NOVEMBER 2020

Incident Response Process

Handling Cybersecurity Incidents according to NIST SP-61 Rev. 2

LIFARS
your digital world, **secured**

TABLE OF CONTENTS

LIFARS
your digital world, secured

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

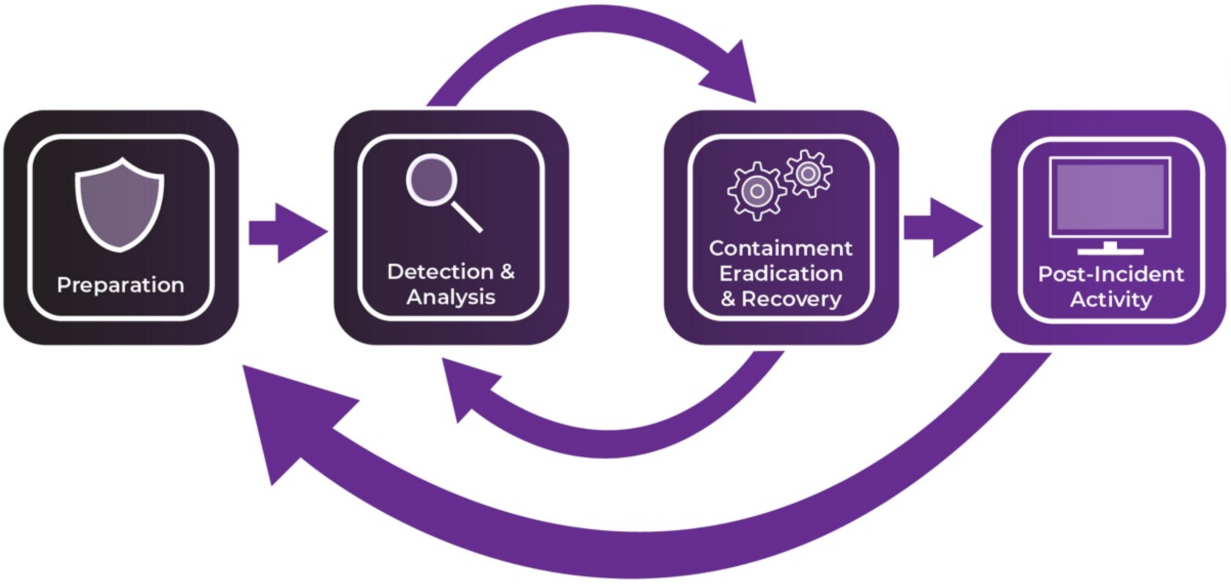
INTRODUCTION

According to ISO/IEC 27035:2011 on Information security incident management, an information security incident is a "single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security".

Incident response is a never-ending process with the end-goal of reducing damage to the organization. To be effective, it requires constantly improving methodology and adapting to new threats.

The incident response process consists of four phases:

- Preparation
- Detection and Analysis
- Containment, Eradication, & Recovery
- Post-Incident Activity



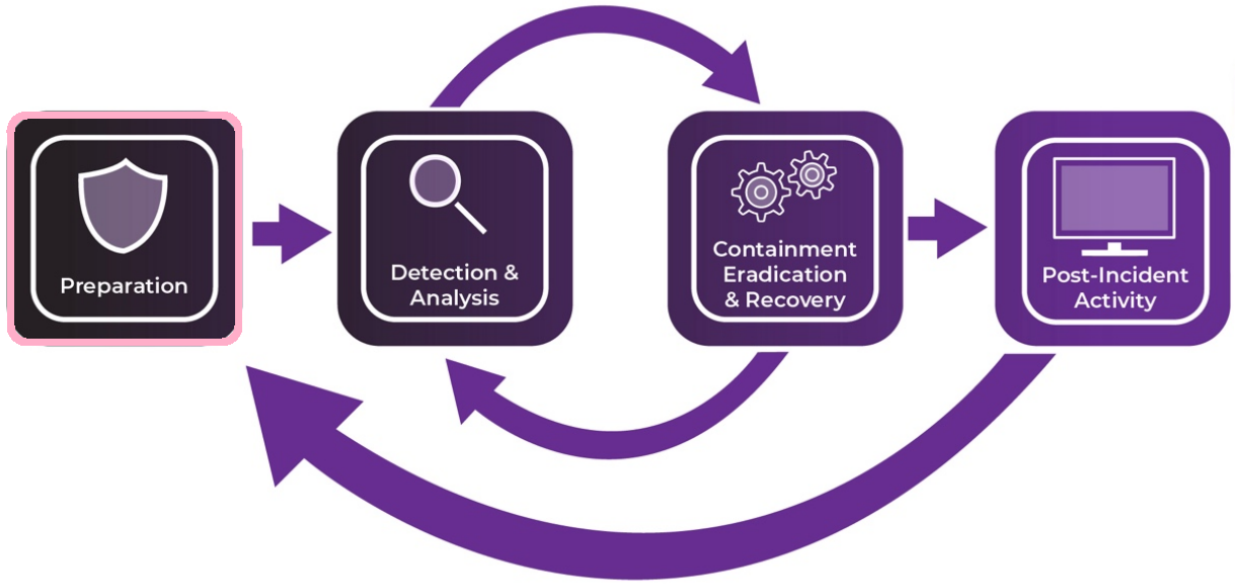
> *With offices in NYC and Europe, we can deploy our team virtually anywhere in the world. For mission critical systems LIFARS implements effective remote cyber incident response by deploying cyber-attack response team to the local enterprise environment.*

