DIGITAL IMMUNITY™
STAY PRODUCTIVE, STAY SECURE

Defense-in-Depth

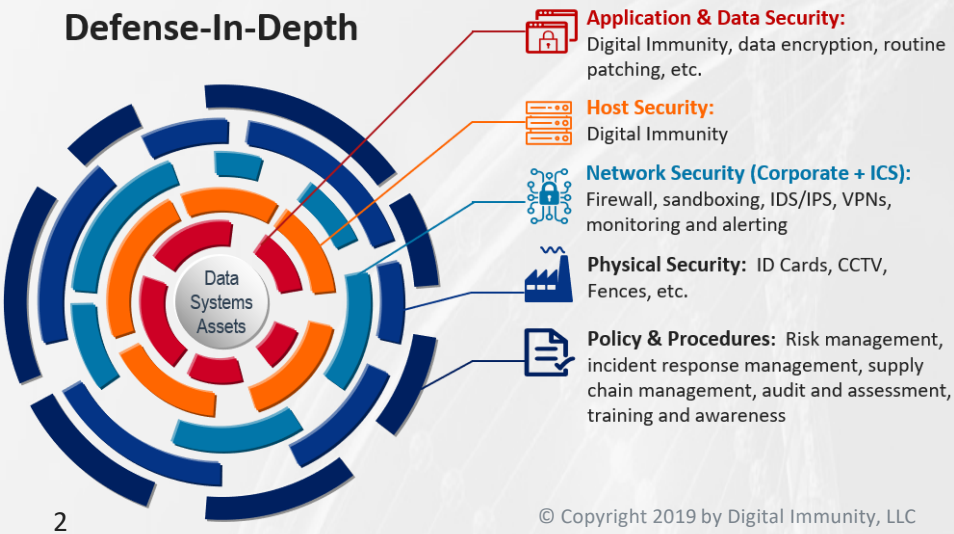
DI PROTECT™ and Intrusion Detection Solutions

Defense-in-Depth: DI PROTECT™ and IDS

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.

One of the common questions we hear often is how do Digital Immunity's products compare and contrast to the Intrusion Detection Systems (IDS) being offered in the Operational Technology (OT) space, such as Indegy, Claroty, Nozomi, Dragos, and others.

Both Digital Immunity (DI) and OT IDS systems do play critical roles in a Defense-in-Depth strategy. Digital Immunity's DI PROTECT™ provides unique benefits which will be further highlighted in this document.



COMPARISON CRITERIA

The criteria to be used for comparison are:

1. Inventory
2. Detection
3. Protection (Passive vs. Active)
4. USB
5. Alerts

1.0 INVENTORY

Getting an accurate and detailed inventory is very important, as highlighted in the first two controls in the SANS 20 Controls Model. The difficulty is no single technology will provide the comprehensive inventory a company needs in order to best protect and assess risk in the enterprise. The unique inventory capabilities of DI PROTECT™ complement the inventory capabilities of OT IDS systems.

1.1 Inventory with OT IDS Systems

The OT IDS systems work in a similar way. A Span Port is setup on a switch/router that passively replicates network traffic to the IDS system. The IDS system then parses network packets and compares them to their own proprietary database of vendor products and packet signatures to determine what assets are running on the network.

A client company's inventory can be built up over time as configuration changes are pushed over the network to the end devices, or they can be input manually. Not all devices have a signature so some amount of manual entry may be necessary to achieve a complete inventory.

These OT IDS systems do not provide detailed information about the operating systems and related applications running on Windows-based systems.

1.2 Inventory with Digital Immunity

DI PROTECT™ only allows the running of code verified as good by the client company. This process of identifying and loading good code into the DI PROTECT™ Map Generator then allows DI PROTECT™ to know exactly what system components are on a given Windows-based system. This can be both commercial off-the-shelf software (COTS) or custom developed software.

