



Identifying Opportunities to Collaborate and Contribute back!

A community-based approach

@Cyb3rWard0g

Roberto Rodriguez 

Principal Threat Researcher at the Microsoft
Threat Intelligence Center (MSTIC) R&D team

Founder of the Open Threat Research community!
[@OTR Community](#)

I ♥ dogs 🐶 and open source!

Empowering others around the 🌐: <https://github.com/OTRF>





"If you want to go fast, go alone.
If you want to go far, go together"

African proverb

"If you want to go fast, go alone.
If you want to go far, go together"

African proverb

"If you want to go fast, go alone.
If you want to go far, go together"

African proverb

If you want to go far, _____

If you want to go
fast and far,

SANS Threat Hunting Summit 2021

- Plan Together
- Empower Others
- Adapt Quickly
- Think Big

Let's Go Together! 🤝

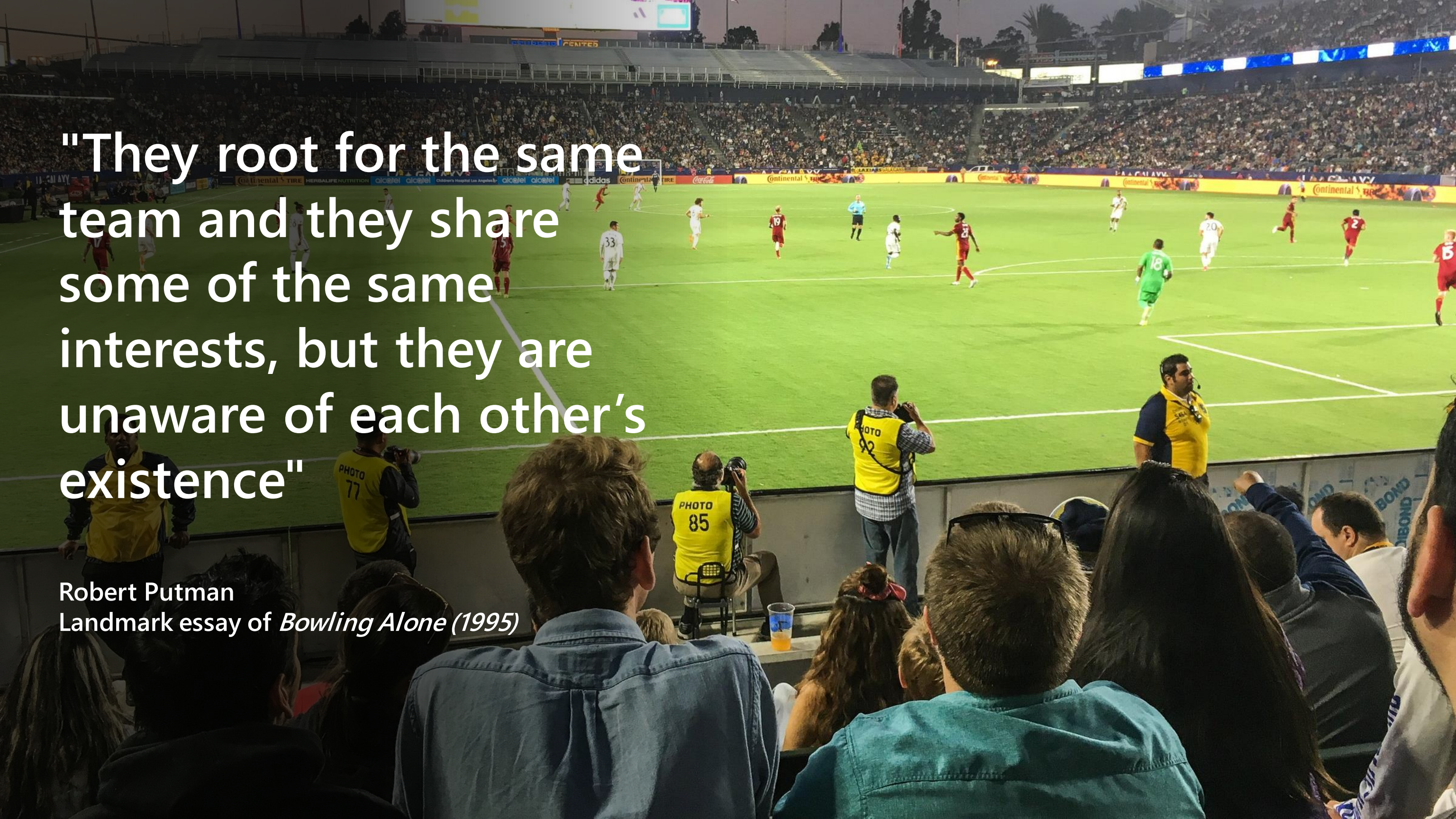


Let's Go Together! 😊



A Community-based Approach!





"They root for the same team and they share some of the same interests, but they are unaware of each other's existence"

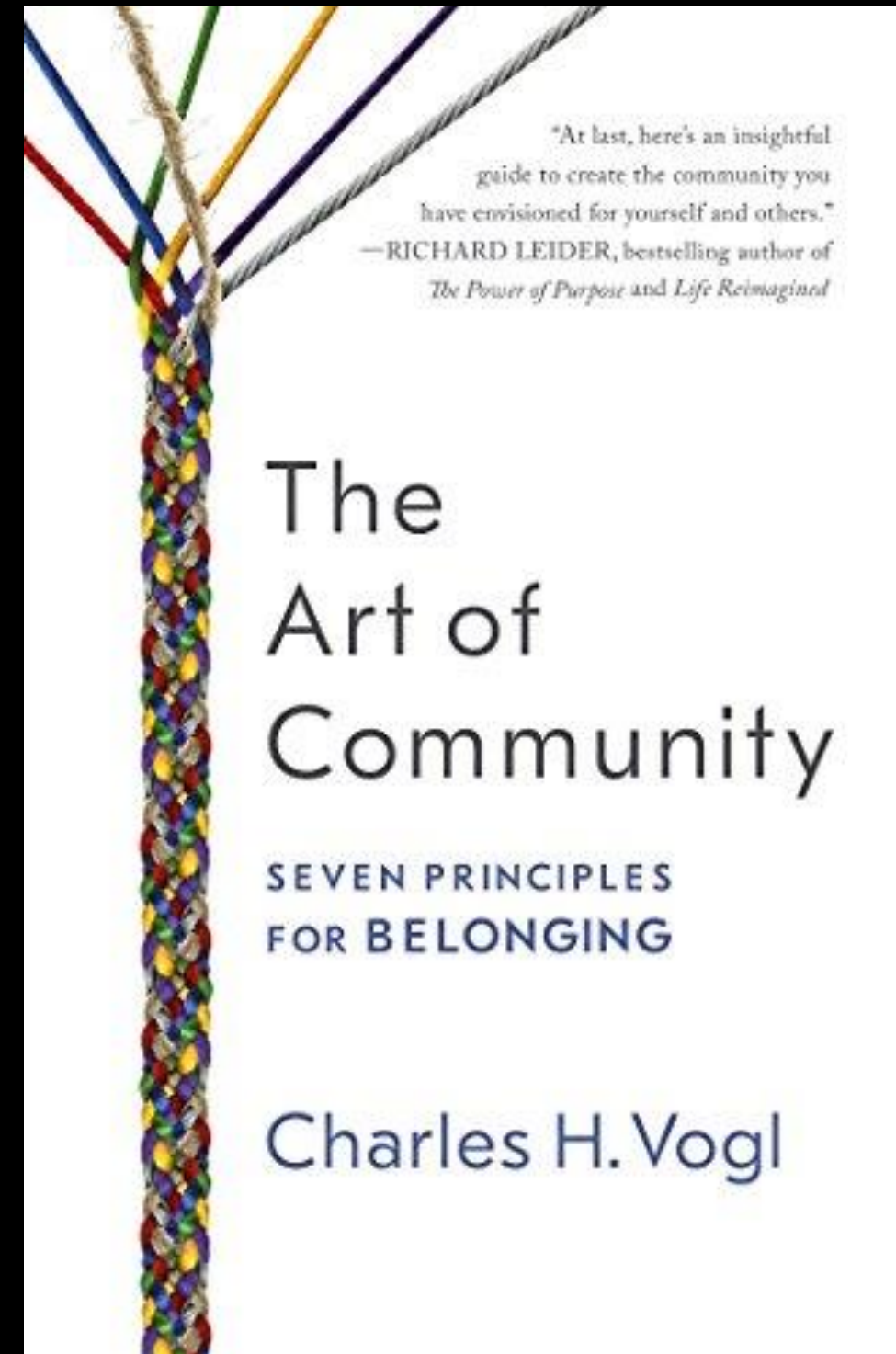
Robert Putman
Landmark essay of *Bowling Alone* (1995)

What is Community?