LIFARS
your digital world, secured

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

PREPERATION

When not actively responding to incidents, the incident response team should spend the time preparing for the next incident. Being well prepared can not only reduce the initial response time, but also the time required to resolve the incident and restore normal business operations. The preparation phase includes preparation of the needed software, hardware tools and documentation & procedure updates. As threats are constantly evolving, a very important part of this phase is also education.



A. Documentation Revision

The incident response team should ensure that their documentation is up to date on a periodic basis. Playbooks & checklists need to be ready and updated with the latest software revisions in mind and must reflect lessons learnt from previous cases. Documentation for common types of incidents can speed up incident response and training of new team members. Periodically check the validity of emergency contacts, escalation contacts and abuse contacts.

Especially important are asset registers, as they allow incident responders to quickly determine which devices might be affected by an attack or a vulnerability.

During this phase, LIFARS collects all the necessary information to respond as soon as possible in case of an incident.

LIFARS
your digital world, secured
244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

B. Jump Bag Revision

The incident response jump bag needs to be always prepared for a rapid incident response. Every jump bag should contain:

- A forensic laptop with enough memory and a high-performance CPU preloaded with necessary forensic software
- Hard drives and write-blockers for drive imaging
- Screw drivers of various types, various adapters, and reductions
- A flash drive with a write-blocking function and pre-loaded live IR tools
- A safe compartment for hard drives and anti-static bags
- Multiple copies of necessary documents, like a chain of custody document
- A camera
- Copies of paper documents, like chain of custody forms, contact lists, incident report and incident handling forms
- Pen and paper
- Non-perishable snacks and drinking water

Outside of incidents, jump bag should be re-stocked and sealed after each incident so that all incident responders know it is ready.

C. Education

It is recommended that management prepares holistic educational and training plan and allocates a percentage of time in between incidents for training and education. Reserving some time for internal trainings and workshops, where the team members can exchange knowledge and experience can be beneficial for the entire team. Alternative options are commercial trainings.

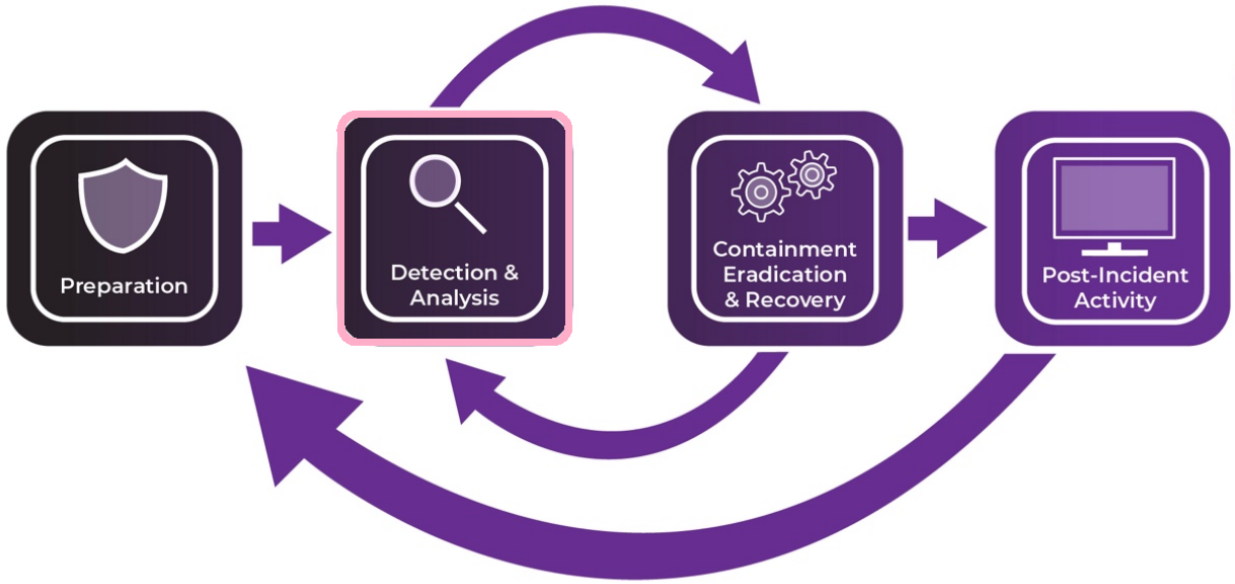
Having a simulated incident from time to time is great for testing the readiness of all hardware, software, and personnel.

