QUANN PROTECT

QUANN USER BEHAVIOUR ANALYSIS

Enhancing detection capabilities to protect businesses against sophisticated emerging threats

As cyber threats become more complex and sophisticated, businesses have to protect themselves against "unknown unknowns" while grappling with the reality that it is impossible to fully secure the enterprise network. It is not practical or possible to lock down every endpoint in the enterprise, and traditional defences based on rules and signatures no longer suffice when businesses do not know what they are protecting themselves against.

Businesses have to operate with the assumption that they have been breached, and the likelihood that advanced threats have infiltrated the network and remained undetected for weeks or even months. At the same time, they have to guard themselves against insider threats as the number of security breaches attributed to human errors or malicious insider attacks continues to grow.

QUANN USER BEHAVIOUR ANALYSIS

Quann User Behaviour Analysis enables businesses to come up with a comprehensive cyber security strategy to deal with both known and unknown threats. It combines user behaviour analysis technology with comprehensive end-to-end monitoring and in-country cyber security expertise to help businesses detect emerging cyber threats and develop an effective response.

Powered by Darktrace's Enterprise Immune System which combines advanced mathematics with machine learning, the technology creates unique behavioural models for every user and device, and for the enterprise as a whole. It then makes use of these models to monitor behaviours and detect anomalies in the business' computer and user activities. Unlike rules or signature-based defences, this approach enables the solution to detect threats without any prior knowledge of what it is looking for.

FEATURES

Use of behavioural model

- Behavioural models are created for every user, device and the organisation as a whole using unsupervised machine learning.
- Normal and abnormal behaviours are learnt in real time to detect emerging anomalies without making use of rules, signatures or assumptions.

Full network visibility

- The entire network is visualised and threats are automatically classified to allow for in-depth investigation.
- Incidents can be replayed so that events can be analysed and correlated over time.
- Detailed reports of anomalies are provided for further investigation.

Retention of data within the business network

- All processing and outputs are kept within the business' data centres to prevent data leakage.
- Data is not sent out via the cloud or accessed by any third party except under instructions from the business owner's users, including those managing the business' IT functions.
- The stealthy deployment helps mitigate insider threats.

Easy deployment and integration

- The solution is designed to complement businesses' existing security infrastructure.
- The user behaviour analysis appliance is installed passively into the business infrastructure.
- All user interfaces can be accessed via a web browser.

End-to-end monitoring

- Quann complements user behaviour analysis technology with end-to-end monitoring through our network of in-country intelligence-driven Security Operations Centres.
- Businesses are alerted to new and emerging threats so that pre-emptive measures can be taken.

Access to cyber security expertise

- Leading-edge technology is combined with processes and methodologies to help businesses crystallise and mitigate risks
- Businesses have access to cyber security expertise to help them develop an effective response to threats.

BENEFITS

Enables detection of "unknown unknowns"

Quann User Behaviour Analysis solution is capable of detecting anomalous behaviours within large and complex environments, without any prior knowledge of what it is looking for. This enables it to detect insider and external threats that are able to bypass traditional security defences.

Provides effective security against sophisticated emerging threats

A businesses' cyber defences are significantly boosted by the ability to detect and respond to sophisticated emerging threats. These include remote access attacks linked to dangerous malware, anomalous data transfer, malicious web drive-by attacks and port-scanning for internal company resources.

Improves compliance

A businesses' cyber defences are significantly boosted by the ability to detect and response. The solution helps businesses to ensure compliance with data protection regulations and other governance requirements by detecting illegitimate access to database servers, unauthorised use of administrator credentials, anomalous internal file transfers and risks from bring-your-own-device (BYOD) policies.

Increases the effectiveness of cyber security teams

The combination of leading-edge technology, Quann's expertise and round-the-clock monitoring capabilities enables enterprise cyber security teams to operate more effectively and stay ahead of the cyber security curve. The solution provides real-time alerts to threats as they emerge, helps businesses to prioritise the threats by reducing false positives, and provides the expertise to help them develop an effective response.

QUANN
THE ART AND SCIENCE OF BEING CYBER SECURE

For more information, please contact us at **info@quannsecurity.com**
or visit our website at **quannsecurity.com**