FACT SHEET

Considering Cyber Discovery?

A Strategic Framework from HaystackID™

HAYSTACK™

HaystackID™ Cyber Discovery

Provided for your review and use is a non-comprehensive overview of definitions, depictions (graphical), and descriptions that may be helpful in considering the conduct of cyber discovery. The presented overview* represents a framework based on high-level artificial intelligence lifecycle stages as developed by the European Union Agency for Cybersecurity (ENISA)[1] modified through the lens of traditional eDiscovery planning and practices grounded within the Electronic Discovery Reference Model (EDRM)[2]. The modification attempts to combine computer-centric artificial intelligence and machine learning models with data and legal discovery developed protocols and tools to provide a high-level generic reference model for considering cyber discovery stages and tasks.

Defining Cyber Discovery: Definitions, Depiction, and Discussion

In discussing the framing of cyber discovery stages and tasks within a generic reference model, it is first important to provide several definitions that may be helpful in understanding the relationships between cyber discovery, data discovery, and legal discovery.

Reference Definitions

Cyber Discovery: The application of a combination of data discovery and legal discovery approaches to enable the exploration of patterns, trends, and relationships within unstructured and structured data with the objective of uncovering insight and intelligence to proactively or reactively respond to cybersecurity-centric challenges.[3]

Data Discovery: The exploration of patterns and trends within unstructured data with the objective of uncovering insight.[4]

Legal Discovery (eDiscovery): The process of identifying, preserving, collecting, processing, searching, reviewing, and producing electronically stored information that may be relevant to a civil, criminal, or regulatory matter with the objective of uncovering intelligence.[5]

Insight: The understanding of cause and effect based on the identification of relationships and behaviors within a model, context, or scenario.[6]

Intelligence: The ability to acquire and apply knowledge and skills.[7]

Reference Descriptions (Stages and Tasks)

Preparation: Initiation of the Cyber Discovery Process

- **Cyber Discovery Goals:** Identifies the purpose of cyber discovery requirements. Links the purpose with the questions to be answered by the models, protocols, and tools to be used in the cyber discovery approach. Identifies model, protocol, and tool types based on the questions to be answered.

- **Data Collection and Ingestion:** Identifies the input data to be collected and ingested and the corresponding context metadata. Organizes ingestion according to model and protocol requirements, importing data in a stream, batch, or multi-model fashion.

- **Data Exploration:** Identifies the attributes of data collected and ingested as assessed for use with potential models and protocols. Considers data appropriateness for answering questions related to cyber discovery goals.

- **Data Processing:** Converts, integrates, and normalizes ingested data to facilitate data use as part of selected models and protocols with required applications necessary for answering questions related to cyber discovery goals.

