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

The CCFP will be designated an inactive credential August 21, 2020. The credential will remain a recognized (ISC)² 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.

EC-Council

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

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™ Certification

EnCE® Certification

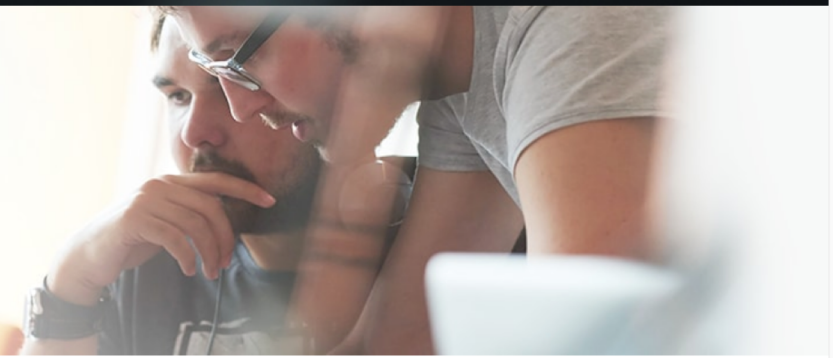
EnCEP® Certification

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

Introduction to the Incident Response Process

Incident Response ISO and NIST References

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:

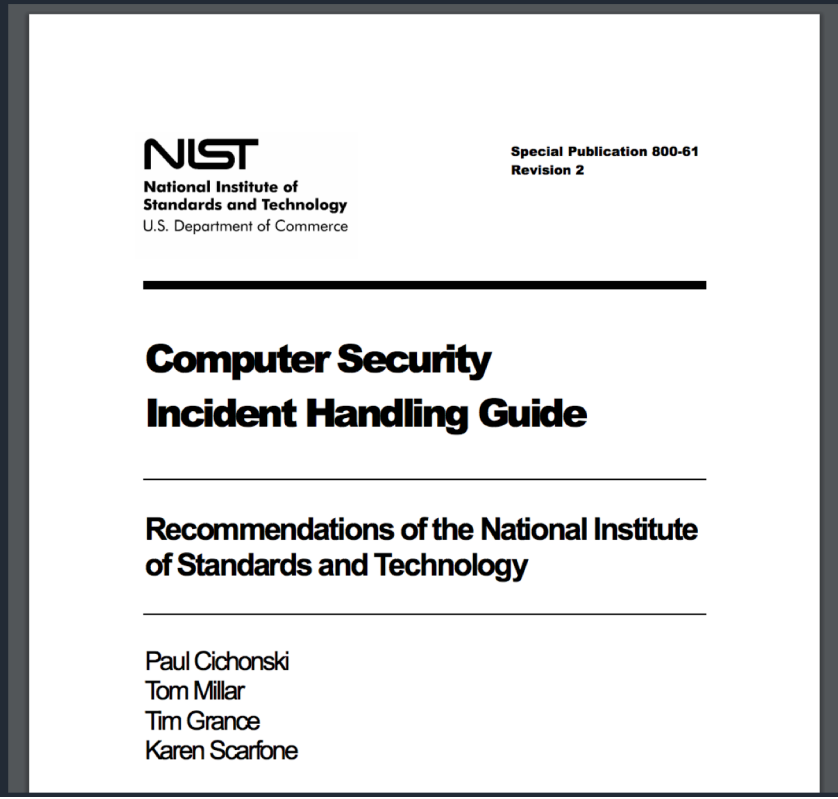
- SP 800-61 Revision 2: “Computer Security Incident Handling Guide”
- SP 800-83 Revision 1: “Guide to Malware Incident Prevention and Handling”
- SP 800-86: “Guide to Integrating Forensic Techniques into Incident Response”

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:


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

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

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

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

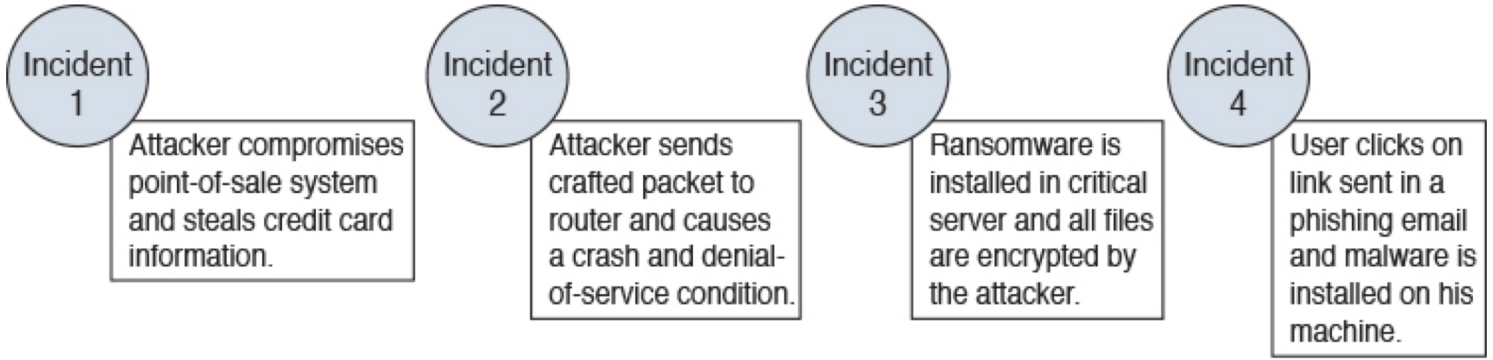
What is an Incident?

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



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

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.

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

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

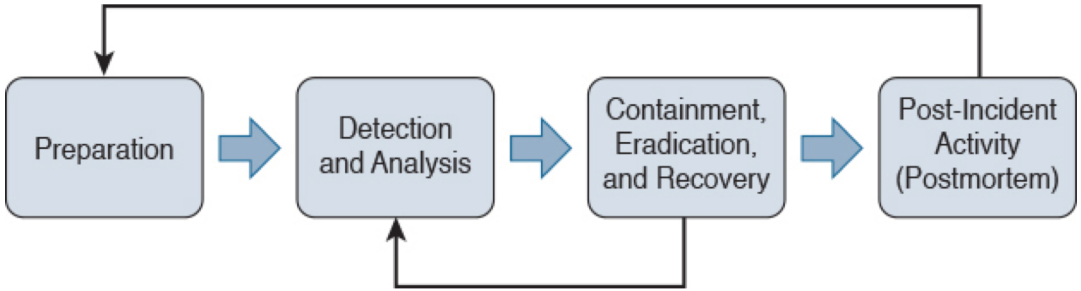
True positive: a successful identification of a security attack or a malicious event.

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

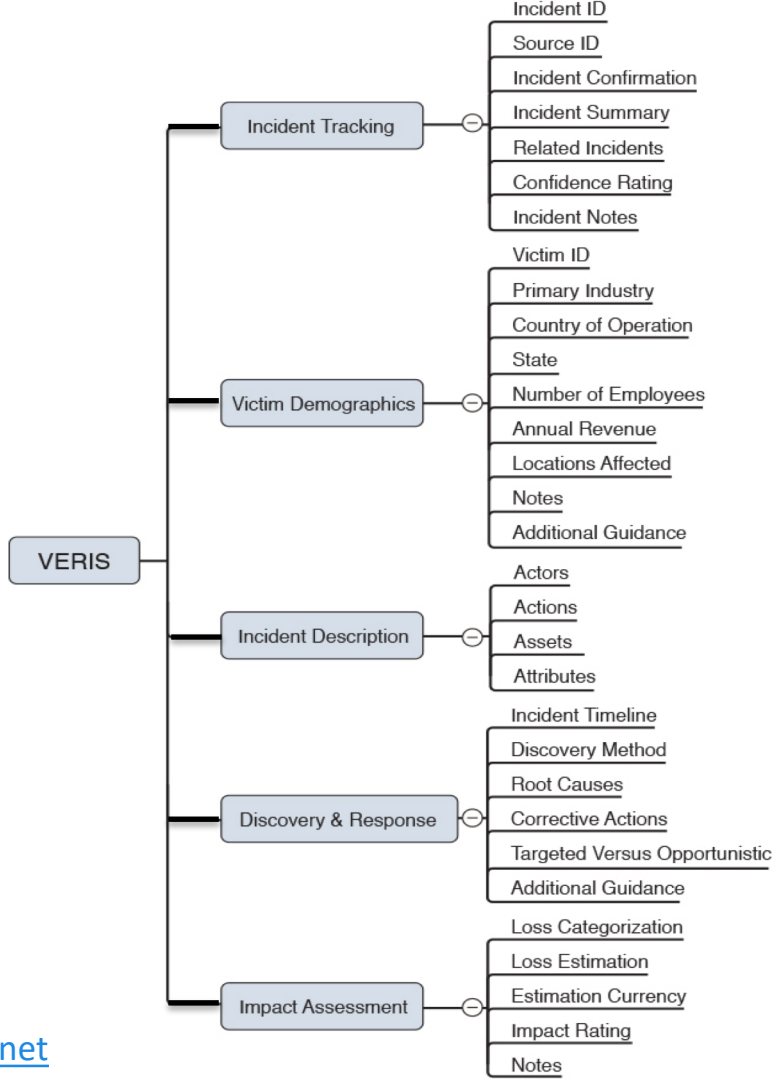
True negative: when the intrusion detection device identifies an activity as acceptable behavior and the activity is actually acceptable.

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

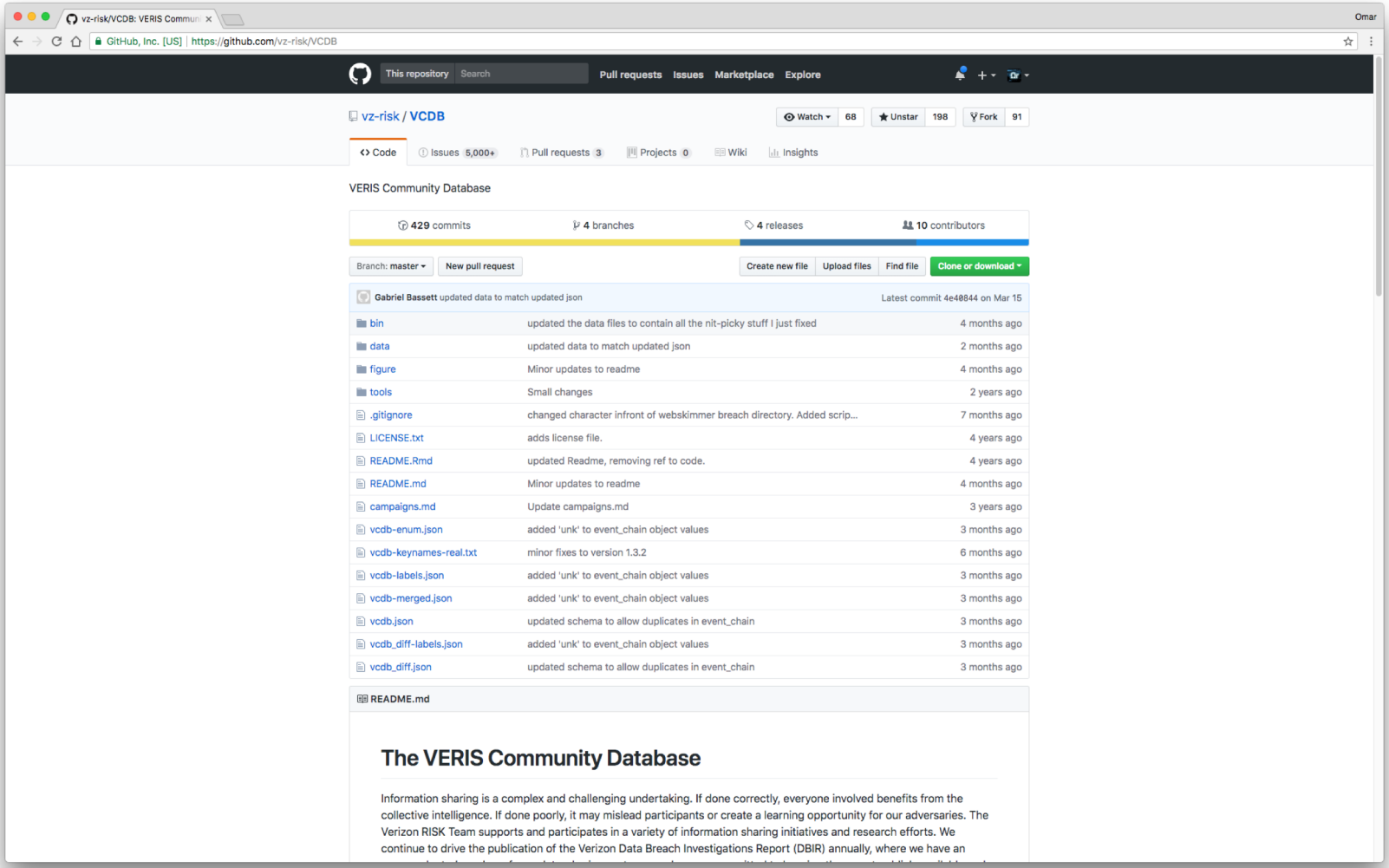
The Incident Response Process (reference NIST 800-61r2)



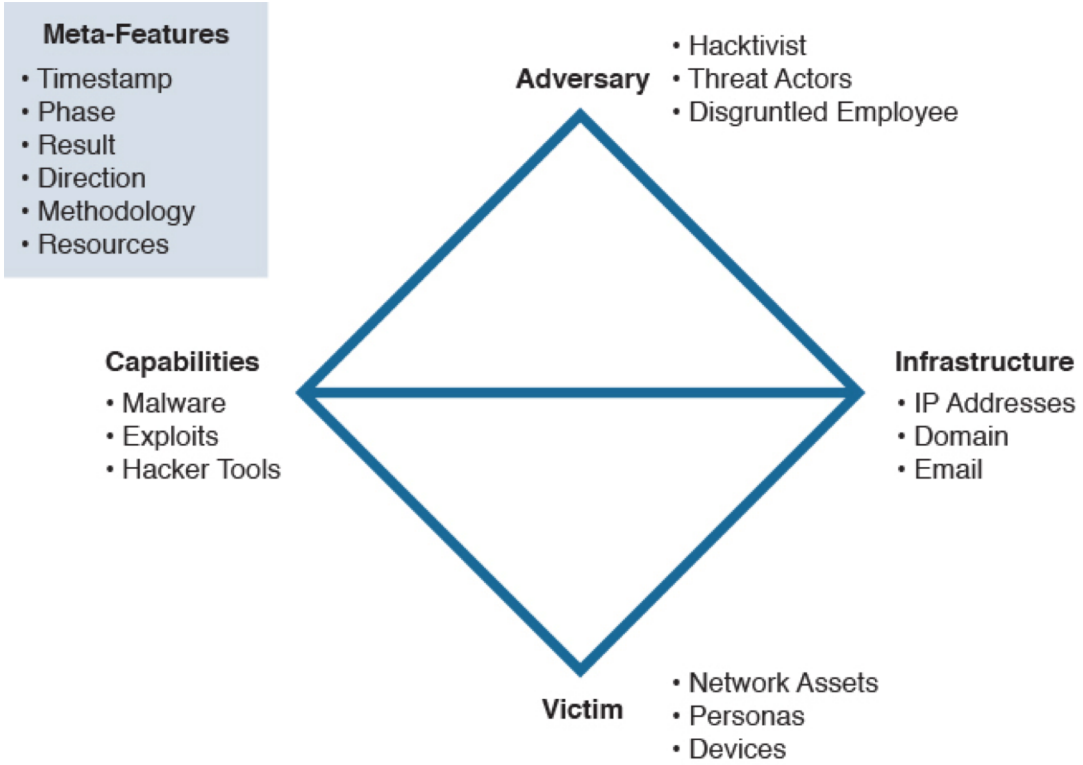
The Vocabulary for Event Recording and Incident Sharing (VERIS)



