How it Works

personam™

INSIDER THREAT DETECTION

know

FRAUD | THEFT | SABOTAGE

Insider threat Detection

Detect the Threat

Monitor all network activity

Sensors are placed at strategic locations on the network to observe all data transfers to and from the organization's critical resources, such as shared file systems, mail servers, and CMS applications. All internet traffic is also monitored.

Build behavior profiles for every person and device

Advanced data analytics algorithms running on the appliance add each data transfer record observed by the sensors to the behavior profile of the user account or device that originated the transmission. This provides the system with a rich history of how each actor uses the network.

Discover cohort groups

The system places the people and devices with the most similar behaviors together into cohort groups. This provides additional insight into how behavior patterns are distributed throughout the organization. Behaviors can be monitored for threatening changes, and compared to cohorts for unexpected differences.

Detect the threat

Using robust behavior profiles, an understanding of organizational patterns, and advanced machine learning algorithms, the system will detect pre-existing and emerging attacks by insiders who have the access and intent to commit crimes.

Get peace of mind. Contact Personam today for a trial.

Personam™

PersonamInc.com