- People that share common interests.
- People that are welcomed and appreciated for who they are.
- Mutual concern for one another.
- Helping others grow in the ways they hope to.
- Growth can be technical, social or internal.

Thanks Gregory Bell for sharing!

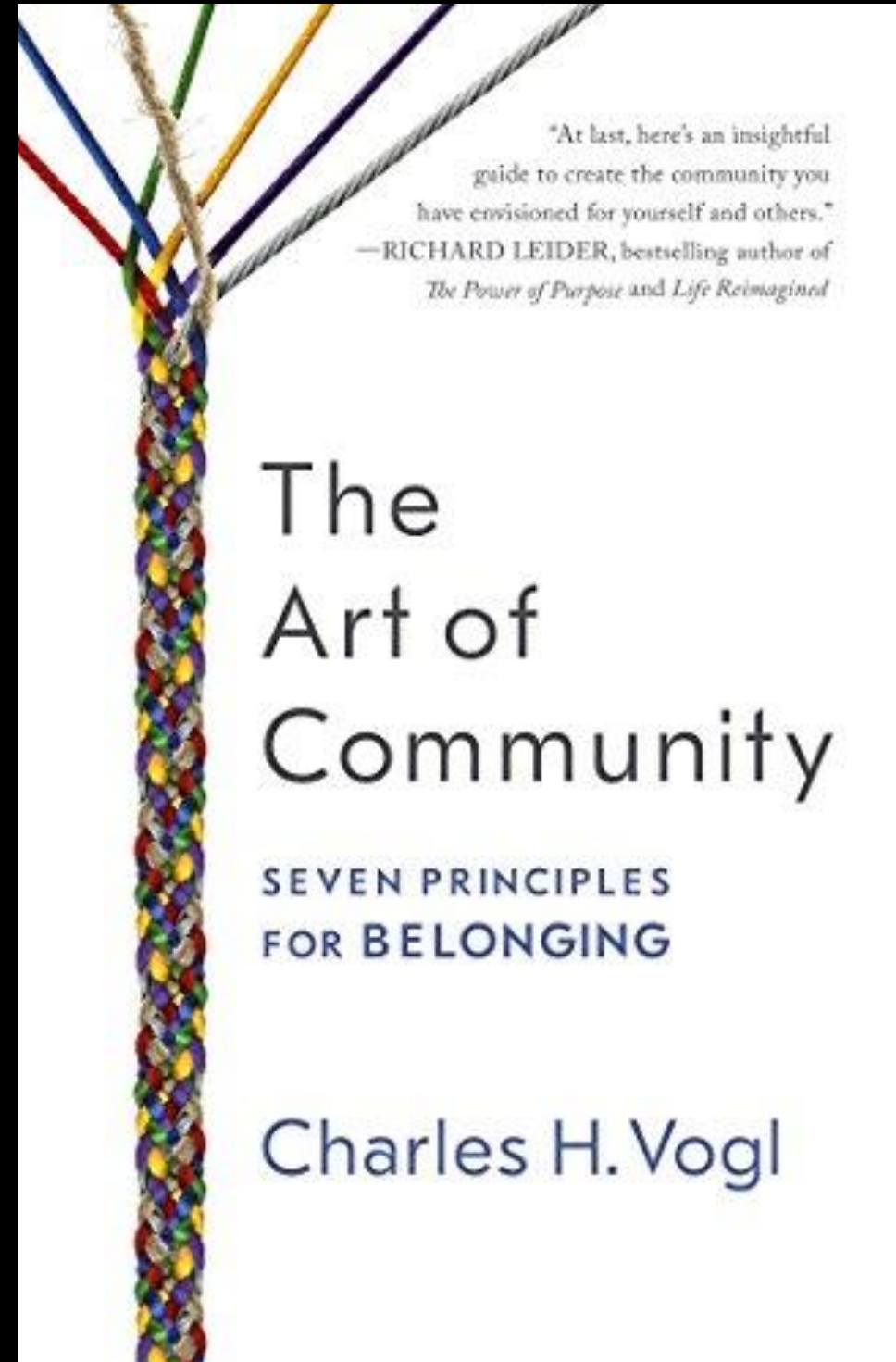
<https://www.amazon.com/Art-Community-Seven-Principles-Belonging-ebook/dp/B01E4KC0U4>



What is Community?

- People that share common interests.
- People that are welcomed and appreciated for who they are.
- **Mutual concern for one another.**
- Helping others grow in the ways they hope to.
- Growth can be technical, social or internal.

Thanks Gregory Bell for sharing!



<https://www.amazon.com/Art-Community-Seven-Principles-Belonging-ebook/dp/B01E4KC0U4>

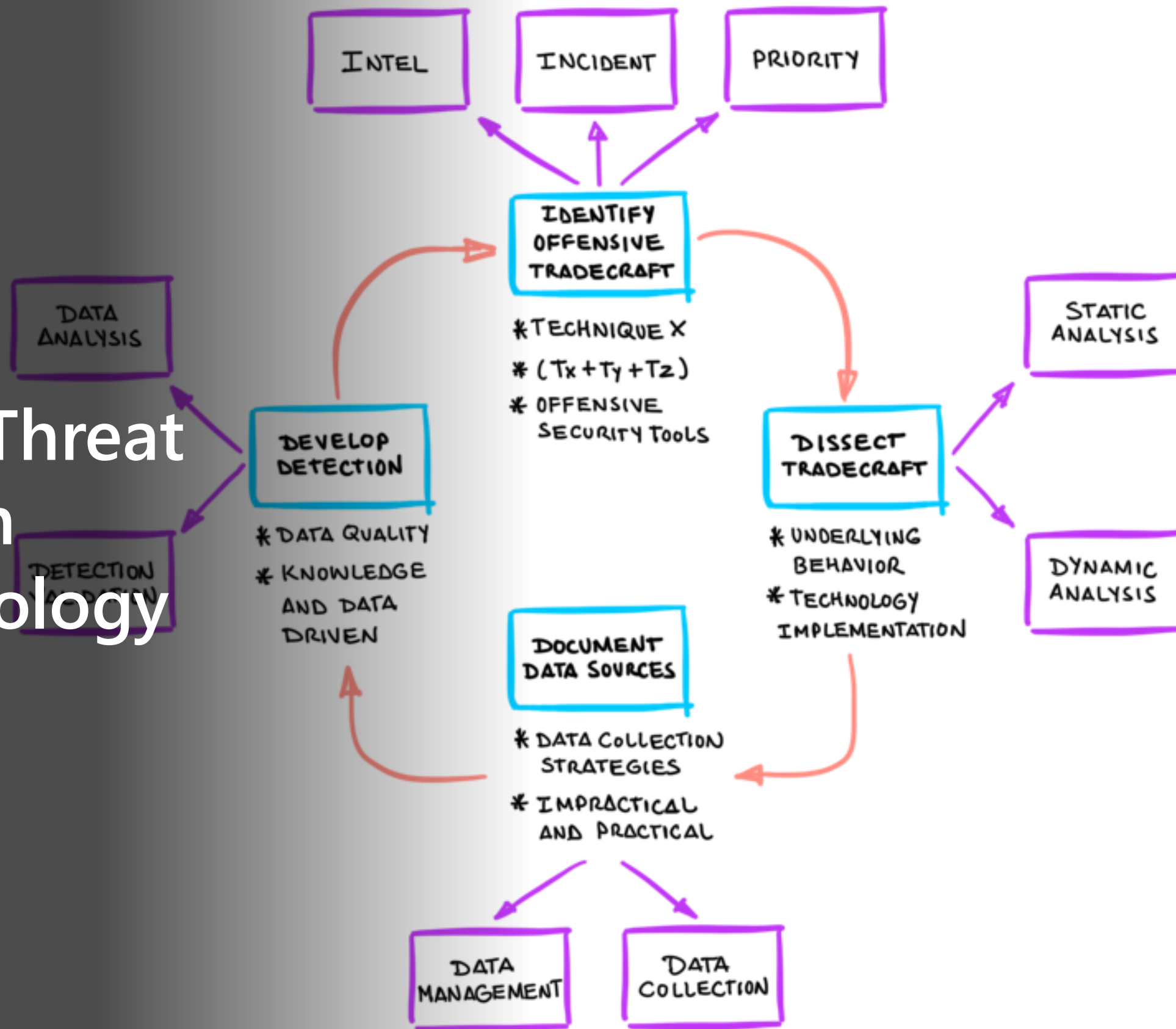
**"Everybody is a Genius. But If
You Judge a Fish by Its Ability to
Climb a Tree, It Will Live Its Whole
Life Believing that It is Stupid"**

