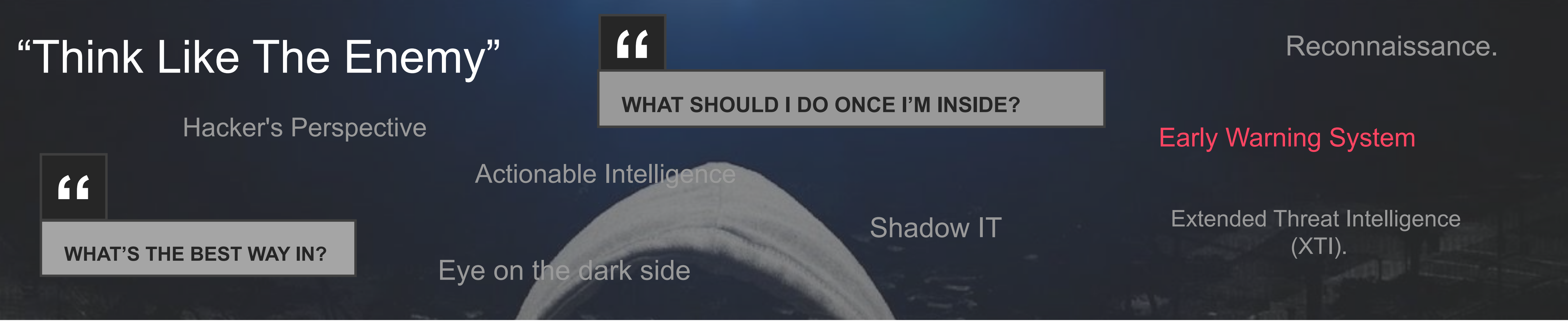


“Think Like The Enemy”

Hacker's Perspective

“ WHAT’S THE BEST WAY IN?

“ WHAT SHOULD I DO ONCE I’M INSIDE?

Actionable Intelligence

Eye on the dark side

Shadow IT

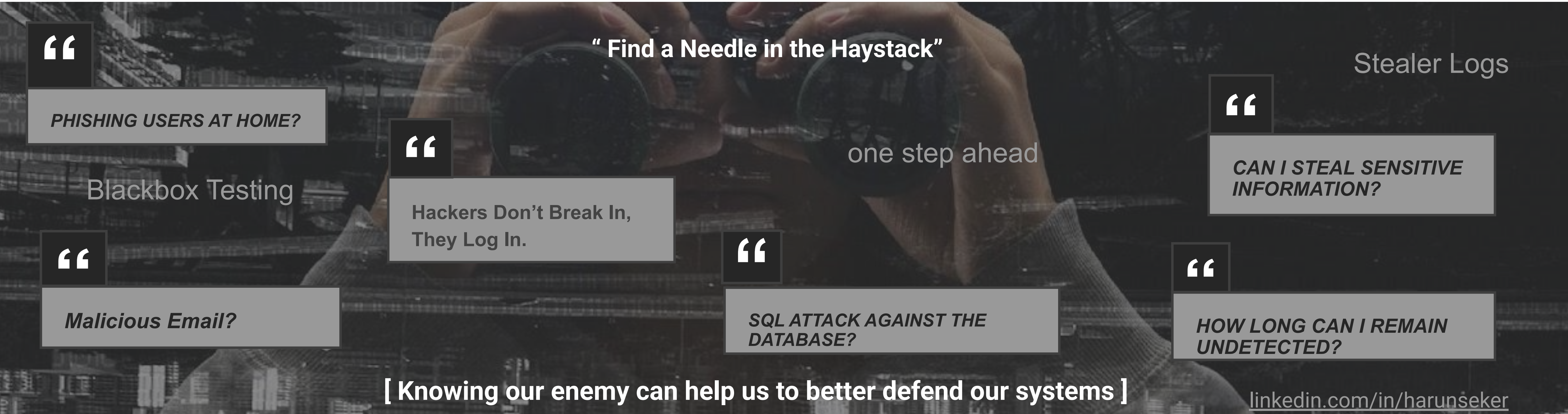
Reconnaissance.

Early Warning System

Extended Threat Intelligence (XTI).

Cyber Threat Intelligence

[A Comprehensive Career Guide]



“ Find a Needle in the Haystack”

“ *PHISHING USERS AT HOME?*

Blackbox Testing

“ *Malicious Email?*

“ Hackers Don’t Break In, They Log In.

one step ahead

“ *SQL ATTACK AGAINST THE DATABASE?*

Stealer Logs

“ *CAN I STEAL SENSITIVE INFORMATION?*

“ *HOW LONG CAN I REMAIN UNDETECTED?*

[Knowing our enemy can help us to better defend our systems]

linkedin.com/in/harunseker

Core Skills required for CTI

1 **Threat Analysis and Research**

- Advanced data analysis techniques
- Proficiency in threat actor profiling
- Ability to identify patterns in complex datasets

2 **Technical Expertise**

- Understanding of networking protocols, firewalls, and intrusion detection systems
- Malware analysis and reverse engineering skills
- Forensic techniques

3 **Communication and Reporting**

- Writing clear and concise intelligence reports
- Translating technical findings for non-technical stakeholders

4 **Continuous Learning**

Staying updated on the latest cybersecurity trends and technologies

5 **AI and Machine Learning**

- Leveraging AI for faster threat detection and predictive capabilities

6 **Cloud Security**

- Expertise in securing multi-cloud environments

7 **IoT Security**

- Understanding vulnerabilities in IoT devices and embedded systems

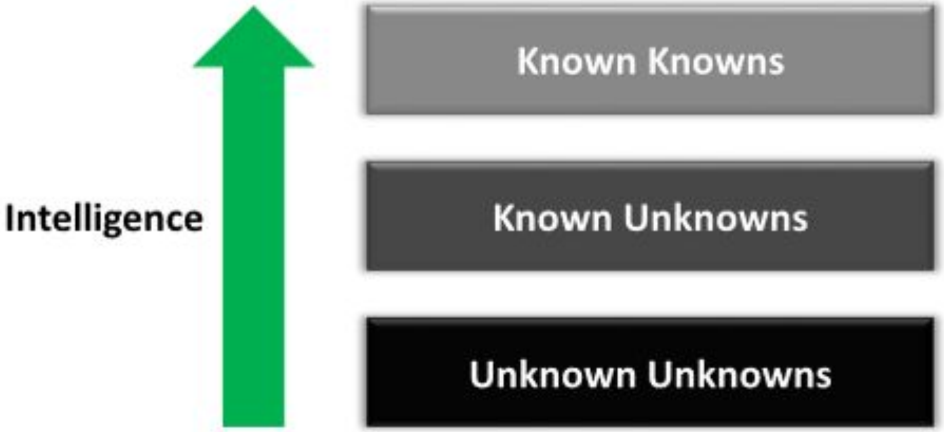
8 **Dark, Deep, and Surface Web Monitoring**

- Proficiency in using specialized tools for dark web monitoring
- Understanding the structure and navigation of the dark web
- Ability to gather and analyze threat intelligence from various web layers
- Knowledge of dark web marketplaces, forums, and communication channels

Key Concepts and Frameworks

● The Intelligence Life Cycle	● SIGMA
● Cyber Kill Chain	● STIX/TAXII : Standardized threat information exchange
● Diamond Model	● Traffic Light Protocol (TLP)
● Pyramid Of Pain	● Logical Fallacies and Cognitive Biases
● Indicators of Compromise - IoCs	● Proactive Threat Hunting ○ Identifying and neutralizing potential threats before they materialize
● MITRE ATT&CK Framework ○ Comprehensive knowledge base of adversary tactics and techniques	● Extended Threat Intelligence (XTI) ○ Integrating broader contextual information for more comprehensive threat analysis.
● Courses of Actions Matrix	● Zero-Trust Principles ○ Implementing security measures that require verification for every user and device
● YARA	

What is Cyber Threat Intelligence?



- The concept of turning "unknown unknowns" into "known knowns" is a crucial aspect of effective threat intelligence and cybersecurity strategy.
- Unknown unknowns represent threats or vulnerabilities that an organization is not aware of and cannot anticipate.
- The goal is to identify these hidden risks and convert them into known threats that can be addressed.

Cyber Threat Intelligence (CTI) is a subfield of cybersecurity that focuses on the structured collection, analysis, and dissemination of data regarding potential or existing cyber threats.

It provides organizations with insights necessary to anticipate, prevent, and respond to cyberattacks by understanding the behavior of threat actors, their tactics, and the vulnerabilities they exploit.

