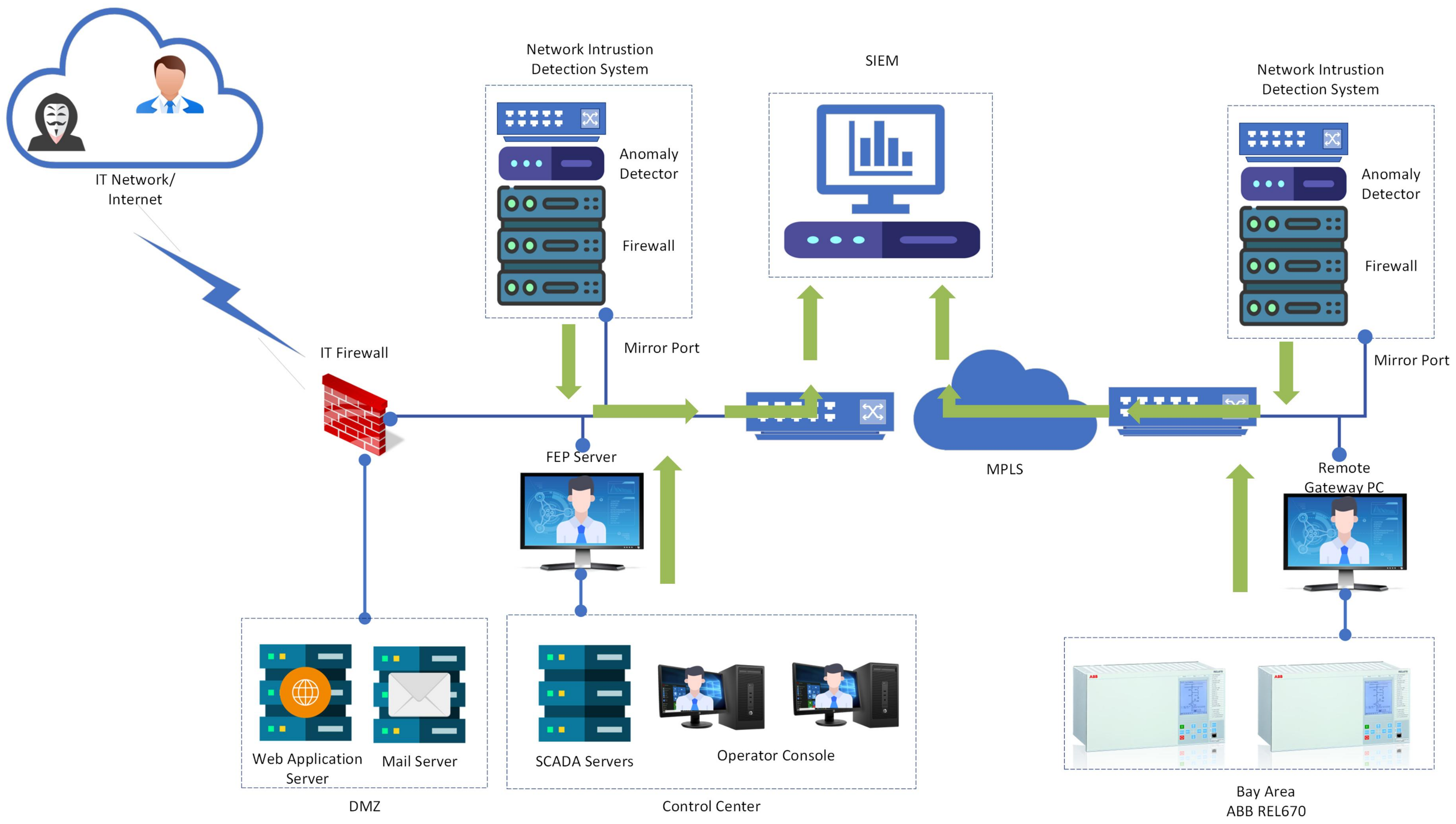
Machine Learning based Intrusion Detection for Power Grid

Objectives:

- Build a behavior based distributed firewall to monitor substation network
- Define rule-based policy framework to identify anomalous behavior of the system
- Develop Deep Packet Inspection for grid specific protocols
- Develop malware agnostic host integrity checker for Windows OS
- Develop IDS and visualization tools for OT operations
- Automate the real-time analysis of system parameters using ML based data driven models



Architecture:

- Proposed architecture of where our Intrusion-Detection System will be installed
- The HIDS analyses and generates alerts against anomalies detected in controller PCs and operator consoles
- Similarly, the NIDS captures, analyses and generates alerts against malicious traffic detected in communication of Bay area devices.

