SAVANNA

WHITE PAPER

Analyzing Cybersecurity Risk with Savanna

Thetus Corporation, 326 SW Broadway, Portland, Oregon 97209, USA.

TABLE OF CONTENTS

EXECUTIVE OVERVIEW

Lurking in the shadows behind your favorite websites and apps, cyber attacks are more prevalent than ever. Cybersecurity has become a high-profile issue, with large corporations around the world experiencing security breaches on a regular basis. As the variety of available technology systems evolves and grows every day, from personal computers, tablets, and beyond, the number of systems that enterprises need to defend grows too. Combine this with the constantly evolving nature of cyber threats and it becomes apparent that new approaches to cybersecurity are necessary.

Corporate leaders must make decisions based upon their present understanding of risks, regardless of how imperfect the available information. Anecdotal knowledge provides spotty insights, commercial media is too broad, and quantitative data requires appropriate context. Yet by synthesizing these and other forms of data into a comprehensive narrative, corporate analysts can anticipate risks with accuracy and efficiency.

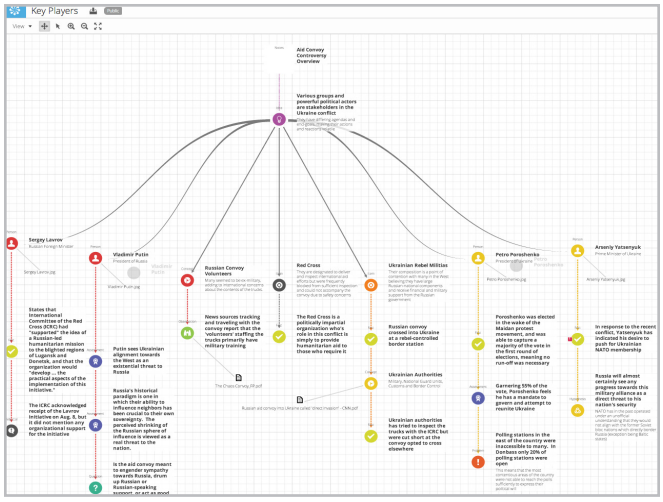
Employing models to extend the utility of qualitative information, and working within a single shareable, secure platform, analysts can further operationalize tacit knowledge and contextualize information, providing decision-makers with the insight needed to prepare for the unknown.

To address this rapid evolution and development of cyber threats, enterprises are turning to big data analytics to detect and defend against attacks. However, the sheer volume of data reporting and false positive rates are daunting to analyze and require a solution to extend data results. Savanna's dynamic, all-source analysis environment, combined with Splunk's Enterprise Security machine data-gathering platform, gives analysts the ability to investigate each point of interest, discovering connections and evidence to implement strategies for prevention methods.

ANTICIPATING OUTCOMES WITH SAVANNA

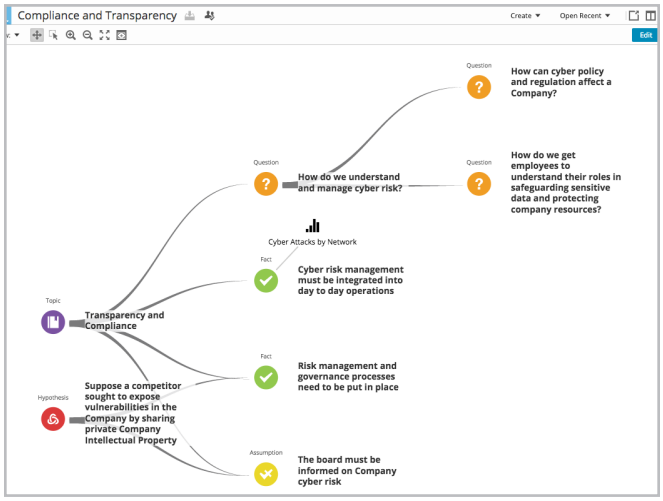
Threats to quickly evolving technology systems require a unique, multi-faceted approach to assessing and dealing with potential risks. With the appropriate tools and expertise, stakeholders can anticipate potential outcomes and prepare accordingly.

