

A decorative background graphic consisting of a network of interconnected nodes and lines. The nodes are represented by small circles, some of which are solid blue, some are solid grey, and some are hollow blue. The lines are thin and grey, connecting the nodes in a complex, web-like pattern. This graphic is positioned in the top-left and bottom-right corners of the slide, framing the central text.

Automating Threat Hunting on the Dark Web and other nitty-gritty things

\$whoami

- ◎ Apurv Singh Gautam (@ASG_Sc0rpi0n)
- ◎ Security Researcher, Threat Intel/Hunting
- ◎ Cybersecurity @ Georgia Tech
- ◎ Prior: Research Intern at ICSI, UC Berkeley
- ◎ Hobbies
 - ◎ Contributing to the security community
 - ◎ Gaming/Streaming (Rainbow 6 Siege), Hiking, Lockpicking, etc.
- ◎ Social
 - ◎ Twitter - @ASG_Sc0rpi0n
 - ◎ Website – <https://apurvsinghgautam.me>

Agenda

- ◎ Introduction to the Dark Web
- ◎ Why hunting on the Dark Web?
- ◎ Methods to hunt on the Dark Web
- ◎ Can the Dark Web hunting be automated?
- ◎ Process after hunting?
- ◎ OpSec? What's that?
- ◎ Conclusion



A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines, with some nodes highlighted in grey and others in white.

1.

Introduction to the Dark Web

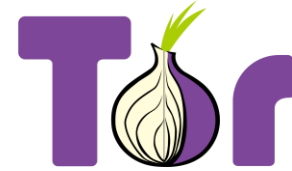
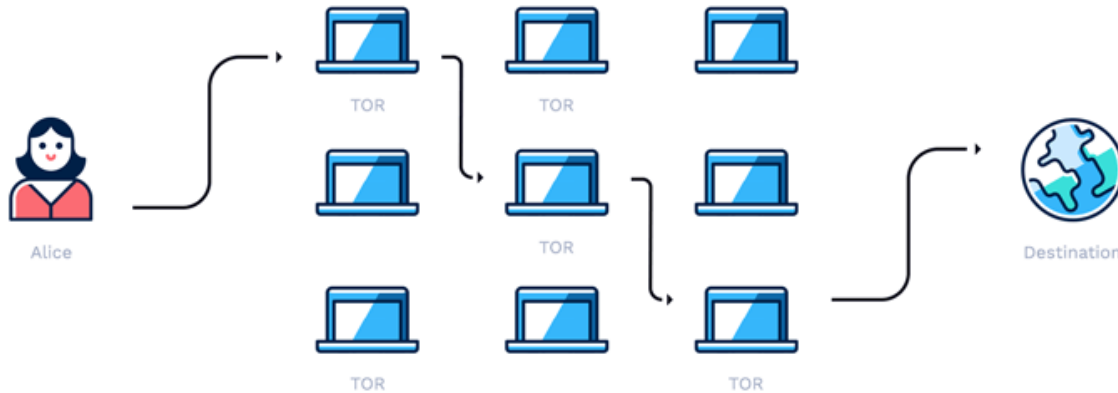
Clear Web? Deep Web? Dark Web?



Image Source: UC San Diego Library

Accessing the Dark Web

- ◎ Tor /I2P/ZeroNet
- ◎ .onion domains/.i2p domains
- ◎ Traffic through relays



What's all the Hype?

◎ Hype

- Vast and mysterious part of the Internet
- Place for cybercriminals only
- Illegal to access the Dark Web

◎ Reality

- Few reachable onion domains
- Uptime isn't ideal
- Useful for free expression in few countries
- Popular sites like Facebook, NYTimes, etc.
- Legal to access the Dark Web



Relevant sites?

- ◎ General Markets
- ◎ PII & PHI
- ◎ Credit Cards
- ◎ Digital identities
- ◎ Information Trading
- ◎ Remote Access
- ◎ Personal Documents
- ◎ Electronic Wallets
- ◎ Insider Threats



Image Source: Intsights

Cost of products?

- ◎ SSN - \$1
- ◎ Fake FB with 15 friends - \$1
- ◎ DDoS Service - \$7/hr
- ◎ Rent a Hacker - \$12/hr
- ◎ Credit Card - \$20+
- ◎ Mobile Malware - \$150
- ◎ Bank Details - \$1000+
- ◎ Exploits or 0-days - \$150,000+
- ◎ Critical databases - \$300,000+

Product Listings



USA FRESH CREATED BANK OF AMERICA BANK DROP + EMAIL ACCESS + PHONE ACCESS + DEBIT CARD + COOKIES

-ALLOW 1-5 DAYS FOR DELIVERY UPON ORDERING YOU WILL RECEIVE -BANK ACCOUNT USER AND PASS-EMAIL ...