Planning: Model and Protocol Planning

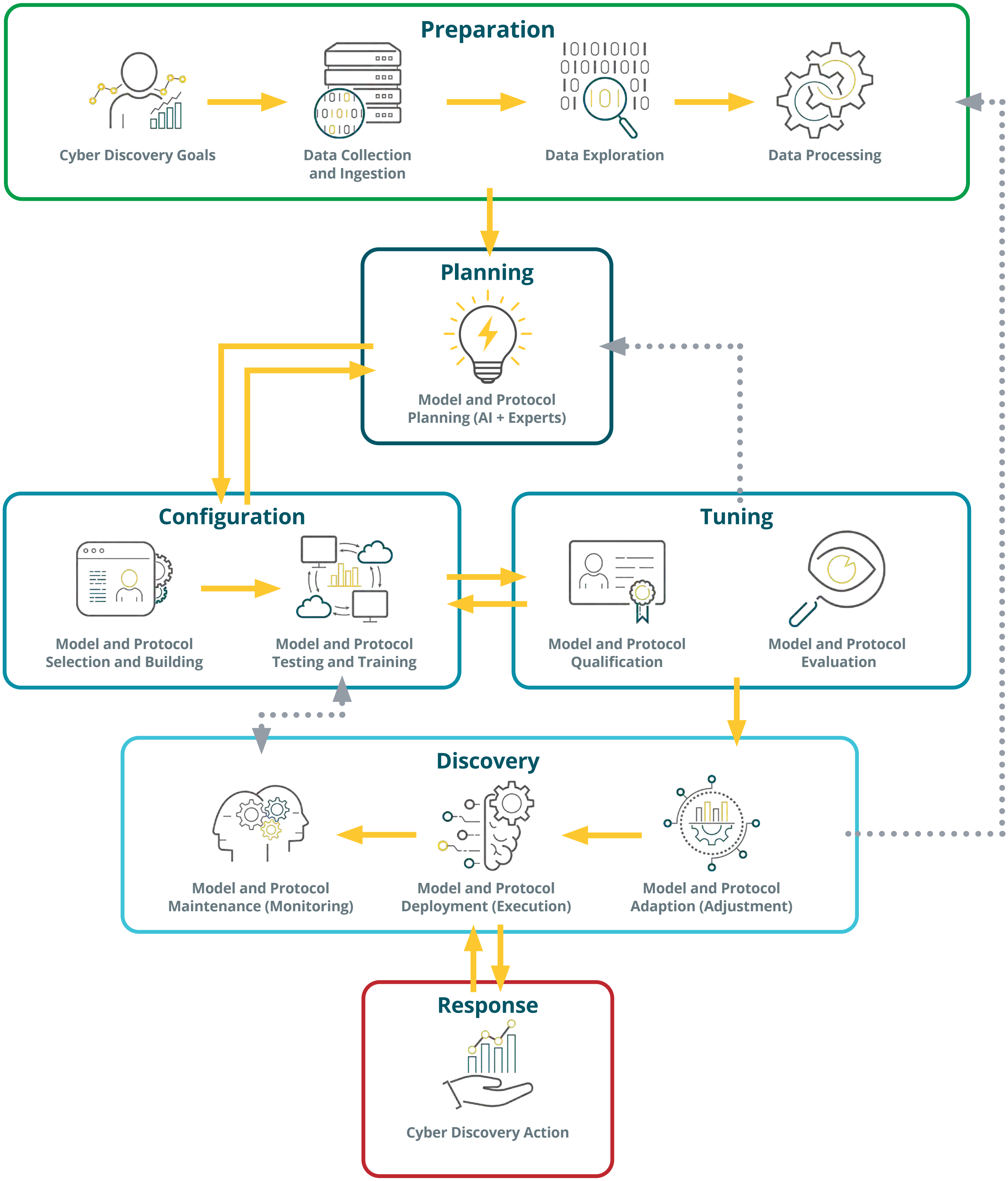
- **Model and Protocol Planning (AI + Experts):** Identifies the data set dimensions based on preparation stage efforts and determines the most effective models, protocols, and tools to be selected, built, tested, trained, and tuned prior to cyber discovery.

Configuration: Selection, Building, Testing, and Training

- **Model and Protocol Selection and Building:** Selection and building (customization) of the models, protocols, and tools most suitable for the identified cyber discovery goals.

- **Model and Protocol Testing and Training:** Applies the selected models, protocols, and tools against a training set of appropriate data to validate selected cyber discovery approaches.

*Considering Cyber Discovery: From Preparation to Response**


Preparation
Cyber Discovery Goals
Data Collection and Ingestion
Data Exploration
Data Processing
Planning
Model and Protocol Planning (AI + Experts)
Configuration
Model and Protocol Selection and Building
Model and Protocol Testing and Training
Tuning
Model and Protocol Qualification
Model and Protocol Evaluation
Discovery
Model and Protocol Maintenance (Monitoring)
Model and Protocol Deployment (Execution)
Model and Protocol Adaption (Adjustment)
Response
Cyber Discovery Action

Tuning: Qualification and Evaluation

- **Model and Protocol Qualification:** Applies the selected models, protocols, and tools against a validation set of appropriate data to qualify selected cyber discovery approaches.

- **Model and Protocol Evaluation:** Applies the selected models, protocols, and tools against a validation set of appropriate data to evaluate selected cyber discovery approaches.

Discovery: Adaptation, Deployment, and Maintenance

- **Model and Protocol Adaptation (Adjustment):** Leverages pre-trained and pre-tuned models, protocols, and tools to serve as the starting point for faster and more efficient achievement of cyber discovery goals as defined by cyber discovery objective questions.