Savanna, Thetus Corporation's flagship browser-based analysis platform, enables analysts to model complex problems. By identifying key information and visualizing relationships between structured and unstructured data, Savanna users construct holistic narratives that convey known risks as well as information gaps.



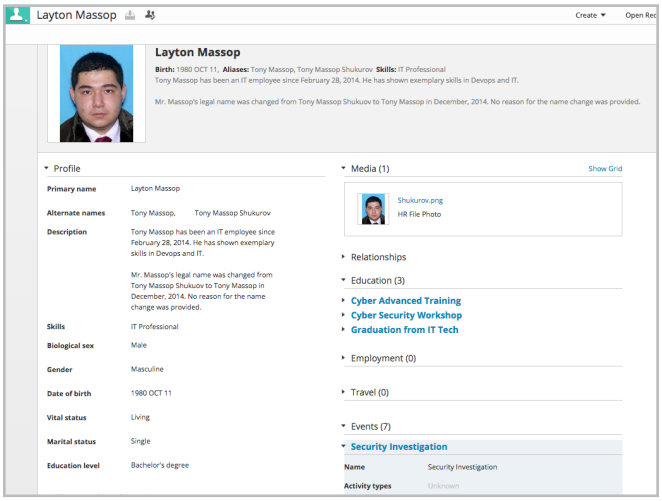
Synthesize Information

In assessing cyber threat risks, analysts must use various forms of data, including text, video, audio, quantitative data, and geographical data. Savanna's search and upload capabilities enable users to unite diverse data formats into a single view.



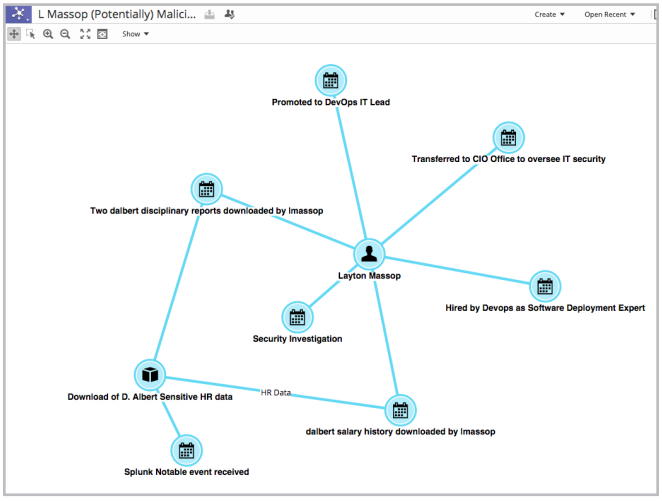
Contextualize and synthesize information with Crumbnet

Savanna Crumbnets serve as white boards for free-form analysis. Crumbnets allow analysts to capture questions, hypotheses, and assumptions to create an analysis narrative and place relevant data in context (e.g., Analyst's Notebook Charts, documents, images, other Crumbnets, videos, and much more). Analysts use Crumbnets to collaboratively ask and answer questions, pose hypotheses, note assumptions and state relevant facts to contextualize data. Crumbnets also serve as a navigation tool to guide audiences through the analysis.



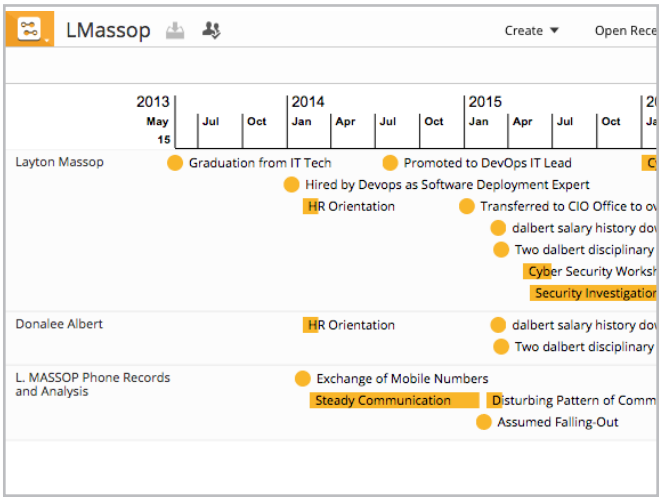
Build interconnected information networks with Occurrences

