Nil Ortiz
Senior R&D Cybersecurity Engineer
at I2CAT Foundation

From detection to prediction: How behaviour analytics is changing cyber defence

Cyber security teams have become increasingly effective at detecting known threats. Modern SIEMs, EDR platforms and IDS technologies can identify malware signatures, anomalous traffic and suspicious events within seconds. The real challenge, however, is no longer simply answering *"What happened?"* but rather *"What is likely to happen next?"*.

This shift from reactive detection to predictive cyber defence is becoming particularly important for operators of critical infrastructure and essential services, where every minute of incident response matters. Water utilities, telecommunications providers, healthcare organisations and industrial operators cannot afford to wait until malicious activity becomes a major incident.

Predictive behaviour analytics offers a practical way to shorten this gap.

ECCC
Funded by the European Union

Funded by the European Union's Digital Europe Programme under Grant Agreement No 101249732. The views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority (European Cybersecurity Industrial, Technology and Research Competence Centre). Neither the European Union nor the granting authority can be held responsible for them.

Behaviour tells a richer story than individual alerts

Most cyber attacks are not a single event.

They are sequences of seemingly legitimate activities that gradually diverge from normal operational behaviour. A privileged account starts accessing systems it has never touched before. A workstation begins authenticating at unusual hours. Service accounts suddenly communicate with external infrastructure.
Individually, these events may appear benign. Yet together, they reveal a behavioural pattern.

User and Entity Behaviour Analytics (UEBA) focuses precisely on this problem. Rather than relying exclusively on predefined signatures or static rules, UEBA learns how users, devices and services normally behave and continuously measures deviations from those baselines.

Machine learning becomes particularly valuable because modern enterprise environments are too dynamic for manually crafted rules to remain effective over time. Organisations evolve continuously: employees change roles, infrastructure scales, cloud services are introduced, and legitimate behaviour shifts accordingly. Effective behavioural models must therefore adapt while remaining capable of identifying genuinely suspicious activity.

Prediction is more than anomaly detection

Behaviour analytics is often misunderstood as simply "finding anomalies".
In practice, prediction requires combining multiple dimensions of information:

- Historical behavioural baselines
- Current activity
- Contextual information
- Organisational risk
- External threat intelligence

A user logging in from a new workstation may not represent a risk.

The same user accessing sensitive assets outside business hours while communicating with infrastructure associated with known threat actors presents a very different picture.

Prediction therefore becomes a probabilistic assessment rather than a binary decision.

Instead of asking whether an event is malicious, the system estimates the likelihood that a sequence of behaviours will evolve into a security incident.
This enables analysts to focus on behaviours that indicate increasing risk, rather than reacting to every isolated anomaly.

ECCC
Funded by the European Union

Funded by the European Union's Digital Europe Programme under Grant Agreement No 101249732. The views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority (European Cybersecurity Industrial, Technology and Research Competence Centre). Neither the European Union nor the granting authority can be held responsible for them.

Enriching behavioural models with Cyber Threat Intelligence

Machine learning performs best when behaviour is interpreted within context. This is where Cyber Threat Intelligence (CTI) significantly improves predictive capabilities.

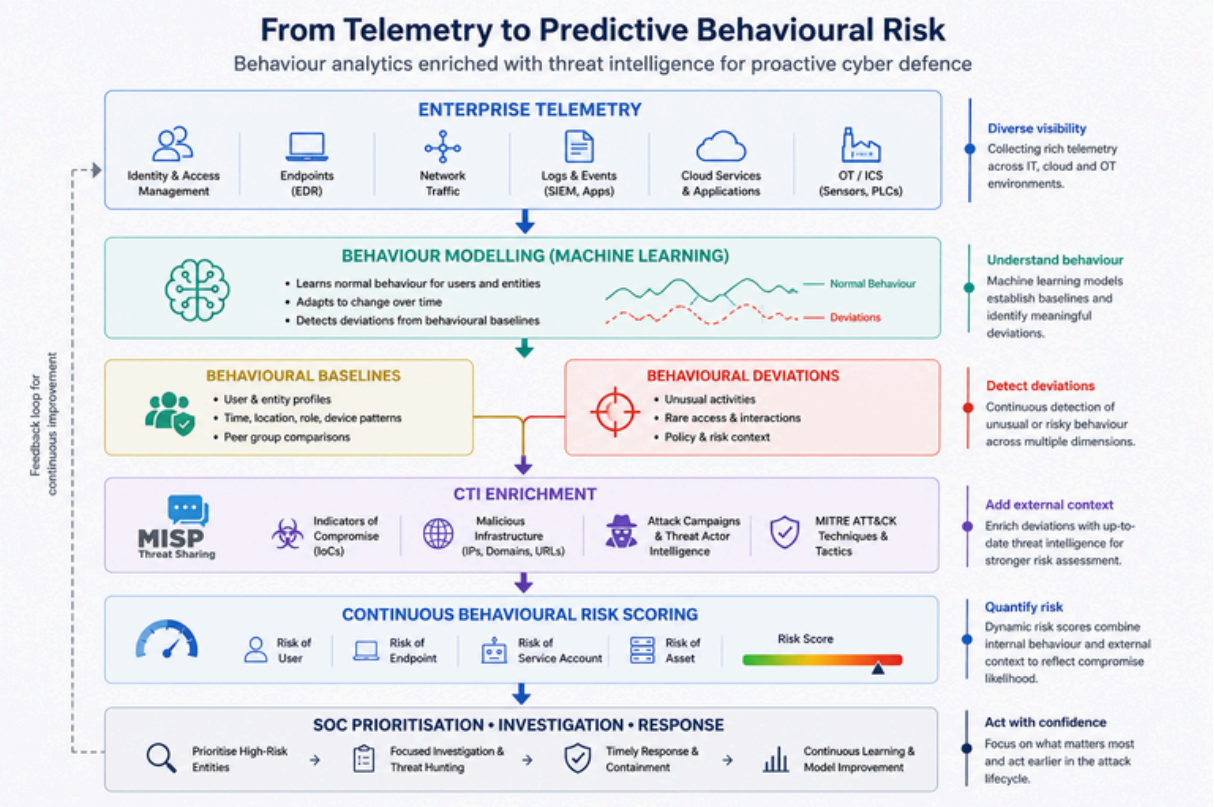
Threat intelligence platforms such as MISP provide continuously updated information about malicious infrastructure, Indicators of Compromise (IoCs), attack campaigns and adversary techniques.

