Cybersecurity Offensive and Defensive Techniques in 3 Hours

Omar Santos

Follow @santosomar

About // Omar Ωr Santos

https://h4cker.org

@santosomar

https://h4cker.org/discord

/in/santosomar

h4cker.org/github

Omar Santos is an active member of the security community, where he leads several industry-wide initiatives and standard bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants that are dedicated to increasing the security of the critical infrastructure.

Omar is the author of over 20 books and video courses; numerous white papers, articles, and security configuration guidelines and best practices. Omar is a Principal Engineer of Cisco's Product Security Incident Response Team (PSIRT) where he mentors and lead engineers and incident managers during the investigation and resolution of security vulnerabilities.

Omar is often presenting at many cybersecurity conferences and he is the co-lead of the DEF CON Red Team Village (redteamvillage.io). He is also the chair of the OASIS Common Security Vulnerability Framework (CSAF) Technical Committee and the co-chair of the Forum of Incident Response and Security Teams (FIRST) PSIRT Open Source Security Working Group.

Omar has been quoted by numerous media outlets, such as TheRegister, Wired, ZDNet, ThreatPost, CyberScoop, TechCrunch, Fortune Magazine, Ars Technica, and more.

Omar's PGP Key: 0x8e19a9d13af27edc

Learning Path: https://h4cker.org/learning-path

AGENDA

- Understanding Offensive and Defensive Security Methodologies
- So, You Want to Be a Hacker? What are the cybersecurity skills that are necessary in today's environment?
- How to Build, Manage, and Operate Cybersecurity Teams
- Introduction to Threat Hunting
- Effective Threat Intelligence
- Enterprise-wide Ethical Hacking and Continuous Monitoring

POLL 1

What is your level of familiarity with Cybersecurity?

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

POLL 2

Why are you interested in this course?

1. Just curious and want to learn more about Cybersecurity Red/Blue Teams.
2. I am preparing for a cybersecurity certification.
3. I am part of a Red Team.
4. I am part of a Blue Team.

DISCLAIMER | WARNING

The information provided on this training is **for educational purposes only**. The **author**, O'Reilly, or any other entity **is in no way responsible for any misuse of the information**.

Some of the tools and technologies that you will learn in this training class may be illegal depending on where you reside. Please check with your local laws.

Please practice and use all the tools that are shown in this training in a lab that is not connected to the Internet or any other network.

Understanding Offensive and Defensive Security Methodologies

What is a Red Team?

An offensive security team that will perform an organizational assessment beyond a traditional penetration testing engagement.

A red team can comprised of full-time employees of an organization or it can be contracted (outsourced).

Additional Reference: http://h4cker.org/rb/1

What is a Blue Team?

A dedicated defensive security team (or teams) that will monitor and defend the organization against cybersecurity incidents.

A blue team can also be comprised of full-time employees (often different teams) of an organization or it can be contracted (outsourced to a managed security service provider (MSSP)).

Additional Reference: http://h4cker.org/rb/1

Why Red Teaming?

Adversarial testing process (mimicking a real-life threat actor).

Red teams focus on organizational assessments vs. testing a specific target (depending on the organization's objective).

Red teams can also target humans and use social engineering.

Red teams often create custom exploits for specific vulnerable systems.

Additional Reference: http://h4cker.org/rb/1

Incorporate Business Processes

Red Teams often incorporate business processes such as:

- Evaluating new vendors and their products get incorporated into the corporation
- Evaluating how new employees get onboarded.

Additional Reference: http://h4cker.org/rb/1

Tradecraft:

"…within the intelligence community, refers to the techniques, methods and technologies used in modern espionage (spying) and generally, as part of the activity of intelligence. This includes general topics or techniques (dead drops, for example), or the specific techniques of a nation or organization".

https://en.wikipedia.org/wiki/Tradecraft

Understanding the Red Team Environment

What is the goal of having the red team?

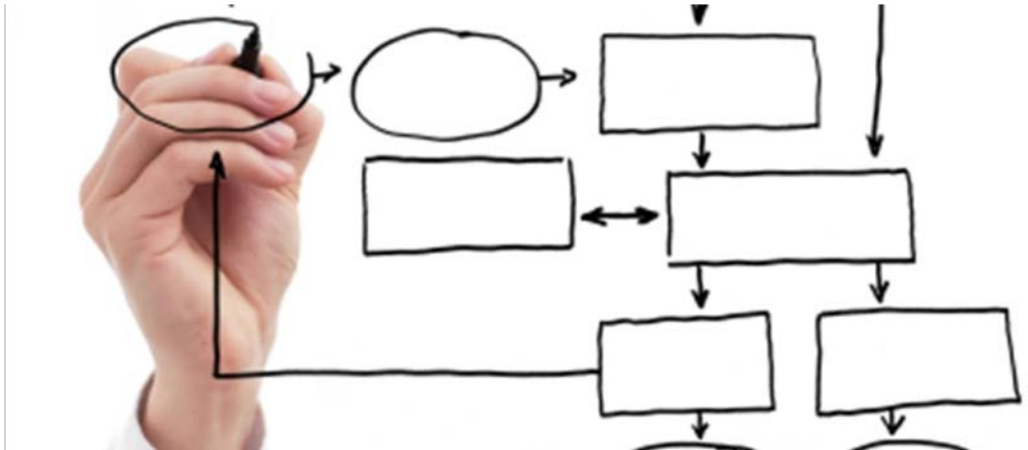
Who do they report to?

How is it structured?

Additional Reference and Video: http://h4cker.org/rb/2

Hacking is a lot more than cool tools…

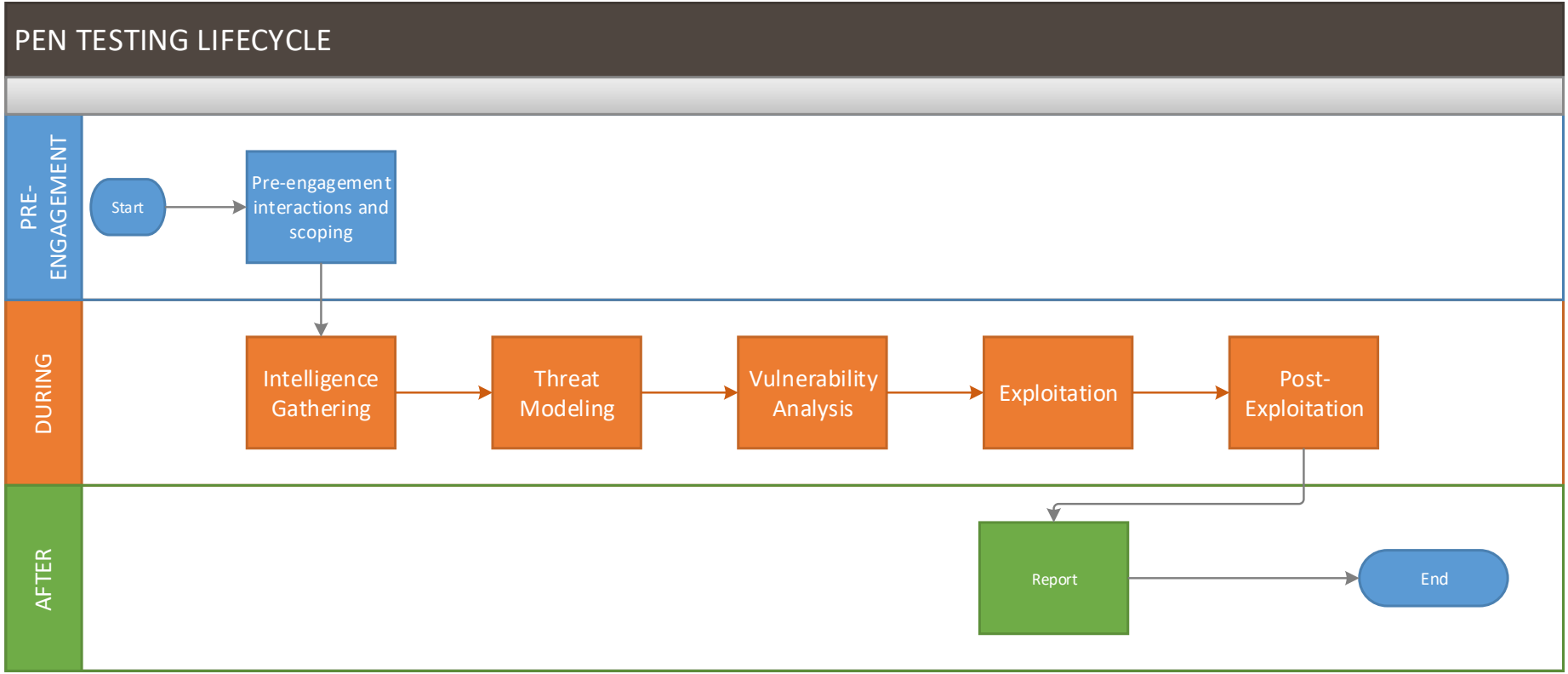
- Methodologies
- Research
- Think like an attacker
- Combine social engineering with technical capabilities



Are Red Team Methodologies the same as traditional penetration testing?

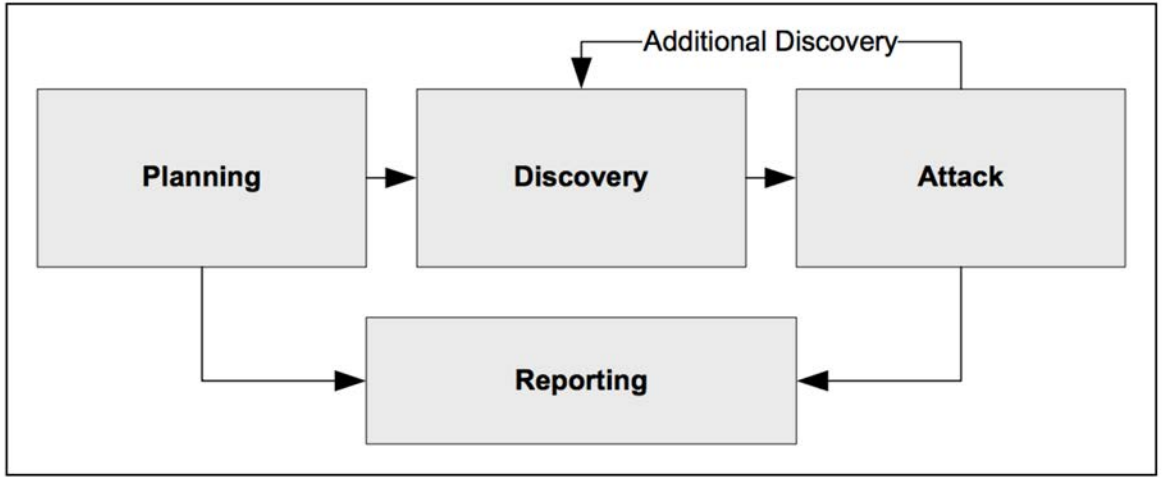
PEN TESTING METHODOLOGIES

- Penetration Testing Execution Standard
  http://www.pentest-standard.org
- OWASP Testing Guide
  https://www.owasp.org/index.php/OWASP_Testing_Project
- NIST 800-115: Technical Guide to Information Security Testing and Assessment
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
- Open Source Security Testing Methodology Manual (OSSTMM)
  http://www.isecom.org/research/



Aligned with: http://www.pentest-standard.org

NIST 800-115



http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Scope in Traditional Penetration Testing vs. Red Teams Engagements

Additional Reference and Video: http://h4cker.org/rb/2

Social Engineering and How to Target Employees

Additional Reference and Video: http://h4cker.org/rb/3

Internal and External Recon

Internal and external recon in red teams include the elements of passive and active recon in traditional pen testing; however, it also entails additional enterprise-wide methodologies.

For example, a red team member could already have access to internal email archives, forums, bug databases, code repositories, etc.

Additional Reference and Video: http://h4cker.org/rb/2

Reports are different…

Additional Reference and Video: http://h4cker.org/rb/2

Persistent Access: For How Long?

Additional Reference and Video: http://h4cker.org/rb/5

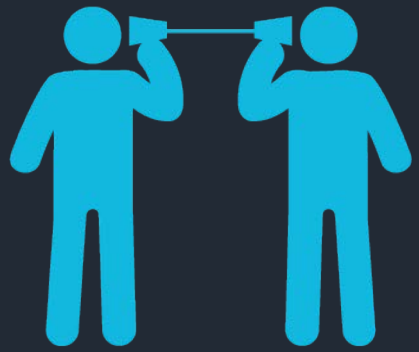
The Hybrid Approach: Purple Teams

The concept of Purple Teams

https://h4cker.org/references/ts-whitepaper.pdf

Regardless of the terminology or what is being used, the Purple Team concept can be applied to each of these based on the level of maturity of the organization.

https://h4cker.org/references/ts-whitepaper.pdf



Communication Among All Cybersecurity Teams

Additional Reference and Video: http://h4cker.org/rb/2

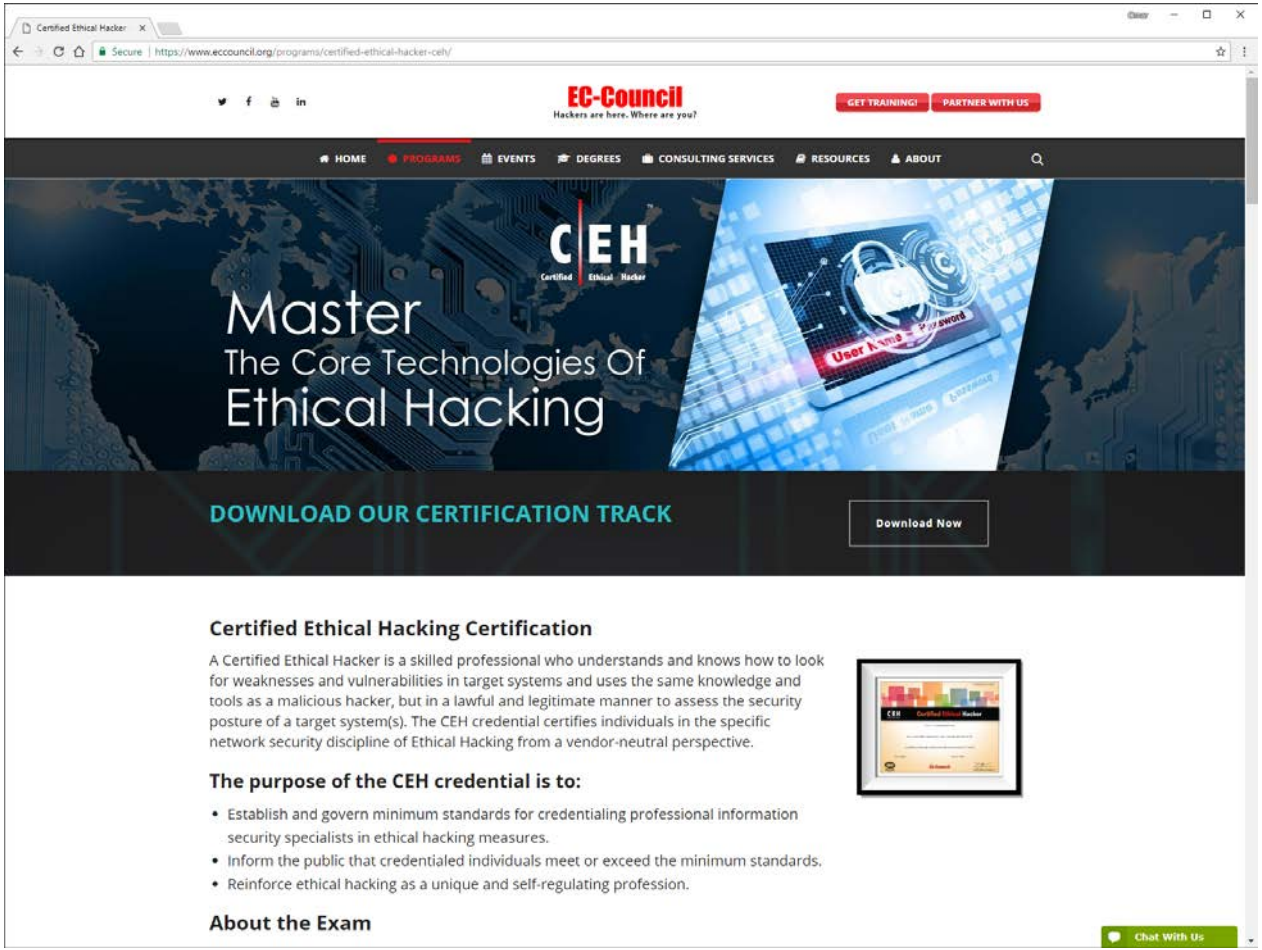
So, You Want to Be a Hacker? What are the cybersecurity skills that are necessary in today's environment?

POLL 3

How are you planning to continue learning and enhancing your cybersecurity skills?

