

CAP ANOMALY SPOTTER

Anomaly Detection for identity and access management

Identity and access management (IAM) is the security and business discipline that enables the right individuals to access the right resources at the right times and for the right reasons. It addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements. Solutions with the focus on governance and compliance is often called IGA (Identity Governance and Administration).

Opportunity for advanced machine learning analytics in identity and access management

Gartner predicts that by 2018, analytics, machine learning and policies will replace more than 50% of manual access certification and request approval tasks, up from less than 2%. More and more organizations come to the conclusion that traditional access certification methods are “inexact, labor-intensive, error-prone and insufficient to properly address inherent risks,” (Gartner 2016)

CAP Anomaly Spotter solution for IAM

Company: A global IT security product company

The challenge: Our customer wanted an advanced analytic module to their network monitoring and IAM products that they offer to enterprise customers. The products monitor the secured traffic in the enterprise network and monitor and manage the access privileges of the employees in the company.

Our solution: We adopted the CAP Anomaly Spotter engine to the specific use cases relevant in our customer's products. The CAP module is fully integrated into customer's product platform through a simple, though custom-made interface component. The CAP module processes the data in parallel to the main product and filters out unusual events that may indicate reason for intervention by the security administrator of the company. These events may include: unusual behavior of the network device or user or in case of access right management: conflicting access rights or rights belonging to orphan accounts. The results of the CAP analysis are displayed to the user as part of the parent product's user interface.

Benefits of CAP Anomaly Spotter

- ▶ Detects and highlights the most noteworthy anomalous events and incidents using advanced machine learning analytics.
- ▶ Improves efficiency and decreases the cost of operations by automating the detection of the most noteworthy events in the system.
- ▶ Improves the service quality at the enterprise and employee level
- ▶ Modular integration is cost-effective and flexible. CAP Anomaly Spotter operates in parallel, and does not affect the performance of the parent product.

About CAP Data Technologies

CAP Data Technologies is a Finnish technology startup providing data analytics solutions utilizing our advanced anomaly detection technology. CAP Anomaly Spotter has the ability to detect previously unknown behavior in the system without relying on pre-set rules or fingerprints.

Contact CAP Data Technologies

tuomo.sipola@capdatatechnologies.com tel: +358 40 753 2169
markku.ranta@capdatatechnologies.com tel: +358 50 324 6233

Try out the free trial version on our web site
www.capdatatechnologies.com