Sold by **MasterSplinter0** - 20 sold since March 22, 2020 **Vendor Level 1** **Trust level 2**


	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

Default - 4 days - USD + 0.00 / order

Purchase price: **USD 90.00**

Qty: 1   

0.009510 BTC / 1.389318 XMR



NordVPN.com - [LIFETIME NORDVPN PREMIUM ACCOUNT]

Website: <https://nordvpn.com> Imagine VPN as a hack-proof, encrypted tunnel for online traffic to flow. Nobody can see thr...



Sold by **MissPinky** - 95 sold since December 11, 2018 **Vendor Level 4** **Trust level 4**

Unlimited items available for auto-dispatch

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow, MultiSig

Private Message - 1 days - USD + 0.00 / order

Purchase price: **USD 9.99**

Qty: 1    

0.001067 BTC / 0.229919 LTC / 0.154214 XMR



USA Bank login Cracker Bruter

banks brute/check 2020...guys here is all bank bruter, its really easy to use all u need is a good combo list and proxies -----...

Sold by **TheCashier** - 3 sold since April 26, 2020 **Vendor Level 1** **Trust level 2**

Unlimited items available for auto-dispatch

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

default - 1 day - USD + 0.00

Purchase price: **USD 3.00**

Qty: 1    

0.000319 BTC / 0.068368 LTC / 0.045537 XMR

AVERAGE COST OF ONE ACCOUNT FOR DIFFERENT ONLINE SERVICES

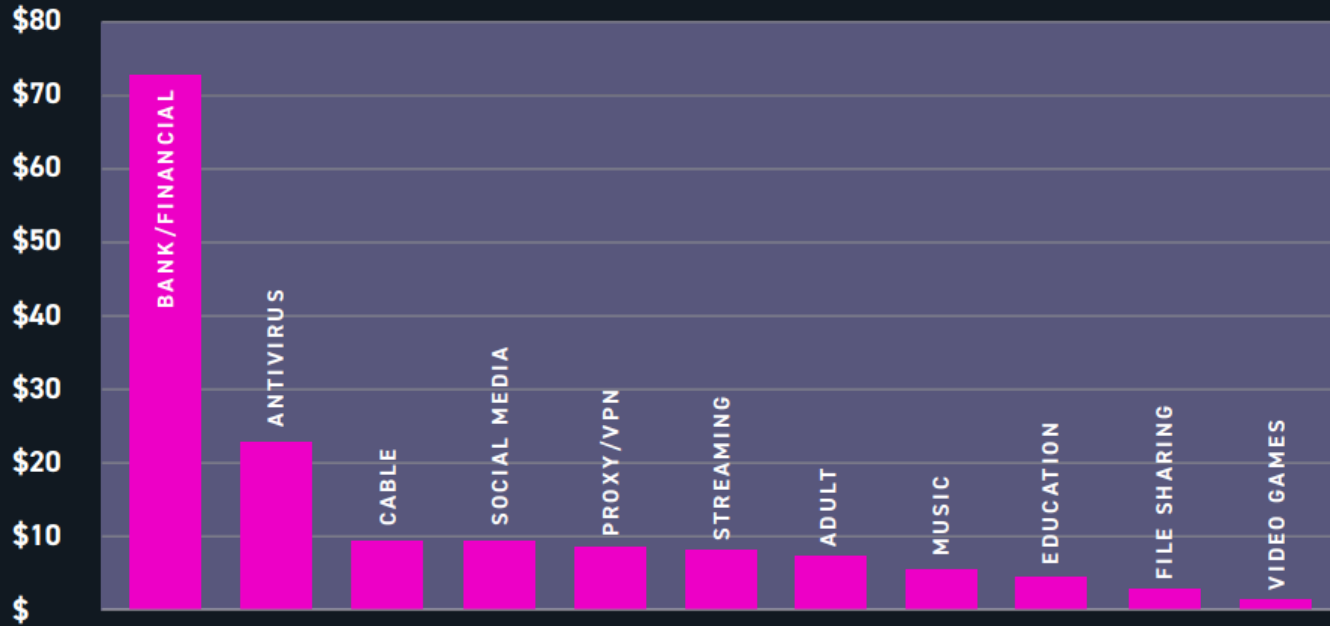


Image Source: Digital Shadows

AVERAGE PRICES OF BRUTE-FORCING TOOLS BY TARGET INDUSTRY

BANK/FINANCIAL

\$74.30

MULTIPACK

\$9.07

CRYPTOCURRENCY

\$5.64

SOCIAL

\$3.27

TECHNOLOGY

\$2.24

EDUCATION

\$0.99

VIDEO GAMES

\$0.90

Image Source: Digital Shadows

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines, with some nodes highlighted in grey and others in white.

2.

Why hunting on the Dark Web?

What is Threat Hunting?

- ◎ Practice of proactively searching for cyber threats
- ◎ Hypothesis-based approach
- ◎ Uses advanced analytics and machine learning investigations
- ◎ Proactive and iterative search



Why So Serious (Eh! Important)?