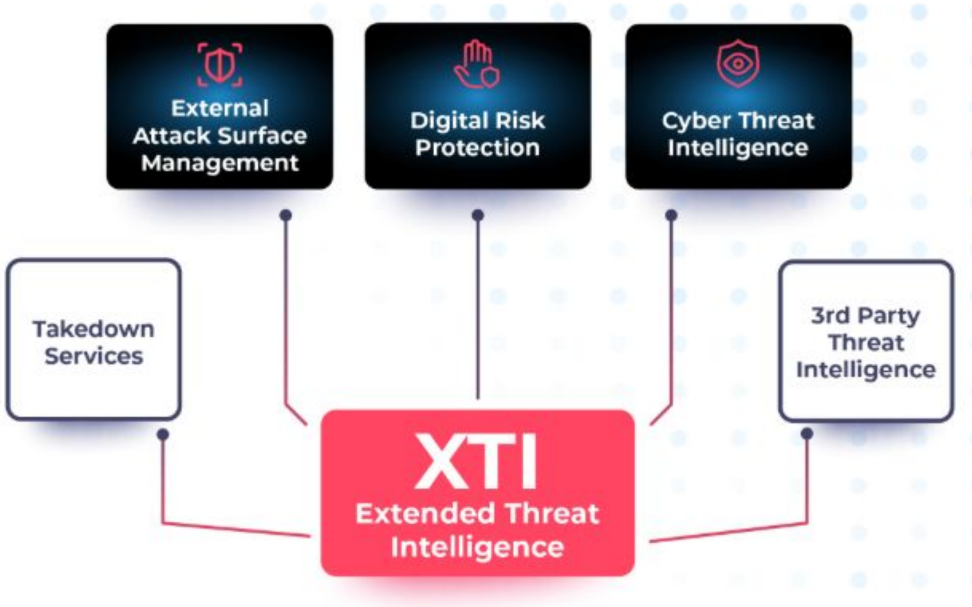
This process involves:

- Continuous monitoring and analysis of the threat landscape
- Proactive threat hunting to uncover hidden risks
- Leveraging advanced technologies and methodologies to identify emerging threats

What is Extended Threat Intelligence?

SOCRadar®

Your Eyes Beyond


External Attack Surface Management
Digital Risk Protection
Cyber Threat Intelligence
Takedown Services
3rd Party Threat Intelligence
XTI
Extended Threat Intelligence

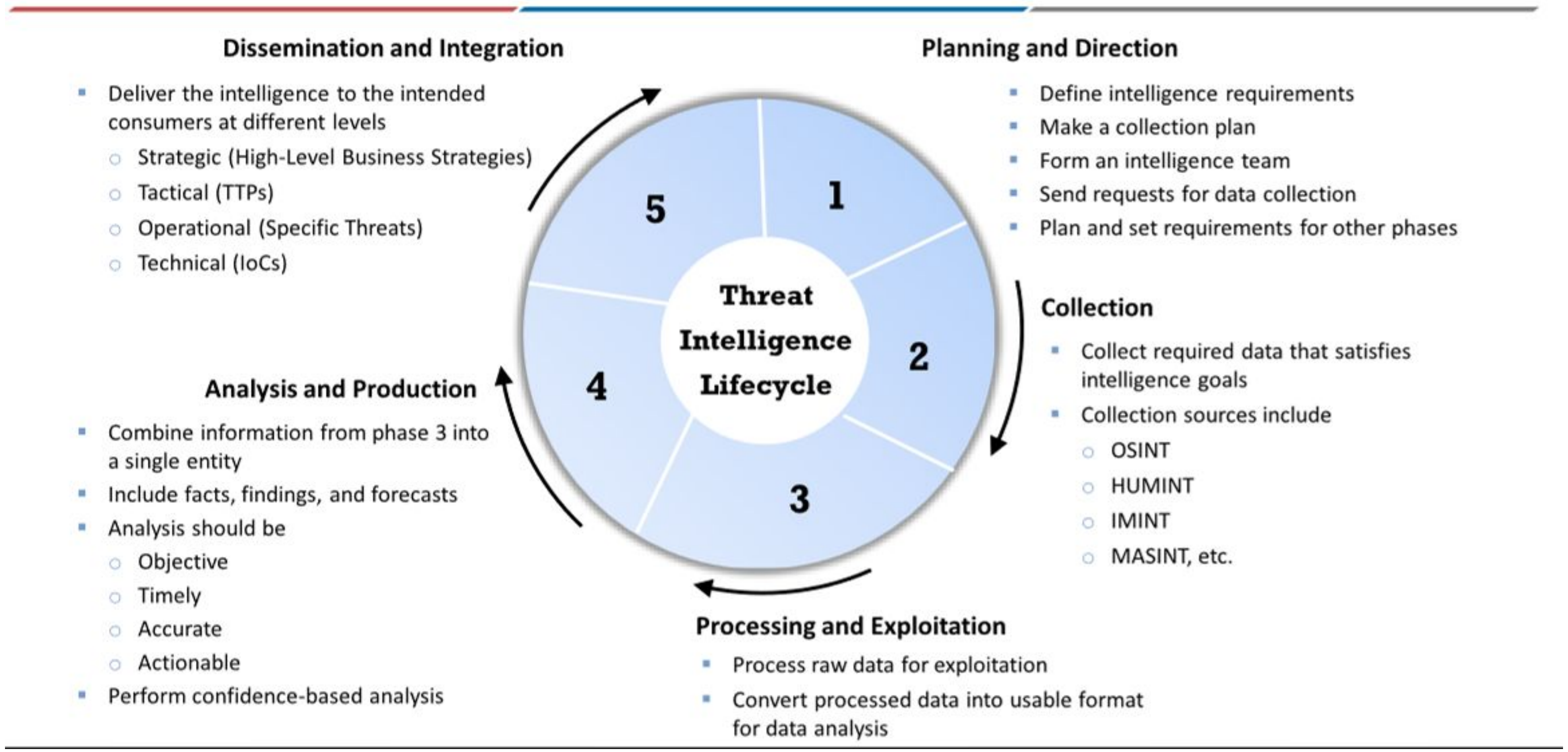
SOCRadar calls their approach Extended Threat Intelligence (XTI) because it combines three key components:

1. Cyber Threat Intelligence (CTI)
2. Digital Risk Protection (DRP)
3. External Attack Surface Management (EASM)

This extended approach aims to provide a more comprehensive and proactive security posture. SOCRadar's philosophy is that providing only threat intelligence is not sufficient for full-fledged proactive security. By combining these three elements, SOCRadar aims to help security teams detect blind spots before attackers can exploit them.

SOCRadar's XTI platform aims to facilitate this process by providing a comprehensive view of an organization's digital footprint, potential vulnerabilities, and emerging threats, thus helping to transform unknown unknowns into actionable intelligence.

The Intelligence Life Cycle



Planning and Direction

- Define intelligence requirements
- Make a collection plan
- Form an intelligence team
- Send requests for data collection
- Plan and set requirements for other phases

Collection

- Collect required data that satisfies intelligence goals
- Collection sources include
  - OSINT
  - HUMINT
  - IMINT
  - MASINT, etc.

Processing and Exploitation

- Process raw data for exploitation
- Convert processed data into usable format for data analysis

Analysis and Production

- Combine information from phase 3 into a single entity
- Include facts, findings, and forecasts
- Analysis should be
  - Objective
  - Timely
  - Accurate
  - Actionable
- Perform confidence-based analysis

Dissemination and Integration

- Deliver the intelligence to the intended consumers at different levels
  - Strategic (High-Level Business Strategies)
  - Tactical (TTPs)
  - Operational (Specific Threats)
  - Technical (IoCs)

A cyclical process consisting of six stages:

1) **Direction/Discovery:** Defining intelligence requirements.

2) **Collection:** Gathering raw data from various sources.