Albert Einstein

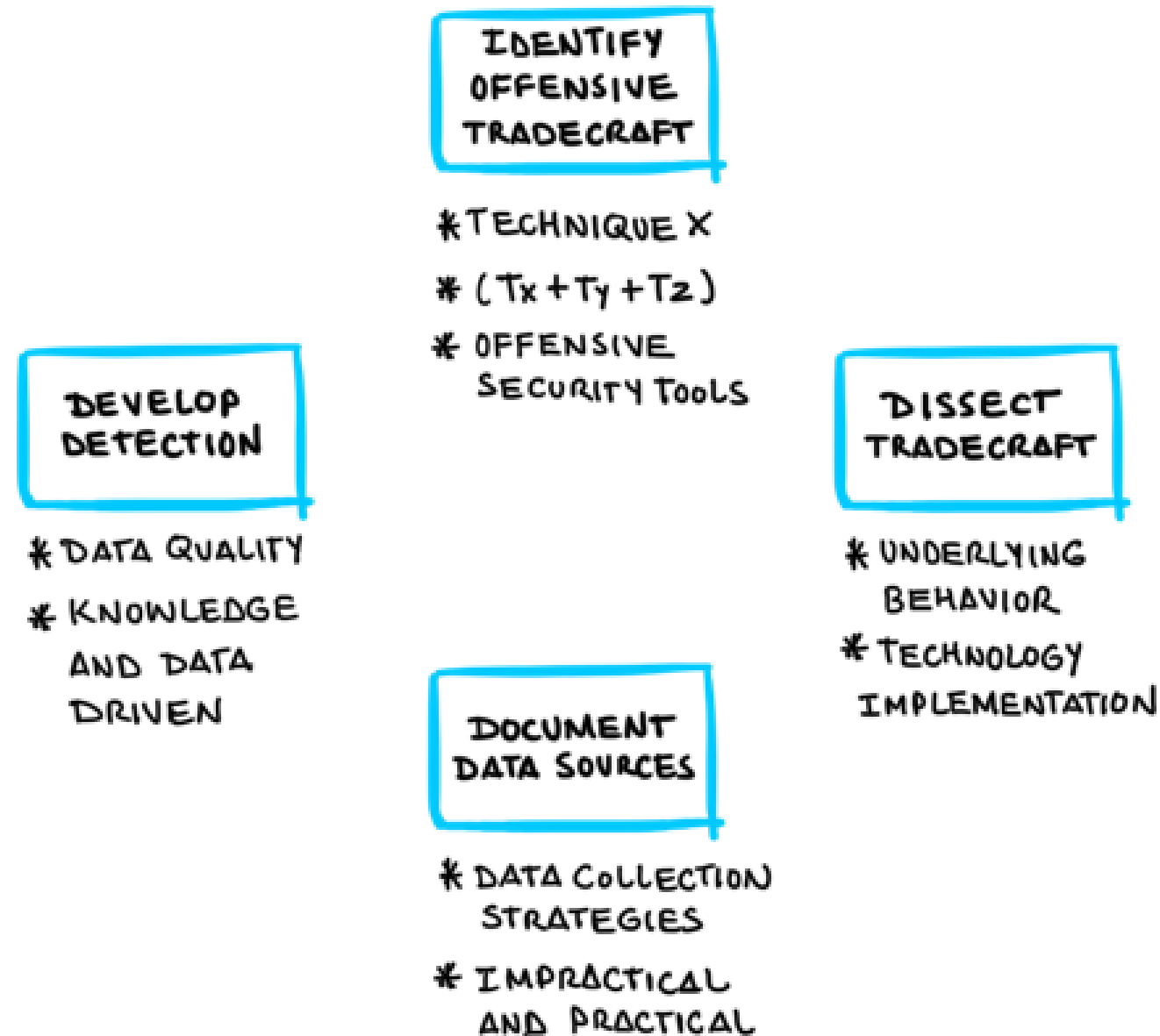
A Few Opportunities to Collaborate



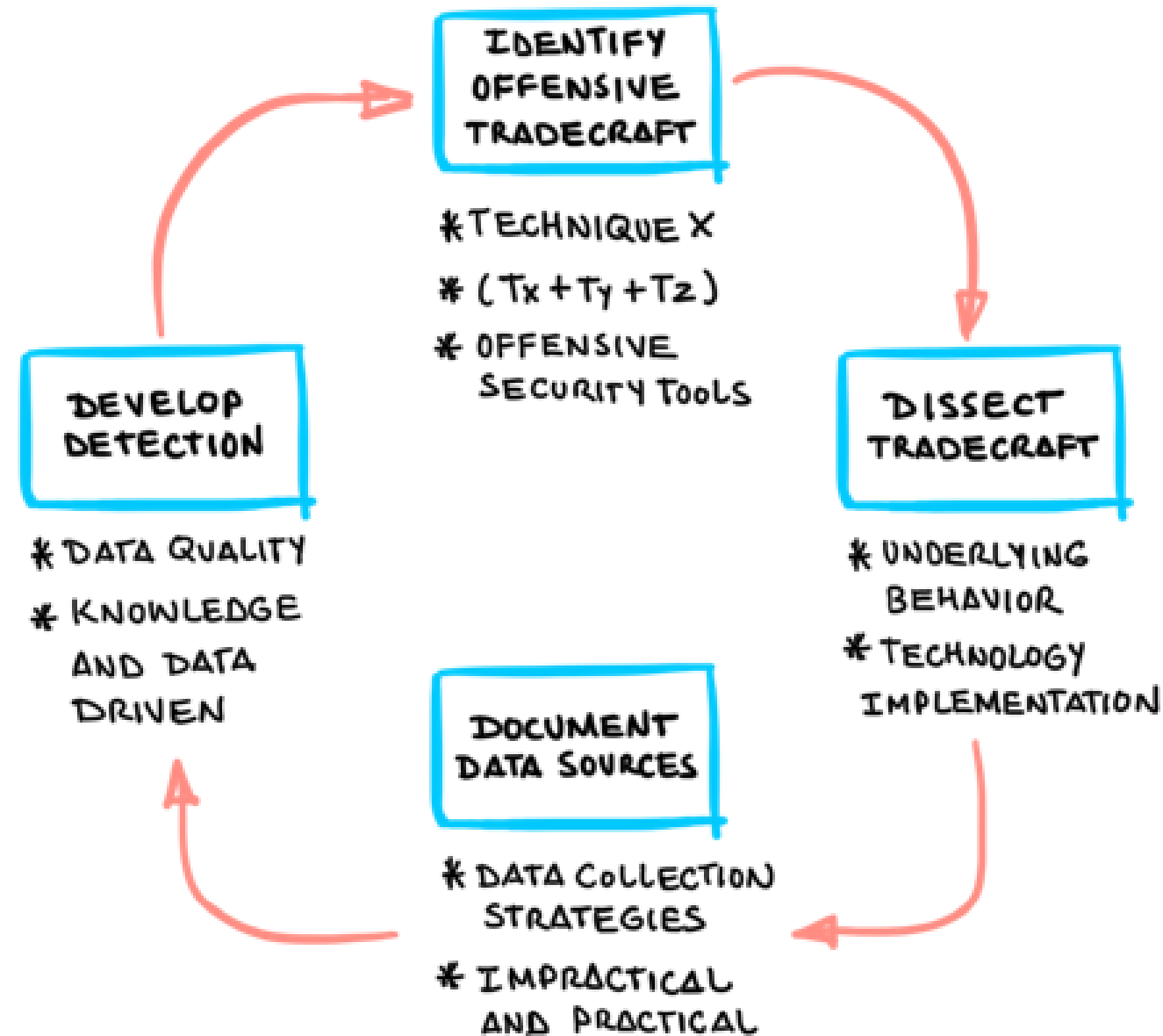
A Basic Threat Research Methodology