DI PROTECT™ provides an accurate and detailed understanding of what software is running on a system. This information can then be rolled up by a company to correlate with ICS-CERT and CVE vulnerabilities.

Digital Immunity does not provide information about controllers and their associated cards.

1.3 Inventory Summary

Both IDS and DI PROTECT™ provide valuable and complementary insight into an overall OT inventory.

2.0 DETECTION

The NIST Framework includes Detection as one of the key overall components to an effective cybersecurity defense-in-depth strategy.

The IT department provides various detection capabilities for the enterprise. When it comes to manufacturing, the IT tools and staff are generally less knowledgeable of manufacturing and can create risks, particularly to production, if they take action in this OT space.

Defining a detection strategy for OT can involve several parts:

- Firewall alerts
- Endpoint device alerts
- IDS alerts
- SIEM correlations

2.1 OT Intrusion Detection

The OT IDS systems, when fully operational, include a growing number of known anomalies to trigger alerts. The IDS can also baseline "normal" operations and trigger alerts for abnormal patterns.

The challenge with any detection tool is tuning the signal-to-noise ratio. If too noisy, engineers will start ignoring the alerts. If alerting is too restricted, engineers may not be alerted if something bad is occurring.

One of the misconceptions is that an IDS will provide protection for the OT systems. This can be true as a second step after becoming aware of anomalous activity and someone then takes action to mitigate the risk. The question is, will this action be too late?

2.2 Digital Immunity's Detection

Digital Immunity provides two levels of detection for Windows-based workstations and server systems.

1. **Notify Mode**

   In Notify Mode, any software is allowed to execute.

   It is good to run DI PROTECT™ in notify mode for a period of time to make sure all software necessary to run on an end device is properly configured before locking it down in Terminate Mode.

   An additional use for Notify mode is to setup a Honey Pot. OT software can be running on the device and talking to a controller thus mimicking a production system. In Notify mode if malware is bouncing around the environment and executes on this Honey Pot, then all the rich forensics captured by DI PROTECT™ will be available for forensics investigation.

   The detailed forensics are best viewed within the DI PROTECT™ Control Center console. In addition, syslog information can be sent to a SIEM for correlation.

2. **Terminate Mode**

   Running in Terminate mode provides DI PROTECT™'s amazing prevention against malware/ransomware/zero-days.

   Once in Terminate mode, companies can reassess their patching strategies and limit the emergency patching events seen in the past with malware such as WannaCry, NotPetya, and vulnerabilities including BlueKeep.

   Terminate mode also provides forensics, but since the malware is not allowed to execute, the forensics will be brief. An alert will be triggered and sent to both DI PROTECT™'s Control Center console as well as sending syslog information to a SIEM. It is important to understand, an alert coming from DI PROTECT™ will be a HIGH-FIDELITY alert –- an engineer should take action immediately because this means an attempt was made to run unapproved or malicious foreign code.

3.0 PROTECTION

Protection is what differentiates Digital Immunity.

3.1 IDS Does Not Protect

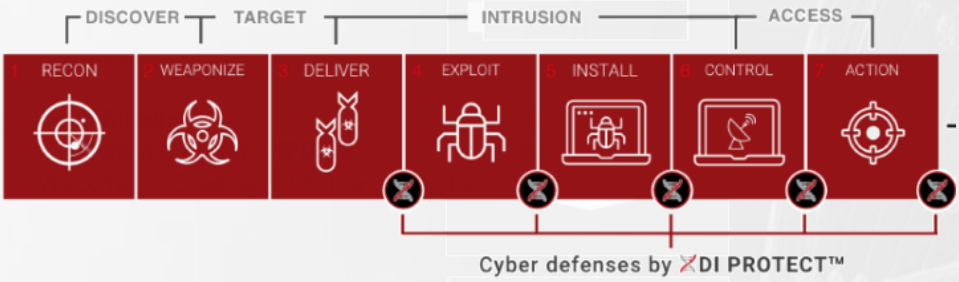
Although an IDS is an important part of a defense-in-depth strategy, the OT IDS systems do not offer inherent protection.

