# 🛟 Incident Response Plan

# INCIDENT RESPONSE PLAN

An **Incident Response Plan (IRP)** provides a structured approach for detecting, responding to, and recovering from cybersecurity incidents. Below is a detailed IRP tailored for a cybersecurity team associated with Capybara Unlimited, a medium-sized organization.

By integrating this detailed IRP, cybersecurity teams can ensure they are prepared to handle incidents efficiently and minimize their impact on the organization.

# 🏆 I. Objectives

# I Objectives

## I.1 Minimize Impact:

Reduce damage to systems, data, and operations by rapidly detecting, containing, and mitigating security incidents.

## I.2 Restore Operations:

Safely and efficiently restore affected services, business processes, and IT systems after verifying that threats have been eradicated.

## I.3 Enhance Security Posture:

Identify vulnerabilities, gaps, and root causes through post-incident analysis and implement improvements to strengthen defenses and response capabilities.

## I.4 Meet Regulatory Requirements:

Ensure compliance with all legal, regulatory, industry, and internal policies, including breach notifications, evidence handling, and incident documentation.

# 🔭 II. Scope

# II Scope

This Incident Response Plan applies to all organizational data, information systems, networks, applications, and related infrastructure, regardless of location (on-premises, cloud, hybrid, or remote). It applies to all personnel—including employees, contractors, managed service providers, and third-party vendors—who interact with or support organizational systems.

The plan covers cybersecurity, privacy, and operational security incidents that may impact confidentiality, integrity, or availability of data or services. It is applicable during normal operations, after-hours, and emergency conditions.

# 🕵️ III. Roles & Responsibilities

# III Roles & Responsibilities

The IR team consists of:

## III.1 Incident Command(IR Manager)

Leads and coordinates all incident response activities, makes operational decisions, and ensures alignment with organizational objectives.

## III.2 SOC Analysts

Monitor, detect, analyze, and escalate security events using SIEM, EDR, and related tools.

## III.3 Forensic Specialists

Perform in-depth investigations, acquire and preserve evidence, identify attack vectors, and support legal or disciplinary processes.

## III.4 IT Administrators

Execute containment, eradication, and recovery tasks as directed by the IR team. Maintain system integrity during response efforts.

## III.5 Legal and Compliance Team

Provide guidance on regulatory obligations, liability risks, and breach notification requirements. Coordinate with law enforcement and ensure evidence handling is compliant.

## III.6 Communications / Public Relations

Manage approved internal and external communications regarding the incident, ensuring accuracy and coordination with Legal, Executive Leadership, and Incident Command.

## III.7 All Employees

Report suspicious activity promptly, follow IR team instructions, and refrain from sharing incident-related information outside authorized channels.

# 🌱 IV. Incident Response Lifecycle

# IV Incident Response Lifecycle

Follow the **NIST Cybersecurity Framework's Incident Response Process**:

- IV.1 Preparation
  - IV.1.1 Develop policies
  - IV.1.2 Train personnel
  - IV.1.3 Implement tools
  - IV.1.4 Create playbooks
- IV.2 Detection and Analysis
  - IV.2.1 Identify incidents
    - IV.2.1.a SIEM
    - IV.2.1.b EDR
    - IV.2.1.c Network logs
  - IV.2.2 Classify incidents
    - IV.2.2.a Severity levels
    - IV.2.2.b Type
  - IV.2.3 Collect evidence
    - IV.2.3.a Logs
    - IV.2.3.b Malware
    - IV.2.3.c Email headers
  - IV.2.4 Decision points
    - IV.2.4.a Escalate to leadership
    - IV.2.4.b Scope-based containment
- IV.3 Containment
  - IV.3.1 Immediate steps
    - IV.3.1.a Affected systems
    - IV.3.1.b Affected accounts
    - IV.3.1.c Firewall rules

- IV.3.2 Short-term actions
  - IV.3.2.a Disable infected devices
  - IV.3.2.b Redirect to alternative systems
- IV.3.3 Long-term actions
  - IV.3.3.a Patch management
  - IV.3.3.b Network segmentation

IV.4 Eradication
- IV.4.1 Remove malware
  - IV.4.1.a Remove infection (automated)
  - IV.4.1.b Remove infection (manual)
- IV.4.2 Address root cause
  - IV.4.2.a Root cause analysis
  - IV.4.1.b Remove persistence mechanisms