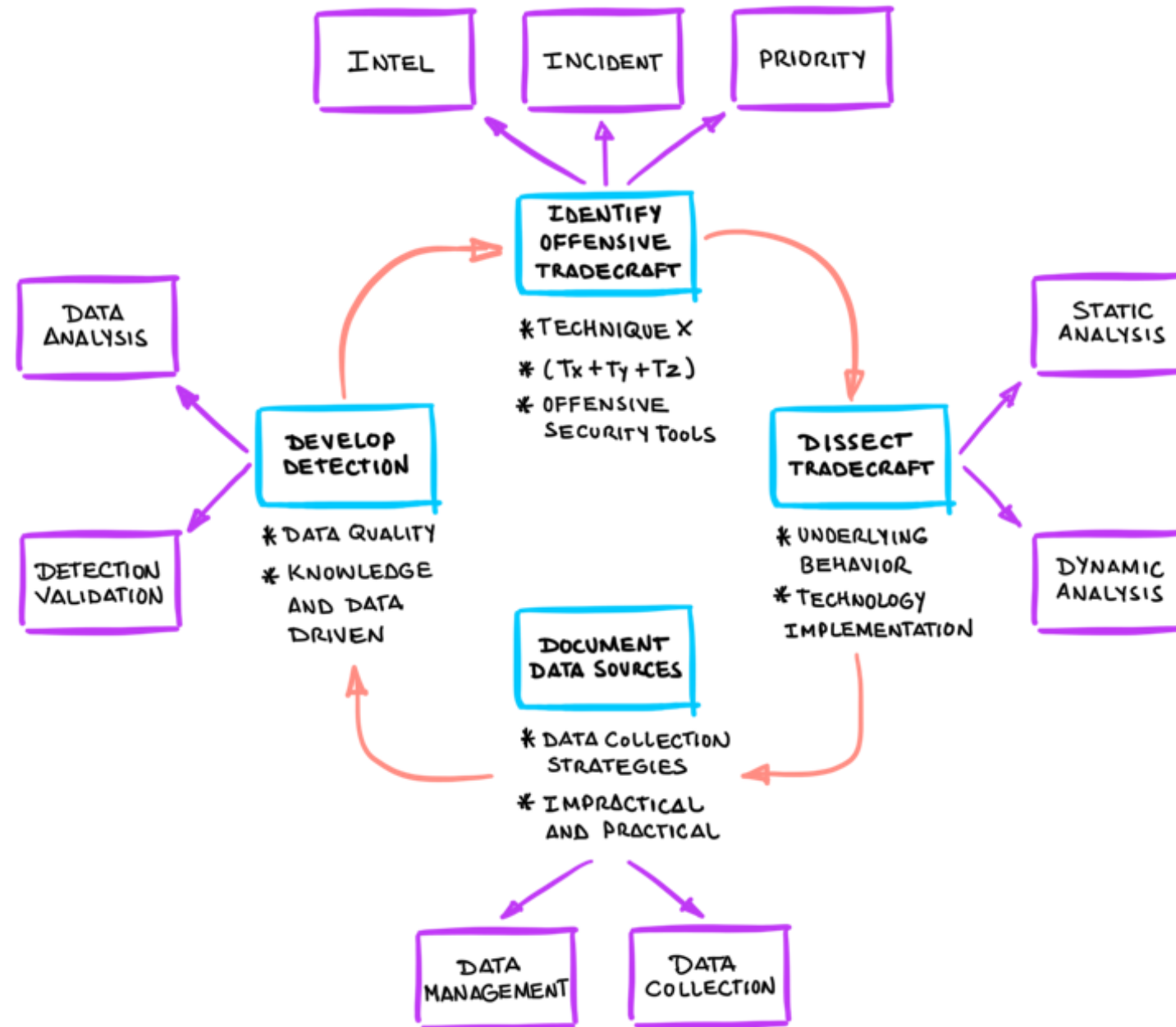
A Basic Threat Research Methodology



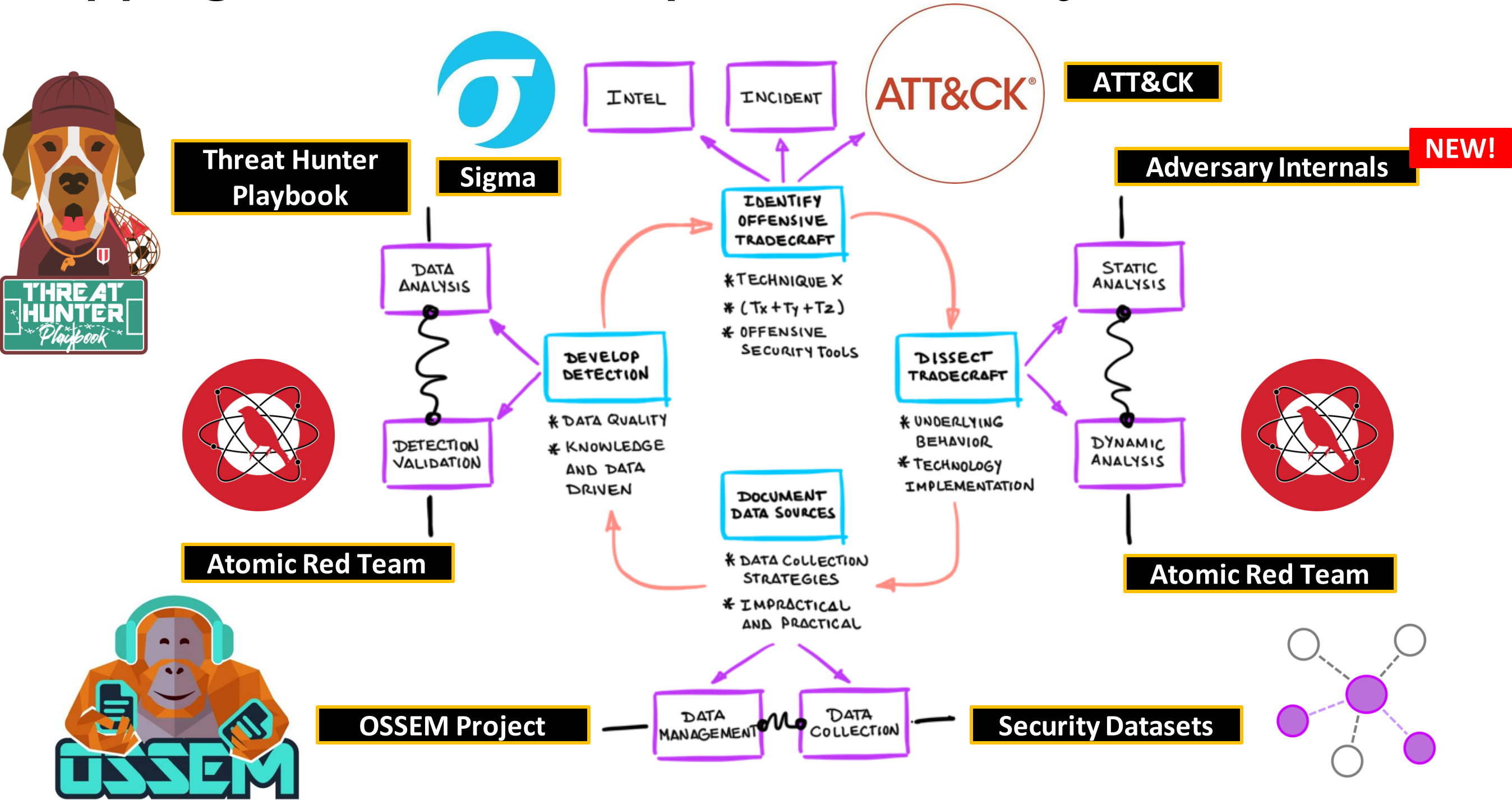
A Basic Threat Research Methodology



