UEBA

LogPoint UEBA

LogPoint enables analysts to achieve situational awareness before, during and after responding to breaches. LogPoint enables analysts to correlate, observe and report unusual activities through the complete IT landscape. To further reduce the time to detection and effectively managing the breach LogPoint offers UEBA.

Through Machine Learning LogPoint UEBA builds baselines for every entity in the network, without creating predefined rules or signatures. By evaluating actions against baselines, the LogPoint UEBA module detects the unknowns.

In short: Combine SIEM and UEBA in an easy to use package that acts as a force-multiplier for your security analysts by reducing expert-rules, false positives and prioritizing alerts.

These are just some of the benefits:

- Detect the low and slow attacks
- Shorter detection time
- Increased efficacy
- Leverage UEBA analytics
  with log-enrichment
- Simple installation and configuration
- Predictive pricing

In this scenario, we can do analytics on the output of the UEBA module. We can identify Data Exfiltration attempts, credentials being misused, unusual AD activity (logins etc).

LOGPOINT

wwwlogpoint.com