Case Study for a Cyber Threat Monitoring Platform

Identification of Potential Security Vulnerabilities and Data Leaks

Powered by Artificial Intelligence

traversals

Introduction

World of Cyber Threats

The average time it takes to identify a cyber security incident is 197 days, according to the 2018 Cost of a Data Breach Study by the Ponemon Institute, funded by IBM. Companies that identify and combat an incident within 30 days have a significant advantage over their less responsive competitors and save an average of $1 million in containment costs.

“Employing dark web monitoring solutions that allow the use of focused filters to identify key phrases, such as your brand and product names, that may contain information that can negatively affect your organization is a good start in your effort to glean useful intelligence from the dark web,” McMillen said.

Collected data should be pre-evaluated and, if relevant, confirmed or re-evaluated by an analyst. The aim is to provide realisable insights. Detected threats can indicate various risks within the company.

The best protection is to combine the intelligence of qualified investigators and AI to effectively transform raw data into actionable intelligence.

Traversals’ Solution

The Traversals Cyber Threat Monitoring Platform is aimed at all companies seeking active protection for their business, brand, reputation or company assets of any type. It continuously monitors all levels of the internet to identify cyber threats such as data leaks. With the help of AI, false alarms are reduced and true positives increased.

Phase one of the platform will focus on the digital footprint of enterprises. Upcoming phases will include classical cyber threat

intelligence and integrate additional sources of information such as, door access control systems. A correlation with the latter helps to identify the source of the data leak.

Technical Overview

Enterprise Knowledge Graph

The Traversals Cyber Threat Monitoring Platform allows enterprises to securely store relevant entity information such as HR data, IT data or product/project information in an easily searchable environment that is accessible to both investigators and processing machines. In addition to the entity information, the Enterprise Knowledge Graph also stores information about the relationships between entities, such as hierarchies.

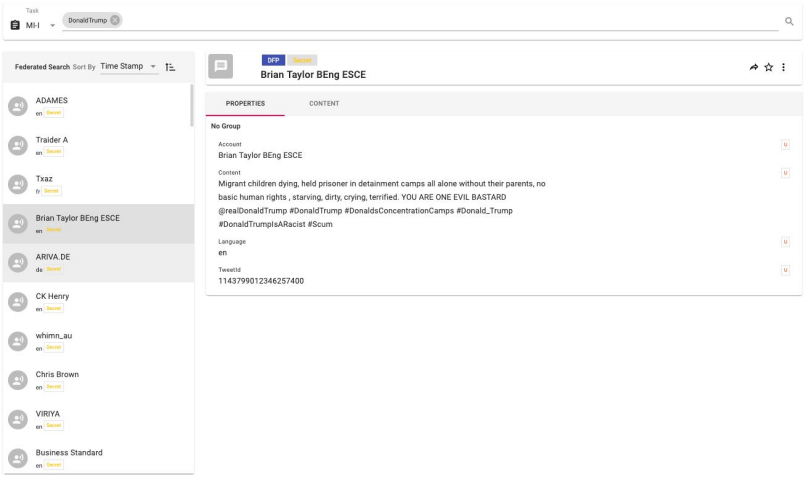
All data stored in the system is categorized with configurable classification levels as known in the US, such as UNCLASSIFIED, SECRET or TOP SECRET, or according to the German system, such as VS-VERTRAULICH, GEHEIM or STRENG GEHEIM. It guarantees confidentiality of the information. Through an attribute-based access control system, it can be guaranteed that analysts and processing machines only see the information to which they have access. All queries and mutations executed by an analyst or even a machine, are logged and available for security audits.

Federated Search

Traversals Cyber Threat Monitoring Platform seamlessly bridges and connects common search engines of both dark and surface web and other open-source data sources with your enterprise data by offering a single point of search. The Federated Search acts as a data virtualization layer within the platform. External data providers are secured via TOR.

Natural Language Processing and Artificial Intelligence are used before each search to enhance and improve search results. For example, search terms are translated into different languages or supplemented by synonyms. In addition, Natural Language Processing provides access to foreign-language databases by translating the search query and retranslating the found texts.

