

mistralai/magistral-small-2509

Good day.

You will be used to help create a Incident Response playbook. Designed for a specific scenario.

Some baseline rules before we begin.

Structure your answers in a well-organised manner top to bottom.

You are not allowed to lie.

If you do not have the information to complete a task inform what information is lacking.

mistralai/magistral-small-2509

> Thought for 51.64 seconds

Good day! I'm ready to help you create an Incident Response playbook tailored to a specific scenario. To start, could you please specify the type of incident this playbook is intended for? For example, is it for a data breach, ransomware attack, phishing campaign, DDoS attack, or something else?

Here's how we can structure the playbook once the scenario is clear:

1. **Introduction and Purpose:** Define the scope and objectives of the playbook.
2. **Roles and Responsibilities:** Identify key stakeholders and their roles during an incident (e.g., Incident Response Team, IT, Legal, PR).
3. **Incident Classification:** Criteria for identifying and classifying the specific type of incident.
4. **Detection and Reporting:**
 - Methods for detecting the incident (e.g., monitoring tools, user reports).
 - Steps for reporting it to the appropriate team.
5. **Containment, Eradication, and Recovery:**
 - Immediate steps to contain the threat (e.g., isolating affected systems).
 - Actions to eradicate the cause (e.g., removing malware, patching vulnerabilities).
 - Procedures for restoring normal operations safely.
6. **Communication Plan:** Who needs to be informed internally and externally, when, and how.
7. **Post-Incident Activities:**
 - Lessons learned and root cause analysis.
 - Updates to policies or defenses based on the incident.

If you provide more details about the scenario, I can help tailor these sections to fit your needs precisely. For example, if it's a ransomware attack, containment might focus on isolating infected systems and preventing lateral movement, while recovery would emphasize restoring from backups.

Then to begin.

We will begin working and structuring a Incident Response Playbook focused on the threat of Docuphishing.

Incident Response Playbook for Docuphishing

1. Introduction and Purpose

This playbook outlines the response procedures for docuphishing incidents—attacks that use fake or manipulated documents (e.g., PDFs, Word files) to deceive users into revealing sensitive information or executing malicious actions. The goal is to minimize impact, restore operations, and prevent future attacks.

2. Roles and Responsibilities

- **Incident Response Team Leader:** Coordinates the response effort.
- **IT/Security Team:**
 - Investigates reports of suspicious documents.
 - Isolates affected systems, removes malware, and restores services.
- **HR/Compliance Team:** Ensures policies are followed and provides user training reminders.
- **Legal/PR Team:** Advises on communication if the incident involves data breaches or regulatory reporting.

3. Incident Classification

Incidents are categorized based on severity:

- **Low:** Suspicious document reported; no evidence of compromise.
- **Medium:** User clicked a link or downloaded a file; potential malware infection.
- **High:** Credentials compromised, unauthorized access detected, or data exfiltrated.

4. Detection and Reporting

Indicators of Compromise (IOCs):

- Unexpected attachments from unknown senders or spoofed addresses.
- Documents with suspicious links, macros, or requests for sensitive information (e.g., passwords, financial details).
- Reports from users about odd behavior after opening documents (e.g., pop-ups, redirects).

Reporting Process:

- Users should report suspicious emails/documents immediately to the IT helpdesk via phone (extension XXXX) or email (security@company.com).
- Security tools (e.g., email filters, sandboxing solutions) may automatically flag malicious attachments.

5. Containment, Eradication, and Recovery

Containment Steps:

1. Isolate affected user accounts (disable network access if necessary).
2. Block sender domains at the email gateway to prevent further attacks.
3. Instruct users not to interact with suspicious documents; preserve evidence for analysis.

Eradication Steps:

1. Scan devices of compromised users for malware using updated antivirus tools.
2. Remove or quarantine malicious files (e.g., PDFs, macros).
3. Reset passwords for all compromised accounts and related services (email, cloud storage).

Recovery Steps:

- Restore affected systems from clean backups after verifying their integrity.
- Re-enable access to systems only after confirming they are malware-free.

6. Communication Plan

- **Internal Communication:**
 - Notify IT and security teams immediately upon detection.
 - Inform leadership and HR for awareness campaigns or policy updates.
- **External Communication:**
 - Consult legal to determine if regulatory reporting is required (e.g., for data breaches under GDPR, CCPA).
 - Prepare a statement for stakeholders if reputational risk arises.