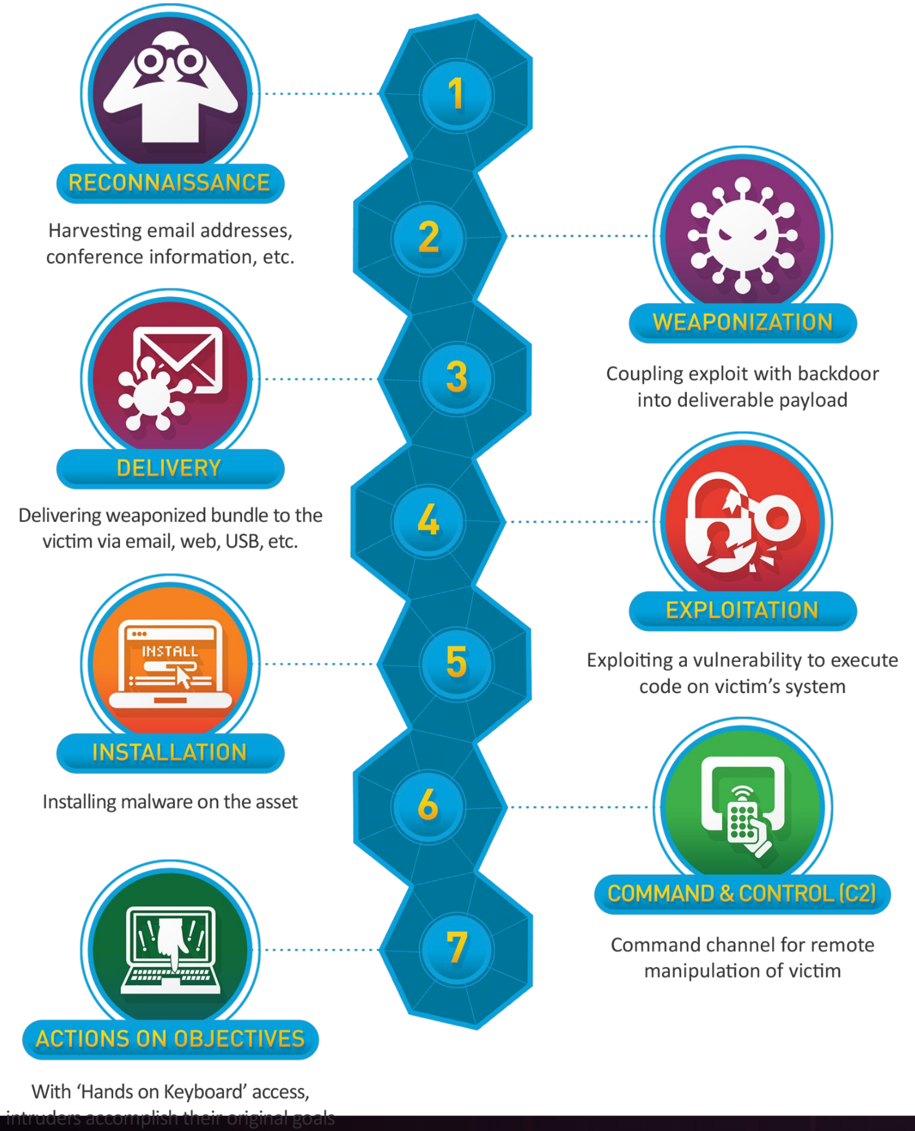
3) **Processing:** Transforming raw data into a usable format.

4) **Analysis:** Interpreting data to produce actionable intelligence.

5) **Dissemination/Action:** Sharing intelligence with stakeholders.

6) **Feedback:** Evaluating the effectiveness of the intelligence and refining the process.

Cyber Kill Chain



1 RECONNAISSANCE
Harvesting email addresses, conference information, etc.

2 WEAPONIZATION
Coupling exploit with backdoor into deliverable payload

3 DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION
Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION
Installing malware on the asset

6 COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

A model developed by Lockheed Martin that describes the stages of a cyber attack: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives. It helps security teams understand and interrupt the attack process.

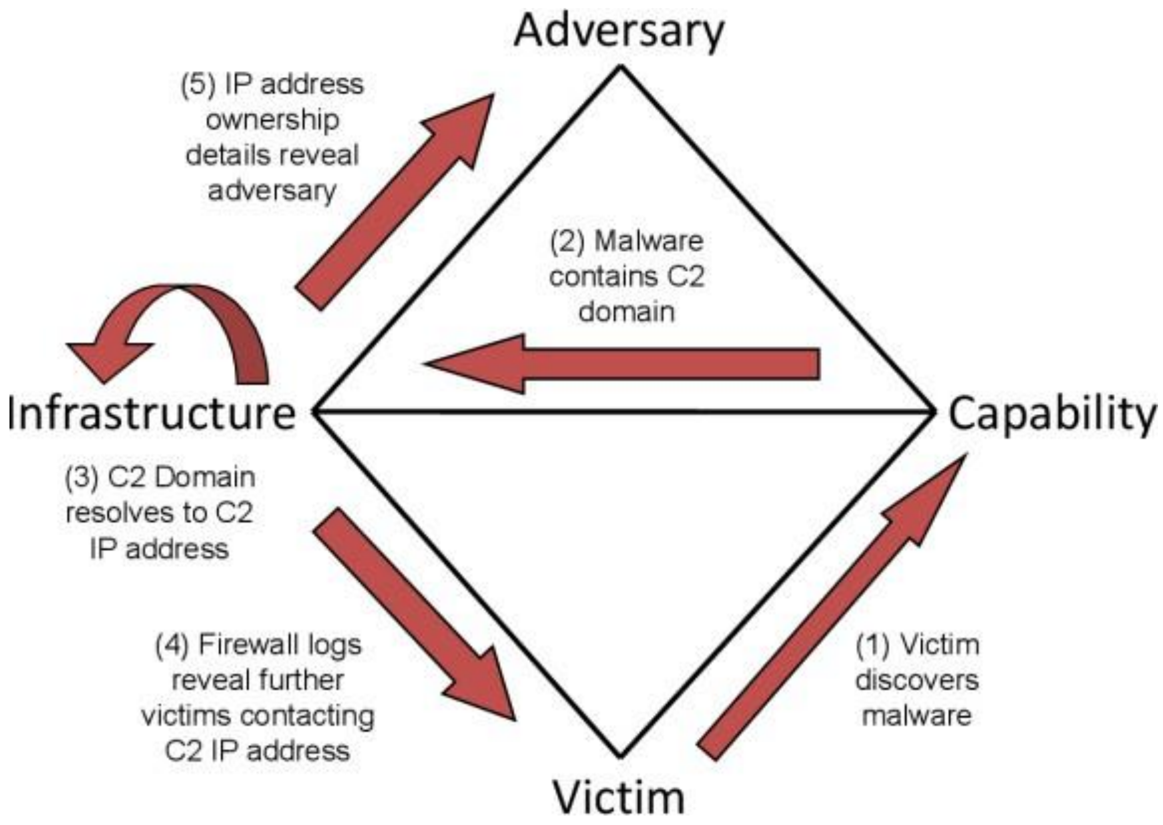
<u>Mnemonics to help remember :</u>

"Real Women Date Engineers In Commando Armor" (RWDEICA)

▶️The Cyber Kill Chain
https://www.youtube.com/watch?v=LqCbpiDyN8o

▶️Breaking The Kill Chain: A Defensive Approach
https://www.youtube.com/watch?v=II91fiUax2g

Diamond Model


Adversary
(5) IP address ownership details reveal adversary
(2) Malware contains C2 domain
Infrastructure
Capability
(3) C2 Domain resolves to C2 IP address
(4) Firewall logs reveal further victims contacting C2 IP address
(1) Victim discovers malware
Victim

A framework for analyzing cyber incidents using four core features: Adversary, Infrastructure, Capability, and Victim. It helps analysts understand the relationships between these elements and provides a comprehensive view of an attack.

📘 "The Diamond Model of Intrusion Analysis" by Sergio Caltagirone, Andrew Pendergast, and Chris Betz.

A comprehensive guide that presents a structured method for analyzing cyber intrusions.

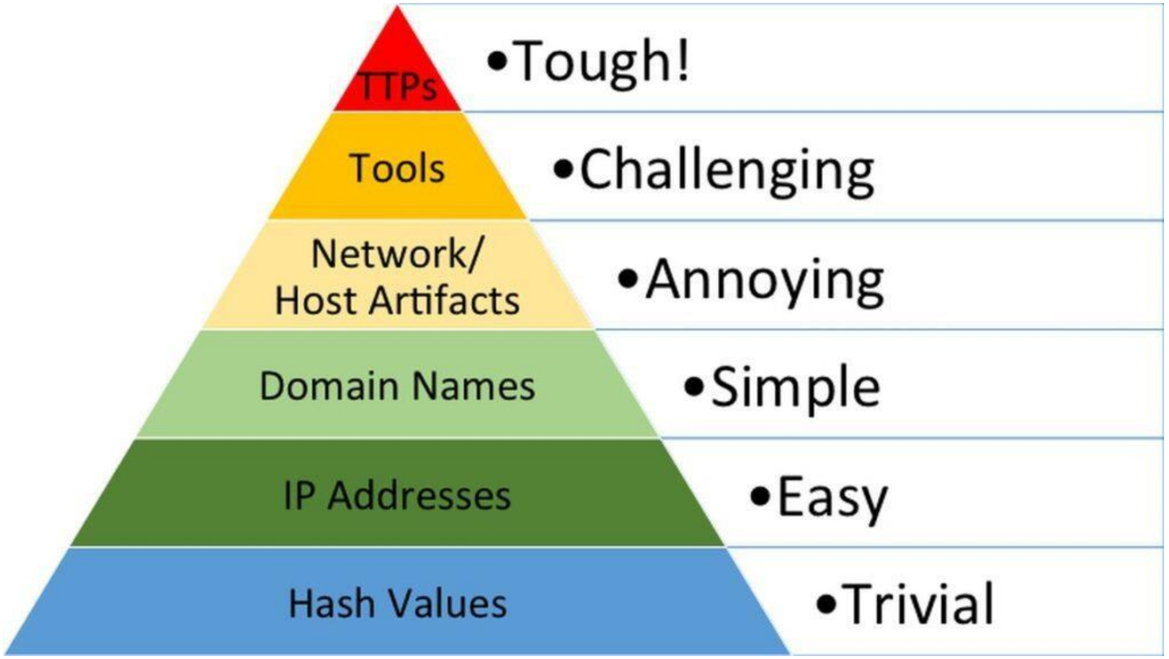
▶️ Diamond Model of Intrusion Analysis - An Overview