- ◎ Hacker forums, darknet markets, dump shops, etc.
- ◎ Criminals can learn, monetize, trade, and communicate
- ◎ Identification of compromised assets
- ◎ Can potentially identify attacks in earlier stages
- ◎ Direct impacts – PII (Personal Info), financial, EHRs (healthcare records), trade secrets
- ◎ Indirect impacts – reputation, revenue loss, legal penalties



Benefits of Threat Hunting

- ◎ Keep up with the latest trends of attacks
- ◎ Prepare SOCs/Incident Responders
- ◎ Get knowledge of TTPs (Tactics, Techniques, Procedures) to be used
- ◎ Reduce damage and risks to the organization

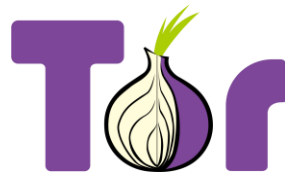
A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines, with some nodes highlighted in grey and others in white.

3.

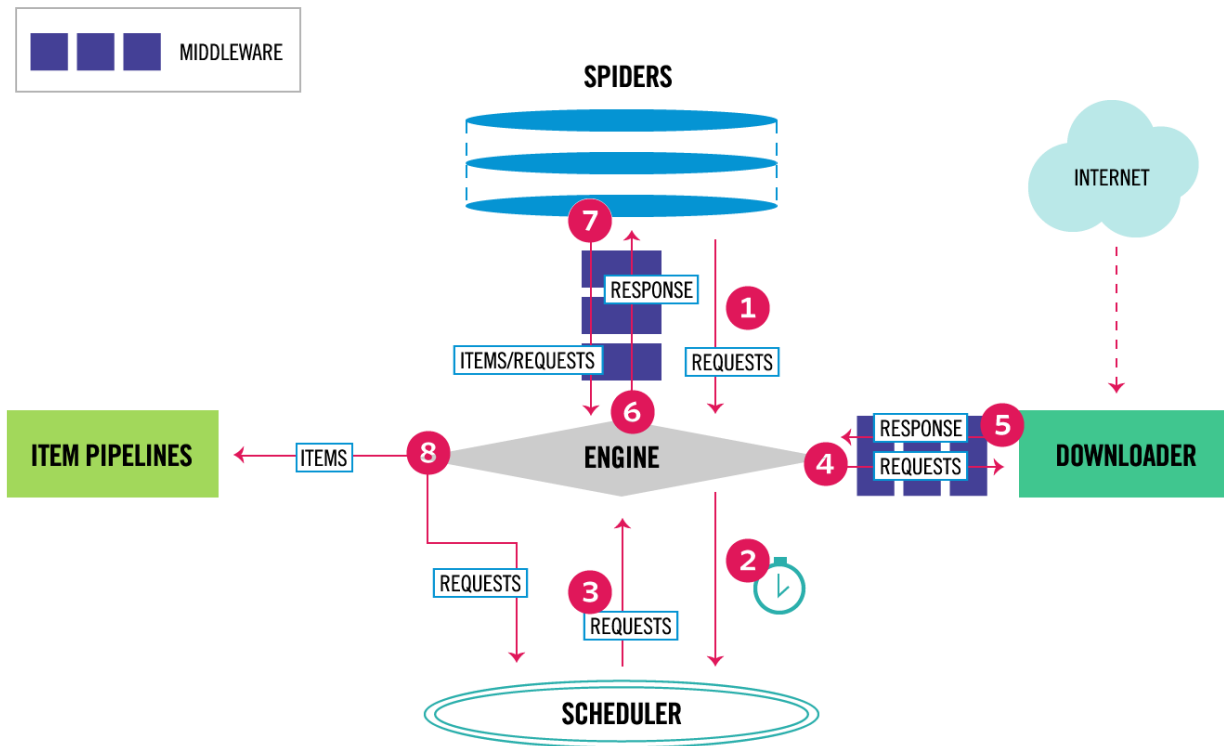
Methods to hunt on the Dark Web

Tools

- ◎ Python
- ◎ Scrapy
- ◎ Tor
- ◎ OnionScan
- ◎ Privoxy
- ◎ and many more...



How Scrapy Works?



