Why do you need UEBA?

User and Entity Behavioral Analytics (UEBA) solutions have been around for some time, and you may be wondering what they are and if you need one. UEBA tools analyze the behaviour of users and entities (hosts, devices, files and transactions) to find interesting or malicious behaviours and patterns. Essentially, UEBA makes your security team smarter by accelerating detection and response to threats without increasing the workload of your security analysts. It increases the ability to focus your security resources where they can be most effective – reducing the noise from events by delivering condensed, prioritized and contextualized insights to the security analyst who can then better respond to threats. The best UEBA engines, along with orchestration and automation, are built on top of SIEM systems.

SIEM + UEBA offers a machine-learning based approach to detecting known unknowns and reacting to threats that are not detectable through other means. In addition to shorter detection times SIEM + UEBA provides more actionable evidence during investigations and higher efficacy and accuracy of the alerts and incidents generated. Our LogPoint UEBA works by using machine learning to build baselines for every entity in the network, without creating predefined rules or signatures. By evaluating actions against these baselines, the LogPoint UEBA module detects the unknowns and eliminates the need for expert rules or a rules-based system in a company's SIEM, reducing the cost of implementation and freeing up security analysts to focus on finding real threats in the system. The use of analytics instead of matching with signatures or rules allows the data to paint a clearer picture of what is and isn't – normal.

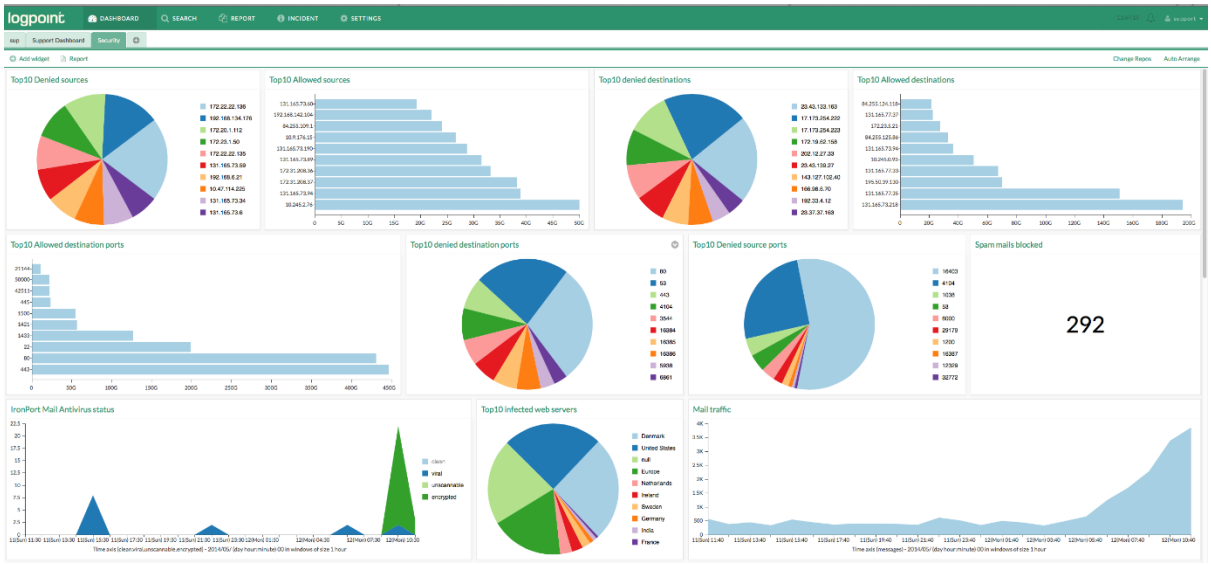
According to our CPO, Christian Have, "*With our UEBA engine, we can begin the move away from describing known-good and known-bad situations with expert-rules (signatures). The UEBA and its underlying algorithms are building baselines, not for the network as a whole, but for every individual entity (user/document/web-page etc.) that it observes. These patterns of observed behaviour are represented as clusters of activity in coordinate systems. Whenever a new observation comes in, we evaluate the distance of this particular activity from groups of accepted and "learned" behaviours. This powerful implementation of machine learning algorithms is packaged in LogPoint UEBA to detect misuse of credentials, lateral movement in the network and attempts to exfiltrate data.*"

LogPoint UEBA introduces a more effective method for monitoring and reacting to anomalous activities. The UEBA module is built on sophisticated machine learning principles, and thus

doesn’t require configuration of rules or threshold values to work – it automatically adapts itself to the given infrastructure.

The module includes use cases for misuse of credentials, data exfiltration and lateral movement. These use cases come out-of-the-box with the UEBA module, and include continuous calculation of risk-scores for users and entities. Meaning that the analyst will be presented with an actionable “to-do list” of the most abnormal users or entities in their network to investigate. The risk-scores can then be used as enriched meta-data on existing logs for additional use cases such as SAP, custom applications, SharePoint and others. Because our LogPoint SIEM translates data into one common language, it is more readable and understandable, allowing the UEBA tool to work more effectively and efficiently across the entire infrastructure.

To learn more about the LogPoint UEBA module please contact Full Control Networks.



Your local LogPoint partner is:

Full Control Networks
Tel: 01677 428700
info@fullcontrolnetworks.co.uk
www.fullcontrolnetworks.co.uk