IV.5 Recovery
- IV.5.1 Restore operations
  - IV.5.1.a Restore from backup
  - IV.5.1.b Validate backup integrity
- IV.5.2 Monitor post-incident
  - IV.5.2.a Watch for re-infection
  - IV.5.2.b Reduce visibility gaps

IV.6 Post-Incident Analysis
- IV.6.1 Conduct review
  - IV.6.1.a Create timeline
  - IV.6.1.b Evaluate processes
- IV.6.2 Document findings
  - IV.6.2.a Incident report
  - IV.6.2.b Lessons learned
- IV.6.3 Implement changes
  - IV.6.3.a Update IR processes
  - IV.6.3.b Implement mitigations

# IV.1 Preparation

Laying the groundwork before an incident happens.

## IV.1.1 Develop policies

Define what counts as an incident, how serious different incidents are, who is responsible for what, and how escalation works.

### IV.1.2 Train personnel

Provide regular training and run practice simulations (tabletop exercises) so everyone knows their role during an incident.

### IV.1.3 Implement tools

Set up tools that help detect, investigate, and respond to incidents—such as log monitoring, endpoint protection, and secure backups. Ensure availability of SIEM, IDS/IPS, forensic tools, and backup systems.

### IV.1.4 Create playbooks

Prepare step-by-step guides for handling common incident types (malware, phishing, denial-of-service(DoS), etc.).

## IV.2 Detection and Analysis

Understanding what happened and how serious it is.

### IV.2.1 Identify incidents

Monitor systems and alerts for signs of suspicious or harmful activity, using:

- **SIEM:** organizes and analyzes security logs for unusual patterns
- **EDR:** alerts on suspicious activity on computers/servers
- **Network logs:** show unusual network traffic

### IV.2.2 Classify incidents

Determine how severe the incident is (Low, Medium, High, Critical) and what type of incident it is (Malware, Phishing, Insider Threat, DoS/DDoS, Data Breach).

#### IV.2.2.a Severity levels

- Low
- Medium
- High
- Critical

#### IV.2.2.b Type

- Malware
- Phishing
- Insider threat
- DoS/DDoS
- Data Breach

## IV.2.3 Collect evidence

Gather logs, malware samples, email information, and other data that helps understand what happened. Preserve evidence in case legal or regulatory action is needed.

### IV.2.3.a Logs

Logs (system, application, network).

#### IV.2.3.b Malware

Malware samples.

#### IV.2.3.c Email headers

Email headers for phishing attempts.

## IV.2.4 Decision points

#### IV.2.4.a Escalate to leadership

Escalate to leadership for high-severity incidents or when sensitive data may be exposed.

#### IV.2.4.b Scope-based containment

Determine containment steps based on scope and impact of the incident

# IV.3 Containment

Limiting the damage and stopping the attack from spreading

## IV.3.1 Immediate steps

### IV.3.1.a Affected systems

Isolate or disconnect affected systems from the network to prevent the attack from spreading and to protect evidence.

### IV.3.1.b Affected accounts

Disable, reset, or quarantine compromised user accounts to stop unauthorized

### IV.3.1.c Firewall rules

Block known malicious IP addresses, URLs, or domains at the firewall or security gateway to stop active threats from communicating with systems.

## IV.3.2 Short-term actions

### IV.3.2.a Disable infected devices

Isolate infected devices from the network to stop the threat from spreading. Do not wipe, reimage, or turn off devices unless instructed by the forensics team so that evidence remains intact.

### IV.3.2.b Redirect to alternative systems

Redirect legitimate users to backup or alternate systems (if available) so business operations can continue while the affected system is being contained.

## IV.3.3 Long-term actions

### IV.3.3.a Patch management

Apply security patches and updates that address the vulnerabilities exploited during the incident to prevent attackers from returning.

### IV.3.3.b Network segmentation

Improve network segmentation and access controls so that if attackers breach one system, they cannot easily move to others.

# IV.4 Eradication

## IV.4.1 Remove malware

### IV.4.1.a Remove infection (automated)

Use approved antimalware, antivirus, or EDR tools to automatically remove malicious files, terminate malicious processes, and clean infected devices. Reboot and apply updates if required to complete automated remediation.