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

Detection and Analysis

Security teams should proactively search for any threats inside the infrastructure as they need to make sure that no threats are currently residing inside their networks. Such process is called threat hunting. Threat hunting always starts with assuming breach, after which security analysts can look for threat artifacts. Threat intelligence plays an important part in the threat hunting process, as it can help the team to pinpoint both present and even future threats. After confirming assumption, the incident response process is initiated.

However, not all incidents are hard to detect. Some are obvious, like ransomware attacks. No matter the complexity, each incident needs to be well-documented and analyzed.



A. Threat Artifact Sources

Threats can be detected by reviewing either system or network artifacts. System sources worth monitoring for threats include:

- Endpoint Protection software
- EDR solution
- Operating system logs
- System vulnerability reports

Network sources include:

- Network-based IDS/IPS solution
- DNS logs
- Access logs
- VPN connection logs

LIFARS
your digital world, secured
244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

However, monitoring of such sources require a team with experienced security analysts, who can distinguish important entries from irrelevant, and write effective rules. Efficient tools can reduce the number of advanced personnel needed, but no software can completely replace security analysts.

LIFARS Managed Threat Hunting and Response can provide you with both next-generation detection tools and expert analysis to uncover even the most hidden threats.

B. Incident Documentation

After detection of an incident, the incident responders should start documenting the entire process that lead to the detection and archive any artifacts. Any steps taken in resolving the incident should be documented, including photos of the affected machines for incidents that would require it. Hash values of each artifact needs to be recorded and the data in a secure way to prevent any damage and tampering.

LIFARS will provide secure storage during our investigation for artifacts and will provide the documentation you need in case you decide to pursue legal action.

C. Incident Analysis

Each security incident should be verified and analyzed. Having known-good images of system and hardware firmware is strongly recommended, so that you can distinguish legitimate files and behaviors from malicious. You can submit hashes of suspicious files to various open-source tools to verify suspicious binaries. Just make sure to not upload any confidential or sensitive files. In some cases, even hashes can be confidential.

Correlate data from multiple logs, as many types of malicious activities usually leave traces in multiple logs. Try to predict possible impacts of the incident, as it will help you prioritize incidents.

LIFARS uses team of experts to analyze the traces, potential impacts and provide recommended next steps.