HUMINT

- ◎ Human Intelligence
- ◎ Most dangerous and difficult form
- ◎ Most valuable source
- ◎ Infiltrating forums, markets, etc.
- ◎ Become one of them
- ◎ How threat actors think
- ◎ Can be very risky
- ◎ Time consuming

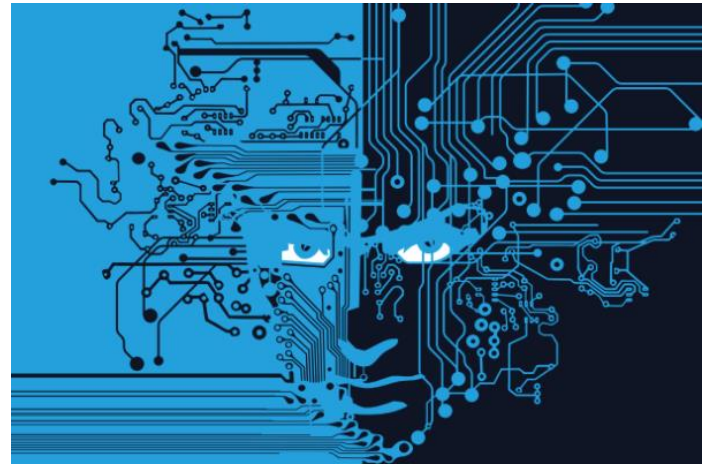


Image Source: Intsights

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines, with some nodes highlighted in grey and others in white.

4.

**Can dark web hunting
be automated?**

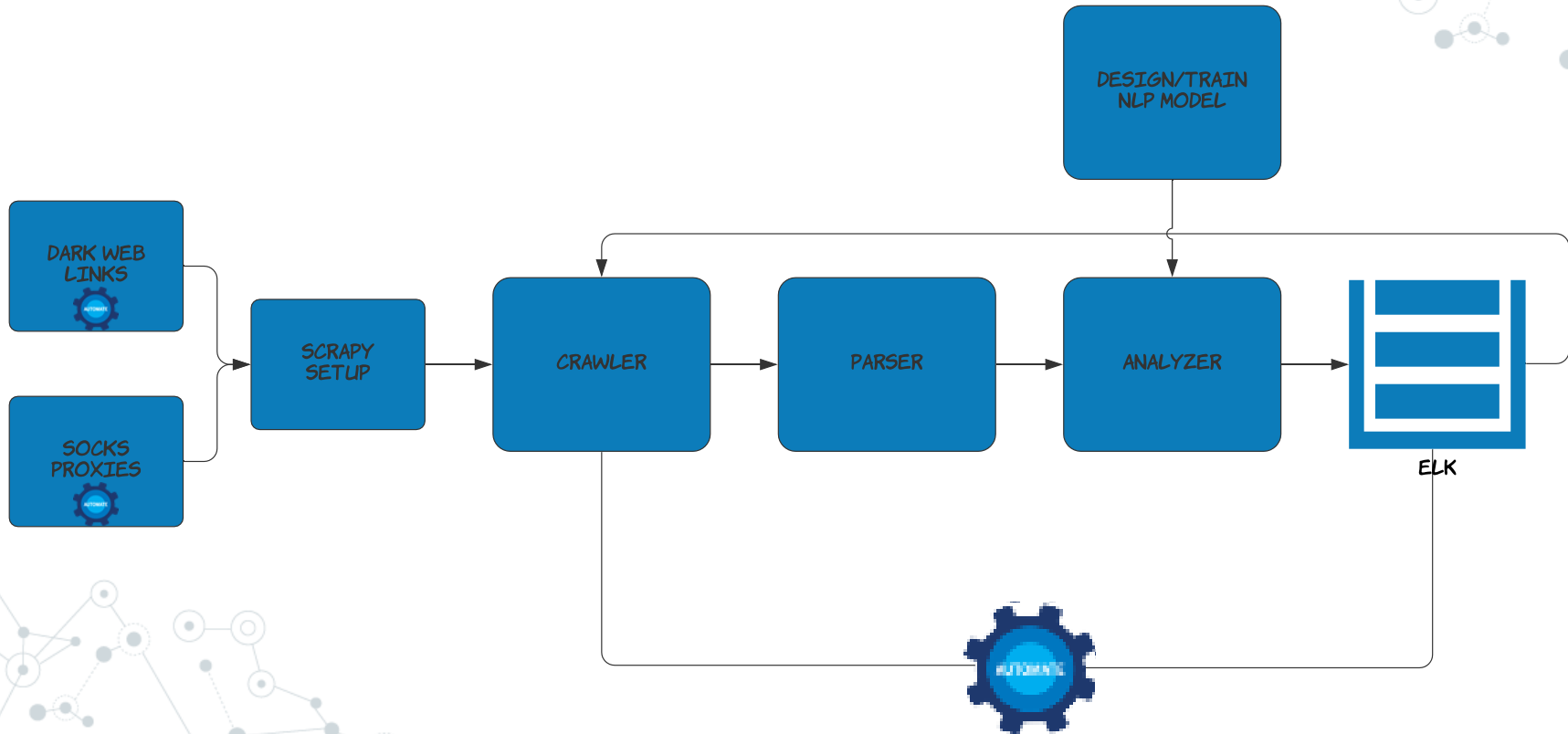
Setting up TH Lab

- ◎ Lab/VM
- ◎ Physical or Cloud
- ◎ Isolate the network
- ◎ Install relevant tools
 - Scrapy
 - Privoxy
 - Tor
 - ELK
 - Python libraries