### IV.4.1.b Remove infection (manual)

If automated tools cannot fully remediate the threat, manually identify and remove remaining malicious files, processes, registry entries, scheduled tasks, and other persistence mechanisms.

## IV.4.2 Address root cause

### IV.4.2.a Root cause analysis

Determine exactly how the attacker gained access, what weaknesses were exploited, and why existing defenses did not stop the attack.

### IV.4.1.b Remove persistence mechanisms

Remove any methods the attacker used to maintain long-term access—such as rogue user accounts, scheduled tasks, malicious scripts, startup entries, or unauthorized remote access tools.

# IV.5 Recovery

## IV.5.1 Restore operations

### IV.5.1.a Restore from backup

Rebuild affected systems using clean, verified backups or fresh installations to ensure the malware or attacker access is fully removed.

### IV.5.1.b Validate backup integrity

Check backups to confirm they are clean, uncorrupted, and free of malware before restoring systems. Then verify restored systems operate normally and are not reinfected.

### IV.5.2 Monitor post-incident

#### IV.5.2.a Watch for re-infection

Monitor restored systems closely for any signs that the attacker is attempting to return or that malware remains present.

#### IV.5.2.b Reduce visibility gaps

Turn on additional logging, alerting, or monitoring related to the methods the attacker used, so similar threats can be detected earlier in the future.

## IV.6 Post-Incident Analysis

### IV.6.1 Conduct review

#### IV.6.1.a Create timeline

Create a detailed, step-by-step timeline of the incident, including when the attacker entered, what actions they took, when the incident was detected, and how the response unfolded. This timeline supports lessons learned and future improvements.

#### IV.6.1.b Evaluate processes

Assess how well detection, containment, eradication, and recovery activities worked. Review communication, escalation timing, decision-making, and any gaps in tools or staffing to identify areas that need improvement.

### IV.6.2 Document findings

#### IV.6.2.a Incident report

Produce a comprehensive incident report that includes what happened, how it was detected, the impact, actions taken, lessons learned, and recommendations for preventing similar incidents.

#### IV.6.2.b Lessons learned

Summarize key lessons learned and outline recommended improvements. Share appropriate findings with leadership and relevant teams to guide future readiness.

### IV.6.3 Implement changes

#### IV.6.3.a Update IR processes

Update the Incident Response Plan, procedures, and playbooks to incorporate lessons learned and strengthen future response capabilities.

#### IV.6.3.b Implement mitigations

Implement security improvements—such as updated controls, patches, training, monitoring, or tooling—to address the vulnerabilities and weaknesses revealed during the incident.

# 💬 V. Communication Plan

# V Communication Plan

## V.1 Internal Communication

### V.1.a Immediate Notifications

Notify executive leadership, the Incident Response Team (IRT), Legal, Compliance, and all affected business units immediately upon incident confirmation.

### V.1.b Ongoing Internal Updates

Provide timely and regular updates to leadership and key stakeholders throughout the incident response lifecycle, including containment, eradication, and recovery status.

## V.2 **External Communication**

### V.2.a **Notifications to Customers, Partners, and External Stakeholders**

Notify customers, partners, vendors, or other external stakeholders *when required by law, regulation, contractual obligations,* or when the incident poses a material risk to them.

All communications must be coordinated through Legal, Communications/PR, and the Incident Response Lead.

### V.2.b **Regulatory and Legal Reporting Requirements**

Assess the incident against all applicable regulatory reporting requirements (e.g., state breach laws, federal regulations, industry mandates, international standards).
If the incident meets mandatory reporting thresholds:

- Notify regulators within legally required timeframes
- Ensure accuracy, transparency, and completeness
- Document all reporting decisions and communications

If the incident **does not** meet mandatory thresholds, retain documentation of the assessment and consult with Legal before issuing any optional disclosures.

### V.2.c **Public Disclosure and Media Communication**

Coordinate all public statements—including media responses, press releases, or website notices—through Legal and Communications/PR.
Public messaging must be:

- Factually accurate
- Consistent
- Aligned with regulatory requirements
- Mindful of protecting ongoing investigations and customer trust

No employee should make public statements about the incident unless authorized.

