Threats don’t follow templates. Neither should you. The Elastic Stack gives you the edge you need to keep pace with the attack vectors of today and tomorrow. Let’s start with understanding what security analytics is and how it can be maximized.

**Security analytics** is the process of using data collection, aggregation, and analysis tools for security monitoring and threat detection. Depending on the types of tools installed, security analytics solutions can incorporate large and diverse data sets into their detection algorithms. Security analytics data can be collected in several ways, including from:

- Network traffic
- Endpoint and user behavior data
- Cloud resources
- Business applications
- Non-IT contextual data
- Identity and access management data
- External threat intelligence sources

Recent technological advancements in security analytics include adaptive learning systems that fine-tune detection models based on experience and learnings, as well as anomaly detection logic. These technologies accumulate and analyze real-time data that includes:

- Asset metadata
- Geo-location
- Threat intelligence
- IP context
These forms of data can then be used for both immediate threat response and investigations.

Security analytics has a variety of use cases, from improving data visibility and threat detection to network traffic analysis and user behavior monitoring. Some of the most common security analytics use cases include:

- Analyzing user behavior to detect potentially suspicious patterns
- Analyzing network traffic to pinpoint trends indicating potential attacks
- Identifying improper user account usage, such as shared accounts
- Detecting data exfiltration by attackers
- Detecting insider threats
- Identifying compromised accounts
- Investigating incidents
- Threat hunting
- Demonstrating compliance during audits

Above all, the primary goal of security analytics is to turn raw data from disparate sources into actionable insights to identify events that require an immediate response through the correlation of activities and alerts. In doing so, security analytics tools add a critical filter to the volumes of data generated by users, applications, networks, and other security solutions in place.

Elastic Stack is one of the most powerful solutions to address these security analytics use cases in well-defined manner. Let’s take an example here.

In our network, we have collected the Network packet data from the servers/machines using packet-beat. We have also collected the data from the audited log (Linux as well as Mac machines) files from these machines using file-beat. We have also collected the data of system information like cpu, memory, process named etc. from these machines using metric-beat.

All these beats data create data filter and enrichment using logstash pipeline and sends the output of logstash to Elasticsearch as database. These logstash pipeline filter the messages coming from these beats as well as it enriches the data like geo location, agent module and send to Elasticsearch cluster.

Based on the collected data into Elasticsearch, we have created separate index for each beat. Below is the snapshot.
Once the data is ingested in Elasticsearch Indexes, we have built some visualization / dashboards for this data and then built Machine Learning jobs on this data for every security analytics use case. Machine Learning feature is a part of X-Pack of Elastic Stack.

These ML (Machine Learning) jobs create the data patterns based on the ingested data and detect the anomalies. Anomalies detection will help us to analyze the attacker behavior on how he does the attack on our Network and System. It will also provide additional information about How, Who and Where it did attack. So, imagine that if you are Security Admin, you will get lot of useful information on each and every step of attacker’s move and you will be able to prevent this attack. And this is happening in real-time, so you will quickly get the insights and can take the preventive actions. You can create alerts on this ML if any anomalies are detected; and this info will be sent to your email or slack or any third-party integration tool.

Below is one of the ML jobs of DNS Exfiltration / Tunneling.
Now in the above example, this ML job detected the anomalies (red square dot) and provided information that “vodkaroom.ru” domain is used by an attacker for DNS tunneling. It also provides information that there is machine “server_101” used by attacker to access this DNS.

Now, you might be curious to know more about “server_101” activities. So, we have generated visualization/dashboards which can link to this anomalies detection to go in further depth. Below is the screenshot.
In the above visualization, it indicates the metrics of “server_101” which provides information as to how “server_101” gets compromised using ssh login failure (brute force attacker is typical method along with port scan).
It also provides from which location these DNS got access. Below is the screen shot.

Obviously, there are a high number of sub-domains which send DNS query once attacker start controlling your DNS tunnel. Below is a screen shot.
So now, let us do some more analysis using Graph feature in Elastic Stack which comes with X-Pack. Graphs provide connections between your data sets which you like to see. Here, we like to see who is accessing this “server_101” from where DNS “vodkaroom.ru” got access and what other DNS these users are accessing so that you as a security admin can take preventive measures.

Below are the screen shots.
If you look at this Graph (actually, it is a motion graph while the data is moving), you can see the “vodkaroom.ru” DNS is accessed by user “mikep” and “asawari”. Now we like to know more about the other domains that are accessed by these users. So, we click on “+” on mikep user and see more details. Below is the screenshot.

This is really important use case when you are seriously looking into security of your infra and you’d like to start with SIEM tools, you’ll surely need to look at Elastic Stack.

So, in the above graph, you can clearly see that “mikep” user accessing the other domains like “secuirymagzine.com”, which might have become potential threats.

Security is a major concern for all enterprises especially when massive data is coming in/out from your infra. You as a Security Admin would like to get more insights from this log data. Elastic gives you immense benefits and you can use these as “Security Information and Event Management” (SIEM).

Email us if you like to get more details/demo about this use case as well as some other interesting use cases on Elastic.