A Basic Threat Research Methodology



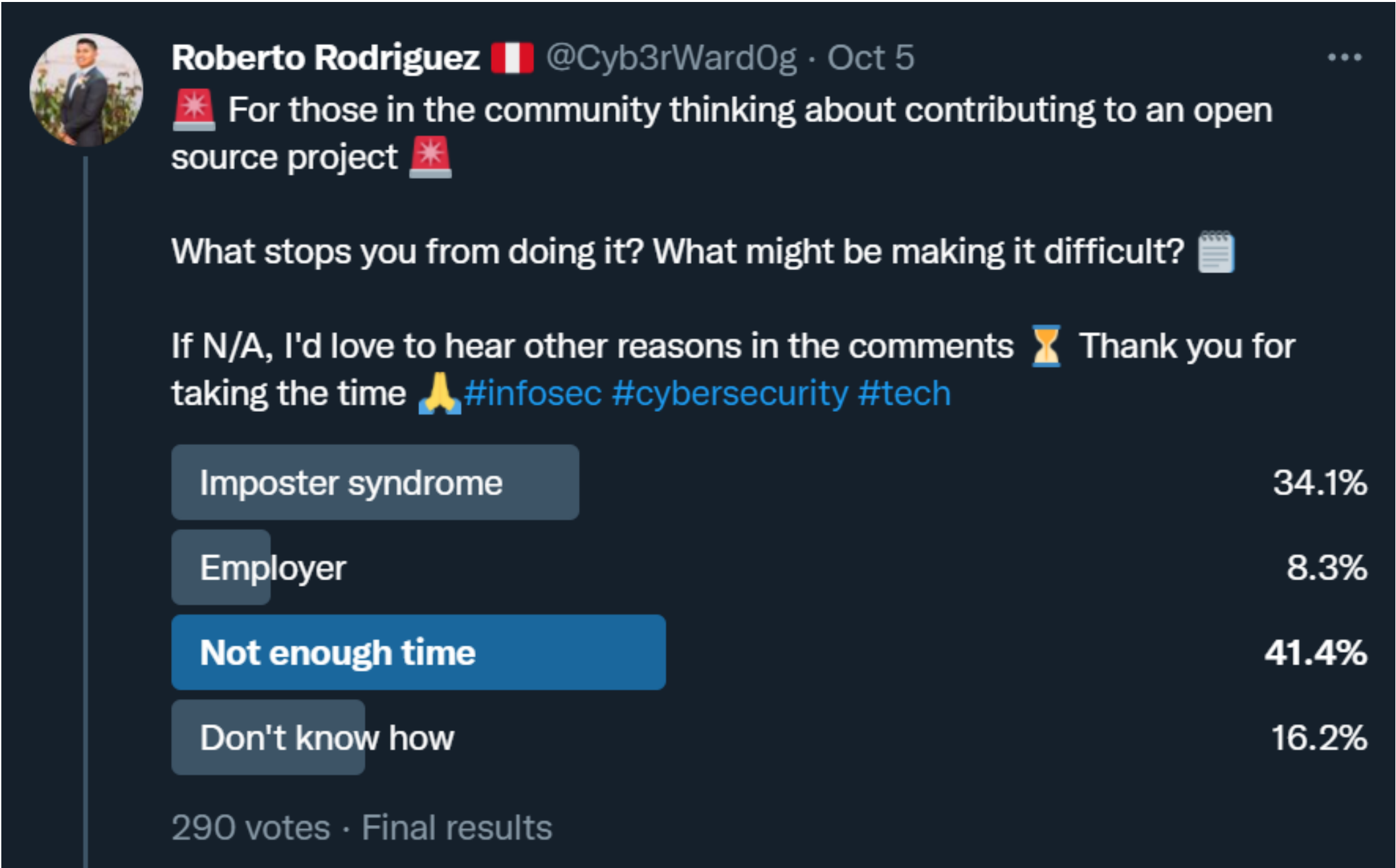
Mappings Processes to Open Source Projects



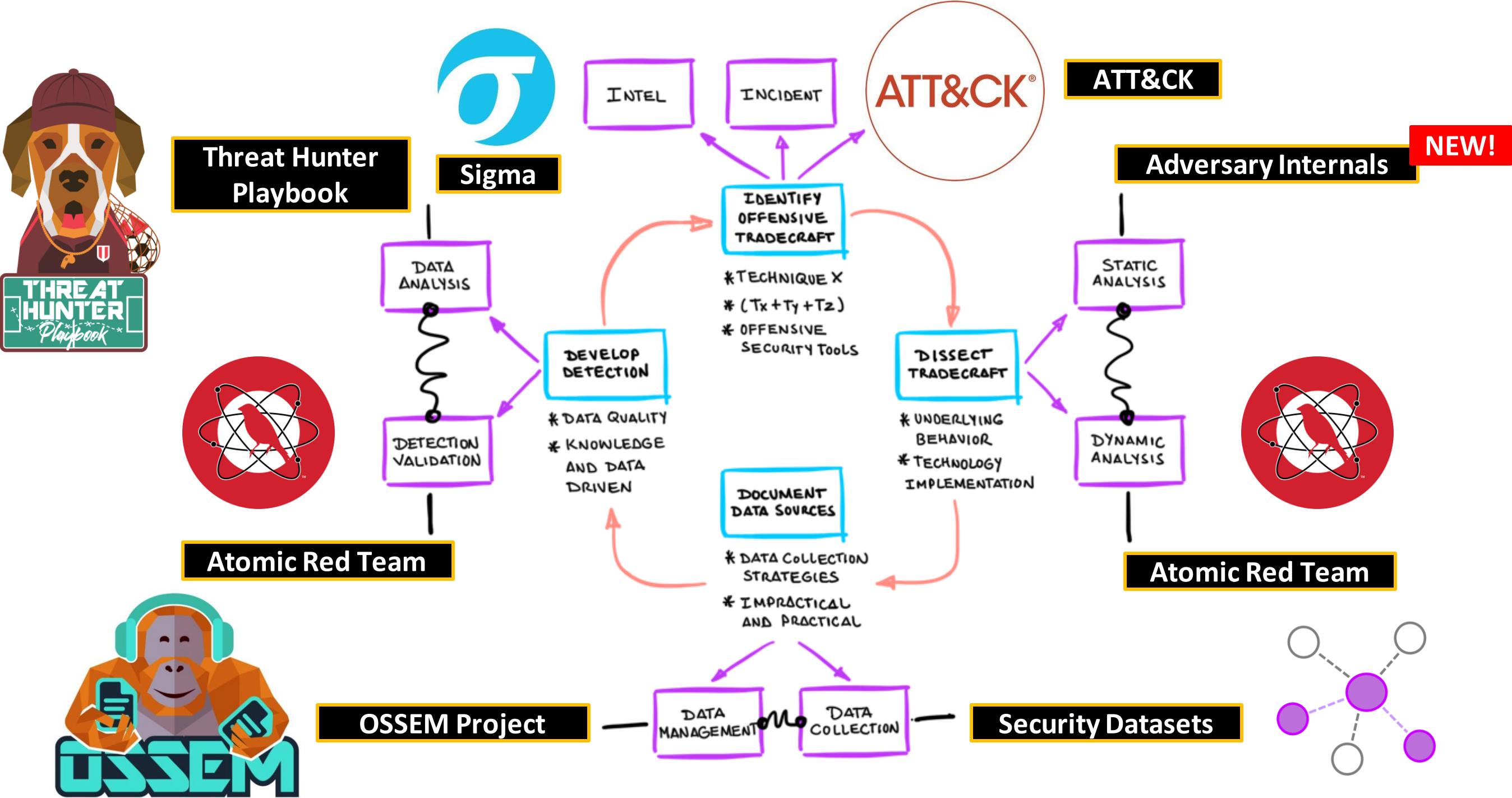
Are we doing this yet?



