

# INTRODUCTION TO DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR)

Omar Santos

 Follow @santosomar



**OMAR SANTOS**

## About Me:

- Principal Engineer at Cisco's Product Security Incident Response Team (PSIRT) - Security Research and Operations.
- Over 20 years of experience in cybersecurity.
- Author of over 20 books and video courses.



Follow @santosomar

# AGENDA

- Introduction to the Incident Response Process
- Building an Incident Response Team
- The Incident Response Plan
- Incident Response Playbooks
- Digital Forensics Fundamentals
- Network and Host-based Evidence Collection and Handling

## POLL 1

What is your level of familiarity with Digital Forensics and Incident Response?

1. Beginner (less than 1 year of experience).
2. Intermediate (2-3 years of experience)
3. Expert (considerable DFIR experience).

## POLL 2

Why are you interested in this course?

1. Just curious and want to learn more about DFIR.
2. I am preparing for a cybersecurity certification.
3. My job is DFIR.

# DFIR Certifications





## Interactive NICE Framework Mapping

SANS and GIAC Certifications has partnered with the National Security Workforce to place over 35 cyber security courses and corresponding GIAC certifications within an easy to read framework (commonly known as the NICE Framework.) The interactive framework below will help you identify the SANS courses and certifications you need to advance your career as a Federal Employee.

Many of the courses and certifications found on the NICE Framework are DoDD 8140 (DoDD 8570) compliant. Visit the [DoDD 8140](#) resource page for the full list of associated GIAC Certifications.

[How to use the NICE Framework Mapping](#)

[Download the Full NICE Mapping PDF](#)

Hover over the area of interest on the NICE Framework to get started.



<https://www.giac.org/certifications/niceframework>

[REGISTER FOR EXAM](#)[SIGN IN](#)[ABOUT](#) [CERTIFICATIONS](#) [EDUCATION & TRAINING](#) [MEMBERS](#) [NEWS & EVENTS](#) [ADVOCACY](#) [COMMUNITY](#)

The CCFP will be designated an inactive credential August 21, 2020. The credential will remain a recognized (ISC)<sup>2</sup> certification until that date.



## Certified Cyber Forensics Professional

The CCFP certification indicates expertise in forensics techniques and procedures, standards of practice, and legal and ethical principles to assure accurate, complete, and reliable digital evidence admissible in a court of law. It also indicates the ability to apply forensics to other information security disciplines, such as e-discovery, malware analysis, or incident response.

CCFP addresses more experienced cyber forensics professionals who already have the proficiency and perspective to effectively apply their cyber forensics expertise to a variety of challenges. In fact, many new CCFP professionals likely hold one or more other digital forensics certifications.

Given the varied applications of cyber forensics, CCFP professionals can come from an array of corporate, legal, law enforcement, and government occupations, including:

- Digital forensic examiners in law enforcement to support criminal investigations
- Cybercrime and cybersecurity professionals working in the public or private sectors
- Computer forensic engineers & managers working in corporate information security
- Digital forensic and e-discovery consultants focused on litigation support
- Cyber intelligence analysts working for defense/intelligence agencies
- Computer forensic consultants working for management or specialty consulting firms.



Start Your Journey to Membership Today  
Pick the Certification that's Right for You [>](#)

**EC-Council**



<https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi>

By browsing this site, you are agreeing to our cookie policy. [More Information](#)

X

# CERTIFICATIONS

## Sharpen Your Competitive Edge

Our certification programs are led by the industry pioneers that help advance the careers of over 60,000 expert forensic investigators who consider EnCase technology as the gold standard in the industry.

### Choose Your Certification Path:

CFSR™  
CertificationEnCE®  
CertificationEnCEP®  
Certification

### CFSR™ Certification Program

Cyber security professionals who want to advance their careers are making it a top priority to get certified with cutting-edge techniques in real-world, digital forensic applications. The Certified Forensic Security Responder(CFSR™) will equip you with the breadth and depth of knowledge that you need to become a highly sought-after cyber security forensics expert.

**Prerequisites:**

Host Intrusion Methodology and Investigation + Incident Investigation Classroom / vClass or 12 Months of Qualified Work Experience

[Get Started »](#)[Apply »](#)[Renew »](#)

### EnCE® Certification Program

The EnCase® Certified Examiner(EnCE®) program certifies both public and private

NEED HELP?

X

# Introduction to the Incident Response Process



## ISO

Section 16 of ISO 27002:2013: Information Security Incident Management focuses on ensuring a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

## NIST

Corresponding NIST guidance is provided in the following documents:

- SP 800-61 Revision 2: “Computer Security Incident Handling Guide”
- SP 800-83 Revision 1: “Guide to Malware Incident Prevention and Handling”
- SP 800-86: “Guide to Integrating Forensic Techniques into Incident Response”

# INTRODUCTION TO INCIDENT RESPONSE

Computer security incident response is a critical component of information technology (IT) programs.

The incident response process and incident handling activities can be very complex.

One of the best resources available is NIST Special Publication 800-61:



Special Publication 800-61  
Revision 2

## **Computer Security Incident Handling Guide**

---

**Recommendations of the National Institute  
of Standards and Technology**

---

Paul Cichonski  
Tom Millar  
Tim Grance  
Karen Scarfone

# What is an Event?

## Definition from NIST Special Publication 800-61

“An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.”

Additional Reading: <http://h4cker.org/dfir/irt1.html>

# What is an Incident?

Definition from NIST Special Publication 800-61

“A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.”

Additional Reading: <http://h4cker.org/dfir/irt1.html>

# Examples of Incidents

Incident 1

Attacker compromises point-of-sale system and steals credit card information.

Incident 2

Attacker sends crafted packet to router and causes a crash and denial-of-service condition.

Incident 3

Ransomware is installed in critical server and all files are encrypted by the attacker.

Incident 4

User clicks on link sent in a phishing email and malware is installed on his machine.

# Other Boring Definitions

For your reference only...

False positive is a broad term that describes a situation in which a security device triggers an alarm but there is no malicious activity or an actual attack taking place.

In other words, false positives are “false alarms,” and they are also called “benign triggers.”

False positives are problematic because by triggering unjustified alerts, they diminish the value and urgency of real alerts. If you have too many false positives to investigate, it becomes an operational nightmare, and you most definitely will overlook real security events.

False negatives: the term used to describe a network intrusion device's inability to detect true security events under certain circumstances[md]in other words, a malicious activity that is not detected by the security device.

Additional Reading: <http://h4cker.org/dfir/irt2.html>

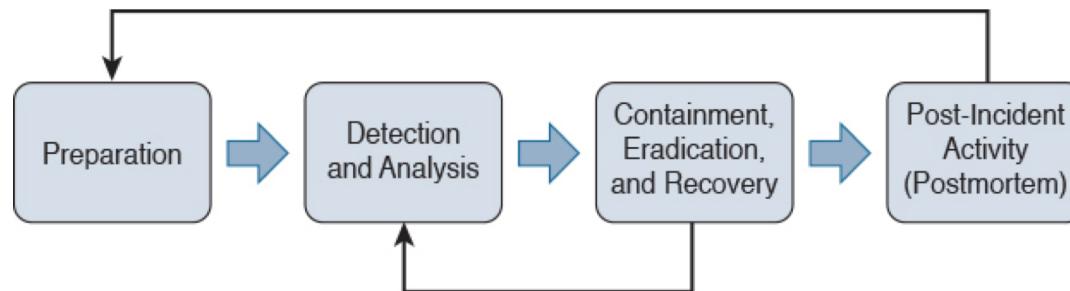
True positive: a successful identification of a security attack or a malicious event.

Additional Reading: <http://h4cker.org/dfir/irt2.html>

True negative: when the intrusion detection device identifies an activity as acceptable behavior and the activity is actually acceptable.

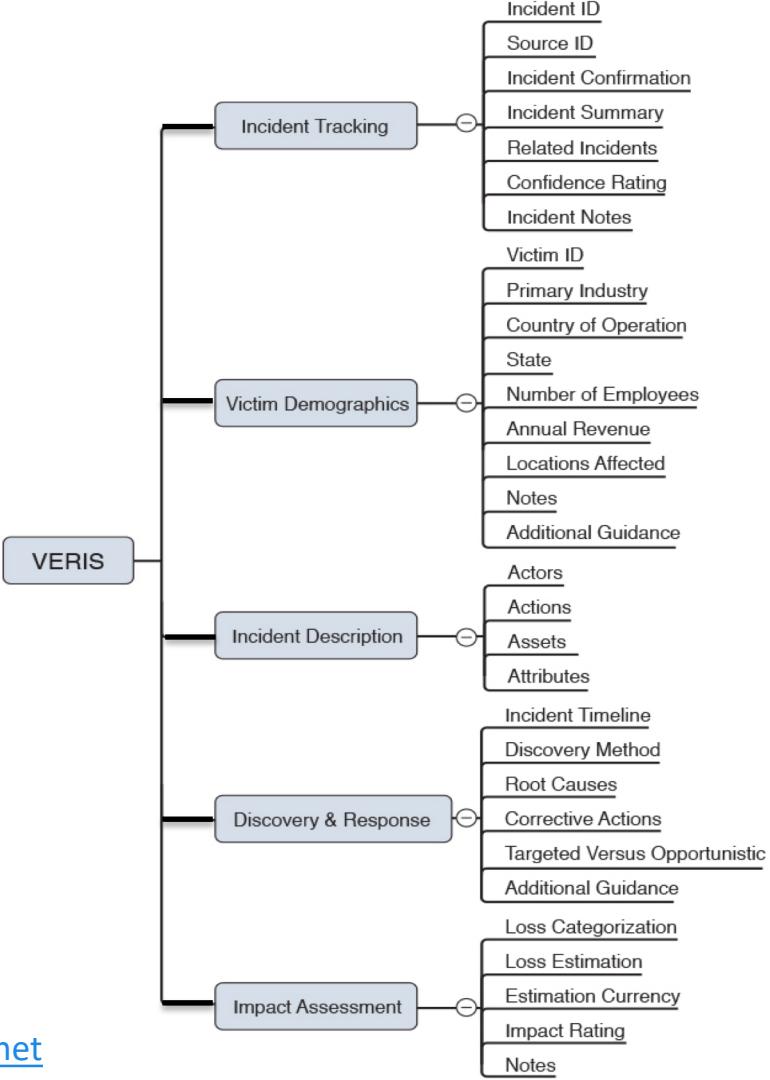
# The Incident Response Process

(reference NIST 800-61r2)



# The Vocabulary for Event Recording and Incident Sharing (VERIS)

<http://veriscommunity.net>



vz-risk/VCDB: VERIS Community Database

This repository

Pull requests Issues Marketplace Explore

vz-risk / VCDB

Code Issues 5,000+ Pull requests 3 Projects 0 Wiki Insights

VERIS Community Database

429 commits 4 branches 4 releases 10 contributors

Branch: master New pull request Create new file Upload files Find file Clone or download

Gabriel Bassett updated data to match updated json Latest commit e4e8844 on Mar 15