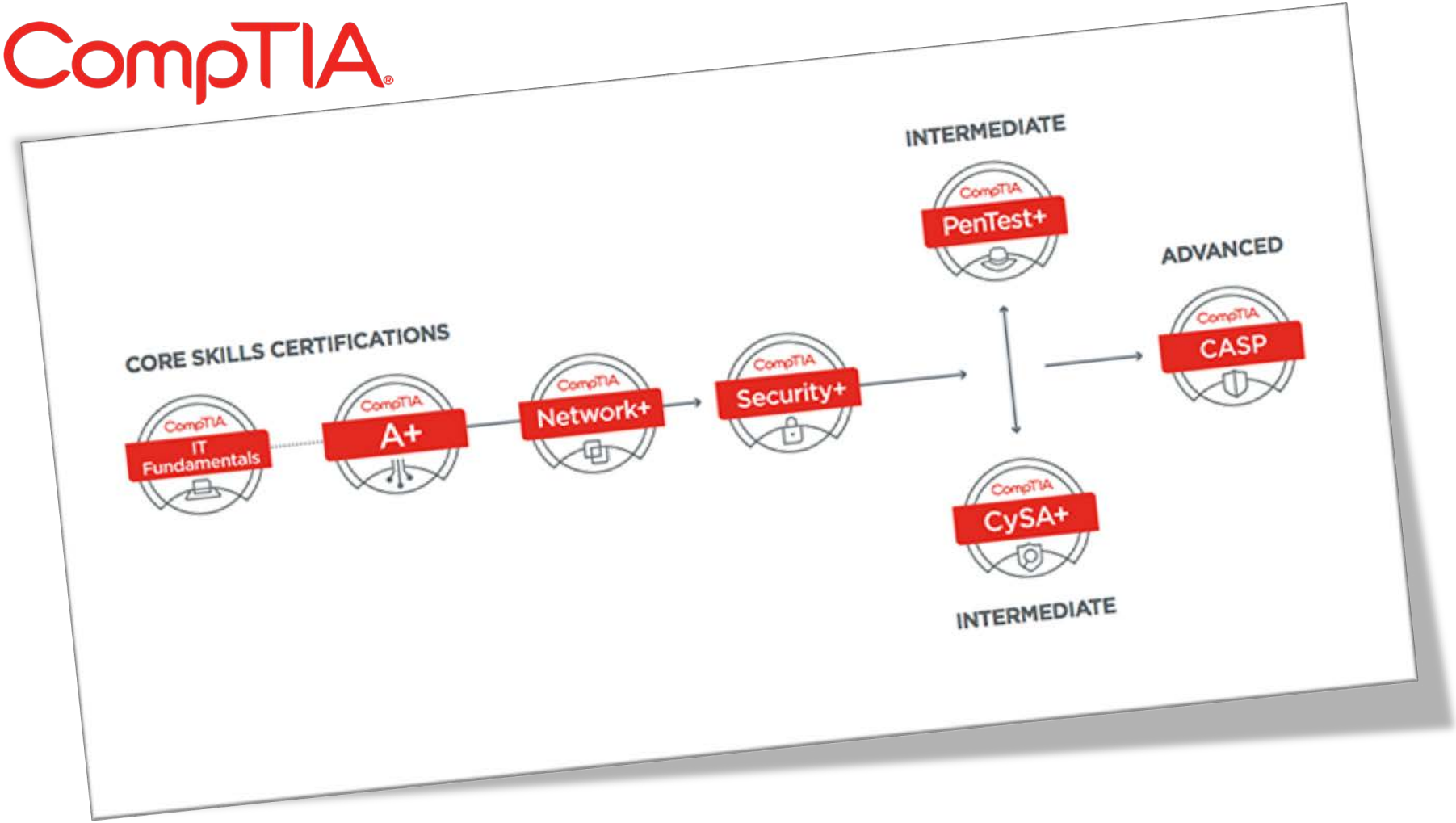
A. Not planning to continue to develop cybersecurity skills
B. Industry certifications
C. Two-year college degree
D. University / bachelors degree
E. Post-graduate degree

CYBERSECURITY AND ETHICAL HACKING CERTIFICATIONS



https://www.eccouncil.org/programs/certified-ethical-hacker-ceh

CompTIA


INTERMEDIATE
CompTIA
PenTest+
ADVANCED
CompTIA
CASP
CORE SKILLS CERTIFICATIONS
CompTIA
IT Fundamentals
CompTIA
A+
CompTIA
Network+
CompTIA
Security+
CompTIA
CySA+
INTERMEDIATE

OFFENSIVE security

Courses Certifications Online Labs Penetration Testing Projects Blog About

Information Security Certifications

Hands-on information security certifications training by Offensive Security.

Information Security Certifications

For Pen Testers and IT Security Professionals

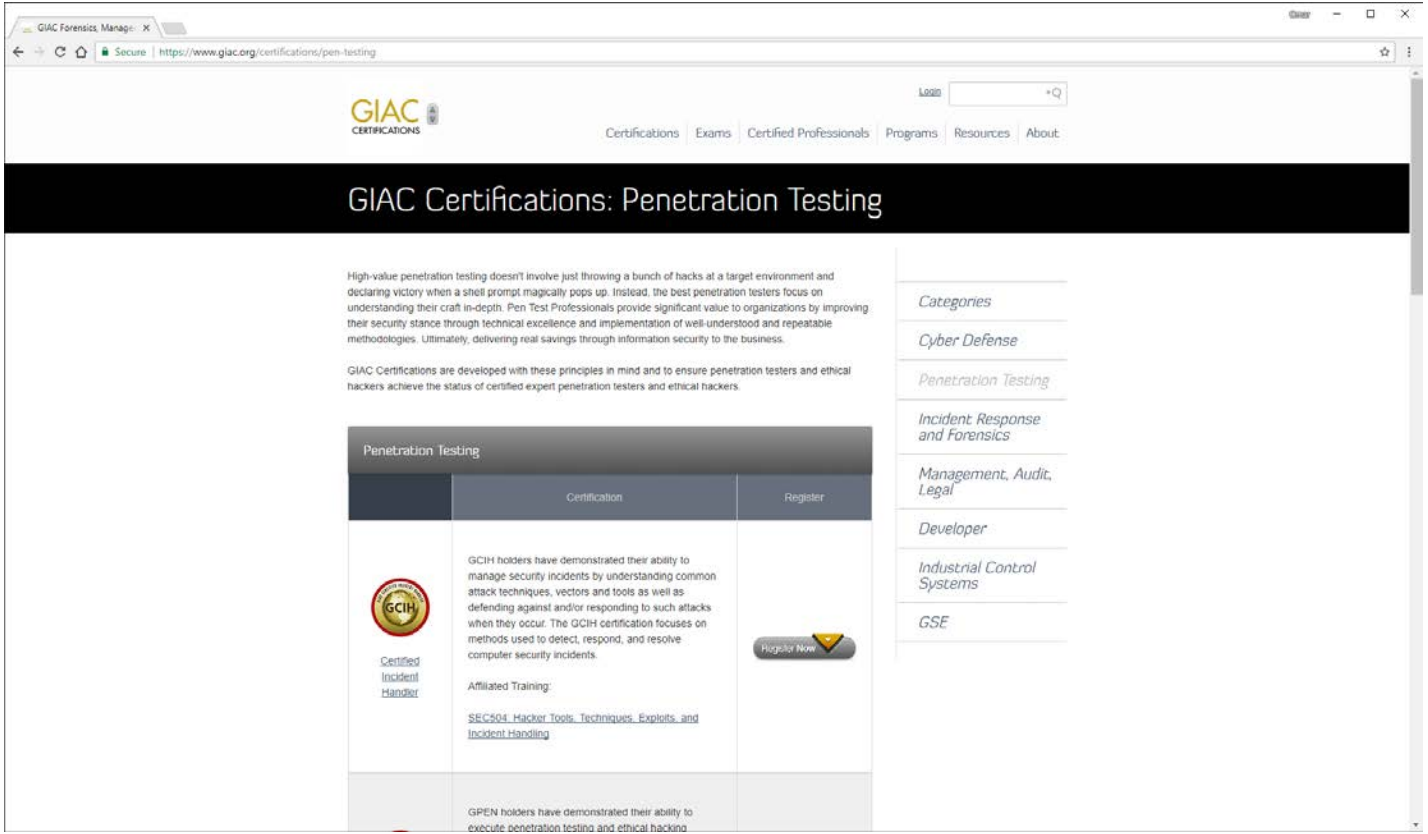
In-demand **Information Security Certifications** and hands-on ethical hacking courses for pen testers and IT security professionals. These ethical hacking certifications are provided by Offensive Security, the creators of Kali Linux.

Accompanying our **hands-on security training** programs are a set of industry leading **Information Security Certifications**, which are considered the most rigorous tests of skill available in the computer security field. These **performance-based certifications** rely entirely on **demonstrated ability and merit**. Instead of relying on outdated multiple choice questions, candidates are presented with a series of **real-world hacking challenges** which they must complete in a limited amount of time. Pass or fail is **based on your actual performance**. From the best penetration testing training comes the **best information security certifications**.

BECOME CERTIFIED NOW!
REGISTER TODAY

https://www.offensive-security.com

GIAC Penetration Testing Certification



https://www.giac.org/certifications/pen-testing

ISC² CERTIFICATIONS

https://www.isc2.org

Certification Tracks	Entry	Associate	Professional	Expert	Architect
Cloud		CCNA Cloud	CCNP Cloud		
Collaboration		CCNA Collaboration	CCNP Collaboration	CCIE Collaboration	
Cybersecurity Operations		CCNA Cyber Ops			
Data Center		CCNA Data Center	CCNP Data Center	CCIE Data Center	
Design	CCENT	CCDA	CCDP	CCDE	CCAr
Industrial		CCNA Industrial			
Routing and Switching	CCENT	CCNA Routing and Switching	CCNP Routing and Switching	CCIE Routing and Switching	
Security	CCENT	CCNA Security	CCNP Security	CCIE Security	
Service Provider		CCNA Service Provider	CCNP Service Provider	CCIE Service Provider	
Wireless	CCENT	CCNA Wireless	CCNP Wireless	CCIE Wireless	

http://www.cisco.com/go/certifications

BREAK

REMEMBER TO CHECK OUT THE RESOURCES AT:

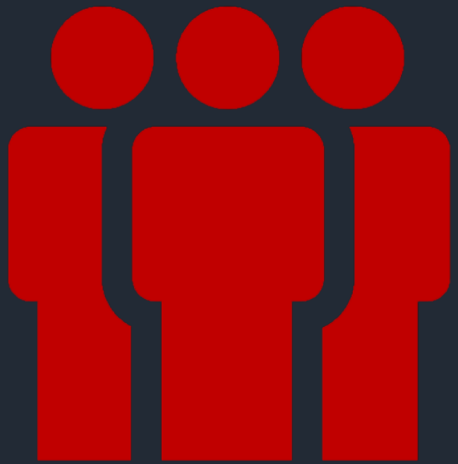
https://theartofhacking.org

https://theartofhacking.org/training

https://theartofhacking.org/github

https://theartofhacking.org/go/training_resources.pdf

How to Build, Manage, and Operate Cybersecurity Teams



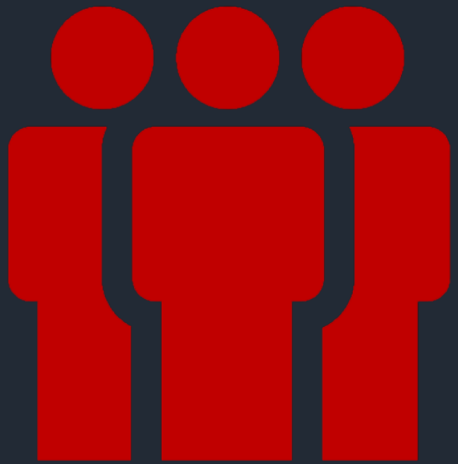
Understand the mission of the red team.

Management sponsorship.

Secure and justify funding.

Understand and create operational processes and policies for the Red Team

Additional Reference and Video: http://h4cker.org/rb/6



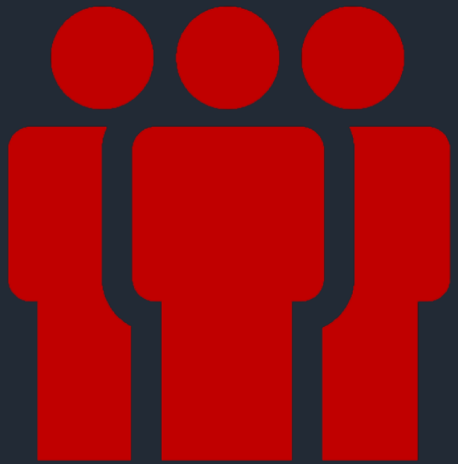
What skills?

Who should you hire?

Technical skills across all your technologies. Is it feasible?

What about administrative skills?

Additional Reference and Video: http://h4cker.org/rb/7



Set clear objectives

Get the right tools

Support the team

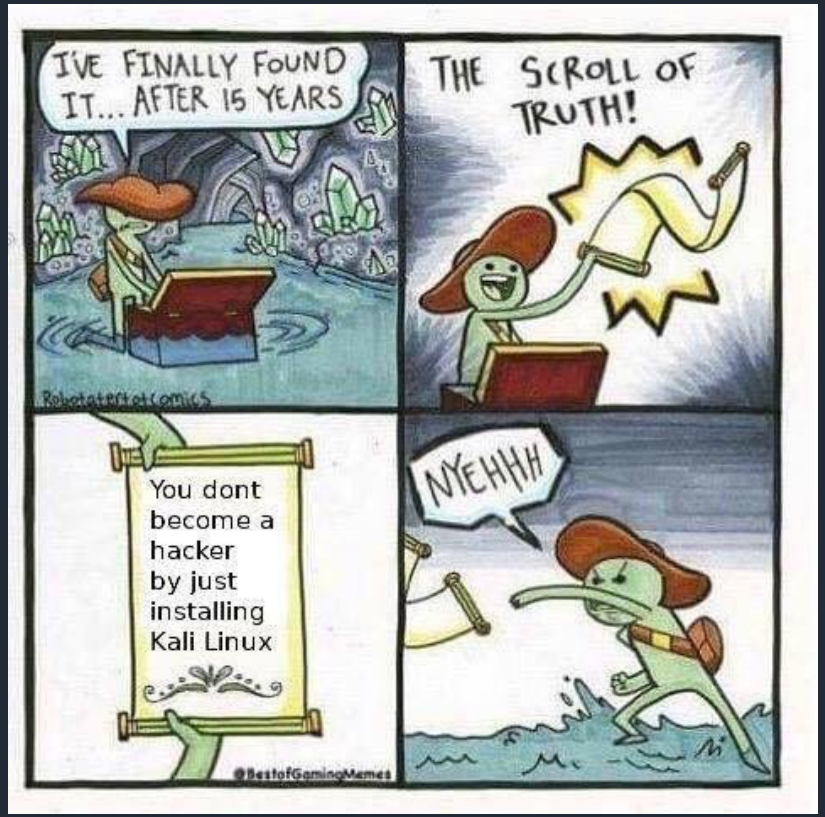
Focus on key issues and biggest risks

How can you measure success? Qualitative and quantitative metrics?

Additional Reference and Video: http://h4cker.org/rb/7

Red Team Tools

Toolz of the trade



Of course, the penetration testing tools will apply:

https://theartofhacking.org/github

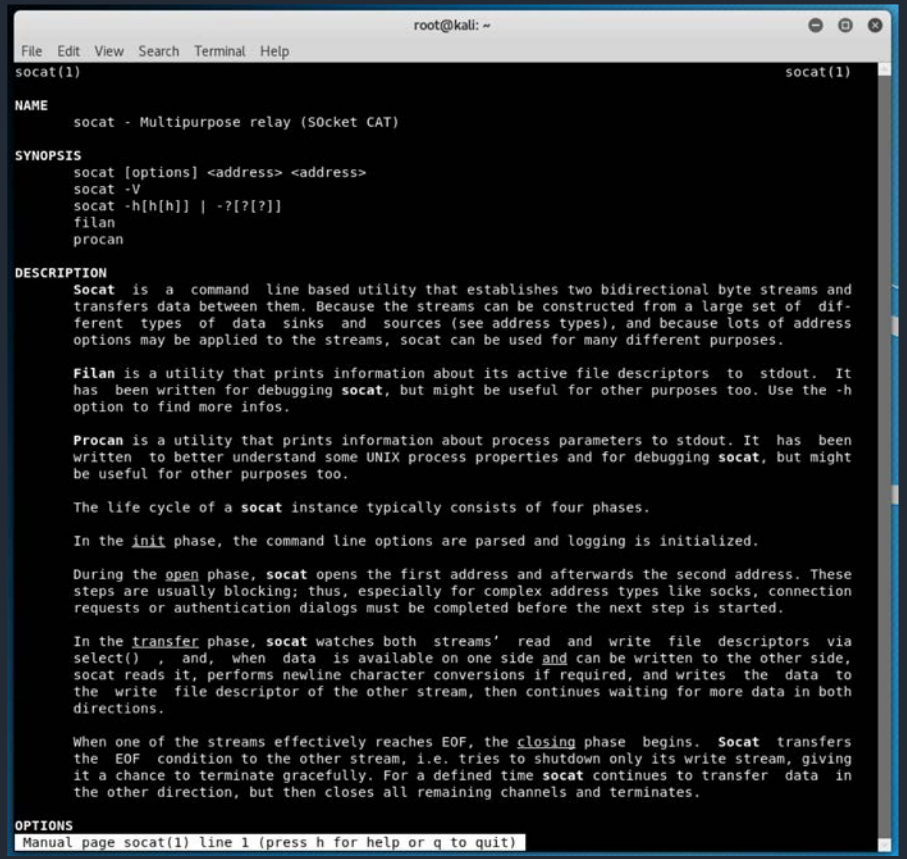
Consider segregating these functions on different assets:

- Phishing SMTP
- Phishing payloads
- Long-term command and control (C2)
- Short-term C2

