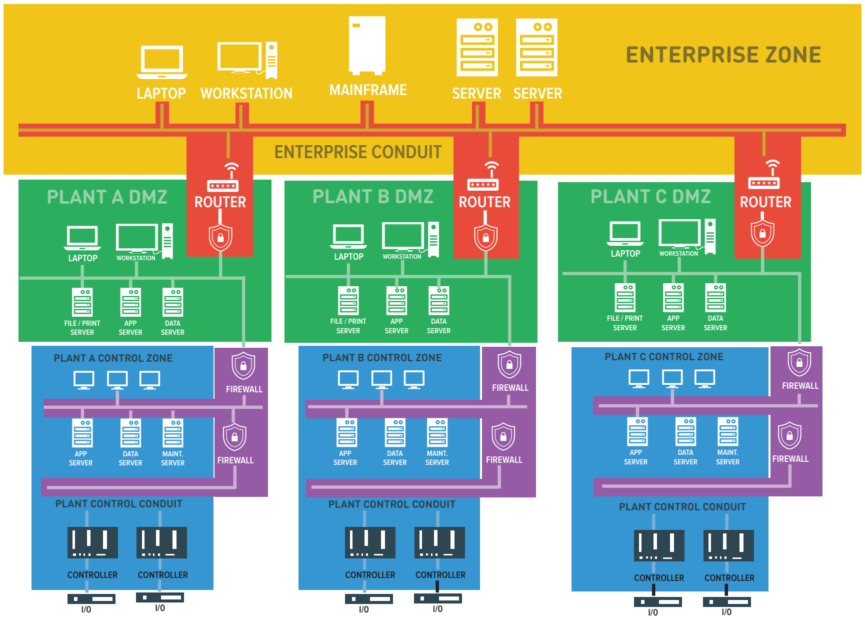
CASE STUDY

Industrial Cybersecurity Solution

exida worked with an **Oil & Gas** company to perform a **Cybersecurity Vulnerability Assessment (CVA)** on a gas refinery process control network.

PROJECT SUMMARY

The initial request from the Oil & Gas company was to perform a Cybersecurity Vulnerability Assessment (CVA) on a gas refinery process control network. The first step was to review all the documentation for the Industrial Control System (ICS), which included all the policies and procedures, network architecture, switch, router, firewalls and their configurations. It is important to review these documents before going onsite, to see what is in place and learn the company's structure. The network diagram received was very detailed and well thought-out with an expertly designed architecture and integrated DMZ similar to what is shown in the example to the right.



(continued)

CHALLENGES

The network architecture was a well designed and constructed solution, showing the plant enterprise zone being separated from the Process Control Network by 3 DMZ firewalls, one for each process control network. However, there was a note stating that this solution had not been implemented.

SOLUTION

The assessment began with taking a high level tour around the facility. It was immediately noted that there were obsolete revisions of Windows operating systems: NT, XP, Server 2000. This is not uncommon in a control system so it was noted, and then continued. The most surprising find during the actual assessment was that, unbeknownst to the customer, multiple vendor supplied NT systems were infected with malware. The irony of this was that the OS was so old the virus didn't know how to handle it so it never propagated. A recommendation was made that the user contact the vendor to get a clean OS load for their equipment, in addition to removing the infestation locally, which proved somewhat successful.

Looking at the network and attached work stations and servers, close to a dozen multi-homed servers were found, some with as many as 6 Network Interface Controller (NIC) cards. A recommendation was made that if this many connections are needed, the systems would be better placed in a DMZ with routed firewall controlled access.

The network architecture was confirmed as a "to-be-implemented design." The DMZ designated switch was mounted and clearly labeled, but had no wires and was powered down. A strong recommendation was made that the DMZ be designed into the network and appropriate routing and firewall rules be implemented.
There was an attempt for remote access connections from the enterprise system and it was discovered that a direct connection was possible from the enterprise system to the PCN. Part of this was due to the multi-homed systems. There was a need for removal of these systems and disabling of remote desktop services except for systems in the DMZ.

It turned out that the device (switches, routers, and firewalls) configurations weren't provided because how to extract them was unknown. Local representatives were then trained on basic procedures on how to work with the devices and downloaded configurations from all switches. Many of the switches were simply pulled out of the box and plugged in, without configuration or applying security measures. It was recommended that a standard configuration including disabling non-secure protocols, limiting access, and using strong passwords be implemented immediately.

RESULTS

The key learning point for the customer was the importance of having properly configured firewalls and network switches to enable zones and conduits to be set up to control the flow of data in and around the PCN.

As a result, exida is continuing to work with the customer to help improve the situation and another cybersecurity vulnerability assessment is being considered.

The key benefits provided by exida was the ability to review the policies, procedures and network architecture in order to identify problem areas, not just from the cybersecurity point of view, but also performance. exida's experts were able to guide the customer and train them on how to support the facility. Understanding the importance of how and what information was flowing through the PCN and external networks enabled exida's experts to correctly identify problems with the firewall configurations.