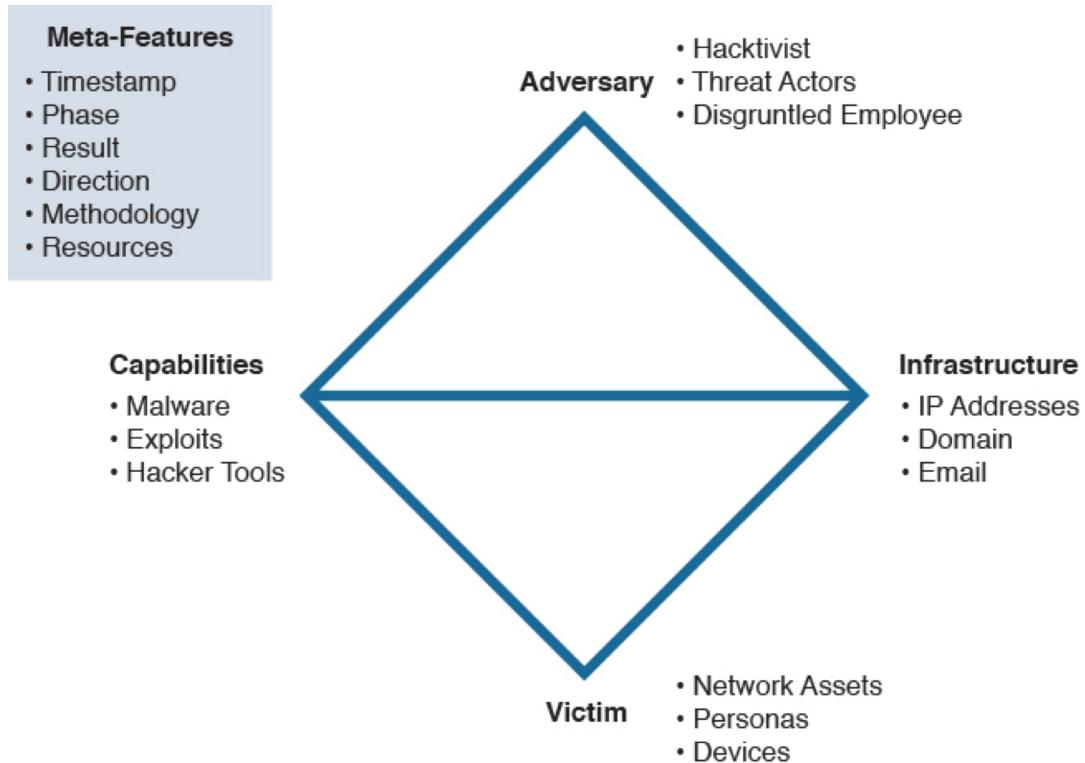
bin	updated the data files to contain all the nit-picky stuff I just fixed	4 months ago
data	updated data to match updated json	2 months ago
figure	Minor updates to readme	4 months ago
tools	Small changes	2 years ago
.gitignore	changed character in front of webskimmer breach directory. Added scrip...	7 months ago
LICENSE.txt	adds license file.	4 years ago
README.Rmd	updated Readme, removing ref to code.	4 years ago
README.md	Minor updates to readme	4 months ago
campaigns.md	Update campaigns.md	3 years ago
vcdb-enum.json	added 'unk' to event_chain object values	3 months ago
vcdb-keynames-real.txt	minor fixes to version 1.3.2	6 months ago
vcdb-labels.json	added 'unk' to event_chain object values	3 months ago
vcdb-merged.json	added 'unk' to event_chain object values	3 months ago
vcdb.json	updated schema to allow duplicates in event_chain	3 months ago
vcdb_diff-labels.json	added 'unk' to event_chain object values	3 months ago
vcdb_diff.json	updated schema to allow duplicates in event_chain	3 months ago

README.md

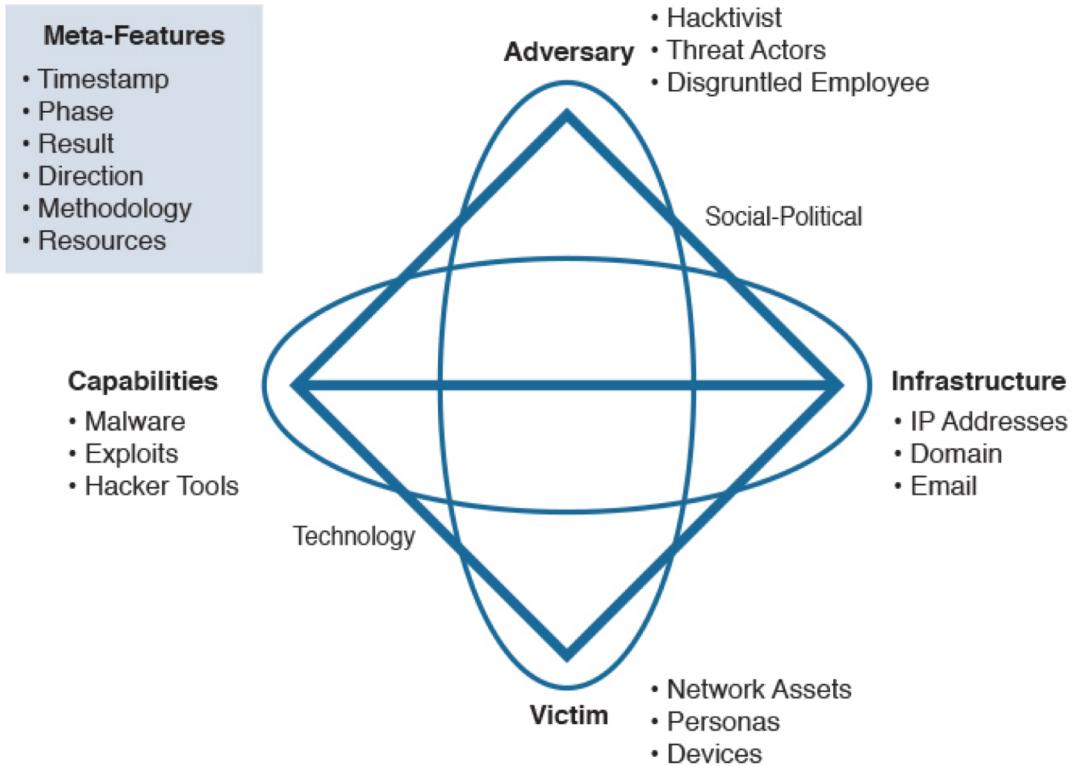
## The VERIS Community Database

Information sharing is a complex and challenging undertaking. If done correctly, everyone involved benefits from the collective intelligence. If done poorly, it may mislead participants or create a learning opportunity for our adversaries. The Verizon RISK Team supports and participates in a variety of information sharing initiatives and research efforts. We continue to drive the publication of the Verizon Data Breach Investigations Report (DBIR) annually, where we have an