https://www.youtube.com/watch?v=3PoQLOJr5WI

▶️ An Introduction to the Diamond Model of Intrusion Analysis by it's Co-Author Sergio Caltagirone

https://www.youtube.com/watch?v=Yb4rg2NbgNw

Pyramid Of Pain

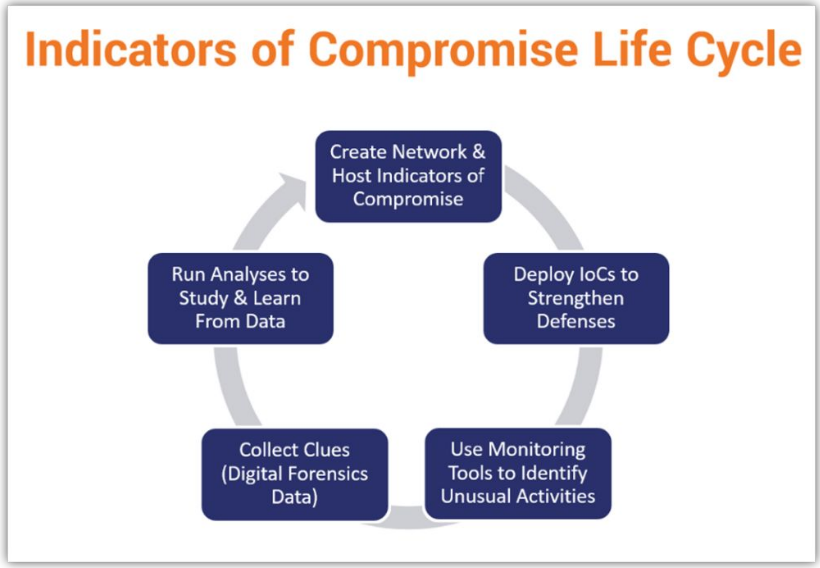


A model that categorizes indicators of compromise (IOCs) based on the difficulty they pose to attackers when changed. From easiest to hardest:Hash Values, IP Addresses, Domain Names, Network/Host Artifacts, Tools, Tactics, Techniques, and Procedures (TTPs).

▶️Finding The MOST Valuable Data - The Pyramid Of Pain Explained https://www.youtube.com/watch?v=O7PSKrgdHAI

▶️ The Secret Origins of the Pyramid of Pain https://www.youtube.com/watch?v=3Xrl6ICxKxI

Indicators of Compromise - IoCs



Indicators of Compromise Life Cycle

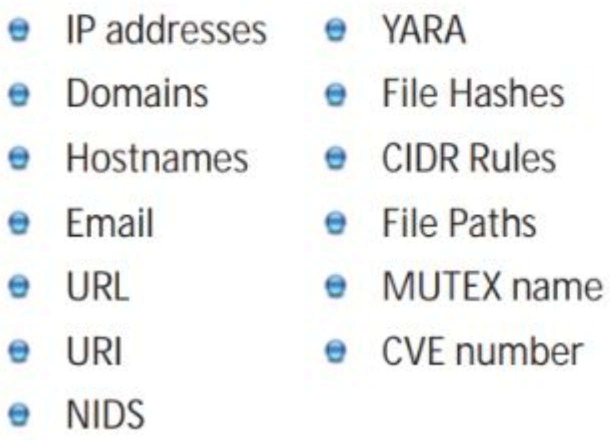
Create Network & Host Indicators of Compromise

Deploy IoCs to Strengthen Defenses

Use Monitoring Tools to Identify Unusual Activities

Collect Clues (Digital Forensics Data)

Run Analyses to Study & Learn From Data



- IP addresses
- Domains
- Hostnames
- Email
- URL
- URI
- NIDS
- YARA
- File Hashes
- CIDR Rules
- File Paths
- MUTEX name
- CVE number

Indicators of Compromise (IoCs) are critical artifacts or evidence that suggest a breach or malicious activity has occurred within an information system. They serve as signals of potential cyber threats and can take various forms, including:

- File Hashes
- IP Addresses
- Domain Names
- URLs
- Email Addresses
- Registry Keys
- Network traffic patterns

IoCs help cybersecurity professionals to detect, respond to, and mitigate cyber threats effectively.

▶️Understanding Indicators of Compromise for Incident Response

https://www.youtube.com/watch?v=zs-AEaSd2vk

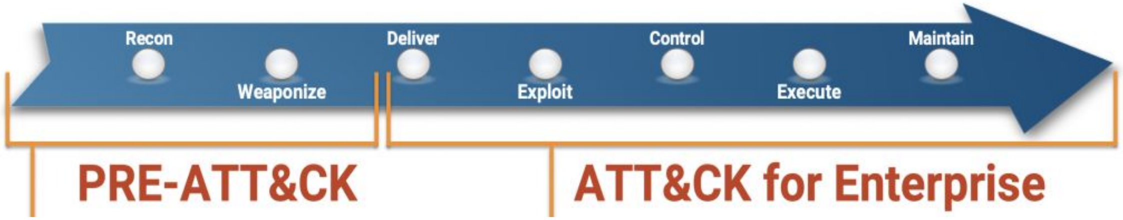
▶️ Pyramid of Pain and Indicator of compromise

https://www.youtube.com/watch?v=nQXtAv7EDrw

MITRE ATT&CK

MITRE ATT&CK is a guide that helps people understand and stop computer hackers by listing the different methods these hackers use. It's like a playbook that shows how to catch and block the bad guys in the digital world.interactive mitre attack framework. According to the latest information from the MITRE ATT&CK framework, as of April 2024 (version 15), the framework contains:

- 14 Tactics
- 202 Techniques
- 435 Sub-Techniques



A globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. It provides a common language for describing cyber attacks and helps organizations improve their security posture.

📘 "MITRE ATT&CK™: Design and Philosophy" by Blake Strom, et al.

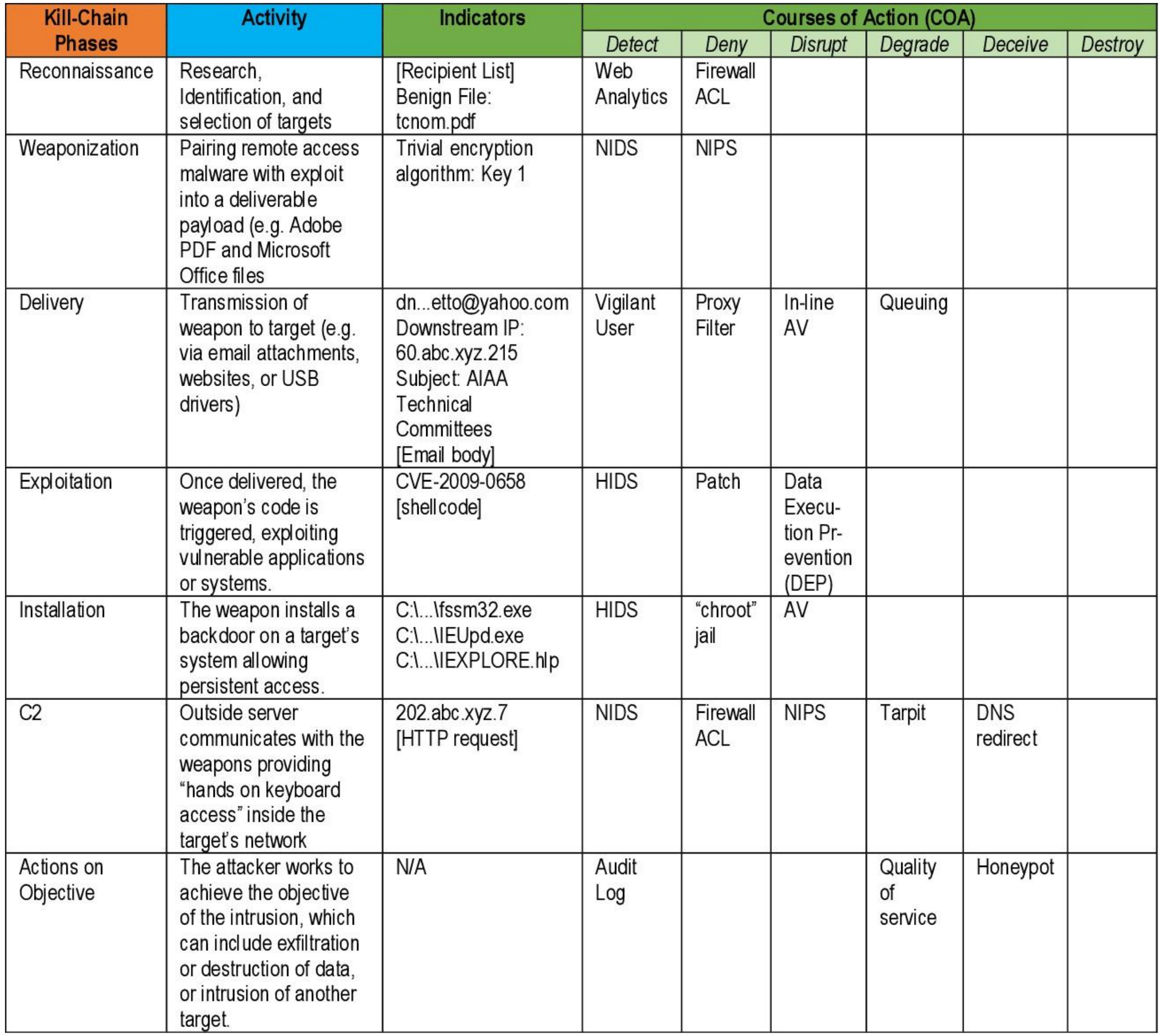
A thorough exploration of the MITRE ATT&CK framework.