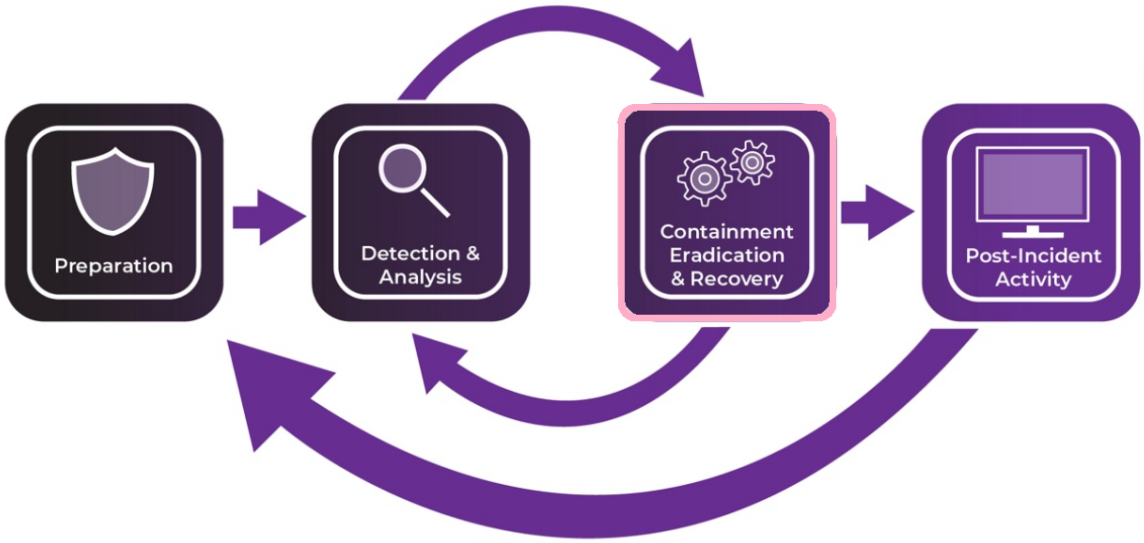
LIFARS
your digital world, secured

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

Containment, Eradication, & Recovery

After a detection, the affected systems should be contained so that we can limit the impact of breach. Removing incident components and business recovery is possible only after containment.

An important part of this phase is not only solving the problem but also removing the cause, for instance fixing the vulnerability that was abused in the attack.



A. Containment

Containment strategy should vary based on the incident and the affected systems. While some systems are expendable and their shutdown will not disrupt business continuity in a major way, some cannot be turned off nor isolated from the network.

Having backup strategies for each incident is important. Backup strategies can reduce the time needed to contain the incident, as well as reduce the down time.

Before containment of specific systems and devices can begin, the incident responders need the full list of devices that might be compromised, as well as understand the methods of exploitation and lateral movement. Otherwise, they risk playing endless game of whack-a-mole with attacker that may be returning right after cleaning the infection from one of the systems. Thus, acquiring evidence and forensic analysis of acquired data is required before choosing the right containment method.

LIFARS
your digital world, secured
244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

The acquired data can include:

- Hard drive images
- Memory images
- Firmware images
- Network logs
- Operating system logs
- Physical devices, including computers and mobile phones

It is important to remember to properly label all forensic data. If someone were to look at the evidence collected 8 months later, he or she should have clear idea of what the evidence contains. Disk images should be labeled with computer name and partitions they contain. Also, network logs should have dates and solutions they were captured on. Furthermore, physical devices should include serial numbers.

In addition to disconnecting the affected devices from the network, the alternative containment methods include blocking users or quarantining the device via security policies or a specialized software (EDR), depending on a type of the incident.

In some cases, containment might lead to the loss of forensic data. For example, malware can detect a loss in connection and subsequently delete itself along with many of its traces. In such cases, LIFARS can use deception techniques to bypass anti-forensic countermeasures.

B. Eradication

Eradication process means completely removing all components of the incident from the affected systems. Missing just one host can lead to the whole infrastructure getting compromised again. Attackers often utilize multiple methods of persistence; therefore, affected systems need to be examined carefully. Threat intelligence can help detect persistent components that might otherwise be missed. Such example is compromised firmware, as firmware examination is usually very expensive and time-consuming.

Eradication can be done either with restoration of a clean image, or via less invasive methods, which remove only the malicious components while leaving the rest of the system and its data intact. The latter can be done by an EDR solution, a cleaning script, or a specialized cleaning tool.

One of the least invasive method are LIFARS' proprietary Cyber Vaccines, which are custom scripts specifically created for each incident type. Cyber Vaccines remove malicious binaries and their persistence methods as well as apply hardening, to prevent lateral movement and re-infection.

It is very important to make sure that any binaries and persistence methods are completely removed. Otherwise there is a risk of the problem resurfacing across the entire infrastructure. In most cases, deploying a clean image is recommended.