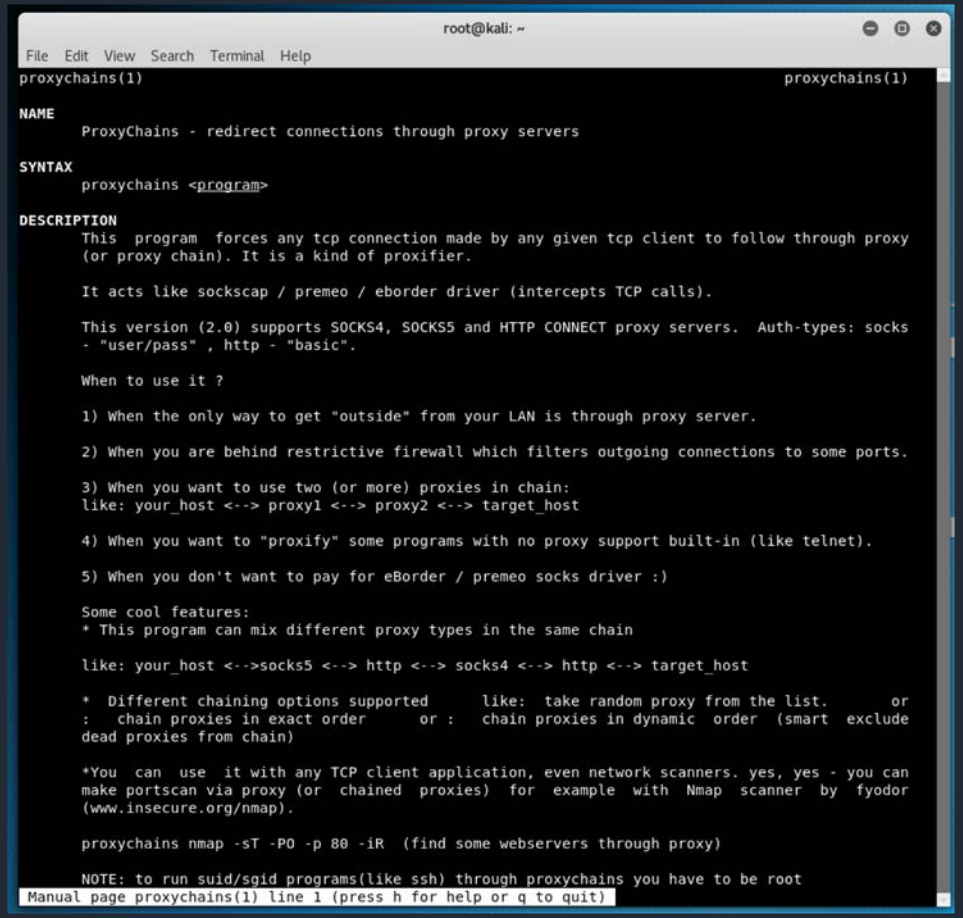
Using Redirectors

Common redirector types:

- SMTP
- Payloads
- Web Traffic
- C2 (HTTP(S), DNS, etc)



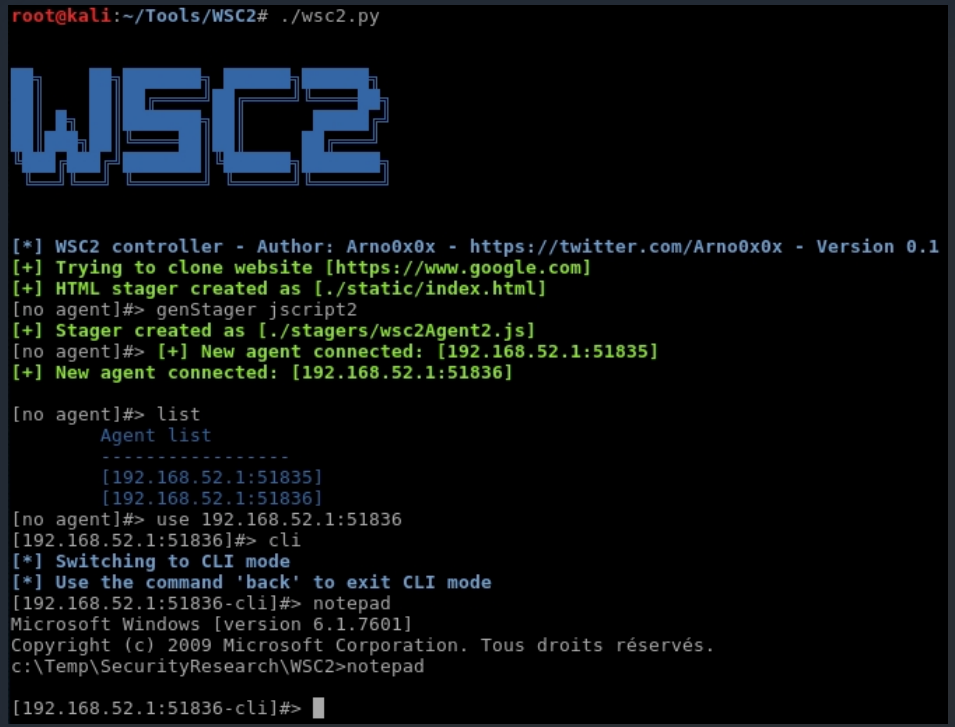
http://www.dest-unreach.org/socat



http://proxychains.sourceforge.net

Proxychains demo

Command and Control



https://github.com/Arno0x/WSC2

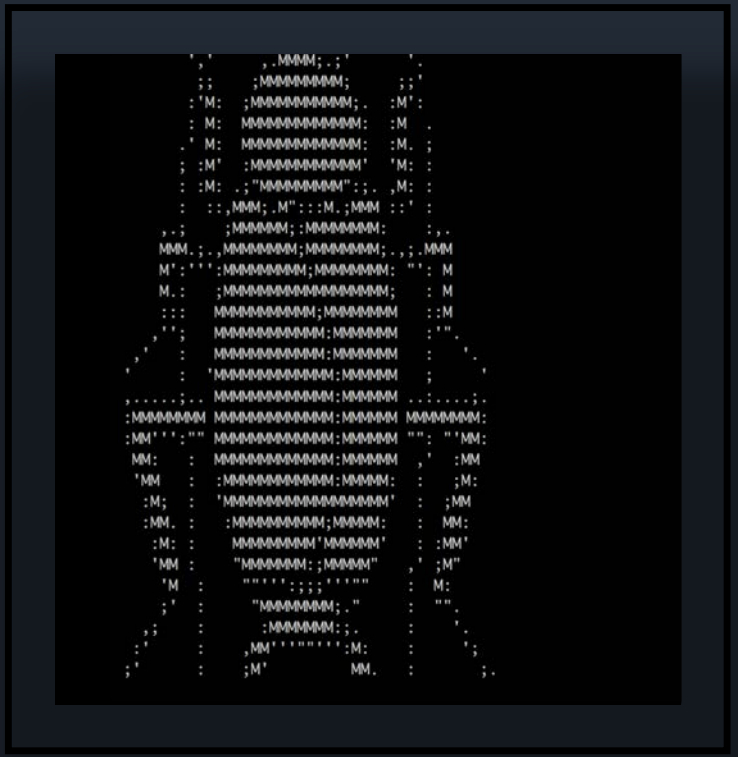
WMImplant

PowerShell based tool that leverages WMI to both perform actions against targeted machines, but also as the C2 channel for issuing commands and receiving results.