# 🎯 VI Key Performance Indicators (KPIs)

# VI Key Performance Indicators (KPIs)

## VI.1 Time to Detect (TTD)

The time elapsed from the first malicious activity or unauthorized action until the incident is detected by monitoring tools or personnel..

## VI.2 Time to Contain (TTC)

The duration from incident detection to effective containment, including isolating affected systems, disabling compromised accounts, and blocking malicious activity.

## VI.3 Time to Recover Baseline Security Posture (TTRBSP)

The time from containment to the full restoration of systems, data, and security controls to their normal, pre-incident state.

## VI.4 Incident Closure Rate

The percentage of incidents fully contained, eradicated, and validated as resolved within the organization's defined response timeframes.

## VI.5 Post-Incident Improvement Rate

The percentage of lessons learned from incidents that result in measurable improvements, such as updated policies, playbooks, security controls, or employee training.

# 🧨 VII. Common Mistakes & Mitigations

# VII Common Mistakes & Mitigations

## VII.1 Overlooking early indicators

### VII.1.a Mistake

Dismissing minor anomalies as false positives.

### VII.1.b Mitigation

Combine automated alert prioritization with regular SIEM tuning and analyst review to ensure early anomalies are investigated and not overlooked.

## VII.2 Inadequate documentation

### VII.2.a Mistake

Failing to log actions during incident response.

### VII.2.b Mitigation

Assign a dedicated scribe or use a standardized incident tracking system to log all actions, decisions, and observations during the response.

# VII.3 Premature recovery

## VII.3.a Mistake

Reconnecting systems before complete eradication.

## VII.3.b Mitigation

Thoroughly validate systems and networks are free of malware or attacker access before reconnecting to production. Use scans, testing, and verification of eradication steps.

# VII.4 Neglecting post-incident reviews

## VII.4.a Mistake

Skipping post-mortem analysis due to time constraints.

## VII.4.b Mitigation

Require post-incident reviews for all incidents, with documented lessons learned, process improvements, and accountability assigned to ensure follow-through.

# 🛠️ VIII. Tools & Techniques

# VIII Tools & Techniques

## VIII.1 Detection

SIEM (Splunk, QRadar), IDS/IPS (Snort, Suricata), EDR (CrowdStrike, SentinelOne).
-SIEM for centralized logging/alerting. Alerts need proper tuning and review by an analyst.
-IDS/IPS for network-based threat detection
-EDR for endpoint threat detection and response

## VIII.2 Containment

NAC (Cisco ISE), firewalls (Palo Alto, Fortinet),VPNs, switch port controls, or cloud access policies.
-NAC can isolate or restrict compromised devices.
-Firewalls block malicious IPs or segments
VPNs, switch port controls, or cloud access policies

## VIII.3 Eradication

Antivirus/Antimalware (Sophos, Malwarebytes, Windows Defender),EDR tools for advanced persistent threats (APT) or manual forensic remediation tools.

## VIII.4 Recovery

Backup solutions (Veeam, Acronis).
-Backups are the primary tool for restoring systems to a known-good state.

## VIII.5 Analysis

Forensic tools (FTK, EnCase, Wireshark, Autopsy, X-Ways, Volatility for memory forensics, or log analysis tools)

# 🧰 IX. Review & Maintenance

# IX Review and Maintenance

## IX.1 Annual updates

Review the IRP at least annually and update it whenever significant changes occur, such as after an incident, changes in systems, emerging threats, or lessons learned. Ensure the plan remains current, practical, and compliant with regulations.

## IX.2 Ongoing Training

Conduct regular training sessions, including quarterly tabletop exercises and hands-on simulations. Tailor training to role-specific responsibilities, track participation, and evaluate effectiveness to ensure readiness.

## IX.3 First-Party Audits

Conduct regular audits of the IRP and incident response practices using a combination of internal experts and trusted, confidential external reviewers. This ensures the plan is effective, objective, and aligned with best practices while protecting sensitive internal information and confidentiality.