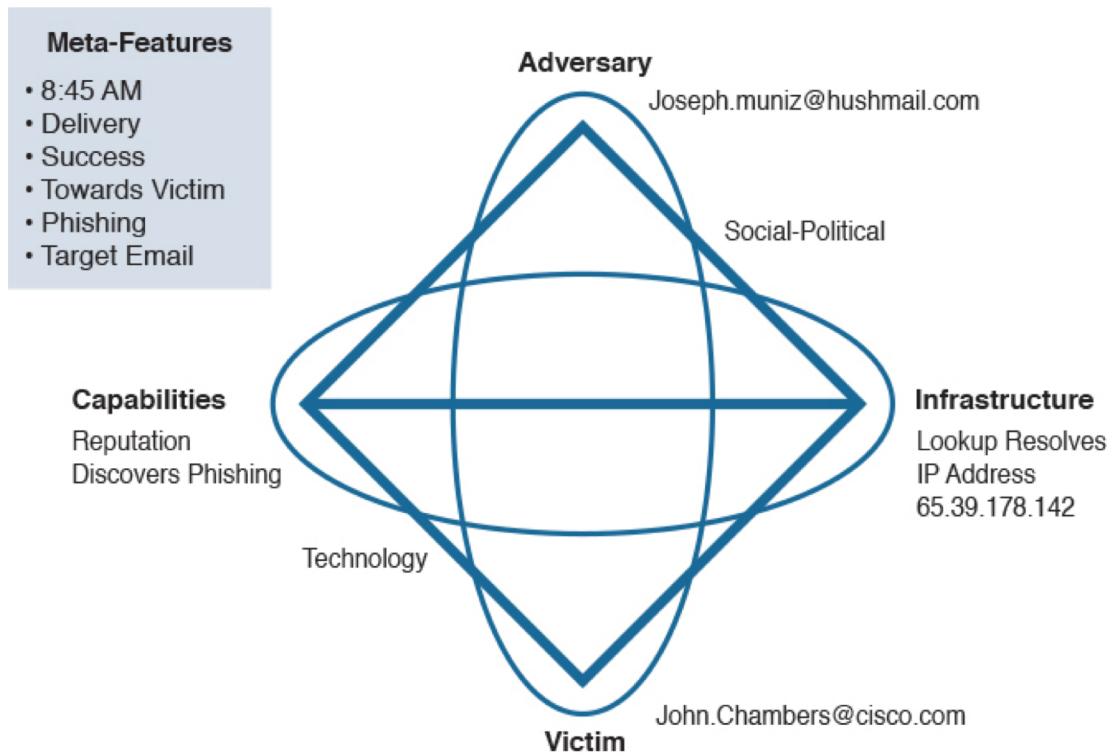
# The Diamond Model of Intrusion



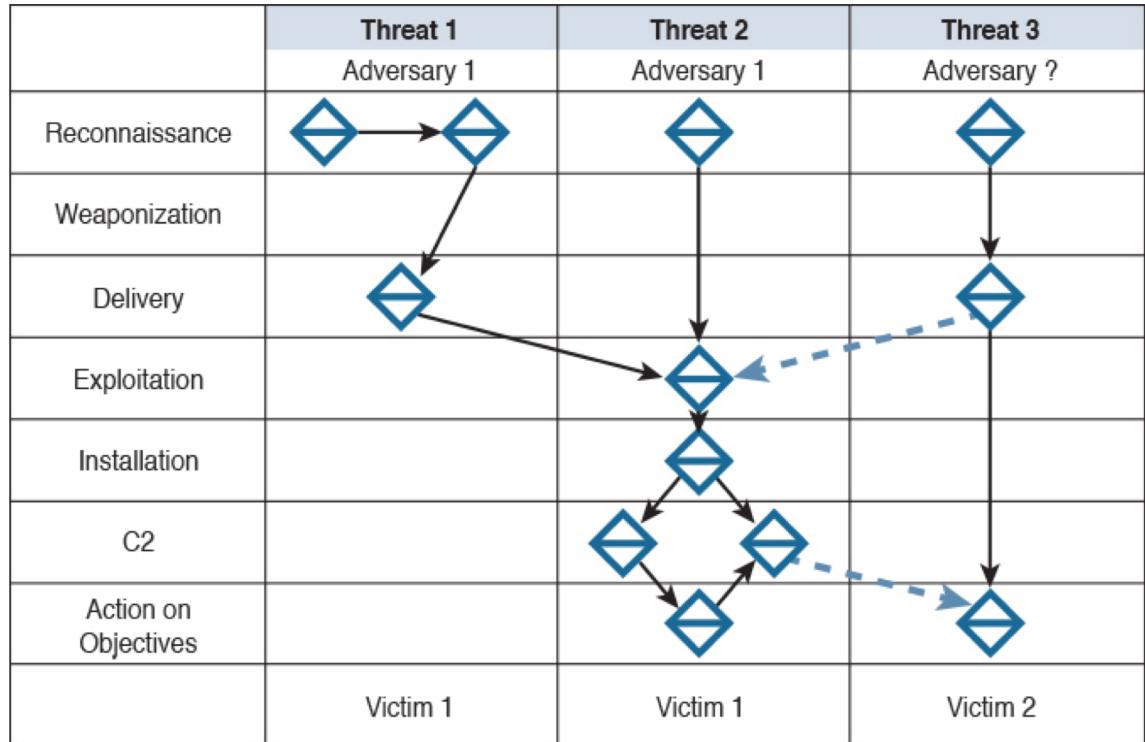
# The Diamond Model of Intrusion



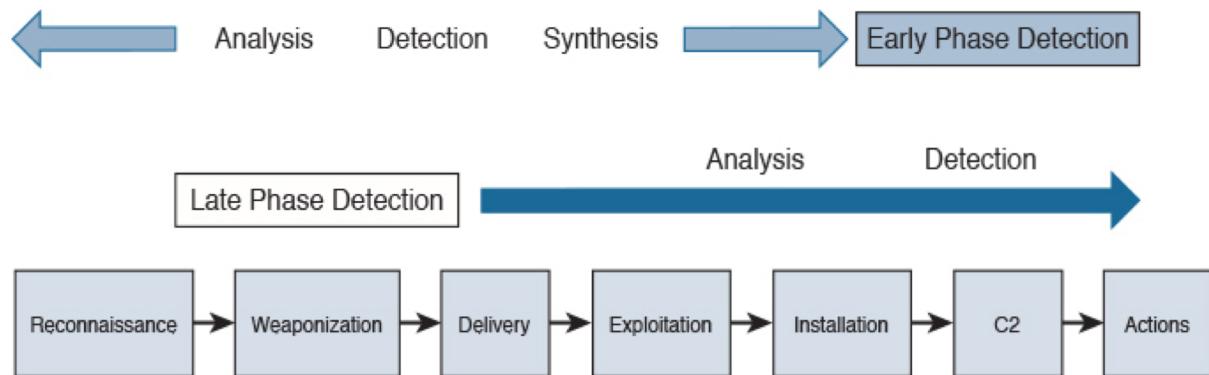
# The Diamond Model of Intrusion



# The Diamond Model of Intrusion



# Early and Late Detection in the Kill Chain Example



# Incident Response Teams

- Computer Security Incident Response Team (CSIRT)
- Product Security Incident Response Team (PSIRT)
- National CSIRTS and Computer Emergency Response Teams (CERTs)
- Coordination center
- Incident response teams of security vendors and managed security service providers (MSSP)

# FIRST

The screenshot shows the official website for FIRST (Forum of Incident Response and Security Teams). The header features the FIRST logo with the tagline "Improving Security Together". A navigation bar at the top includes links for About FIRST, Membership, Initiatives, Standards & Publications, Events, Education, and Blog. The main content area has two columns. The left column, titled "About FIRST", contains a sidebar with links to Mission Statement, History, Organization, FIRST Policies, Partners & Affiliates, Newsroom, Procurement, and Contact. Below this is a section titled "Members around the world" featuring a map of the world where countries are shaded green to indicate FIRST member presence. A link "View the distribution of FIRST Teams around the world, per country." is provided. The right column, also titled "About FIRST", contains text describing the organization's history, its role in responding to the 1989 Internet worm, and its mission to handle thousands of security vulnerabilities. It also highlights the variety of teams it brings together from government, commercial, and academic sectors.

**About FIRST**

- Mission Statement
- History
- Organization
- FIRST Policies
- Partners & Affiliates
- Newsroom
- Procurement
- Contact

**Members around the world**



View the distribution of FIRST Teams around the world, per country.

**About FIRST**

FIRST is the Forum of Incident Response and Security Teams. The idea of FIRST goes back until 1989, only one year after the CERT(r) Coordination Center was created after the infamous Internet worm. Back then incidents already were impacting not only one closed user group or organization, but any number of networks interconnected by the Internet.

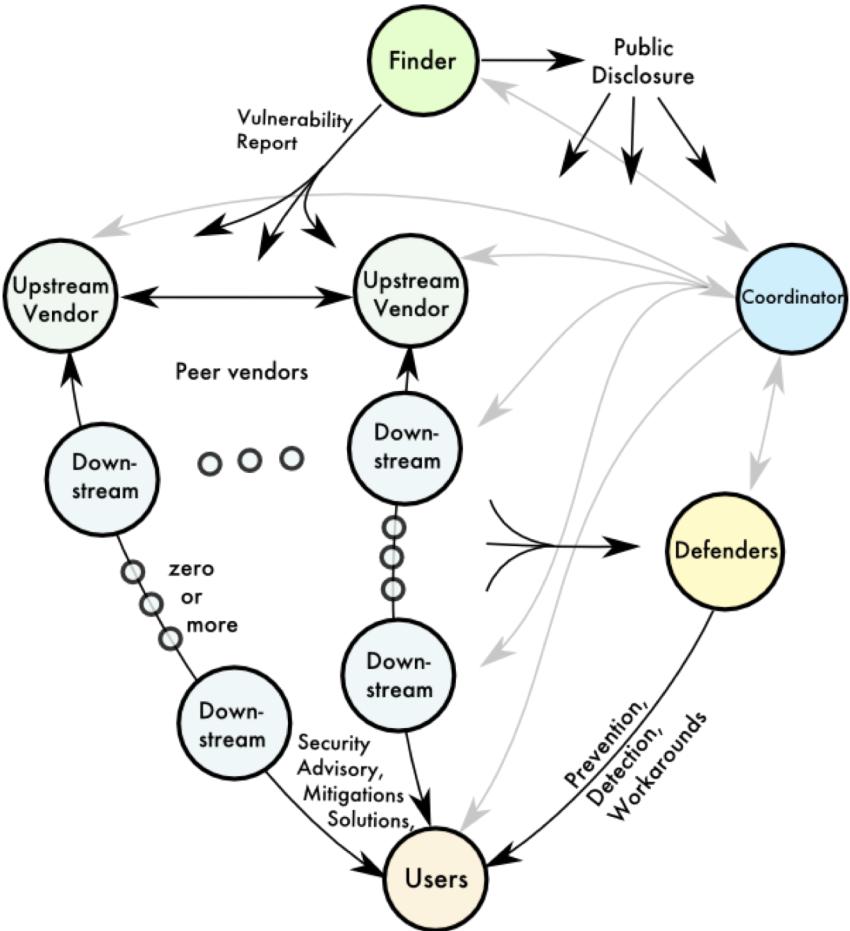
It was clear from then on that information exchange and cooperation on issues of mutual interest like new vulnerabilities or wide ranging attacks - especially on core system like the DNS servers or the Internet as a critical infrastructure itself - were the key issues for security and incident response teams.

Since 1990, when FIRST was founded, its members have resolved an almost continuous stream of security-related attacks and incidents including handling thousands of security vulnerabilities affecting nearly all of the millions of computer systems and networks throughout the world connected by the ever growing Internet.

FIRST brings together a wide variety of security and incident response teams including especially product security teams from the government, commercial, and academic sectors.

<https://first.org>

# Multi-Party Coordination



# Building an Incident Response Team

1

The first step to building a Computer Security Incident Response Team (CSIRT) is the decision and sponsorship by senior management of the creation of such team.

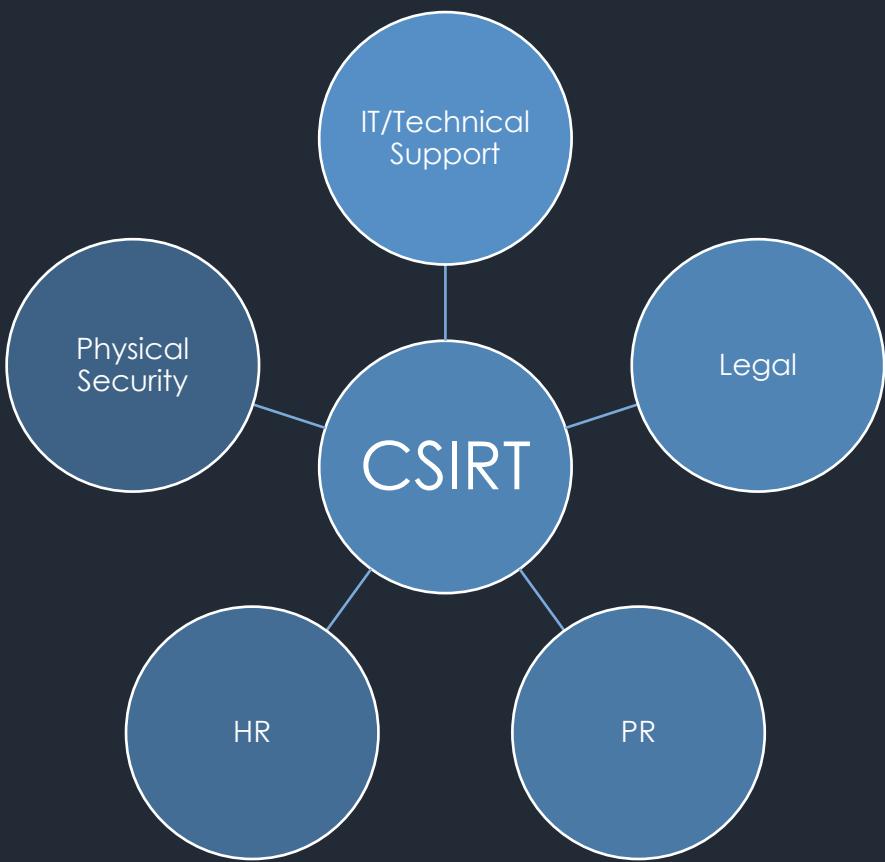
2

Then create the CSIRT charter including all the key elements that will drive the creation of such team.

Creating the Incident Response Team

## THE INCIDENT RESPONSE CHARTER SHOULD:

- Obtain senior leadership support
- Define the constituency
- Create a mission statement
- Outline the CSIRT service deliverables
- Proactive services
- Reactive services



CSIRT Support Teams

## CSIRT MEMBER ROLES

- Incident Response Coordinators
- CSIRT Senior Analysts
- CSIRT Analysts
- Security Operations Center (SOC) Analyst
- IT Security Engineer / Analysts

A CSIRT may also need to interface with law enforcement and government agencies at times, especially if they are targeted as part of a larger attack perpetrated against a number of similar organizations.

Having these relationships can help you with intelligence sharing and resources in the event of an incident.