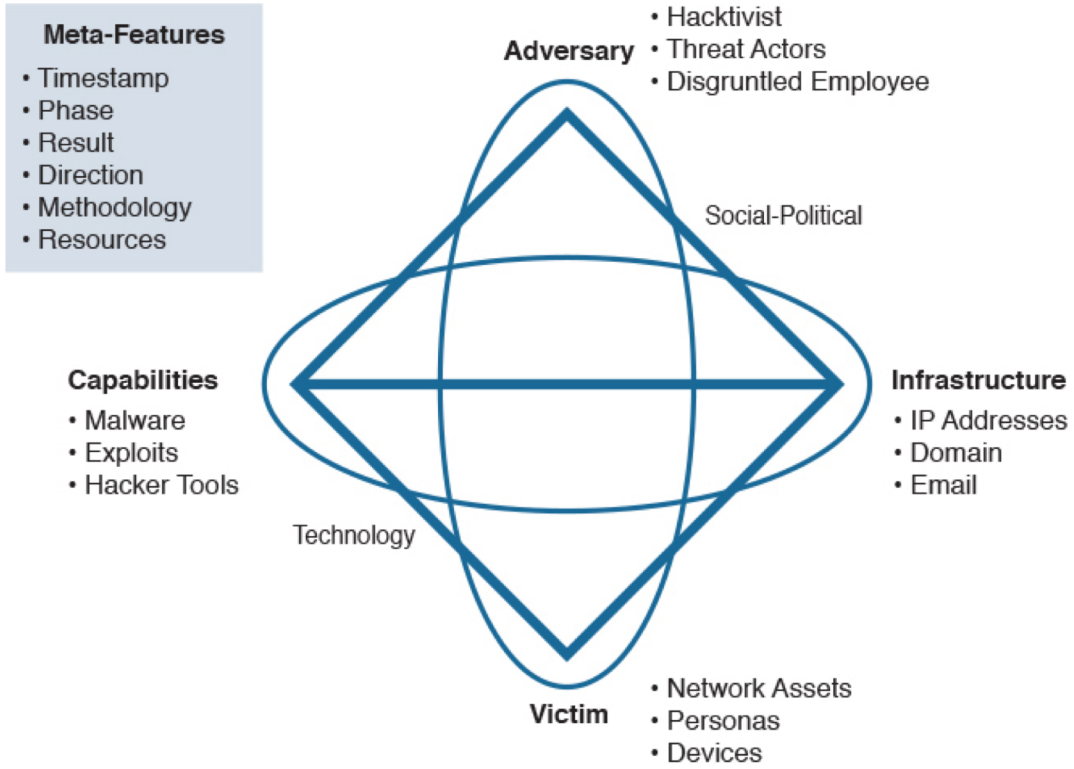
http://veriscommunity.net


vz-risk/VCDB: VERIS Commun
Omar
GitHub, Inc. [US] | https://github.com/vz-risk/VCDB
This repository
Search
Pull requests
Issues
Marketplace
Explore
vz-risk / VCDB
Watch 68
Unstar 198
Fork 91
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 4e40844 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 infront 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

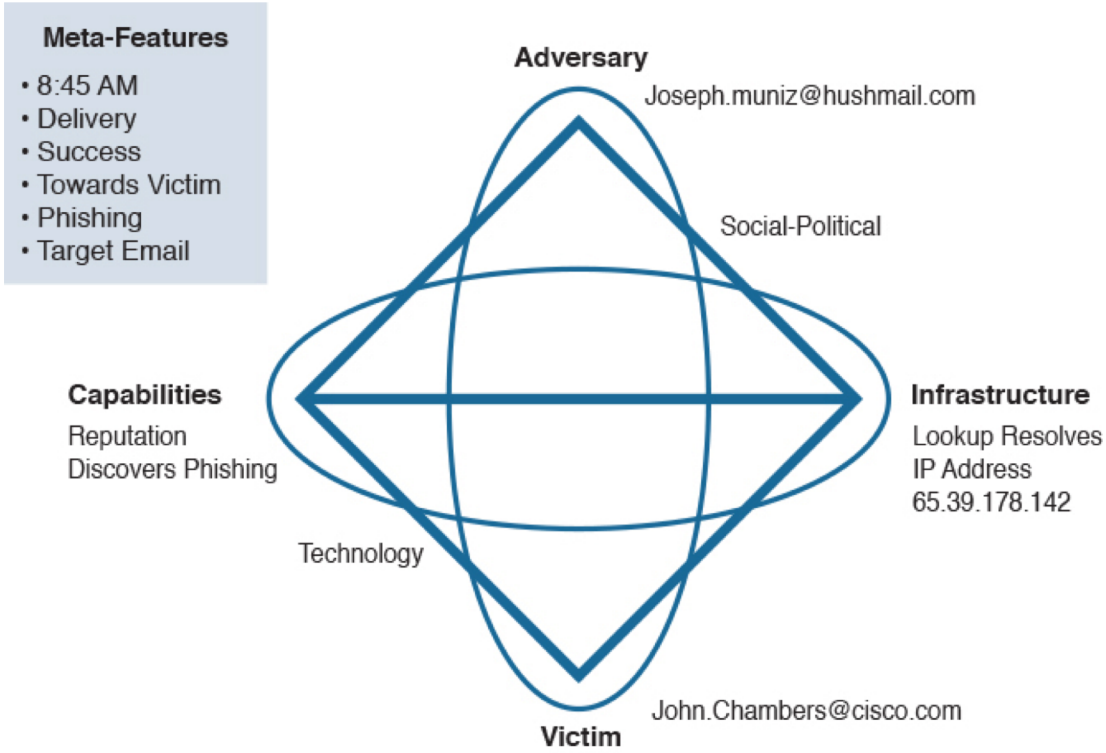
The Diamond Model of Intrusion



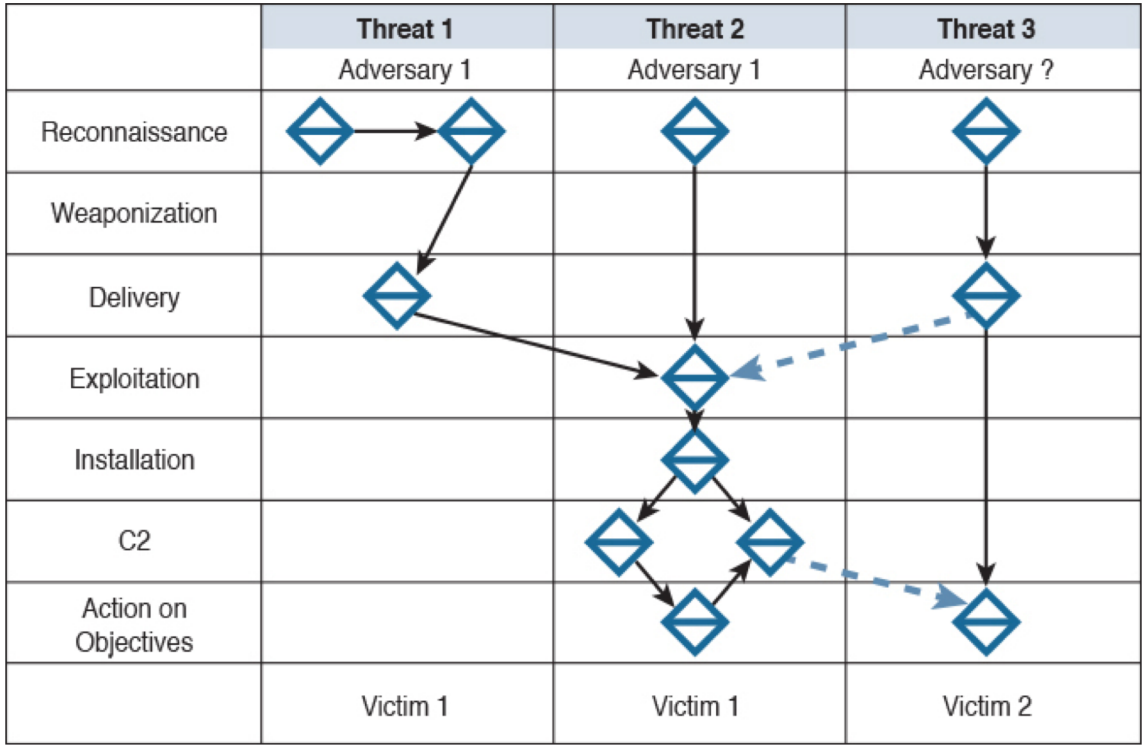
The Diamond Model of Intrusion



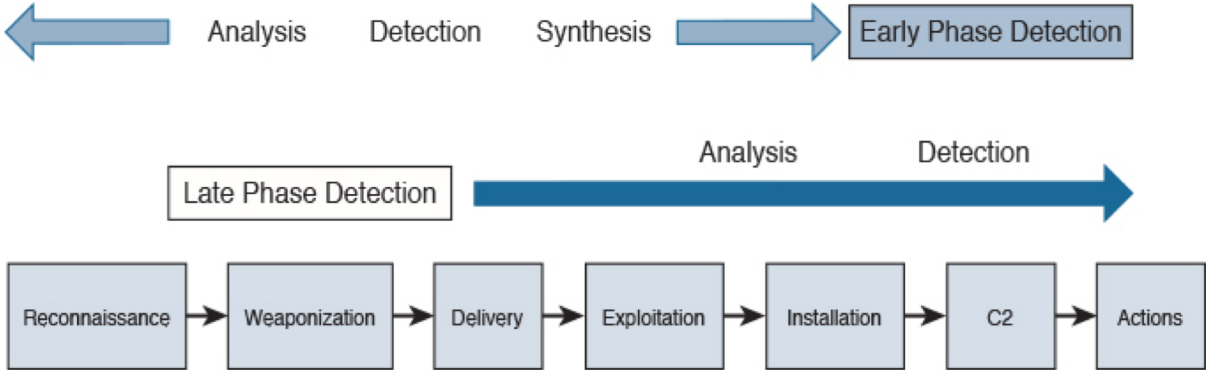
The Diamond Model of Intrusion



The Diamond Model of Intrusion



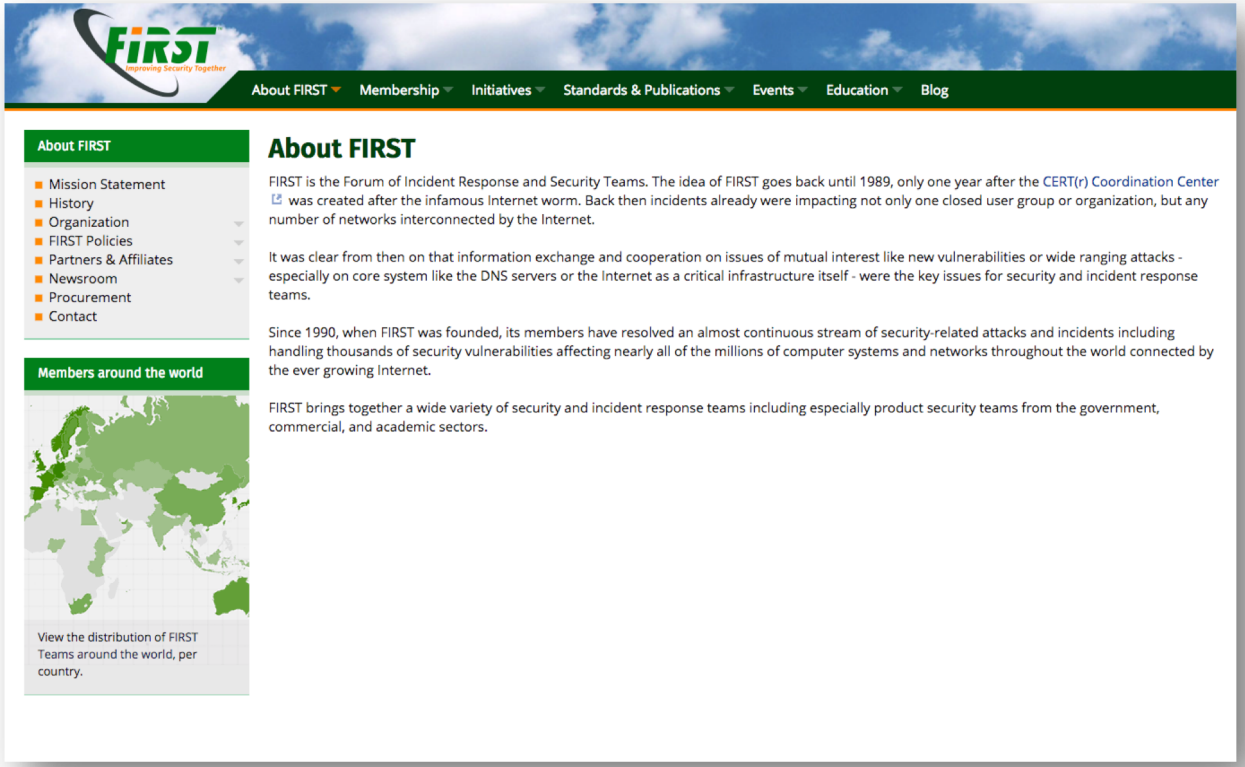
Early and Late Detection in the Kill Chain Example



Incident Response Teams

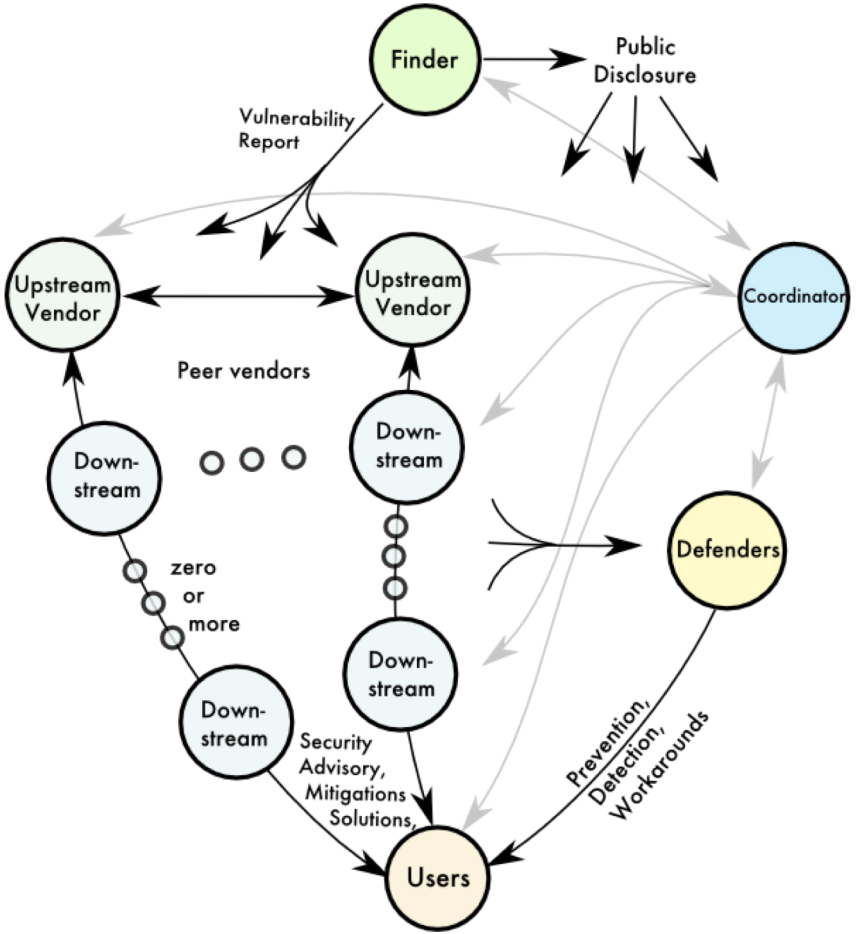
- Computer Security Incident Response Team (CSIRT)
- Product Security Incident Response Team (PSIRT)
- National CSIRTs and Computer Emergency Response Teams (CERTs)
- Coordination center
- Incident response teams of security vendors and managed security service providers (MSSP)

