Cybersecurity Incident Containment and Response

This checklist is designed to guide businesses in preparing for, containing, and responding to cybersecurity incidents.

It includes prerequisites to ensure an effective response framework is in place and detailed steps for handling incidents as they arise.

#0. Prerequisites: Building an Incident Response Framework

☐ Establish an Incident Response (IR) Team, their roles and responsibilities.
☐ Develop an Incident Response Plan (IRP)
☐ Set Up Tools and Technologies: Implement logging, monitoring, and forensic tools
☐ Ensure all critical systems log to a central location for quick analysis.
☐ Regularly Backup Data: Maintain offline backups and verify restoration capabilities.
☐ Implement Network Segmentation: Isolate critical systems to limit the spread of incidents.
☐ Conduct Cybersecurity Awareness Training for employees to recognize phishing, malware, and other threats.
☐ Define Escalation Paths: Establish a clear protocol for reporting and escalating incidents.
☐ Test the Plan: Conduct tabletop exercises and mock incidents to test readiness.

 # 1. Identify the Incident

☐ Detect unusual activity through monitoring tools or user reports.
☐ Analyze logs and alerts to confirm the nature of the incident.
☐ Classify the incident based on severity (e.g., data breach, ransomware, unauthorized access).

 # 2. Contain the Incident

☐ Immediate Containment: Disconnect affected systems from the network to prevent further spread.
☐ Short-Term Containment: Apply access controls or isolation to affected segments.
☐ Long-Term Containment: Develop patches, reconfigure systems, or implement security enhancements.

 # 3. Eradicate the Threat

☐ Identify root cause and eliminate malicious software, unauthorized users, or vulnerabilities.
☐ Remove affected files, reset credentials, and revoke compromised access tokens.
☐ Update security configurations and apply patches to prevent reoccurrence.

 # 4. Recover Operations

☐ Restore systems from clean backups to a secure state.
☐ Validate system integrity and monitor for residual activity.
☐ Resume operations with heightened monitoring in place.

 # 5. Post-Incident Review

☐ Conduct a debrief with the incident response team to document lessons learned.
☐ Update the Incident Response Plan based on findings.
☐ Improve processes, tools, and training to address identified gaps.

Supporting Tools and Practices

☐ Endpoint Detection and Response (EDR): Use EDR solutions to identify and respond to endpoint threats.
☐ Threat Intelligence: Leverage real-time threat intelligence to anticipate and address new attack vectors.
☐ Network Traffic Analysis (NTA): Monitor for unusual patterns to detect and contain threats early.
☐ Access Control: Enforce least privilege principles and regularly audit permissions.
☐ Incident Logs: Maintain detailed logs of incidents for compliance and forensic investigations.

Need a hand with the next step?

If you have a question about any of these steps, or need help setting up a more advanced or tailored solution, we're here for you!

Feel free to send us an email at contact@403bits.com.

For simpler queries, we'll gladly share advice or point you in the right direction — free of charge!

And if you're facing a more complex challenge or want to save time, our experts can take over and deliver a comprehensive setup that perfectly fits your needs.

We're here to help you build security and efficiency
so you can focus on growing your business!

If you liked this checklist or have improvement suggestions, - let us know contact@403bits.com.