https://github.com/ChrisTruncer/WMImplant

DropboxC2 from Arno0x0x

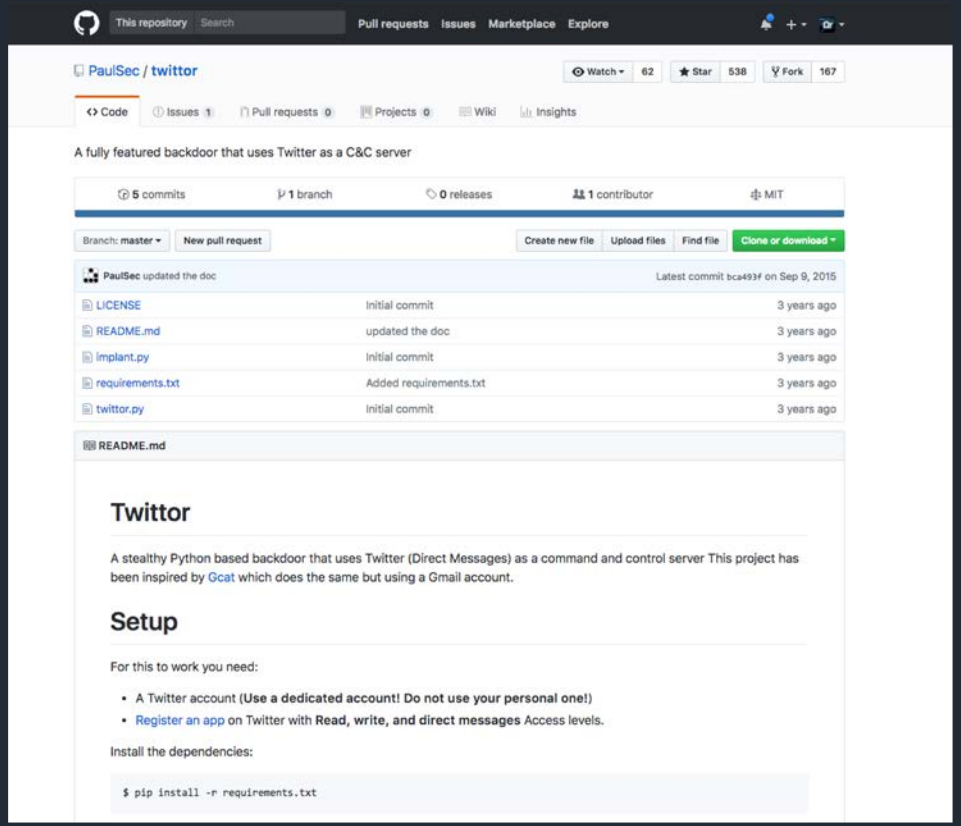
https://github.com/santosomar/DBC2



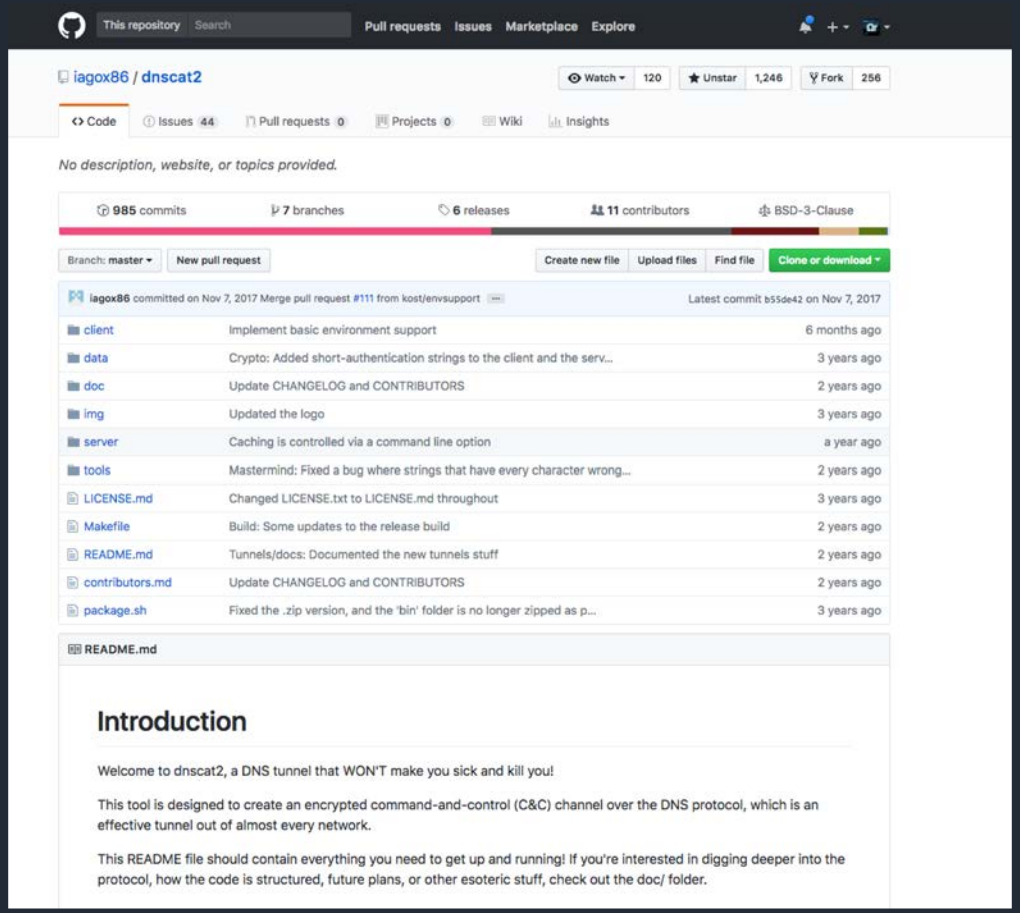
TrevorC2 by Dave Kennedy

https://github.com/trustedsec/trevorc2

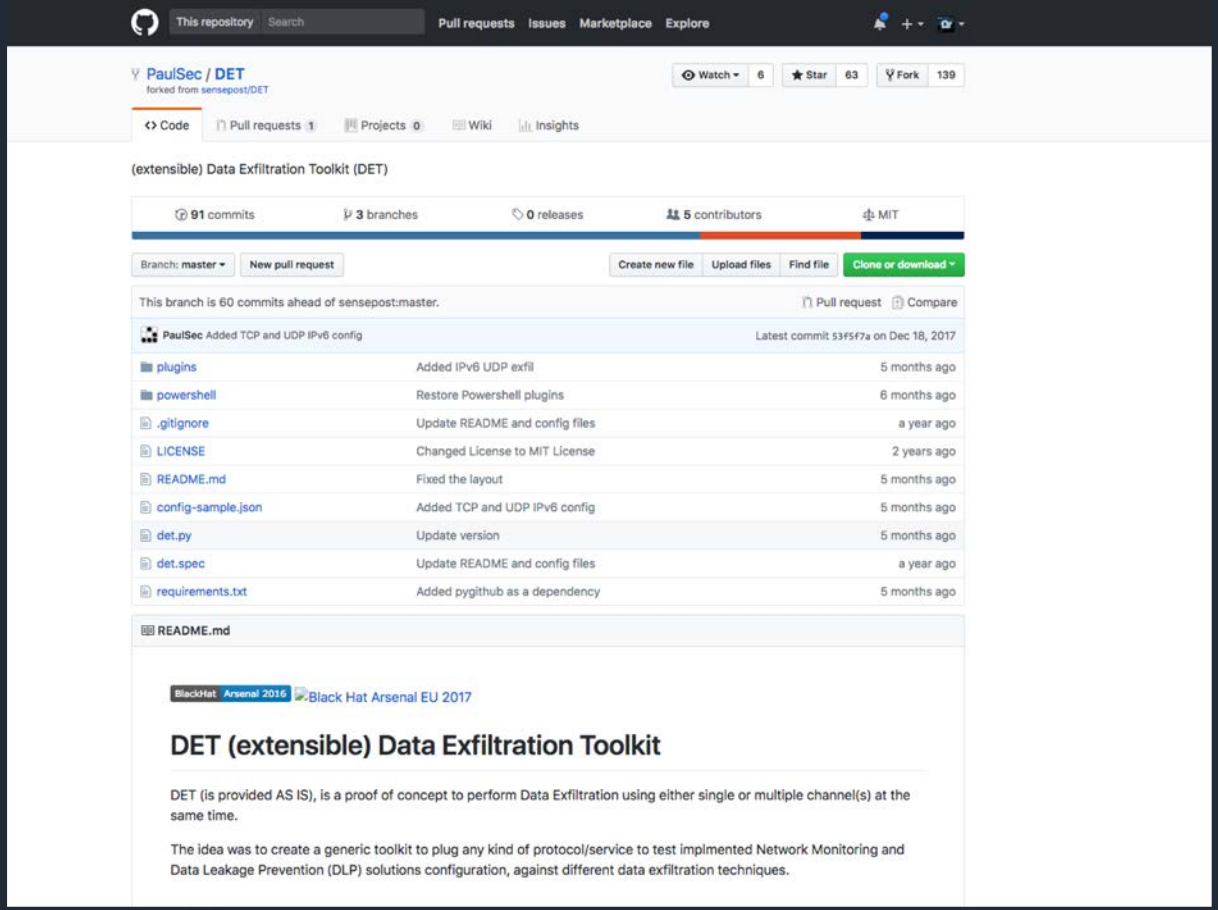
Trevor Demo



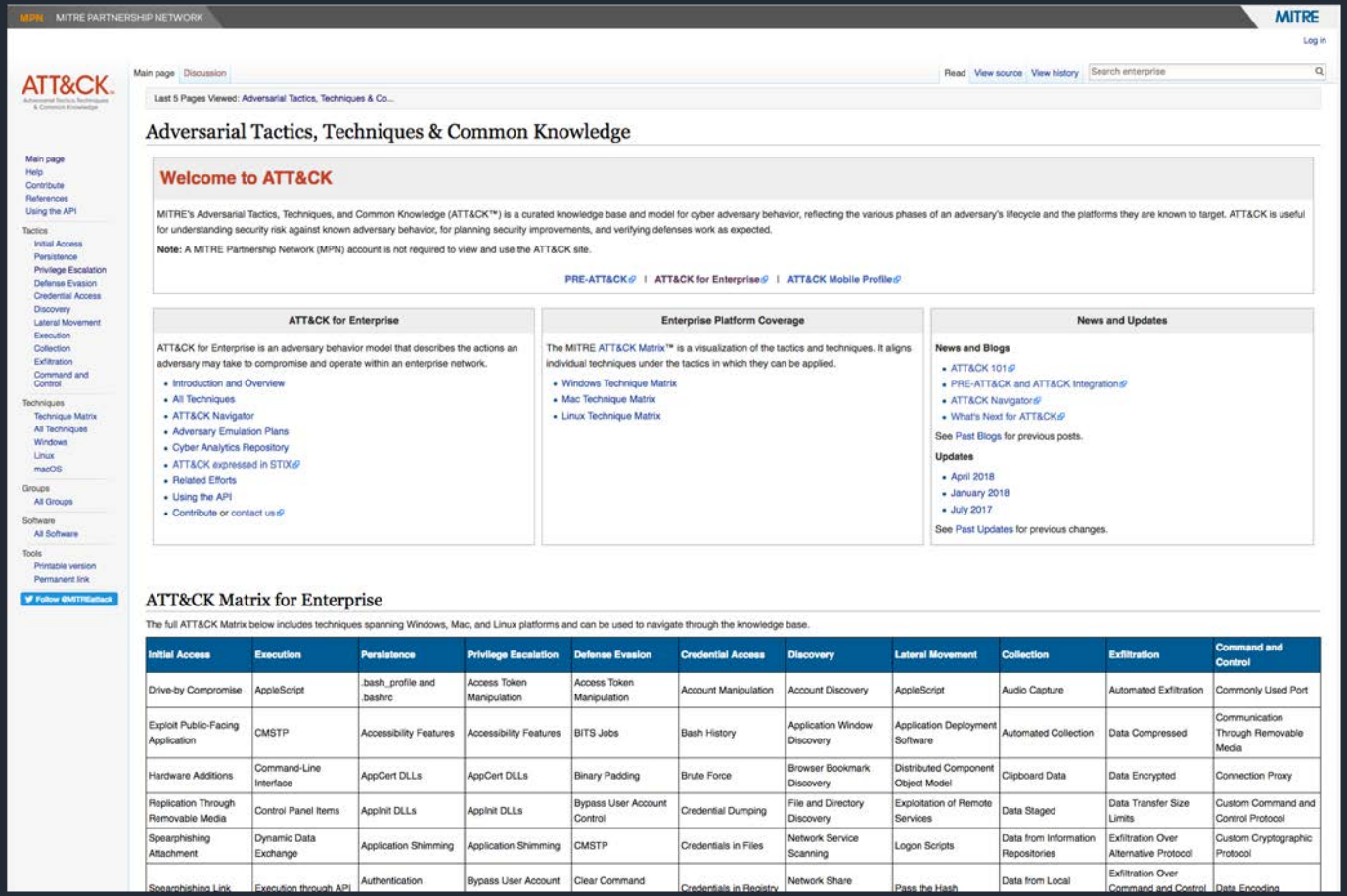
https://github.com/PaulSec/twittor



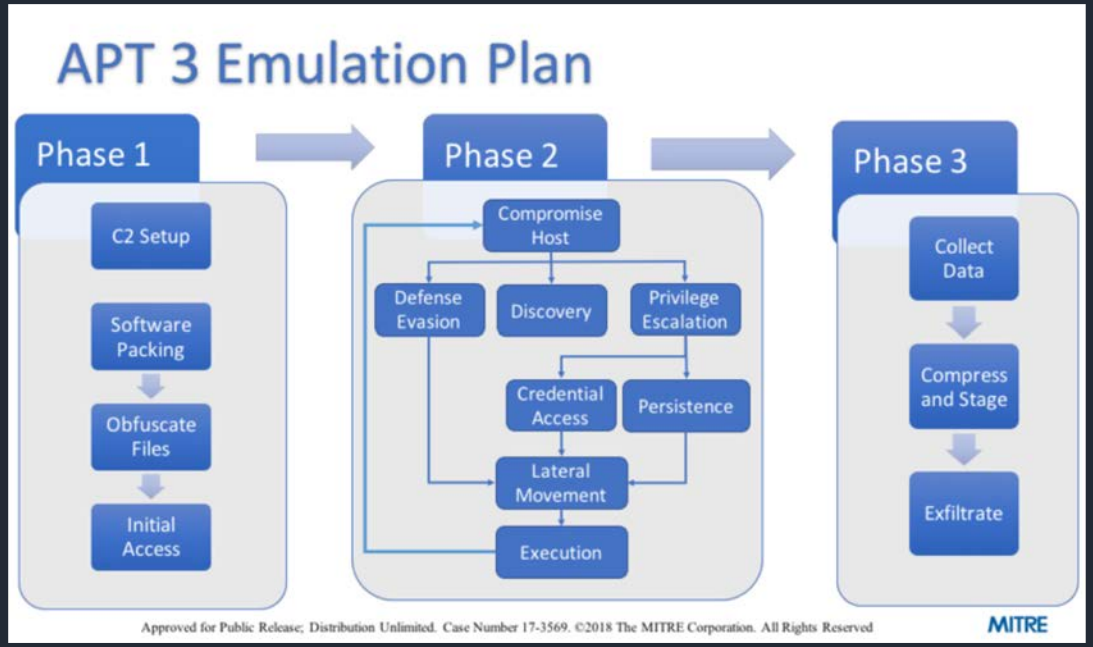
https://github.com/iagox86/dnscat2



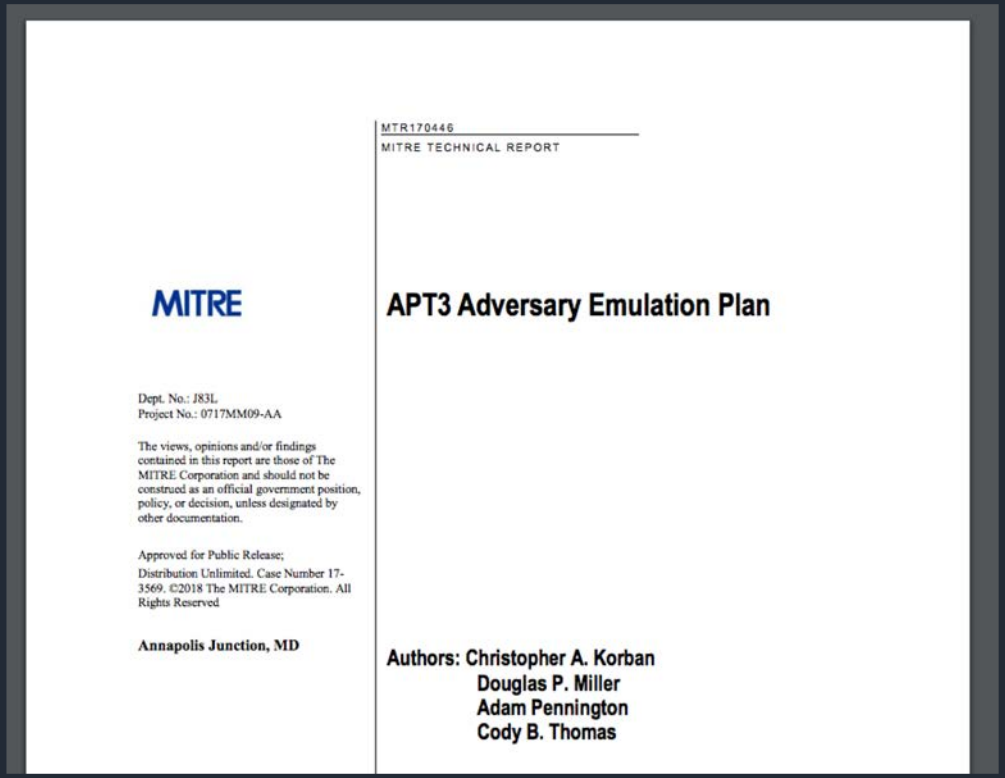
https://github.com/PaulSec/DET



https://attack.mitre.org



https://attack.mitre.org/wiki/Adversary_Emulation_Plans



MTR170446

MITRE TECHNICAL REPORT

MITRE

APT3 Adversary Emulation Plan

Dept. No.: J83L
Project No.: 0717MM09-AA

Annapolis Junction, MD

Authors: Christopher A. Korban
Douglas P. Miller
Adam Pennington
Cody B. Thomas

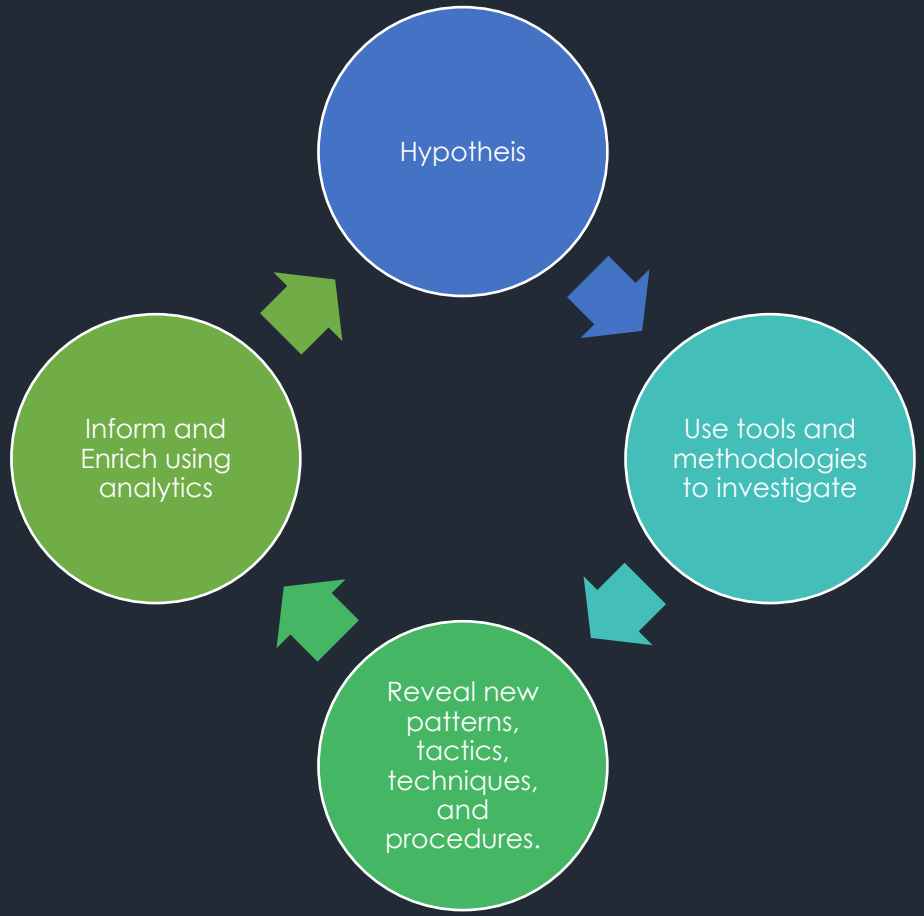
https://attack.mitre.org/w/img_auth.php/6/6c/APT3_Adversary_Emulation_Plan.pdf

Introduction to Threat Hunting

What is Threat Hunting?

"the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions."

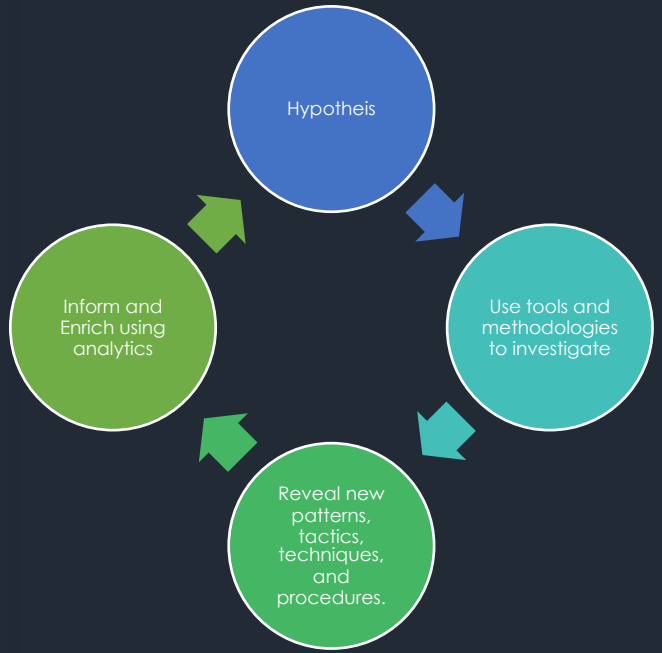
http://sqrrl.com/media/Framework-for-Threat-Hunting-Whitepaper.pdf



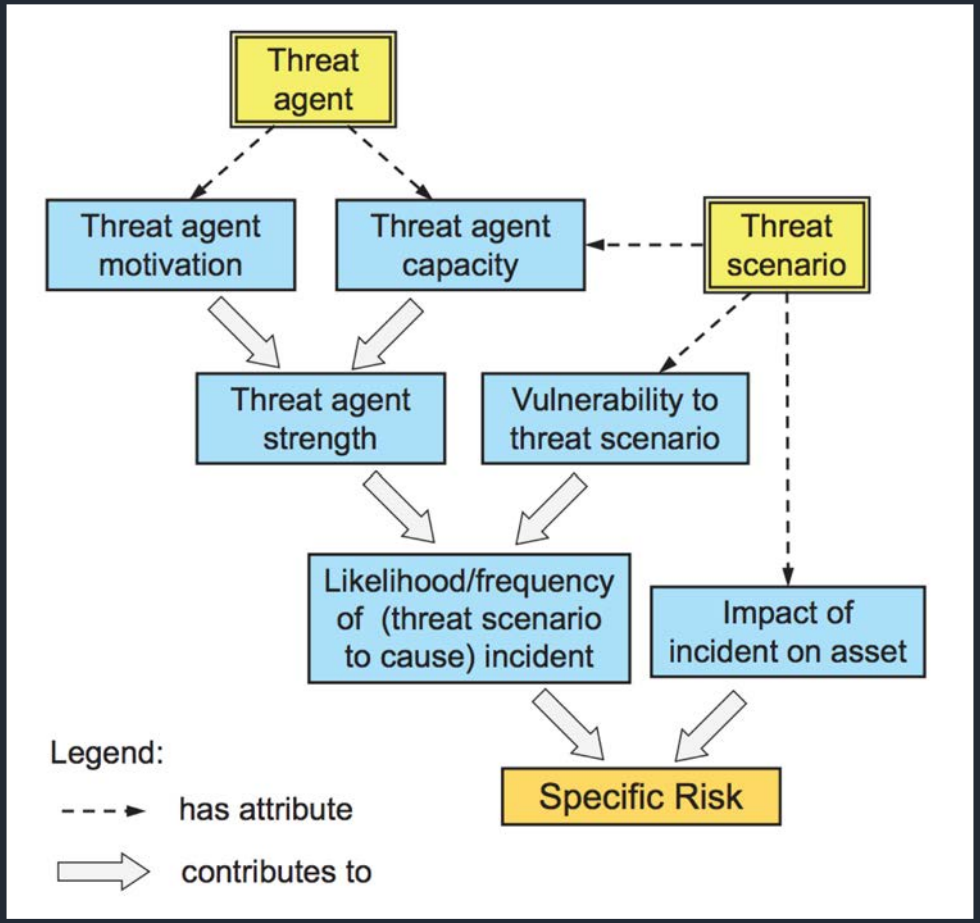
The Threat Hunting Process

HUNTING LOOP STEPS

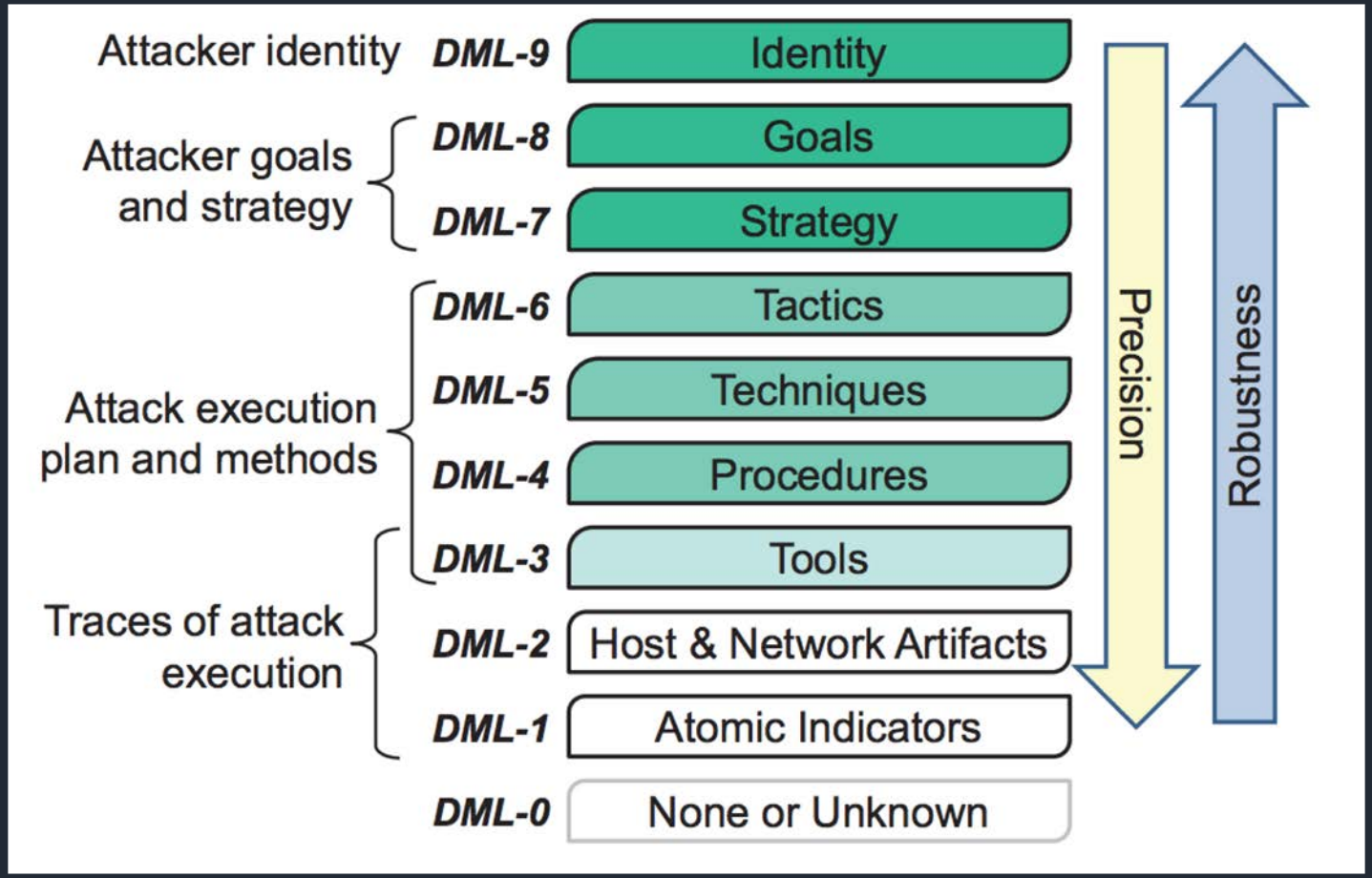
	HM0 Initial	HM1 Minimal	HM2 Procedural	HM3 Innovative	HM4 Leading
DATA COLLECTION	Little or no data collection	Moderate collection of some types of data from a few key points in the IT environment	High collection of certain types of data throughout the IT environment	High collection of certain types of data throughout the IT environment	**High collection of many types of data throughout the IT environment**
HYPOTHESIS CREATION	Respond to existing automated alerts from SIEM, IDS, Firewall, etc.	Review threat intelligence to develop new hypotheses	Review threat intelligence and "friendly intelligence" to develop new hypotheses	Review threat intelligence, "friendly intelligence", and manual cyber risk scoring (i.e. "crown jewel analysis") to develop new hypotheses	**Review threat intelligence, "friendly intelligence", and automated cyber risk scoring to develop new hypotheses**
TOOLS & TECHNIQUES FOR HYPOTHESIS TESTING	Alert consoles, SIEM searches; No proactive investigation	Utilize SIEM or log analysis tools to conduct basic search via full-text or SQL-like queries	Utilize simple tools and histograms to search and analyze data based on existing hunting procedures	Leverage visualizations and graph searches. Develop new hunting procedures	**Advanced visualizations and graph searches. Publish, and automate new hunting procedures**
PATTERN & TTP DETECTION	None; Only SIEM/ IDS alerts	Identifying IOCs at bottom of PoP like domains, URLs, and hashes	Identification of IOCs at bottom and middle of PoP and mapping trends of those IOCs over time	Able to detect adversary TTPs and other IoCs at the top of the PoP	**Automatic complex TTP discovery and campaign tracking; Active sharing of IoCs with information sharing organization**
ANALYTICS AUTOMATION	None	Integrates threat intel feeds into automated alerting for basic matching	Build a library of effective hunting procedures and performs them on a regular schedule	Build a library of effective hunting procedures and performs them frequently; basic data science (standard deviation, outlier detection)	**Automate effective hunting procedures to continuously improve alerting capabilities; advanced data science (machine learning)**



