1. Incident Response Plan Template

This will be used by students to create their own Incident Response Plans (IRP).

[Your Company's Name] Incident Response Plan

Section 1: Preparation

- What steps will the company take to prepare for future cyber threats?
    - Example: Install firewalls, train employees, perform regular updates.

Section 2: Detection

- How will the company detect unusual network activity or cyberattacks earlier?
    - Example: Network monitoring tools, alerts for suspicious traffic, anomaly detection.

Section 3: Response

- What steps will the company take when a cyberattack is detected?
    - Example: Isolate infected systems, block malicious IPs, notify security teams.

Section 4: Recovery

- How will the company recover and restore normal operations after a breach?
    - Example: Restore systems from backups, investigate the breach, run post-attack forensics.

Section 5: Prevention

- What long-term strategies will the company use to prevent future breaches?
    - Example: Implement two-factor authentication, regular security updates, penetration testing.

---

2. War Room Scenario Recap Worksheet

War Room Scenario Recap Worksheet

Part 1: What Went Right

- List two things your team did well during the War Room simulation.
    1. _____
    2. _____

Part 2: What Went Wrong

- List two things your team could have improved.
    1. _____
    2. _____

Part 3: Lessons Learned

- What's one lesson you'll take away from this simulation that can help your team in future incidents?
    - _____

---

3. Red Team Consultant Prompt Sheet

Red Team Consultant Prompt Sheet

Consultant Prompts

1. Did your team consider insider threats as a source of attack?
2. How would you handle a DDoS attack?
3. How would you monitor for unusual data exfiltration patterns?
4. What contingency plans do you have in place for a total network lockdown?
5. Have you considered using encryption to protect sensitive data?

---

1. Timestamp: 10:01:12
   Source IP: 192.168.1.25
   Destination IP: 192.168.1.1
   Traffic Volume (MB): 1.2
   Activity: Normal Internal Access
   Notes: Routine login from workstation

2. Timestamp: 10:03:45
   Source IP: 192.168.1.42
   Destination IP: 192.168.1.3
   Traffic Volume (MB): 15.6
   Activity: Large file transfer
   Notes: Backup operation in progress

3. Timestamp: 10:05:28
   Source IP: 192.168.1.67
   Destination IP: 10.0.0.5
   Traffic Volume (MB): 50.0
   Activity: Unusual outgoing traffic
   Notes: Possible data exfiltration attempt

4. Timestamp: 10:07:12
   Source IP: 192.168.1.25
   Destination IP: 192.168.1.8
   Traffic Volume (MB): 2.1
   Activity: Internal network request
   Notes: Routine server access

5. Timestamp: 10:09:35
   Source IP: 192.168.1.78
   Destination IP: 172.16.0.1
   Traffic Volume (MB): 0.3
   Activity: DNS query
   Notes: Normal external access

6. Timestamp: 10:12:45
   Source IP: 192.168.1.90
   Destination IP: 10.0.0.9
   Traffic Volume (MB): 100.4
   Activity: Data upload
   Notes: Potential high-volume upload

7. Timestamp: 10:15:22
   Source IP: 192.168.1.42
   Destination IP: 192.168.1.2
   Traffic Volume (MB): 5.6
   Activity: File sharing
   Notes: Internal document sharing

8. Timestamp: 10:17:50
   Source IP: 192.168.1.89
   Destination IP: 192.168.1.1
   Traffic Volume (MB): 1.1
   Activity: Normal internal traffic
   Notes: Routine internal communication