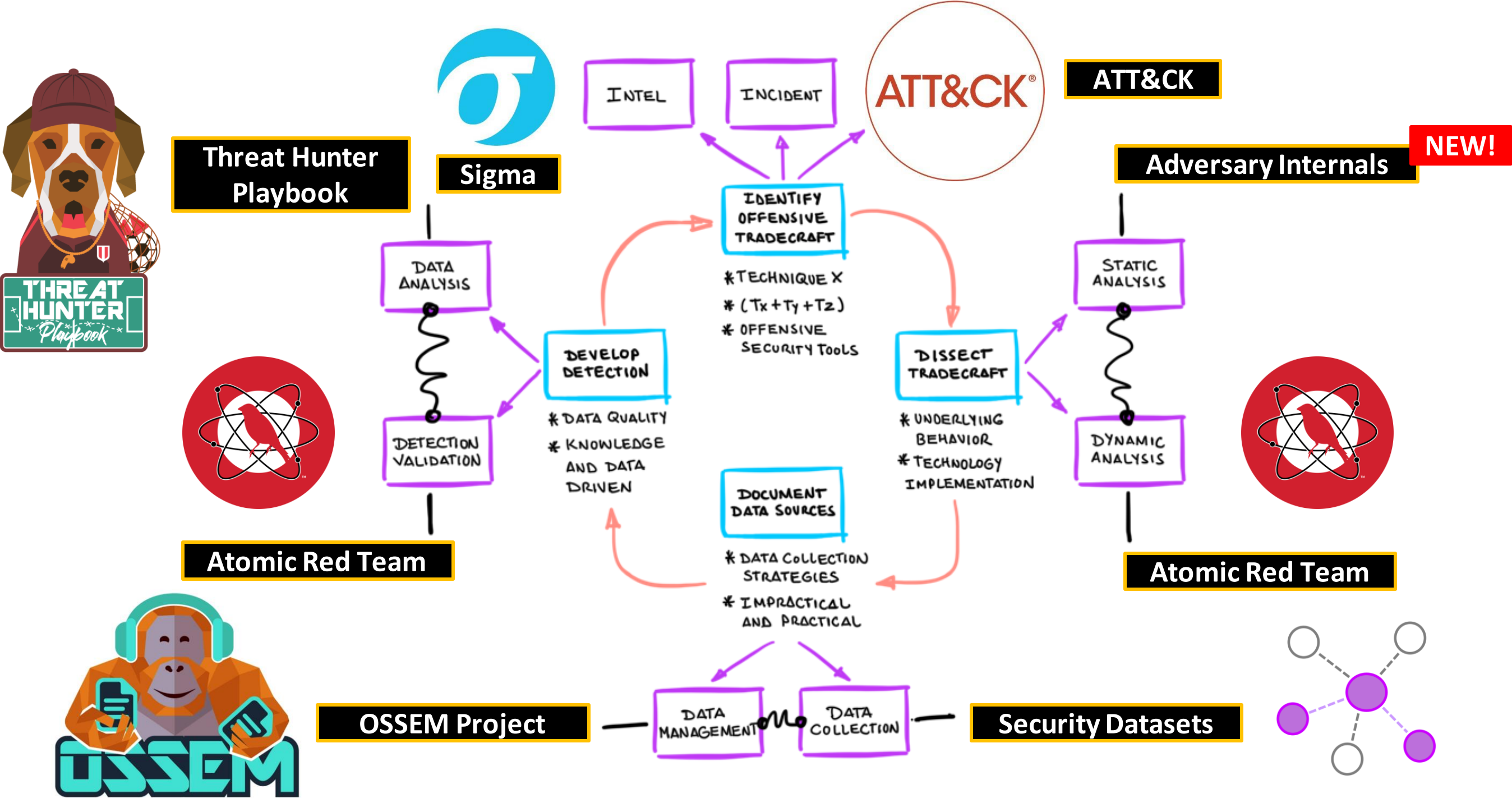
Community Poll Results



Map Your Own Processes to Open Source Projects



Bring Your Own Contribution (BYOC)



Job Requirements -> Do it at work!

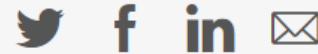
Threat Hunter - Microsoft Threat Intelligence Center

Hyderabad, Telangana, India

Apply now >

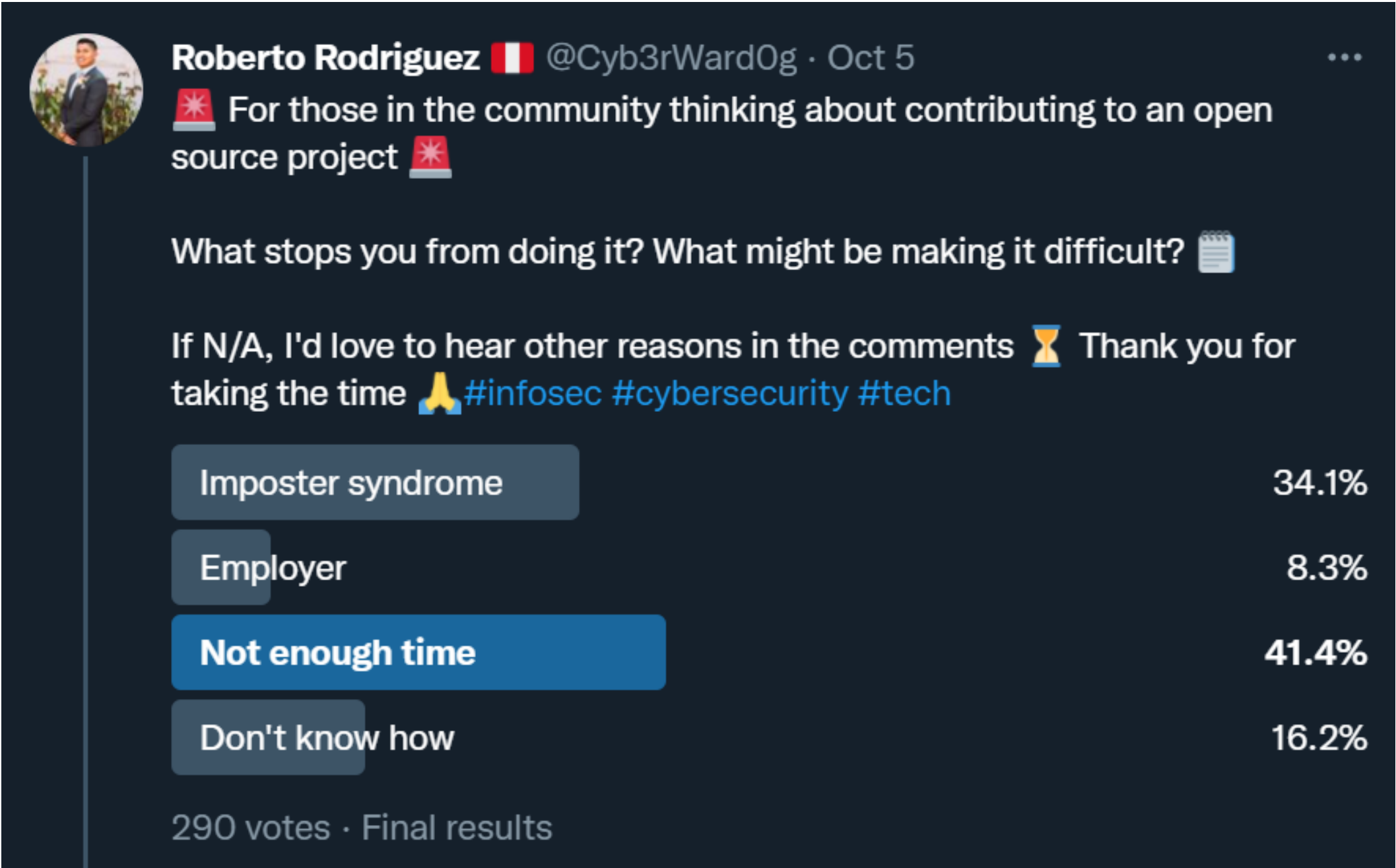
Refer someone >

☆ Save



- Coding and scripting experience, particularly those related to security and data science like KQL, Python, Jupyter Notebooks, R, PowerShell, Common Query languages (SQL, DAX, PowerQuery) is a plus.
- Ability to automate repeatable security tasks through scripts and logic apps and share it with the wider group.
- Knowledge of common attacks and defense in Linux environments a plus.
- Familiarity with developer environment tools like Github/Visualstudio/TFS to share code, track work. etc. is a plus.
- Experience building a community and sharing blog posts, technical write-ups, articles etc.
- Self-motivated and results-oriented, with excellent interpersonal and communication skills.

Community Poll Results



Imposter Syndrome



What is Imposter Syndrome?

- I have not done enough.
- I feel like a fraud. I do not know enough.
- I doubt I am capable of doing it.
- It is only luck! I do not deserve it.
- I need to do more to prove I actually work.

Types:

- Perfectionist
- The superwoman/man
- The natural genius
- The soloist
- The expert

A few tips!

- Think about something that has gone well!
- Accept a compliment.
- Make a list of your achievements.
- Try a new challenge that feels manageable.
- Do NOT compare yourself with another person.
- Do NOT freeze! ;)

A few tips!

- Think about something that has gone well!
- Accept a compliment.
- Make a list of your achievements.
- Try a new challenge that feels manageable.
- Do NOT compare yourself with another person.
- Do NOT freeze! ;)



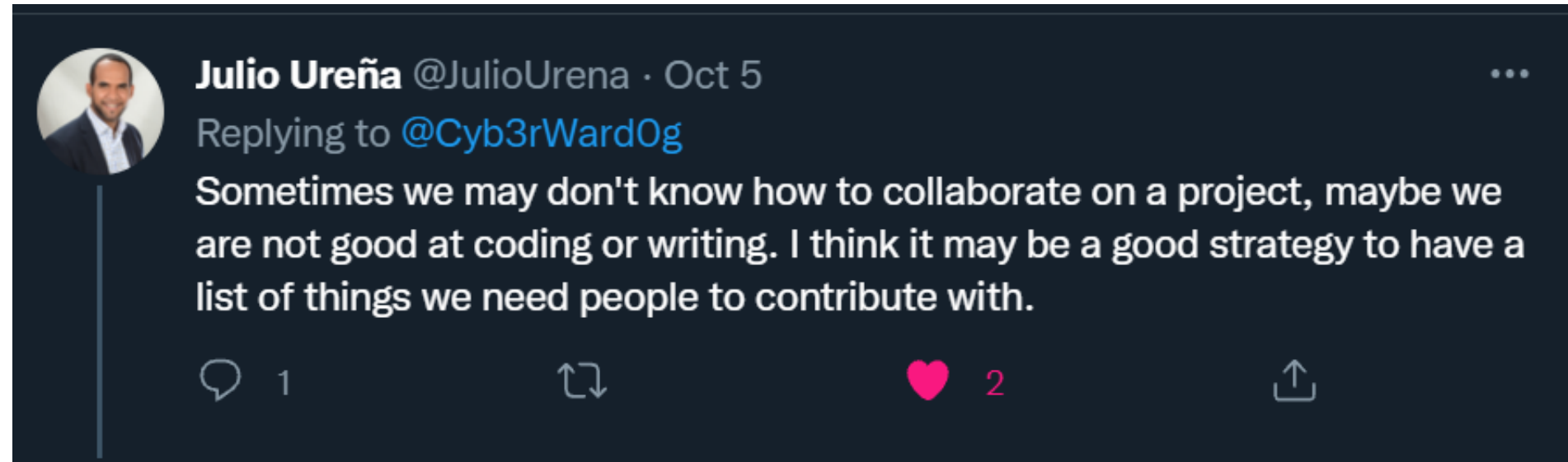
Do not know how!