7. Post-Incident Activities

1. **Review:** Assess how the attack succeeded (e.g., bypassed email filters, user training gaps).

2. **Improve Defenses:**

- Enhance email filtering to catch malicious document attachments.
- Conduct phishing simulations with docuphishing scenarios for user awareness.

3. Documentation: Update this playbook based on lessons learned.

Next Steps:

- Would you like to refine any section or add specific tools/procedures your team uses (e.g., SIEM, EDR)?
- Should we include a checklist or timeline for critical actions?

Before we continue, go over your last response 5 times to identify any potential flaws in the workflow.

Revised Incident Response Playbook for Docuphishing

1. Introduction and Purpose

Unchanged, but emphasize the need to address both technical and human factors.

2. Roles and Responsibilities

Add:

- **Forensics Team:** For high-severity incidents, preserve system images before cleanup for analysis.

3. Incident Classification (Updated)

High Severity:

- Credentials compromised AND signs of data exfiltration or lateral movement.
- Malware detected that persists beyond the initial document (e.g., backdoors).

4. Detection and Reporting

IOCs (Expanded):

- Documents with embedded exploits, zero-day vulnerabilities (require manual review by security analysts).
- Requests for sensitive information (e.g., "Please confirm your password to view this document").
- Unusual outbound traffic from user devices (potential exfiltration).

Reporting:

- Users can report via a dedicated, non-punitive channel (e.g., phishing@company.com or a web form) with reassurance that reports won't result in discipline.

5. Containment, Eradication, and Recovery

Containment (Enhanced):

1. Isolate affected user account, device, network shares, and shared drives to prevent lateral movement.
2. Block sender domain at email gateway and flag similar domains for monitoring.
3. For high-severity cases:
 - Shut down outbound internet access for the affected system to halt potential exfiltration.

Eradication (Enhanced):

1. Forensic imaging of compromised systems before any changes are made (for RCA).
2. Scan for malware, including memory analysis to catch non-file-based threats.
3. Check for persistence mechanisms:
 - Scheduled tasks, startup items, or registry changes (Windows) or launch agents (macOS/Linux).
4. Reset passwords for all accounts and enforce MFA where possible.

Recovery:

- Restore systems from clean backups; verify integrity with checksums before going live.

6. Communication Plan

Add:

- **Law Enforcement:** Notify if financial fraud, identity theft, or significant data loss occurs.
- **Third Parties:** Consult legal for notifications to banks, clients, or regulators (e.g., under GDPR, notification may be required within 72 hours).

7. Post-Incident Activities

1. Root Cause Analysis (RCA):

- Identify how the document bypassed filters and if any user actions could have prevented it.
- Document findings in a report due within 5 business days of containment.

2. Improvements:

- Update email filters with new IOCs; test for zero-day scenarios.
- Conduct docuphishing simulations monthly to train users.

3. Timeline:

- Playbook review and updates: Every 6 months or after a significant incident.

Next Steps:

- Should we include escalation procedures for off-hours incidents (e.g., contact numbers)?
- Are there specific tools (EDR, SIEM) your team uses that should be referenced in the checklist?

Please do include a checklist for a quick reference.

Revised Incident Response Playbook for Docuphishing

1. Introduction and Purpose

This playbook outlines steps to respond to docuphishing incidents, ensuring swift containment, eradication, and recovery while preserving evidence.

2. Roles and Responsibilities

- IT Helpdesk: Initial triage and reporting.
- Security Team: Investigation and containment.
- Forensics Team: High-severity cases; system imaging for RCA.
- Legal/Compliance: External notifications (law enforcement, regulators).

Quick Reference Checklist

1. Initial Response

- User reports suspicious document via phishing@company.com or hotline (+1234).
- Verify sender address, domain, and requests for sensitive information.
- Confirm if the document was opened; note symptoms (pop-ups, redirects).

2. Containment

- Isolate:**
 - User account + device from network shares and critical systems.
 - For high severity: Disable outbound internet access on compromised system.
- Block sender's domain at email gateway; flag similar domains for monitoring.

3. Eradication

- Preserve evidence:** Capture forensic images of affected systems *before* cleanup.
- Scan for malware (file + memory); check persistence mechanisms:
 - Scheduled tasks, registry changes, startup items.
- Reset passwords for all user accounts; enforce MFA where possible.