Occurrences are the problem-specific building blocks of an information network. With Occurrences, Savanna users can quickly access and add new discoveries and pull on existing data to connect information. With Occurrence templates, analysts can set requirements, define important fields and identify information gaps. These templates capture problem-specific information in a uniform way, eliminating redundancy and creating a common analytical framework that analysts can build on. Occurrences are fully sourced and linked between related profiles, allowing users to easily navigate between connected information.



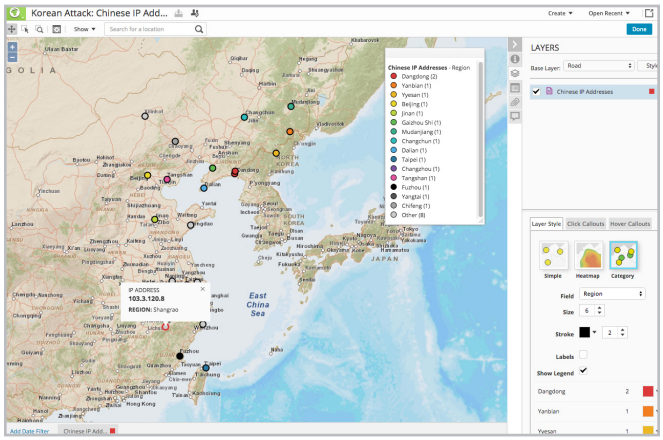
Visualize connections and relationships with Linknet

Analysts can add multiple Occurrences from the information network to a Linknet to view interconnected people, places, organizations, events and things by simply dragging and dropping. Occurrences in the Linknet are fully sourced, allowing analysts to easily access information about individual entities on the Linknet. Analysts can also run network analytics to gather statistical measures about the Linknet data, such as centrality, density, distance and more.



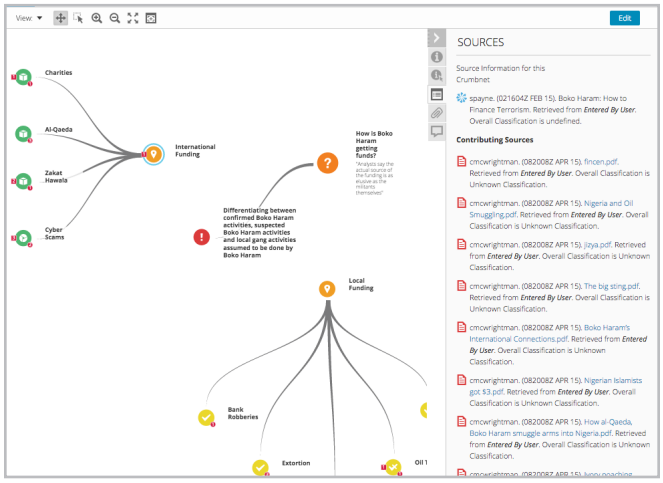
Temporally visualize information with Timeline

With Timeline, analysts can temporally visualize Occurrences (people, organizations, places, events and things) and their associated events by simply dragging Occurrences onto the Timeline. With Timeline, users can interact with Occurrence events by zooming, panning, drilling down for more specific information, and filtering with a temporal filter.



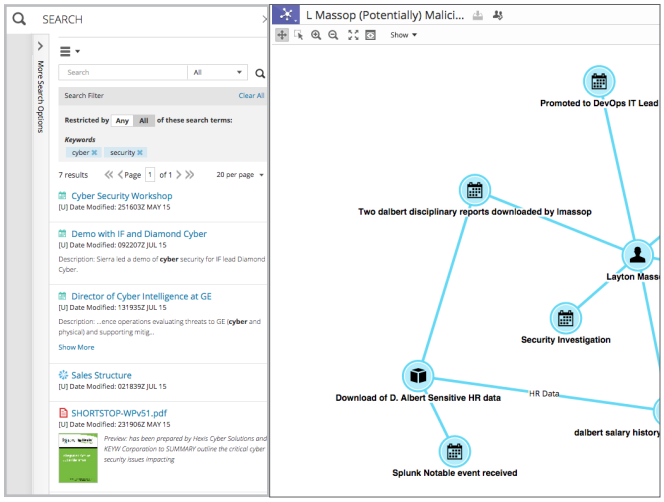
Visualize geographic data in Savanna's enterprise-level mapping tool

