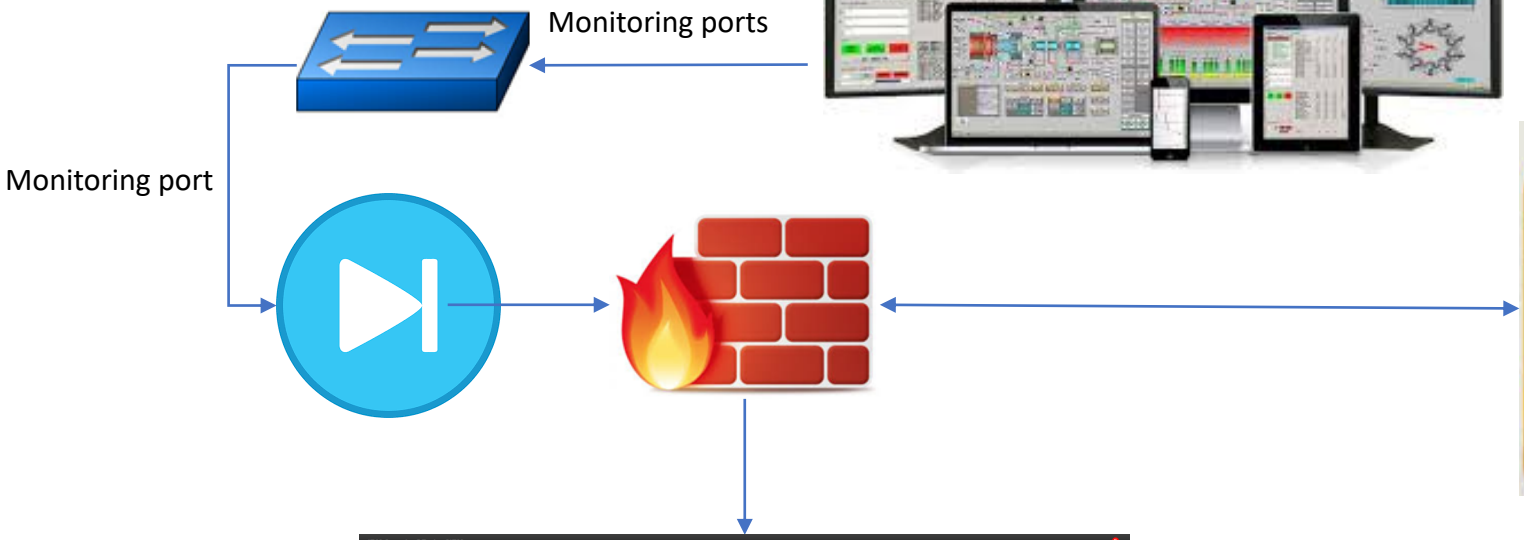
Operational Technology (OT) Network

RTU

IDS/IPS

Relay

Plants Network



Plant System

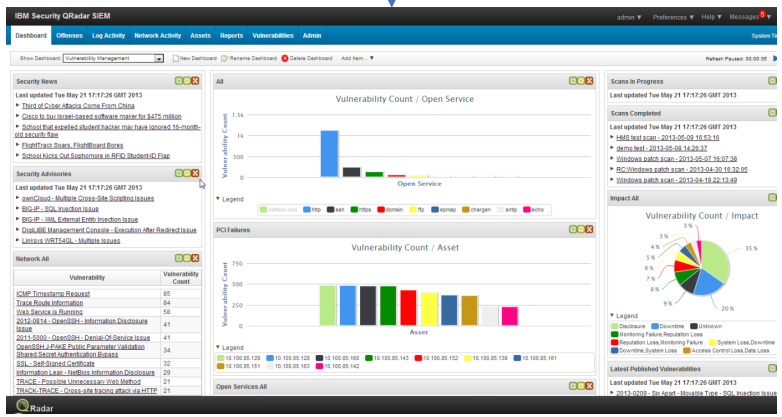
Human Machine Interface (HMI)

Programmable Logic controller (PLC)

Remote terminal Unit (RTU)