FIRST



https://first.org

Multi-Party Coordination



https://first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0

Building an Incident Response Team

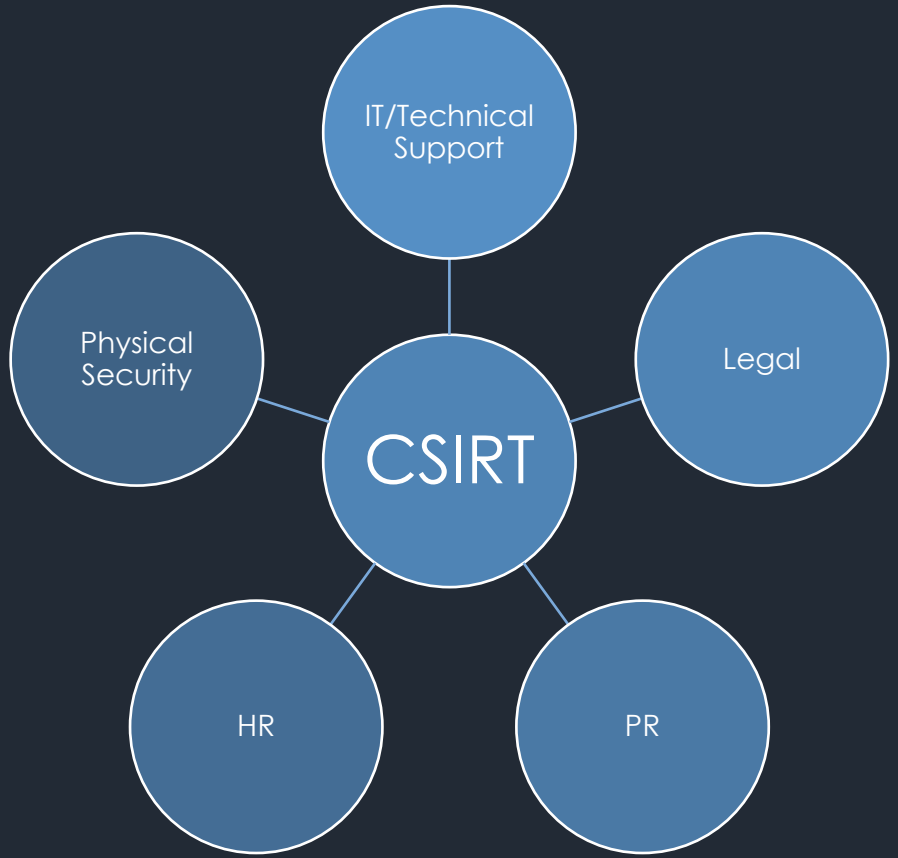
1. The first step to building a Computer Security Incident Response Team (CSIRT) is the decision and sponsorship by senior management of the creation of such team.

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

The Incident Response Plan

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."

Standard Operating Procedures (SOPs)

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

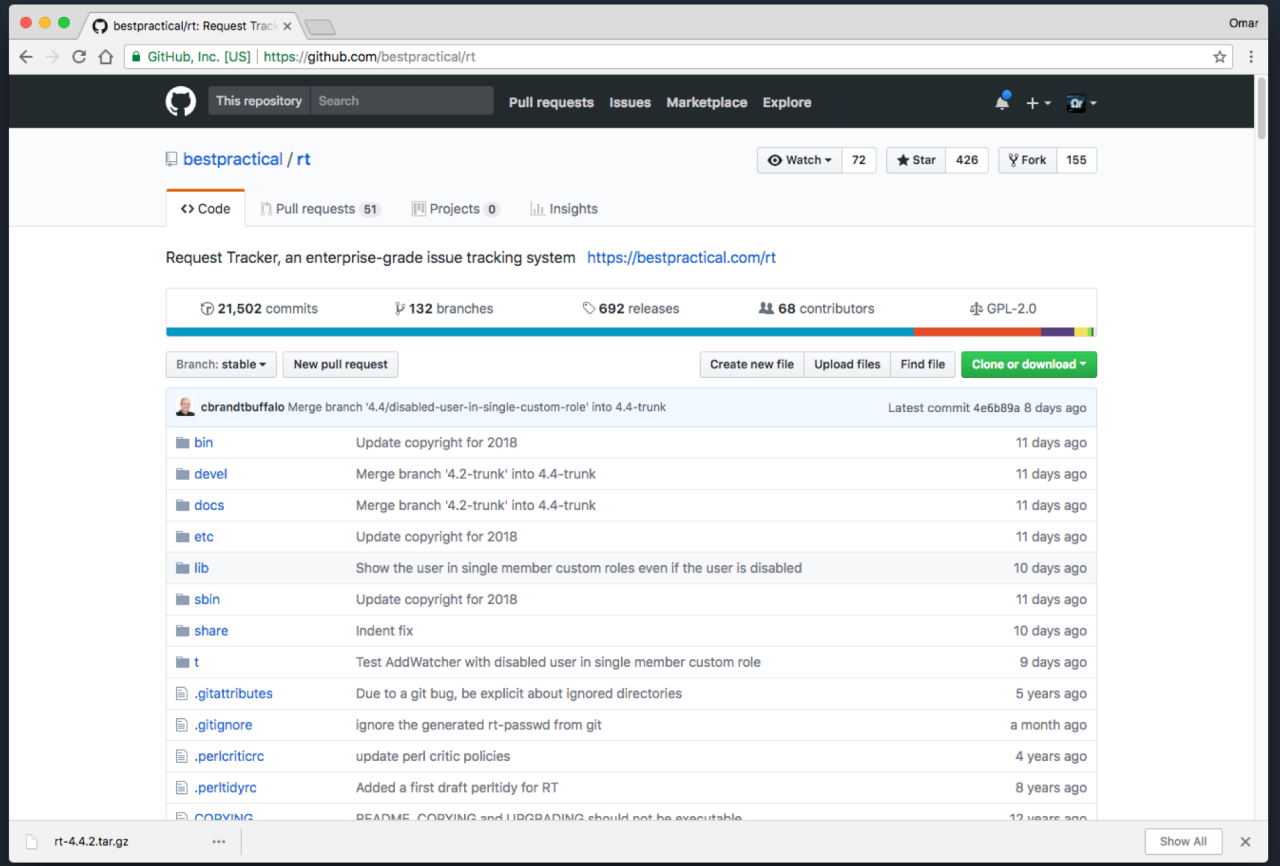
Incident Classification

- 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.