Interesting search results can be manually or automatically imported into the Cyber Threat Monitoring Platform's integrated repository, leveraging enterprise functions such as additional automatic processing or permission control. By using Federated Search, organizations can easily and quickly find and persist critical information that would otherwise remain hidden.



Traversals Cyber Threat Monitoring Platform features a federated search that allows a single point of search on top of search engines and data sources.

Automated Searches

Processing modules running in the Cyber Threat Monitoring Platform leverage the information stored in the Enterprise

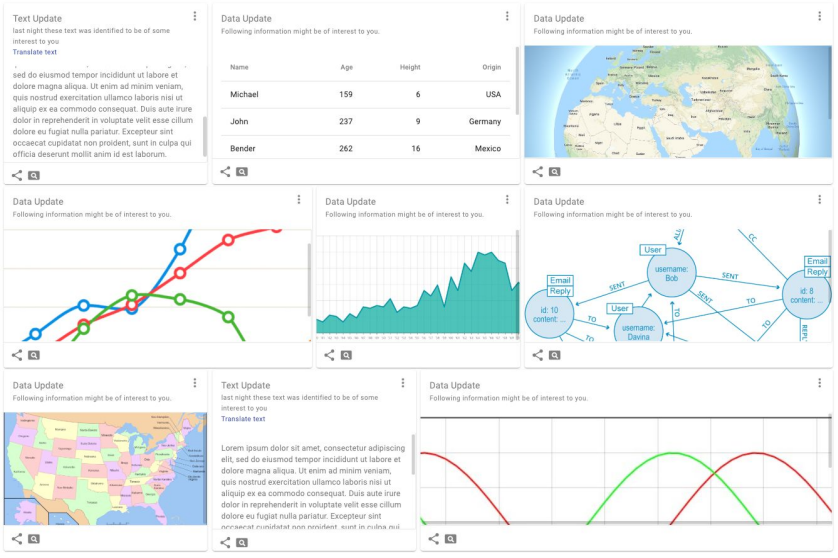
Knowledge Graph, e.g., product names or email addresses, and automatically query against Federated Search.

Results of the automated searches are forwarded to the Cyber Threat Monitoring Platform's notification feeds to shorten response time.

Automatic searches ensure that changes in prior knowledge are immediately taken into account. Even if no active search is performed, the system works in the background to immediately detect possible cyber threats.

Notification Feeds

Notification feeds in the Cyber Threat Monitoring Platform give investigators a continuous picture of interesting search results. Notifications contain information about the when, where, and what, and have a classification level derived from the information stored in the Enterprise Knowledge Graph.

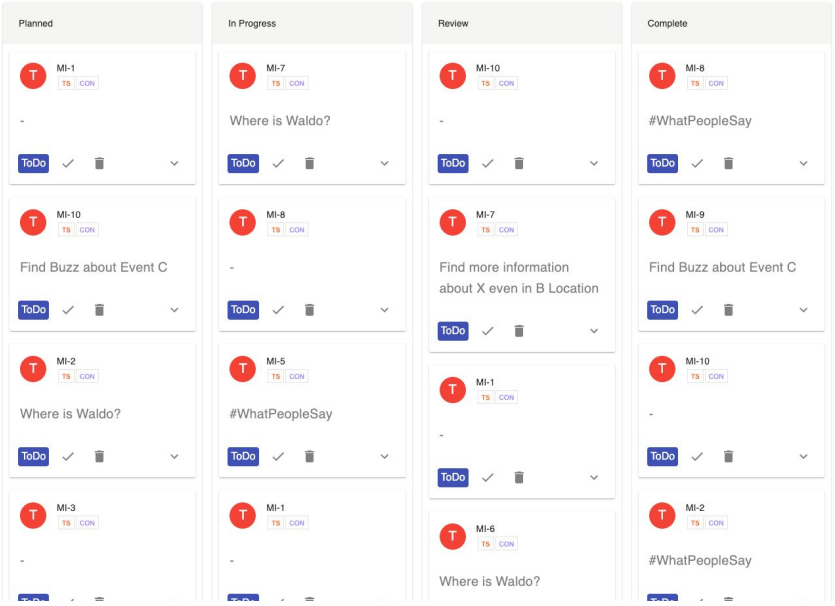


Traversals Cyber Threat Monitoring Platform features

notification feed which delivers the user a constant update of incoming information.