Rather than analysing behavioural anomalies in isolation, behavioural analytics can correlate observations with external intelligence. Examples include:

- Communication with IP addresses associated with active campaigns
- Domains linked to recent phishing operations
- Malware indicators observed targeting similar sectors
- Attacker techniques mapped to the MITRE ATT&CK framework

The result is not simply detecting unusual behaviour, it is understanding whether that behaviour resembles known adversary activity.

This additional context helps distinguish between harmless deviations and behaviours that warrant immediate investigation, ultimately reducing alert fatigue and improving confidence in security decisions.



ECCC
Funded by the European Union

Funded by the European Union's Digital Europe Programme under Grant Agreement No 101249732. The views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority (European Cybersecurity Industrial, Technology and Research Competence Centre). Neither the European Union nor the granting authority can be held responsible for them.

From isolated events to dynamic risk scoring

One of the most promising developments in cyber security is the move away from alert-centric operations towards continuous risk assessment.

Traditional security platforms often generate hundreds or even thousands of alerts every day. While many are technically accurate, they frequently lack sufficient context to help analysts determine which require immediate attention.

Modern behavioural analytics approaches instead maintain a continuously evolving risk profile for users, endpoints and other critical entities.
Each new observation contributes to this assessment:

- Recent behavioural deviations
- Privilege level
- Asset criticality
- Observed attack techniques
- Threat intelligence confidence
- Historical incident data

Risk therefore becomes dynamic rather than static. Rather than treating every alert equally, security teams can prioritise investigations based on the entities whose behavioural evolution suggests an increasing likelihood of compromise. This enables analysts to spend less time triaging low-value alerts and more time investigating genuinely high-risk situations.

Predictive analytics within the CIPHER project

Within CIPHER, Work Package 2 focuses on advancing cyber-risk and threat assessment methods that support proactive cyber defence across essential sectors. Rather than relying solely on reactive detection mechanisms, the objective is to provide organisations with better situational awareness and earlier indicators of potential compromise.

One of the tools being developed within this work is PreventUEBA, a behavioural risk assessment component that applies machine learning techniques to model user and entity behaviour while enriching observations with Cyber Threat Intelligence obtained through MISP.

By correlating behavioural deviations with external intelligence and attacker tradecraft, PreventUEBA aims to move beyond simple anomaly detection towards continuous behavioural risk assessment. The goal is not to generate more alerts, but to provide analysts with meaningful risk scores that reflect both internal observations and the evolving external threat landscape.

This approach allows security teams to identify users or systems whose behaviour increasingly resembles known attacker techniques before a full incident develops, enabling earlier investigation and more informed decision-making.

ECCC

Funded by the European Union

Funded by the European Union's Digital Europe Programme under Grant Agreement No 101249732. The views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority (European Cybersecurity Industrial, Technology and Research Competence Centre). Neither the European Union nor the granting authority can be held responsible for them.

Predictive analytics is therefore not intended to replace security analysts.

Rather, it augments their expertise by highlighting where their attention is likely to have the greatest operational impact.

Looking ahead

Predictive behaviour analytics is not about predicting the future with certainty.

Cyber security remains an adversarial domain in which attackers continually adapt their techniques and defenders must respond just as quickly. No machine learning model can eliminate uncertainty, nor should automated systems be expected to replace human expertise.

However, by combining behavioural modelling, machine learning and continuously updated threat intelligence, organisations can make better-informed decisions earlier in the attack lifecycle. The result is faster detection of emerging threats, more effective prioritisation of investigations and a stronger understanding of organisational cyber risk.

For operators of critical infrastructure and essential services, even modest improvements in early risk assessment can significantly reduce response times and minimise operational impact.

As cyber threats continue to evolve in both sophistication and scale, organisations will increasingly need capabilities that anticipate malicious activity rather than simply documenting it after the fact. Behaviour analytics enriched with Cyber Threat Intelligence represents an important step towards that goal, helping security teams become not only faster at responding to attacks, but better at anticipating them before they escalate.

FOLLOW US!

ECCC

Funded by the European Union

Funded by the European Union's Digital Europe Programme under Grant Agreement No 101249732. The views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority (European Cybersecurity Industrial, Technology and Research Competence Centre). Neither the European Union nor the granting authority can be held responsible for them.