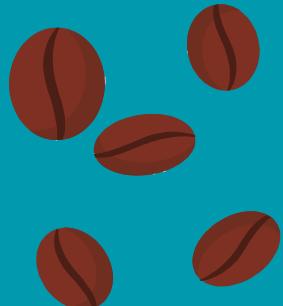
Examples:

- High Technology Crime Investigation Association (HTCIA): <https://htcia.org>
- Infragard: <https://www.infragard.org>
- ISACs: <https://www.nationalisacs.org>
- Local Law enforcement

## THE INCIDENT RESPONSE CHARTER SHOULD:

- Obtain senior leadership support
- Define the constituency
- Create a mission statement
- Outline the CSIRT service deliverables
- Proactive services
- Reactive services

# BREAK



**REMEMBER TO CHECK OUT THE RESOURCES AT:**

<https://theartofhacking.org>

<https://theartofhacking.org/training>

<https://theartofhacking.org/github>

[https://theartofhacking.org/go/training\\_resources.pdf](https://theartofhacking.org/go/training_resources.pdf)

# The Incident Response Plan

3

The policy elements described in NIST Special Publication 800-61 include:

- Statement of management commitment
- Purpose and objectives of the incident response policy
- The scope of the incident response policy
- Definition of computer security incidents and related terms
- Organizational structure and definition of roles, responsibilities, and levels of authority
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact forms

NIST's incident response plan elements include the following:

- Incident response plan's mission
- Strategies and goals of the incident response plan
- Senior management approval of the incident response plan
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization

NIST also defines standard operating procedures (SOPs) as:

“...a delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team. SOPs should be reasonably comprehensive and detailed to ensure that the priorities of the organization are reflected in response operations.”

Not all incidents are equal in their severity and threat to the organization.

**High-severity.** Examples:

- Confirmed network intrusion
- Physical compromise of critical systems
- Compromise of critical accounts
- Targeted attacks and exfiltration of sensitive data

**Moderate (medium) severity.** Examples:

- Anticipated or ongoing DoS
- Confined malware infection
- Unusual system performance or behavior

**Low severity incident.** Examples:

- Lost or stolen mobile device containing encrypted confidential information.
- Policy or procedural violations

- Tracking incidents are a critical responsibility of the CSIRT.
- All actions taken by the CSIRT and other personnel during an incident should be clearly documented during an incident.
- Unique identifiers should be used.

## Incident Tracking

# CISRT / Incident Tracking Tools



Incident Tracking

bestpractical/rt: Request Tracker

GitHub, Inc. [US] | https://github.com/bestpractical/rt

This repository Search Pull requests Issues Marketplace Explore

Watch 72 Star 426 Fork 155

bestpractical / rt

Pull requests 51 Projects 0 Insights

Request Tracker, an enterprise-grade issue tracking system <https://bestpractical.com/rt>

21,502 commits 132 branches 692 releases 68 contributors GPL-2.0

Branch: stable New pull request Create new file Upload files Find file Clone or download

cbrandtbuffalo Merge branch '4.4/disabled-user-in-single-custom-role' into 4.4-trunk Latest commit 4e6b89a 8 days ago

bin Update copyright for 2018 11 days ago

devel Merge branch '4.2-trunk' into 4.4-trunk 11 days ago

docs Merge branch '4.2-trunk' into 4.4-trunk 11 days ago

etc Update copyright for 2018 11 days ago

lib Show the user in single member custom roles even if the user is disabled 10 days ago

sbin Update copyright for 2018 11 days ago

share Indent fix 10 days ago

t Test AddWatcher with disabled user in single member custom role 9 days ago

.gitattributes Due to a git bug, be explicit about ignored directories 5 years ago

.gitignore ignore the generated rt-passwd from git a month ago

.perlcriticrc update perl critic policies 4 years ago

.perltidyrc Added a first draft perltidy for RT 8 years ago

COPYING README\_COPYING and UPGRADE should not be executable 12 years ago

rt-4.4.2.tar.gz ... Show All X

# Request Tracker

CrowdStrike/falcon-orchestrator X Omar

GitHub, Inc. [US] | <https://github.com/CrowdStrike/falcon-orchestrator>



CROWDSTRIKE  
FALCON ORCHESTRATOR

CrowdStrike Falcon Orchestrator is an extendable Windows-based application that provides workflow automation, case management and security response functionality. The tool leverages the highly extensible APIs contained within the CrowdStrike Falcon Connect program.

## Video Demonstration

Check out the following [video](#) on YouTube for a project overview and demonstration of Falcon Orchestrator.

## Support

As an open source project this software is not officially supported by CrowdStrike. As such we ask that you please refrain from sending inquiries to the CrowdStrike support team. The project maintainers will be working with active community contributors to address bugs and supply new features. If you have identified a bug please submit an issue through GitHub by following the contribution guidelines. You can also post questions or start conversations on the project through our [community forums](#) page.

You can also join the project chat room to discuss in greater detail, click [slack](#) 5+ to sign up. Please note that the email you sign up with will be viewable by other users. If you wish to keep your company name anonymous you should use a personal email that holds no affiliation.

## Getting Started

opensourcesec/CIRTKit: Tools

GitHub, Inc. [US] | https://github.com/opensourcesec/CIRTKit

README.md

# CIRTKIT

*One DFIR console to rule them all. Built on top of the [Viper Framework](#)*

---

[build](#) [unknown](#)

## Documentation

- Please see the [wiki](#) for more information about CIRTKit and documentation

## Roadmap

### Future integrations

- Bit9
- Palo Alto Networks
- EnCase/FTK

### Future modules

- Packet Analysis (possibly Dshell)
- Javascript Unpacking/Deobfuscation

Mitigation, Memory Analysis, Forensics

CIRT Kit

A screenshot of a web browser window showing the Demisto Enterprise homepage. The URL in the address bar is <https://www.demisto.com/>. The page features a dark background with a green abstract wave pattern. At the top, there is a navigation bar with links for PRODUCT, WHY DEMISTO?, COMPANY, COMMUNITY, BLOG, PARTNERS, and RESOURCES, along with a "FREE COMMUNITY EDITION" button. A red arrow points upwards from the bottom right towards this button. The main title "Demisto Enterprise" is displayed prominently in white text. Below it, the tagline "The one and only product to unify" is shown. At the bottom, three service offerings are listed: "INCIDENT MANAGEMENT", "SECURITY ORCHESTRATION", and "INTERACTIVE INVESTIGATION", each preceded by a green circular icon.

Demisto Enterprise - Comprehend, Automate, Investigate

https://www.demisto.com/

DEMISTO

PRODUCT WHY DEMISTO? COMPANY COMMUNITY BLOG PARTNERS RESOURCES FREE COMMUNITY EDITION

# Demisto Enterprise

The one and only product to unify

INCIDENT MANAGEMENT

SECURITY ORCHESTRATION

INTERACTIVE INVESTIGATION

Demistro

certsocietegenerale/FIR: Fast Incident Response

GitHub, Inc. [US] | https://github.com/certsocietegenerale/FIR/

README.md

build passing

## What is FIR? Who is it for?

FIR (Fast Incident Response) is an cybersecurity incident management platform designed with agility and speed in mind. It allows for easy creation, tracking, and reporting of cybersecurity incidents.

FIR is for anyone needing to track cybersecurity incidents (CSIRTs, CERTs, SOCs, etc.). It's was tailored to suit our needs and our team's habits, but we put a great deal of effort into making it as generic as possible before releasing it so that other teams around the world may also use it and customize it as they see fit.

STARRED INCIDENTS

Date	Category	Subject	Business Lines	Severity	Status	Detection	Leader	Last Action	Plan	Lvl	IH	Edit
2015-03-10	★ Phishing	http://phishingsite.com/url/	Sub BL 1	2	Open	CERT	CERT	Abuse 16 hours ago	B	C1	dev	edit

Open Blocked Old Tasks

Date	Category	Subject	Business Lines	Severity	Status	Detection	Leader	Last Action	Plan	Lvl	IH	Edit
2015-03-10	★ Phishing	http://phishingsite.com/url/	Sub BL 1	2	Open	CERT	CERT	Abuse 16 hours ago	B	C1	dev	edit
2015-01-15	★ Phishing	test	Demo BusinessLine 1	1	Open	CERT	None	Opened 2 months ago	None	C1	dev	edit
2015-01-05	★ Phishing	test	Demo BusinessLine 1, Demo BusinessLine 2	2	Open	P0le	None	Alerting 2 months ago	None	C1	dev	edit
2015-01-05	★ Phishing	test	Demo BusinessLine 1, Demo BusinessLine 2	2	Open	P0le	None	Opened 2 months ago	None	C1	dev	edit
2014-12-17	★ IS Integrity	Alerte Jokeware	Demo BusinessLine 1	1	Open	SOC	None	Opened 3 months ago	None	C1	dev	edit
2014-12-17	★ Phishing	phishing	Demo BusinessLine 1, Demo BusinessLine 2	2	Open	CERT	CERT	Info 3 months ago	B	C1	dev	edit

(page 1 of 1)

FIR New event Dashboard Incidents Events Stats search... Currently logged in as dev | Logout | Admin

Incident / Phishing / test

Opened on Jan 15, 2015, 5:47 p.m. by dev

DESCRIPTION	CORRELATED ARTIFACTS
phishing copying our brand website on http://newwebsite.com/testurl	Type: Value Hostnames: evlwebsite.com

# Fast Incident Response (FIR)

sandialabs/scot: Sandia Cyber Omni Tracker

GitHub, Inc. [US] | https://github.com/sandialabs/scot

This repository Search Pull requests Issues Marketplace Explore

Watch 38 Star 164 Fork 37

Code Issues 2 Pull requests 0 Projects 0 Wiki Insights

Sandia Cyber Omni Tracker (SCOT) <http://getscot.sandia.gov>

perl javascript cyber-security incident-response

7,787 commits 3 branches 6 releases 10 contributors

Branch: master New pull request Create new file Upload files Find file Clone or download

brymon68 Merge branch 'master' of baltig.sandia.gov:scot/SCOT Latest commit 28ee11c 23 days ago

File	Description	Time Ago
bin	testing programs for queue	a month ago
demo	adding env to demo	a month ago
docker-configs	fixes to open source mongo and commented out ldap stuffs	a month ago
docker-scripts	update to restore script for docker	2 months ago
docs	Preliminary work for beamup	2 months ago
etc	so close, so close	a year ago
install	updating default config files	a month ago
lib	undiscovered regex bug in sourcefire parser	23 days ago
pkgs	Initial SCOT release	4 years ago
pubdev	Merge branch 'master' of baltig.sandia.gov:scot/SCOT	24 days ago
public	added remove event emitter functionality when changing between ids	24 days ago
script	Initial SCOT release	4 years ago

# Sandia Cyber Omni Tracker (SCOT)

Secure | https://scotdemo.com/#/intel/4

Alert Event Incident Intel More Incident Handler: undefined

Mute Notifications Create Intel Export to CSV Full Screen Toggle (f)

ID	Location	Subject	Created	Updated	Sources	Tags	Owner	Entries	Views
4	demosite	Twitter feed reporting new malicious md5 dump	5/4/2018, 11:00:37 AM	5/4/2018, 11:00:38 AM	twitter	md5	kelly	1	0
3	demosite	Twitter feed reporting 0 day	5/4/2018, 11:00:36 AM	5/4/2018, 11:00:37 AM	twitter	0day	joplin	1	0
2	demosite	Malicious Screen Savers	5/4/2018, 11:00:29 AM	5/4/2018, 11:00:30 AM	fitzgerald		pilgrim	2	0
1	demosite	Mandiant APT1 Report	5/4/2018, 11:00:23 AM	5/4/2018, 11:00:40 AM	mandiant	threat_actor	joplin	1	0

Previous Page 1 of 1 50 rows Next

### Intel 4: Twitter feed reporting new malicious md5 dump

Owner: kelly Updated: 05/04/18 11:00:38 am Tags: md5 Sources: twitter

Add Entry Upload File Toggle Flair Viewed By History Intel History Permissions View Entities Links Create & Link Signature Print Delete Intel Marked Objects

[17] 05/04/2018 11:00:38 am by kelly (updated on 05/04/2018 11:00:38 am)

Reply Edit

MD5 dump containing a list of known bad hashes.