▶️ The Anatomy of an ATT&CK https://www.youtube.com/watch?v=2icKi2q6NS4

▶️ MITRE ATT&CK Framework for Beginners https://www.youtube.com/watch?v=GYyLnff2XRo

▶️ Workshop: MITRE ATT&CK Fundamentals https://www.youtube.com/watch?v=1cCt2XZr2ms

Courses of Action Matrix



Kill-Chain Phases	Activity	Indicators	Courses of Action (COA)					
			Detect	*Deny*	*Disrupt*	*Degrade*	*Deceive*	*Destroy*
Reconnaissance	Research, Identification, and selection of targets	[Recipient List] Benign File: tcnom.pdf	Web Analytics	Firewall ACL				
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files	Trivial encryption algorithm: Key 1	NIDS	NIPS				
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drivers)	dn...etto@yahoo.com Downstream IP: 60.abc.xyz.215 Subject: AIAA Technical Committees [Email body]	Vigilant User	Proxy Filter	In-line AV	Queuing		
Exploitation	Once delivered, the weapon’s code is triggered, exploiting vulnerable applications or systems.	CVE-2009-0658 [shellcode]	HIDS	Patch	Data Execution Prevention (DEP)			
Installation	The weapon installs a backdoor on a target’s system allowing persistent access.	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEXPLORE.hlp	HIDS	“chroot” jail	AV			
C2	Outside server communicates with the weapons providing “hands on keyboard access” inside the target’s network	202.abc.xyz.7 [HTTP request]	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target.	N/A	Audit Log			Quality of service	Honeypot	

A tool used to map out potential responses to different types of cyber threats. It helps organizations prepare and quickly respond to various attack scenarios.

📘 Courses of Action Matrix in Cyber Threat Intelligence

https://warnerchad.medium.com/courses-of-action-matrix-in-cyber-threat-intelligence-82bf49243e46

YARA

A tool used to create pattern-matching rules for malware detection. It allows analysts to create descriptions of malware families based on textual or binary patterns.

▶️ What are Yara Rules (and How Cybersecurity Analysts Use Them)

https://www.youtube.com/watch?v=BM23_H2GGMA

📘 Writing YARA rules

https://yara.readthedocs.io/en/stable/writingrules.html

SIGMA

Sigma is a generic and open signature format that allows you to describe relevant log events straightforwardly. The rule format is flexible, accessible to write, and applicable to any log file. The primary purpose of this project is to provide a vendor-neutral structured format in which researchers or analysts can describe their detection methods and make them shareable with others, which can be converted using the online resource uncoder.io and applied to different SIEMs and detection platforms.

https://github.com/Neo23x0/sigma

https://github.com/SigmaHQ/sigma

▶️ Getting Started With Sigma Rules :

https://www.youtube.com/watch?v=dwEOmAa2LK8

📘 Creating Effective Sigma Rules with AI:

https://www.youtube.com/watch?v=d5089LlPtRY&t=3s

STIX / TAXII

STIX (Structured Threat Information eXpression) is a standardized language for sharing threat intelligence. TAXII (Trusted Automated eXchange of Intelligence Information) is the protocol used to exchange STIX data between parties.

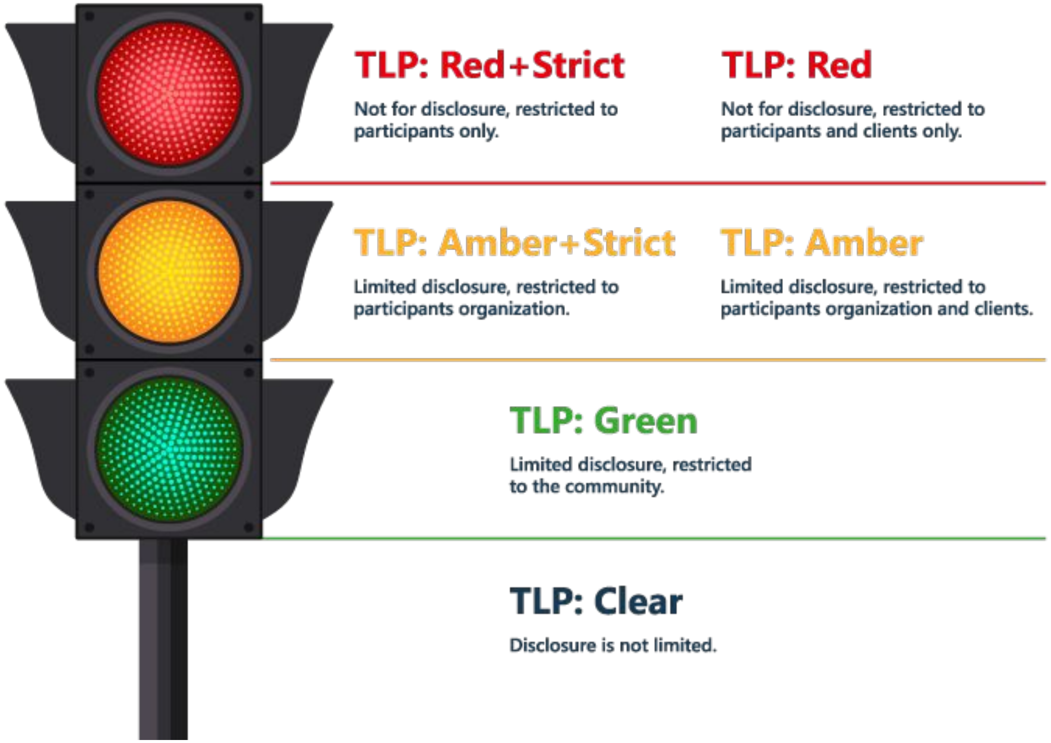
▶️ What Are STIX/TAXII? https://www.youtube.com/watch?v=L7Ykky6Ntd0

▶️ Introduction To STIX/TAXII 2 Standards https://www.youtube.com/watch?v=qAb7hL0HQ2M

📘 What are STIX/TAXII? https://www.anomali.com/resources/what-are-stix-taxii

📘 How STIX, TAXII and CybOX Can Help With Standardizing Threat Information https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information

Traffic Light Protocol (TLP)



TLP: Red+Strict

Not for disclosure, restricted to participants only.

TLP: Red

Not for disclosure, restricted to participants and clients only.

TLP: Amber+Strict

Limited disclosure, restricted to participants organization.

TLP: Amber

Limited disclosure, restricted to participants organization and clients.

TLP: Green

Limited disclosure, restricted to the community.

TLP: Clear

Disclosure is not limited.

https://envisionit.com/resources/articles/the-traffic-light-protocol-simplifying-sensitivity-labels-in-microsoft-365

A set of designations used to ensure that sensitive information is shared with the appropriate audience.

It uses four colors: RED (restricted), AMBER (limited disclosure), GREEN (community-wide), and WHITE (unlimited).