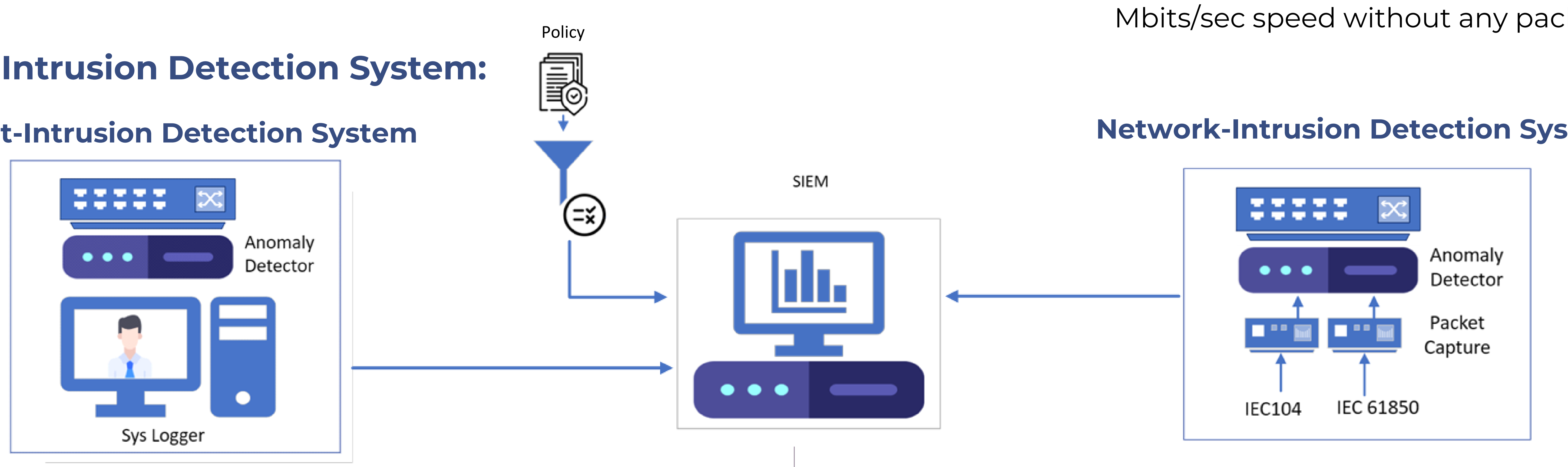
Highlights:

- Developed 'WinObserve' application that acts as an integrity checker for the Windows host
    - Monitors users, processes, resources, and data files
- Developed multi-threaded real-time DPI engine for
    - IEC-61850(GOOSE,SMV and MMS)
    - IEC 60870-5-104
- Framed ruleset based on grid and network protocols
    - DPI engine was tested for 100 Mbits/sec speed without any packet loss