098f6bcd4621d373cade4e832627b4f6 8253053f2c9e565a136264e6f96aa57b 5a105e8b9d40e1329780d62ea2265d8a ad0234829205b9033196ba818f7a872b

SCOT Demo

defpoint/threat\_note: DPS' Light... | GitHub, Inc. [US] | https://github.com/defpoint/threat\_note

Omar

This repository Search Pull requests Issues Marketplace Explore

Watch 52 Star 286 Fork 72

Code Issues 43 Pull requests 1 Projects 0 Wiki Insights

### DPS' Lightweight Investigation Notebook

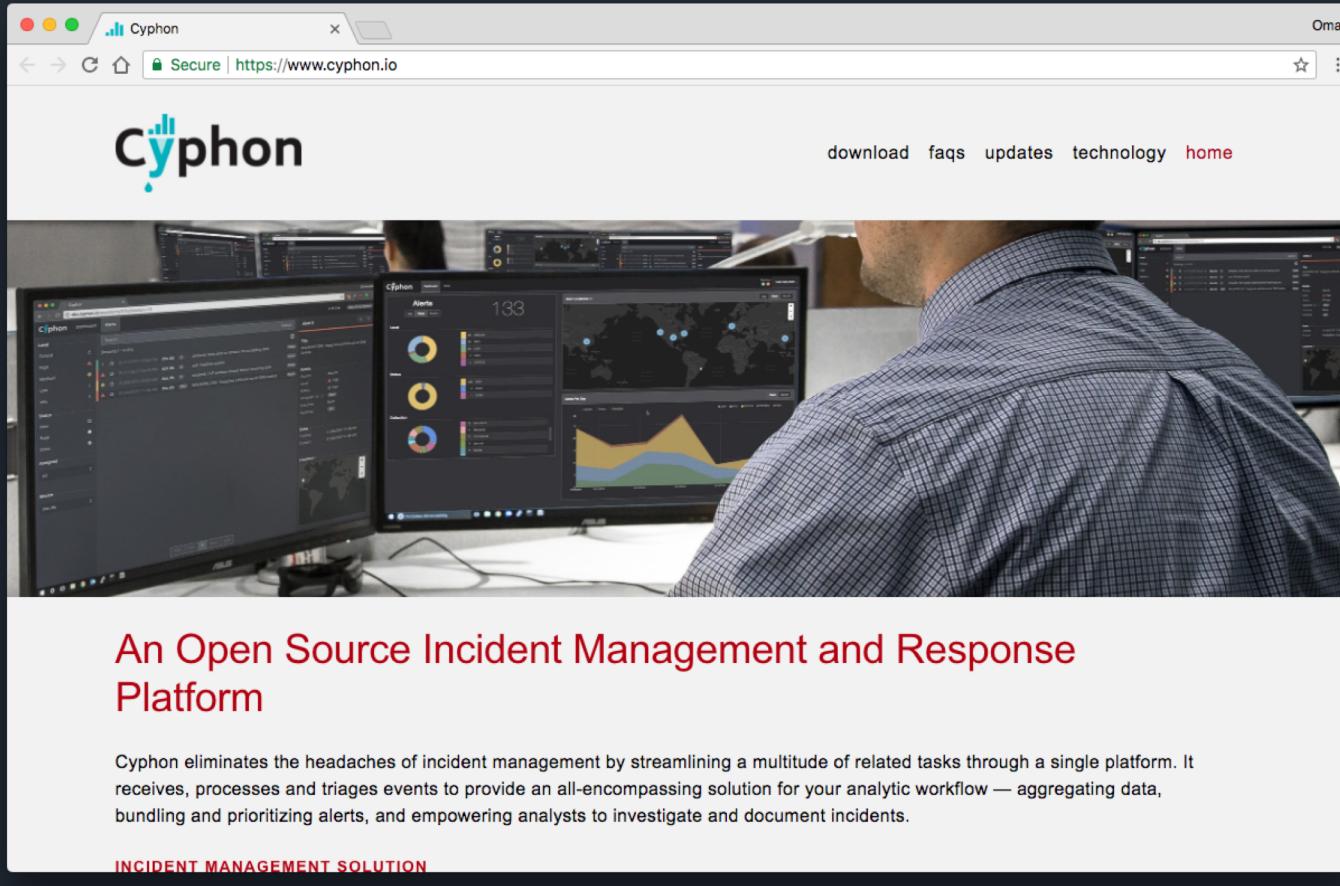
396 commits 2 branches 0 releases 11 contributors Apache-2.0

Branch: master New pull request Create new file Upload files Find file Clone or download

null brianwarehime Merge pull request #163 from k3vb0t/master ... Latest commit 7c56e5a on Aug 15, 2016

	docker	Resolved dependency issues.
	threat_note	Fixed error with cuckoo database, added some(albeit way to many) exce...
	.editorconfig	added html specific editorconfig
	.gitignore	expanded venv ignore
	.pre-commit-config.yaml	added simple precommit hook
	CONTRIBUTING.md	added development requirements and how to set it up
	LICENSE	Initial commit
	Profile	Change server back to threat_note
	README.md	Minor update to include web address.
	requirements-dev.txt	Updated to reflect changes to ODNS API
	requirements.txt	Updated to reflect changes to ODNS API

threat\_note

A screenshot of a web browser window showing the Cyphon website. The title bar reads "Cyphon" and "Secure | https://www.cyphon.io". The page features the Cyphon logo at the top left, and a navigation menu with links for "download", "faqs", "updates", "technology", and "home". Below the menu is a large photograph of a man in a checkered shirt working at a desk with multiple computer monitors displaying various data visualizations and dashboards. The text "An Open Source Incident Management and Response Platform" is centered below the photo, followed by a descriptive paragraph about the platform's capabilities. A red button labeled "INCIDENT MANAGEMENT SOLUTION" is visible at the bottom left.

**Cyphon**

download faqs updates technology home



An Open Source Incident Management and Response Platform

Cyphon eliminates the headaches of incident management by streamlining a multitude of related tasks through a single platform. It receives, processes and triages events to provide an all-encompassing solution for your analytic workflow — aggregating data, bundling and prioritizing alerts, and empowering analysts to investigate and document incidents.

INCIDENT MANAGEMENT SOLUTION

Cyphon

Security Operations | Enterprise

Omar

Secure | https://www.servicenow.com/products/security-operations.html

service<sup>now</sup>

PRODUCTS SOLUTIONS SERVICES & SUPPORT PARTNERS EVENTS ABOUT US

SEARCH GLOBE MORE



DEMO NOW

CALL

SERVICENOW SECURITY OPERATIONS

## Identify, Prioritize, and Respond to Threats Faster

ServiceNow® Security Operations is an Enterprise Security Response engine offering security incident response, vulnerability response, configuration compliance, and threat intelligence. It's built on the intelligent workflows, automation, orchestration, and deep connection with IT of the ServiceNow platform.

ServiceNOW (commercial)

# Incident Response Playbooks

4

Playbooks help with:

- Incident detection
- Response actions
- Communication

## Why Create a Playbook?

The purpose of a security playbook is to provide all stakeholders with a clear understanding of their responsibilities and procedures before, during, and after a security incident.

Playbooks can't respond  
to incidents on their own<sup>7</sup>



\* ownership

\* follow-up

\* comms



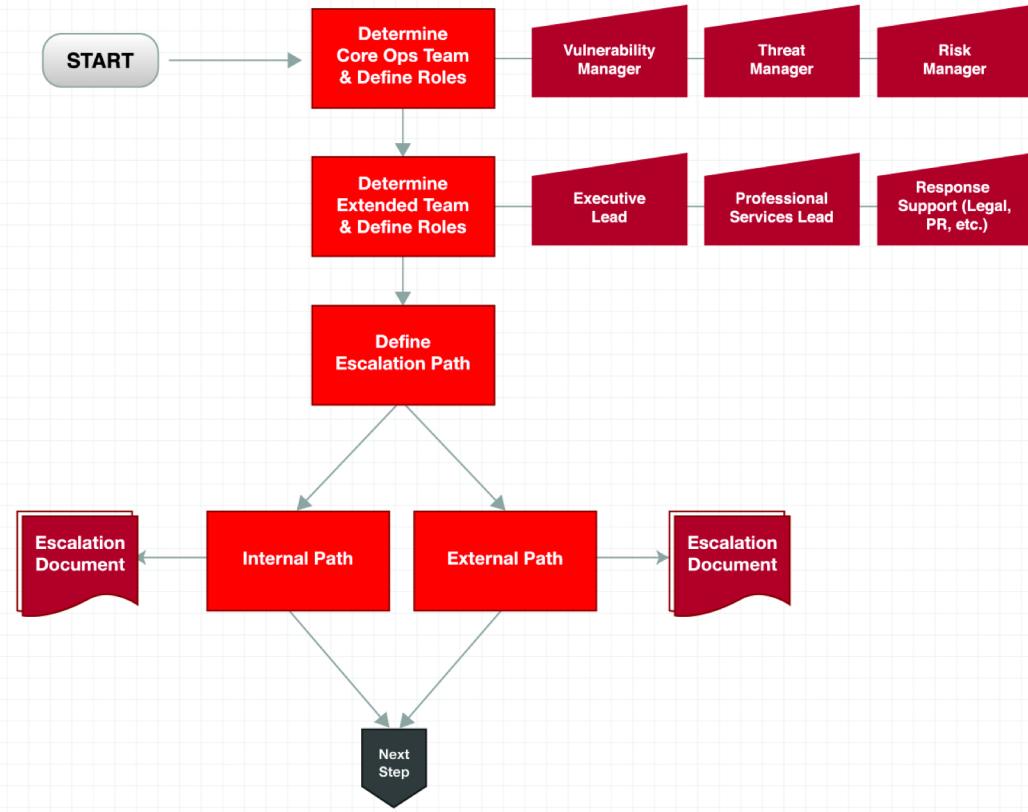
# Scheduling

- real-time necessary ?
- enough analysts to keep up ?
- when to escalate ?

Metrics?