4. Recovery

- Restore systems from clean backups; verify integrity with checksums.
- Re-enable access only after confirming malware-free status.

5. Post-Incident

- Document incident details (who/what/when) for RCA within 24 hours.
- Update email filters with new IOCs; schedule docuphishing training.

3. Incident Classification

- Low: Suspicious document reported, no interaction or symptoms.
- Medium: Document opened but no malware detected (e.g., phishing link not clicked).
- High: Malware confirmed, credentials compromised, or signs of data exfiltration.

4. Detection and Reporting

IOCs:

- Mismatched sender domain/name.
- Requests for sensitive information (e.g., "Please verify your password").
- Embedded exploits (zero-day; escalate to security analysts).

Reporting Channels:

- Phone: Security hotline (ext. 5000, 24/7).
- Email: phishing@company.com with subject line "Docuphishing Report".

5. Containment

- Immediate Actions:**
 - Isolate user device from all network shares and critical systems.
 - Block sender's domain at email gateway; monitor similar domains.
- High Severity:**
 - Disable outbound internet access to halt potential exfiltration.

6. Eradication

1. Evidence Preservation: Forensic imaging of affected systems (for RCA).
2. Malware Removal:
 - File and memory scans using updated tools.
 - Check for persistence mechanisms (e.g., scheduled tasks, registry entries).
3. Credential Hygiene:
 - Password reset for all user accounts + related services (email, cloud storage).
 - Enforce MFA for affected users.

7. Recovery

- Restore systems from clean backups; verify integrity with checksums.
- Re-enable access only after confirming malware-free status via two scans.

8. Communication Plan

- Internal:
 - Notify IT, security teams immediately; brief HR for user training triggers.
- External:
 - Consult legal for notifications to:
 - Regulators (e.g., GDPR: within 72 hours if data breach).
 - Law enforcement (for financial fraud or identity theft).
 - Third parties (banks, partners) as advised by legal.

9. Post-Incident Activities

1. Root Cause Analysis (Due in 5 days):
 - How did the document bypass filters?
 - Could user training have prevented it? Document findings.
2. Improvements:
 - Update email filters with new IOCs; test for zero-day scenarios.
 - Conduct docuphishing simulations monthly to train users.
3. Timeline:
 - Playbook review every 6 months or after a high-severity incident.

Next Steps:

- Should we include escalation procedures for off-hours incidents (e.g., contact numbers)?
- Are there specific tools (EDR, SIEM) your team uses that should be referenced in the checklist?

Please do include the escalation procedures for off-hours incidents.

Do include in the playbook a procedure of designated staff authorised to mainly handle the escalated incident should there be need.(Incident response team)

And repeat the procedure 5 times to try to remove any additional flaws.



Final Incident Response Playbook for Docuphishing

1. Introduction

This playbook provides a structured response to docuphishing incidents, including off-hours escalation and designated roles for the Incident Response Team (IRT).

2. Roles and Responsibilities

Incident Response Team (IRT):

- **Incident Lead:** Oversees process; reports to executives.
 - Primary: John Doe (john.doe@company.com | +1234567890)
 - Backup: Jane Smith (+1234567891), Mary Green (for nights).
- **Security Analyst:** Threat assessment, containment approvals.
 - Primary: Alice Lee; Backup: Bob Brown.
- **IT Administrator:** Executes technical actions (checklist below).
 - On-call rotation published monthly.
- **Legal Representative:** Compliance checks and notifications.
 - Primary: Sarah White (+1234567892).

Authority:

- IRT has authority to:
 - Isolate systems, disable network access.
 - Notify regulators (with legal rep's approval).
 - Allocate up to \$10K for immediate response actions.

3. Off-Hours Escalation Procedure

1. **Step 1:** Helpdesk receives report → Classify severity:
 - Low/Medium: On-call IT staff notified.
 - High: Call security lead #1 + text backup team on Signal (group ID: IRTeam).
2. **Step 2:** If no IRT response within 20 mins:
 - CEO on-call designates an acting lead from pre-approved list:
 - CISO, IT Director, or Chief Compliance Officer.
 - Acting lead forms the IRT and takes full authority for the incident.



4. Quick Reference Checklist (Repeatable Procedure)

Initial Response

- User reports via phishing@company.com or hotline (+1234).
- Verify sender domain; confirm if document was opened.
- Classify severity → Escalate high incidents per above procedure.

