C&W Business

Cybersecurity
Local presence, Global expertise

Incident Response Playbook

Take the Incident Response Readiness Assessment now to uncover insights that will strengthen your cybersecurity defences!

A strategic approach to Incident Response

The National Institute of Standards and Technology (NIST) developed guidelines under the Federal Information Security Management Act (FISMA) of 2002 to enhance the security of agency operations. While originally intended for Federal agencies, these standards are often embraced by non-governmental organisations to mitigate risks from computer security incidents, focusing on detection, analysis, and effective incident handling.

Purpose

C&W Business is committed to keeping our region safe by leveraging the latest technology and following these best practices. Our goal is to empower organisations with practical guidance for building a robust Incident Response programme that prioritises detecting, analysing, and managing incidents. With our dedicated 24/7 team of engineers, we provide unwavering support to help you face cyberthreats and minimise the impact of attacks. Our framework is designed to be adaptable, allowing you to tailor it to your organisation's unique security needs and mission requirements. Together, we can create a safer digital environment for everyone.

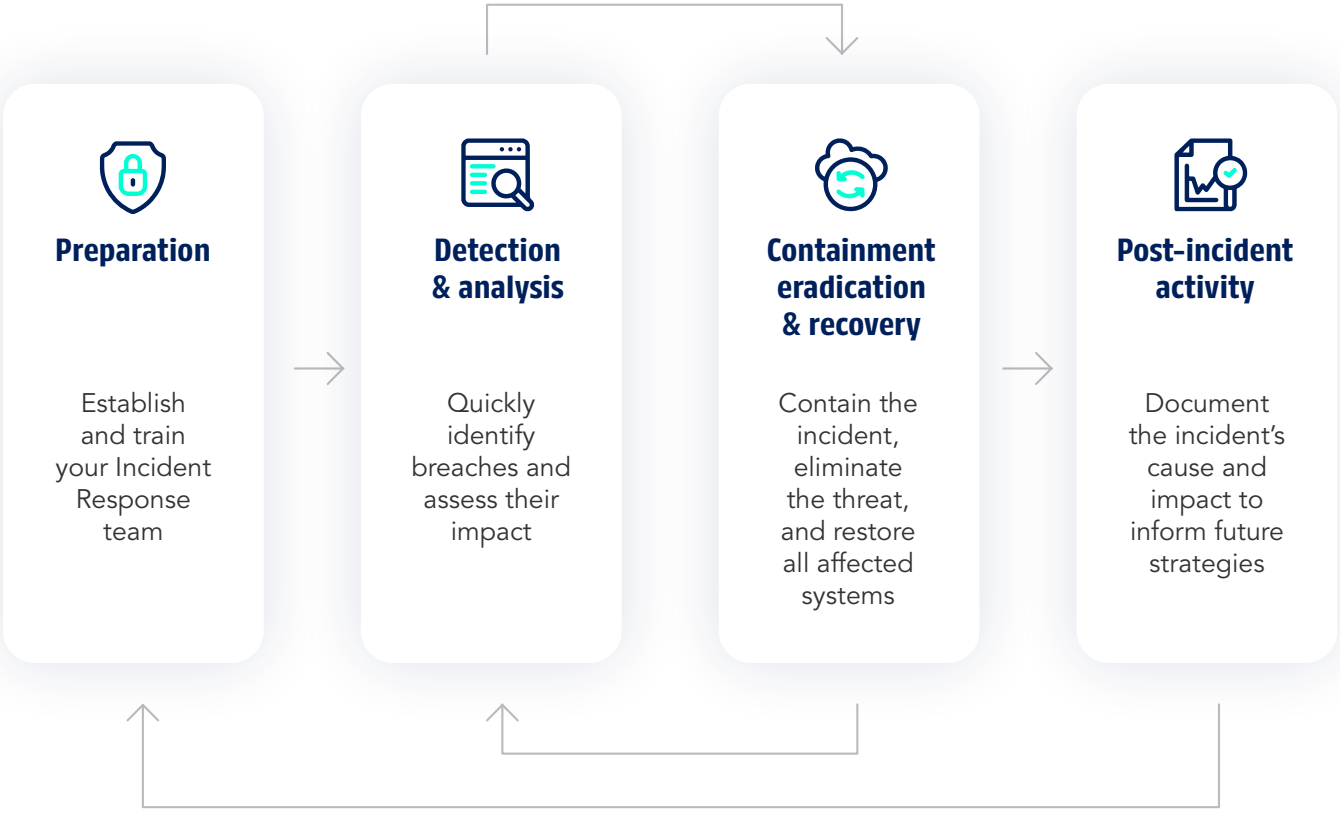
When to use it

Use this playbook for incidents involving confirmed malicious cyberactivity or when a major incident is suspected but not yet ruled out. Examples include lateral movement, credential theft, data exfiltration, or network intrusions affecting multiple users or systems, and compromised administrator accounts.

This playbook is not for incidents with low impact, such as accidental information leaks, phishing emails without compromise, or malware on a single device that poses no real threat to national security or public safety.

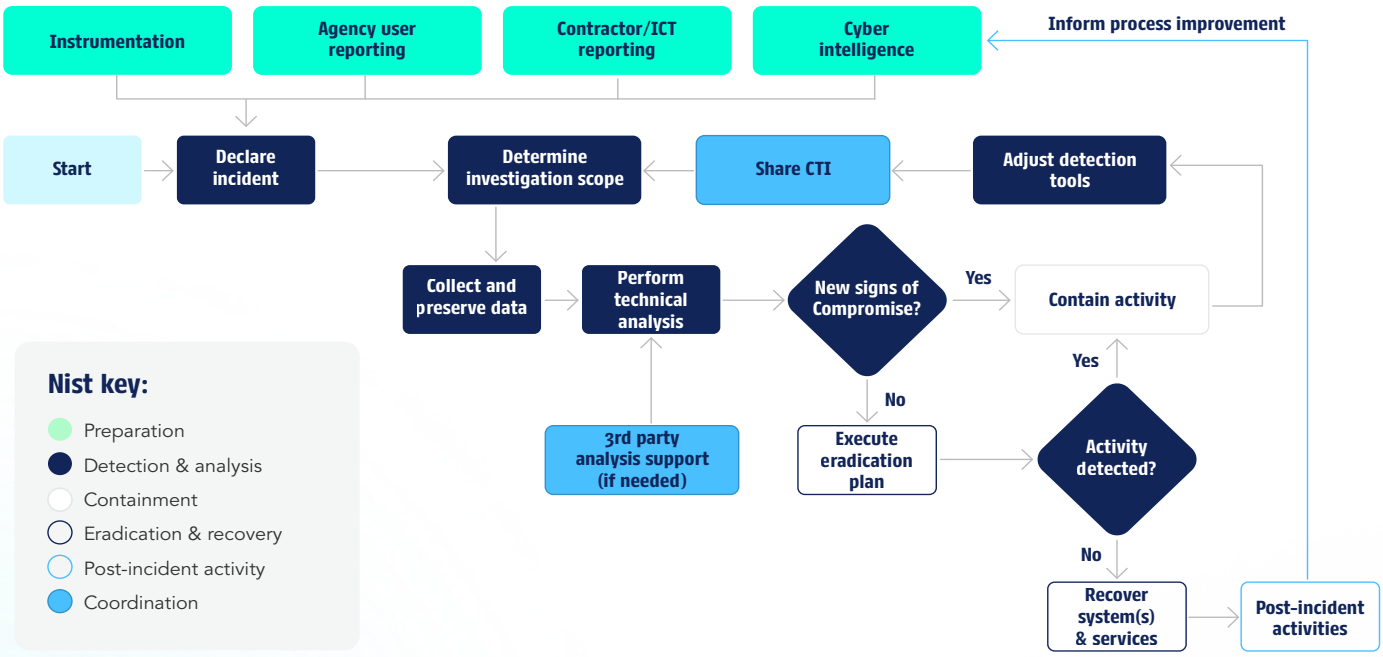
Incident Response life cycle

The framework of successful Incident Response consists of four key phases, each working to get your organisation closer to a resilient cybersecurity posture. By following these phases, you can effectively navigate and manage incidents, minimising their impact on your operations. Understanding this framework is essential for fostering a proactive security culture.