Agile Task Board

Being secure means being agile. The world of security moves fast and attackers prey on organizations with sticky feet. They benefit from the fact that organizations change only slowly. Staying agile and keeping the Cyber Threat Monitoring Platform up to date and relevant enables companies to focus on today's primary threat vectors and not those from six months ago. The Cyber Threat Monitoring Platform features an Agile Task Board with classification levels, such as UNCLASSIFIED, SECRET or TOP SECRET, known from the Enterprise Knowledge Graph. The Agile Task Board promotes collaboration, understanding of requirements, team connectivity and time to value.



Traversals Cyber Threat Monitoring Platform includes an Agile Task Board to keep pace with a rapidly changing world of security.

Operational Overview

System Size

The Cyber Threat Monitoring Platform is based on Traversals' Data Fusion Platform. It is horizontal scalable in all aspects. Entry-level systems can start with six CPU cores running on a Laptop and scale to multiple IT racks for mass data processing and high availability.

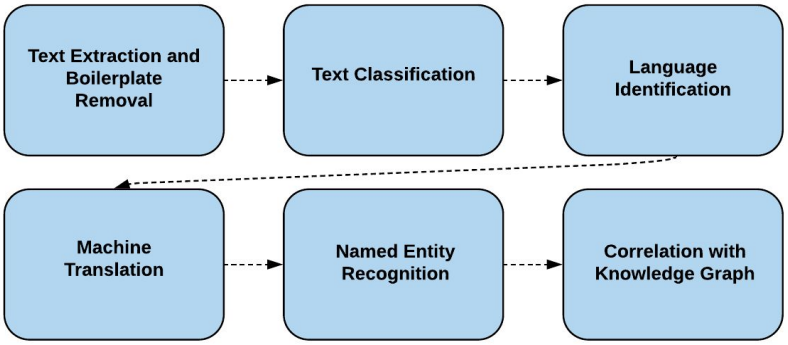
Constant and Secure Updates

Since the data world is constantly and quickly changing, it is necessary to keep monitoring systems permanently up to date. The Cyber Threat Monitoring Platform is part of Traversals' Secure Software Supply Chain which ensures that secure libraries without known vulnerabilities/threats are used.

System Extensions

Natural Language Processing

The Cyber Threat Monitoring System is a modular system based on Traversals' Data Fusion Platform. Thus, it can be extended easily and efficiently with new processing modules, entity types and user interface elements.



Extension of the Cyber Threat Monitoring Platform with an AI

powered NLP chain.

In this way, additional Natural Language Processing and other AI modules can be added, e.g., machine translation for making foreign language texts understandable or named entity recognition for creating new entities in the Enterprise Knowledge Graph.

Additional Data Sources

As the Cyber Threat Monitoring Platform is based on Traversals' Data Fusion Platform, new data sources can be added at any time. The semantic model for the Federated Search and the Enterprise Knowledge Graph can be extended with new entities and relations, e.g. to integrate door control systems for the localization of a data leak.

Make Data Speak Your Language

Traversals is an analysis and intelligence company based in Erlangen/Germany. It offers software products and related services for companies and authorities. Traversals plays a decisive role in making data understandable for people who are not data scientists.

For More Information

If you have questions or would like to discuss this data sheet, please contact us. As an advocate of innovative IT solutions, we are committed to keeping a dialogue open on technologies, processes and best practices that will help us to support our customers.

Contact

Web: www.traversals.com
Phone: +49 9131 92790 0
Fax: +49 9131 92790 99
Email: info@traversals.com