Containment

- Isolate affected device (network shares, critical systems).
- Block sender's domain at email gateway.
- For high severity: Disable outbound internet access.

Eradication

- Capture forensic images of compromised systems.
- Scan for malware (file + memory); check persistence mechanisms.
 - Scheduled tasks, registry changes, startup items.
- Reset passwords; enforce MFA for affected accounts.

Recovery

- Restore from clean backups; verify integrity with checksums.
- Re-enable access only after confirming malware-free status.

Post-Incident (Within 24 Hours)

- Document incident details for RCA (due in 5 days).
- Update email filters with new IOCs; schedule training simulation.

5. Decision Matrix

Condition	Action
Malware confirmed	Legal rep notifies regulators within 2 hours; isolate affected segment.
Credentials compromised	Reset passwords + MFA enforcement within 1 hour; audit logs.
Critical systems at risk	Incident lead briefs CEO; consider shutdown of affected services.

6. Communication Plan

Internal:

- IRT communication: Secure Slack channel #incident-response; Zoom bridge (ID: 123456).
- Updates to executives every 2 hours for high-severity incidents.

External:

- Legal rep coordinates with PR for public statements if required.
- Third-party vendors notified only after legal approval.

7. Review and Retirement

- Playbook reviewed quarterly; updated after major incidents or changes in regulations.
- Incident retired when:
 - Systems confirmed clean (verification by IT admin + security analyst).
 - Lessons learned meeting held with all stakeholders.



Now with this information, we will move on to a next step to apply and fulfill the following steps. Some of them has already been completed from you earlier answers. So now follow it top to bottom and fill in each selected step.

The scenario is Docuphishing as we started writing the playbook for.

1. Select a cyber incident scenario (e.g., ransomware, data breach).
2. Define IR phases: preparation, detection, containment, eradication, recovery, and lessons learned.
3. Develop communication templates for management, legal, and technical teams.
4. Create a step-by-step playbook and runbook (who does what, when, and how).
5. Use an LLM to draft communication templates, refine workflow language, and suggest checklist items."

Final Incident Response Playbook for Docuphishing

1. Scenario

Docuphishing: A social engineering attack where malicious documents (e.g., PDFs, Word files) are sent to trick users into revealing information or installing malware.

2. IR Phases and Workflow

Phase	Key Actions
Preparation	<ul style="list-style-type: none">- Employee training on identifying suspicious documents.- Regularly test backup solutions; maintain an approved document list.
Detection	<ul style="list-style-type: none">- User reports via phishing@company.com or hotline (+1234).- Verify sender domain and document source; classify severity.
Containment	<ul style="list-style-type: none">- Isolate affected systems (network, shares); block malicious domains.- For high-severity: Disable outbound internet access for affected segment.
Eradication	<ul style="list-style-type: none">- Capture forensic images; scan for malware, persistence mechanisms.- Reset passwords + enforce MFA for compromised accounts.
Recovery	<ul style="list-style-type: none">- Restore from clean backups (verified with checksums).- Re-enable access only after confirming malware-free status.
Lessons Learned	<ul style="list-style-type: none">- Retrospective meeting within 5 days; document findings and recommendations.

3. Communication Templates

For Management:

Subject: [URGENT] Docuphishing Incident – Status Update

Body:

Dear [Name],

A docuphishing incident was detected at [time]. The IRT has been activated. Current phase: [containment/eradication/recovery]. Potential impact: [brief description]. Next update in [X] hours.

Regards,

[Incident Lead Name]

For Legal Team:

Subject: Docuphishing Incident – Compliance and Notification Requirements

Body:

Dear Legal Team,

A docuphishing incident involving [number] employees has been identified. Please assess if regulatory notification is required (e.g., GDPR, CCPA). Prepare draft statements for external parties if necessary.

For Technical Team:

Subject: Docuphishing Incident – Immediate Actions Required

Body:

Team,

Malicious document [filename] confirmed. Immediate actions:

1. Isolate affected systems (list attached).
2. Run malware scans; check persistence mechanisms.
3. Submit IOCs to SIEM for monitoring. Coordinates in Slack #incident-response.

4. Playbook and Runbook

Playbook Steps:

1. Preparation:

- Train employees quarterly on docuphishing risks.
- Maintain a whitelist of approved document formats (e.g., .pdf, .docx from trusted sources).