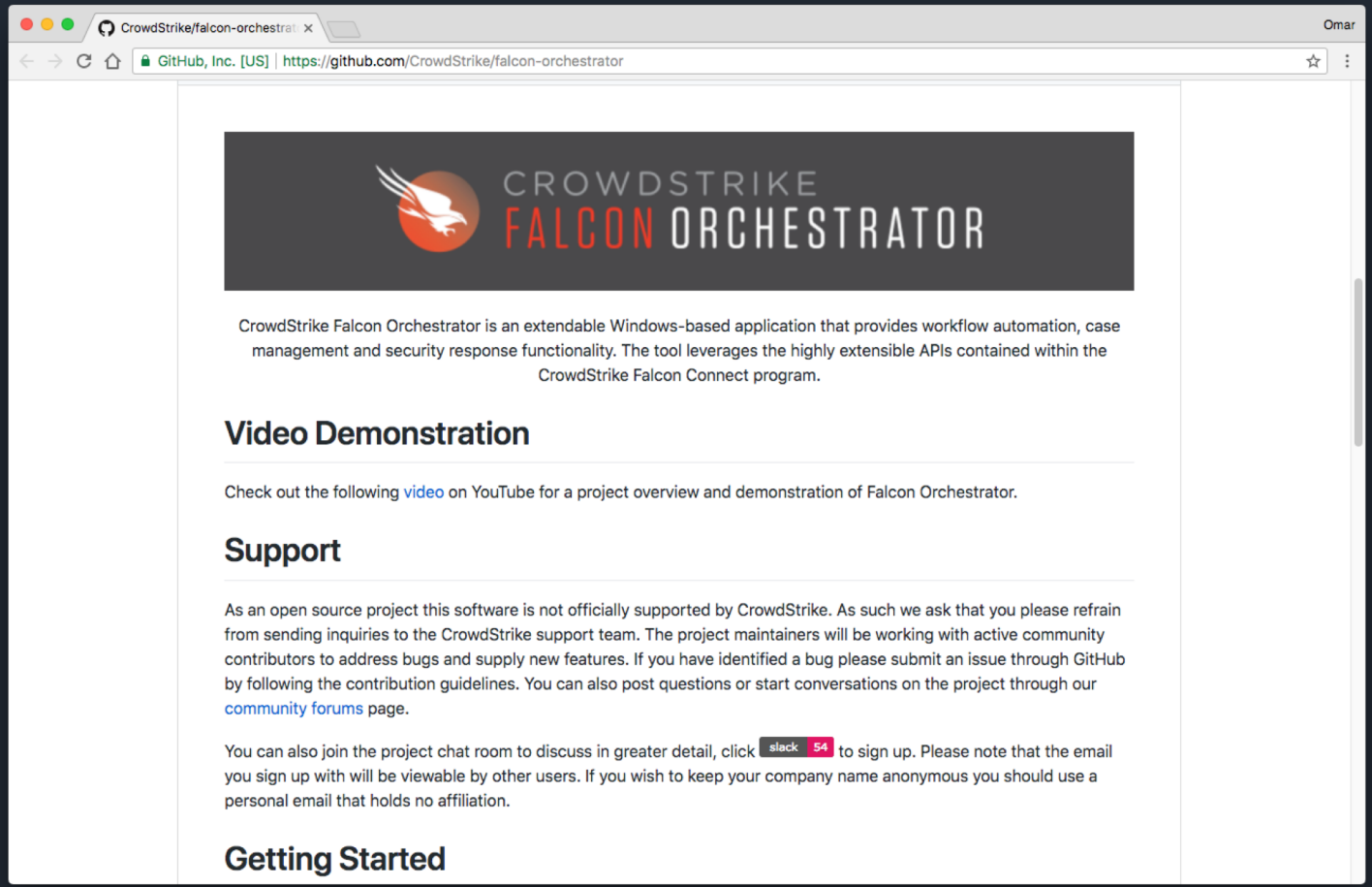
Incident Tracking

CISRT / Incident Tracking Tools

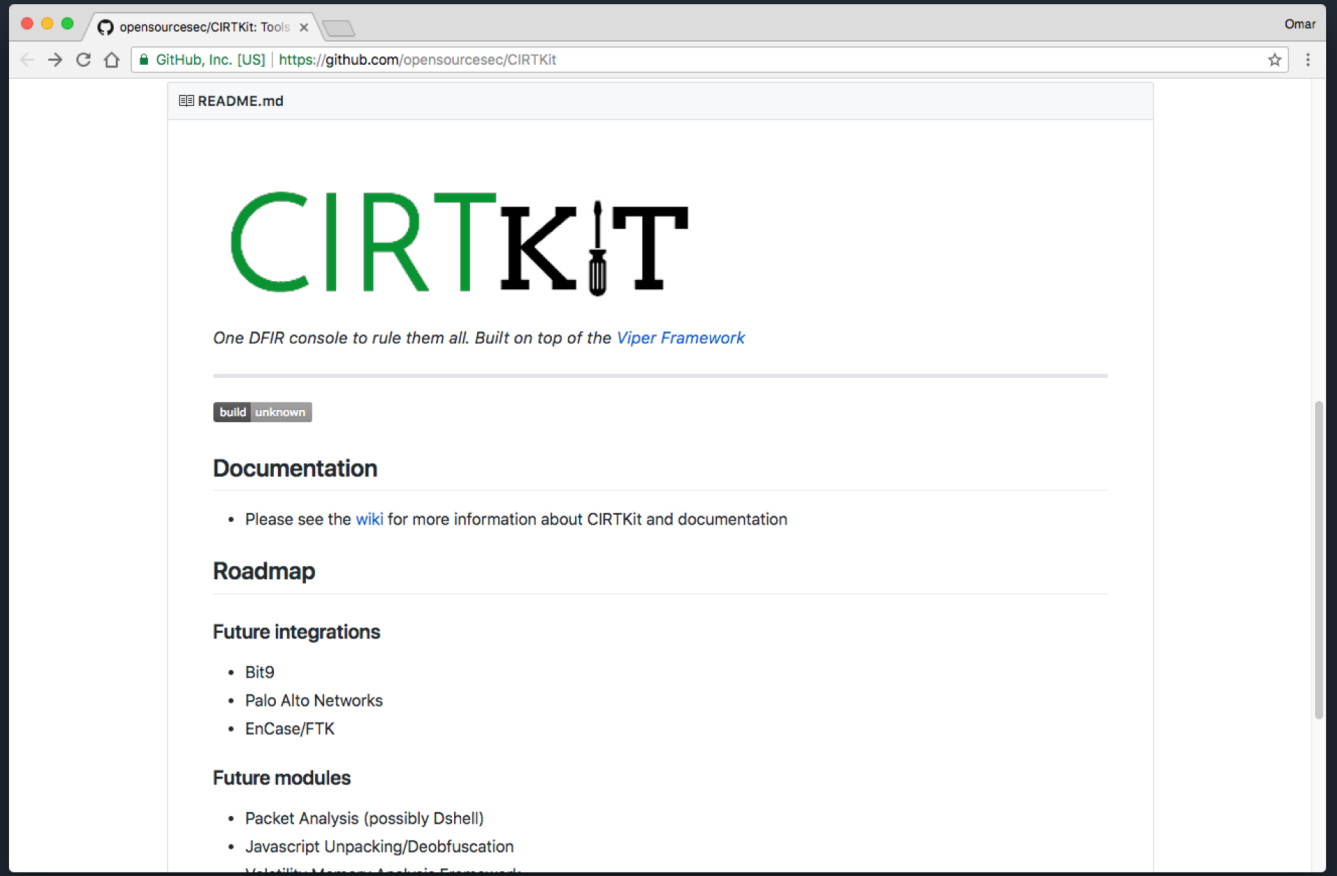
Incident Tracking



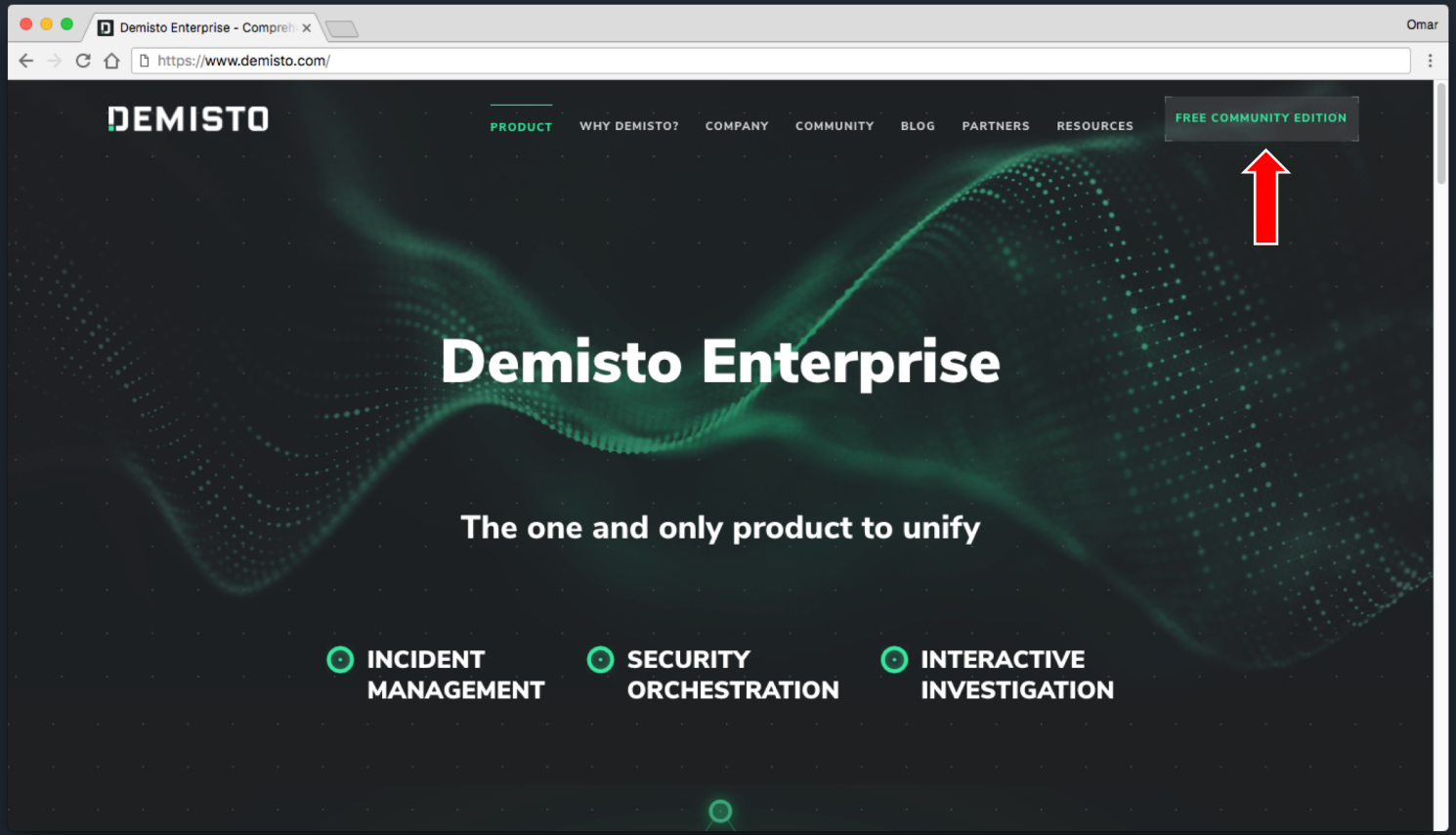
Request Tracker



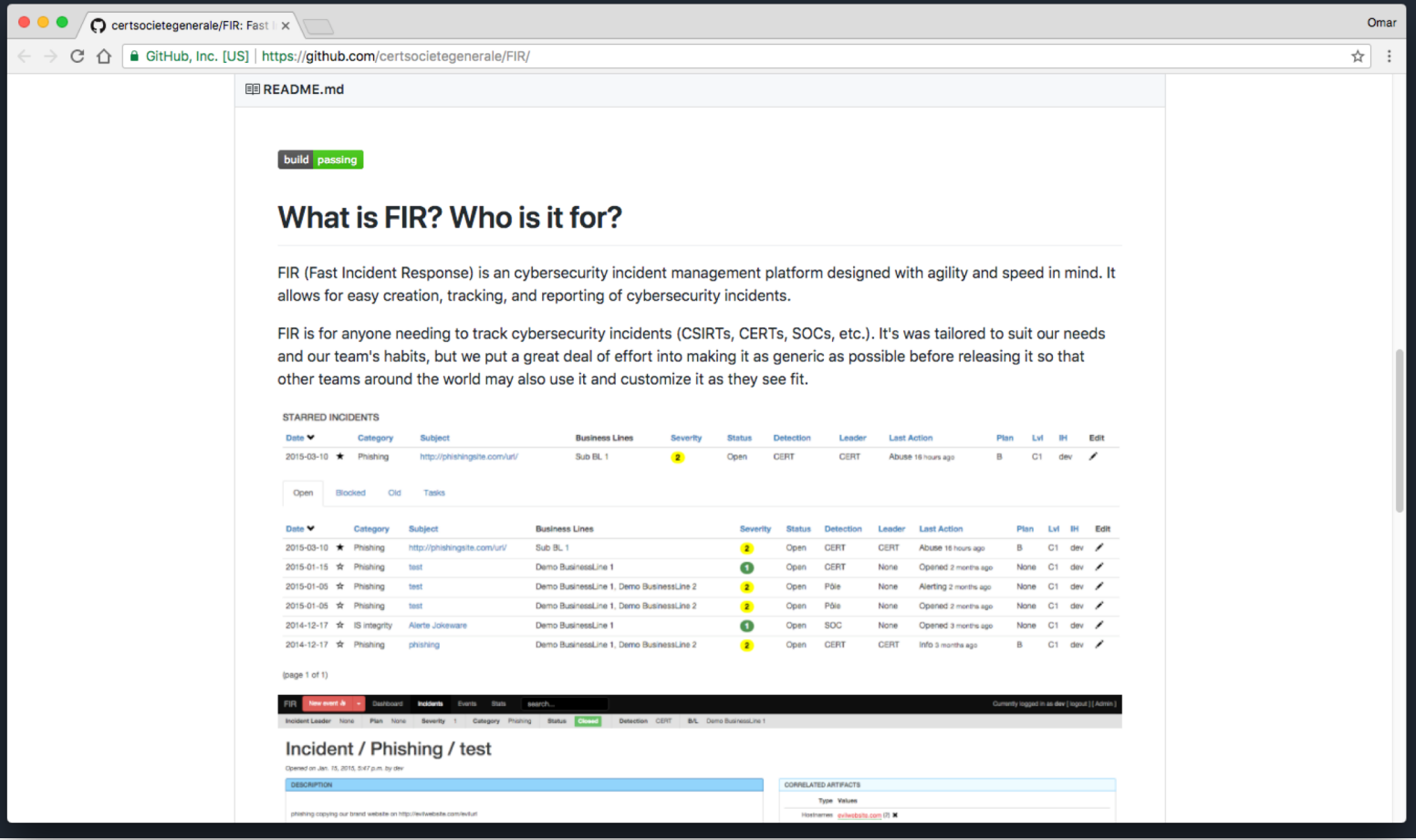
Falcon Orchestrator


opensourcesec/CIRTKit: Tools
Omar
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

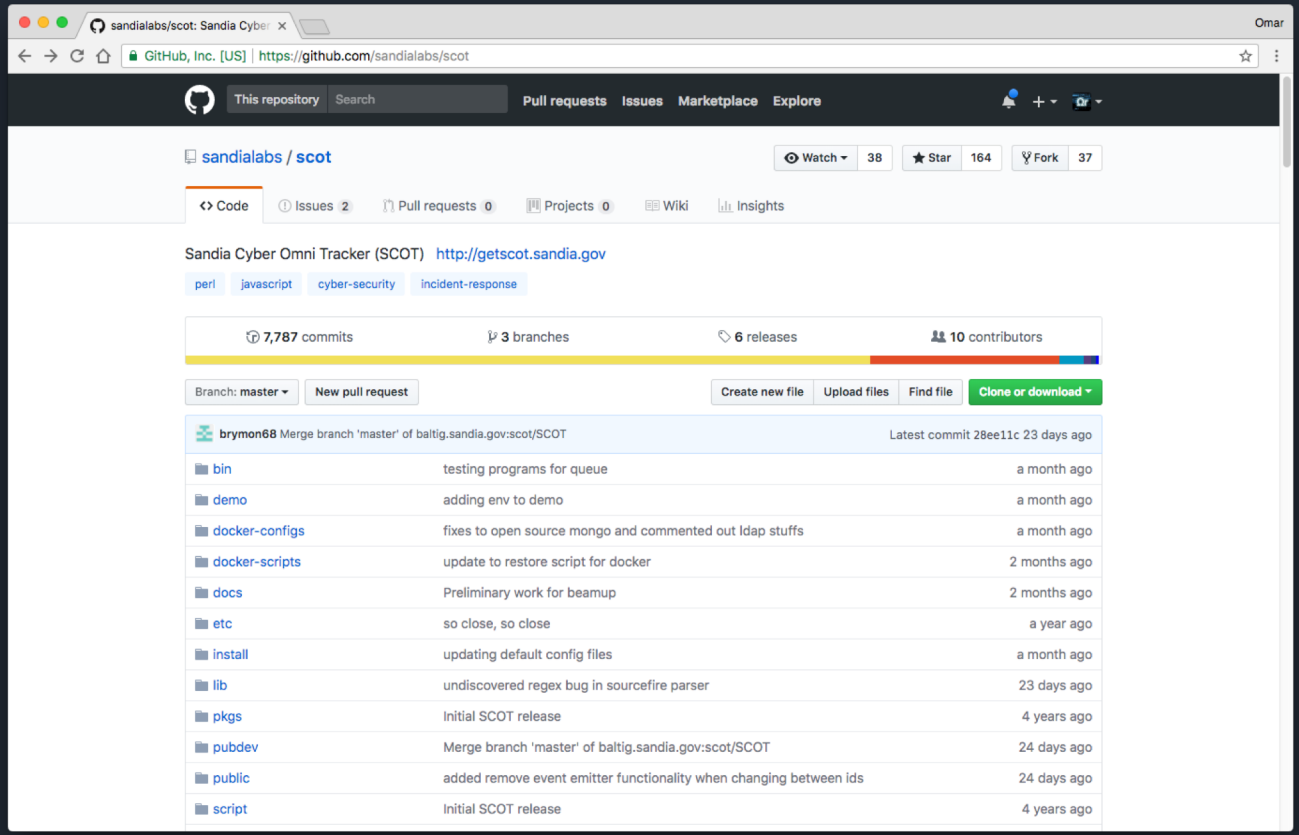
CIRT Kit


Demisto Enterprise - Compreh
Omar
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

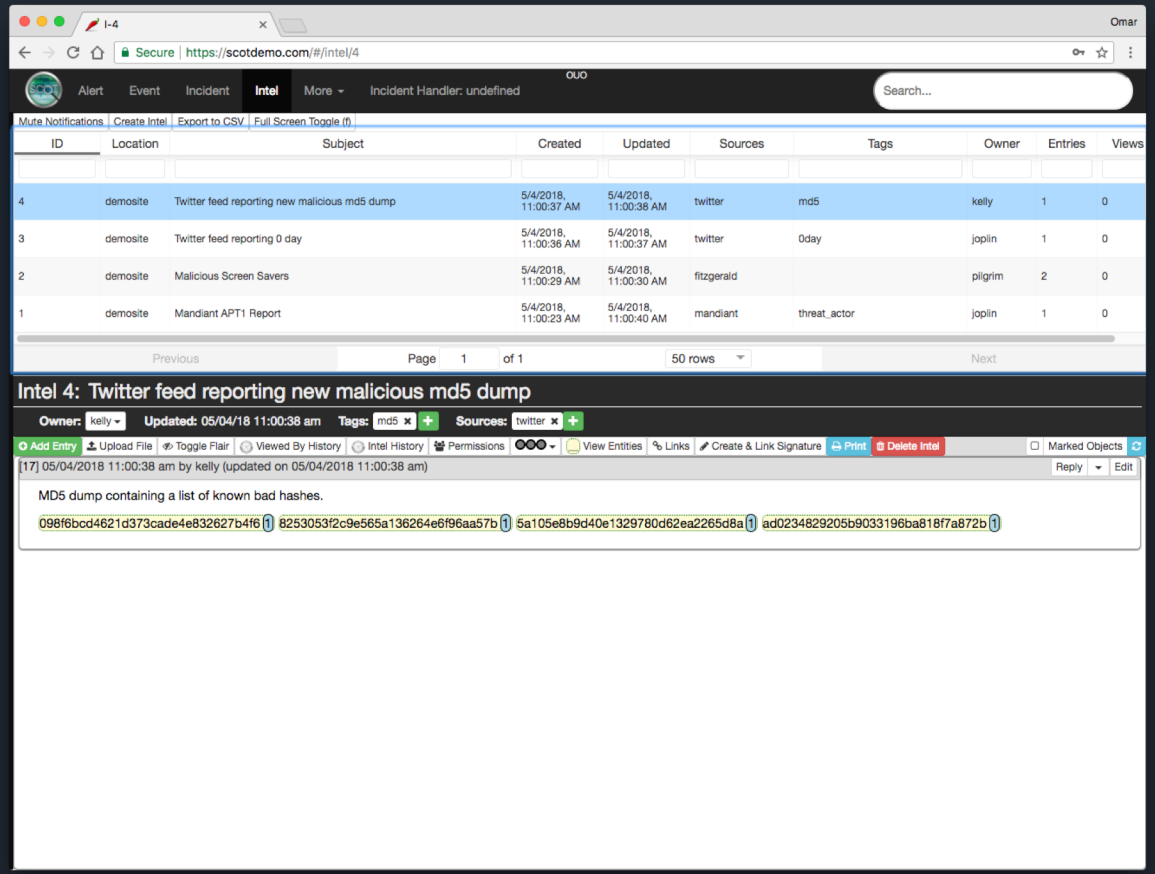
Demistro



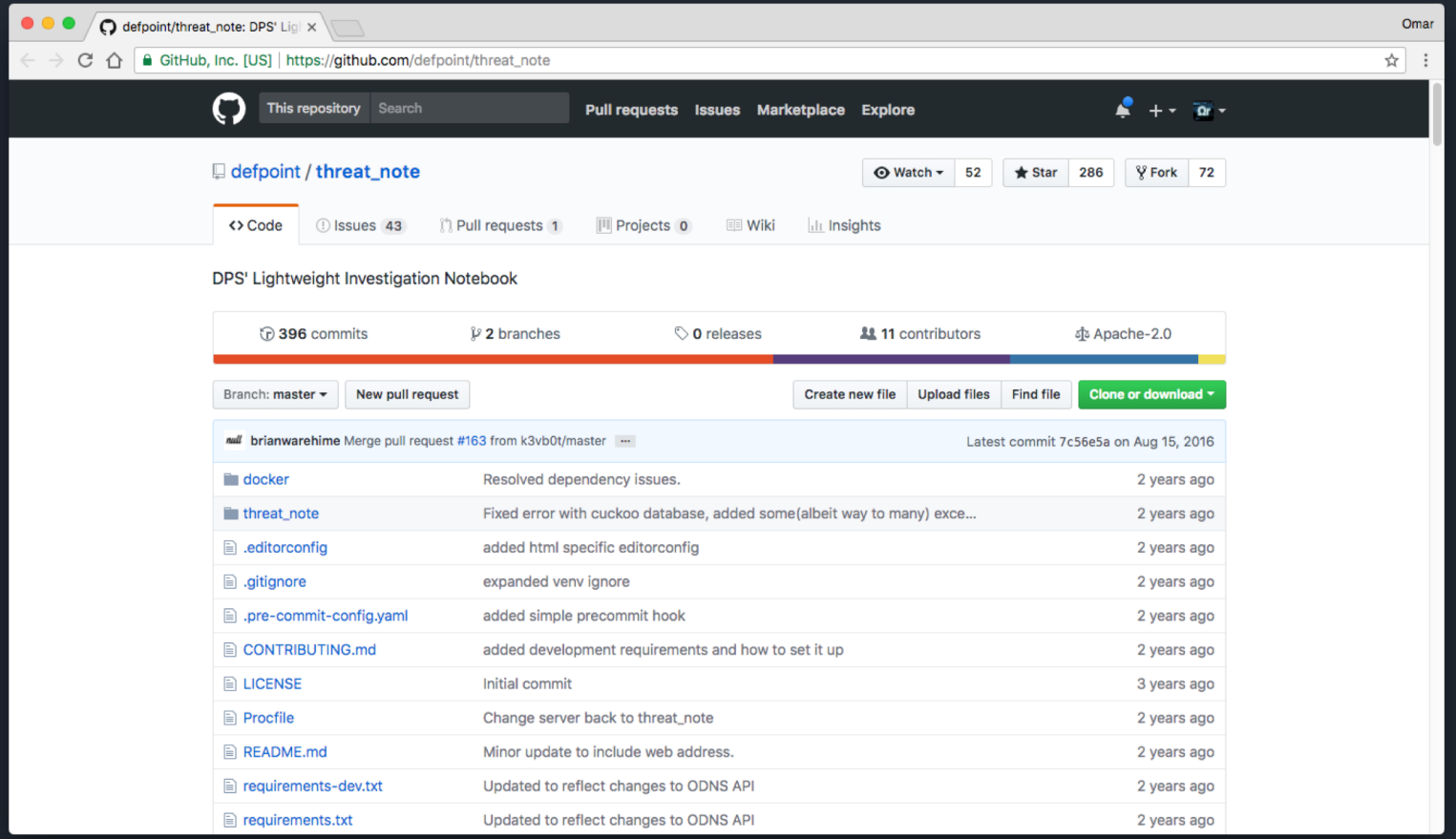
Fast Incident Response (FIR)