Image Source: Hayden James

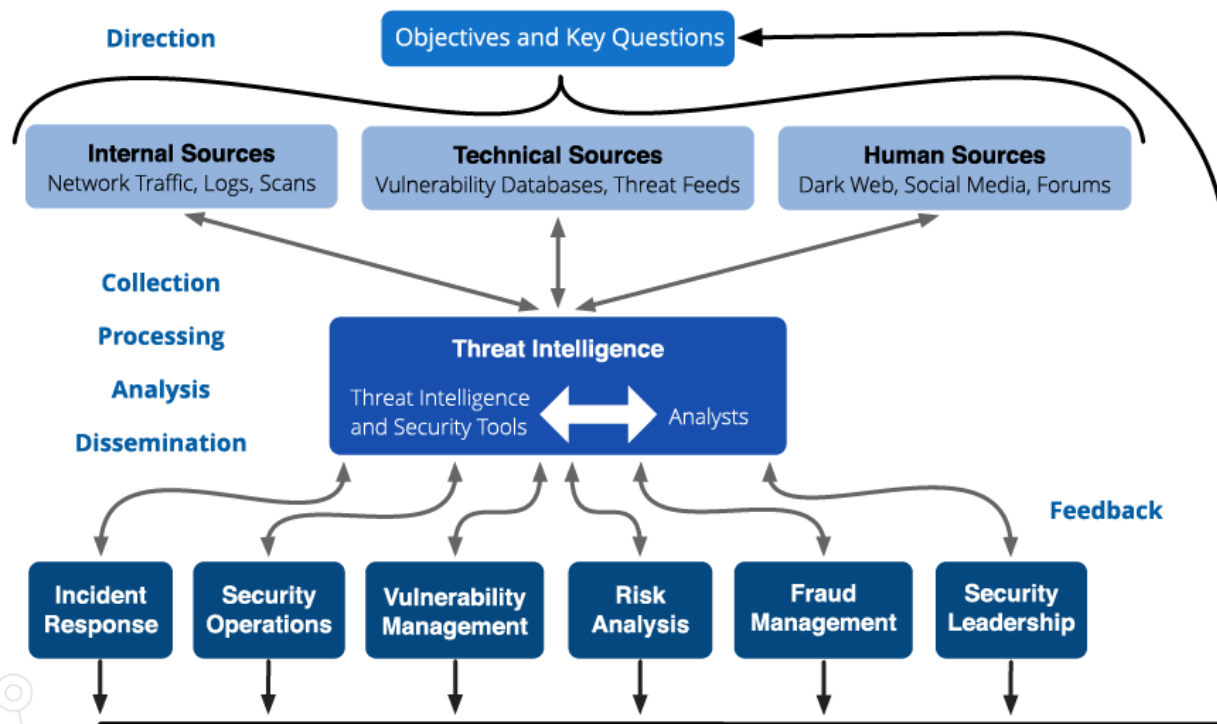
Automated Hunting Architecture



A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting different levels of connectivity or importance. The lines are thin and gray, creating a mesh-like structure.

5. **Process after hunting**

Let's talk about TI Lifecycle



Threat Modelling

- ◎ “works to identify, communicate, and understand threats and mitigations within the context of protecting something of value” – OWASP
- ◎ Define critical assets
- ◎ Understand what attackers want
- ◎ Threat actor capability and intent
- ◎ Sources to target

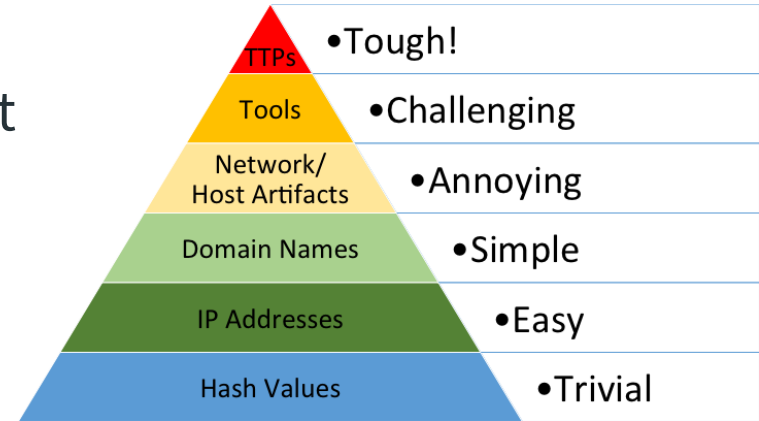


Image Source: David Bianco

Data Collection/Processing

- ◎ Collecting data from clear web
 - Pastebin
 - Twitter
 - Reddit
- ◎ Collecting data from dark web
 - Forums
 - Markets

