A nuclear facility disabled in Iran; 6,5 million credentials stolen from LinkedIn; and a nationwide attack on the German parliament. These are just a few examples of headlines that occur almost daily in the news.

Hackers nowadays design complex attacks to maximize the damage in a facility. These targeted attacks use background knowledge to hide their communication inside a computer network, which makes the discovery of such viruses a challenge.

In practice, fully automated techniques generate too many false alarms when trying to detect targeted attacks whereas manual inspection is impractical due to the vast volumes of data. In the thesis were therefore aimed for a hybrid approach by combining human intelligence with the speed of automated techniques using visualization and data-mining. The result is a new software system Eventpad to quickly reveal undesired patterns in large event collections.

Besides the discovery of Ransomware and the detection of Voice Over IP fraud, the software was successfully used for detection of illegal waste dumping in a nature preserve and discovery of bottlenecks in patient cancer treatments. Besides numerous awards and laudatory reviews from industry, the technology obtained a valorization grant to continue development of the software in the startup AnalyzeData.