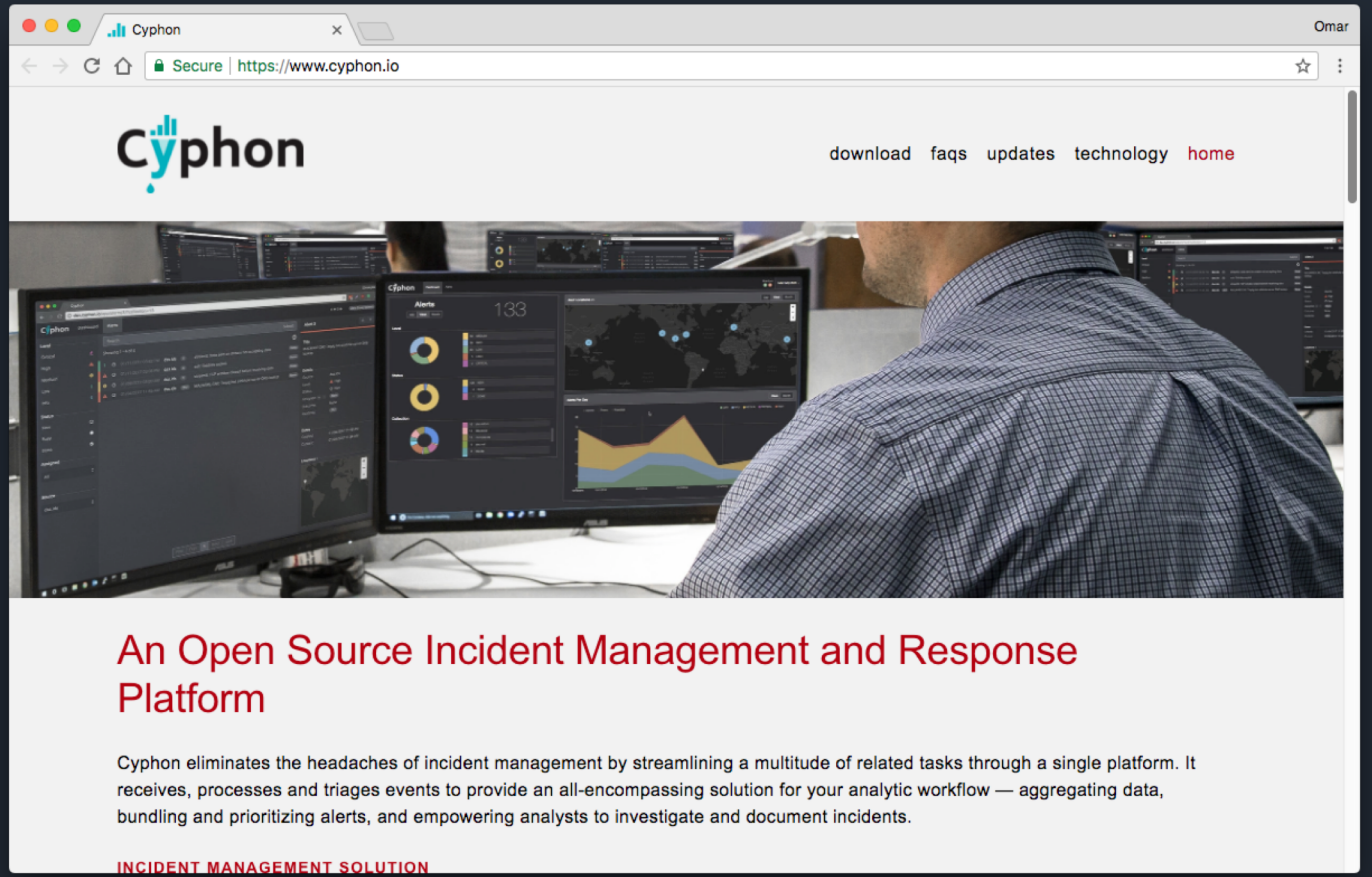
Sandia Cyber Omni Tracker (SCOT)


I-4
Omar
Secure https://scotdemo.com/#/intel/4
Alert Event Incident Intel More Incident Handler: undefined
Search...
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

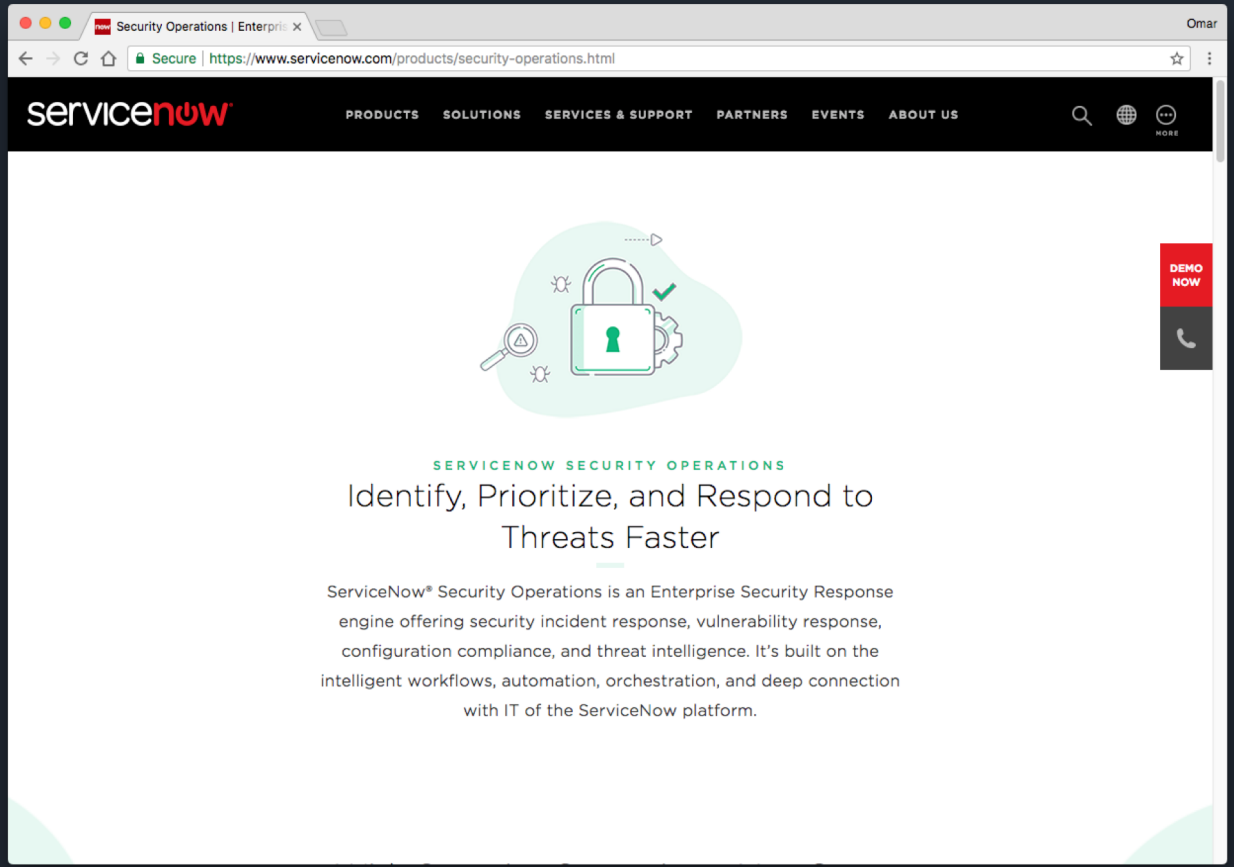
SCOT Demo


defpoint/threat_note: DPS' Lig
Omar
GitHub, Inc. [US] | https://github.com/defpoint/threat_note
This repository
Search
Pull requests
Issues
Marketplace
Explore
defpoint / threat_note
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
brianwarehime Merge pull request #163 from k3vb0t/master
Latest commit 7c56e5a on Aug 15, 2016
docker Resolved dependency issues. 2 years ago
threat_note Fixed error with cuckoo database, added some(albeit way to many) exce... 2 years ago
.editorconfig added html specific editorconfig 2 years ago
.gitignore expanded venv ignore 2 years ago
.pre-commit-config.yaml added simple precommit hook 2 years ago
CONTRIBUTING.md added development requirements and how to set it up 2 years ago
LICENSE Initial commit 3 years ago
Procfile Change server back to threat_note 2 years ago
README.md Minor update to include web address. 2 years ago
requirements-dev.txt Updated to reflect changes to ODNS API 2 years ago
requirements.txt Updated to reflect changes to ODNS API 2 years ago

threat_note


Cyphon
Omar
Secure | https://www.cyphon.io
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



ServiceNOW (commercial)

Incident Response Playbooks

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!

* ownership
* follow-up
* comms

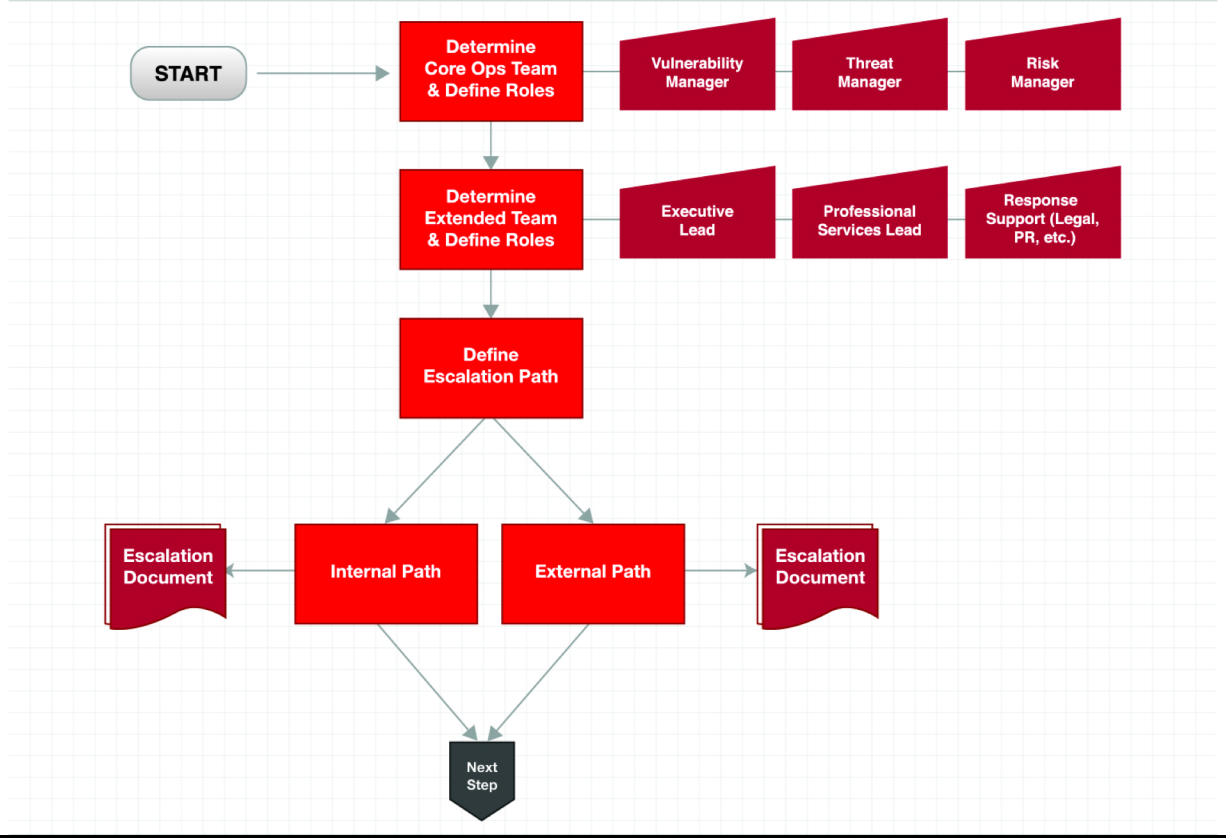
Scheduling

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

Metrics?

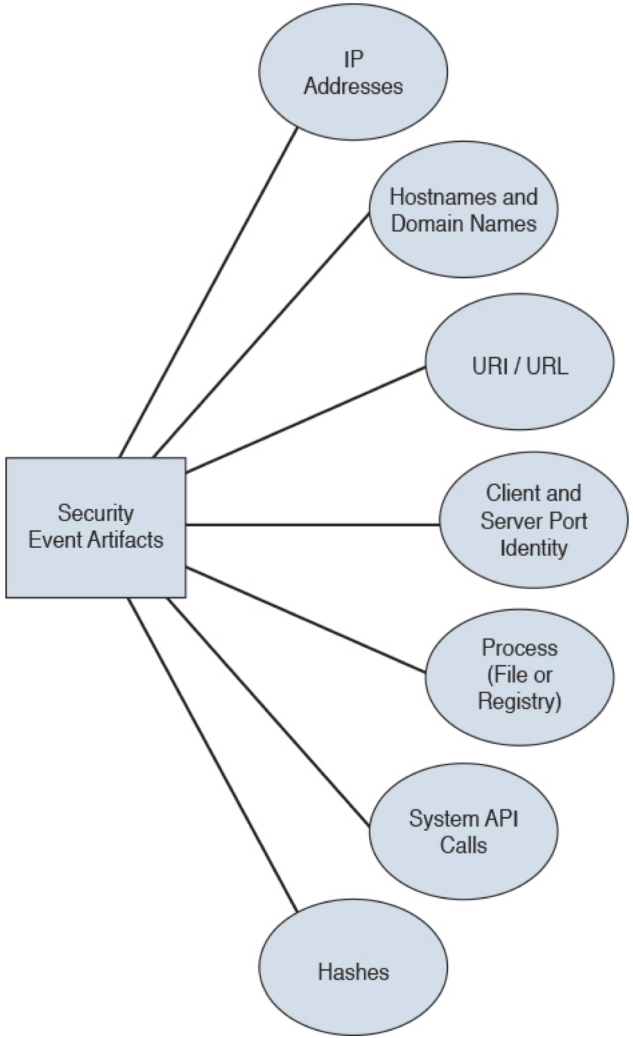
- What to do to avoid duplicate events, tickets, and incidents ?

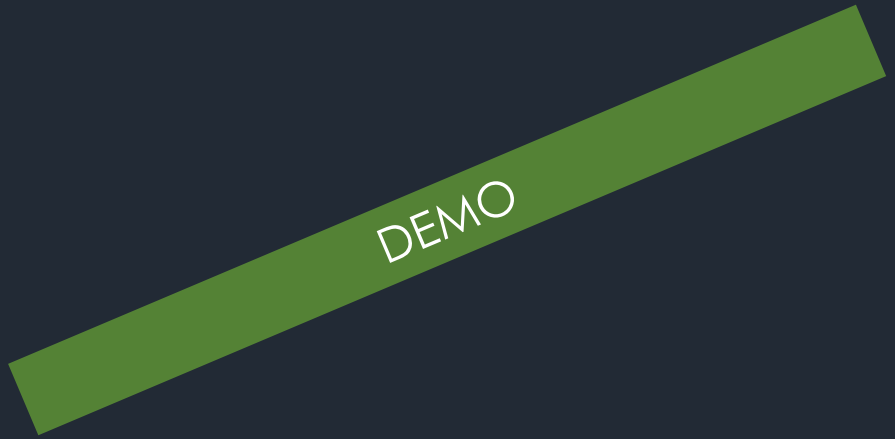
- What mitigating capabilities and supporting policies exist ?