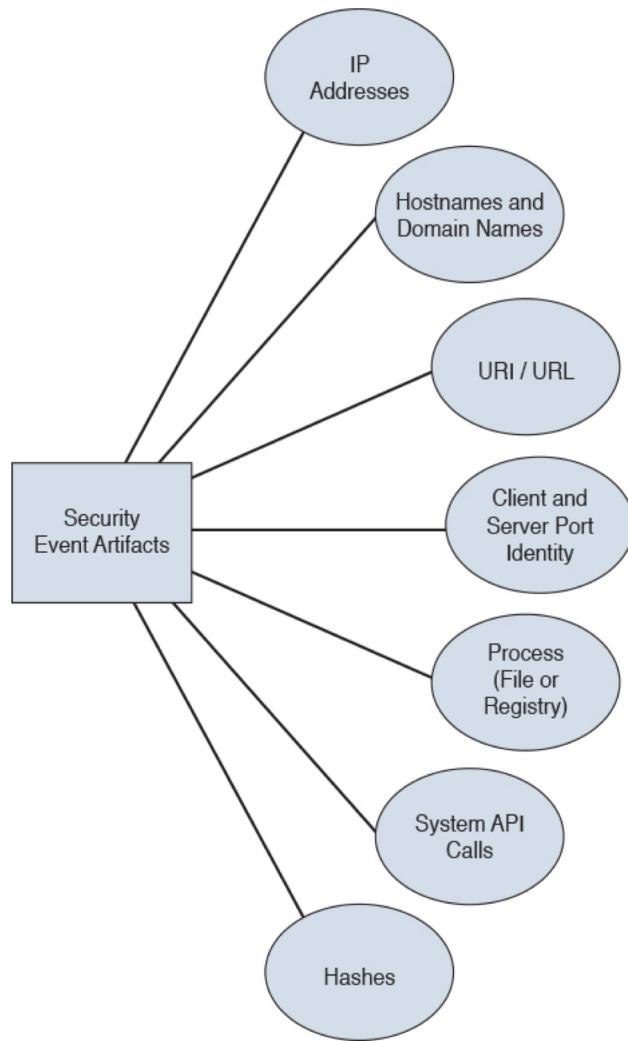


- What to do to avoid duplicate events, tickets, and incidents ?
- What mitigating capabilities and supporting policies exist ?



DEMO

<https://www.incidentresponse.com/playbooks>





DEMO

<https://incident.veriscommunity.net/s3/example>

CSIRT Support Teams

Map of FIRST CSIRT Case Classification schema to VERIS

Information on VERIS can be found at [veriscommunity.net](http://veriscommunity.net)

Information on CSIRT Case Classification can be found at [http://www.first.org/\\_assets/resources/guides/csirt\\_case\\_classification.html](http://www.first.org/_assets/resources/guides/csirt_case_classification.html)

Point of contact: VERIS@verizon.com

VERIS Case Classification Schema:

#	Source Variable	Notes from CSIRT Case Classification	Notes and questions from Verizon	Security Incident	Action External	Action Internal	Action Partner	Action Malware	Action Hacking	Action Social	Action Misuse	Action Physical	Action Error	Action Environmental	Asset Variety	Asset Governance	Attributed to
				variety; motive; country, variety; notes	variety; motive; country, variety; notes	industry; motive; country, variety; notes	industry; motive; country, variety; notes	vector; variety	vector; variety	target; vector; variety	vector; variety	location; vector; variety	vector; variety	vector; variety	vector; variety	vector; variety	
1	Denial of service	DOS or DDoS attack.	Assuming this actually results in availability issues. If just an attack, there would be no attribute. Assuming no particular asset is always implied.	Confirmed	Unknown												Unknown
2	Forensics	Any forensic work to be done by CSIRT.	This isn't an incident as defined by VERIS (doesn't imply damage, loss, or compromise of security attributes of assets).	No													
3	Compromised Information	Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.	The only thing that can be directly inferred is loss of confidentiality. No particular actors, actions, or assets implied. Data variety unknown. If known, they'd need to be recorded on a per-incident basis.	Confirmed													Unknown
4	Compromised Asset	Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.	The only thing that can be directly inferred is loss of confidentiality. No particular actors, actions, or assets implied. Data variety unknown. If known, they'd need to be recorded on a per-incident basis.	Confirmed	Unknown												Unknown
5	Unlawful activity	Theft / Fraud / Human Injury / Data Breach. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.	The only thing that can be directly inferred is that this is a suspected incident.	Suspected													
6	Internal Hacking	Reconnaissance or Suspicious Activity originating from inside the Company corporate network, excluding malware.	Can't infer actor since this could be an external actor moving around inside the network or an insider behaving badly. Assume action is hacking footprinting. Can't infer any particular asset.	Suspected													
7	External Hacking	Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet, excluding malware).	Can directly infer actor is external. Assume action is hacking footprinting. Can't infer any particular asset.	Suspected	Unknown												
8	Malware	A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset).	Assuming confirmed infection. Assuming external actor. Can't infer any particular variety of malware.	Confirmed													Unknown
9	Email	Spammed email, SPAM, and other email security-related events.	Assuming this didn't actually compromise attributes of an asset. If it did, those details will need to be recorded on an incident basis.														
10	Consulting	Security consulting unrelated to any confirmed incident.	This isn't an incident as defined by VERIS. Specific actions that can be inferred are a specific variety of misuse that can be applied to many of them.														
11	Policy Violations	Sharing offensive material, sharing/possession of copyright material. Deliberate violation of Infsec policy by an employee. Unauthorized access to all computer, network, or application. Unauthorized escalation of privileges or deliberate attempt to subvert access controls.	Can directly infer infosec integrity/authenticity attribute. A specific variety of misuse that can be applied to many of them.	Confirmed		Unknown											
12																	
13																	
14																	
15																	
16																	
17																	
18																	
19																	
20																	
21																	
22																	
23																	
24																	
25																	
26																	
27																	
28																	
29																	
30																	
31																	

DEMOCR

<http://veriscommunity.net/veris-mapping.html>

FIRST CSIRT Case Categories and VERIS

MITRE ATT&CK

Secure | https://attack.mitre.org/wiki/Main\_Page

MPN MITRE PARTNERSHIP NETWORK

ATT&CK™  
Adversarial Tactics, Techniques & Common Knowledge

Main page Discussion

Last 5 Pages Viewed: AppleScript [object Object] LLMNR/NBT-NS Poisoning [object Object] Software: Pupy [object Object] Software: Responder [object Object] Adversarial Tactics, Techniques & Co...

Read View source View history Search enterprise

Main page Help Contribute References Using the API

Tactics

- Initial Access
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Execution
- Collection
- Exfiltration
- Command and Control

Techniques

- Technique Matrix
- All Techniques
- Windows
- Linux
- macOS

Groups

- All Groups

Software

- All Software

Tools

- Printable version
- Permanent link

Follow @MITREattack

## Welcome to ATT&CK

MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting known tactics, techniques, and common knowledge used by adversaries. ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and for verifying defenses work as intended.

Note: A MITRE Partnership Network (MPN) account is not required to view and use the ATT&CK site.

PRE-ATT&CK | ATT&CK for Enterprise

### ATT&CK for Enterprise

ATT&CK for Enterprise is an adversary behavior model that describes the actions an adversary may take to compromise and operate within an enterprise network.

- Introduction and Overview
- All Techniques
- ATT&CK Navigator
- Adversary Emulation Plans
- Cyber Analytics Reports
- ATT&CK expressed in...
- Related Efforts
- Using the API
- Contribute or contact us!

### ATT&CK Matrix for Enterprise

The full ATT&CK Matrix below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and	Access Token	Access Token	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port

### DEMO

### News and Updates

News and Blogs

- ATT&CK 101
- PRE-ATT&CK and ATT&CK Integration
- ATT&CK Navigator
- What's Next for ATT&CK

See Past Blogs for previous posts.

Updates

- April 2018
- January 2018
- July 2017

See Past Updates for previous changes.

Cyber Threat Intelligence Tech X

Secure | https://oasis-open.github.io/cti-documentation/ Omar

Home STIX TAXII Contribute FAQ Resources Looking for... STIX 1.x? TAXII 1.x?

## Sharing threat intelligence just got a lot easier!

### STIX™

A structured language for cyber threat intelligence

Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI). STIX enables organizations to share CTI with one another in a consistent and machine readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively. STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.

STIX Relationship Example

[Learn More](#)

### TAXII™

A transport mechanism for sharing cyber threat intelligence

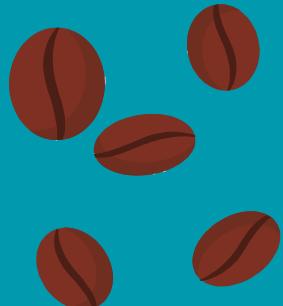
Trusted Automated Exchange of Intelligence Information (TAXII™) is an application layer protocol for the communication of cyber threat information in a simple and scalable manner. TAXII is a protocol used to exchange cyber threat intelligence (CTI) over HTTPS. TAXII enables organizations to share CTI by defining an API that aligns with common sharing models. TAXII is specifically designed to support the exchange of CTI represented in STIX.

TAXII Collections

[Learn More](#)

<https://oasis-open.github.io/cti-documentation>

# BREAK



**REMEMBER TO CHECK OUT THE RESOURCES AT:**

<https://theartofhacking.org>

<https://theartofhacking.org/training>

<https://theartofhacking.org/github>

[https://theartofhacking.org/go/training\\_resources.pdf](https://theartofhacking.org/go/training_resources.pdf)

# Digital Forensics Fundamentals

5



Cybersecurity forensics (or digital forensics) has been of growing interest among many organizations and individuals due to the large number of breaches during the last few years.

# Three broad categories of cybersecurity investigations:

- Public investigations: These investigations are resolved in the court of law.
- Private investigations: These are corporate investigations.
- Individual investigations: These investigations often take the form of e-discovery.



# DiscoveryBriefs

[https://www.youtube.com/watch?v=9Mp261PDj\\_E](https://www.youtube.com/watch?v=9Mp261PDj_E)

# Collecting Evidence from Endpoints and Servers

- Cybersecurity forensic evidence can take many forms, depending on the conditions of each case and the devices from which the evidence was collected.
- To prevent or minimize contamination of the suspect's source device, you can use different tools, such as a piece of hardware called a write blocker, on the specific device so you can copy all the data (or an image of the system).



There are three general types of evidence:

- Best evidence
- Corroborating evidence
- Indirect or circumstantial evidence

# Evidence Preservation

- Use write-protected storage devices.
- The storage device you are investigating should immediately be write-protected before it is imaged and should be labeled to include the following:
  - Investigator's name
  - The date when the image was created
  - Case name and number (if applicable)

<http://h4cker.org/dfir/irt4.html>

# Chain of Custody

- Chain of custody is the way you document and preserve evidence from the time that you started the cyber forensics investigation to the time the evidence is presented in court.
- It is extremely important to be able to show clear documentation of the following:
  - How the evidence was collected
  - When it was collected
  - How it was transported
  - How it was tracked
  - How it was stored
  - Who had access to the evidence and how it was accessed

<http://h4cker.org/dfir/irt4.html>

# Network and Host-Based Evidence Collection and Handling

# Imaging Process in Digital / Cyber Forensics

- The imaging process is intended to copy all blocks of data from the computing device to the forensics professional evidentiary system.
- This is sometimes referred to as a “physical copy” of all data, as distinct from a logical copy, which only copies what a user would normally see.
- Logical copies do not capture all the data, and the process will alter some file metadata to the extent that its forensic value is greatly diminished, resulting in a possible legal challenge by the opposing legal team.
- Therefore, a full bit-for-bit copy is the preferred forensic process.
- The file created on the target device is called a forensic image file.

