Advanced analytics is one of the biggest reasons many companies include Big Data technologies within their Cybersecurity arsenal. Elysium Analytics' Security Intelligence and Analytics (SIA) Solution not only enables a platform for creating custom advanced analytics, but also includes a very sophisticated analytic in its Insider Threat Detection (ITD) application. This datasheet describes the high-level features of the ITD application.

Why Monitor Employee Behavior?

Many security breaches were performed by actors who had legitimate access to the data and were located inside of the company network. InfoSecurity reports 43% of data breaches were performed by Insiders. Poneman Institute reports even higher numbers and goes on to report the cost of such breaches can be higher than external attacks. Dark Reading reports that 55% of companies have experienced an insider threat issue, 62% of employees have access to data they should not see, and only 9% of companies believe their insider prevention methods are effective.

Clearly more needs to be done for this important topic.

Data Categories Collected

Elysium's ITD application starts by monitoring three primary categories of behavior:

- E-mail Activity
- Internet browsing activity
- System login patterns

More importantly, since Elysium's solutions are all open solutions, organizations can extend the solution to include activity in business-specific applications. For instance healthcare companies could monitor patient lookups or financial companies can monitor transactions. Elysium started with these three categories since virtually all companies have email, Internet access, and system logins.

Features Tracked

Within each category of employee behavior the ITD application tracks several different statistics to fuel the analytic algorithm. For instance within email some of these statistics include:

- Average size of messages for the day
- Largest message of the day
- Number of messages each day
- Number of attachments each day
- Etc.

Dimensions Tracked

In order to enable the sophisticated analytic within the ITD application, the above features for all behavior categories are tracked in two dimensions:

- By comparing to each user's own history
- By comparing each user to the community

While a typical mid-sized organization can have events numbering in the millions per day, the summary statistics will likely be tens of thousands per day since it is derived from the number of features times the number of users times 90 days (by default).

Analytic Result

Collecting lots of statistics is great for data scientists and statisticians, however most security analysts want the actual analysis performed for them. Therefore the ITD algorithm crunches each day's activities, and with a dynamically evolving weighting scheme and a cumulative probability distribution, it provides a single "risk score" for each user.

- Single "risk score" for each user

With this score a security analyst can easily focus on the riskiest users in their environment on any given day.

[1] From https://www.infosecurity-magazine.com/news/insider-threats-reponsible-for-43/

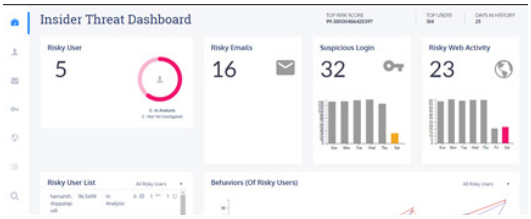
[2] From https://app.clickdimensions.com/blob/softchoicecom-anjf0/files/ponemon.pdf

[3] From https://www.darkreading.com/vulnerabilities---threats/8-surprising-statistics-about-insider-threats/d/d-id/1326653

continued...

Analyst Dashboard

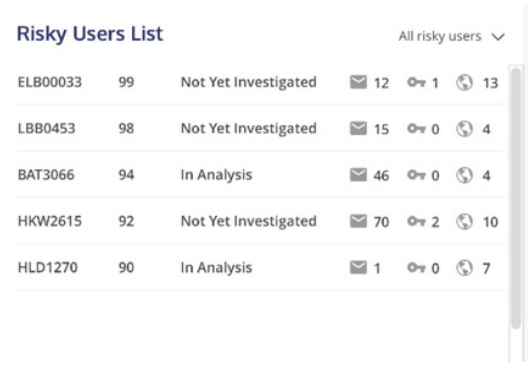
Elysium designed a user-friendly dashboard for the security analyst to begin their daily review of user behavior.



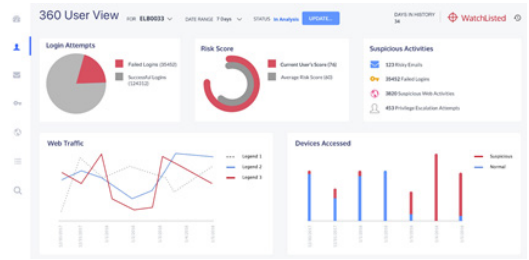
At a glance the security analyst can see the riskiest user in their environment along with several other key indicators. Quickly the analyst can see the distribution of high, medium, and low risk users as well as geographic distribution and the recent trend.

Investigation Support

A heat-map on the Overview dashboard enables the security analyst to quickly drill-down into the details of any user's activity.

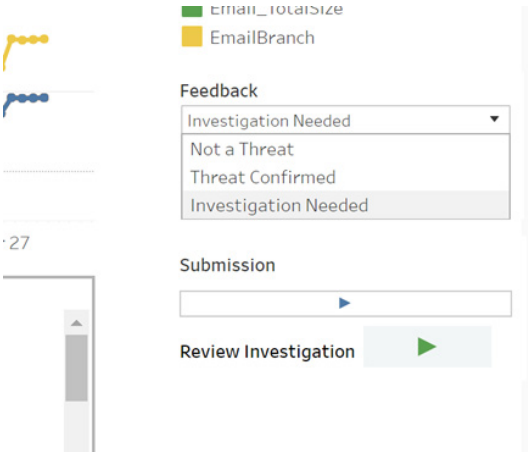


From the Overview dashboard the analyst is taken directly to a category view of a single user's activity for any given category. From the category view the analyst can quickly see a breakdown of the deviation in activity from the user's own history compared to the community of users, a trend for this user over the past 90 days, and can dig into the details of individual records for the user.



Machine Learning Feedback Loop

Every organization is different. While Elysium's ITD application comes with a good, tested set of weights for the various features, your organization may have different characteristics. That's why it is critical to provide a feedback mechanism for the security analyst to enable machine learning algorithms to "train" the analytic:



With this input the system will get smarter and smarter as time goes on.

More Information

Contact Elysium Analytics today for more information on how advanced analytics can help your organization.