

Achieving proactive security analytics designed for growth

 **Industry:**
IT Business Intelligence

 **Product:**
Securionix Next Gen SIEM with UEBA

 **Solution:**
User & Entity Behaviour Analytics

THE CHALLENGE

Within 24 months, one leading credit checking organisation was anticipating unprecedented growth of its data handling and operations. Their free version of Alien Vault (SIEM), which traditionally had delivered their security analytics, no longer aligned with the long-term security strategy of the business. It generated lengthy logs, provided no clear insight, and degraded the performance and abilities of the SOC team to confidently handle incidents.

THE SOLUTION

Securionix SIEM with UEBA is a security operations and analytics platform. Introducing it has enabled the business to move away from looking at logs by delivering clear graphics with group alerts to seamlessly identify where and when in the kill chain an event took place. It identifies affected users, services and systems, facilitating swift remedial action and flagging anomalies in user behaviour, thus enabling a rapid response to any malicious activity.

THE BENEFITS

Our customer can now gain insight and visibility of the details of each incident or event also grouping those connected. They can mitigate false positives and focus on real concerns, whilst aligning their budgets with users for easier forecasting. And, with proactive monitoring and management of users with risk profiles for each employee, they can easily protect the organisation's IP & reputation.



HANDD
BUSINESS SOLUTIONS