2. Detection:

- User reports incident via designated channels.
- Verify if document was opened and if macros/scripts were executed.

3. Containment:

- Isolate user accounts; disable network shares for affected systems.
- Block sender's domain at email gateway (if confirmed malicious).

4. Eradication:

- Forensic imaging of compromised endpoints.
- Scan for malware, check registry/startup items for persistence.

5. Recovery:

- Restore from clean backups; verify integrity with checksums.
- Monitor affected systems for 72 hours post-recovery.

Runbook (Timeline and Responsibilities):

Role	Task	Timeline
Helpdesk	Log incident; classify severity.	Immediate
Security Analyst	Verify malicious document; identify IOCs.	Within 15 mins
IT Administrator	Isolate systems; block sender domain at gateway.	Within 30 mins
Incident Lead	Form IRT (Zoom bridge ID: 123456); brief executives if high severity.	Within 20 mins
Legal Representative	Assess notification requirements; prepare draft statements.	Within 1 hour

5. Additional Checklist Items Suggested by LLM

- Notify all users who received the phishing email to check for signs of compromise.
- Document incident timeline with timestamps for all actions (for RCA).
- Verify backup integrity before recovery; ensure no malware is present in backups.

This playbook is designed to be adaptive. If specific details are missing (e.g., tools used, exact regulatory requirements), please provide them for further refinement.



Can you repeat the last prompt by expanding and going further into the 2 part please.

Expanded Incident Response Playbook for Docuphishing

1. Playbook Steps (Detailed)

Preparation Phase:

- Conduct quarterly training sessions with real-world docuphishing examples.
- Maintain a whitelist of trusted document formats and sources (e.g., only .pdf, .docx from approved vendors).
- Ensure regular backup tests are conducted monthly; verify backup integrity using checksums.

Detection Phase:

- Users report suspicious documents via phishing@company.com or hotline (+1234).
- Security team verifies sender domain against known good senders (SPF, DKIM checks).
- Classify severity based on:
 - Number of recipients affected (low: <5, medium: 6-20, high: >20).
 - Document type (e.g., executable disguised as PDF = high).

Containment Phase:

- Helpdesk isolates user account from network shares and critical systems using Active Directory.
- IT blocks sender's domain at email gateway using Mimecast or similar tool.
- For high severity: Disable outbound internet access for affected segment via Palo Alto firewall rules.

Eradication Phase:

- Capture forensic images of compromised endpoints using FTK Imager.
- Scan systems with antivirus (CrowdStrike) and EDR tools for malware.
- Check for persistence mechanisms: registry keys, startup scripts, scheduled tasks.

Recovery Phase:

- Restore from clean backups; verify integrity using SHA-256 checksums.
- Re-enable access only after confirming malware-free status with two scans (initial + follow-up).
- Monitor affected systems for 72 hours post-recovery for signs of reinfection.

Lessons Learned Phase:

- Conduct a retrospective meeting within 5 days to document:
 - What worked, what didn't.
 - Recommendations for policy or tool improvements (e.g., stricter email filters).

2. Expanded Runbook

Role	Task	Tools/Processes Used	Timeline	Dependencies
Helpdesk	Log incident; classify severity using predefined matrix.	ServiceNow, severity classification guide.	Immediate	None
Security Analyst	Verify malicious document with YARA rules and VirusTotal uploads.	YARA, VirusTotal, SIEM (Splunk).	Within 15 mins	Helpdesk classification
IT Administrator	Isolate affected systems via Active Directory; block sender domain at Mimecast.	Mimecast, Palo Alto firewall, AD.	Within 30 mins	Security Analyst verification
Incident Lead	Form IRT on Zoom bridge (ID: 123456); brief executives for high-severity incidents.	Communication plan, executive summary template.	Within 20 mins	Helpdesk classification
Legal Representative	Assess notification requirements per GDPR/CCPA; draft statements.	Compliance tools, regulatory guidelines.	Within 1 hour	Incident Lead confirmation of severity
PR Team	Prepare internal and external communications if public disclosure needed.	PR templates, social media guidelines.	If high severity	Legal approval
Vendor (EDR)	Assist with forensic analysis if malware detected; provide remote support.	CrowdStrike Falcon, remote access tools.	As requested	Security Analyst request

Additional Checklist Items

- Notify all users who received the phishing email to check for signs of compromise (e.g., unexpected pop-ups).
- Document incident timeline with timestamps for all actions (for Root Cause Analysis - RCA).
- Verify backup integrity before recovery; ensure no malware is present in backups.
- Update email filters to block similar threats based on identified IOCs.