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

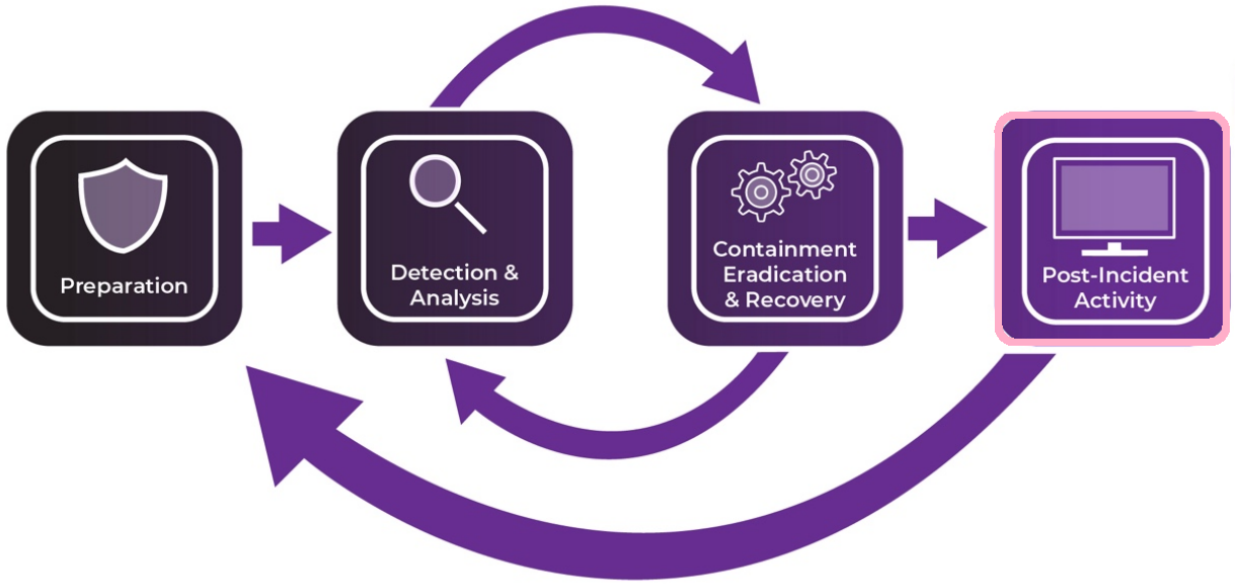
C. Recovery

In this phase, the affected systems are brought back online. The systems should put back into production only after the incident response team provides written consent that it is safe to do so. All the systems should be monitored and validated, to make sure they are working as intended and no malicious or undesirable activity is happening.

Components of the systems should be updated, and any unsupported parts of the infrastructure should be replaced to prevent future breaches. Ensure that any credentials that had been used in the attack or might had been accessed by attackers are invalidated. Cryptographically validate system and firmware to ensure their integrity.

Post-Incident Activity

Solving incident should not end the incident response process. Each incident should be analyzed to further improve security features, detection measures and response mechanism.



A. Lessons learned

After the incident, security improvements of the entire infrastructure ensue. Analyzing the TTPs (tactics, techniques, and procedures) leveraged in the incident will help apply new mitigations and remove attack vectors. If human failure played a part in the incident, prepare related workshops and trainings to prevent such failures.

If any malicious activity was missed by SIEM, try to improve data aggregation and correlation rules to log it in the future. Do not forget to forward the TTPs and the IOCs to internal threat intelligence.

The incident response should also be examined with the goal of reducing overall response time and remove unnecessary slowdowns.

B. Data retention

In case you decide to pursue legal action, the data should be stored and protected against tampering. The period for which the data should be kept is subject to internal policies and local regulations.

LIFARS
your digital world, secured
244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

LIFARS' Incident Response Retainer

With LIFARS on retainer a cybersecurity incident or a data breach will be handled with high priority under strict SLAs. Have your own Computer Security Incident Response Team (CSIRT) on call and ready for deployment as your private 911 cyber-emergency.

Repurpose unused hours for some of LIFARS's proactive or advisory services and strengthen your security posture to make the most of your investment.

What is an IR Retainer?

During a cybersecurity incident, time is of the essence. Contracting LIFARS on retainer reduces the delay between notification and first actions, and ultimately will decrease the overall cost of the incident: not only all the paperwork is preapproved, enabling for a very quick start, but also LIFARS CSIRT (LISIRT) will have the technical information related to your environment. There are four tiers of IR Retainers available that vary in response times, complexity, cost and flexibility. They range from best effort incident response with minimal initial costs and no additional services all the way to comprehensive in-depth relationship and integration of LIFARS to your structures. LISIRT then acts like your own

CSIRT performing a wide range of proactive and reactive services and ensuring continual improvement of your security posture. There is also an option to design a custom tier of IR Retainer to meet your specific needs. You can repurpose unused hours to make use of some of our proactive services such as penetration testing, implementation of a technical vulnerability program, or a threat hunt.

LISIRT

LIFARS Computer Security Incident Response Team

To learn more about our IR Retainer, contact one of our Cyber Resiliency Experts today!

LIFARS
your digital world, **secured**

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com

Ending Notes

The right incident response team, with the right tools and the right preparation can mean the difference between minor, localized outage, and global, long-lasting downtime.

It is important to have all the policies, methodologies, and procedures well-prepared, so you can reduce the unnecessary downtime.

References

NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide

ISO/IEC 27035:2011 Information security incident management

LIFARS' Incident Response Retainer

LIFARS
your digital world, secured

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 contact@lifars.com