Incident Response process

The Incident Response process begins with identifying and declaring the incident. In this context, "declaration" means notifying the government and agency network defenders, not formally declaring a major incident as defined by law or policy. The process is divided into phases, with each step explained in detail. Many activities are iterative and may continue to evolve until the incident is fully resolved. Check out the following image for an outline of the process.



Preparation

Preparing for major incidents is essential to minimise their impact on the organisation. Key preparation activities include understanding and documenting Incident Response policies, instrumenting the environment to detect suspicious activity, establishing staffing plans, and educating employees and collaborators on cyberthreats and reporting procedures. Leveraging Cyberthreat Intelligence (CTI) also helps proactively identify potential malicious actions.

Preventing incidents

Minimising incidents is crucial for protecting business processes, as weak security controls can overwhelm response teams and worsen impacts. A truly empowered Incident Response team, alongside properly trained IT staff, can promote strong security practices, identify vulnerabilities, and assist in risk assessments.

Actions to take:

Document Incident Response plans

Detail the coordination leads, escalation protocols for major incidents, and contingency resource plans for effective response.

Establish notification procedures

Define policies for notifying relevant stakeholders and interacting with law enforcement.

Implement monitoring telemetry

Utilise telemetry to monitor systems and networks effectively.

Use detection tools

Deploy antivirus software and intrusion detection systems to enhance security.

Train personnel

Ensure staff are well-trained in Incident Response and recovery protocols.

Conduct regular recovery exercises

Adhere to continuity planning guidelines from the Presidential Policy Directive, including annual tests and drills to stay prepared.

Detection and analysis

Detecting and assessing cybersecurity incidents is crucial for effective Incident Response, necessitating clear processes and monitoring technologies. Start by reporting incidents to the government and notifying agency IT leadership, including the Office of Management and Budget for major incidents. Define the investigation's scope through data analysis to evaluate access levels and impacts. Collect and preserve relevant data, including logs from various sources, for potential law enforcement use. Finally, perform technical analyses to correlate findings and assess anomalies against established baselines.

Attack vectors

Cyberincidents can originate from various attack vectors, making it essential for organisations to be prepared for common methods rather than creating detailed responses for every possible scenario. Key vectors include external/removable media, attrition attacks like DDoS, web-based and email attacks, impersonation tactics, improper usage by authorised users, and the loss or theft of devices.

Understanding these vectors helps define effective response strategies tailored to specific incident types.

Signs of an incident

Detecting incidents is challenging due to the diverse methods and high volume of potential signs, often resulting in thousands of alerts daily. Signs can be classified as precursors, indicating possible future incidents, or indicators, which confirm that an incident may have already occurred.

Examples include suspicious log entries as precursors and alerts from intrusion detection systems as indicators.

Actions to take:

Declare an incident

Report the incident to the government for investigation support.

Determine investigation scope

Gather data to identify: Types of access involved, affected assets, and any adversarial activity.

Collect and preserve data

Ensure data is handled according to established protocols for incident verification and attribution.

Conduct initial assessment

Analyse preliminary data to assess the potential impact and severity of the incident.

Establish communication channels

Set up secure communication channels for sharing information with relevant stakeholders.

Monitor for ongoing activity

Continuously monitor systems for any signs of continued adversarial activity during the investigation.

Containment

Containment is crucial in Incident Response to prevent overwhelming resources and minimising damage, making it a key early consideration. It allows time to develop a tailored remediation strategy, emphasising the importance of predetermined strategies and procedures for effective decision-making, such as shutting down systems or disconnecting from networks. Since containment strategies vary by incident type, organisations should create distinct strategies for each major incident, ensuring clear documentation to guide decision-making processes.

Actions to take:

Measure strategy effectiveness

Analyse the effectiveness of the strategy, distinguishing between partial and full containment.

Preserve evidence

Determine the need for preserving evidence related to the incident.

Evaluate service availability

Consider the impact on service availability, including network connectivity and services provided to external parties.

Estimate implementation time and resources

Assess the time and resources required to implement the containment strategy.

