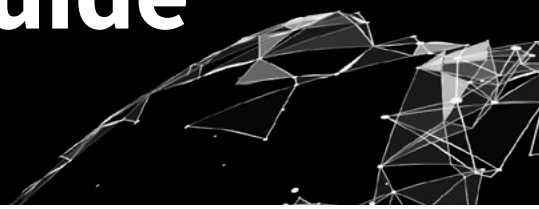
GETTING STARTED

Incident Response Guide



Basic Response Actions

Every security incident is different and requires a unique response. Mature incident response plans may consist of comprehensive flow-charts and detailed playbooks for an exhaustive list of eventualities. These are typically built through experience—either by hiring experienced incident response analysts or by teams who, over time and across multiple incidents, meticulously document which response actions work and which don't. Problematically, as an incident response plan becomes more sophisticated, it also becomes more specific to the organization who developed it and less applicable to others.

In this way, a generalized incident response plan (IRP) can be hugely beneficial because it can demonstrate, on a conceptual level, where to start and how to move forward with remediation. Whether you're dealing with a strain of ransomware like LockerGoga or a trojan like Emotet, you'll often end up following a lot of the same response and remediation actions.

How to Use This Guide

The aftermath of a breach or other incident can be chaotic, and the last thing you want is to be making up an incident response plan on the fly. This guide provides a list of basic response actions that security teams can follow as they respond to and remediate incidents. From here, teams can iterate and work toward their own custom and comprehensive incident response plans.

You will find basic response actions for:

- **HIGH CRITICALITY:** Initiate response within 2 hours
- **MEDIUM CRITICALITY:** Initiate response within 4 hours
- **LOW CRITICALITY:** Initiate response within 24 hours

There's a lot of nuance in responding to a security incident, and the best IRPs will consider an organization's tooling, internal expertise, and other factors. The IRP guidance listed here is not comprehensive, as it lacks critical organizational context. We hope that security teams can use this as a building block to create a brand new response process or improve their existing one.

High Criticality Incidents

INITIATE INCIDENT RESPONSE PLAN WITHIN 2 HOURS

CATEGORY	DESCRIPTION	EXAMPLES
HIGH MALICIOUS	Active and/or successful deployment of malware that poses a direct threat to confidentiality, integrity, or availability of data or systems.	Successful exploitation of a vulnerability or known exploit, including usage of core system binaries in a known malicious fashion.
HIGH SUSPICIOUS	Activity that is not directly attributable to malware but is indicative of an immediate and/or active threat or compromise.	Including but not limited to account manipulation, potential exfiltration of data, or remote access to or from an untrusted external source.

Common Steps for Response and Remediation

1. Assess the scope of the incident. Investigate alerts from active security tools and acknowledge any new detections.
2. Isolate affected endpoint(s) from the network to prevent malware from moving laterally throughout the environment.
3. Kill running process(es) associated with malware.
4. Delete malicious binaries.
5. Block command and control IP addresses at network perimeter.
6. Ban malicious MD5 or SHA2 hashes with whitelisting tool or other relevant product.
7. Remove persistence mechanisms (Scheduled Tasks, Autorun Keys, etc.).
8. Minimize risk of a future attack by assessing administrative controls. Review account usage and reset passwords, limit administrative access where possible, and disable unnecessary file sharing access.
9. Patch vulnerable systems.
10. Mark relevant detections and alerts as remediated.

Escalation Procedure

1. Contact appropriate incident responder(s).
2. Incident response specialists initiate pre-defined response plan specific to the severity and type of the incident.
3. Complete initial scoping assessment to determine systems and data affected by the incident.
4. Notify appropriate personnel if scoping assessment determines that the sensitive data was affected by the incident.
5. Notify relevant stakeholders when the incident has been successfully remediated.
6. Prepare after-action report documenting response process and distribute to appropriate personnel.

Medium Criticality Incidents

INITIATE INCIDENT RESPONSE PLAN WITHIN 4 HOURS

CATEGORY	DESCRIPTION	EXAMPLES
MEDIUM MALICIOUS	Malware identified on an endpoint that does not represent an immediate substantive threat (e.g., no direct execution, indication of ongoing activity, or use of core system binaries).	Direct download of malware (not resulting from exploit or prior compromise) that has not executed, or delivery of a malicious document where the embedded payload has not executed. This classification includes aggressive adware behaving in a manner more consistent with malware, such as changing core system properties and performing system reconnaissance.
MEDIUM SUSPICIOUS	Activity not directly attributable to malware that still poses a security risk or raises suspicion due to context or lack thereof). This can include abnormal activity that requires additional context from the customer, such as environment and domain information.	Remote access to external domains (such as SSH to Dynamic DNS domains) and the use of accessibility tools to bypass Windows logon requirements. Also includes dual-use tools or other activities that are not obviously malicious.

Common Steps for Response and Remediation

1. Assess the scope of the incident. Investigate alerts from active security tools and acknowledge any new detections.
2. Isolate affected endpoint(s) from the network to prevent malware from moving laterally throughout the environment.
3. Kill running process(es) associated with malware.
4. For suspicious activity, investigate details within endpoint data and determine if behavior is legitimate or malicious.
5. Delete any malicious binaries present within the environment.
6. Ban malicious MD5 or SHA2 hashes with whitelisting tool or other relevant product.
7. Mark relevant detections and alerts as remediated.

Escalation Procedure

1. Primary responder will initiate remediation within 4 hours.
2. Document response actions and notify relevant stakeholders as needed upon remediation.

Low Criticality Incidents

INITIATE INCIDENT RESPONSE PLAN WITHIN 24 HOURS

CATEGORY	DESCRIPTION	EXAMPLES
LOW: ADWARE	These applications use deceptive techniques to ensure installation, including masquerading as other known software, claiming to benefit the user, and bundling additional unwanted software. Adware is often bundled with known applications in order to add the appearance of legitimacy.	Unwanted software that surreptitiously performs actions such as changing browser settings and homepages, redirecting search results, and displaying advertisements to the user.
LOW: RISKWARE	Tools that are typically installed intentionally but are designed to circumvent security policy and controls. Some have legitimate use cases in certain scenarios, but on a broader scale introduce additional risk due to their nature and method of use.	Programs designed to prevent an endpoint from sleeping and proxy software used to evade internet content filtering.
LOW: PEER-TO-PEER (P2P)	Ad hoc and uncontrolled usage of a decentralized, distributed computing architecture.	P2P software is commonly used with sharing digital content (music, movies, games). This introduces risk via pirated content, resource consumption (network and computer), data exposure, and unintended malware downloads.

(Continued on next page)

Common Steps for Response and Remediation (Low)

1. Acknowledge detection(s).
2. Kill running process(es).
3. Contact affected end user.
4. Uninstall unwanted programs.
5. Mark as remediated.

Escalation Procedure (Low)

1. Primary responder will remediate detection within 24 hours.
2. Document response actions and notify relevant stakeholders as needed upon remediation.