Help future contributors!

Create a roadmap!

- Create a backlog with new ideas!
- Share the roadmap of the project or **help create one!**



Help future contributors!

Create a roadmap!

- Create a backlog with new ideas!
- Share the roadmap of the project or **help create one!**

<input type="checkbox"/>	9 Open ✓ 0 Closed	Author ▾	Label ▾	Projects ▾
<input type="checkbox"/>	<input checked="" type="radio"/> User Entity might need to be broken down into Managed identity and service principal #35 opened on Sep 1 by Cyb3rWard0g		enhancement	
<input type="checkbox"/>	<input checked="" type="radio"/> Update Python Script Excel/MD to YAML : Ability to convert to event relationship template #30 opened on Jun 23 by ashwin-patil		feature infrastructure	
<input type="checkbox"/>	<input checked="" type="radio"/> Data Objects: Computer & Host #26 opened on Jun 18 by Cyb3rPandaH		documentation hot fix	
<input type="checkbox"/>	<input checked="" type="radio"/> OSSEM Relationships Mapping - Volume Data Source #7 opened on Apr 25 by Cyb3rPandaH		feature research	
<input type="checkbox"/>	<input checked="" type="radio"/> OSSEM Relationships Mapping - Snapshot Data Source #6 opened on Apr 25 by Cyb3rPandaH		feature research	
<input type="checkbox"/>	<input checked="" type="radio"/> OSSEM Relationships Mapping - Cloud Storage Data Source #5 opened on Apr 25 by Cyb3rPandaH		feature research	
<input type="checkbox"/>	<input checked="" type="radio"/> Relationships Mapping - Cloud Service Data Source #4 opened on Apr 25 by Cyb3rPandaH		feature research	
<input type="checkbox"/>	<input checked="" type="radio"/> OSSEM Relationships Mapping - Network Traffic Data Source #3 opened on Apr 25 by Cyb3rPandaH		feature structure	
<input type="checkbox"/>	<input checked="" type="radio"/> Review Relationships Schemas and ATT&CK structure #1 opened on Feb 23 by Cyb3rWard0g			

Tag issues!

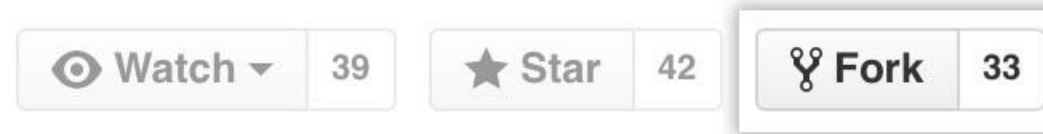
Make it easier!

is:issue label:create-pull is:open

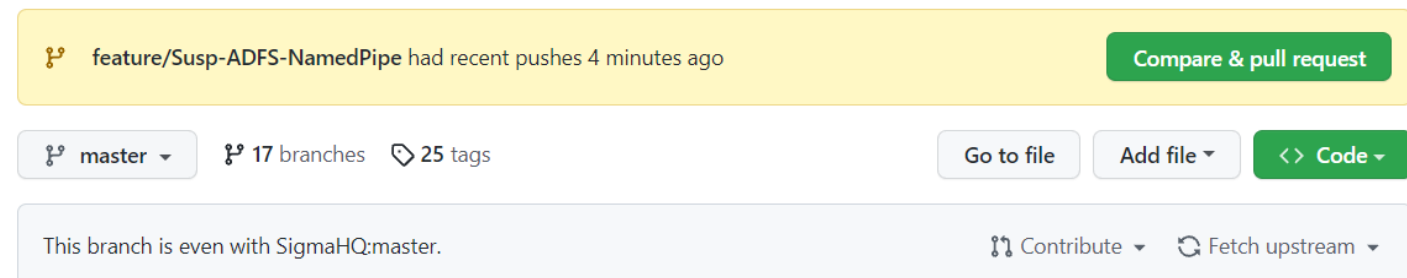
The screenshot shows the GitHub web interface for the repository **SigmaHQ / sigma**, which is marked as **Public**. The navigation bar includes links for **Code**, **Issues** (with a badge showing 129), **Pull requests** (with a badge showing 18), **Discussions**, **Actions**, and **Wiki**. The **Issues** tab is selected, and a search bar at the top of the issues list contains the query **is:issue label:create-pull is:open**. Below the search bar, there is a button to **Clear current search query, filters, and sorts**. The results section shows **1 Open** and **2 Closed** issues. The first issue listed is **Wrong EventID windows/builtin/win_susp_lsass_dump.yml**, which has a green circle icon and a **create-pull** button. The issue details show it was **#1831**, opened on **Aug 12** by **robnantes**.

You Are One Pull Request Away!

- Download Git: <https://git-scm.com/downloads>
- Browse to the project > click **Fork**.



- Clone fork: *git clone repo && cd repo*
- Create branch: *git checkout -b 'feature/new'*
- Make changes to local repo ...
- Add changes to the local index: *git add .*
- Record changes locally: *git commit -m 'comment'*
- Update remote refs (fork): *git push*
- Browse to fork > **Create pull request**



You Are One Pull Request Away!

Open a pull request

Create a new pull request by comparing changes across two branches. If you need to, you can also [compare across forks](#).



base repository: SigmaHQ/sigma ▾

base: master ▾



head repository: OTRF/sigma ▾

compare: feature/Susp-ADFS-NamedPipe ▾

✓ **Able to merge.** These branches can be automatically merged.



Detect suspicious named pipe connections to an AD FS WID

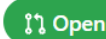
Write

Preview

H B I ≡ <> 🔗 ≡ ≡ ☑ @ ↗ ↶ ▾

Locally, the AD FS Windows Internal Database (WID) does not have its own management user interface (UI), but one could connect to it via a specific named pipe. The named pipe information can be obtained directly from the ConfigurationDatabaseConnectionString property of the SecurityTokenService class from the WMI ADFS namespace.

Detect suspicious named pipe connections to an AD FS WID #2128



Cyb3rWard0g wants to merge 1 commit into [SigmaHQ:master](#) from [OTRF:feature/Susp-ADFS-NamedPipe](#) 📄



Conversation 0



Commits 1



Checks 0



Files changed 1



Cyb3rWard0g commented now

Contributor 😊 ⋮

Locally, the AD FS Windows Internal Database (WID) does not have its own management user interface (UI), but one could connect to it via a specific named pipe. The named pipe information can be obtained directly from the ConfigurationDatabaseConnectionString property of the SecurityTokenService class from the WMI ADFS namespace.

Open PowerShell and run the following commands:

```
$ADFS = Get-WmiObject -Namespace root/ADFS -Class SecurityTokenService
$conn = $ADFS.ConfigurationDatabaseConnectionString
$conn
```

A threat actor can use this method to extract sensitive information from the AD FS WID. Information such as certificates used to, for example, sign a SAML token and impersonate a user.

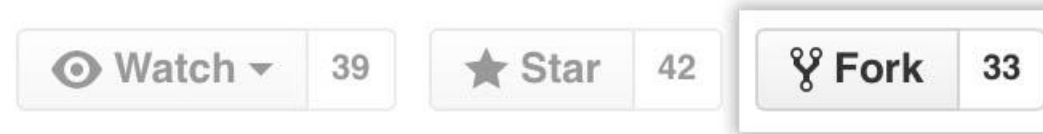


added rule to detect suspicious named pipe connections to an AD FS se... ⋮

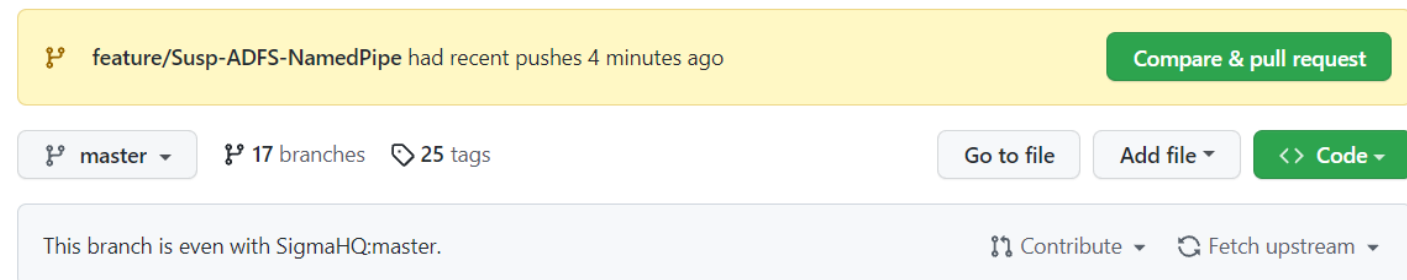
7f17eae

You Are One Pull Request Away!