Using geographic data or a CSV file containing geographic coordinates, analysts can create and stylize maps to complement their analysis. Automated mapping of data sets facilitates visualization of large quantities of geographic information while customization tools allow the user to modify colors, base layers, and data visibility.



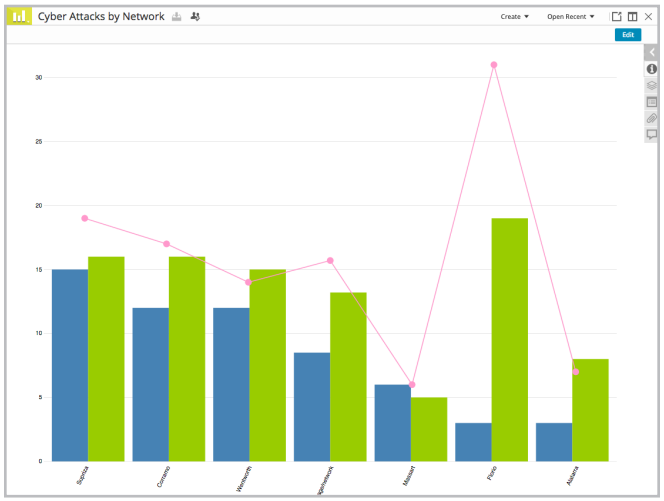
Support analysis conclusions with evidence created in Savanna and from other sources

Analysts collaborate on Crumbnets to support their conclusions with content created in Savanna, such as a screenshot image of a Map and relevant research. Viewers explore evidence in the form of documents, images, videos, maps, notes, quantitative data, and profiles of people, places and organizations.



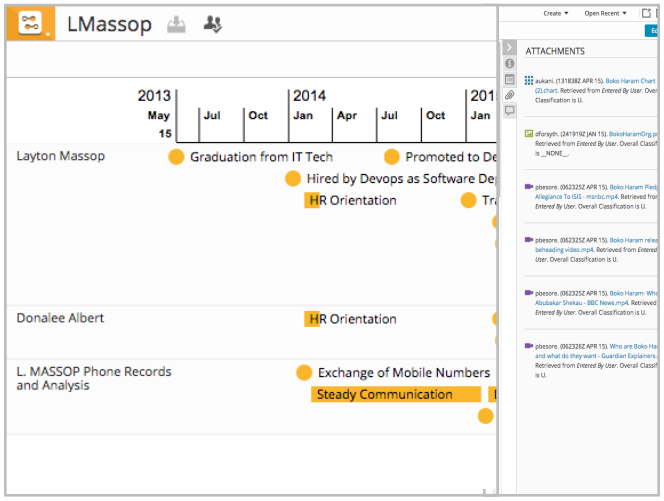
Discover external data and Savanna model content through keyword search and filtering

Savanna's search capabilities enable analysts to find relevant content among public material on the shared network, as well as through external sources with data access layers (DALs). Users can discover relevant data by keyword, file type, date published, classification level, and more. Searches can then be saved to a Space, where analysts receive alerts when new content related to the search parameters becomes available.



