DATA SHEET

END USER BEHAVIOURAL ANALYTICS

Managed Security Services

AT A GLANCE

We use a defense grade advanced anomaly detection system to detect threats that your existing security solutions can't see.

Our SOC team uses the anomaly detection systems to identify malicious anomalous activity arising from zero day exploits, malware or insider activity. Our 24x7 SOC monitors the environment to alert your security team if something of concern is detected.

We leverage the best available technology to offer a defense grade security system, monitored by 24x7 Security Analysts with a higher quality of service and less cost than delivering a monitoring service in-house.

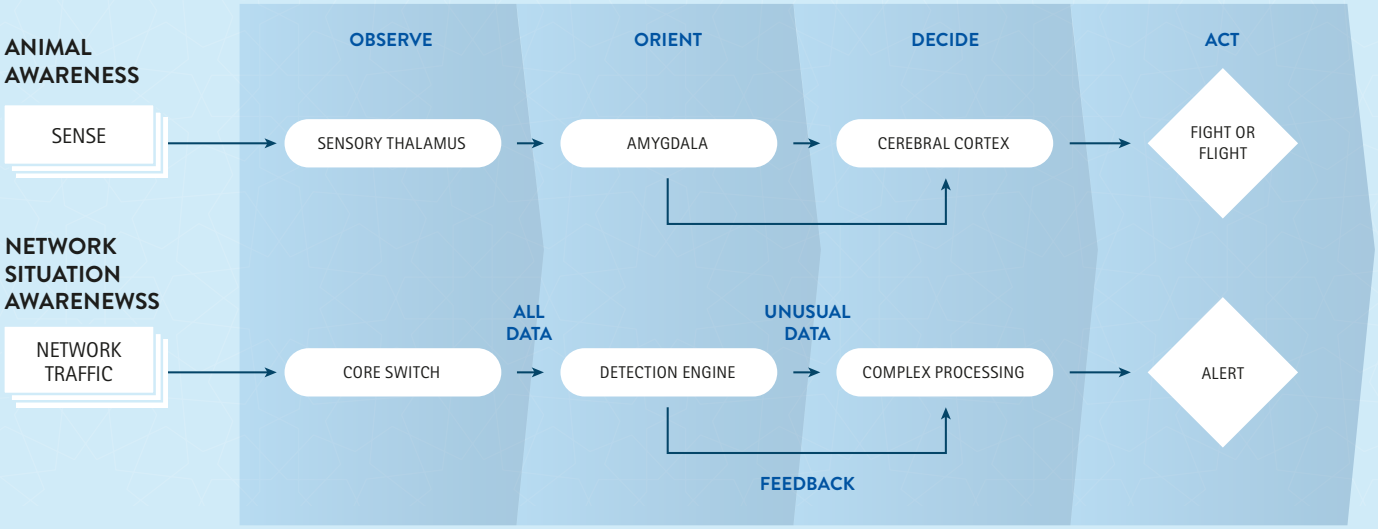
HOW IT WORKS

This service detects operational anomalies within packet communication behavior to detect high risk activity and threats. We use state of the art techniques to provide an analytics service based on big data streaming, data science, machine learning and behavioural analysis to detect attacker behaviours and user anomalies within networks. All detections are correlated and prioritised to show an attack in context, and our platform's machine-learning adapts as attacks evolve.

The software which we use was first developed for the UK Government in 2011 and was declassified for commercial sale in 2013. Since then it has been constantly developed to become today's most advanced method of identifying threats to a network. The software is split into two parts; the first part using bio-inspired techniques to identify how unusual and threat-like network traffic is. The software then uses this information to determine how deep the analysis into the data needs to be. The system then runs analysis on all network traffic to determine any behaviour that could be threatening, this includes:

- Data exfiltration
- Pre-attack phase activity
- Network reconnaissance
- Network pivoting
- Privilege escalation
- Anonymising data
- Policy breaches or bring your own device based threats
- Brute-force behaviour
- Command and control activity
- Malicious users/network misuse

Using behavioural analytics, we can instantly detect and alert operational and security practitioners of anomalous and suspicious activities within their organisations.



Contact Us: Sales@siconsult.com

DATA SHEET

END USER BEHAVIOURAL ANALYTICS

Managed Security Services

FEATURES & BENEFITS

24x7 Service

Our 24x7 Behavioural Analytics service provides visibility into threats and risks which cannot be detected by SIEM, IPS and other security tools. We integrate with our own SIEM / SOC to provide real time 24x7 alerting and investigation. The outcome is continuous monitoring of all IPs, devices & protocols by leveraging our Anomaly Detection Platform to provide analysis and prioritised reporting to instantly identify a cyber attack at any phase and describe what the cyber attacker is doing.

Active Attack Detection

Unlike traditional security, our Anomaly Detection Platform provides real-time detection of all phases of an ongoing cyber-attack. The solution detects command and control, internal reconnaissance, lateral movement, data exfiltration and botnet monetization behaviours.

Automatic Correlation & Consolidation of Hosts

We correlate a Threat Certainty Index and automatically consolidate all detections and confidence scores to quickly reveal the specific hosts that pose the greatest risk to the network so that teams can immediately focus on the detections that matter most.

Data Science Based Detection

Our Anomaly Detection Platform uses a patent-pending combination of data science, machine learning, and behavioural analysis to reveal the fundamental characteristics of malicious activity without the need for numerous signatures and reputation-based rules.

Prioritising Key Assets

During investigations our Anomaly Detection Platform automatically learns the naturally occurring communities in your networks and provides a visual map of the relationship between threats, hosts and key assets. This ensures that security teams can quickly see threats in the context of other network assets and the potential impact of the attack.

Easy Access to Attack Details

Vectra ensures that the proof of a threat detection is always immediately available. Whether investigating specific detections or hosts, security operations and incident response teams can access packet captures in one click for further analysis.

Variety of Detection Triage

Custom detection categories enable the staff to track misconfigurations and high-risk applications or out-of policy user behaviour that can potentially enable or obscure a cyber-attack.