DIGITAL IMMUNITY™
STAY PRODUCTIVE, STAY SECURE

DI PROTECT™

The Purdue Model and Digital Immunity

DIGITAL IMMUNITY

Stay Productive. Stay Secure.

The Purdue Model and Digital Immunity

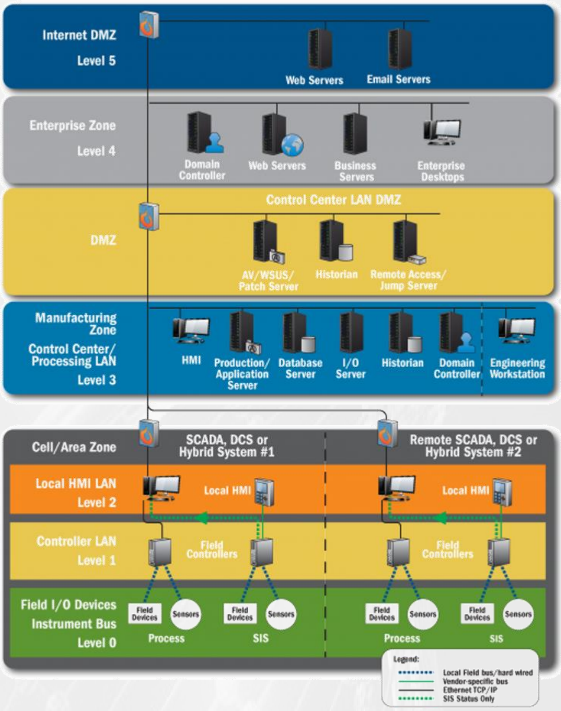
These days, many of us want to know more about a product or service before engaging a vendor. To that end, Digital Immunity is creating a collection of concise documents - an Education Series - to educate and engage potential customers. During this learning process, you may want to engage with our staff to delve deeper into the product, delivery models, licensing and more. Once you contact us, we will ensure the right team members are engaged to help you finalize your assessment and demonstrate the associated Return-On-Investment.

This document will outline food for thought when implementing Digital Immunity's DI PROTECT™ in a manufacturing environment based on the Purdue, or ISA/95, models.

PURDUE MODEL

Many people in the OT/ICS community are aware of the Purdue Model and the inter-relationships between systems and data flows. Software vendors and consulting companies are also becoming well versed in this model and use it to describe the overlay of their technology and services.

In this document we'll look inside the Manufacturing Zone of the Purdue Model, levels 3, 2, and1.



NETWORK SEGMENTATION

One of the most common cyber-threat interventions, leveraging the Purdue Model, is to implement a DMZ between a corporation's enterprise network and the manufacturing networks at each site. This DMZ, implemented correctly, provides many benefits to manufacturing sites, including:

- Increases the difficulty for malware to find a pathway from the corporate network into manufacturing, and vice versa.
- Common industrial control protocols are not visible from the enterprise network. Bad actors will need to find the manufacturing networks and may get detected in this process.
- Increases understanding of the network and better understanding of what VLANs make up manufacturing, helping with controls, detection efforts, investigations, etc.

Network segmentation is critical to a good Defense-in-Depth strategy and should be considered a high-priority for most corporations. Having said this, additional protection and detection mechanisms for manufacturing networks are needed.

OT/ICS SYSTEMS

The architecture of DI PROTECT™ fits well with OT/ICS systems. The ability to:

- Create reference platforms that can be re-used across like devices
- Deploy lightweight sensors to devices with virtually no impact to the device
- Provide significantly improved protection to devices from malware/ransomware/zero-days

- Roll-up alerts in a multi-tier model allowing regional, functional, and corporate views of various dashboard and alert information.

Windows OS-based HMIs, Engineering Workstations, and Application Servers are primary benefactors of increased protections provided by Digital Immunity's solution. Let's face it - most malware is designed for Windows systems. Therefore, significantly strengthening protections on these systems is a wise business decision.