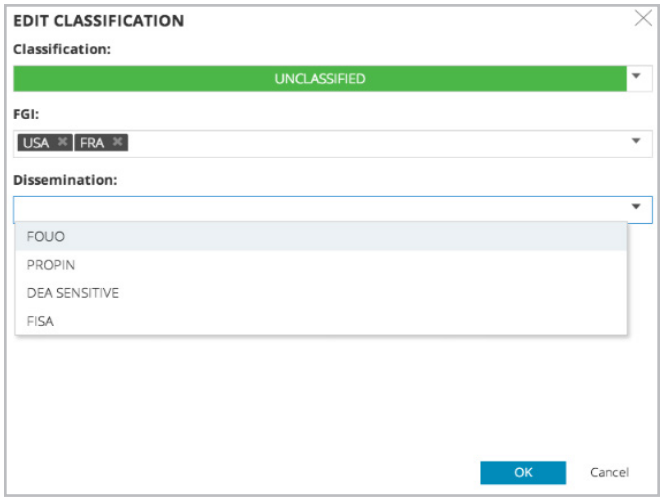
Visualize structured data as charts

With the Graphic tool, users can visualize structured data inside Savanna as charts (pie, bar, line) by simply dragging and dropping datasets onto the Graphic background. With Graphic, analysts can pick multiple columns of data to visualize on the chart, and choose custom style settings to visually differentiate the data.



Understand how information changes over time by tracking provenance and lineage

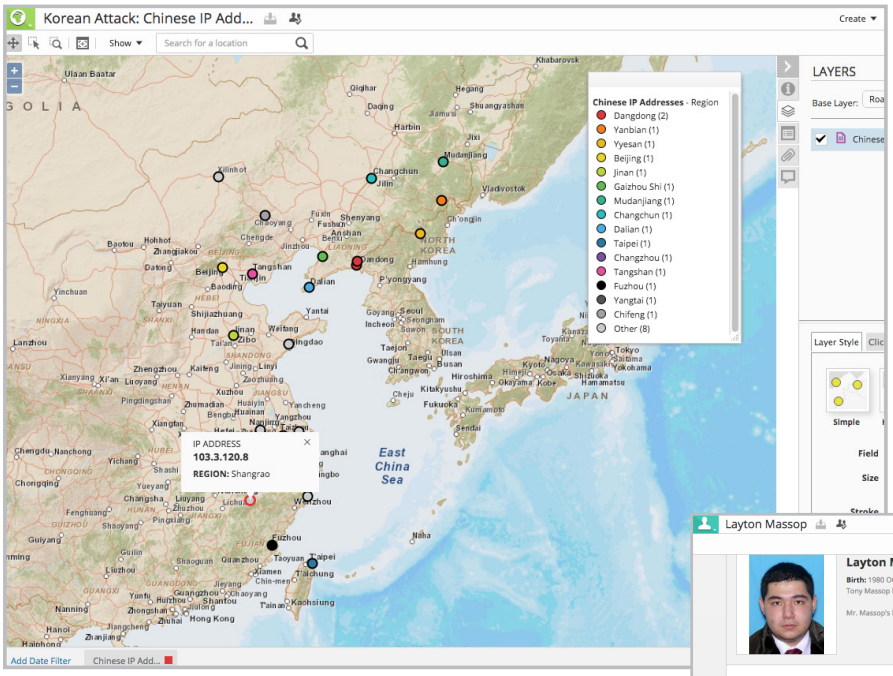
Savanna users have multiple options to describe information, including adding citation details, linking to contributing sources, attaching reference materials, and organizing related information in a Space. Savanna automatically captures details like citations and user activity for content created within Savanna.



Manage privacy settings to control access to classified information

Administrative controls enable careful management of user access to information. Users select private or public settings for material they create or upload. They can also mark information according to its classification level, thereby permitting public view of the information only for those users whose accounts are set to the same classification level.