This expanded playbook provides more granular instructions and clarifies roles, tools, and dependencies. If specific details are missing (e.g., exact tools used at your organization), please provide them for further customization.

This is our current IR playbook plan.

Without adding to it can you see any potential improvements.

"IR Plan (Aligned with NIST SP 800-61 Rev. 2):

1. Preparation

Develop IR plan (3.1.1 Preparing to Handle Incidents)

Implement Analysis Hardware and Software (3.1.1 Preparing to Handle Incidents)

Awareness training (3.1.2 Preventing Incidents)

Make sure proper security measures are taken on endpoints (AV, FW, ETC) (3.1.2 Preventing Incidents)

Configure email security, detection tools (3.1.2 Preventing Incidents)

Threat intelligence integration (3.1.2) (regular checks for leaked emails, passwords etc. On the dark web)

2. Detection & Analysis

Identify suspicious emails (3.2.1. Attack Vectors)

Validate incident & classify severity (3.2.2 Signs of an Incident)

Check file hashes using OSINT tools (3.2.3 Sources of Precursors and Indicators)

Collect evidence and/or logs (3.2.3 Sources of Precursors and Indicators)

Determine scope of campaign (3.2.4 Incident Analysis)

Perform initial triage (3.2.4 Incident Analysis)

Document all findings (3.2.5 Incident Documentation)

Determine incident priority (P1-4) (3.2.6 Incident Prioritization)

Notify stakeholders (3.2.7 Incident Notification)

3. Containment, Eradication & Recovery

3a. Containment:

Isolate compromised systems (3.3.1 Choosing a Containment Strategy)

Evidence gathering (3.3.2 Evidence Gathering and Handling)

Identify Attacker (3.3.3 Identifying the Attacking Hosts)

3b. Eradication

Block sender(s) (3.3.4 Eradication and Recovery)

Block IOCs (filehashes, Urls, Subjects, Ips, etc) (3.3.4 Eradication and Recovery)

Disable compromised accounts (3.3.4 Eradication and Recovery)

Disable systems (3.3.4 Eradication and Recovery)

3c. Recovery

Unisolate systems (3.3.4 Eradication and Recovery)

Reinstall compromised systems (3.3.4 Eradication and Recovery)

Reset compromised accounts (3.3.4 Eradication and Recovery)

Monitor for reinfection (3.3.4 Eradication and Recovery)

Validate normal functionality (3.3.4. Eradication and Recovery)

4. Post-Incident Activity

Lessons Learned (3.4.1. Lessons Learned)

Update IR plan (3.4.2. Using Collected Incident Data)

Ensure Proper Incident Documentation and Storage (3.4.3. Evidence Retention) "



Improved IR Playbook (Aligned with NIST SP 800-61 Rev. 2)

1. Preparation

- Develop IR plan (3.1.1) + Conduct quarterly tabletop exercises focused on docuphishing scenarios.
- Implement Analysis Hardware and Software (3.1.1) *Include tools for document analysis (e.g., YARA rules, OLEVBA for macros).*
- Awareness training (3.1.2) + Include phishing simulations with docuphishing examples.
- Ensure proper security measures on endpoints (AV, FW, etc.) (3.1.2) *Ensure EDR is configured to detect document-based exploits.*
- Configure email security, detection tools (3.1.2) + Enable sandboxing for email attachments and macros.
- Threat intelligence integration (3.1.2) *Automate checks for leaked credentials using APIs (e.g., Have I Been Pwned).*

2. Detection & Analysis

- Identify suspicious emails (3.2.1) *Use email gateway with sandboxing to auto-detect malicious documents.*
- Validate incident & classify severity (3.2.2) + Include docuphishing-specific indicators (e.g., unexpected macros).
- Check file hashes using OSINT tools (3.2.3) + Scan for embedded scripts/macros.
- Collect evidence/logs (3.2.3) *Document chain of custody for forensic integrity.*
- Determine scope of campaign (3.2.4) *Check if the campaign targets specific departments/roles.*
- Perform initial triage (3.2.4) + Prioritize based on document type (e.g., executable disguised as PDF = higher risk).
- Document all findings (3.2.5)
- Determine incident priority (P1-P4) (3.2.6) + Define docuphishing-specific criteria for P1-P4.
- Notify stakeholders (3.2.7)

