Every interaction, client, and device should be accounted for and continuously monitored to detect vulnerabilities in an operational technology (OT) process. This paper focuses on the evaluation of one of the two major schools of thought in the field: active monitoring. Active monitoring involves inserting test data into the network and collecting information on how various components interact with traffic. It is a faster process than its passive counterpart but requires carefully tailored traffic to avoid system disruption. Along the same line of thinking, multiple active defense measures known as model-based defenses exist, such as dynamic watermarking and packet-delays. These defenses stealthily inject data, usually noise, into a system to serve as a signature and validate the component. The authors recognize three key challenges in this approach: the sheer number of components and large amount of data involved in such processes, the risk of mimicking and/or learning the signature, and ensuring that the injected data does not significantly affect the system behavior. Massive advancements in the field of “big data” have enabled efficient handling of copious amounts of data while extracting meaningful information from them to create a system signature. On one hand, such techniques can be used to create system signatures that do not disrupt the system. On the contrary, the authors recognize that such signatures can be learned and even mimicked by a technologically adept adversary. This paper utilizes reduced order modeling (ROM) techniques to detect patterns in industrial systems and create signatures and performs an assessment of system security if the data is available to the aforementioned formidable adversary.