SPOTLIGHT: NOTABLE THREAT, LAYTON MASSOP



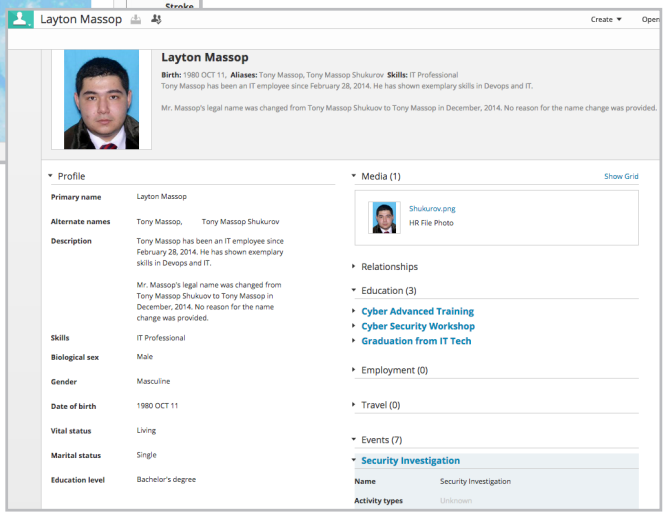


Figure on left: Map showing verified cyber attacks.

Figure below: Person Occurrence dossier of notable threat, Layton Massop.

Because of the complex, quickly evolving nature of this problem, a collaborative and holistic environment is necessary for effective analysis and dissemination. Savanna's collaborative workspace and unique, model-based approach are ideal for analyzing complex problems like cybersecurity threats.

With Savanna's dynamic Occurrence dossiers, analysts can collaboratively populate an information network about a potential cyber attacker that Splunk Enterprise named a Notable Threat, starting with a Person Occurrence to capture information about "Layton Massop." Occurrences are building blocks that capture people, organizations, things, places and events related to a problem. Under its Events section, a report of when Massop first triggered the Splunk security alert is added.

With Linknet (Savanna's link charting tool) multiple Occurrences from the information network visualize connections between Massop and other employees at his company.

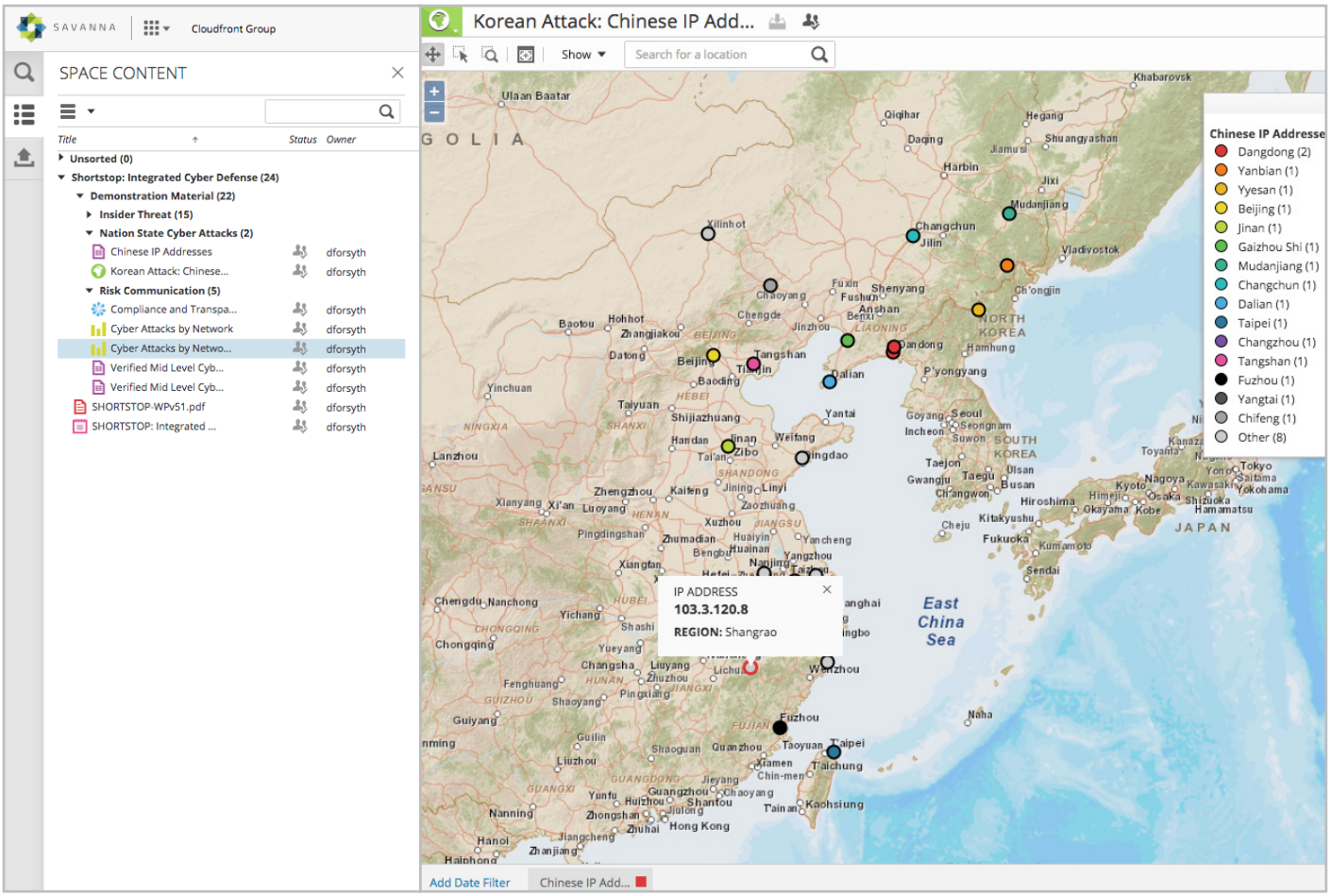
A geospatial visualization of a CSV of verified cyber attacks provides a visual snapshot of where and when the attacks were committed. The temporal filter drills down to specific months or years to quickly visualize changes by time period.