# Appendix

# APPENDIX

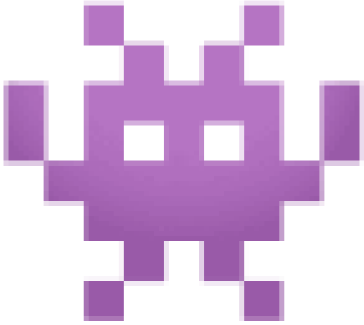
capybara Unlimited

# 📚 Playbooks

📚

# IR PLAYBOOKS

# 👾 Malware Infection



# Malware Infection Playbook

## 1. Identify and contain the malware

Quickly detect and limit the spread of the malware to minimize damage.

### 1.1 Identify and isolate infected systems

Quickly detect affected systems and isolate them from the network to prevent further spread. Collect logs, memory snapshots, and disk images for analysis without exposing other systems.

### 1.2 Conduct preliminary analysis

Gather initial indicators of compromise (e.g., suspicious files, processes, connections) from isolated systems to inform containment and eradication strategies.

## 2. Perform static analysis of the malware sample

Analyze the malware file without executing it to understand its characteristics.

### 2.1 Inspect file structure and metadata

Examine the malware file's properties, including size, hash values, and embedded metadata.

### 2.2 Extract embedded strings and suspicious code

Use tools like VirusTotal, IDA Pro, Ghidra, to identify readable text and suspicious code within the file.

# 3. Perform dynamic analysis in a controlled environment

Observe malware behavior in real-time to understand its operational capabilities.

## 3.1 Execute malware on a clean system

Execute malware in a secure, isolated sandbox or virtual lab environment that mimics the production environment. Collect forensic artifacts without risking production systems.

## 3.2 Record system modifications and activities

Document changes to the registry, file systems, and active processes during execution. Make sure changes are logged in the isolated environment.

# 4. Conduct network traffic analysis

Analyze communication attempts made by the malware to uncover external connections.

## 4.1 Capture network traffic

Capture and analyze network traffic from isolated or mirrored systems to identify connections to command-and-control servers or exfiltration endpoints.

## 4.2 Identify external entities

Look for connections to command-and-control (C2) servers or data exfiltration endpoints.

# 5. Investigate behavioral patterns and persistence mechanisms

Determine how the malware survives and operates over time.

## 5.1 Identify persistence techniques

Investigate changes such as registry modifications, scheduled tasks, or startup files.

## 5.2 Examine behavioral indicators

Look for recurring patterns, such as periodic network requests or file execution. Also checking scheduled tasks, service entries, autoruns, and startup scripts, and correlating with IOC databases.

# 6. Eradicate the malware and recover systems

Remove the malware and restore affected systems to their original state.

## 6.1 Deploy cleanup tools

Use antivirus or specialized malware removal tools to eradicate infections.

## 6.2 Restore from clean backups

Reinstall systems and data using backups confirmed to be malware-free.

## 6.3 Apply mitigations to prevent reinfection

Address any vulnerabilities that permitted the original infection to occur by applying the appropriate mitigation. These can include patching, access control review, and network segmentation.

# 7. Post-incident reporting and prevention

Document lessons learned and strengthen defenses against future incidents.

## 7.1 Generate incident report

Detailed findings, response steps, and impact assessment in a comprehensive report.

## 7.2 Implement prevention measures

Update security policies, patch vulnerabilities, and educate staff to avoid recurrence. Lessons learned should feed back into the IRP, playbooks, training, and monitoring rules.

# 🪝 Phishing

# Phishing Playbook

## 1. Identify and verify the phishing email

Confirm that the suspicious email is a phishing attempt, not a legitimate message.

### 1.1 Analyze email headers and content

Inspect email headers for inconsistencies like mismatched sender domains or unusual reply-to addresses. Review the content for generic greetings, poor grammar, or urgent requests for sensitive information.

### 1.2 Compare against known phishing indicators

Cross-check email elements against known phishing indicators, such as fake links (hover over to inspect URLs), suspicious attachments, or spoofed branding.Reference internal IOC database or threat intelligence feeds.

## 2. Contain the threat

Prevent further exposure or escalation.

### 2.1 Isolate the email

Instruct recipients not to click any links, open attachments, or reply. Move the email to a quarantined folder or flag it as phishing.

### 2.2 Notify IT/security team

Report the phishing email to the organization’s security team immediately, following internal reporting procedures.

## 3. Investigate the impact

Determine the extent of the threat and affected users.

