**Name of Organization**

**Incident Response Toolkit**

December 2021

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

The (Name of Organization) Incident Response Toolkit is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute the handbook to individuals with a need to know. Distribution by other individuals without prior authorization is prohibited. The document is unclassified but contains sensitive information.

**Table of Contents**

[I. Introduction and Purpose 5](#_Toc88583313)

[II. Requirements and Tools 5](#_Toc88583314)

# Introduction and Purpose

Disasters and emergencies can happen suddenly, which can affect normal staffing levels, causing (Name of Organization) public safety departments to become overwhelmed. The (Name of Organization) Office of Emergency Management (OEM) has established this Incident Response tool kit, which provides a guideline for the management and incident responders to Cyber Security.

The overall objective is to respond to cyber security incidents with the correct tools to respond, investigate and manage the process of restoring the (Name of Organization) back to pre-disaster conditions and be able to collect evidence for forensic investigation – internally and provide to legal authorities if needed.

Several options exist for addressing the requirements and needs represented by Incident Response efforts. Included herein is a cursory listing of readily-available Open-Source solutions that, when properly configured and utilized, aid in the performance of tasks associated with Incident Response. This list is not exhaustive and consideration should be paid to the differences between open source and proprietary software. Solutions should be selected carefully based on a number of factors, including total cost of ownership, availability of support, and required feature content.

*Note for Industrial Equipment:*

This toolkit also addresses Industrial equipment which is often substantially older than Enterprise hardware and software. There are also typically strict restrictions on the installation of software or hardware on vendor-supported systems performing critical functions. This means that modern security, forensic, and collection hardware and software will frequently not work on impacted systems. Responders should be prepared with cables, adapters, storage media, and tools appropriate to deal with the era of systems they may encounter in the facility. When in doubt, plan to collect and analyze systems up to 20 years old, with very limited hardware resources.

# Requirements and Tools

Essentials for Cyber Incident Response Toolkits

Here are some essential pieces of equipment that we highly recommend every cyber incident responder have on hand:

* Facility safety documentation / card
* Camera
* Notetaking materials
* Electronics screwdriver set
* Antistatic protection
* Universal control cabinet key set
* Analysis laptop (with authorized, preinstalled, and tested forensic tools and playbooks per Incident Response Plan)
* USB A / C adapters and extension cable
* Ethernet dongle (if the laptop is not equipped with an ethernet port)
* Serial dongle or adapter cable (if the laptop is not equipped with a serial port)
* DVD-R Drive
* DVD-Rs
* Ethernet cable
* Ethernet crossover dongle or cable
* Clean removable hard drives (1 TB+ recommended, hardware-encrypted recommended)
* Write blocker (supporting SATA and IDE laptop and desktop hard drives at a minimum)
* Digital evidence bags and tags
* Chain of custody forms as specified by Incident Response Plan
* Flashlight
* Multitool
* Hard hat\*
* Safety goggles or glasses\*
* Composite toe safety shoes\*
* Hearing protection\*
* Fire-resistant clothing (including undergarments and outerwear) \*

\*If applicable. All Personal Protective Equipment (PPE) should be properly fitted and appropriately rated and certified for the facility and meet local government regulations.