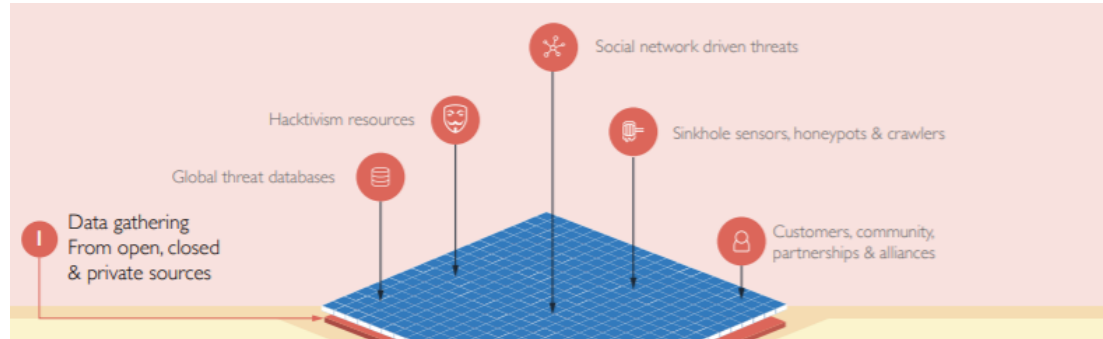


Image Source: Blueliv

Data Analysis

- ◎ NLP/ML/DL techniques
- ◎ Social network analysis
- ◎ Classification
- ◎ Clustering
- ◎ MITRE ATT&CK