### 3.1 Verify user interaction

Assume potential compromise; actively check logs and EDR alerts.

### 3.2 Check affected systems

Use endpoint detection and response (EDR) tools to monitor devices for unusual activity or malware from potential downloads. Use EDR, SIEM, and network logs to detect indicators of compromise.

## 4. Eradicate the threat

Remove malicious elements and secure compromised accounts or systems.

### 4.1 Preserve phishing emails

Leave the phishing emails in user inboxes for the security team to study. Ensure emails are copied to a secure repository for analysis, not left in user inboxes where they could be accidentally clicked.

### 4.2 Secure compromised accounts

If credentials were entered, reset passwords immediately and monitor account activity for unauthorized access.

## 5. Educate and prevent future incidents

Strengthen user awareness and defenses.

### 5.1 Notify all employees

Provide clear, concise guidance on what was phishing, how to identify similar emails, and what actions to take.

### 5.2 Provide training

Conduct phishing awareness sessions and simulated phishing exercises to reinforce detection skills. Integrate lessons learned from this incident into training content.

## 6. Monitor and report

Ensure no residual threats remain and document the incident.

### 6.1 Monitor for reoccurrence

Track systems and user accounts for unusual activity linked to the phishing attempt.

### 6.2 Document the incident

Log the phishing attack, actions taken, and lessons learned to refine future response efforts. Ensure the incident report includes affected users, phishing characteristics, mitigation steps, and recommendations for future prevention.

# 🌊 Denial-of-Service

# Denial-of-Service Playbook

## 1. Identify and characterize the attack traffic

Confirm the nature of the traffic to ensure it’s consistent with a DoS attack rather than a legitimate traffic spike.

### 1.1 Automate detection of unusual number of packets

Use network monitoring tools to identify unusual traffic patterns, such as excessive requests from specific IPs or a high volume of specific packet types. Detection should differentiate between legitimate traffic spikes ( marketing campaigns, seasonal demand) and malicious patterns.
Include anomaly detection using SIEM, NMS, or cloud traffic analytics.

### 1.2 Classify the type of DoS

Characterize the traffic to determine if it aligns with known DoS attack patterns (*e.g.,* SYN flood, ICMP flood). Classify by volumetric, protocol-based, or application-layer attacks.

## 2. Measure traffic volume and bandwidth consumption

Accurately assess traffic volume to prioritize resources and decide on appropriate mitigation strategies.

### 2.1 Assess scope of DoS

Monitor network metrics to assess the scope, including packet size, rate of incoming requests, and bandwidth impact. Include both inbound and outbound traffic metrics. Monitor network metrics including packet rate, size, and bandwidth impact.

### 2.2 Evaluate impact of DoS

Use these metrics to understand the impact on network resources and how severely the attack affects performance. Assess affected services and endpoints to understand performance degradation and prioritize mitigation resources.

## 3. Locate the source of attack traffic

Identify potential malicious sources to inform targeted blocking or rate-limiting actions.

### 3.1 Identify patterns in DoS traffic source

Use IP tracking and network monitoring to identify patterns in IP addresses, geographic sources, or ASN numbers. Identify IP addresses, geographic regions, and ASN patterns associated with the attack.

### 3.2 Analyze identified patterns

Document any consistent IP ranges or indicators that suggest botnet involvement or attack origin. Correlate with threat intelligence to determine if the traffic originates from botnets or known malicious sources.

## 4. Identify affected services and network components

Pinpoint affected systems to prioritize protective measures and service continuity efforts.

### 4.1 Identify affected internal systems

Determine which servers, services, or endpoints are being impacted (e.g., web servers, DNS, application servers). Prioritize mitigation for critical business services to minimize operational disruption.

## 5. Implement and monitor mitigation measures

Ensure mitigation is effectively reducing malicious traffic while maintaining service availability for legitimate users.

## 5.1 Implement firewall rules

Apply network defenses such as firewall rules or rate-limiting based on the type of DoS attack. Apply network defenses such as rate-limiting, firewall rules, or cloud-based DoS mitigation services.

## 5.2 Monitor effectiveness of firewall mitigations

Use network monitoring tools to continuously assess the effectiveness of these defenses. Continuously monitor network performance and mitigation effectiveness to ensure legitimate users maintain access while attack traffic is blocked.