Assess potential damage

Evaluate the potential damage to and theft of resources.

Determine solution duration

Establish the duration of the solution, and if it's an emergency workaround, temporary workaround, or a permanent solution.

Eradication and recovery

The eradication and recovery phase aims to restore normal operations by eliminating all traces of the incident, such as removing malicious code and re-imaging infected systems, while addressing any vulnerabilities exploited during the attack. Before initiating eradication, organisations must ensure that all potential backdoors and adversarial activities are contained, and evidence is collected.

Eradication activities

- Remediate all infected IT environments (e.g., cloud, on-premises, hybrid).
- Reimage affected systems from trusted "gold" sources or rebuild them from scratch.
- Reset passwords on compromised accounts.
- Develop response scenarios for potential alternative attack vectors.
- Ensure adequate time is allocated to check for all persistence mechanisms (backdoors).
- Coordinate with ICT service providers, commercial vendors, and law enforcement.

Recovery activities

- Reconnect rebuilt or new systems to the network.
- Reinforce perimeter security (e.g., adjust firewall rules and access control lists).
- Thoroughly test all systems, including security controls, for functionality.
- Monitor operations for any abnormal behavior post-recovery.
- Conduct a post-incident review to identify lessons learned and improve future response efforts.
- Update Incident Response plans based on the findings of the eradication and recovery phases.

Post-incident activities

Post-incident activities focus on improving future Incident Responses and strengthening cybersecurity measures. Key actions include adjusting sensors and alerts for better detection of adversary Tactics, Techniques, and Procedures (TTPs), finalising reports to fulfill legal and policy requirements, and conducting a lessons-learned analysis to identify areas for improvement. These activities aim to document the incident, enhance organisational readiness, and prevent similar incidents in the future.

Actions to take:

Enhance detection capabilities

Implement enterprise-wide detections for adversary Tactics, Techniques, and Procedures (TTPs) and address any blind spots in coverage.

Monitor for threat persistence

Continuously monitor the environment for signs of adversary presence and emulate TTPs to test the effectiveness of countermeasures.

Complete reporting obligations

Provide necessary post-incident updates per legal and policy requirements and collaborate with the government to close incident tickets.

Validate normal operations

Conduct independent tests to confirm the resumption of normal operations and review cyberthreat intelligence for potential related attacks.

Conduct a lessons-learned analysis

Evaluate the effectiveness of incident handling, capture insights on root causes and procedural gaps, and ensure root causes are addressed.

Improve operational readiness

Identify training needs, review roles and responsibilities for clarity, and enhance tools for better protection, detection, and response actions.

Coordination

Effective Incident Response relies on coordination between the affected Federal Civilian Executive Branch (FCEB) agency and the government. Early and consistent communication is essential, as some agencies possess unique expertise beneficial during incidents. The FCEB agency must report all cybersecurity incidents to the government and follow specific reporting requirements outlined by federal policy. The government should provide tracking, risk ratings, and cyberdefense services to support the Incident Response process. Key coordination activities include notifying them, sharing indicators of compromise (IOCs), and engaging with federal law enforcement when necessary.

Actions to take:

Immediate notification

Inform the government within one hour of incident detection and provide ongoing updates until resolution.

Incident tracking

Secure a tracking number and risk rating from the government promptly after reporting.

Share Indicators of Compromise (IOCs)

Provide relevant log data and cyberthreat indicators to the government, updating them with new information as the incident progresses.

Receive cyber intelligence

Coordinate with the government to access relevant cyberintelligence to inform response efforts.

Engage law enforcement

Report the incident to federal law enforcement as required and assess if escalation to a Cyber Unified Coordination Group (C-UCG) is necessary.

Compliance and coordination

Meet reporting requirements per federal policy and inform relevant stakeholders, while leveraging the government's cyberdefense capabilities for improved Incident Response.

Sources:
Cybersecurity Incident & Vulnerability Response Playbooks (cisa.gov)
Computer Security Incident Handling Guide (nist.gov)

C&W Business

Cybersecurity
Local presence, Global expertise

The path to robust Incident Response

Take the Incident Response Readiness Assessment now to uncover insights that will strengthen your cybersecurity defences!