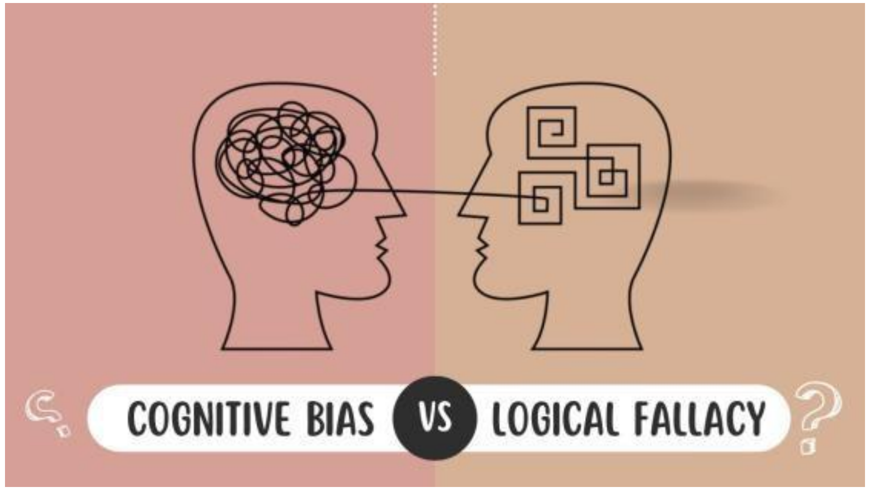
▶️ How to protect secrets

https://www.youtube.com/watch?v=h6IpyZ-YCPs

📘 Traffic Light Protocol (TLP) Definitions and Usage

https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage

Logical Fallacies and Cognitive Biases



Understanding these helps analysts avoid errors in reasoning. Common biases in CTI include confirmation bias (seeking information that confirms existing beliefs) and anchoring bias (relying too heavily on one piece of information).

▶️ Deconstructing the Analyst Mindset https://www.youtube.com/watch?v=Qy-19aRN58M

▶️ 12 Cognitive Biases Explained https://www.youtube.com/watch?v=wEwGBIr_RIw

▶️ 31 logical fallacies in 8 minutes https://www.youtube.com/watch?v=Qf03U04rqGQ

▶️ The Most Common Cognitive Bias https://www.youtube.com/watch?v=vKA4w2O61Xo

Proactive Threat Hunting

PROACTIVE VS REACTIVE

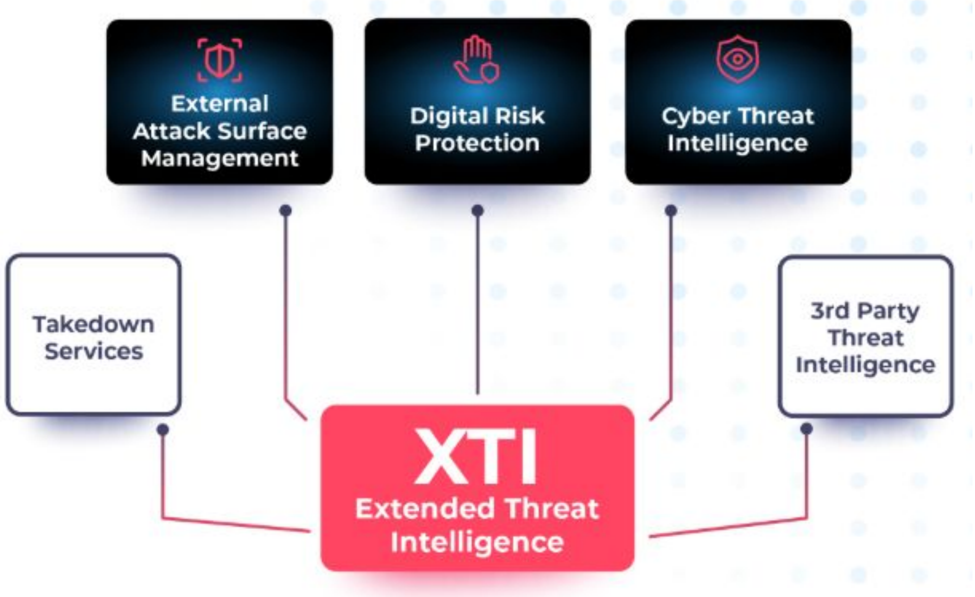
creating or controlling a situation by responding to it before it has happened.**(predictive)**

acting in response to a situation rather than creating or controlling it.

"a proactive rather than a reactive approach"

Identifying and neutralizing potential threats **before** they materialize. A cybersecurity practice that actively searches for hidden threats within a network, rather than waiting for alerts. It involves hypothesis-driven investigations and advanced analytics to uncover sophisticated attacks.

Extended Threat Intelligence (XTI)

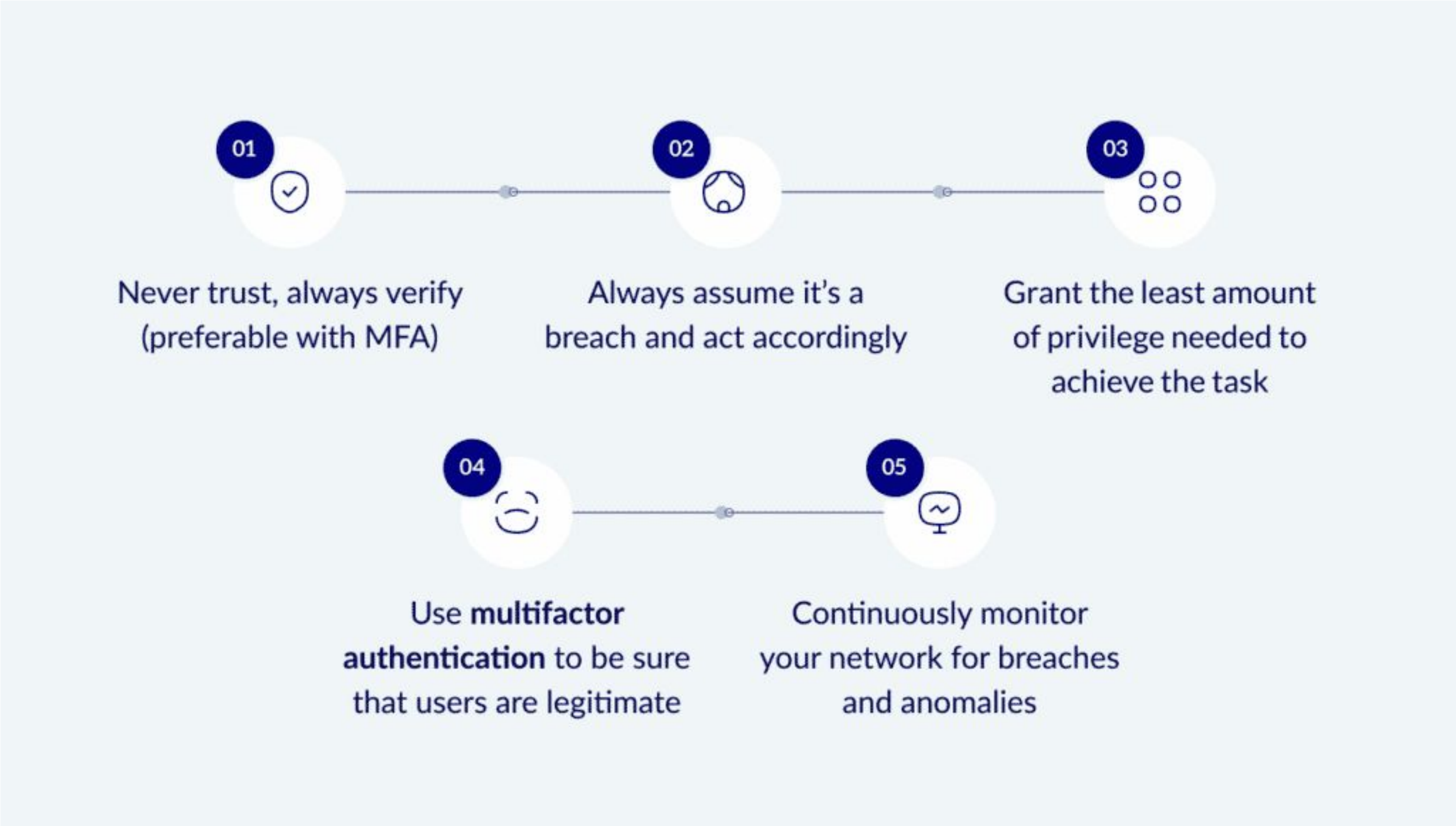

External Attack Surface Management
Digital Risk Protection
Cyber Threat Intelligence
Takedown Services
3rd Party Threat Intelligence
XTI
Extended Threat Intelligence

As an Extended Threat Intelligence (XTI) platform and inventor of the concept, **SOCRadar**'s approach is to effectively combine Cyber Threat Intelligence (CTI), Digital Risk Protection (DRP) External Attack Surface Management (EASM) and Supply Chain Intelligence .

An approach that integrates traditional CTI with broader contextual information, including geopolitical factors, industry trends, and emerging technologies, to provide a more comprehensive threat landscape analysis.