Switches

Relays



IBM QRadar

Integrated Security Operations Center

Plants Network

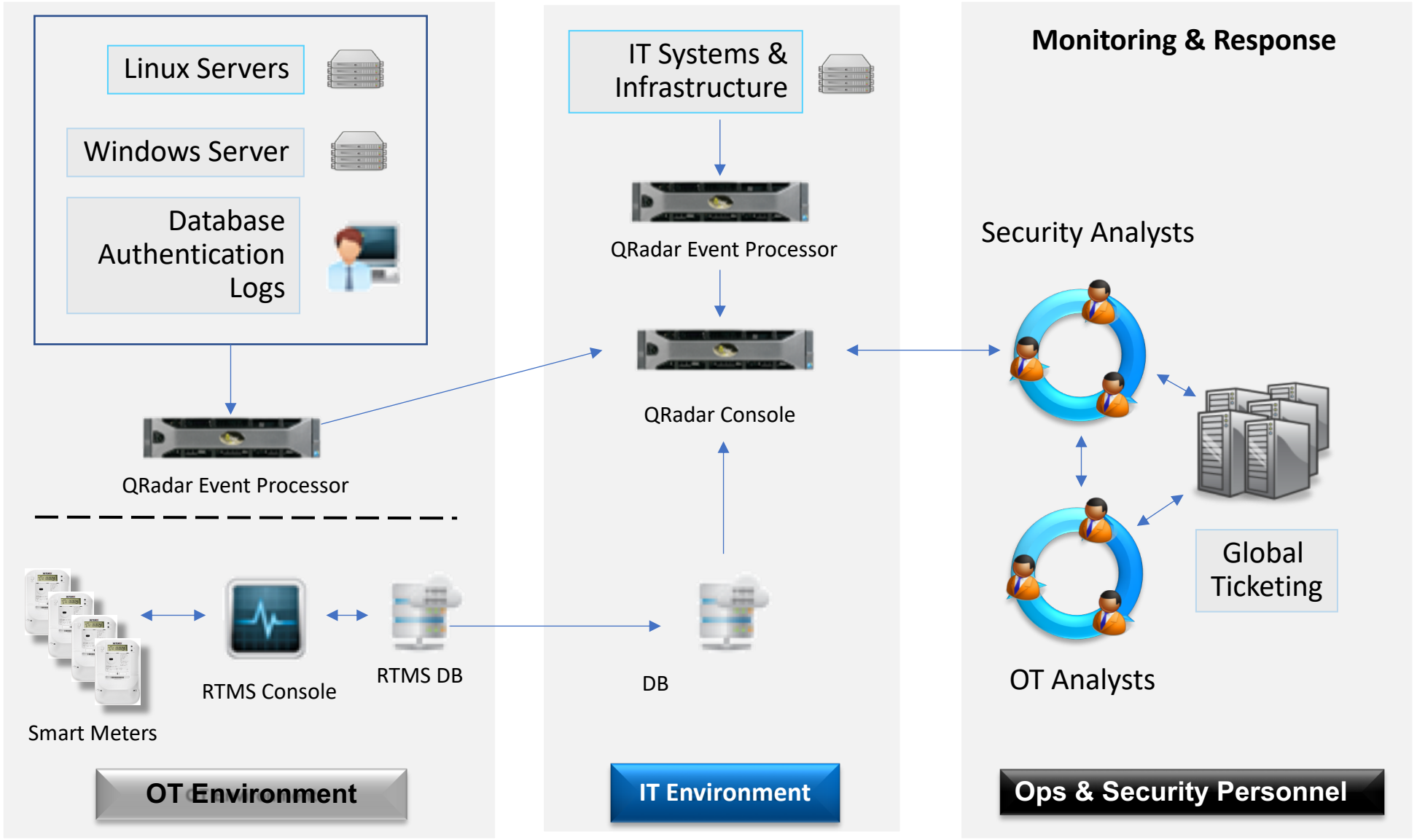
Business Network

OT Network

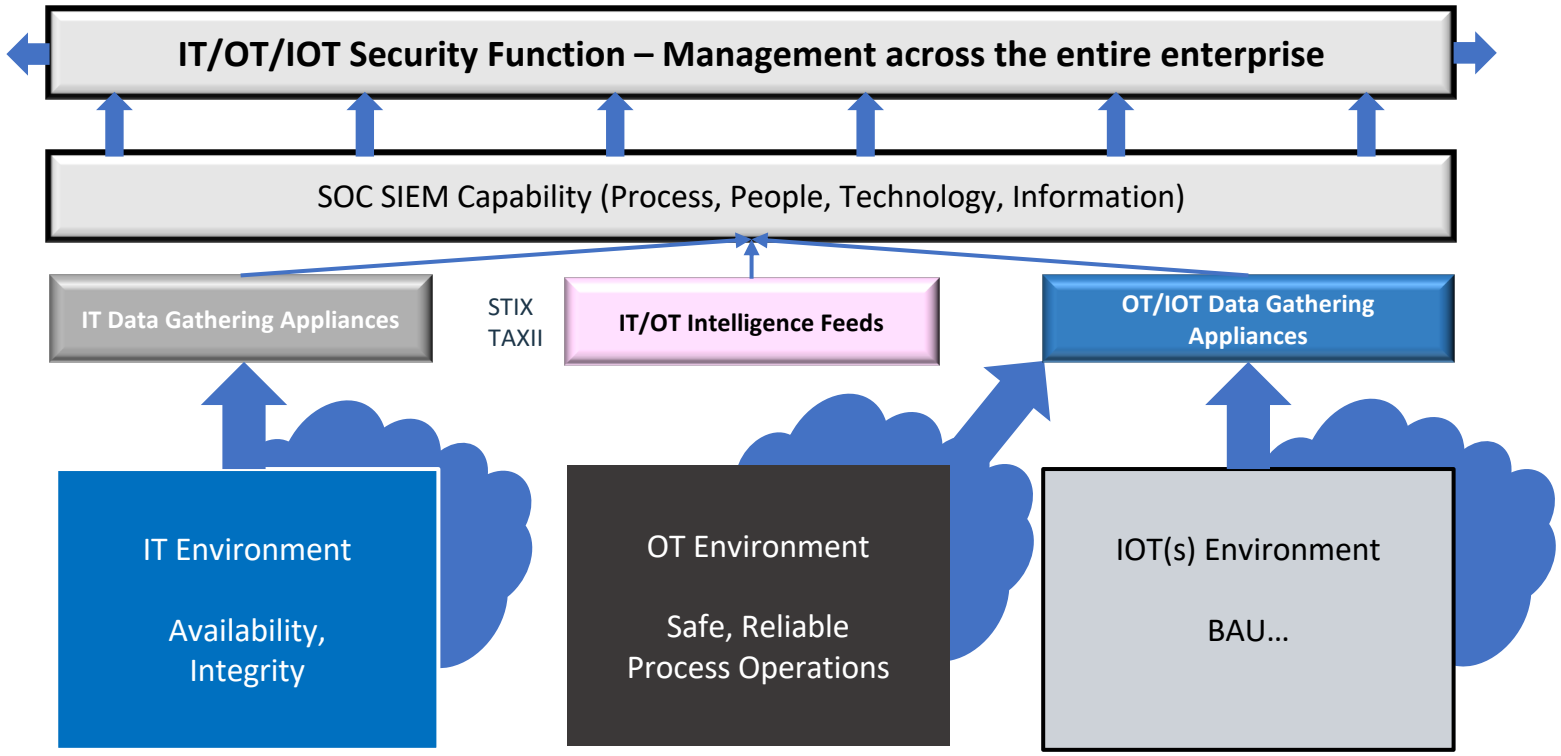
IBM QRadar

Central Console

Simplified Architecture



IBM Defines Security as a Business Capability layer



Common ports and servers used by QRadar

SSH communication on port 22
All the ports that are used by the QRadar console to communicate with managed hosts can be tunneled, by encryption, through port 22 over SSH.

The console connects to the managed hosts using an encrypted SSH session to communicate securely.

These SSH sessions are initiated from the console to provide data to the managed host. For example, the QRadar Console can initiate multiple SSH sessions to the Event Processor appliances for secure communication.

This communication can include tunneled ports over SSH, such as HTTPS data for port 443 and Ariel query data for port 32006. IBM Security QRadar QFlow Collector that use encryption can initiate SSH sessions to Flow Processor appliances that require data.

To provide secure data transfer between each of the appliances in your environment, IBM® Security QRadar® has integrated encryption support that uses OpenSSH. Encryption occurs between managed hosts; therefore, you must have at least one managed host before you can enable encryption.

When encryption is enabled, a secure tunnel is created on the client that initiates the connection, by using an SSH protocol connection. When you enable encryption on a managed host, an SSH tunnel is created for all client applications on the managed host.

When you enable encryption on a non-Console managed host, encryption tunnels are automatically created for databases and other support service connections to the Console.

For example, with encryption enabled on an Event Processor, the connection between the Event Processor and Event Collector is encrypted, and the connection between the Event Processor and Magistrate is encrypted.