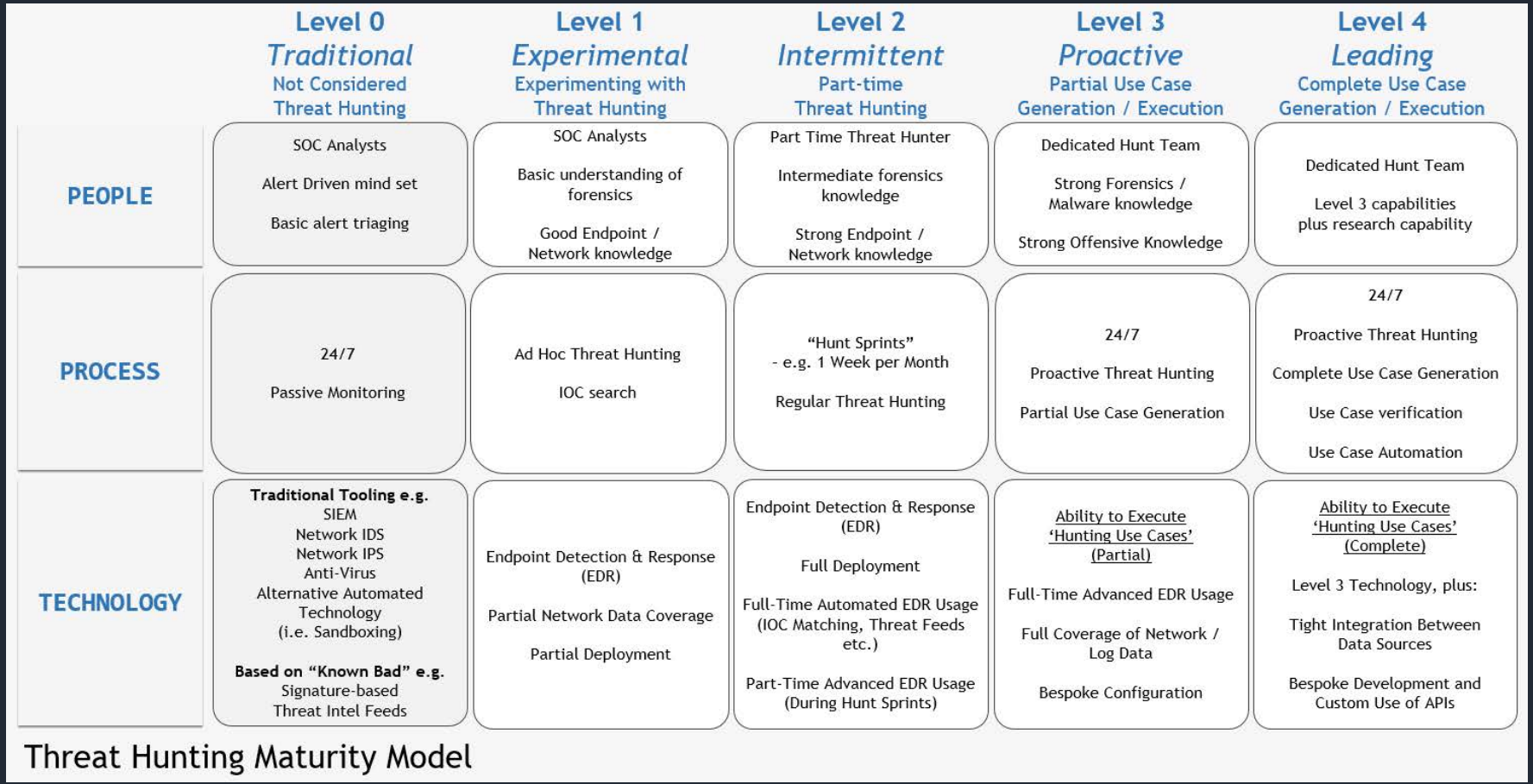
https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper.pdf



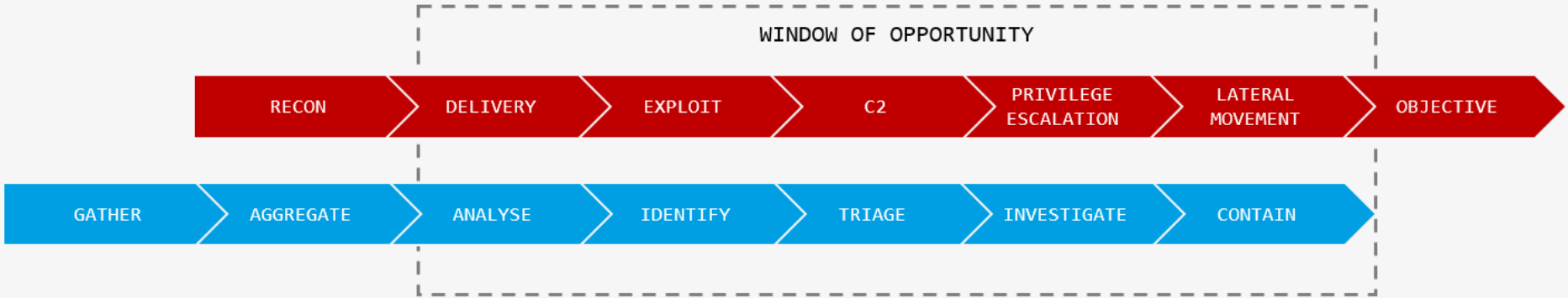
http://h4cker.org/rb/8



http://h4cker.org/rb/8

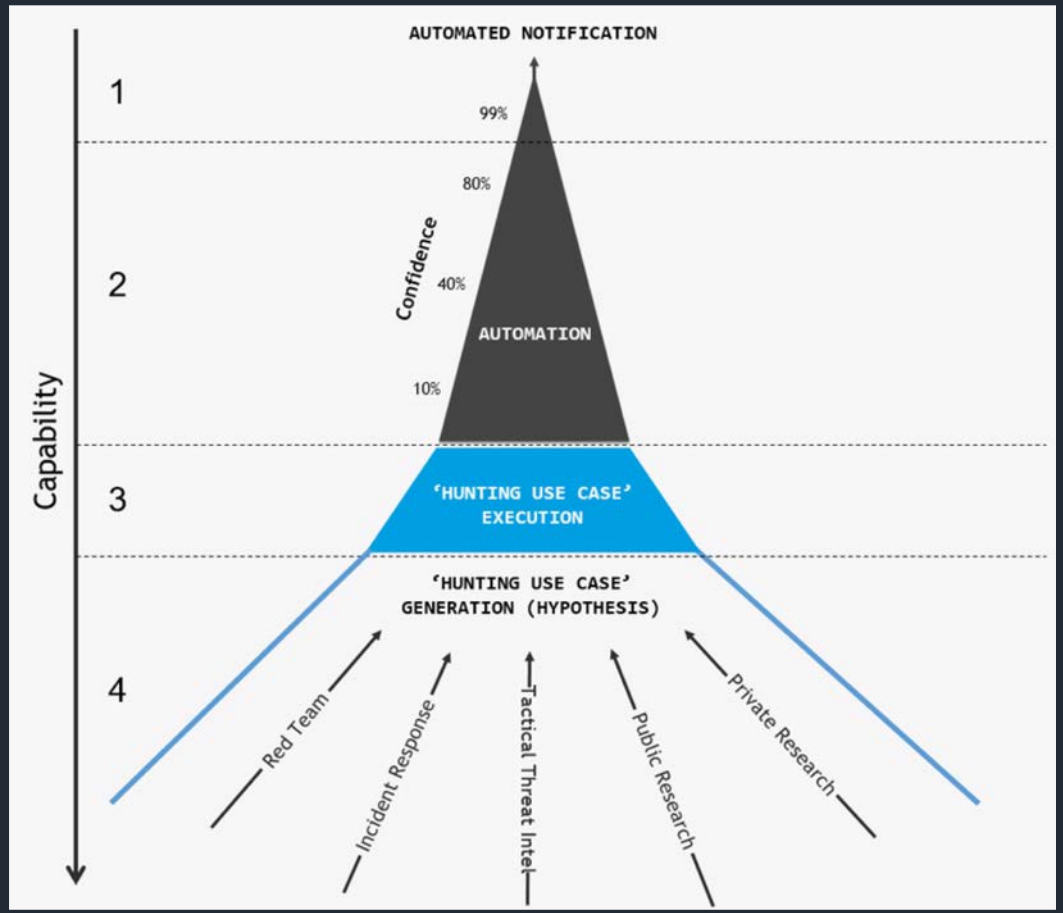


Threat Hunting Maturity Model

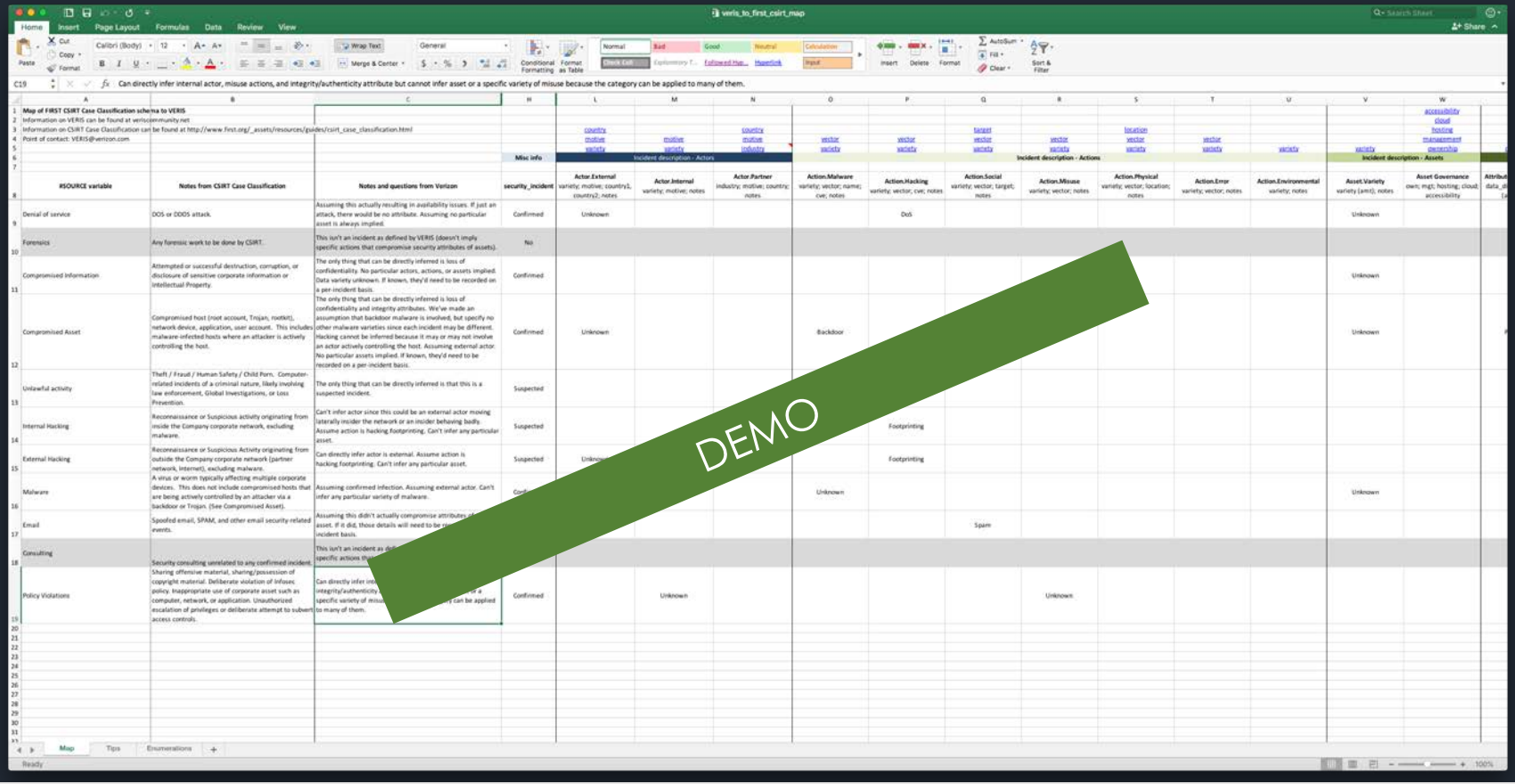


Microsoft's BlueHat conference introduced the concept of a blue team cyber kill chain, as a defender-centric version of the standard attack focussed cyber kill chain. This described the chain of actions a defender needs to go through to find and evict attackers.