With Timeline, users can drop multiple Occurrences, such as various suspected notable threat person Occurrences, onto a visual span of time to draw connections between events within each Occurrence. Visualizing event times from multiple Person Occurrences side-by-side lets the analysts see similar download activity between Massop and an HR employee.

The Result

Now, a report can be compiled in Savanna's Note tool, consisting of supporting evidence that has been created and gathered throughout the analysis process. In Note, analysts can compile findings, such as an image of the Map depicting verified cyber attacks, or add a hyperlink to the Splunk Security app to view similar notable threat reports. Once complete, the Note is shared directly with team members using Savanna and exported to PDF to send to fellow analysts and decision-makers for further action and prevention.

BENEFITS



Decision-making insight

Whether reviewing content from a bird's-eye view or focusing on a detailed event profile, decision-makers gain the critical insight they need to determine when to adjust organizational strategy in response to growing risk indicators.

Agility

Using Savanna's dynamic information management capabilities in coordination with Analyst's Notebook's data analysis tools, organizations can maintain current intelligence needed to respond to rapidly evolving situations and perspectives.

Productivity

Savanna eliminates the time required for integrating analytical output and sharing and formatting files, resulting in more time to devote to analysis and review.

Expanded source material

The ease of uploading and manipulating diverse forms of data frees analysts from technological limits to incorporating all relevant information. Should a growing conflict present incomplete or fuzzy data, analysts can utilize such information in Savanna and update it as clarifying details emerge.

Reduced exposure

Savanna minimizes exposure to error resulting from bad information by offering users the ability to annotate all source material and analysis products. Automatic updates documenting user activity further assign ownership while privacy settings maintain protected data.

CONCLUSION

Complex problems require multi-part solutions. With the rise of tools to mine large data sets, businesses have reaped greater knowledge from structured data[1]. However, complex challenges like identifying and stopping cyber threats require a more nuanced understanding of context.

Only by viewing problem spaces through multiple lenses and exposing inconsistencies can companies identify—and begin to quantify—risks. In doing so, alternatives become clear, imperatives become known, and negative consequences are avoided.

ENDNOTES

1. Furrier, J, "Big Data Is Big Market & Big Business - $50 Billion Market by 2017," Forbes, last modified February 17, 2012, accessed September 25, 2014, from http://www.forbes.com/sites/siliconangle/2012/02/17/big-data-is-big-market-big-business/.

FIND OUT MORE

Learn more about how Savanna can help identify and anticipate risk by visiting our website at www.thetus.com.

326 SW Broadway, Portland OR 97219
P: 1.503.294.0900
F: 503.595.5828