage targets 3 - Remove delivered or quarantined emails |
| 3 | Containment | 1 - Request malicious message is purged from employee email boxes  2 - Block Inbound messages from malicious sender 3 - Implement network Countermeasures |
| 4 | Eradicate (Respond) | 1 - Require Credential reset for any employees contacting a malicious site 3 - Implement network Countermeasures |
| 5 | Recover | 1 - Remove temporary containment measures 2 - notify internal management Chain (resolution) |
| 6 | Learn | 1 - Improvement of Playbook or use case 2 - Update Policies, Procedures and Guidelines |