| **Incident Response Tool** | **Why You Need It** | **Open-Source Options** | | | | | |  | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Log Analysis, Log Management, SIEM | Logs are your richest source for understanding what’s going on in your network, but you’ll need an IR tool that makes sense of all of those logs, and that’s what log analysis is all about. | [• OSSIM (open source security information management)](https://cybersecurity.att.com/products/ossim) | | | | | |  | | | |
|  | | | |
|  | | | |
|  | | | |
| Intrusion Detection Systems (IDS) — Network & Host-based | IDS systems (HIDS and NIDS) monitor server and network activity in real-time, and typically use attack signatures or baselines to identify and issue an alert when known attacks or suspicious activities occur on a server (HIDS) or on a network (NIDS). | [• Snort](https://snort.org/) | | | | | |  | | | |
| [• Suricata](https://suricata.io/download/) | | | | | |  | | | |
| [• BroIDS](https://zeek.org/) | | | | | |  | | | |
| [• OSSEC](https://www.ossec.net/) | | | | | |  | | | |
|  | | | | | |  | | | |
| Netflow Analyzers | Netflow analyzers examine actual traffic within a network (and across the border gateways too). If you are tracking a particular thread of activity, or just getting a proper idea of what protocols are in use on your network, and which assets are communicating amongst themselves, netflow is an excellent approach. | [• Ntop](https://www.ntop.org/) | | | | | |  | | | |
| [• NfSen](http://nfsen.sourceforge.net/) | | | | | |  | | | |
| [• Nfdump](http://nfdump.sourceforge.net/) | | | | | |  | | | |
|  | | | | | |  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
| Vulnerability Scanners | Vulnerability scanners identify potential areas of risk, and help to assess the overall attack surface area of an organization, so that remediation tasks can be implemented. | [• OpenVAS](https://www.openvas.org/) | | | | | |  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
| Availability Monitoring | The whole point of incident response is to avoid downtime as much as possible, so make sure that you have availability monitoring in place, because an application or service outage could be the first sign of an incident in progress. | [• Nagios](https://www.nagios.org/) | | | | | |  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
| Web Proxies | Web Proxies are thought of as being purely for controlling access to websites, but their ability to log what is being connected to is vital. So many modern threats operate over HTTP – being able to log not only the remote IP address, but the nature of the HTTP connection itself can be vital for forensics and threat tracking | [• Squid Proxy](http://www.squid-cache.org/) | | | | | |  | | | |
| [• IPFire](https://www.ipfire.org/features) | | | | | |  | | | |
|  | | | | | |  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
| Asset Inventory | In order to know which events to prioritize, you’ll need an understanding of the list of critical systems in your network, and what software is installed on them. Essentially, you need to understand your existing environment to evaluate incident criticality as part of the Orient/Triage process. The best way to do this is to have an automated asset discovery and inventory that you can update when things change (and as we know, that’s inevitable). | | | [• OCS Inventory](https://ocsinventory-ng.org/?lang=en) | | |  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
| Threat Intelligence Security Research | Threat intelligence gives you global information about threats in the real world. Things like indicators of compromise (IoCs), bad reputation IP addresses, command-and-control servers and more, can be applied against your own network assets, to provide a full context for the threat. | | [• AlienVault OTX](https://cybersecurity.att.com/open-threat-exchange) | |  | | | |
| [• AlienVault Labs](https://cybersecurity.att.com/blogs/labs-research) | |  | | | |
|  | |  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
| Data Capture & Incident Response Forensics Tools | Data Capture & Incident Response Forensics tools is a broad category that covers all types of media (e.g., memory forensics, database forensics, network forensics, etc.). Incident Response Forensics tools examine digital media with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information, all designed to create a legal audit trail. | [• SANS Investigative Forensics Toolkit (SIFT)](https://www.sans.org/tools/sift-workstation/) | | | |  | | | |
| [• Sleuthkit](http://www.sleuthkit.org/) | | | |  | | | |
|  | | | |  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
| Data Capture & Incident Response Forensics Tools | Data Capture & Incident Response Forensics tools is a broad category that covers all types of media (e.g., memory forensics, database forensics, network forensics, etc.). Incident Response Forensics tools examine digital media with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information, all designed to create a legal audit trail. | [• SANS Investigative Forensics Toolkit (SIFT)](https://www.sans.org/tools/sift-workstation/) | | |  | | | |
| [• Sleuthkit](http://www.sleuthkit.org/) | | |  | | | |
|  | | |  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
| System Backup & Recovery Tools Patch Mgmt. and Other Systems Mgmt | System backup and recovery and patch management tools might be something you’ve already got in place, but it’s important to include them here since an incident is when you’ll likely need them most. | [• Opsi (Open PC Server Integration)](https://www.opsi.org/) | | |  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
|  | | | |
| Security Awareness Training Tools and Programs | Security awareness training tools and programs are an essential way to improve your overall security posture and reduce the likelihood of incidents | [• SANS’ Securing the Human](https://www.sans.org/blog/building-an-information-security-program-post-breach-part-iii/) | | |  | | | |
|  | | | |
|  | | | |
|  | | | |
|  |  | | | |

Specific Evidence

Disk Image Creation Tools

* [**AccessData FTK Imager**](http://accessdata.com/product-download/?/support/adownloads#FTKImager) **-** Forensics tool whose main purpose is to preview recoverable data from a disk of any kind. FTK Imager can also acquire live memory and paging file on 32bit and 64bit systems.
* [**Bitscout**](https://github.com/vitaly-kamluk/bitscout) **-** Bitscout helps you build your fully-trusted customizable LiveCD/LiveUSB image to be used for remote digital forensics.
* [**GetData Forensic Imager**](http://www.forensicimager.com/) - Windows based program that will acquire, convert, or verify a forensic image in one of the following common forensic file formats.
* [**Guymager**](http://guymager.sourceforge.net) **-** Free forensic imager for media acquisition on Linux.
* [**Magnet ACQUIRE**](https://www.magnetforensics.com/magnet-acquire/) - allows various types of disk acquisitions to be performed on Windows, Linux, and OS X as well as mobile operating systems.