https://youtu.be/aZxtCKHhAUE?t=160

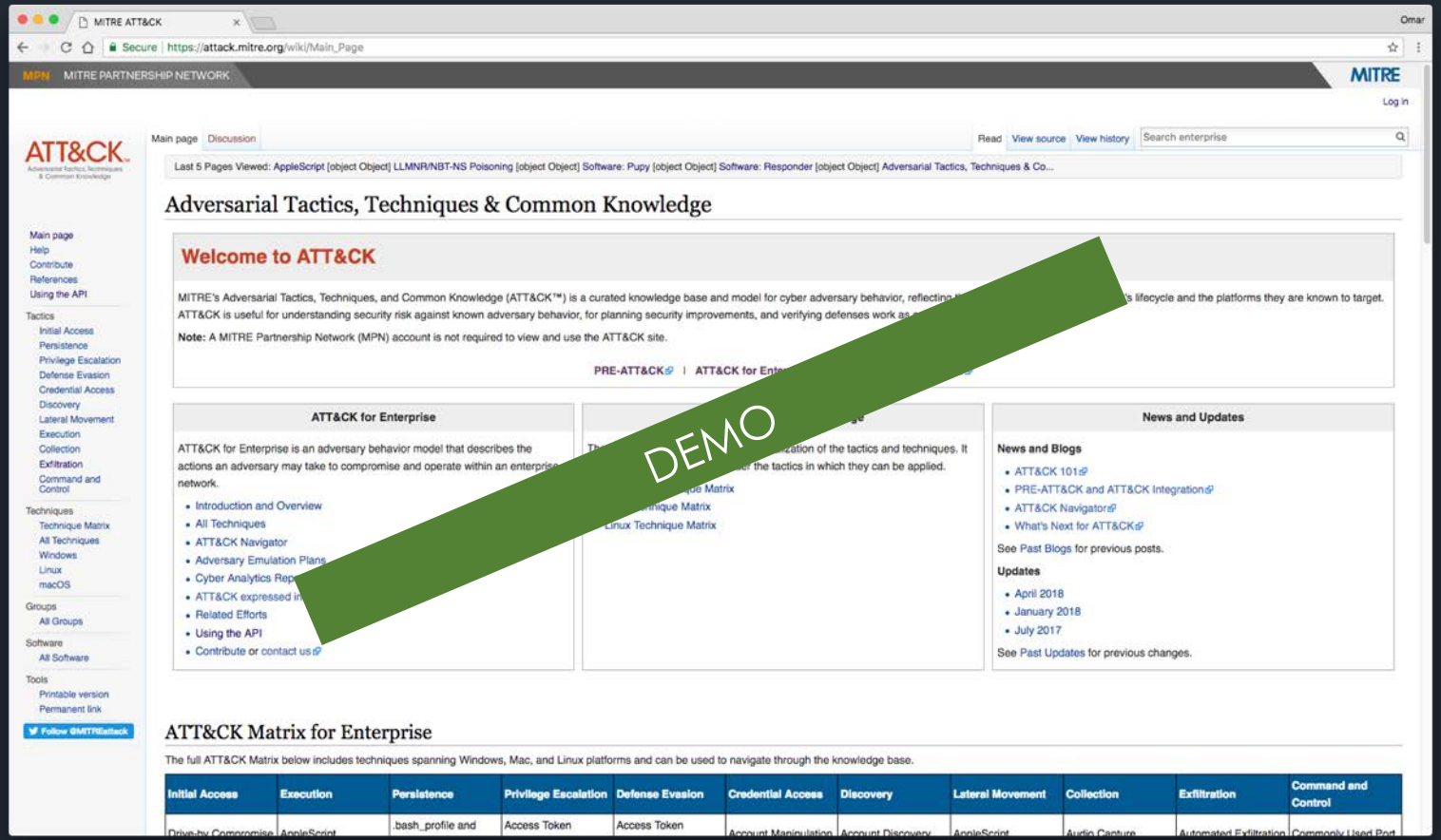


http://h4cker.org/rb/9

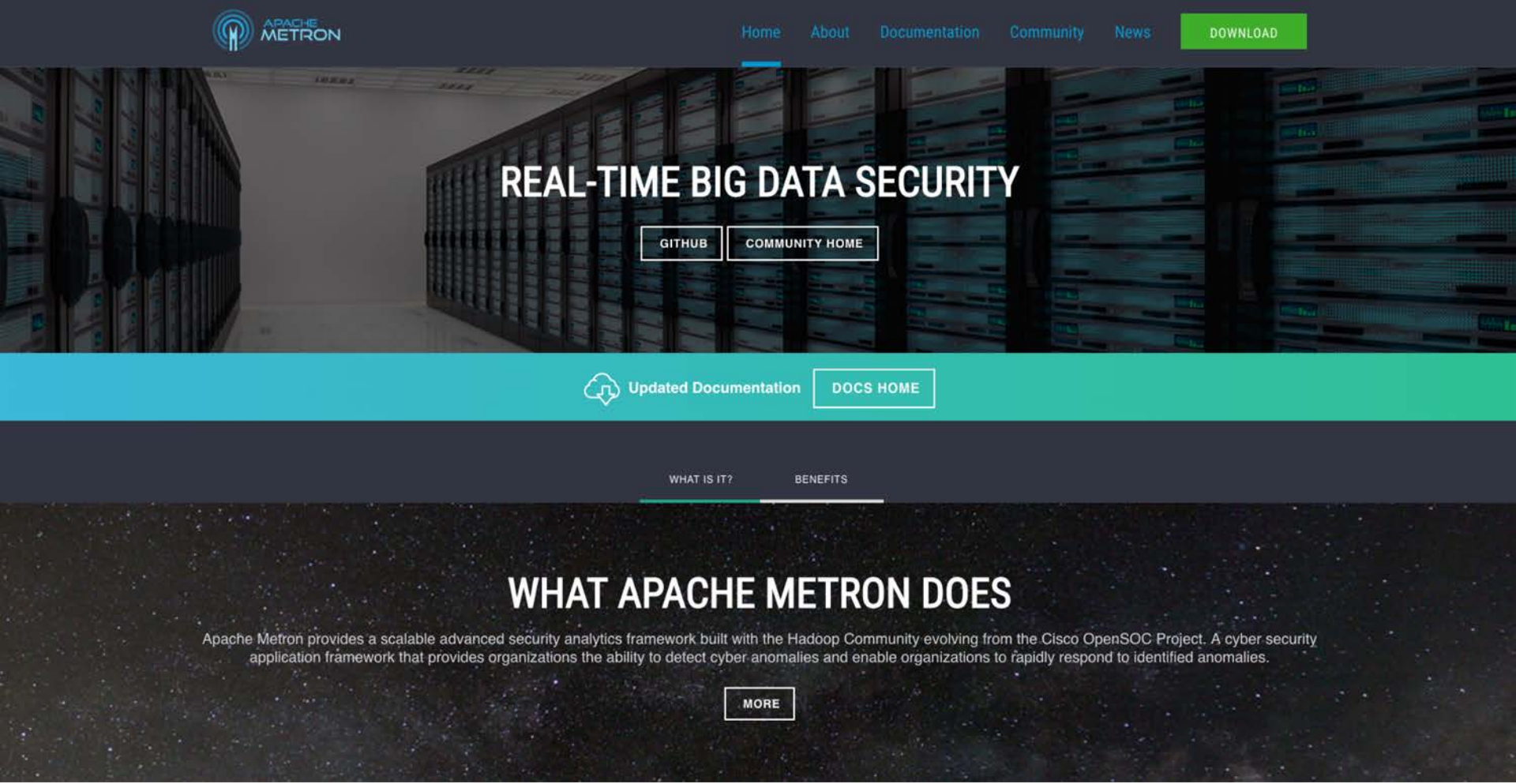


http://veriscommunity.net/veris-mapping.html

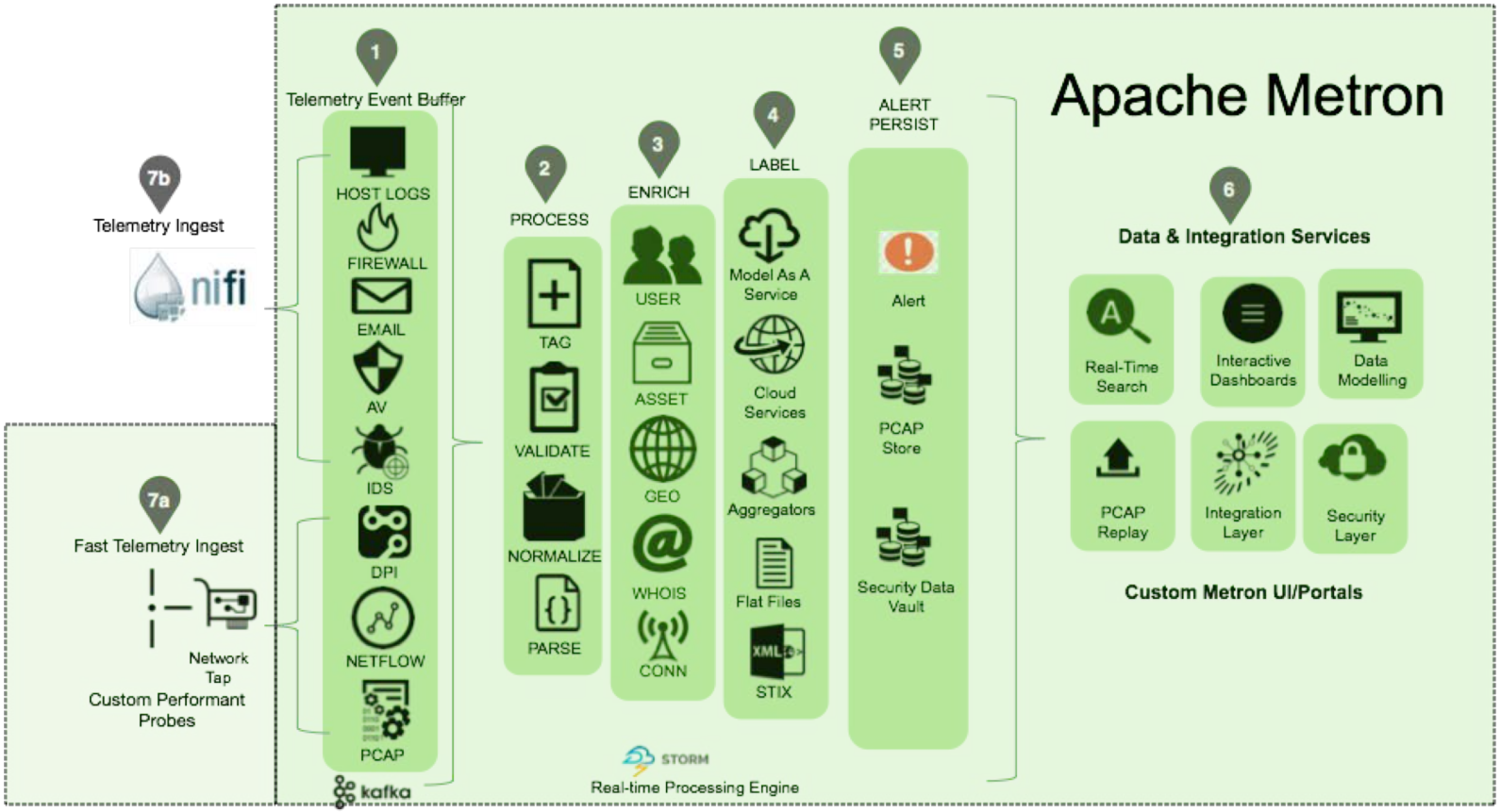
FIRST CSIRT Case Categories and VERIS

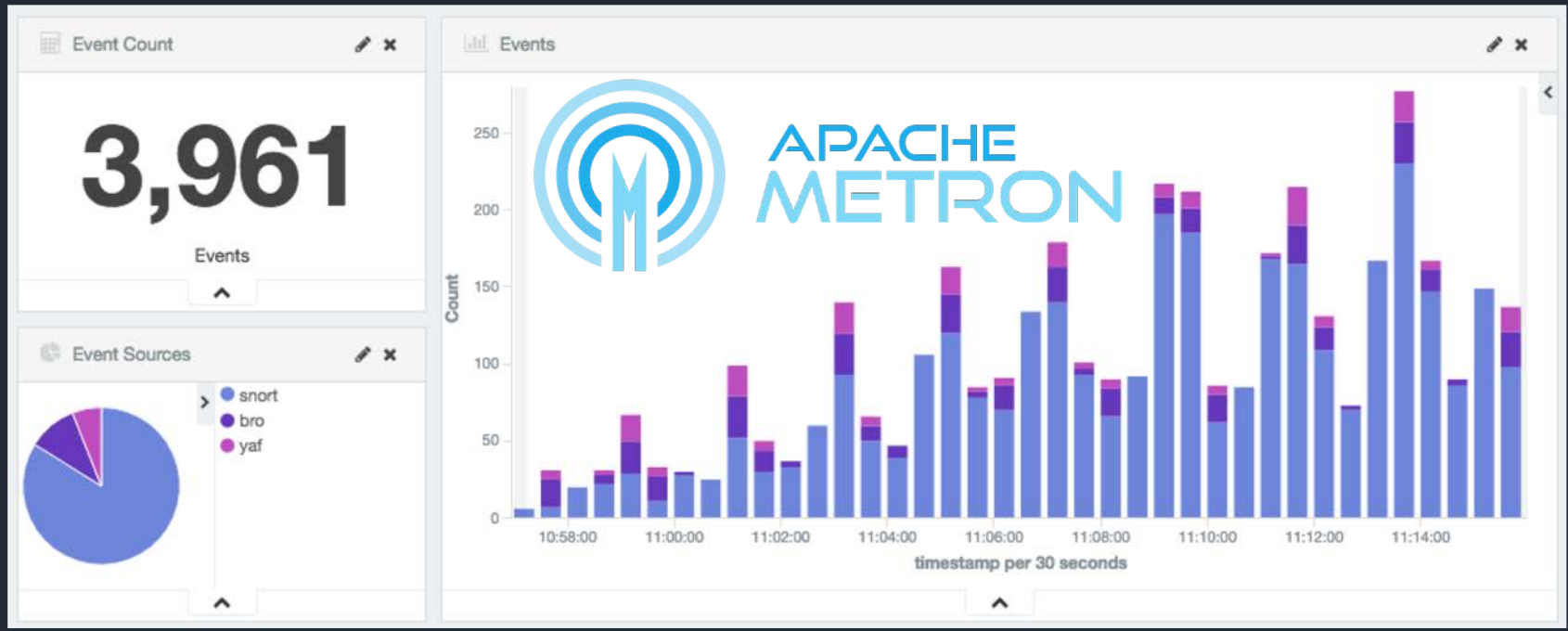

MITRE ATT&CK
Secure | https://attack.mitre.org/wiki/Main_Page
MPN MITRE PARTNERSHIP NETWORK
MITRE
ATT&CK
Main page Discussion
Read View source View history Search enterprise
Adversarial Tactics, Techniques & Common Knowledge
Welcome to ATT&CK
ATT&CK for Enterprise
News and Updates
DEMO
ATT&CK Matrix for Enterprise
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control

MITRE – ATT&CK



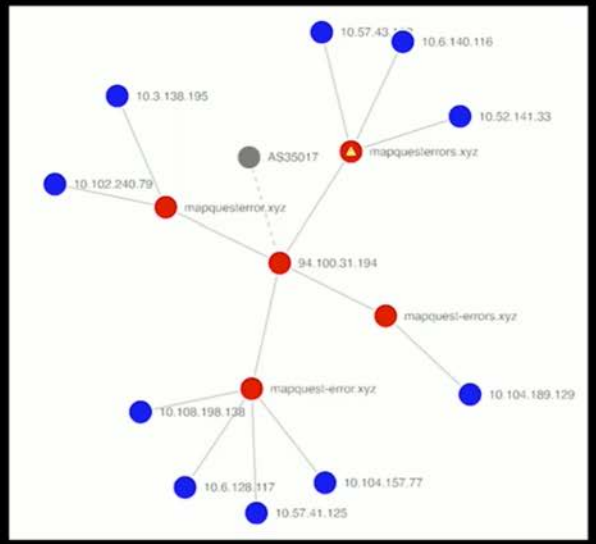
https://metron.apache.org/

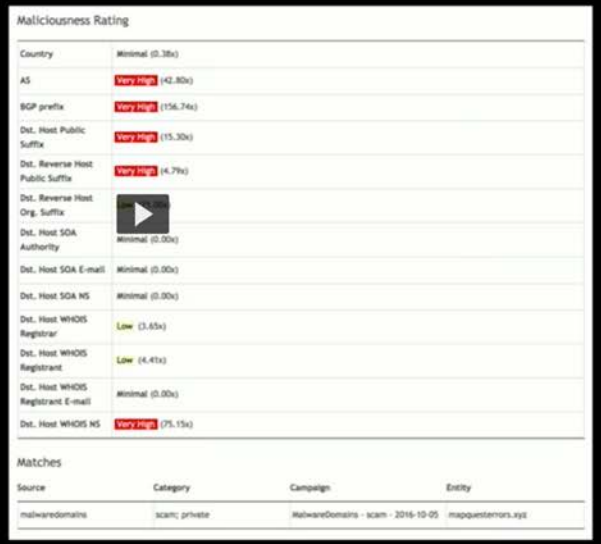

Apache Metron
1
Telemetry Event Buffer
HOST LOGS
FIREWALL
EMAIL
AV
IDS
DPI
NETFLOW
PCAP
kafka
2
PROCESS
TAG
VALIDATE
NORMALIZE
PARSE
3
ENRICH
USER
ASSET
GEO
WHOIS
CONN
4
LABEL
Model As A Service
Cloud Services
Aggregators
Flat Files
XML
STIX
5
ALERT PERSIST
Alert
PCAP Store
Security Data Vault
STORM
Real-time Processing Engine
6
Data & Integration Services
Real-Time Search
Interactive Dashboards
Data Modelling
PCAP Replay
Integration Layer
Security Layer
Custom Metron UI/Portals
7b
Telemetry Ingest
nifi
7a
Fast Telemetry Ingest
Network Tap
Custom Performant Probes



https://github.com/apache/metron

An Example (1)





https://learning.oreilly.com/videos/oreilly-security-conference/9781491985359/9781491985359-video316730

BREAK

REMEMBER TO CHECK OUT THE RESOURCES AT:

https://theartofhacking.org

https://theartofhacking.org/training

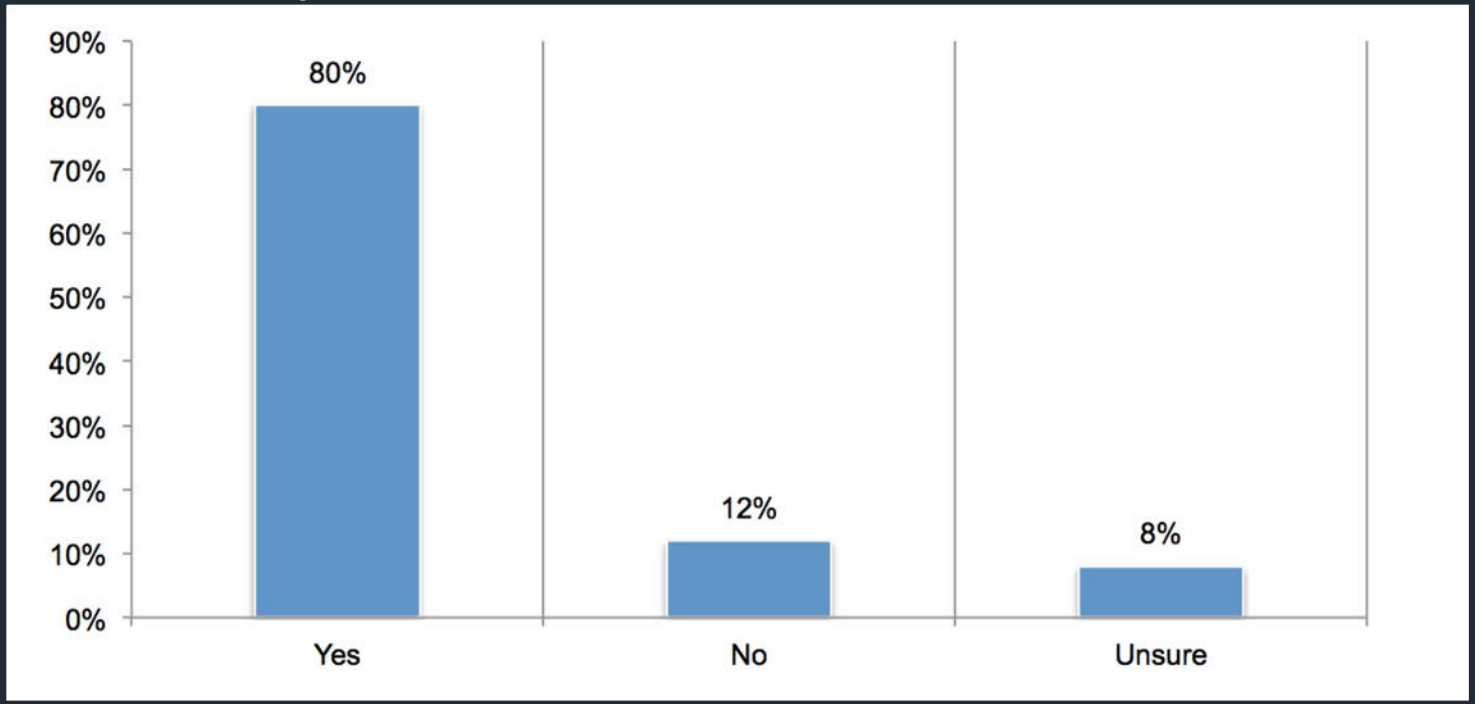
https://theartofhacking.org/github

https://theartofhacking.org/go/training_resources.pdf

Threat Intelligence

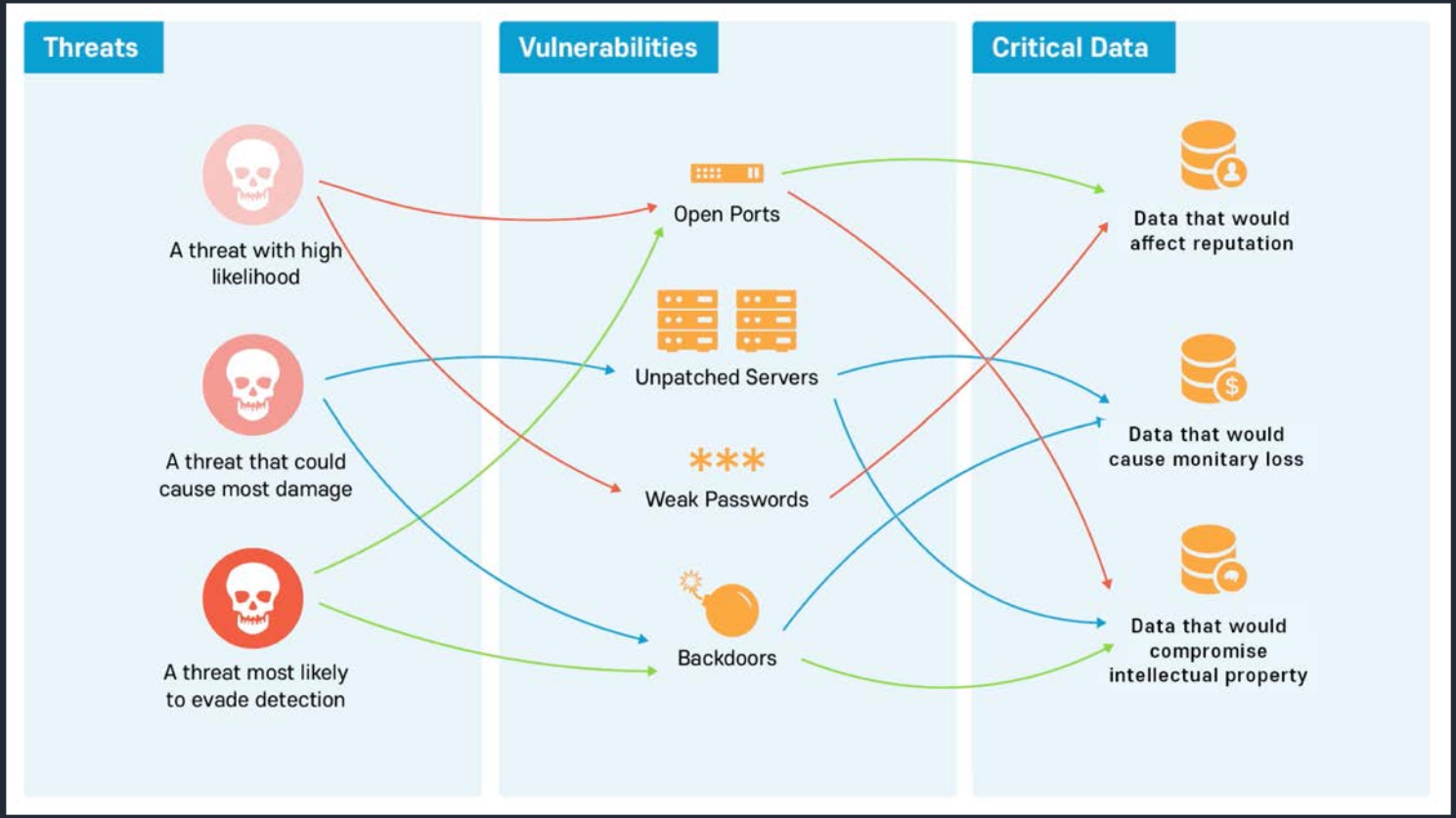
Why Threat Intelligence is Important?

Would threat intelligence have helped prevent or minimize the consequences of an attack?



PONEMON SURVEY

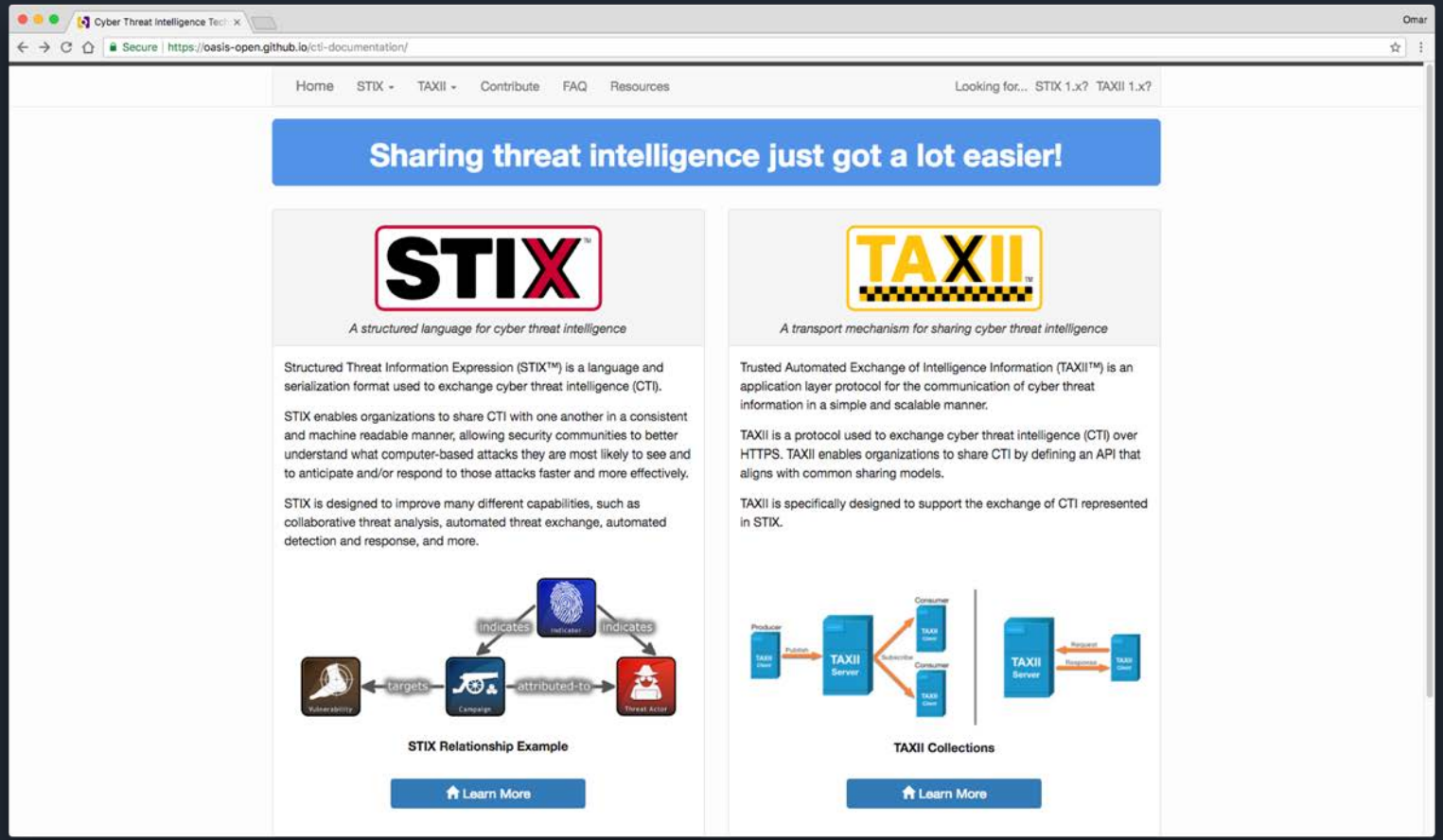
http://h4cker.org/rb/10



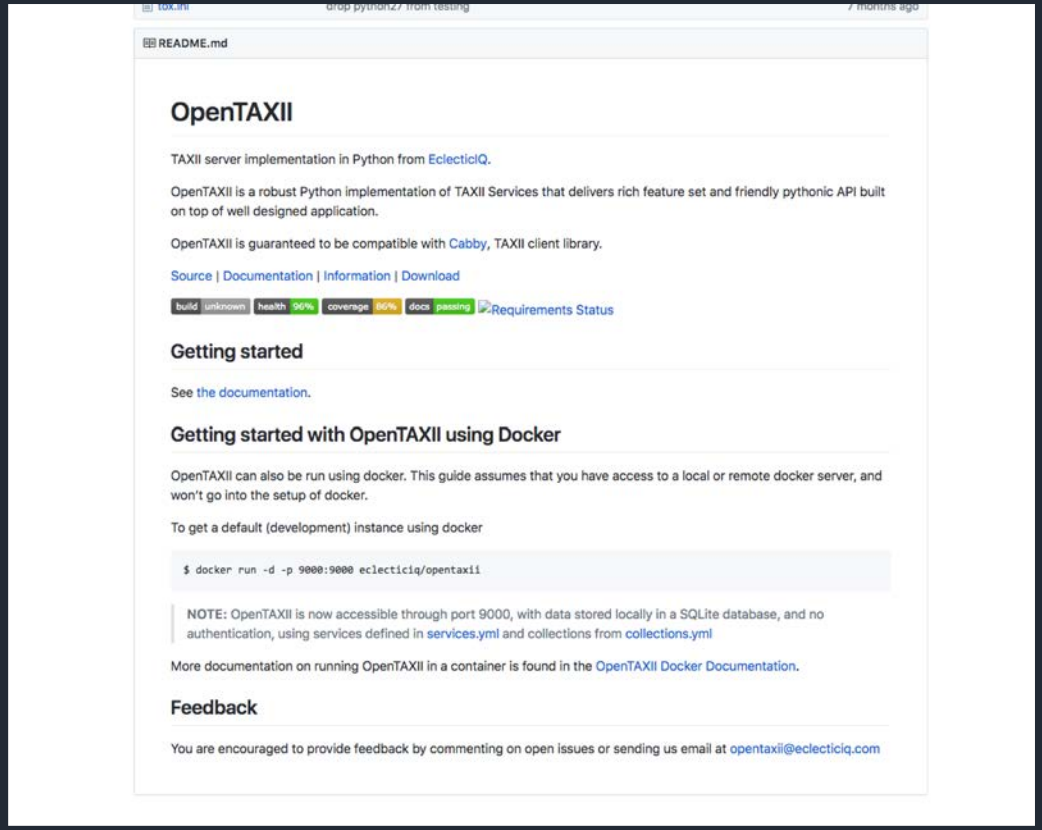
Threat Intelligence and Hunting

```
/*
This is a Yara Rule Example by Omar
*/
rule Super_Bad_Malware
{
  meta:
    author = "OmarOmar"
    threat = "MalWare.Gen0"
  strings:
    HASH = 60844f93dba8f5197f748b3012cd14654a107053
  condition:
    any of them
}
```