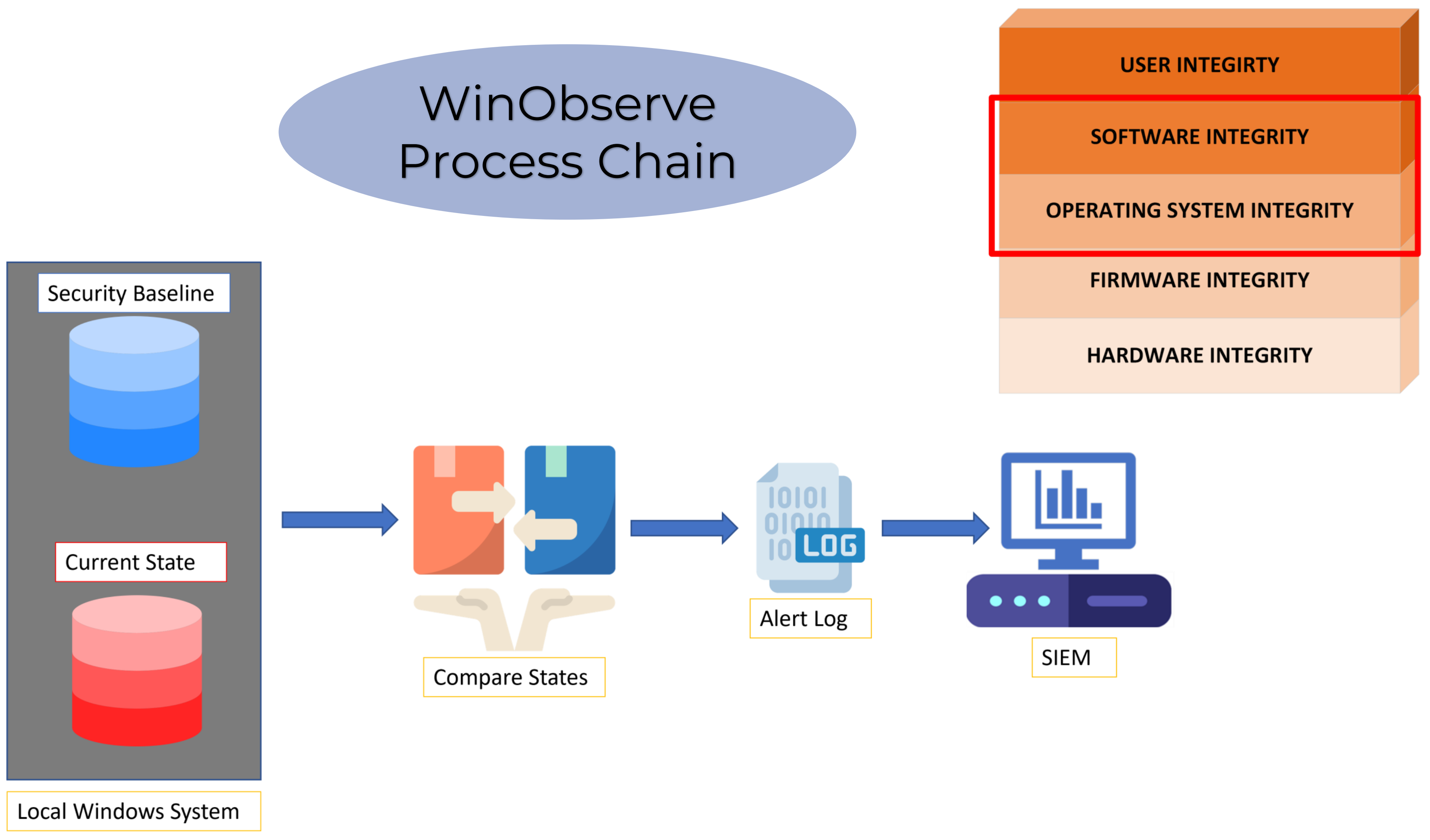
Proposed Intrusion Detection System:

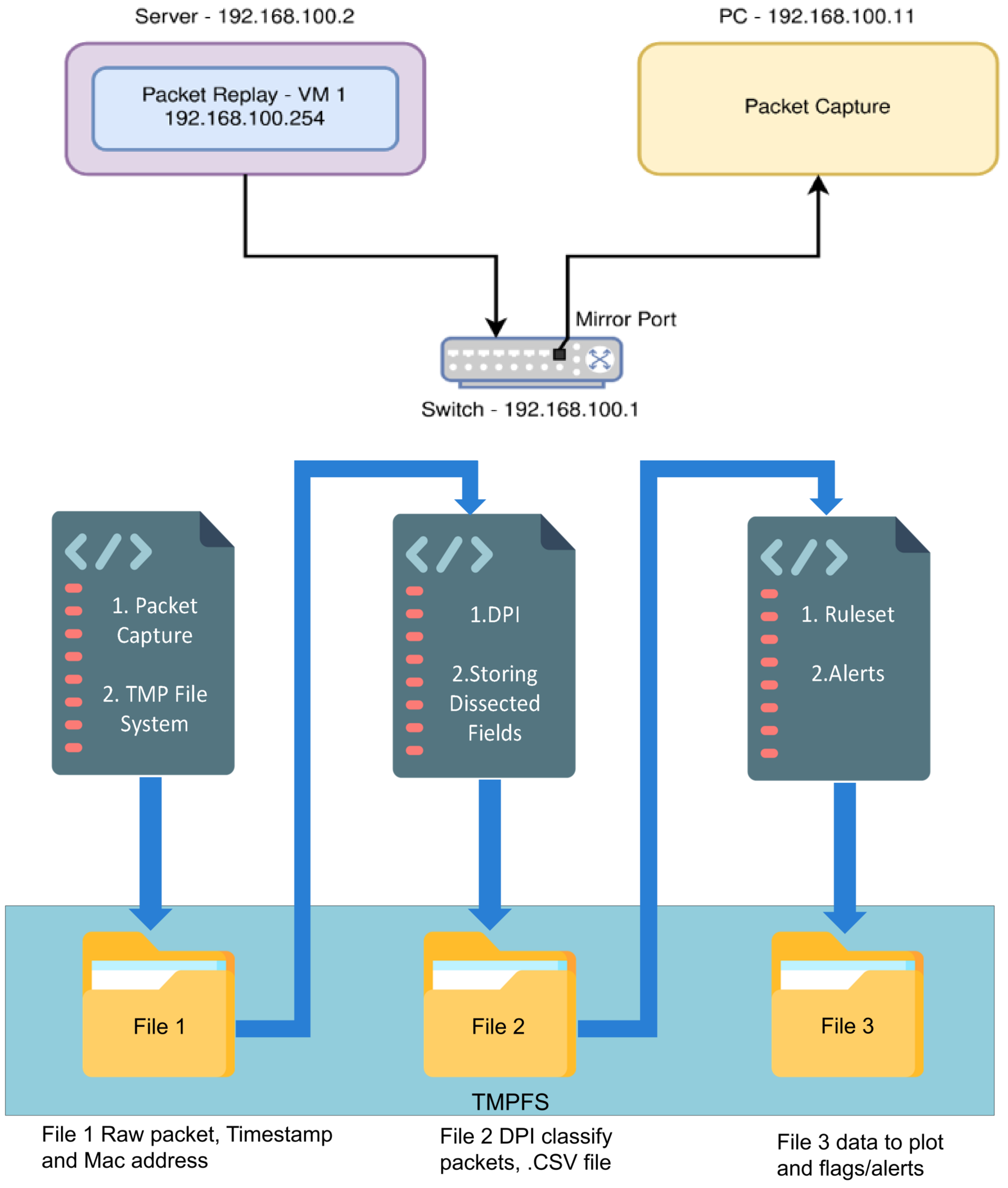
Host-Intrusion Detection System

Network-Intrusion Detection System



Operating System	OS Build, Version, Architecture, Kernel, Files and DLLs
Network	Interfaces and Drivers, Open Ports, Established Connections, Service Ports
Processes	Process Details, Path, Privilege Level
Services	Service Name, Path, Ports used by Service, Privilege Level
Applications	Installed Applications, Path, App Related DLLs
User Environment	Files and Folders, Registry Keys





File 1 Raw packet, Timestamp and Mac address

File 2 DPI classify packets, .CSV file

File 3 data to plot and flags/alerts

Current Progress:

- Development of WinObserve - Host-Integrity Check Application for Windows operating System is in Beta stage
- SIEM dashboard is under development
- Advanced network traffic and protocol-based ruleset are being framed and tested
- A GUI to give system overview and alerts is under development

POWERGRID
CENTER OF EXCELLENCE
IN CYBER SECURITY

Nakade Sourabh Arvind ,Ajil P., Rakshith R., Onkar Joshi, Chandramani Singh, Haresh Dagale

Department of Electronic Systems Engineering