- Download Git: <https://git-scm.com/downloads>
- Browse to the project > click **Fork**.



- Clone fork: *git clone repo && cd repo*
- Create branch: *git checkout -b 'feature/new'*
- **Make changes to local repo ...**
- Add changes to the local index: *git add .*
- Record changes locally: *git commit -m 'comment'*
- Update remote refs (fork): *git push*
- Browse to fork > **Create pull request**



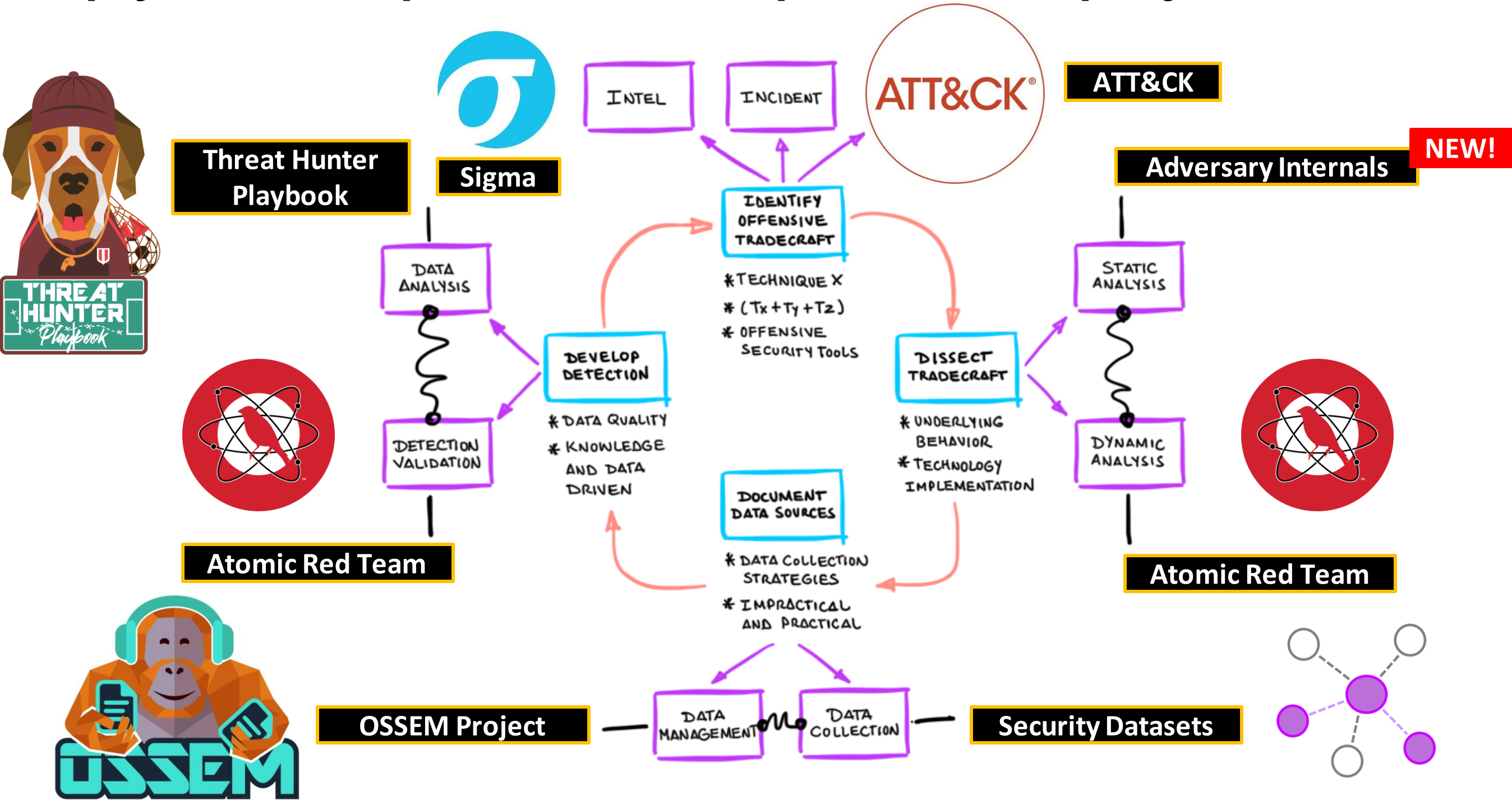
Contribute Back!

Call to Action!



Research Step	Open Source Project	What can you do?
Identify tradecraft	<ul style="list-style-type: none"> MITRE-ATT&CK (https://attack.mitre.org/) TRAM (https://github.com/center-for-threat-informed-defense/tram/) AC3 Threat Sightings (https://mcafee-enterprise.github.io/ac3-threat-sightings/docs/Welcome) MISP (https://github.com/MISP/MISP) RE&CT Framework (https://github.com/atc-project/atc-react) ATC – Mitigation (https://github.com/atc-project/atc-mitigation) ATT&CK Python Client (https://github.com/OTRF/ATTACK-Python-Client) 	<ul style="list-style-type: none"> Help with documentation Share research Add new techniques to ATT&CK Provide feedback
Dissect tradecraft	<ul style="list-style-type: none"> Tiny Tracer (https://github.com/hasherezade/tiny_tracer) NtObjectManager (https://github.com/googleprojectzero/sandbox-attacksurface-analysis-tools/tree/master/NtObjectManager) PerfView (https://github.com/Microsoft/perfview) Adversary Emulation Library (https://github.com/center-for-threat-informed-defense/adversary_emulation_library) Atomic Red Team (https://github.com/redcanaryco/atomic-red-team) Atomic Test Harnesses (https://github.com/redcanaryco/atomic-test-harnesses) Attack Range (https://github.com/splunk/attack_range) Azure Sentinel To-Go (https://github.com/OTRF/Azure-Sentinel2Go) DetectionLab (https://github.com/clong/DetectionLab) Blacksmith (https://github.com/OTRF/Blacksmith) 	<ul style="list-style-type: none"> Help with documentation Contribute atomic tests Share research environments Request new research environments Share how you actually do research Provide feedback
Document data sources	<ul style="list-style-type: none"> OSSEM (https://github.com/OTRF/OSSEM) Azure Sentinel Information Mode – ASIM (https://github.com/Azure/Azure-Sentinel/tree/master/Parsers/ASim) Elastic Common Schema – ECS (https://github.com/elastic/ecs) ATT&CK Data Sources (https://github.com/mitre-attack/attack-datasources) Atomic Data Sources (https://ctid.mitre-engenuity.org/our-work/atomic-data-sources/) Security Datasets (https://github.com/OTRF/Security-Datasets) EVTX Attack Samples (https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES) MacOS Attack Dataset (https://github.com/sbousseaden/macOS-ATTACK-DATASET) PCAP Attack (https://github.com/sbousseaden/PCAP-ATTACK) Attack Data (https://github.com/splunk/attack_data) 	<ul style="list-style-type: none"> Help with documentation Share new sources of data Contribute datasets from your lab environments Provide feedback
Develop Detection	<ul style="list-style-type: none"> MSTICPy (https://github.com/Microsoft/msticpy) Daisy (http://www.ds4n6.io/daisy) Threat Hunter Playbook (https://github.com/OTRF/ThreatHunter-Playbook) Sigma (https://github.com/SigmaHQ/sigma) CAR Analytics (https://github.com/mitre-attack/car) Elastic Detection Rules (https://github.com/elastic/detection-rules) Splunk Security Content (https://github.com/splunk/security_content) Azure Sentinel (https://github.com/Azure/Azure-Sentinel) 	<ul style="list-style-type: none"> Help with documentation Share detection logic Share the research process with other open source tools such as Jupyter Notebooks Provide feedback

Map your own processes to open source projects!





Open Threat Research - Discord server

<https://discord.com/invite/efBGmbQ>

Thank you!

 <https://github.com/OTRF>

 @Cyb3rWard0g