3. Containment, Eradication & Recovery

3a. Containment:

- Isolate compromised systems (3.3.1)
Use VLAN segmentation or group policies.
- Evidence gathering (3.3.2) + Use FTK Imager; document chain of custody.
- Identify Attacker (3.3.3)

3b. Eradication:

- Block sender(s) (3.3.4) + Add to threat intelligence feeds.
- Block IOCs (file hashes, URLs, etc.) (3.3.4)
Include embedded scripts/macros in the blocklist.
- Disable compromised accounts (3.3.4) + Reset passwords for all users who received the phishing email.
- Disable systems (3.3.4) + Patch exploited vulnerabilities.

3c. Recovery:

- Unisolate systems (3.3.4)
After two clean scans.
- Reinstall compromised systems (3.3.4) + Verify backups are malware-free using checksums.
- Reset compromised accounts (3.3.4) + Require MFA re-enrollment for affected users.
- Monitor for reinfection (3.3.4) + For 72 hours with enhanced logging.
- Validate normal functionality (3.3.4)

4. Post-Incident Activity

- Lessons Learned (3.4.1) + Track metrics: MTTD, MTTR. Assign action items with deadlines.
- Update IR plan (3.4.2) + Include docuphishing-specific improvements.
- Ensure proper documentation/storage (3.4.3)

Key Enhancements:

- Added detection for macros/embedded scripts.
- Strengthened recovery with backup verification and MFA re-enrollment.
- Included metrics and action items in Lessons Learned.

This version maintains the original structure while improving docuphishing-specific responses.



Can you go over and work through and focus mainly on the Detection & Analysis section.
Give me the important steps that can be improved from it concerning the docuphishing threat

Improved Detection & Analysis Section (Focused on Docuphishing)

2. Detection & Analysis

1. Identify Suspicious Emails

- Use email gateways with advanced sandboxing (e.g., FireEye, Cylance) to detect malicious documents. *Specifically analyze for:*
- Unexpected attachments (.docm, .xslm, PDFs with embedded JS).
- Emails urging immediate action or containing suspicious links.

2. Validate Incident & Classify Severity

- Confirm docuphishing indicators: *Unexpected macros, obfuscated scripts, requests to enable editing.*
- Use tools like oledump.py for macro analysis.
- Check metadata for unusual authorship or domains.

3. Conduct File Analysis

- **Static Analysis:**
 - Scan files with YARA rules tailored for document exploits (e.g., malicious VBScript, PowerShell snippets).
 - Use PEStudio to analyze document structure without execution.
- **Dynamic Analysis:**
 - Submit the file to a sandbox (Joe Sandbox, Hybrid Analysis) to observe: *Network connections to malicious IPs/domains. Execution of suspicious processes or scripts.*

4. Collect Evidence and Logs

- Gather relevant artifacts: *Windows Event logs for Office activity (Event ID 4104).*
 - User activity logs showing who opened the document.
 - Network logs for outbound connections from the document.
- Document chain of custody to ensure forensic integrity.

5. Determine Scope of Campaign

- Check if the campaign targets specific departments, roles, or individuals.
- Analyze whether documents contain similar patterns (e.g., same exploit kit, C2 servers).

6. Perform Initial Triage

- Prioritize based on: *Risk level of document type (executable disguised as PDF = higher risk).*
 - Presence of known exploits or vulnerabilities (e.g., CVE-2023-XXXX for Office).
 - Whether the document is from a known malicious sender or domain.

7. Document Findings

- Record IOCs, including: *File hashes, embedded script snippets, network connections.*
- Note unusual user behavior that may indicate successful exploitation (e.g., credential access attempts).

8. Determine Incident Priority (P1-4)

- Criteria for docuphishing: *P1: Exploits a zero-day or executes without user interaction. P2: Requires macro enablement but does not immediately execute payloads. P3: Suspicious document with no clear malicious intent yet. P4: Likely false positive (e.g., benign document flagged by heuristic rules).*

9. Notify Stakeholders

- Inform IT, security teams, and relevant business units based on priority.
- Provide a brief summary of findings and next steps.

This section ensures that the detection and analysis process is specifically tailored to docuphishing threats while maintaining a structured approach.

6.83 tok/sec • 2216 tokens • 3.14s to first token • Stop reason: EOS Token Found