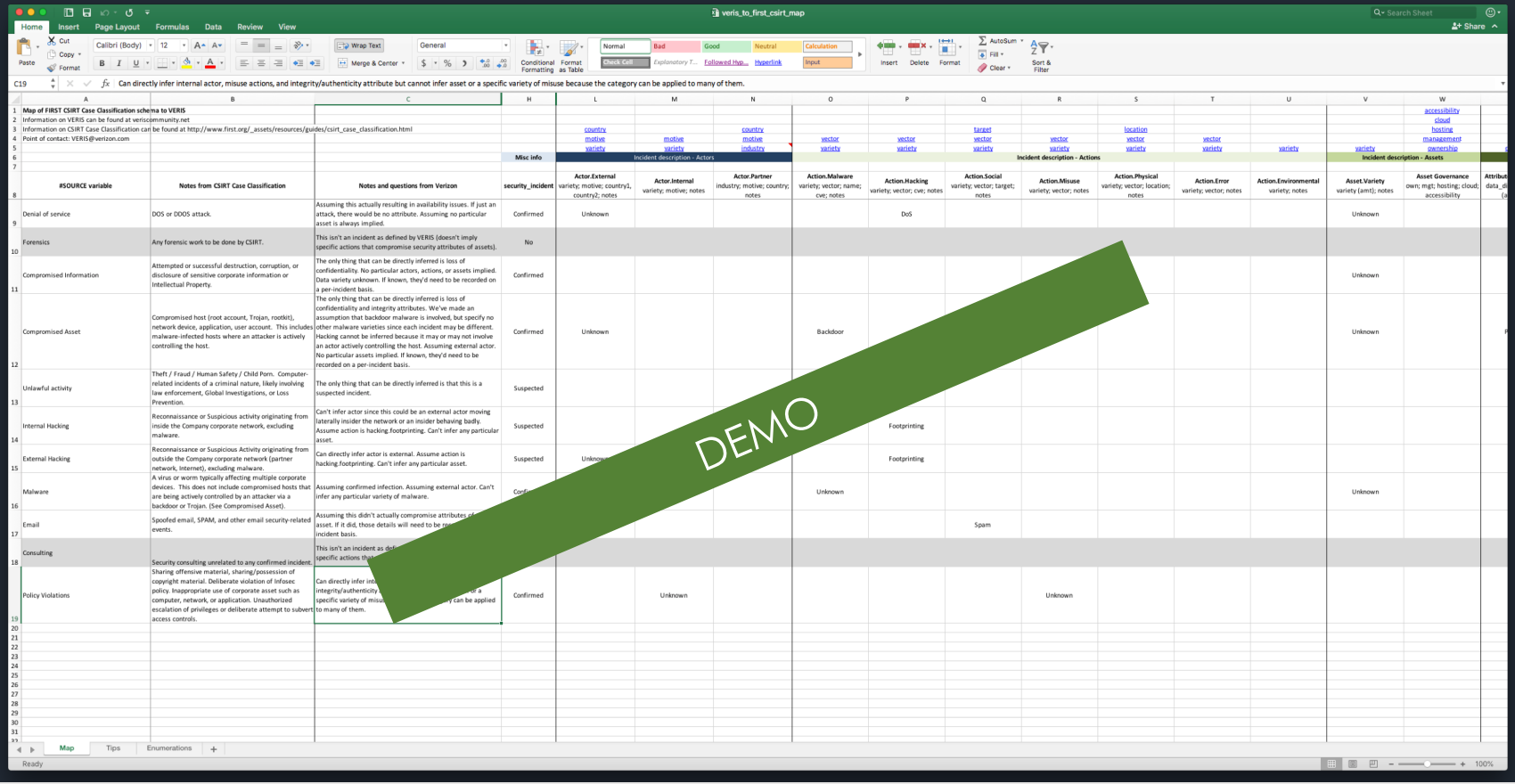
DEMO

https://www.incidentresponse.com/playbooks


IP Addresses
Hostnames and Domain Names
URI / URL
Security Event Artifacts
Client and Server Port Identity
Process (File or Registry)
System API Calls
Hashes

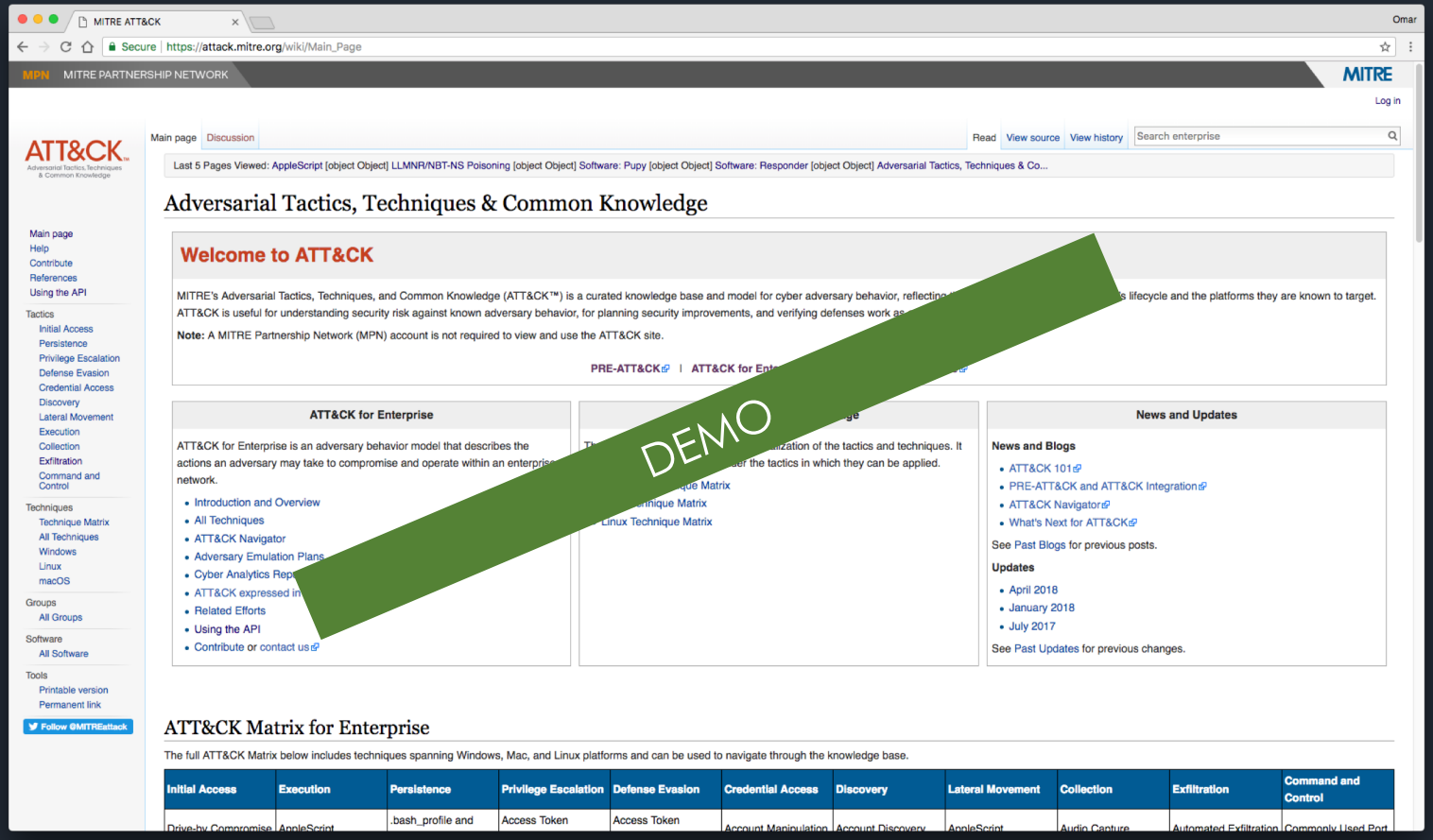


https://incident.veriscommunity.net/s3/example

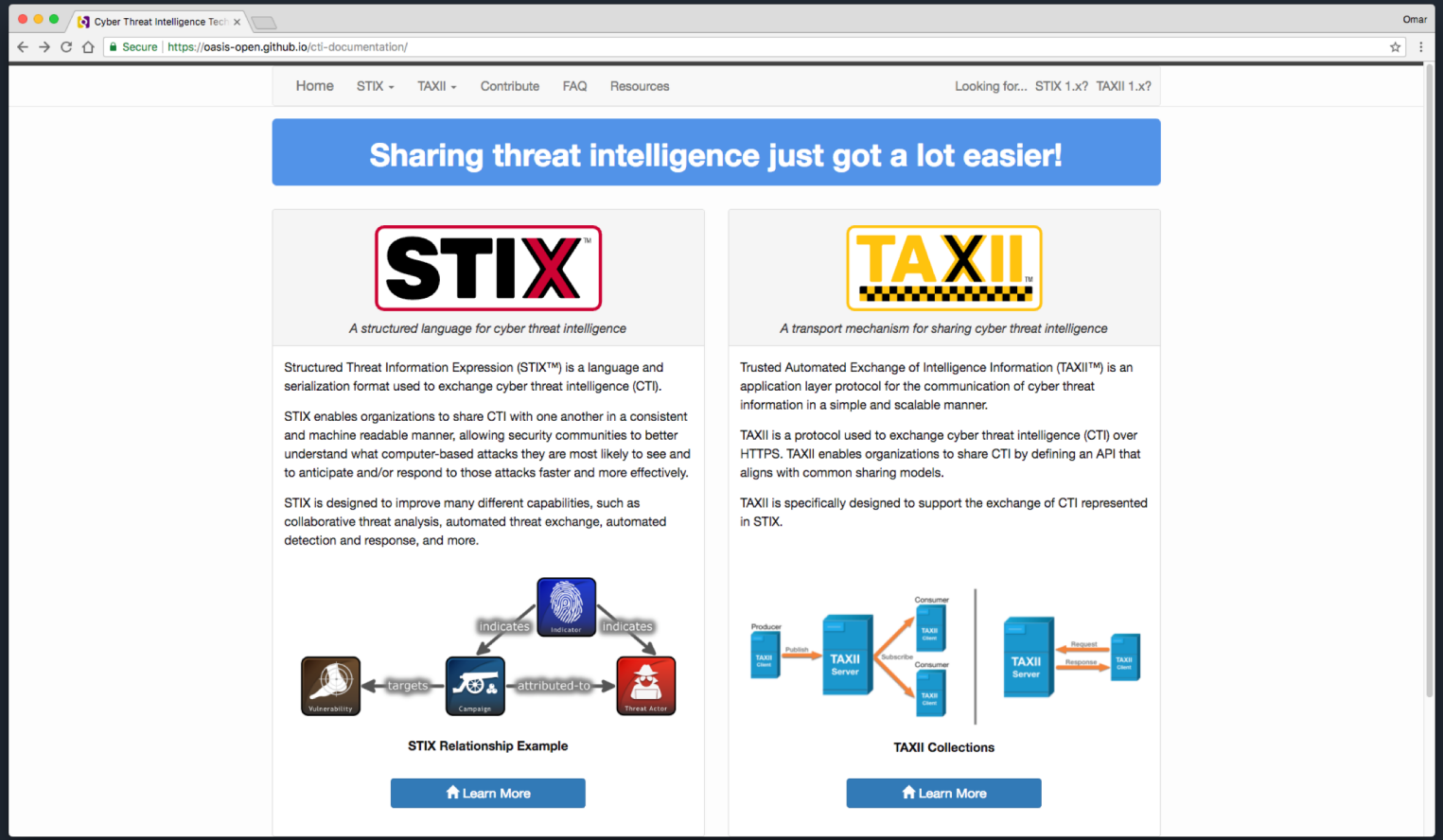


http://veriscommunity.net/veris-mapping.html

FIRST CSIRT Case Categories and VERIS


MITRE ATT&CK
Omar
Secure | https://attack.mitre.org/wiki/Main_Page
MPN MITRE PARTNERSHIP NETWORK
MITRE
Log in
ATT&CK
Adversarial Tactics, Techniques & Common Knowledge
Main page
Discussion
Read
View source
View history
Search enterprise
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...
Adversarial Tactics, Techniques & Common Knowledge
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
lifecycle and the platforms they are known to target.
ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work as
Note: A MITRE Partnership Network (MPN) account is not required to view and use the ATT&CK site.
PRE-ATT&CK | ATT&CK for Ent
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 Rep
ATT&CK expressed in
Related Efforts
Using the API
Contribute or contact us
ization of the tactics and techniques. It
er the tactics in which they can be applied.
que Matrix
hnique Matrix
Linux Technique Matrix
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.
DEMO
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

MITRE – ATT&CK



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

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.

http://h4cker.org/dfir/irt3.html

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

http://h4cker.org/dfir/irt3.html

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 is 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

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.

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

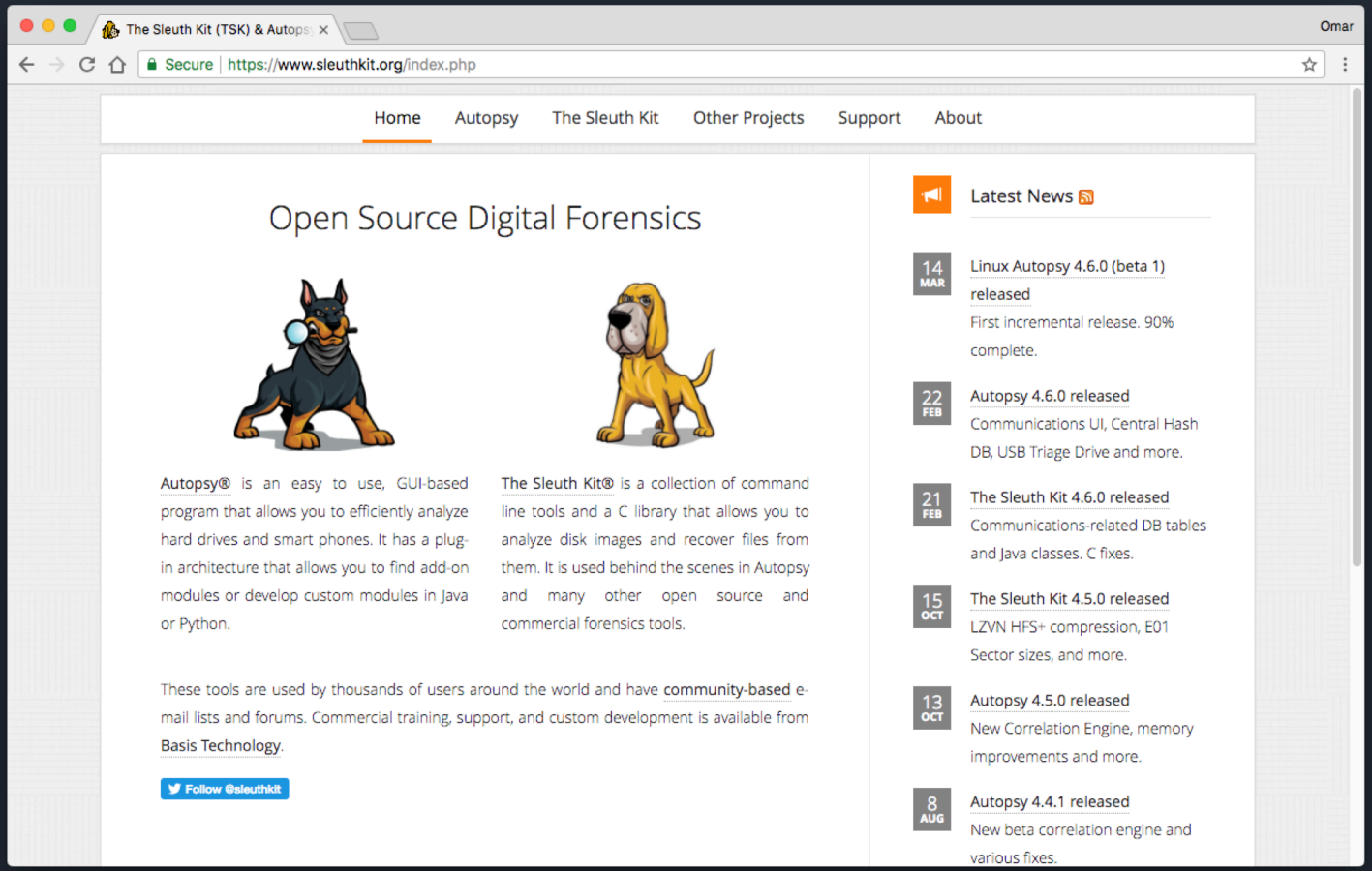
Collecting Evidence from Network Infrastructure Devices