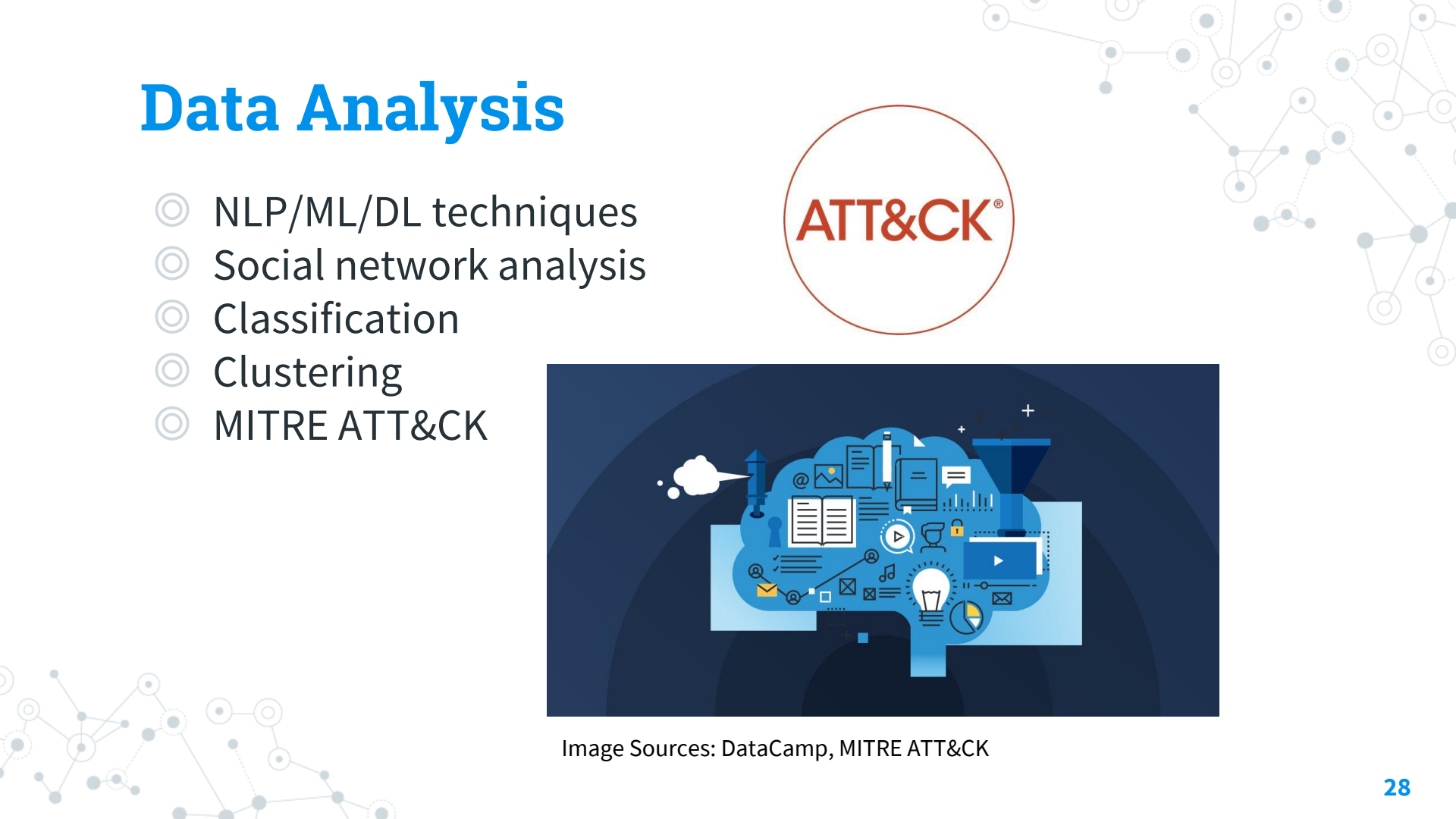
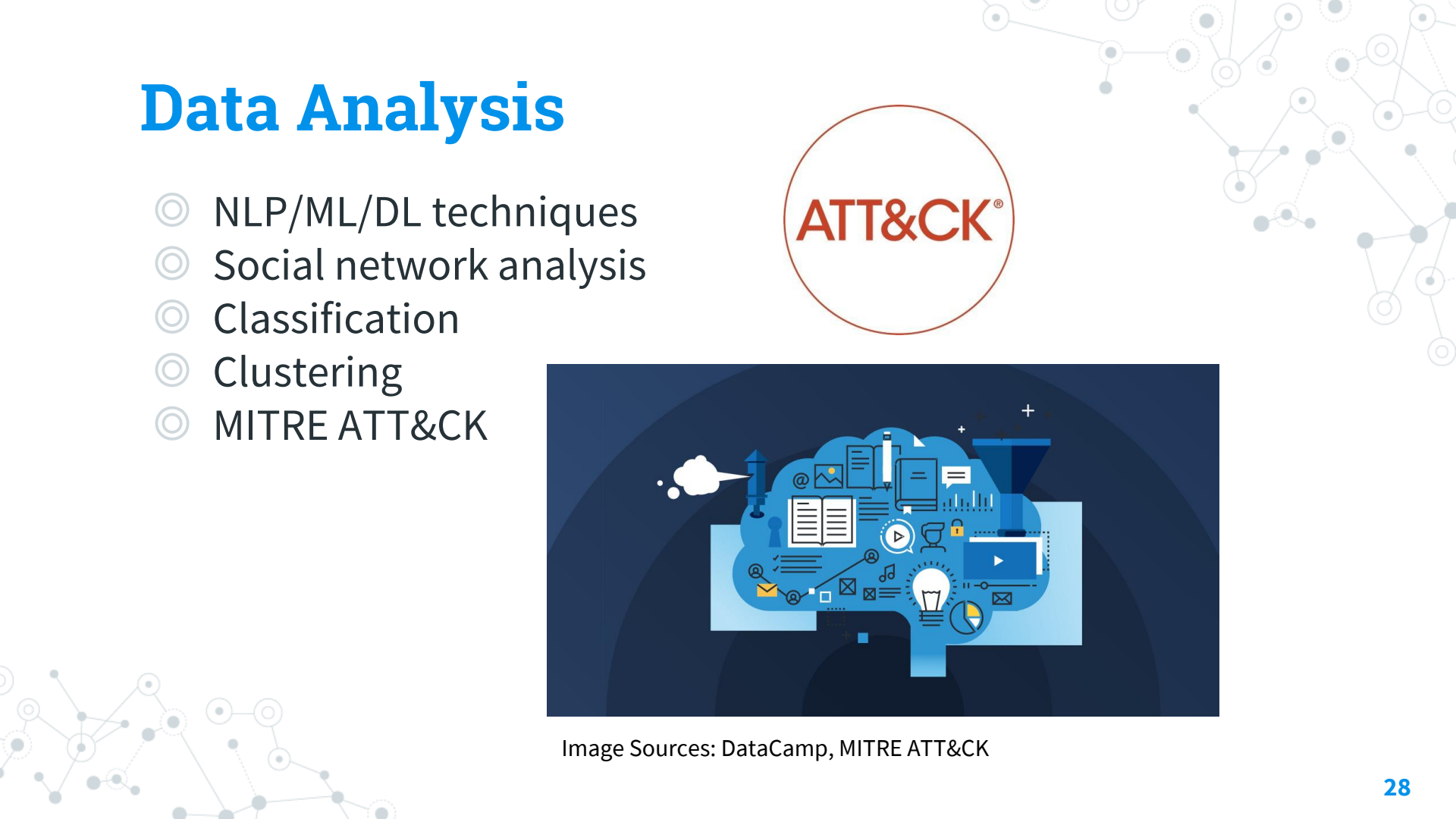


Image Sources: DataCamp, MITRE ATT&CK

28

- # Data Analysis
- ◎ NLP/ML/DL techniques
 - ◎ Social network analysis
 - ◎ Classification
 - ◎ Clustering
 - ◎ MITRE ATT&CK
- 
- 
- Image Sources: DataCamp, MITRE ATT&CK



