**Pre-Built Step-by-Step Actions for Common Cybersecurity Incidents (With Standards & Frameworks)**

These playbooks are aligned with major cybersecurity standards and frameworks, including **NIST SP 800-61r2**, **MITRE ATT&CK**, **ISO/IEC 27035**, and **SANS Incident Response Cycle**.

**🎣 1. Phishing Incident Response Playbook**

*(Mapped to NIST SP 800-61r2 Phases, MITRE ATT&CK T1566 Phishing Technique)*

**Step-by-Step Actions:**

1. **Identification *(NIST Detection & Analysis Phase)***
   * Monitor user reports of suspicious emails (ISO/IEC 27035).
   * Analyze email headers and attachments (T1566 ATT&CK).
   * Search email gateway logs for anomalies.
2. **Containment *(NIST Containment Phase)***
   * Block malicious sender domains/IPs at the gateway (ISO 27035).
   * Remove emails from inboxes using admin tools (SANS Identification step).
   * Isolate any endpoints where links/attachments were activated.
3. **Eradication *(NIST Eradication Phase)***
   * Run endpoint antivirus/EDR scans (mapped to MITRE Defensive Evasion techniques).
   * Reset compromised user credentials.
4. **Recovery *(NIST Recovery Phase)***
   * Reimage affected systems if malware is detected.
   * Restore user services post-cleanup.
5. **Post-Incident Activities *(NIST Lessons Learned Phase)***
   * Update email filters and anti-phishing policies (NIST CSF "Protect" Function).
   * Conduct a phishing awareness training session (ISO 27035).

**2. Ransomware Incident Response Playbook**

*(Aligned to NIST SP 800-61r2, SANS IR Lifecycle, MITRE ATT&CK T1486 Data Encrypted for Impact)*

**Step-by-Step Actions:**

1. **Identification**
   * Detect unusual encryption activities via EDR alerts (NIST Detection Phase).
   * Confirm ransomware signatures using AV scans (ISO 27035 Incident Verification).
2. **Containment**
   * Immediately isolate affected hosts (NIST Containment).
   * Disable suspicious administrative accounts (ISO 27035).
3. **Eradication**
   * Delete ransomware executables and persistence mechanisms (scheduled tasks, registry keys).
   * Apply patches against exploited vulnerabilities (NIST Recovery step).
4. **Recovery**
   * Restore data from known good backups (SANS Recovery Phase).
   * Validate backup integrity prior to restoration (NIST CSF "Recover" Function).
5. **Post-Incident Activities**
   * Conduct a post-mortem to identify the root cause.
   * Enhance backup strategies to include offline storage (NIST CSF "Protect").

**3. Lateral Movement Detection and Response Playbook**

*(Based on MITRE ATT&CK T1075 Pass-the-Hash, NIST SP 800-61, ISO/IEC 27035)*

**Step-by-Step Actions:**

1. **Identification**
   * Monitor for abnormal authentication patterns (NIST Detection Phase).
   * Check for suspicious use of administrative credentials (mapped to MITRE T1075, T1021).
2. **Containment**
   * Isolate systems showing lateral movement behaviors.
   * Reset administrative credentials immediately (ISO 27035).
3. **Eradication**
   * Remove tools such as PsExec or Mimikatz if found (MITRE ATT&CK T1543.003).
   * Eliminate unauthorized scheduled tasks and services.
4. **Recovery**
   * Rebuild or restore affected machines (NIST Recovery Phase).
   * Audit AD permissions and remove excessive privileges (ISO/IEC 27001 Principle of Least Privilege).
5. **Post-Incident Activities**
   * Improve segmentation between network zones (NIST CSF "Protect" and "Detect" Functions).
   * Implement stricter login monitoring and MFA enforcement.

**4. Data Exfiltration Detection and Response Playbook**

*(Mapped to MITRE ATT&CK T1041 Exfiltration Over Command and Control Channel, ISO/IEC 27035)*

**Step-by-Step Actions:**

1. **Identification**
   * Monitor egress traffic using firewall and proxy logs (NIST Detection Phase).
   * Investigate alerts from DLP systems (ISO 27035).
2. **Containment**
   * Block abnormal outbound connections at perimeter firewalls (NIST Containment).
   * Quarantine involved user accounts/systems (SANS Containment Phase).
3. **Eradication**
   * Remove malware tools facilitating exfiltration (MITRE ATT&CK T1041).
   * Patch vulnerabilities used by attackers (NIST Eradication Phase).
4. **Recovery**
   * Validate system integrity and reintroduce cleaned systems (ISO 27035 Recovery).
   * Implement enhanced DLP and egress monitoring rules (NIST CSF "Detect" Function).
5. **Post-Incident Activities**
   * Conduct forensic investigation to confirm the volume and sensitivity of stolen data.
   * Update risk assessments based on data loss findings.
   * Train staff on secure data handling practices (NIST CSF "Protect" Function).

**Conclusion**

Each pre-built playbook ensures that **incident response actions**:

* Follow **recognized standards** (NIST, ISO, SANS).
* Integrate **MITRE ATT&CK** tactics to guide threat detection and eradication.
* Map to the **NIST Cybersecurity Framework functions** (Identify, Protect, Detect, Respond, Recover).
* Enable fast, coordinated, and measurable improvement in the organization's security posture.