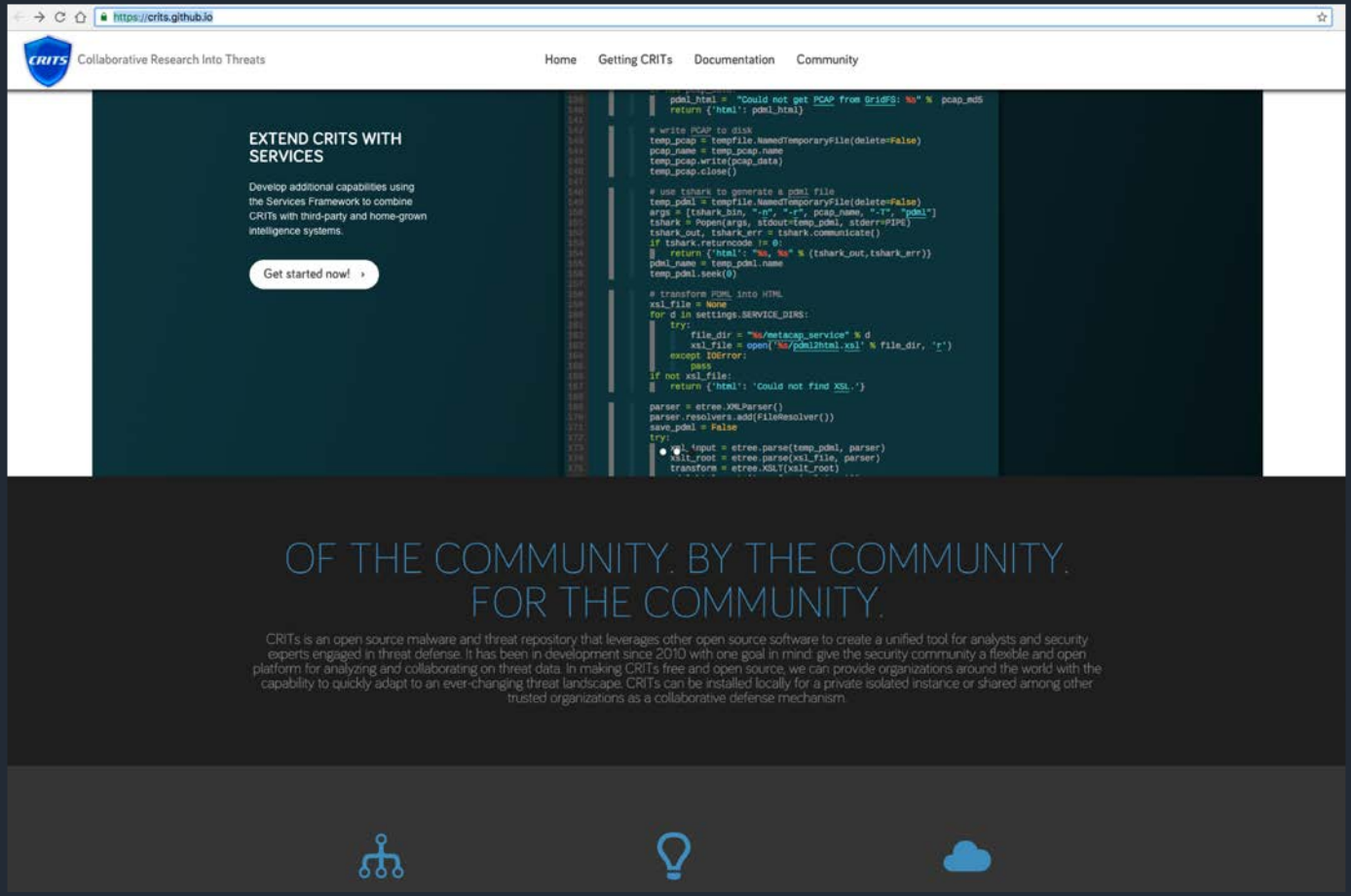
https://virustotal.github.io/yara/



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

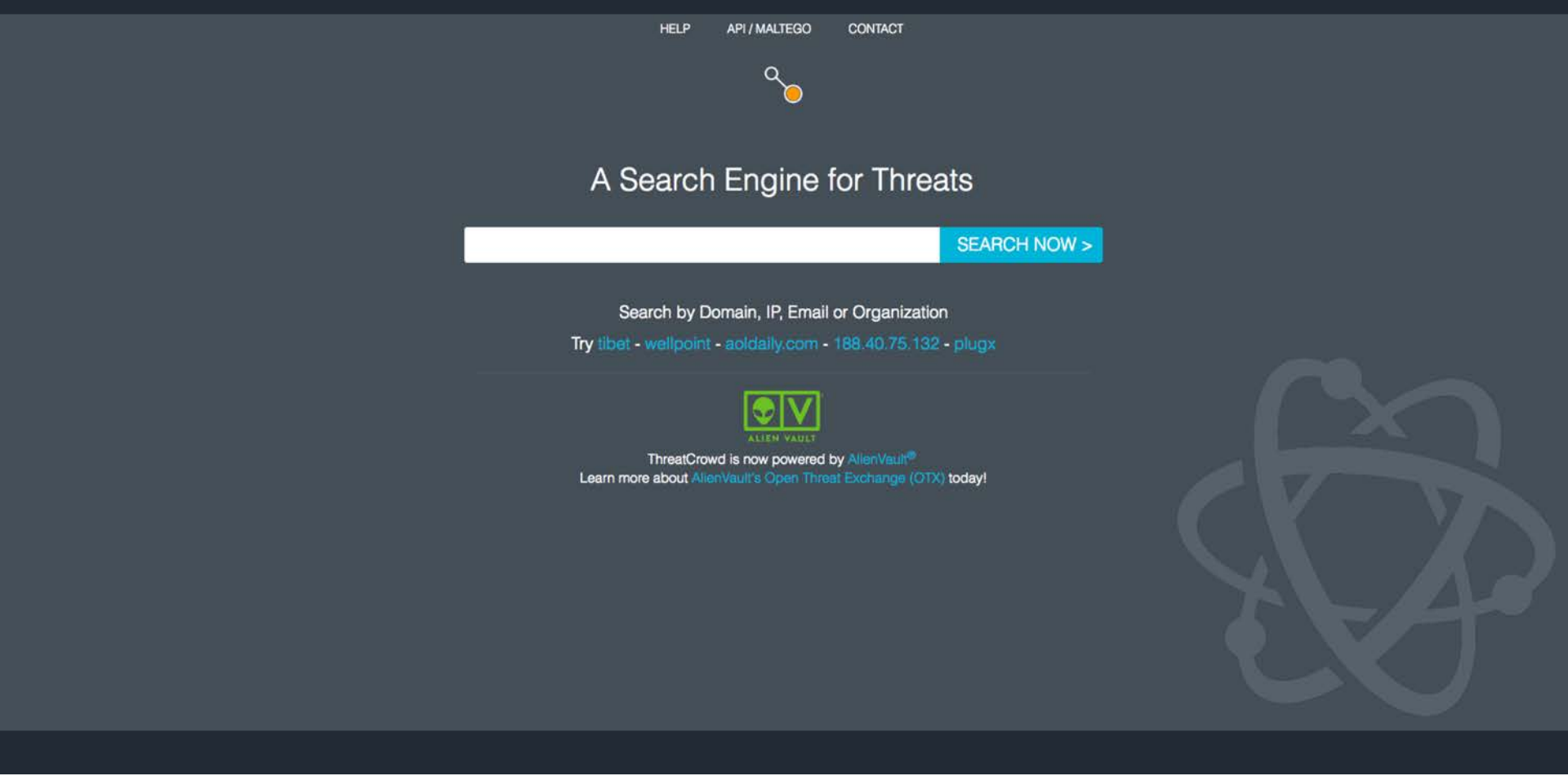


https://github.com/EclecticIQ/OpenTAXII

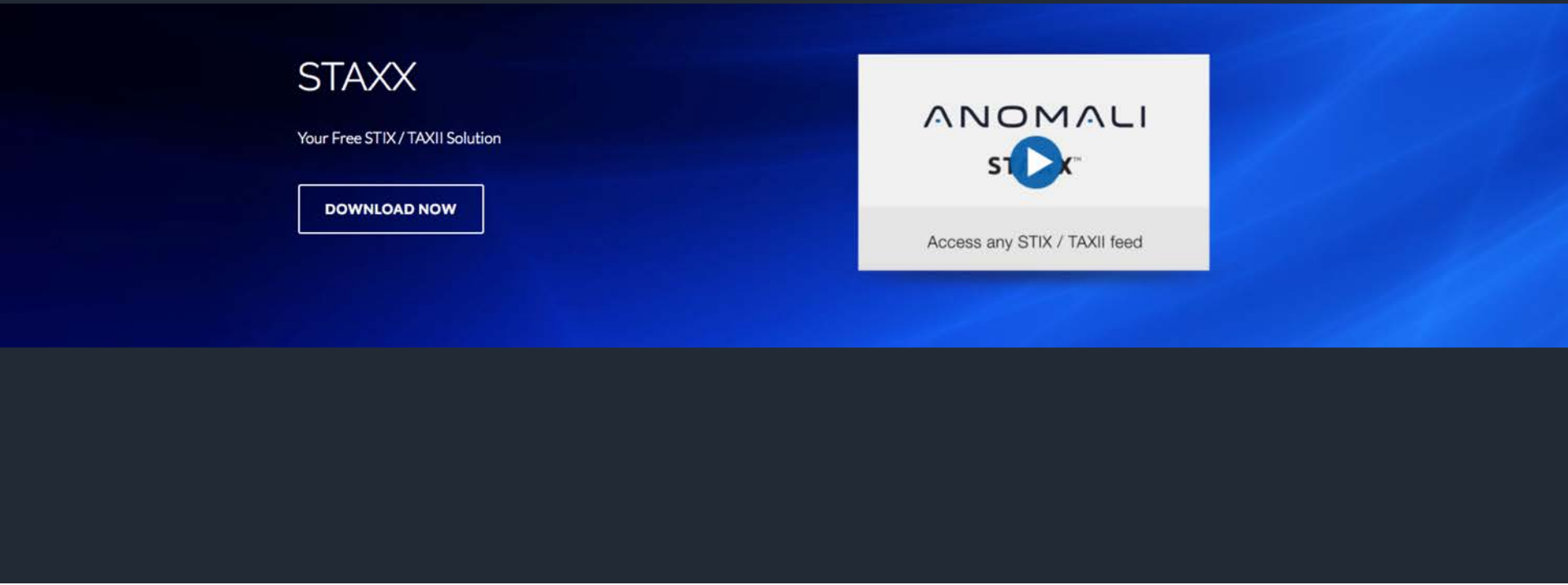


https://crits.github.io

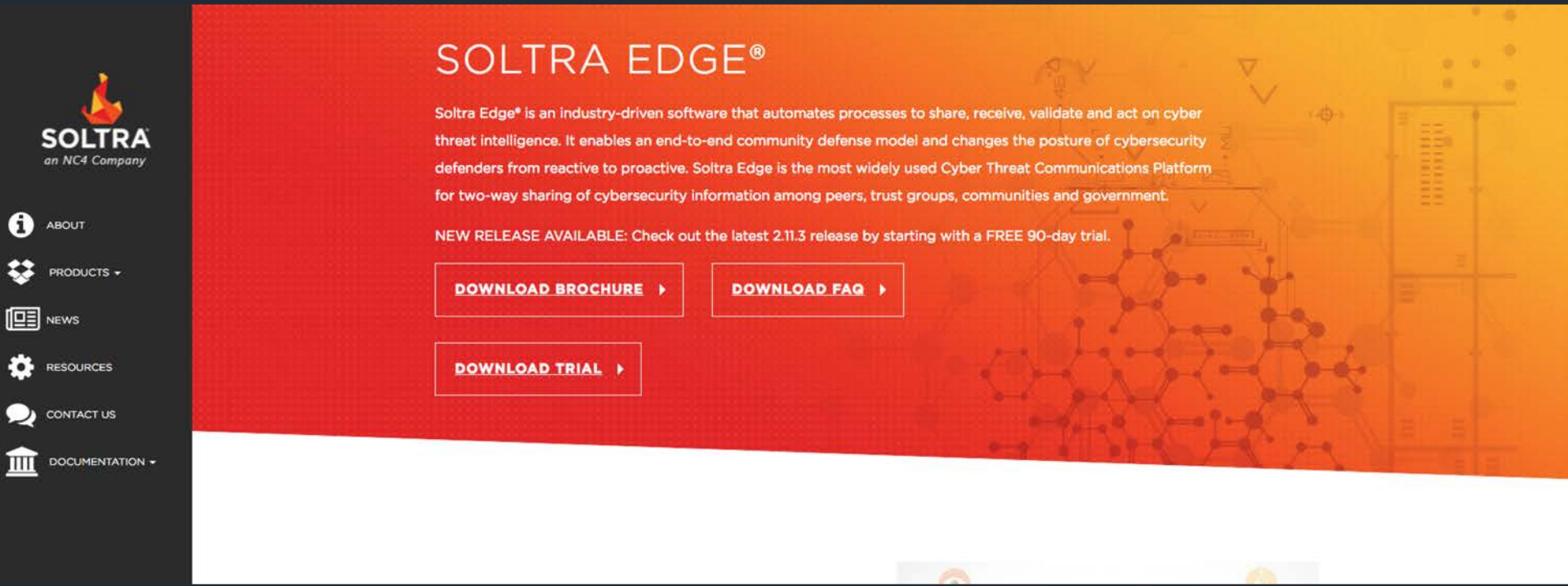
https://github.com/certtools/intelmq



https://www.threatcrowd.org/

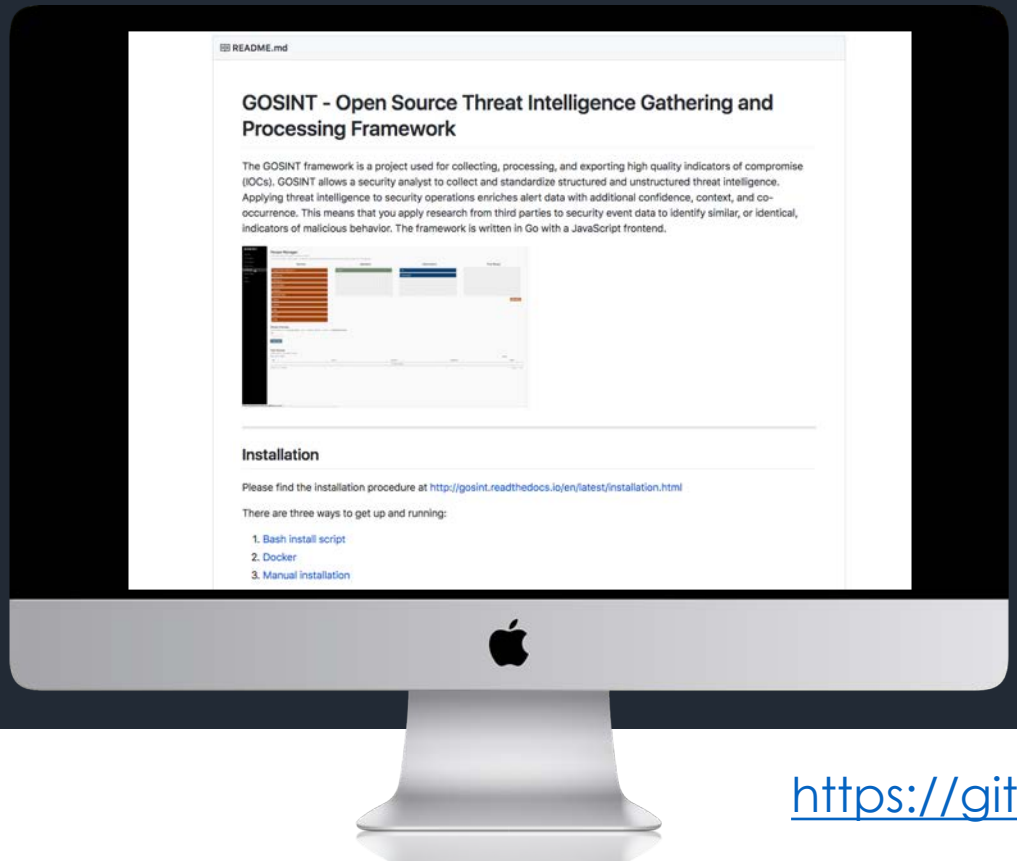


https://www.anomali.com/platform/staxx



http://soltra.com

GOSINT



https://github.com/ciscocsirt/gosint

Cisco Umbrella

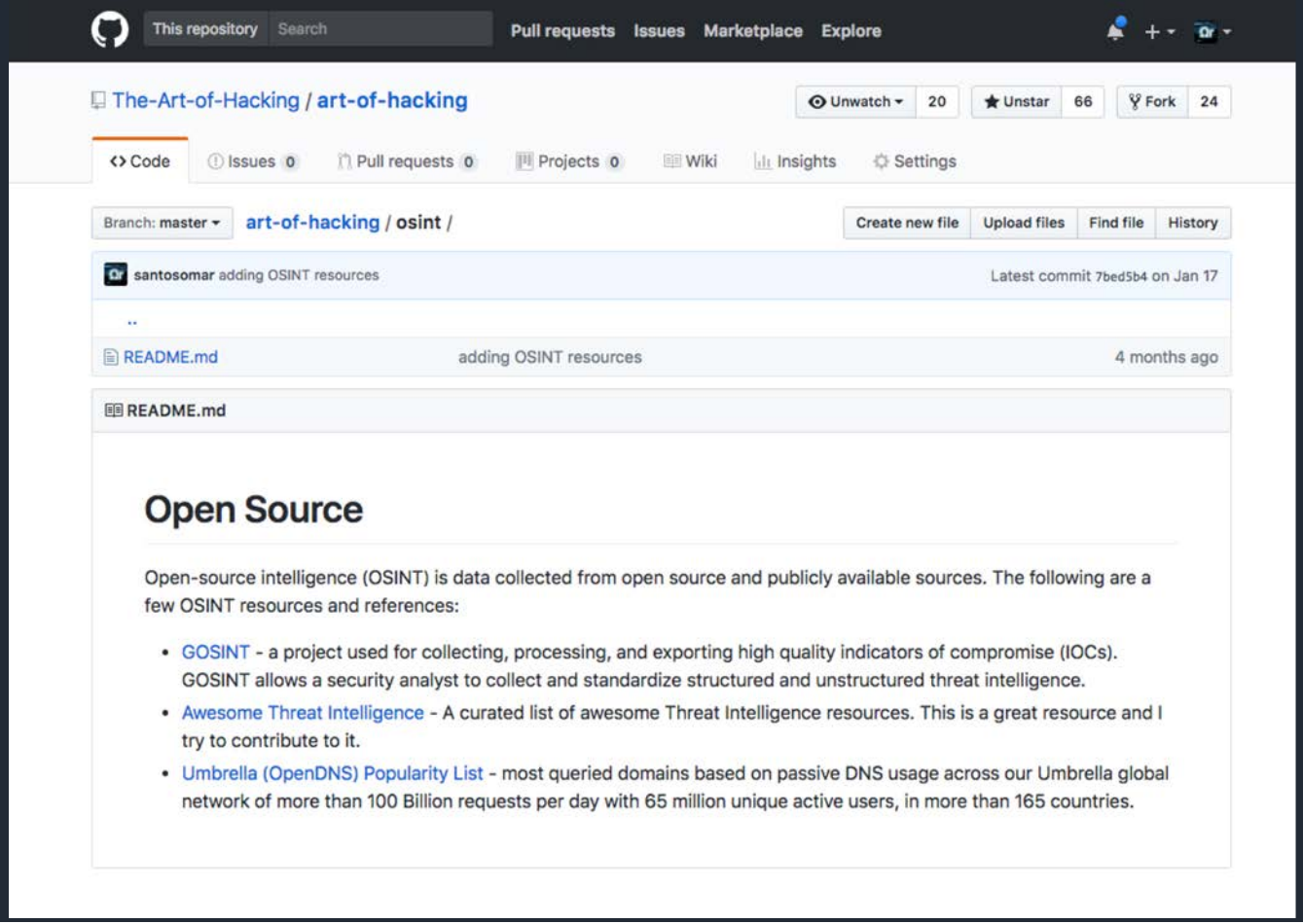
Umbrella Popularity List

The popularity list contains our most queried domains based on passive DNS usage across our Umbrella global network of more than 100 Billion requests per day with 65 million unique active users, in more than 165 countries. Unlike Alexa, the metric is not based on only browser based 'http' requests from users but rather takes in to account the number of unique client IPs invoking this domain relative to the sum of all requests to all domains. In other words, our popularity ranking reflects the domain's relative internet activity agnostic to the invocation protocols and applications where as 'site ranking' models (such as Alexa) focus on the web activity over port 80 mainly from browsers.

As for Alexa, the site's rank is based on combined measure of unique visitors (Alexa users who visit the site per day) and page views (total URL requests from Alexa users for a site). Umbrella popularity lists are generated on a daily basis reflecting the actual world-wide usage of domains by Umbrella global network users and includes root domains, subdomains in addition to TLDs (Alexa list has only this). In addition, Umbrella popularity algorithm also applies data normalization methodologies to smoothen potential biases that may occur in the data due to sampling of the DNS usage data.

Top 1 million
http://s3-us-west-1.amazonaws.com/umbrella-static/top-1m.csv.zip
Top TLDs
http://s3-us-west-1.amazonaws.com/umbrella-static/top-1m-TLD.csv.zip

http://s3-us-west-1.amazonaws.com/umbrella-static/index.html

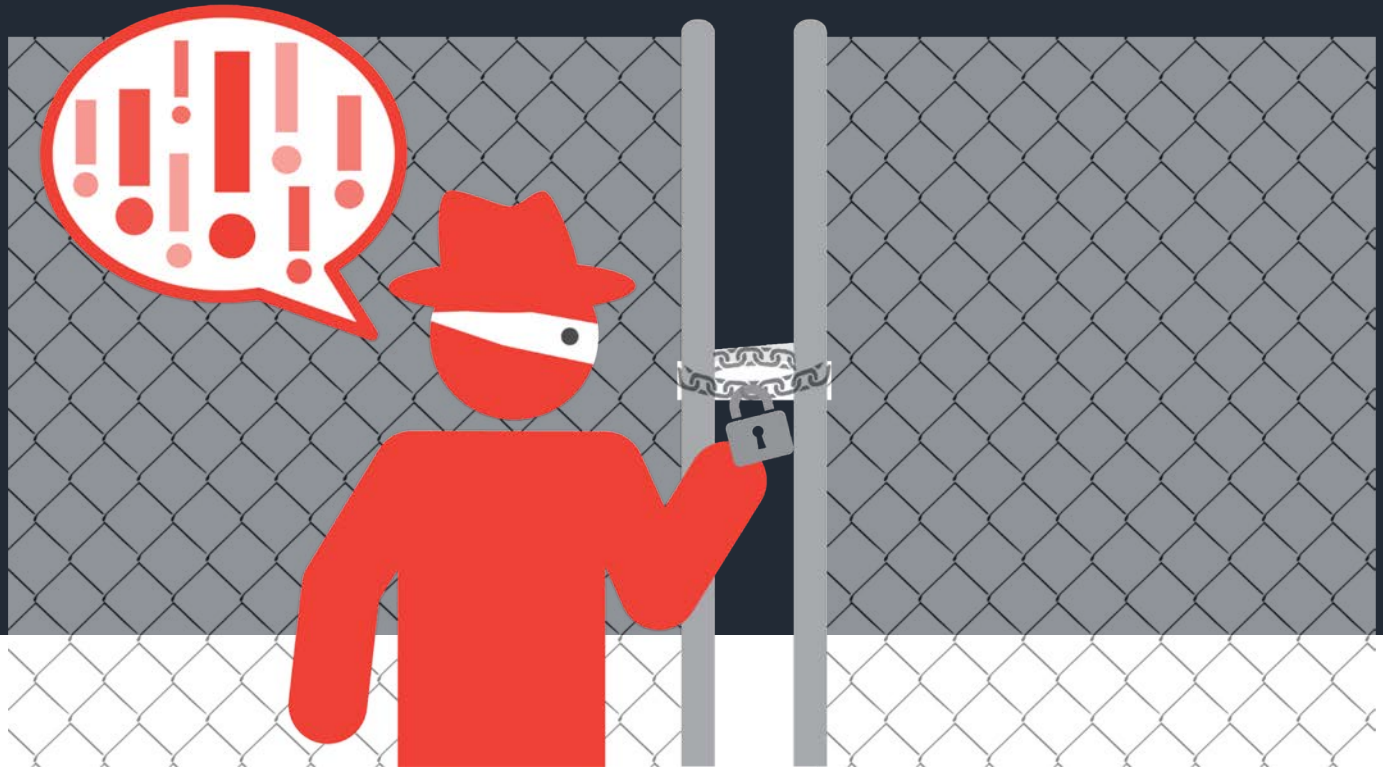


https://github.com/The-Art-of-Hacking/art-of-hacking/tree/master/osint

Enterprise-wide Ethical Hacking and Continuous Monitoring

Before we proceed…

Question: What is the difference between a major breach and a minor breach?



Know where's your critical data!

Monitor and protect it!

Segment your environment!

Penetration Testing

vs

Red Teaming

vs

Vulnerability Management

vs

Continous Monitoring

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!