Question: You are a security operations system analyst and helpful cybersecurity assistant that generates detailed incident response playbooks based on NIST guidelines. please generate a playbook for a worm infections effectively?

Answer:

Title: NIST-Compliant Incident Response Framework Playbook for Worm Infections

1. Preparation:

Objective: Establish contacts, define procedures, and gather information to save time during an incident.

- \*\*Define Actors\*\*:

- Document a contact list of crisis cell actors, ensuring it remains up-to-date.

- \*\*Ensure Tools and Resources\*\*:

- Verify that analysis tools (EDR, Antivirus, IDS, log analyzers) are functional, uncompromised, and up-to-date.

- \*\*Network Mapping\*\*:

- Maintain an architecture map of your networks.

- \*\*Asset Inventory\*\*:

- Ensure an up-to-date inventory of all assets, including configurations and software versions.

- \*\*Security Watch\*\*:

- Perform continuous security monitoring and keep security personnel informed about evolving threat trends.

2. Detection and Analysis:

Objective: Detect the incident, determine its scope, and involve appropriate parties.

- \*\*Detect the Infection\*\*:

- Gather and analyze information from multiple sources:

- Antivirus logs

- IDS/IPS

- EDR

- Suspicious connection attempts on servers and firewalls

- High number of locked accounts

- Suspicious network traffic

- Increased support calls

- High load/system freezes

- Large volumes of email sent

- If symptoms are identified, activate the crisis cell with actors defined in the preparation phase.

- \*\*Identify the Infection\*\*:

- Analyze symptoms to identify the malware, propagation vectors, and countermeasures using:

- CERT bulletins

- External support (antivirus companies, etc.)

- Security websites and threat intelligence providers

- Notify the Chief Information Security Officer (CISO) and, if required, contact national CERT and regulators.

- \*\*Assess Infection Perimeter\*\*:

- Define the boundaries and business impact of the infection.

3. Containment:

Objective: Mitigate the attack’s effects on the targeted environment.

- \*\*Network Isolation\*\*:

- Disconnect infected areas from the Internet and isolate them from other networks.

- Allow business-critical traffic only after ensuring it is not an infection vector.

- \*\*Neutralize Propagation Vectors\*\*:

- Apply relevant countermeasures, including patching, traffic blocking, disabling devices, etc., using tools like:

- EDR

- WSUS

- Windows GPO

- Firewall rules

- Operational procedures

- Monitor the infection using analysis tools (e.g., antivirus console, server logs, support calls).

- \*\*Mobile Devices\*\*:

- Block connections from mobile devices (laptops, smartphones, storage) to prevent propagation.

- Instruct end-users to adhere to directives precisely.

4. Eradication:

Objective: Take actions to remove the threat and avoid future incidents.

- \*\*Identify Remediation Methods\*\*:

- Use resources like:

- Antivirus signature databases

- External support contacts

- Security websites

- Tools like Yara scan, Loki, DFIR-ORC, ThorLite, EDR search

- Define a disinfection process validated by an external entity (CERT, SOC, Incident Response team).

- \*\*Test the Process\*\*:

- Ensure the disinfection process works effectively without damaging services.

- \*\*Deploy Remediation Tools\*\*:

- Use options like:

- EDR

- WSUS and GPO

- Antivirus signature deployment

- Manual disinfection

- Vulnerability patching

- Address worms that block remediation methods by implementing workarounds. Monitor progress through the crisis cell.

5. Recovery:

Objective: Restore the system to normal operations.

- \*\*Verify Steps\*\*:

- Confirm all previous steps were completed successfully and obtain management approval.

- \*\*Step-by-Step Restoration\*\*:

- Gradually reconnect:

- Network traffic used for malware propagation

- Sub-areas of the infected area

- Mobile laptops to the area

- Local networks

- Internet access

- Enforce technical monitoring during the restoration process.

6. Lessons Learned:

Objective: Document the incident’s details, discuss lessons learned, and adjust plans and defenses.

- \*\*Incident Report\*\*:

- Create a comprehensive crisis report detailing:

- Initial cause of the infection

- Actions and timelines of key events

- What worked well and what didn’t

- Incident cost

- Indicators of compromise

- \*\*Post-Incident Review\*\*:

- Analyze effectiveness of the response and identify areas for improvement.

- Update contact lists and refine communication methods.

- \*\*Security Enhancements\*\*:

- Implement additional measures based on lessons learned.

- Regularly review and update security policies and procedures.