Detection & Impact Scoring of Anomalies in Microsoft Entra ID Logs

Stephan van de Ven – s1123881 - Computing Science | Cyber Security

Supervised by: Erik Poll

Second Examiner: Stjepan Picek

Tesorion workplace supervisor: Cees Mandjes

Start / End Dates: 26/01/2026 – 10/07/2026

Short Description

Develop and validate a vendor-independent detection model that automatically finds anomalous behaviour in user identities using Microsoft Entra ID sign-in and audit logs of approximately 40 customers, and assigns an severity level (low, medium, high) to each detection suitable for operational SOC use. This is to create an autonomous generic environment independent of Microsoft's out-of-the-box detection mechanisms that can recognize anomalous behaviour and assess its impact.

Research questions

- Which statistical/AI methods are suitable and robust for detecting identity anomalies in large-scale Entra ID logs in an operational SOC?
- How can anomaly scores be combined with contextual information to produce an actionable severity level?
- How can model performance and practical usefulness be validated when labelled incident data is scarce?

Methods

Data inventory & Privacy: specify required fields and ensure pseudonymization, tenant consent, and retention + processing compliance.

Feature engineering: create behavioural features (login frequency, session duration, time-of-day patterns, etc.) and context features like roles and privileges.

Graph-based approaches: account, device, and asset graphs with anomaly detection.

Collection & Calibration: combine signals into a single anomaly score and apply explainability for SOC analysts. Combine anomaly score with weights to derive severity levels via rule-based scoring or a calibrated classifier.

Validation: use existing detections (including Microsoft Identity Protection alerts) as partial labels, create adversarial scenarios and possible red-team simulations, and perform “human-in-the-loop” labelling with SOC analysts if needed.

Extra information:

On-site / work arrangement at Tesorion: presence 3 days/week on-site, 2 days/week off-site.