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 is the perfect platform for creating custom advanced analytics and includes several analytics ready-to-go to get any organization started.

Why SIEMs Are Not Enough

Despite the growing variety of tools used in today's cybersecurity operation centers, we are still seeing threats make their way past all our defenses. Many newer techniques (like sandboxing) were effective when they first hit the market, but within a year agile adversaries have learned how to circumvent them, and so the trend continues.

Tools like SIEMs and anti-virus look for known threats, using signatures that are available through proprietary or commercially available threat feeds. SIEMs attempt to detect unknown threats using a variety of behavioral rules that have proven to be indicators of compromise. However, SIEMs have fallen short on delivering accurate and complete results for several reasons:

- First they are designed to analyze limited data for short periods of time due to scalability costs.
- Second they do not facilitate advanced analytics, traditionally SIEMs are rule-based solutions.
- Third SIEMs are generally "closed" environments – they do not provide direct access to the data for data scientists.

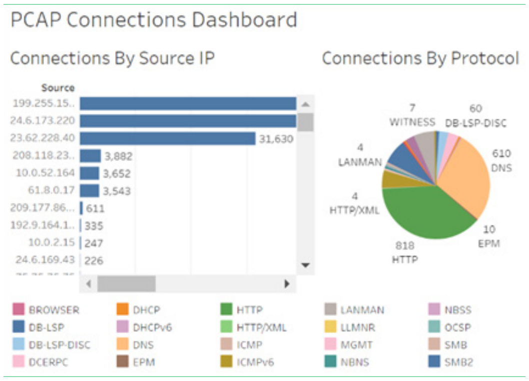
Advanced Analytics

Correspondingly, organizations are turning to advanced security analytics operating on a security data lake, the latest "new" defense. Employing a security data lake is an attempt to accelerate an organization's ability to quickly detect and pinpoint if their networks have been compromised so that appropriate countermeasures can be deployed.

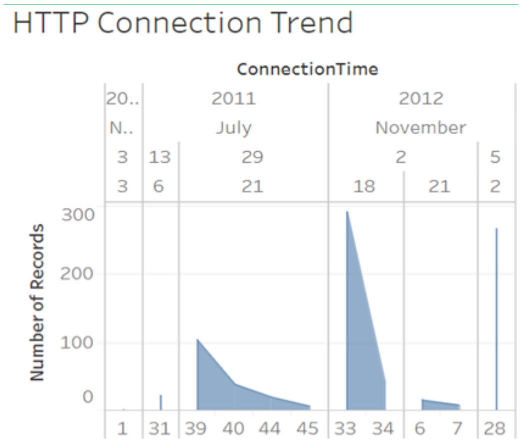
Most recently, industry experts and practitioners believe that accuracy lies in collecting more and more data while retaining it for longer periods of time - sometimes for years.

Economical Scalability

Scale alone isn't the only challenge, the real challenge is to scale efficiently and without immense licensing costs. This is why Elysium built our solution on the latest Hadoop open source technologies.



One testament to the ability to scale is the inclusion of raw packet capture (PCAP) data. Collecting from PCAP sources may be one of the most voluminous sources in any organization's IT infrastructure. Yet it is important to capture this source as it contains virtually all information about communications on your network.



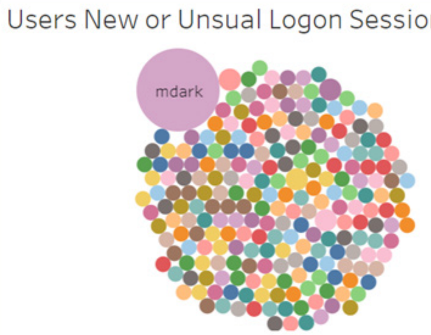
Elysium SIA Solution includes a pre-configured integration with PCAPA or FastCAPA capturing technologies. System administrators can control the capturing end-point from the same

continued...

Ambari console where they can control all processes and services.

Structured Storage

Elysium SIA Solution can store data in both structured and unstructured formats. While unstructured storage is great for ad hoc, interactive queries and forensics investigations, structured storage is far better for Advanced Analytics. For instance when investigators search for a string of characters like “123”, it’s great to find all instances of those characters – whether it’s “123 Main Street”, 123 in a phone number, or 123 in an IP Address. Investigators can apply human intelligence and intuition to what they see on the screen and highlight the records of interest. However with Advanced Analytics, sophisticated algorithms need to automatically connect the meaning of the data elements in order to provide intelligent insights. This is why Elysium performed the extra work to parse many commonly available IT sources as part of the platform implementation.

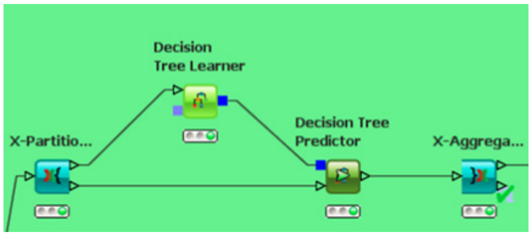


This enables sophisticated anomaly detection algorithms and more advanced reporting.

Data Scientist Workbench

Another important requirement for an Advanced Analytics solution is to provide a platform for Data Scientists to create their own algorithms that are specific to their environment. Elysium’s SIA Solution enables this with several technologies:

- H20 ML Algorithms Integration
- Zeppelin Reporting Interface
- SparkML Machine Learning Library
- Knime Server Integration



Just as important Elysium’s SIA Solution comes with a rich pre-defined schema for cybersecurity information. The schema is designed with layers of abstraction to ensure compatibility with Apache Spot’s Open Data Model (ODM). The schema design also includes integration with several enrichment sources such as DNS lookups and Threat Intelligence feeds.

Results

So what kind of insights can one expect from Elysium’s SIA Solution? Some examples include:

- Users logging in from two different locations in a short time period.
- Anomalous network activity such as two machines communicating on an unusual port.
- Leverage context enrichment sources to correlate across sources.

More Information

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