Company Website: https://socradar.io/
Gartner Peer Insights:
https://www.gartner.com/reviews/market/security-threat-intelligence-services/vendor/socradar
Other ThreatIntel Products - Gartner:
https://www.gartner.com/reviews/market/security-threat-intelligence-services

Zero-Trust Principles



01 Never trust, always verify (preferable with MFA)

02 Always assume it's a breach and act accordingly

03 Grant the least amount of privilege needed to achieve the task

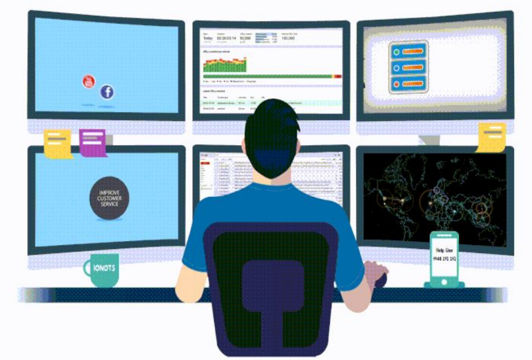
04 Use **multifactor authentication** to be sure that users are legitimate

05 Continuously monitor your network for breaches and anomalies

A security model that assumes no user, device, or network is trusted by default.

It requires continuous verification and applies the principle of least privilege access, enhancing overall security posture.

https://zeronetworks.com/blog/what-is-zero-trust-security-without-the-marketing-bs



Key Responsibilities of a CTIA

Cyber Threat Intelligence Analyst

OPENCTI

LevelBlue Labs

MISP Threat Sharing

A Cyber Threat Intelligence Analyst plays a crucial role in safeguarding organizations from cyber threats by collecting, analyzing, and reporting on threat data. Here are the key responsibilities of a Cyber Threat Intelligence Analyst:

Data Collection: Gather raw data from various sources, including the dark web, intelligence feeds, and other intelligence sources.	**Problem Solving:** Develop innovative solutions to complex security problems, often requiring a creative approach to threat mitigation.
Threat Analysis: Analyze collected data to understand the technical aspects of security and assess the level of threat posed by attacks.	**Continuous Learning:** Stay updated with the latest cybersecurity trends, threats, and technologies to enhance threat detection and response capabilities.
Threat Monitoring: Continuously monitor indicators of compromise (IOCs) and assess potential threats to the organization's networks and data.	**Business Risk Identification:** Identify business risks and refine information into intelligence that is disseminated to higher-level business executives.
Intelligence Reporting: Prepare and present intelligence reports that highlight key findings and propose counteractions to mitigate threats.	**Understanding Adversaries:** Understand the motive of adversaries by analyzing the characteristics and habits of threat actors.
Threat Prioritization: Prioritize threats based on severity and potential impact, focusing on the most critical ones.	**Guide Defense Strategies:** Guide organizations in building effective defense and mitigation strategies.
Collaboration and Communication: Collaborate with IT, incident handling, and SOC teams by generating timely threat reports and effectively communicating findings and recommendations to stakeholders.	**Extracting Threat Intelligence:** Extract threat intelligence that includes contextual information, IOCs, TTPs, consequences, and actionable intelligence about evolving threats.
Technical Proficiency: Utilize various tools and frameworks such as SIEM tools, threat intelligence platforms, and threat intelligence frameworks like MITRE ATT&CK.	**Stay Ahead of Adversaries:** Stay ahead of adversaries by understanding the latest attack TTPs (Tactics, Techniques, and Procedures).

CTI Books

List of general Cyber Threat Intelligence (CTI) books highly recommended for 2025:

📖 "Cyber Threat Intelligence 101" by Gary Ruddell

📖 "Visual Threat Intelligence: An Illustrated Guide For Threat Researchers" by Thomas Roccia

📖 "The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage" by Cliff Stoll

📖 "Structured Analytic Techniques for Intelligence Analysis, 3rd ed." by Randolph H. Pherson and Richards J. Heuer Jr.

📖 "Psychology of Intelligence Analysis" by Richards J. Heuer Jr.

📖 "The Art and Science of Intelligence Analysis" by Julian Richards

📖 "Cyber for Builders: The Essential Guide to Building a Cybersecurity Startup" by Yoav Haleliuk[3]

📖 "Operationalizing Threat Intelligence: A Guide to Developing and Operationalizing Cyber Threat Intelligence Programs"

📖 "Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers" by Andy Greenberg

📖 "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon" by Kim Zetter

Highly recommended videos CTI Videos

1. SOCRadar YouTube channel is likely an extension of their efforts to educate and engage with their audience about cybersecurity topics, while also promoting their Extended Threat Intelligence platform and services.https://www.youtube.com/@SOCRadar
2. ▶️ The Cycle of Cyber Threat Intelligence https://www.youtube.com/watch?v=J7e74QLVxCk
   This video by SANS Institute provides a comprehensive overview of the CTI process and remains a valuable resource.
3. ▶️ Job Role Spotlight: Cyber Threat Intelligence https://www.youtube.com/watch?v=fvYb5-NxoDc
   Amy Bejtlich's insights into the CTI career path are still relevant and informative.
4. ▶️How to become a Cyber Threat Intel analyst: https://www.youtube.com/watch?v=3KFHOamRl-s
   Gary Ruddell provides practical advice on entering the CTI field, making it an excellent resource for beginners.
5. ▶️Mastering Cyber Threat Intelligence: Top Techniques!: https://www.youtube.com/watch?v=4gCVolbDLVo
   This video by Skillweed covers key strategies and best practices in CTI, suitable for both beginners and professionals.
6. ▶️Crash Course on Cyber Threat Intelligence / CTI: https://www.youtube.com/watch?v=O47mVizGlcI
   This comprehensive compilation from TryHackMe's SOC Level 1 pathway provides a thorough overview of CTI topics.
7. ▶️ Threat Hunting Masterclass-Techniques, Tools, and Tips for Beginners:
   https://www.youtube.com/watch?v=y-kFIJ9-eaw
   While focused on threat hunting, this masterclass covers many aspects of CTI that are valuable for analysts.

Top 10 Free Cyber Threat Intelligence Courses

1. MITRE ATT&CK for Cyber Threat Intelligence Training: https://attack.mitre.org/resources/training/cti/
   This comprehensive training by MITRE is highly regarded in the industry and covers essential aspects of using the ATT&CK framework for CTI5.
2. Cyber Threat Intelligence (IBM) on Coursera: https://www.coursera.org/learn/ibm-cyber-threat-intelligence
   Offered by IBM, this course provides a solid foundation in CTI concepts and practices.
3. TryHackMe Cyber Threat Intelligence Module: https://tryhackme.com/module/cyber-threat-intelligence
   TryHackMe offers hands-on, practical learning experiences in CTI4.
4. Cybrary's Intro to Cyber Threat Intelligence: https://www.cybrary.it/course/intro-cyber-threat-intelligence
   This course provides a good introduction to CTI concepts and practices.
5. SANS Cyber Threat Intelligence Course (Free Version): https://www.sans.org/cyber-security-courses/cyber-threat-intelligence/
   While SANS courses are typically paid, they occasionally offer free versions or trials of their CTI course.
6. Mandiant Cyber Threat Intelligence Training (Free Modules): https://www.mandiant.com/academy
   Mandiant offers some free CTI training modules as part of their academy.
7. Recorded Future's Threat Intelligence Grading System (TIGS) Course: https://www.recordedfuture.com/training
   Recorded Future provides free access to their TIGS course, which is valuable for CTI analysts.
8. MISP (Malware Information Sharing Platform) Training Materials: https://www.misp-project.org/documentation/
   MISP offers free training materials for their open-source threat intelligence platform.
9. Open CTI Training Resources: https://www.opencti.io/en/resources
   Open CTI provides free resources and documentation for learning about their open-source CTI platform.
10. OSINT Framework Resources: https://osintframework.com/
    While not a course per se, this collection of OSINT tools and resources is invaluable for CTI analysts and offers opportunities for self-directed learning.

