SCADA SIEM TOOL

For Transmission SCADA Systems

About Product

C-DAC SCADA(Supervisory Control and Data Acquisition System) SIEM(Security Information and Event Management) tool allows to identify threats by continuously monitoring all data generated by IT systems at different phases like network traffic, main memory usage, reviewing files against white listed file profiles in RDS (reference data set) etc. while conducting experiment over SCADA test bed. The monitoring process generates baseline for every experimental activity and identifies all anomalous activities by comparing the same with a reference signature based activity log. The SIEM Dashboard presentation of the monitored activity helps to immediately identify the anomaly at a specific level thereby reducing response time and better forensic investigation.

Features

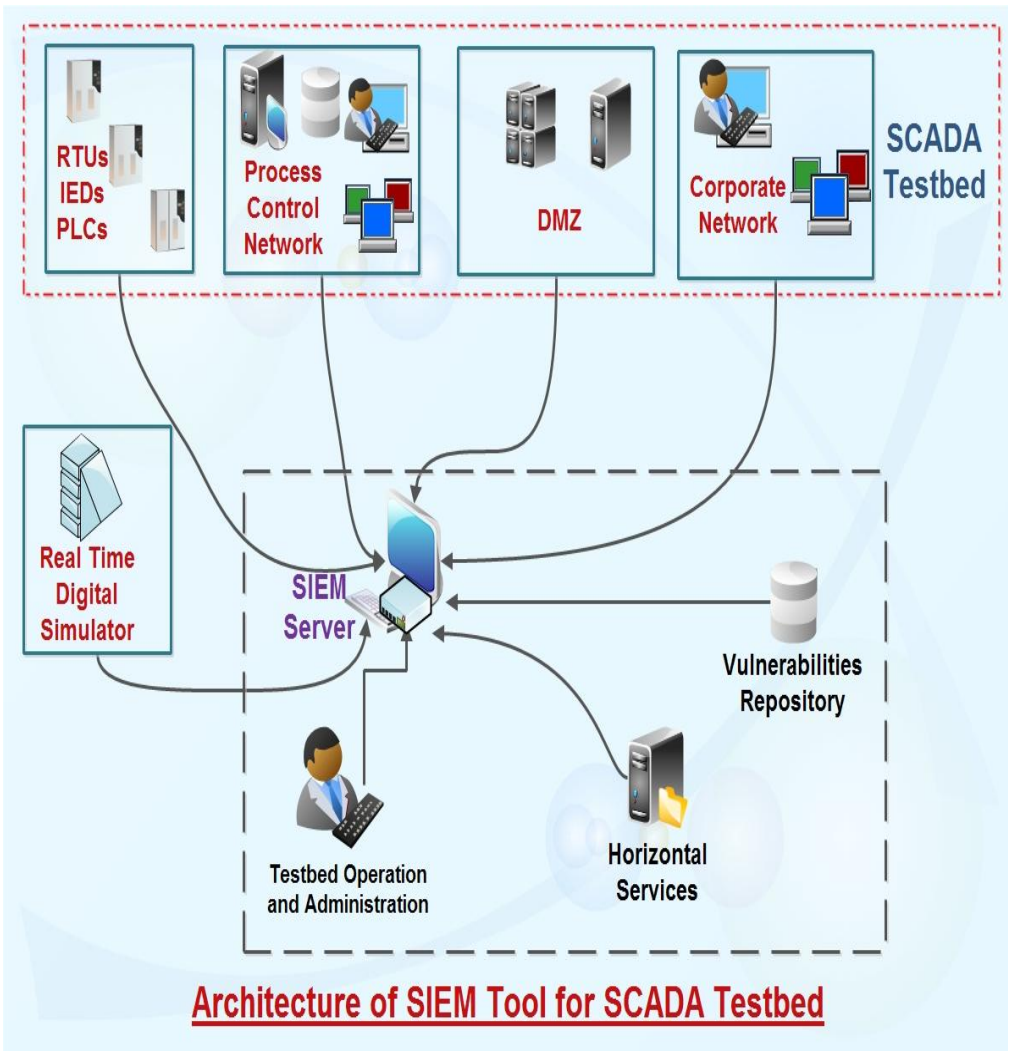
- A complete attack simulation, monitoring and management tool specifically engineered for the SCADA systems.
- Employs C-DAC's Multi Agent based deployment Framework (CMAF) without impacting SCADA System reliability.
- Efficient Analysis through a single window dashboard.
- Uses correlation, data aggregation, and retention for anomaly detection and forensics investigation.

Product Details

- Integrated Simulation, Monitoring and Management.
- Uses agent based model (CMAF) for initiating attack simulation on testbed, gathering and finally updating the results for presentation without impacting other processes.
- Data aggregation covering sources such as Network monitor, Memory analysis and suspicious file profiles.
- Operational Dashboard for analyzing all possible parameters on a single window.
- Fast Forensics with reference lookup and anomaly detection.
- Anomaly detection based on deviation from baseline activity across multiple dimensions of SCADA system activities.
- Correlates events based on common attributes, like same parent process, for presentation.
- Retention of incidence data.
- Instant retrieval of experimental results history.

Product Highlights

- Real time simulation of attacks in a controlled environment (SCADA Testbed).
- Provides configuration for scalability of SCADA testbed.
- SCADA testbed follows Live, Virtual and Constructive (LVC) model.
- Automation for conducting attacks and monitoring over the network with standard in-house CMAF implementation.
- Integrates key features like network monitoring, process monitoring, file monitoring, memory monitoring, signature based file scanning, for in-depth analysis of different attack scenarios.
- Uses open source tools for monitoring.



Architecture of SIEM Tool for SCADA Testbed

Center for Development of Advanced Computing (C-DAC)
Real Time Systems & Smart Grid
Knowledge Park , No 1, Old Madras Road, Byappanahalli, Bangalore-560038.
Telephone No: +91-80-66116400/01/02/03