These systems can send alerts of abnormal activity and manual interventions are required to respond and limit the impact, but no automated actions will occur as a result of an IDS installation.

3.2 Digital Immunity Protection

Protecting Windows-based servers and workstations is what DI PROTECT™ is all about. We'll use the Cyber Kill Chain model below to illustrate DI PROTECT™.

At the bottom of the Cyber Kill Chain framework, shown below, an exploit file can be delivered to a server or workstation protected by DI PROTECT™. But an exploit needs to be executed in order to gain access to a system. When the exploit tries to execute, DI PROTECT™ will recognize this unapproved code, in memory at run-time. When in Terminate mode DI PROTECT™ will stop the execution of this unapproved code so a negative event doesn't occur, while allowing the good processes to continue running. DI PROTECT™ provides this level of protection with extremely low latency and CPU utilization.



Graphic: Cyber Security Kill Chain Framework

4.0 USB's

USB's are an important threat vector in an OT/ICS environment. Thus, having the ability to protect a Windows-based device from malicious code emanating from a USB is valuable.

4.1 IDS and USB's

A USB plugged directly into a Windows-based device will not trigger network traffic, Therefore, it will not be seen by the IDS. Only if the USB insertion triggers malicious code and triggers suspicious network traffic will the IDS see the resulting event.

4.2 Digital Immunity and USB's

DI PROTECT™'s sensor, when in Terminate mode, is always checking binary code to verify whether the code has been approved to run.

For USB insertions, if the code trying to execute is foreign then it will not be allowed to run. Controlling execution of files from USB is a great differentiator with DI PROTECT™.

Alerts and forensics will be generated if a USB is inserted and foreign code attempts to run.

5.0 ALERTS

Alerts were discussed in the sections above and this section will offer some additional thoughts on the capabilities of OT IDS systems and DI PROTECT™.

5.1 IDS Alerts

OT IDS systems will have a view of a broader set of assets talking to one another across the network, which can include operator workstations, engineering workstations, HMI's, controllers, and local historians.

In an OT context, systems tend to be stable, talk to the same IP's, and utilize consistent protocols. This stability allows for a level of fingerprinting of normal activity. IDS vendors can then leverage this understanding to look for anomalous activity and trigger alerts.

As these OT IDS alerts are triggered, staff will need to investigate and correlate with other information. A challenge companies are facing is who does the investigation? Many times, IT staff does not have the context and/or access necessary to conduct an investigation into OT assets. While OT staff are generally time-constrained, working to ensure operations are running and process improvements are being implemented. Each organization needs to determine the best process for managing these OT alerts.

5.2 Digital Immunity Alerts

DI PROTECT™'s alerts will come from the Windows-based assets protected by DI PROTECT™ .

When in Terminate mode, an alert triggered by DI PROTECT™ has one meaning: unapproved binary code is trying to run!

A DI PROTECT™ alert, therefore, has a lot of significance! An engineer needs to determine whether:

- The code is good and needs to be run through the DI PROTECT™ process to legitimize running in the future, or
- The code is not good and engineers need to investigate what was trying to run on the system. Did this occur in other systems? What does the forensics data show?

6.0 SUMMARY

For a company's Defense-in-Depth strategy, network segmentation, IDS, Digital Immunity and other technologies are important components to consider and implement.

The value of prevention provided by Digital Immunity is compelling. As the old saying goes "An ounce of prevention is worth a pound of cure". Preventing malware from negatively impacting a Windows-based system, Windows being a primary threat vector, helps significantly reduce the potential impact of malware. In addition, because of Digital Immunity's strong cyber-threat prevention, companies can gain immediate ROI by reassessing their patching strategy, particularly the need for unplanned patching events.

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