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

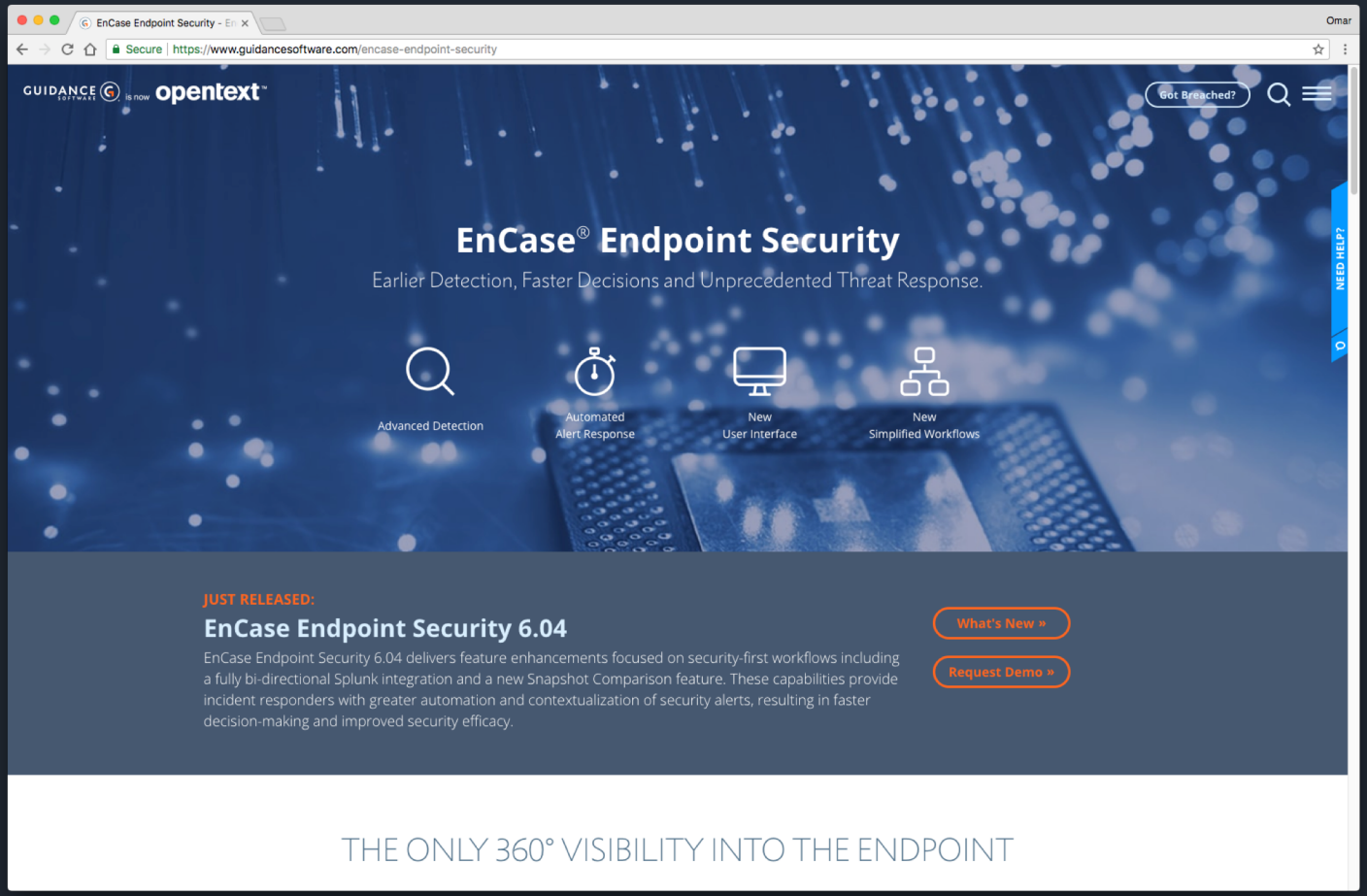
http://h4cker.org/dfir/irt4.html

Digital Forensic Tools

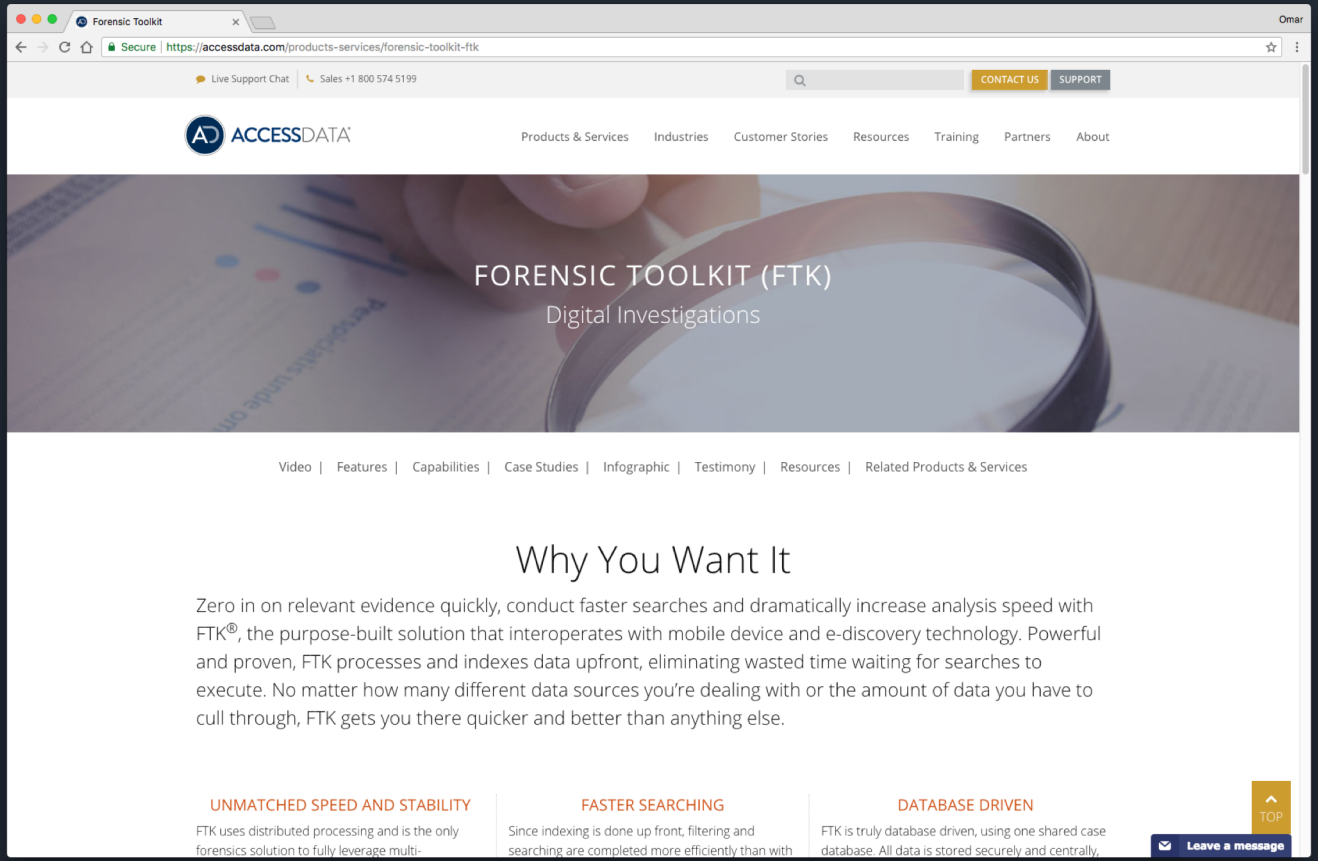
Tools of the Trade



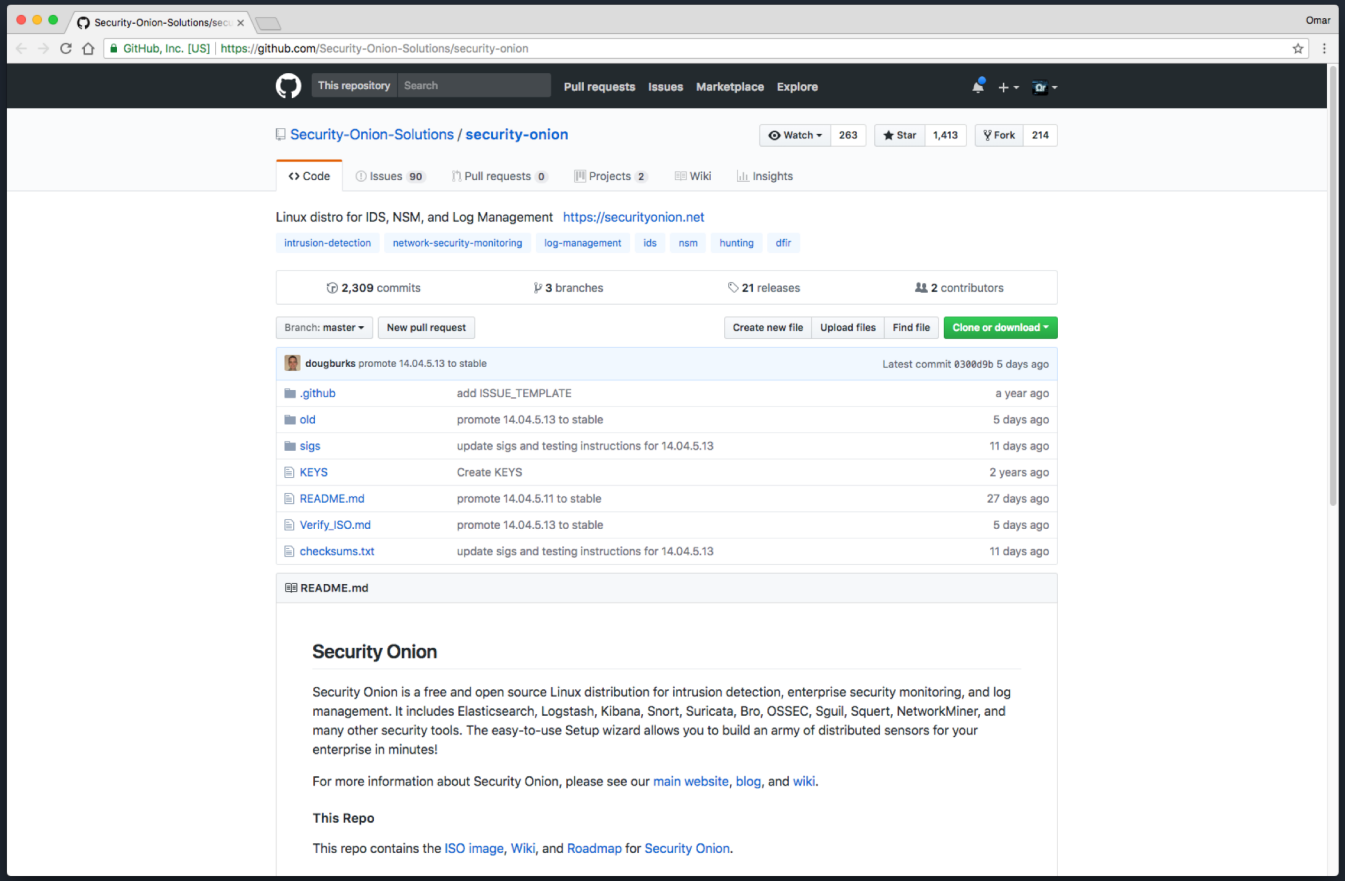
Sleuth Kit & Autopsy


EnCase Endpoint Security - En
Omar
Secure | https://www.guidancesoftware.com/encase-endpoint-security
GUIDANCE SOFTWARE is now opentext™
Got Breached?
EnCase® Endpoint Security
Earlier Detection, Faster Decisions and Unprecedented Threat Response.
Advanced Detection
Automated Alert Response
New User Interface
New Simplified Workflows
NEED HELP?
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

