# Top 7 Open Source Incident Response Tools

cynet.com/blog/the-7-best-free-and-open-source-incident-response-tools

## The 7 Best Free and Open-Source Incident Response Tools

### What Is Incident Response?

Being prepared is key to responding to security incidents in an accurate and level-headed manner. When disaster hits, there's an ocean of difference between responding to incidents using calculated clear steps and plunging head first into reactive mode. But just what does "being prepared" entail?

As we discussed in the effort to respond effectively to incidents, you'll need to devise a repeatable, standardized, and documented incident response (IR) plan ahead of time. This plan should include the following six steps:

- **Preparation:** See where you may be vulnerable. Use this information to create your IR policies and then determine who will be on your cyber incident response team.
- **Implementation:** Make sure you have IR tools that grant visibility into assets and activities and make it easy to identify false positives.
- **Assessment and Triage:** Determine what happened and how it occurred.
- **Containment:** Contain the incident and shut down the affected systems to prevent further damage.
- **Recovery:** Return to normal operations. Restore systems back into their environment, replace contaminated files with clean ones, and deploy missing patches.
- **Post-Incident Activity:** Update and harden your system, fix flaws, boost employee awareness, and invest in better tools in order to prevent future attacks.

In this post, we'll investigate some of the many tools incident response teams have at their disposal to ensure that incidents are resolved optimally—with as little damage as possible. We'll also explore the move to SOAR technologies that incorporate IR tools to help analysts respond to incidents faster and more effectively than ever before.

### The 7 Best Open-Source Incident Response Tools

When it comes to incident response tools, you've got a lot of choices—both paid and open source. But when you're creating your IR plan or dealing with an incident, it's not the ideal time to stop what you're doing and decide which paid tool to go with. We recommend using open-source tools in such scenarios. They are free—and some are

actually quite robust, with the ability to complement your existing toolset. They also allow you to get started quickly, without spending months deciding which tool to use. Then, perhaps at a later stage, you can consider moving to paid tools.

Here we'll explore the seven best  IR tools currently available:

## 1. Cynet 360

Cynet is an IR platform – free to use for incident responders. It  provides incident responders with a complete set of remediation actions to address infected hosts, malicious files, attacker-controlled network traffic, and compromised user accounts. With Cynet 360, IR teams can get complete visibility of their environment in less than one hour—and it only takes one click to remediate attacks. The central management allows you to distribute other open-source incident response across the environment, and you can build your own remediation policies for automated threat blocking and removal. You can also see the attack scope and all indicators immediately, which vastly reduces investigation time. **Cynet also has a 24/7 Incident Response team to assist organizations that have been attacked**. Contact them here

## 2. GRR Rapid Response

Google's GRR Rapid Response framework allows analysts to conduct remote live forensics. It also helps IR teams respond in a swift and scalable manner for faster triage and remote analysis. It's comprised of two parts: the GRR client, which is deployed on the system to be investigated, and the GRR server, which helps analysts implement actions and process the data they have collected.

## 3. AlienVault

AlienVault OSSIM (Open Source Security Information and Event Management) is an SIEM tool that helps analysts get a comprehensive view of their system. It does this by providing log and asset management, with information from other security tools to gain context.

## 4. Cyphon

Cyphon provides analysts with tools to collect, process, and triage incidents. It collects data from sources such as message logs, APIs, and email—and makes it simple to analyze while allowing you to collect as much or little data as you need.

## 5. Volatility

This popular memory forensics framework allows analysts to investigate and extract intelligence from volatile memory dumps. Volatility provides data on network connections, processes that are running, process IDs, and more—and exports that data to a text file.

## 6. Sans Investigative Forensics Toolkit (SIFT) Workstation

SIFT Workstation is an Ubuntu-based toolkit that comes with everything analysts need to execute in-depth digital forensic investigations. It can also be downloaded as a VMware appliance.

## 7. TheHive Project

TheHive Project is a free open-source IR platform that allows multiple analysts to work simultaneously on incident investigations. It gives analysts the ability to set up notifications for new task assignments and to preview new events and alerts with multiple sources, such as email digests and SIEM alerts. Built-in templates allow analysts to gain key insights and identify the right measures to take for faster remediation.

## The Shift to SOAR Platforms

The above tools are definitely beneficial and should be a part of any organization's IR plan. But in today's increasingly complex cyber landscape, organizations need to automate as many tasks as possible to keep their heads above water. This need has led to an emerging group of tools, called a SOAR platform, that combine incident response, automation, and threat intelligence. Automating and orchestrating routine incident response tasks allows analysts to spend more time investigating incidents that call for greater insight.

The term SOAR Platform, coined by Gartner in 2017, stands for Security Orchestration Automation and Response. SOAR platforms allow organizations to collect and combine large amounts of data from many sources.

SOAR capabilities include:

- **Orchestration:** The ability to connect to and integrate various tools.
- **Automation:** The ability to collect data automatically and enrich events.
- **Response:** The ability to allow analysts to manage, collaborate, and share data regarding incidents for better outcomes.

Using a SOAR platform vastly cuts down on incident response time. Considering the worldwide shortage of qualified security analysts, this is exactly what is needed to keep up with increasing challenges. Security experts agree that by the end of 2020, 15% of all organizations with security teams of over five members will be using a SOAR platform. This move will provide users with better detection and faster response to attacks.