Evidence Collection

* [**bulk\_extractor**](https://github.com/simsong/bulk_extractor) - scans a disk image, a file, or a directory of files and extracts useful information without parsing the file system or file system structures. Because of ignoring the file system structure, the program distinguishes itself in terms of speed and thoroughness.
* [**Cold Disk Quick Response**](https://github.com/rough007/CDQR) - Streamlined list of parsers to quickly analyze a forensic image file (dd, E01, .vmdk, etc.) and output nine reports.
* [**CyLR**](https://github.com/orlikoski/CyLR) **-** The CyLR tool collects forensic artifacts from hosts with NTFS file systems quickly, securely and minimizes impact to the host.
* [**artifactcollector**](https://github.com/forensicanalysis/artifactcollector) **-** The artifact collector project provides a software that collects forensic artifacts on systems.
* [**ir-rescue**](https://github.com/diogo-fernan/ir-rescue) **-** Windows Batch script and a Unix Bash script to comprehensively collect host forensic data during incident response.
* [**Live Response Collection**](https://www.brimorlabs.com/tools/) **-** Automated tool that collects volatile data from Windows, OSX, and \*nix based operating systems.
* [**Margarita Shotgun**](https://github.com/ThreatResponse/margaritashotgun) **-** Command line utility (that works with or without Amazon EC2 instances) to parallelize remote memory acquisition.
* [**UAC**](https://github.com/tclahr/uac) **-** UAC (Unix-like Artifacts Collector) is a Live Response collection tool for Incident Repone that makes use of built-in tools to automate the collection of Unix-like systems artifacts. Supported systems: AIX, FreeBSD, Linux, macOS, NetBSD, Netscaler, OpenBSD and Solaris.

Threat Collection/Intelligence

* [**Mandiant Threat Intelligence**](https://www.mandiant.com/advantage/threat-intelligence?utm_source=google&utm_medium=cpc&utm_content=paid-search&gclid=CjwKCAjwwsmLBhACEiwANq-tXD-SUf-Dw9Rkb9hRH5TSDIGBQRMZNLKMBV1GubmFLVhEqFTZj0X2XhoCNY0QAvD_BwE&gclsrc=aw.ds) **-** Mandiant Threat Intelligence module provides organizations of all sizes visibility into the latest threats directly from the frontlines.
* [**Automated Indicator Sharing**](https://www.dhs.gov/cisa/automated-indicator-sharing-ais) **-** Private companies are able to report cyber threat indicators with the DHS, which are then distributed via the Automated Indicator Sharing website. This database helps reduce the effectiveness of simple attacks by exposing malicious IP addresses, email senders, and more.
* **I**[**nfraGard Portal**](https://www.infragard.org/) **-** The FBI’s InfraGard Portal provides information relevant to 16 sectors of critical infrastructure. Private and public sector organizations can share information and security events, and the FBI also provides information on cyber attacks and threats that they are tracking.
* **@abuse.ch:** [Ransomware Tracker](https://ransomwaretracker.abuse.ch/) collects data related to ransomware attacks so that security teams can check IP addresses and URLs against those that are known to be involved in attacks. The tracker provides detailed information on the servers, sites, and infrastructure that have been exploited by ransomware actors, as well as recommendations for preventing attacks.
* **SANS** [Internet Storm Center](https://isc.sans.edu/) - It uses a distributed sensor network that takes in over 20 million intrusion detection log entries per day to generate alerts regarding security threats. The site also provides analysis, tools, and forums for security professionals.
* [**VirusTotal**](https://www.virustotal.com/gui/home) **-** uses dozens of antivirus scanners, blacklisting services, and other tools to analyze and extract data from files and URLs submitted by users. The service can be used to quickly check incidents like suspected phishing emails, and every submission is retained in its database to build a global picture of cyber threats.
* **Cisco** [**Talos Intelligence**](https://www.talosintelligence.com/) **-** unmatched tools and experience provide information about known threats, new vulnerabilities, and emerging dangers. Talos also provides research and analysis tools.
* [**VirusShare Malware Repository**](https://virusshare.com/) **-** an online repository of malware created and maintained by J-Michael Roberts, a digital forensics examiner. The site gives researchers, incident responders, and forensic investigators access millions of malware samples.
* **Google** [**Safe Browsing**](https://safebrowsing.google.com/) **-** identifies dangerous websites and shares the information to raise awareness of security risks. Safe Browsing finds thousands of unsafe sites every day, many of which are legitimate sites that have been compromised by hackers.