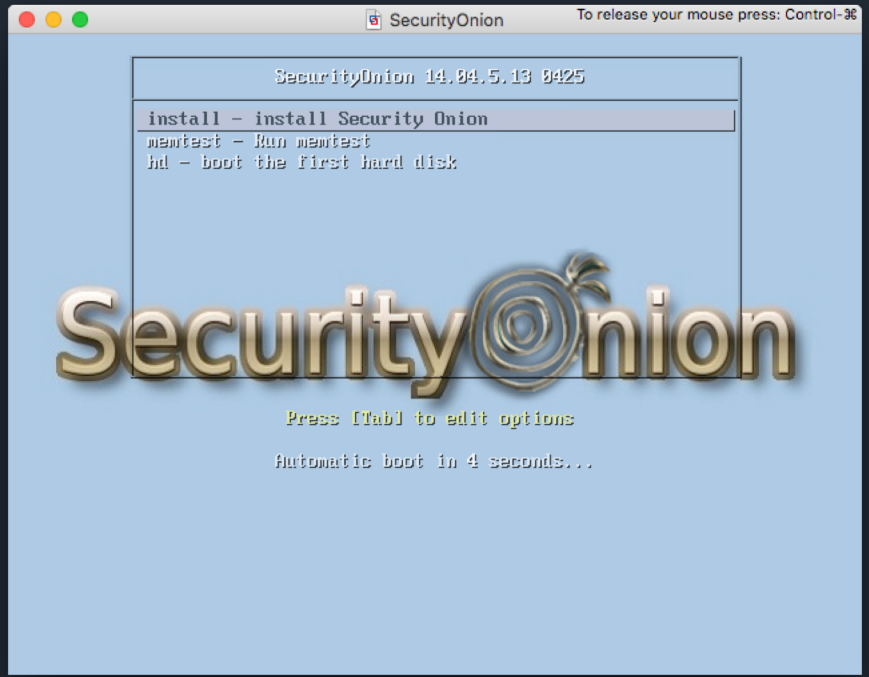
EnCase



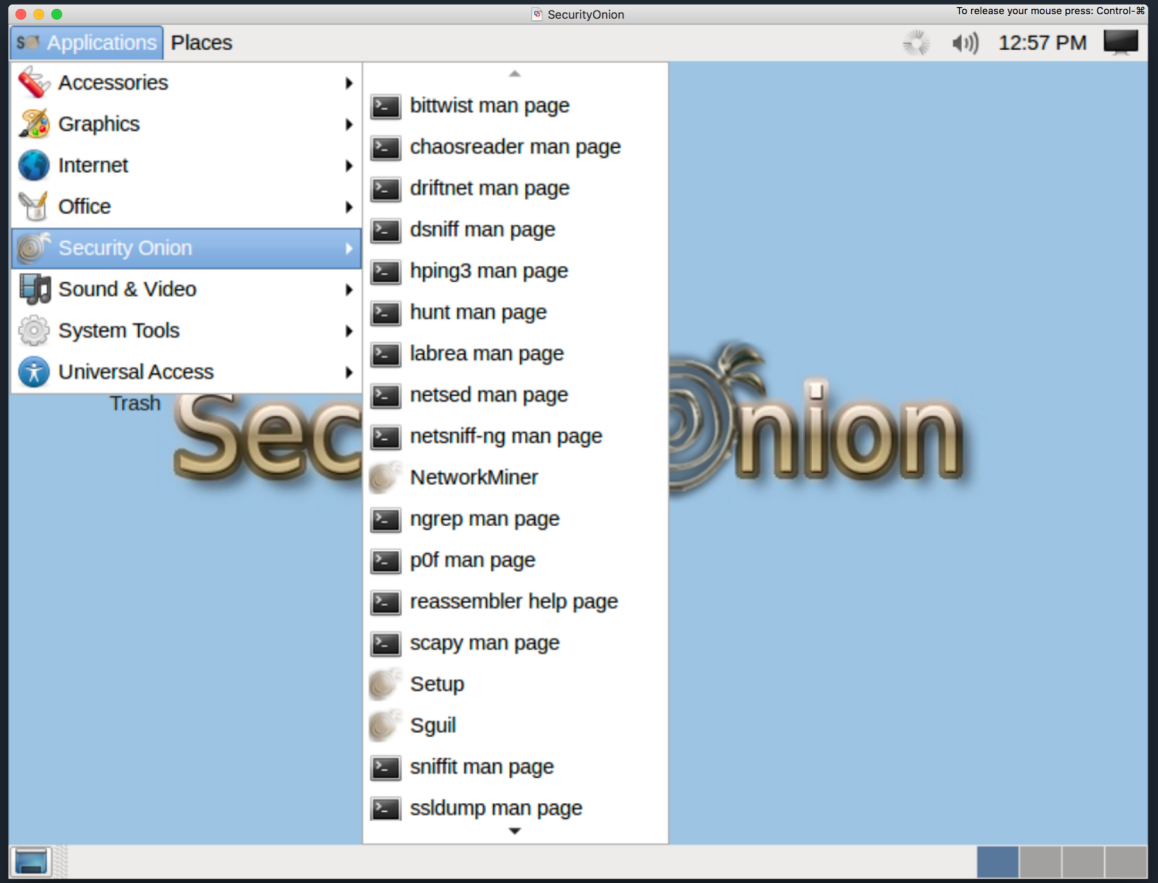
Access Data Forensics Toolkit



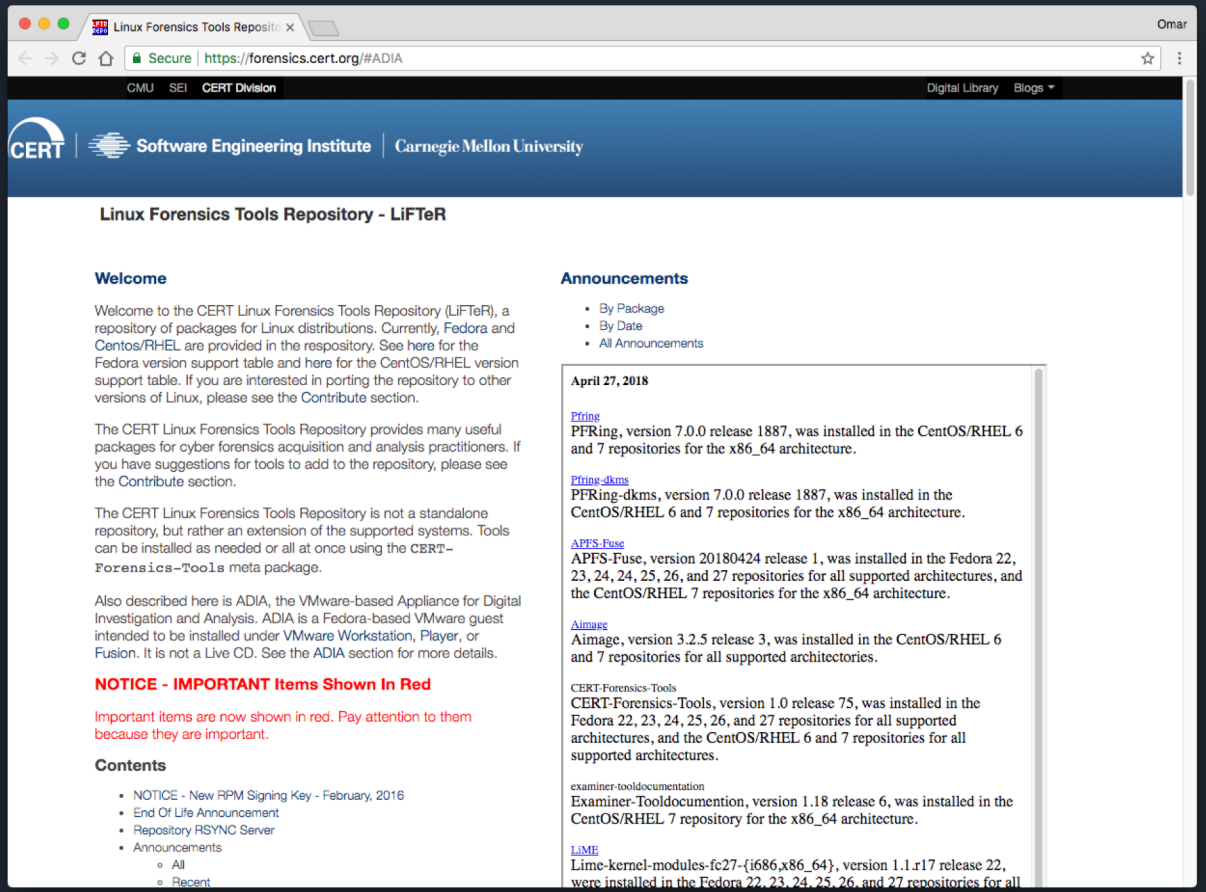
Security Onion



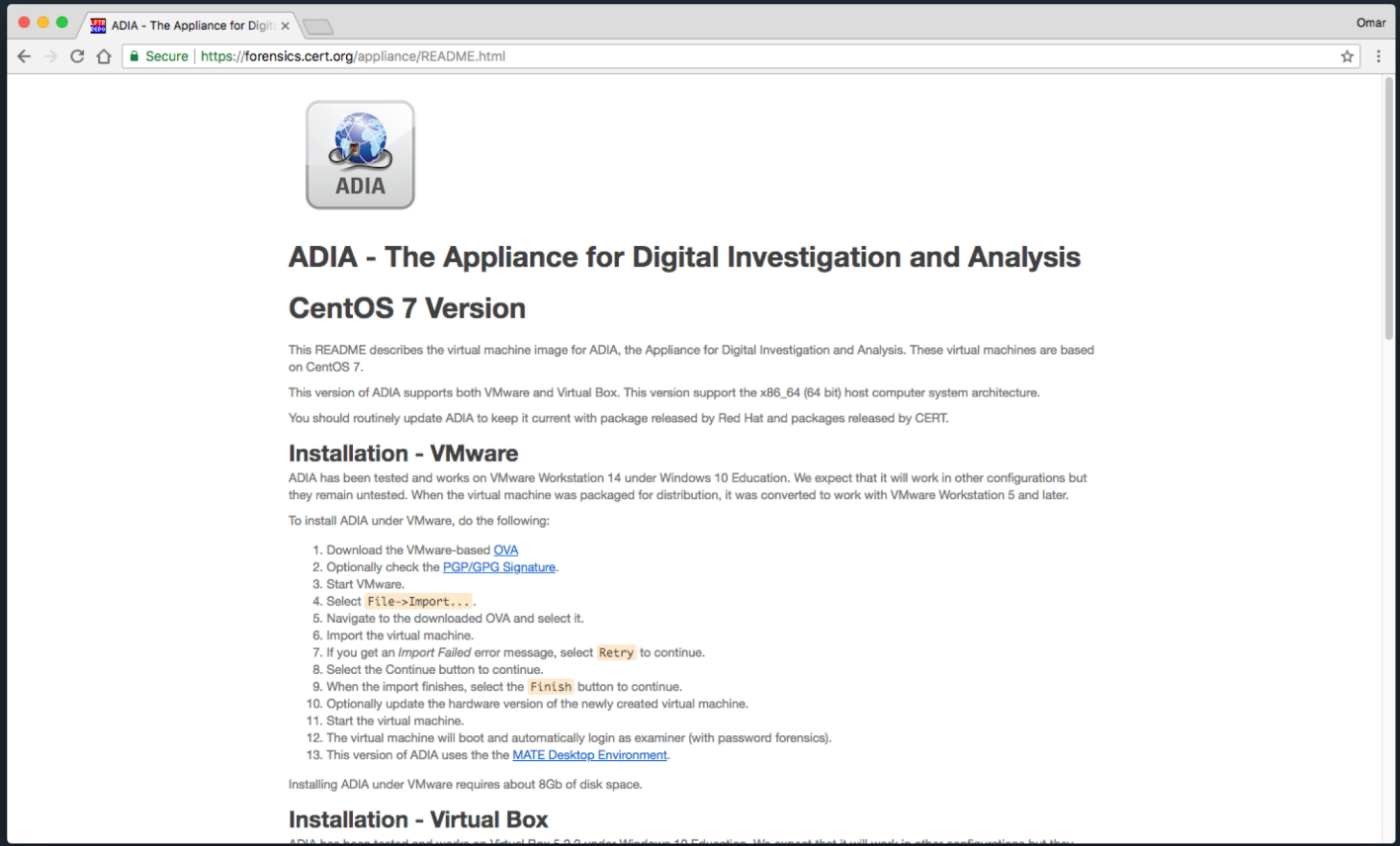
Security Onion



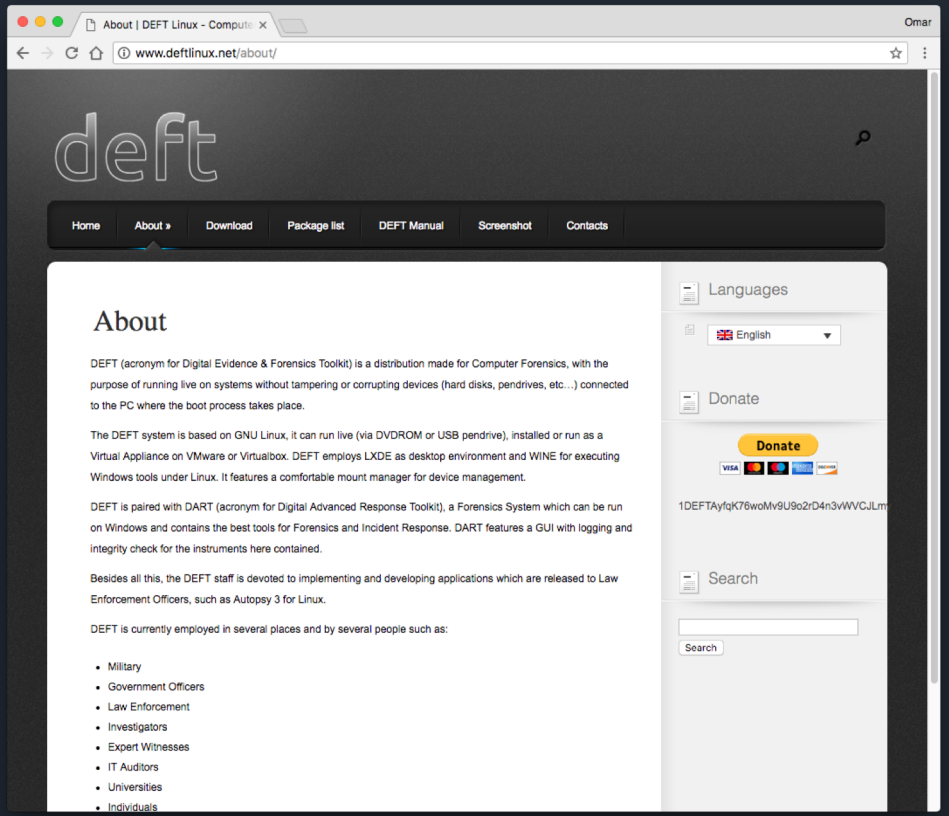
Security Onion


Linux Forensics Tools Reposit
Omar
Secure | https://forensics.cert.org/#ADIA
CMU SEI CERT Division
Digital Library Blogs
CERT | Software Engineering Institute | Carnegie Mellon University
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 respository. 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
PFRing, version 7.0.0 release 1887, was installed in the CentOS/RHEL 6 and 7 repositories for the x86_64 architecture.
Pfring-dkms
PFRing-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, 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 architectories.
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-Tooldocumention, 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

LiFTer


ADIA - The Appliance for Digit
Omar
Secure | https://forensics.cert.org/appliance/README.html
ADIA
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


About | DEFT Linux - Compute
Omar
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
Donate
1DEFTAyfqK76woMv9U9o2rD4n3vWVCJLm
Search
Search

deft

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

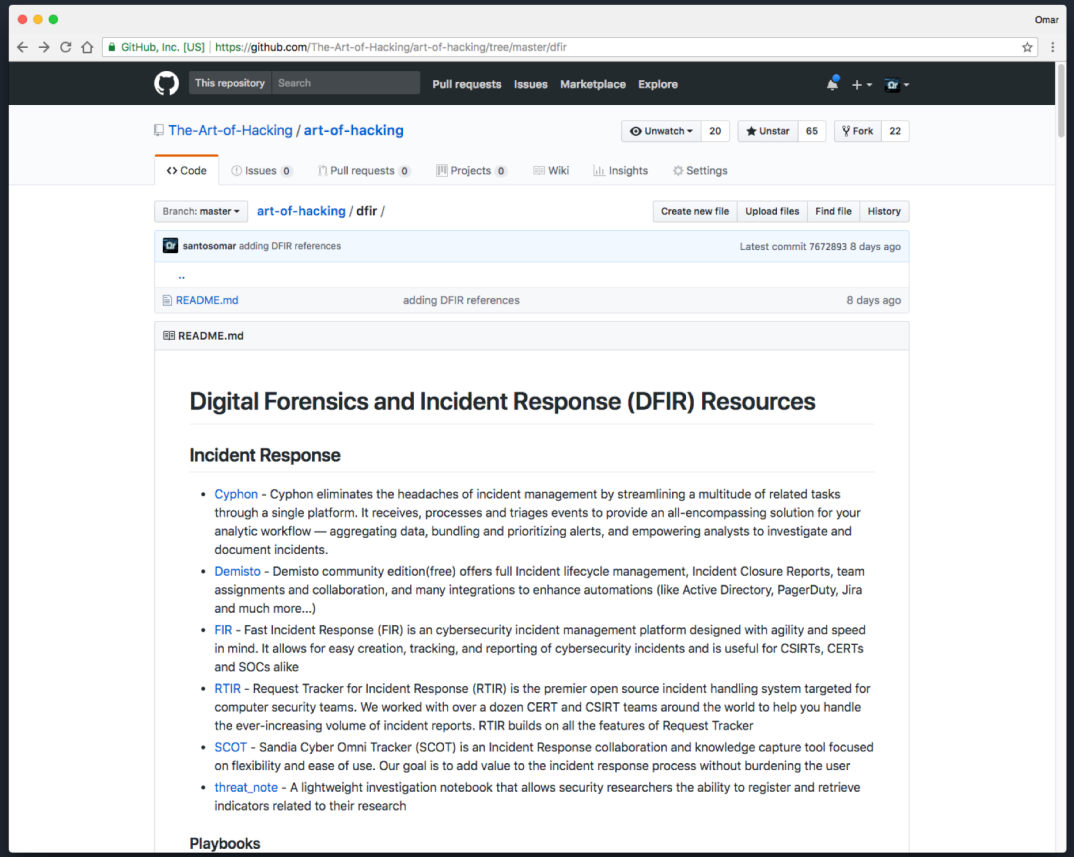
However, there is a shortage of knowledge on how to perform forensics and integrity verification in infrastructure devices (routers, switches, firewalls, etc.)

Infrastructure Devices

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



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

QUESTIONS?

THANK YOU!