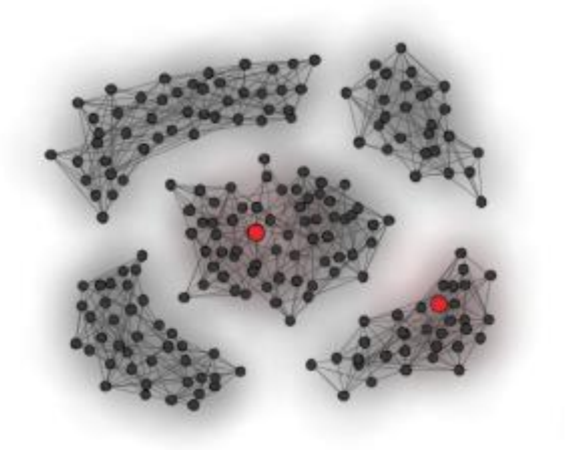
Cyberlytic

Profiler Analytics

Anomaly Detection

Waiting until something breaks before we fix things is usually a good philosophy in life. However, when we consider sensitive data, there is zero room for error. At Cyberlytic, we are implementing novel strategies to analyse anomalous behaviour in web traffic, reducing the pitfalls that standard signature and rule based techniques are susceptible to. These methods help detect emerging and sophisticated cyber threats in real time, reducing the effort for human intervention or interaction.



To analyse irregular activity, or anomalous behaviour, we implement advanced machine learning techniques that adapt to their environment. The science behind machine learning is to process data subject to actions performed on previous results, and the incoming information received. These self-learning, unsupervised algorithms then profile normal web traffic behaviour, inferring their own decisions. Metrics are obtained that are unique to a web server, and follow a rigorous and continuous assessment. Decisions are finally carried out by the set of algorithms to accurately quantify the severity of the threat, and enhance the learning procedure. This approach adapts and evolves immediately from its inception, which uncovers anomalous trends or activity in complex data streams.

Risk Classification

The Profiler couples the detection of anomalous activity with the detection of known malicious events. Specifically, the detection engine combines statistical inference and a fingerprinting methodology to distinguish SQL injection attacks (SQLi), Cross-Site Scripting (XSS), and Bash injection. The coupling of the anomaly detection engine with the detection of known attacks acts as a filter that further reduces both false positives and false negatives. The consequence is the reporting and distillation of only truly malicious requests to the web application. Meta-data of the malicious event and attacker is also determined from the request. In particular, the position of the attack in the attack lifecycle is calculated, the page and field where the event occurred is provided, and the geo-location of the attacker is determined.

Further triage and distillation of malicious events is achieved through the generation of a risk score associated with each event. The Profiler not only analyses the sophistication of the request itself, but, since each aspect of the web application is profiled, it can competently investigate the effectiveness of the malicious event through the analysis the server's response invoked by the request. To this, the Profiler also builds a profile of each user of the web application highlighting their capability as a threat to the web service. In doing so, the Profiler not only learns from the nature of the traffic flowing through the web service, but also about the behaviours of specific users using the web service. A risk score and associated risk label is attached to each malicious event; the risk score is given by a number between 1 and 100, and a risk label ranges from 'Low' to 'Critical'.