# The Most Common File Types for Forensic Images

- .AFF
- .ASB
- .E01
- .DD or raw image files
- Virtual image formats such as .VMDK and .VDI

# SANS Forensics Resource



Interested in learning  
more about security?

## SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

### An Overview of Disk Imaging Tool in Computer Forensics

The objective of this paper is to educate users on disk imaging tool ; issues that arise in using disk imaging, recommended solutions to these issues and examples of disk imaging tool. Eventually the goal is to guide users to choose the right disk imaging tool in computer forensics.

<https://www.sans.org/reading-room/whitepapers/incident/overview-disk-imaging-tool-computer-forensics-643>

# Collecting Evidence from Mobile Devices

- Mobile devices such as cell phones, wearables, and tablets are not imaged in the same way as desktops.
- Also, today's Internet of Things (IoT) world is very different from just a few years ago.
- The hardware and interfaces of these devices, from a forensic perspective, are very different.
- In some cases, not only does evidence need to be collected from mobile devices, but also from mobile device management (MDM) applications and solutions.

# Collecting Evidence from Network Infrastructure Devices

- Syslog
- DHCP events
- NetFlow
- Authentication, authorization, and accounting (AAA) logs
- VPN logs
- Firewall logs

<http://h4cker.org/dfir/irt4.html>

# Digital Forensic Tools



Tools of the Trade

The Sleuth Kit (TSK) & Autopsy X

Secure | https://www.sleuthkit.org/index.php

Home Autopsy The Sleuth Kit Other Projects Support About

## Open Source Digital Forensics



**Autopsy®** is an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones. It has a plugin architecture that allows you to find add-on modules or develop custom modules in Java or Python.

**The Sleuth Kit®** is a collection of command line tools and a C library that allows you to analyze disk images and recover files from them. It is used behind the scenes in Autopsy and many other open source and commercial forensics tools.

These tools are used by thousands of users around the world and have community-based email lists and forums. Commercial training, support, and custom development is available from [Basis Technology](#).

[Follow @sleuthkit](#)

### Latest News

14 MAR Linux Autopsy 4.6.0 (beta 1) released First incremental release. 90% complete.

22 FEB Autopsy 4.6.0 released Communications UI, Central Hash DB, USB Triage Drive and more.

21 FEB The Sleuth Kit 4.6.0 released Communications-related DB tables and Java classes. C fixes.

15 OCT The Sleuth Kit 4.5.0 released LZVN HFS+ compression, E01 Sector sizes, and more.

13 OCT Autopsy 4.5.0 released New Correlation Engine, memory improvements and more.

8 AUG Autopsy 4.4.1 released New beta correlation engine and various fixes.

EnCase Endpoint Security - En X

Secure | https://www.guidancesoftware.com/encase-endpoint-security

GUIDANCE is now opentext™

Got Breached? Q ≡

NEED HELP?

# EnCase® Endpoint Security

Earlier Detection, Faster Decisions and Unprecedented Threat Response.

Advanced Detection      Automated Alert Response      New User Interface      New Simplified Workflows

**JUST RELEASED:**

## EnCase Endpoint Security 6.04

EnCase Endpoint Security 6.04 delivers feature enhancements focused on security-first workflows including a fully bi-directional Splunk integration and a new Snapshot Comparison feature. These capabilities provide incident responders with greater automation and contextualization of security alerts, resulting in faster decision-making and improved security efficacy.

[What's New »](#)

[Request Demo »](#)

THE ONLY 360° VISIBILITY INTO THE ENDPOINT

EnCase

Forensic Toolkit X

Secure | <https://accessdata.com/products-services/forensic-toolkit-ftk>

Live Support Chat | Sales +1 800 574 5199

CONTACT US SUPPORT

Products & Services Industries Customer Stories Resources Training Partners About

 ACCESSDATA®

# FORENSIC TOOLKIT (FTK)

## Digital Investigations

[Video](#) | [Features](#) | [Capabilities](#) | [Case Studies](#) | [Infographic](#) | [Testimony](#) | [Resources](#) | [Related Products & Services](#)

### Why You Want It

Zero in on relevant evidence quickly, conduct faster searches and dramatically increase analysis speed with FTK®, the purpose-built solution that interoperates with mobile device and e-discovery technology. Powerful and proven, FTK processes and indexes data upfront, eliminating wasted time waiting for searches to execute. No matter how many different data sources you're dealing with or the amount of data you have to cull through, FTK gets you there quicker and better than anything else.

**UNMATCHED SPEED AND STABILITY**  
FTK uses distributed processing and is the only forensics solution to fully leverage multi-

**FASTER SEARCHING**  
Since indexing is done up front, filtering and searching are completed more efficiently than with

**DATABASE DRIVEN**  
FTK is truly database driven, using one shared case database. All data is stored securely and centrally.

[Leave a message](#)

TOP

# Access Data Forensics Toolkit

Security-Onion-Solutions/sec X GitHub, Inc. [US] | https://github.com/Security-Onion-Solutions/security-onion Omar

This repository Search Pull requests Issues Marketplace Explore

Security-Onion-Solutions / security-onion Watch 263 Star 1,413 Fork 214

Code Issues 90 Pull requests 0 Projects 2 Wiki Insights

Linux distro for IDS, NSM, and Log Management <https://securityonion.net>

intrusion-detection network-security-monitoring log-management ids nsm hunting dfir

2,309 commits 3 branches 21 releases 2 contributors

Branch: master New pull request Create new file Upload files Find file Clone or download

dougburks promote 14.04.5.13 to stable Latest commit 0300d9b 5 days ago

.github	add ISSUE_TEMPLATE	a year ago
old	promote 14.04.5.13 to stable	5 days ago
sigs	update sigs and testing instructions for 14.04.5.13	11 days ago
KEYS	Create KEYS	2 years ago
README.md	promote 14.04.5.11 to stable	27 days ago
Verify_ISO.md	promote 14.04.5.13 to stable	5 days ago
checksums.txt	update sigs and testing instructions for 14.04.5.13	11 days ago

README.md

## Security Onion

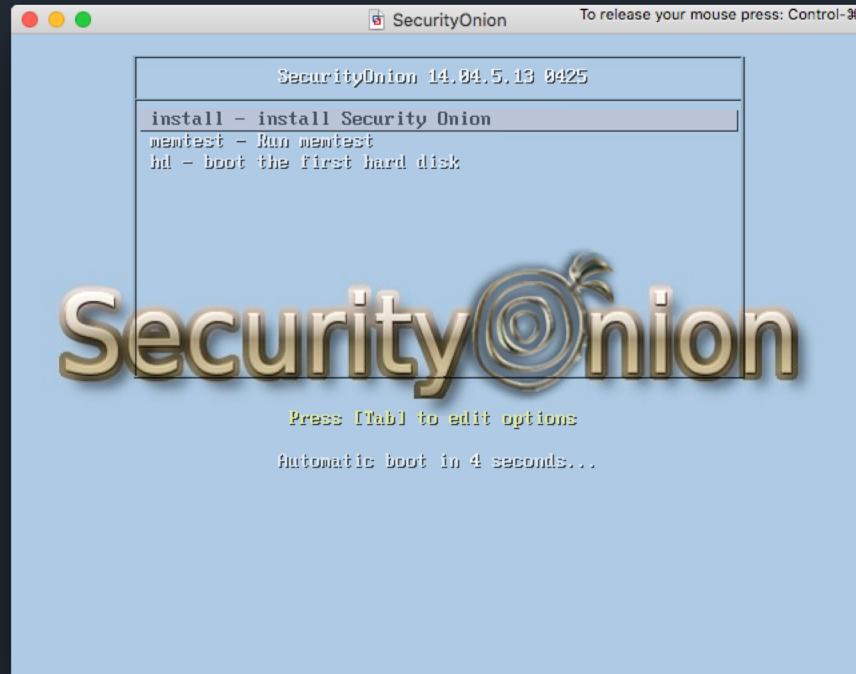
Security Onion is a free and open source Linux distribution for intrusion detection, enterprise security monitoring, and log management. It includes Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro, OSSEC, Sguil, Squert, NetworkMiner, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!

For more information about Security Onion, please see our [main website](#), [blog](#), and [wiki](#).

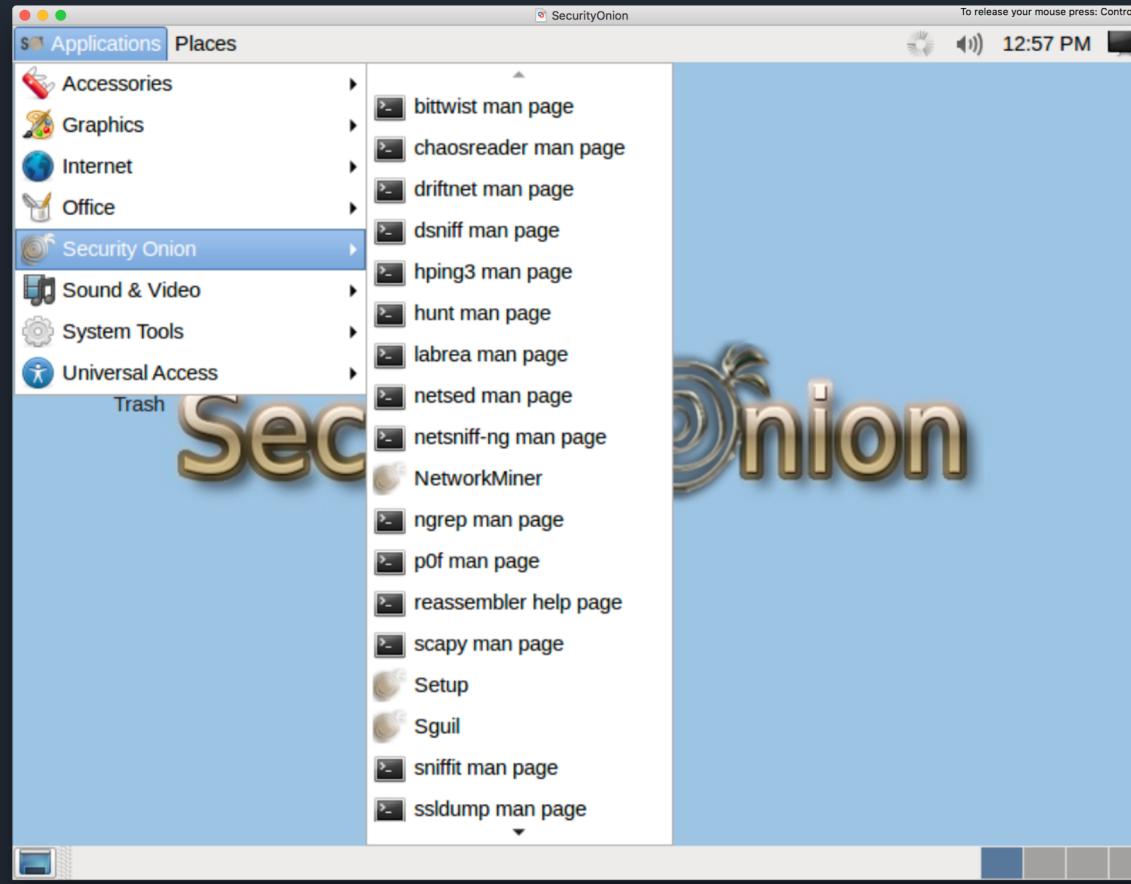
This Repo

This repo contains the [ISO image](#), [Wiki](#), and [Roadmap](#) for Security Onion.