The next layer to consider are systems, albeit one step removed from directly touching the automation process, yet, are extremely critical to on-going production operations. These include systems such as Manufacturing Execution Systems (MES), Process Control Historians, and Alerts/Log management.

One of the exciting directions in the OT space are authentication controls between HMI's and Controllers. By authenticating communication channels and end-to-end communication with controllers (e.g. CIP Security), the ability to initiate a man-in-the-middle attack or direct attack on controllers is significantly lessened. With DI PROTECT™ protecting the Windows-based system (e.g. HMI) and new protocols such as CIP Security protecting the communication channel/PLC, the future can become much more secure.

QUALITY CONTROL SYSTEMS

In manufacturing environments, personnel and equipment are aligned to repeatably produce a product per specifications to meet customer requirements.

Quality control personnel are tasked with checking to ensure product specifications are met. Checkpoints during the manufacturing process may be established to ensure intermediate specifications are met that have an impact on the quality of the final product. The key point is quality control systems are integral to the manufacturing process and if negatively impacted also can shut-down production.

Therefore, when looking at the manufacturing ecosystem, one must consider other systems that may benefit from the extra protections provided by DI PROTECT™.

CONDUITS AND SERVICES

Other conduits and services can be considered as risk points to manufacturing operations and therefore worthy of additional protection. Some examples to consider are:

- Jump servers to gain access into manufacturing network zones
- Remote Access systems providing pivot points into manufacturing
- Dual NIC'd systems spanning VLANs
- Corporate Services
  - Backups
  - Software delivery tools
  - AD
- HVAC systems

These systems can provide pathways into manufacturing and therefore bring risks to the Defense-in-Depth cybersecurity controls. An additional layer of hardening, by implementing DI PROTECT™, can provide valuable protection to this last line of defense.

SUMMARY

Protecting key Windows devices inside manufacturing networks is the last mile of defense. If malware or a bad actor gets past firewalls, IDS's, and gains control of these endpoints, manufacturing operations will be at risk.

An installation program, taking into account the various systems key to the manufacturing process, is very important. It may not be possible to include all these systems in an initial deployment; therefore, it is important to prioritize and proceed with the most critical systems first to protect the overall business, then continue with future phases to protect the most critical systems making up the manufacturing ecosystem.

About Digital Immunity

Digital Immunity, an IQT Portfolio company that is revolutionizing cyber-threat protection, bridges the gap between real-time threat prevention and 24/7, mission critical environments so security no longer takes a back seat to production. We provide advanced malware prevention on mission critical devices in Operational Technology environments, with no impact to production or system performance.

"Revolutionizing cyber-threat prevention in Operational Technology environments."

Founded in 2015 and headquartered in Burlington, MA, Digital Immunity provides revolutionary cyber-threat prevention solutions, DI PROTECT™, for modern cyberwarfare. Our patented Digital DNA Mapping technology prevents advanced threats, including APT's and zero-day attacks, from executing in memory at runtime, hardening your mission critical operating systems and applications, with no disruption of good processes or production. Using Digital Immunity's Control Center you can mobilize your security team with real time actionable alerts and forensics artifacts in context.

What Makes Digital Immunity Different?

- In memory at run time prevention
- Works in air-gapped environments - completely self-contained
- Real prevention, unlike traditional AV detection - no preexisting knowledge of threats needed
- Hardening of OS and Applications
- No false positives
- No patch fatigue
- No extraction of data for analysis in the cloud
- Provide threat intelligence in context via the Control Center dashboard
- Remediation takes place on the device
- Works on "gray" systems as well due to DNA mapping process
- Doesn't need to learn or update – not dependent on AI or machine/behavioral learning

Contact Us

60 Mall Road, Suite 309,
Burlington, MA 01803

Phone: (781) 425-8655
Email: Sales@digitalimmunity.com
Web: www.digitalimmunity.com