Data Analysis

- ◎ NLP/ML/DL techniques
- ◎ Social network analysis
- ◎ Classification
- ◎ Clustering
- ◎ MITRE ATT&CK

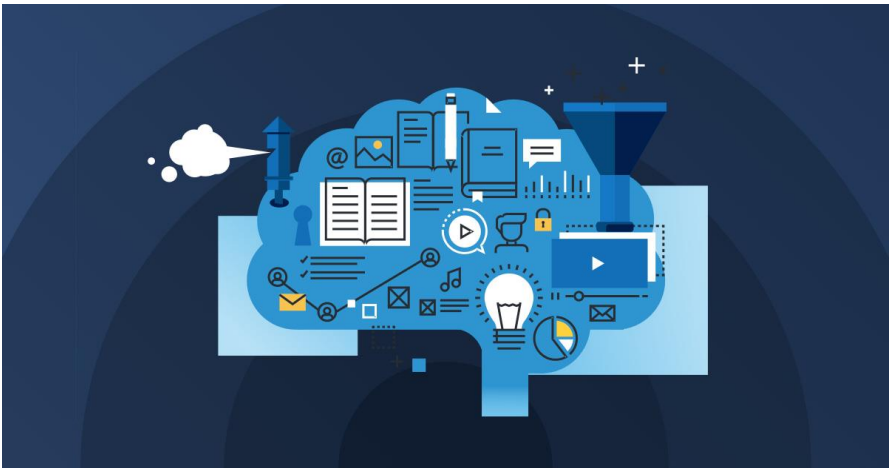



Image Sources: DataCamp, MITRE ATT&CK

28

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting different levels of connectivity or importance. The lines are thin and gray, creating a mesh-like structure.

6.

OpSec? What is that?

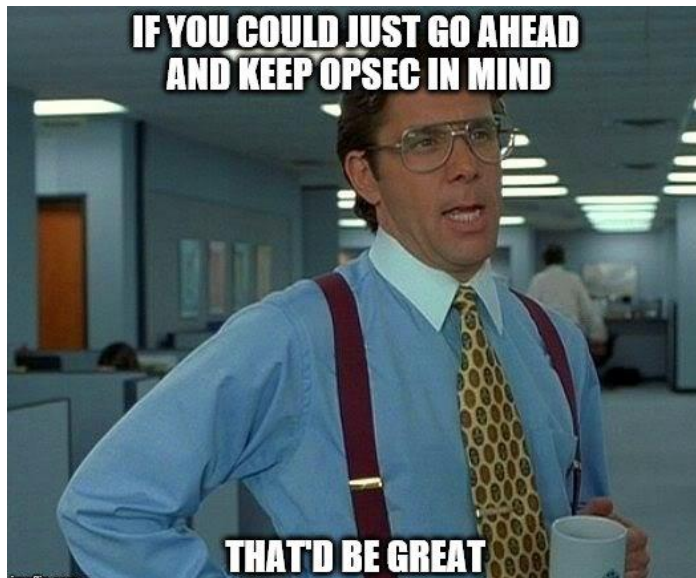
What is OpSec?

- ◎ Actions taken to ensure that information leakage doesn't compromise you or your operations
- ◎ Derived from US military – Operational Security
- ◎ PII – Personally Identifiable Information
- ◎ Not just a process – a mindset
- ◎ OpSec is Hard



Maintaining OpSec in your lifestyle

- ◎ Hide your real identity
- ◎ Use VM/Lab or an isolated system
- ◎ Use Tor or Tor over VPN always
- ◎ Change Time zones
- ◎ Never talk about your work
- ◎ Maintain different persona
- ◎ Take extensive notes
- ◎ Use password manager



A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting different levels of connectivity or importance. The lines are thin and gray, creating a mesh-like structure.

7. Conclusion

What we discussed so far?

- ◎ Little about the Dark Web
- ◎ Dark Web forums/marketplaces
- ◎ Dark Web threat hunting
- ◎ Scrapy
- ◎ HUMINT
- ◎ Automating the Dark Web hunting
- ◎ Little about threat intelligence lifecycle
- ◎ A little about OpSec

I don't know how to conclude but..

- ◎ Dark Web threat hunting is hard but worth the effort
- ◎ Keep OpSec in mind
- ◎ Look at more than one resource
- ◎ Takes a lot of resources and team effort
- ◎ Usage of MITRE ATT&CK framework

Resources

- ◎ Blogs & White papers by Recorded Future
- ◎ White papers by IntSights
- ◎ Blogs by Palo Alto's Unit 42
- ◎ Blogs by CrowdStrike
- ◎ Blogs by CloudSEK
- ◎ White papers by Digital Shadows
- ◎ Darkweb Cyber Threat Intelligence Mining by Cambridge University Press

Thanks!

Any questions?

You can contact me at:

Twitter: @ASG_Sc0rpi0n

LinkedIn: /in/apurvsinghgautam