Top 10 Threat Intelligence Certifications

1. CTIA: Certified Threat Intelligence Analyst by EC-Council https://www.eccouncil.org/train-certify/certified- threat-intelligence-analyst-ctia
2. GCTI: GIAC Cyber Threat Intelligence https://www.giac.org/certifications/cyber-threat-intelligence-gcti
3. RCIA – Rocheston Cyberthreat Intelligence Analyst: https://www.rocheston.com/certification/Cyberthreat-Intelligence-Analyst/
4. CCTIA by the NICCS – Certified Cyber Threat Intelligence Analyst :

   https://niccs.us-cert.gov/training/search/cybertraining-365/certified-cyber-threat-intelligence-analyst
5. CTI (Center for TI) Certificates: https://www.centerforti.com/certifications
6. The Certified Threat Intelligence Analyst – Cyber Intelligence Tradecraft:

   https://www.treadstone71.com/index.php/cyber-intelligence-training/cyber-intelligence-tradecraft-certification
7. The OSINT Pathfinder Programme: https://arnoreuser.com/
8. CPTIA – CREST Practitioner Threat Intelligence Analyst:

   https://www.crest-approved.org/examination/crest-practitioner-threat-intelligence-analyst/index.html
9. CRTIA – CREST Registered Threat Intelligence Analyst:

   https://crest-approved.org/examination/crest-registered-threat-intelligence-analyst/index.html
10. CCTIM – CREST Certified Threat Intelligence Manager:

    https://crest-approved.org/examination/crest-certified-threat-intelligence-manager/index.html

Top 10 Threat Intelligence Conferences to Attend in 2025

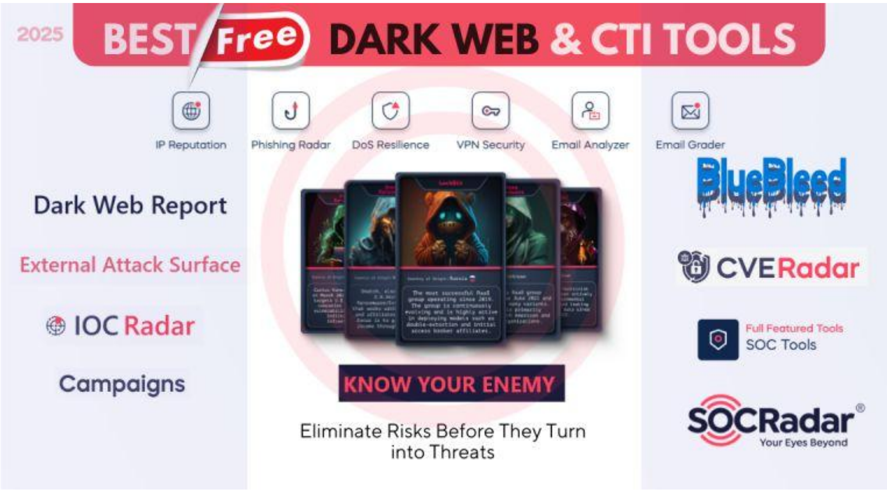
1. SANS Cyber Threat Intelligence Summit & Training 2025 (January 27 to February 3):
   https://www.sans.org/cyber-security-training-events/cyber-threat-intelligence-summit-2025/
2. 4th IEEE International Conference on AI in Cybersecurity (ICAIC) (February 5-7):
   https://icaic-conferences.ca
3. Zero Trust World 2025 (February 19-21):
   Registration link not provided in the search results.
4. Black Hat USA 2025 (August 3-8):
   https://blackhat.informatech.com/usa/2025/ (inferred based on the Asia link)
   Black Hat Asia 2025 (April 1-4):
   https://blackhat.informatech.com/asia/2025/5
5. Innovate Cybersecurity Summit 2025 (April 6-8 & October 5-7):
   https://abnormalsecurity.com/blog/announcing-innovate-2025
6. RSA Conference 2025 (April 28 to May 1):
   Registration link not provided in the search results.
7. Gartner Security & Risk Management Summit 2025 (June 9-11):
   https://www.gartner.com/en/conferences/hub/cybersecurity-conferences
8. FIRST Annual Conference (June 22-27):
   https://www.first.org/conference/2025/registration-options
9. DEF CON 33 (August 7-10):
   DEF CON typically does not offer pre-registration and requires cash payment at the door.
10. InfoSec World 2025 (October 25-30):
    https://events.infosecworldusa.com/2025

Lists of awesome Threat Intelligence resource

- Awesome Intelligence: https://github.com/ARPSyndicate/awesome-intelligence
- Awesome-threat-intelligence: https://github.com/hslatman/awesome-threat-intelligence
- Awesome threat detection Resources: https://github.com/0x4D31/awesome-threat-detection
- Awesome open source intelligence tools and resources: https://github.com/jivoi/awesome-osint
- Get the latest technical details on significant advanced malware activity: https://www.trellix.com/en-us/advanced-research-center.html
- 10 of the Best Open Source Threat Intelligence Feeds: https://d3security.com/blog/10-of-the-best-open-source-threat-intelligence-feeds/
- Weekly Threat Briefing—Cyber Threat Intelligence Delivered to You: Anomali Weekly Threat Briefing
- Threat Intelligence Defined and Explored: https://www.forcepoint.com/cyber-edu/threat-intelligence
- Cyber Threat Intelligence Feeds: https://thecyberthreat.com/cyber-threat-intelligence-feeds/
- Deepdark CTI : https://github.com/fastfire/deepdarkCTI/tree/main

Best FREE Dark Web & CTI Tools - 2025

Dark Web Monitoring, Cyber Threat Intelligence, Attack Surface Management, and Supply Chain Intelligence are crucial for modern cybersecurity – kudos to SOCRadar® Extended Threat Intelligence for providing these essential tools for free.



⏩Dark Web Report : https://socradar.io/labs/dark-web-report/

- Checks if personal/organizational data appears on dark web markets, forums, or Telegram channels.

⏩External Attack Surface Discovery: https://socradar.io/labs/external-attack-surface/

- Identifies internet-facing assets vulnerable to cyberattacks using threat intelligence algorithms.

⏩BlueBleed Detection: https://socradar.io/labs/bluebleed/

- Flags data leaks from misconfigured cloud storage (AWS, Azure, Google) across 150K+ companies.

⏩Threat Actor Intelligence: https://socradar.io/labs/threat-actor/

- Profiles APT groups (e.g., APT 42) and ransomware operations with rankings and tactics.

⏩DarkMirror Monitoring: https://lnkd.in/ddYnU9Rp

- Tracks dark web news trends across 1018 industries and 28K+ threat actor discussions.

⏩Campaign Analysis: https://socradar.io/labs/campaigns/

- Details active cyber campaigns (e.g., Lazarus Group's CookieMiner) with IOCs and reports.

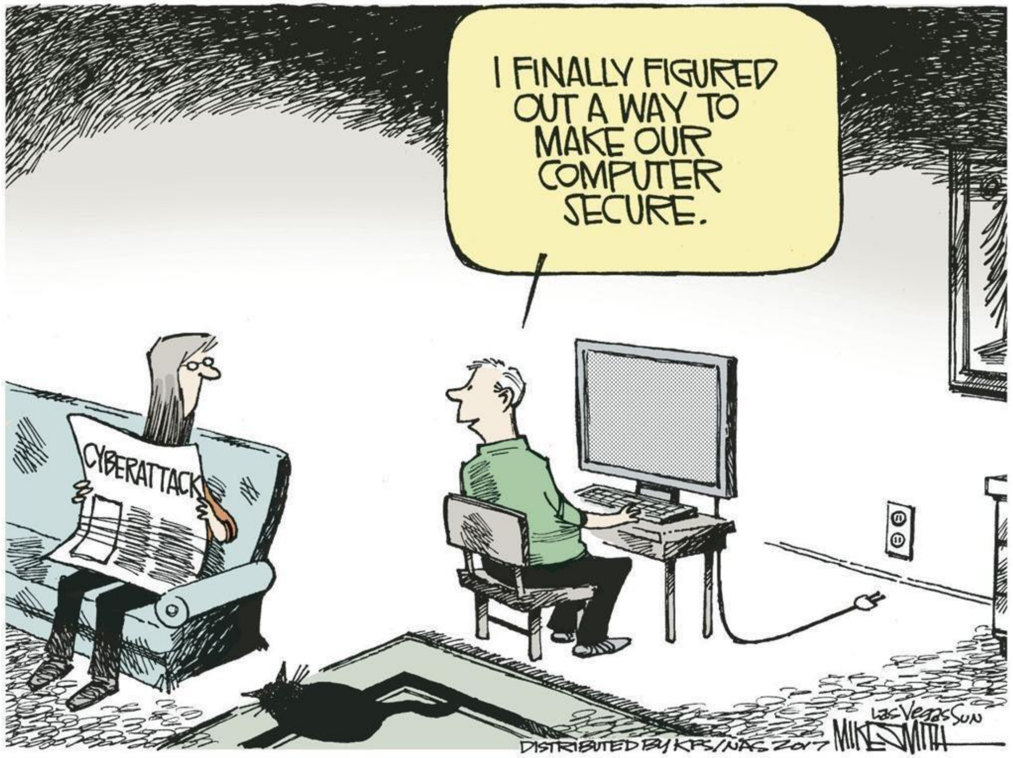
⏩IOC Radar: https://socradar.io/labs/ioc-radar/

- Provides AI-enriched indicators of compromise (IPs, domains) linked to malware/attackers.

⏩CVE Radar: https://socradar.io/labs/cve-radar/

- Monitors vulnerability trends and risk scores using dark/web data and community insights.

SOCRadar Free Tools Link: https://socradar.io/labs/


I FINALLY FIGURED OUT A WAY TO MAKE OUR COMPUTER SECURE.
CYBERATTACK
DISTRIBUTED BY KFS/NAS 2017
MIKE SMITH
Las Vegas Sun

Harun Seker

linkedin.com/in/harunseker