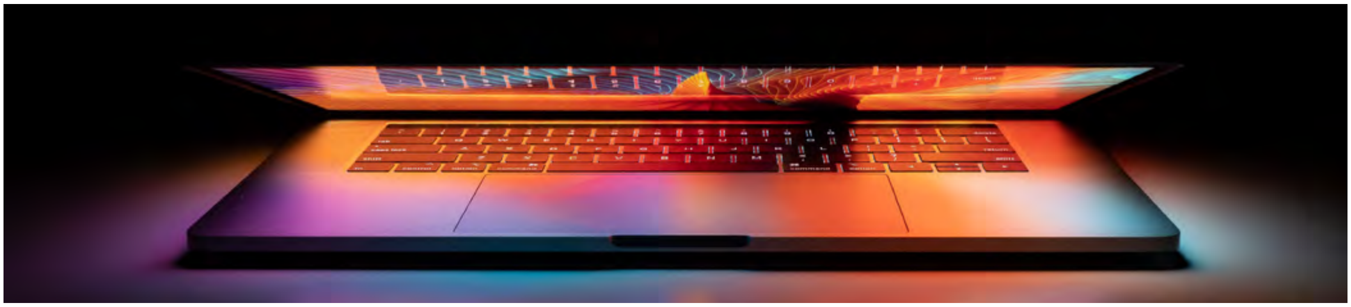
- **Model and Protocol Deployment (Execution):** Takes trained models, protocols, and tools and makes them available to data scientists, data providers, and data reviewers to answer questions defined in cyber discovery objective questions.

- **Model and Protocol Maintenance (Monitoring):** Monitors models, protocols, and tools and their impact on the achievement of defined cyber discovery objectives.

Response: Cyber Discovery Understanding

- **Cyber Discovery Action:** Assesses the value proposition of the deployed models, protocols, and tools. Estimates (before deployment) and verifies (after deployment) the achievement of insight and intelligence objectives that can answer defined cyber discovery goal questions and drive an appropriate business, legal, or regulatory response.

This non-all-inclusive reference model may be useful for visualizing one potential approach to cyber discovery. It may also be useful for framing discussions that dive deep into the conduct of specific cyber discovery actions ranging from proactive cybersecurity assessments to reactive post-data breach discovery and review efforts in support of incident responses.



References

[1] European Union Agency for Cybersecurity, 2020. *Artificial Intelligence Cybersecurity Challenges*. [online] European Union Agency for Cybersecurity. Available at: https://digital-strategy.ec.europa.eu/en/library/report-artificial-intelligence-cybersecurity-challenges [Accessed 2 May 2021].

[2] EDRM | Empowering the Global Leaders of eDiscovery. 2021. EDRM. [online] Available at: https://edrm.net/. [Accessed 2 May 2021]

[3] Robinson, R., 2021. *Considering Cyber Discovery? A Strategic Framework.* [online] ComplexDiscovery. Available at: https://complexdiscovery.com/ [Accessed 2 May 2021].

[4] All, A., 2014. *Data Discovery Is Changing Business Intelligence.* [online] Enterprise Apps Today. Available at: http://www.enterpriseappstoday.com/business-intelligence/data-discovery-is-changing-business-intelligence.html [Accessed 2 May 2021].

[5] Grossman, M. and Cormack, G., 2013. The Grossman-Cormack Glossary of Technology-Assisted Review. *Federal Courts Law Review*, [online] 7(1). Available at: https://www.fclr.org/fclr/articles/html/2010/grossman.pdf [Accessed 2 May 2021].

[6] Wikipedia. 2021. *Insight*. [online] Available at: https://en.wikipedia.org/wiki/Insight [Accessed 2 May 2021].

[7] In: *Lexico (Oxford)*. 2021. Intelligence. [online] Available at: https://www.lexico.com/definition/intelligence [Accessed 2 May 2021].

Source: HaystackID

Learn More. Today.

Contact us today to learn more about how HaystackID can help solve specific and critical Cyber Discovery challenges with offerings to include our ReviewRight® Protect™ post-data breach discovery and review services.

About HaystackID

HaystackID™ is a specialized eDiscovery services firm that helps corporations and law firms securely find, understand, and learn from data when facing complex, data-intensive investigations and litigation. HaystackID mobilizes industry-leading cyber discovery services, enterprise managed solutions, and legal discovery offerings to serve more than 500 of the world's leading corporations and law firms in North America and Europe. Serving nearly half of the Fortune 100, HaystackID is an alternative cyber and legal services provider that combines expertise and technical excellence with a culture of white-glove customer service. In addition to consistently being ranked by Chambers, the company was recently named a worldwide leader in eDiscovery services by IDC MarketScape and a representative vendor in the 2021 Gartner Market Guide for E-Discovery Solutions. For more information about its suite of services, including programs and solutions for unique legal enterprise needs, go to HaystackID.com.