# Security Onion



Security Onion



Security Onion

Linux Forensics Tools Repository - LiFTeR

Welcome

Welcome to the CERT Linux Forensics Tools Repository (LiFTeR), a repository of packages for Linux distributions. Currently, Fedora and CentOS/RHEL are provided in the repository. See here for the Fedora version support table and here for the CentOS/RHEL version support table. If you are interested in porting the repository to other versions of Linux, please see the Contribute section.

The CERT Linux Forensics Tools Repository provides many useful packages for cyber forensics acquisition and analysis practitioners. If you have suggestions for tools to add to the repository, please see the Contribute section.

The CERT Linux Forensics Tools Repository is not a standalone repository, but rather an extension of the supported systems. Tools can be installed as needed or all at once using the `CERT-Forensics-Tools` meta package.

Also described here is ADIA, the VMware-based Appliance for Digital Investigation and Analysis. ADIA is a Fedora-based VMware guest intended to be installed under VMware Workstation, Player, or Fusion. It is not a Live CD. See the ADIA section for more details.

**NOTICE - IMPORTANT Items Shown In Red**

Important items are now shown in red. Pay attention to them because they are important.

Contents

- NOTICE - New RPM Signing Key - February, 2016
- End Of Life Announcement
- Repository RSYNC Server
- Announcements
  - All
  - Recent

Announcements

- By Package
- By Date
- All Announcements

April 27, 2018

PfRing

PF\_RING, version 7.0.0 release 1887, was installed in the CentOS/RHEL 6 and 7 repositories for the x86\_64 architecture.

PfRing-dkms

PF\_RING-dkms, version 7.0.0 release 1887, was installed in the CentOS/RHEL 6 and 7 repositories for the x86\_64 architecture.

APFS\_Fuse

APFS-Fuse, version 20180424 release 1, was installed in the Fedora 22, 23, 24, 25, 26, and 27 repositories for all supported architectures, and the CentOS/RHEL 7 repositories for the x86\_64 architecture.

Aimage

Aimage, version 3.2.5 release 3, was installed in the CentOS/RHEL 6 and 7 repositories for all supported architectures.

CERT-Forensics-Tools

CERT-Forensics-Tools, version 1.0 release 75, was installed in the Fedora 22, 23, 24, 25, 26, and 27 repositories for all supported architectures, and the CentOS/RHEL 6 and 7 repositories for all supported architectures.

examiner-tooldocumentation

Examiner-ToolDocumentation, version 1.18 release 6, was installed in the CentOS/RHEL 7 repository for the x86\_64 architecture.

LIME

Lime-kernel-modules-fc27-{i686,x86\_64}, version 1.1.r17 release 22, were installed in the Fedora 22, 23, 24, 25, 26, and 27 repositories for all

ADIA - The Appliance for Digital Investigation and Analysis

Secure | https://forensics.cert.org/appliance/README.html



## ADIA - The Appliance for Digital Investigation and Analysis

### CentOS 7 Version

This README describes the virtual machine image for ADIA, the Appliance for Digital Investigation and Analysis. These virtual machines are based on CentOS 7.

This version of ADIA supports both VMware and Virtual Box. This version support the x86\_64 (64 bit) host computer system architecture.

You should routinely update ADIA to keep it current with package released by Red Hat and packages released by CERT.

#### Installation - VMware

ADIA has been tested and works on VMware Workstation 14 under Windows 10 Education. We expect that it will work in other configurations but they remain untested. When the virtual machine was packaged for distribution, it was converted to work with VMware Workstation 5 and later.

To install ADIA under VMware, do the following:

1. Download the VMware-based [OVA](#)
2. Optionally check the [PGP/GPG Signature](#).
3. Start VMware.
4. Select **File->Import....**
5. Navigate to the downloaded OVA and select it.
6. Import the virtual machine.
7. If you get an *Import Failed* error message, select **Retry** to continue.
8. Select the **Continue** button to continue.
9. When the import finishes, select the **Finish** button to continue.
10. Optionally update the hardware version of the newly created virtual machine.
11. Start the virtual machine.
12. The virtual machine will boot and automatically login as examiner (with password forensics).
13. This version of ADIA uses the the [MATE Desktop Environment](#).

Installing ADIA under VMware requires about 8Gb of disk space.

#### Installation - Virtual Box

ADIA has been tested and works on Virtual Box 5.2.2 under Windows 10 Education. We expect that it will work in other configurations but they remain untested.

About | DEFT Linux - Computer

www.deftlinux.net/about/

# deft

Home About > Download Package list DEFT Manual Screenshot Contacts

## About

DEFT (acronym for Digital Evidence & Forensics Toolkit) is a distribution made for Computer Forensics, with the purpose of running live on systems without tampering or corrupting devices (hard disks, pendrives, etc...) connected to the PC where the boot process takes place.

The DEFT system is based on GNU Linux, it can run live (via DVDROM or USB pendrive), installed or run as a Virtual Appliance on VMware or Virtualbox. DEFT employs LXDE as desktop environment and WINE for executing Windows tools under Linux. It features a comfortable mount manager for device management.

DEFT is paired with DART (acronym for Digital Advanced Response Toolkit), a Forensics System which can be run on Windows and contains the best tools for Forensics and Incident Response. DART features a GUI with logging and integrity check for the instruments here contained.

Besides all this, the DEFT staff is devoted to implementing and developing applications which are released to Law Enforcement Officers, such as Autopsy 3 for Linux.

DEFT is currently employed in several places and by several people such as:

- Military
- Government Officers
- Law Enforcement
- Investigators
- Expert Witnesses
- IT Auditors
- Universities
- Individuals

Languages

English

Donate

1DEFTAyfqK76woMv9U9o2rD4n3vWVCJLm

Search

Search

A screenshot of a web browser window displaying the 'About' page of the DEFT Linux website. The main content area describes the DEFT system as a digital forensics toolkit based on Linux, mentioning its compatibility with various operating systems and its integration with DART. It also highlights its use by law enforcement agencies and other professionals. A sidebar on the right contains three modules: 'Languages' (with English selected), 'Donate' (with a yellow 'Donate' button and logos for Visa, MasterCard, American Express, and PayPal), and 'Search' (with a search input field and a 'Search' button). The browser's address bar shows the URL www.deftlinux.net/about/. The top navigation bar includes links for Home, About, Download, Package list, DEFT Manual, Screenshot, and Contacts. The title of the page is 'About | DEFT Linux - Computer'.

deft

A lot of people have an understanding and tools to perform forensics on Endpoints and Servers (Linux, OS X, Windows, etc).

However, there is a shortage of knowledge on how to perform forensics and integrity verification in infrastructure devices (routers, switches, firewalls, etc.)

Cisco IOS Device Integrity Assurance:

<https://www.cisco.com/c/en/us/about/security-center/integrity-assurance.html>

Cisco IOS-XE Device Integrity Assurance:

<https://www.cisco.com/c/en/us/about/security-center/ios-xe-integrity-assurance.html>

Cisco ASA Device Integrity Assurance:

<https://www.cisco.com/c/en/us/about/security-center/intelligence/asa-integrity-assurance.html>

The screenshot shows a GitHub repository page for 'The-Art-of-Hacking / art-of-hacking'. The repository has 20 stars, 65 forks, and 22 open pull requests. A pull request titled 'adding DFIR references' by 'santosomar' is shown, which adds references to the README.md file. The README.md file contains a section titled 'Digital Forensics and Incident Response (DFIR) Resources' with a 'Incident Response' subsection listing various tools like Cyphon, Demisto, FIR, RTIR, SCOT, and threat\_note.

## Digital Forensics and Incident Response (DFIR) Resources

### Incident Response

- [Cyphon](#) - Cyphon eliminates the headaches of incident management by streamlining a multitude of related tasks through a single platform. It receives, processes and triages events to provide an all-encompassing solution for your analytic workflow — aggregating data, bundling and prioritizing alerts, and empowering analysts to investigate and document incidents.
- [Demisto](#) - Demisto community edition(free) offers full Incident lifecycle management, Incident Closure Reports, team assignments and collaboration, and many integrations to enhance automations (like Active Directory, PagerDuty, Jira and much more..)
- [FIR](#) - Fast Incident Response (FIR) is an cybersecurity incident management platform designed with agility and speed in mind. It allows for easy creation, tracking, and reporting of cybersecurity incidents and is useful for CSIRTs, CERTs and SOCs alike
- [RTIR](#) - Request Tracker for Incident Response (RTIR) is the premier open source incident handling system targeted for computer security teams. We worked with over a dozen CERT and CSIRT teams around the world to help you handle the ever-increasing volume of incident reports. RTIR builds on all the features of Request Tracker
- [SCOT](#) - Sandia Cyber Omni Tracker (SCOT) is an Incident Response collaboration and knowledge capture tool focused on flexibility and ease of use. Our goal is to add value to the incident response process without burdening the user
- [threat\\_note](#) - A lightweight investigation notebook that allows security researchers the ability to register and retrieve indicators related to their research

### Playbooks

<https://github.com/The-Art-of-Hacking/art-of-hacking/tree/master/dfir>

## CCNA CYBER OPS

- [CCNA Cyber Ops SECFND 210-250 Video Course](#)
- [CCNA Cyber Ops SECOPS 210-255 Video Course](#)
- [Learning Path: CCNA Cyber Ops SECFND \(210-250\) and SECOPS \(210-255\)](#)
- [CCNA Cyber Ops SECFND 210-250 Official Cert Guide](#)
- [CCNA Cyber Ops SECOPS 210-255 Official Cert Guide](#)
- [Cisco NetFlow for Cyber Security Big Data Analytics](#)

## CCNA SECURITY

- [CCNA Security Video Course](#)
- [CCNA Security 210-260 Official Cert Guide](#)
- [Cisco Firepower and Advanced Malware Protection LiveLessons](#)
- [Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP](#)
- [Cisco NetFlow for Cyber Security Big Data Analytics](#)

## ETHICAL HACKING

- [Security Penetration Testing \(The Art of Hacking Series\) LiveLessons](#)
- [Wireless Networks, IoT, and Mobile Devices Hacking \(The Art of Hacking Series\)](#)
- [Enterprise Penetration Testing and Continuous Monitoring The Art of Hacking](#)

## OTHER SAFARI CYBERSECURITY LIVE TRAINING

- [Ethical Hacking - Penetration Testing](#)
- [Cybersecurity Blue Teams vs Red Teams](#)
- [Introduction to Digital Forensics and Incident Response \(DFIR\)](#)
- [Introduction to Cybersecurity](#)



[https://theartofhacking.org/go/training\\_resources.pdf](https://theartofhacking.org/go/training_resources.pdf)

QUESTIONS?

THANK YOU!