DIGITAL IMMUNITY
STAY PRODUCTIVE, STAY SECURE

Securing OT/ICS Beyond the Network Layer

3 Reasons Network Security is NOT Enough to Keep OT/ICS Systems Productive and Secure

According to a March 2019 “Cyber Security in Operational Technology” (OT) report conducted by Ponemon Institute, “cyberattacks are relentless and continuous against OT environments. Most organizations in the OT sector have experienced multiple cyberattacks causing data breaches and/or significant disruption and downtime to business, operations, plants and operational equipment.” In fact, 90% of OT organizations that were represented in Ponemon’s study experienced at least one damaging cyberattack over the past two years.

Unlike the Information Technology (IT) side of the house, OT engineers struggle to improve cybersecurity because they lack enough visibility into OT systems and applications and have a limited view of areas of risk and where they are vulnerable to attack. Operational Technology and Industrial Control System (ICS) environments are very different from IT environments in several ways: system performance requirements, reliability requirements, types of operating systems and applications, risk management goals, network and security architectures, and overall security goals. OT’s primary focus has traditionally been uptime and production, not security. As a result of the growing threat, however, C-level executives are now very involved in understanding and addressing cyber risk and driving security initiatives into the OT environment. In addition, there is a clear trend in the convergence of OT/IT environments.

In an attempt to gain visibility across OT environments, companies including manufacturers are implementing network-based solutions that, through traffic monitoring and behavioral anomaly detection, alert OT engineers to indicators of compromise (IoC) and possibly malicious activity. These tools also give visibility into the systems that are connected to the plant network, but lack visibility in to operating systems and related applications. While network monitoring is an important component of a Defense-in-Depth strategy (DIDS), network-based security is not enough to keep OT and ICS systems productive and secure, lacking prevention capabilities against cyber-attacks on critical systems, a very important component of your DIDS. Here are three reasons why.

1. Hardware-based Security Can be Cost Prohibitive

Most manufacturing networks have been running for many years and have evolved slowly from flat architectures to more segmented architectures; as part of a defense-in-depth strategy. Implementing security network zones and segments via firewalls can reduce network attack surface and increase the time to infiltrate a network, but segmentation alone cannot prevent cyber-attacks from occurring against operating systems and related applications.

In order to protect critical systems, some companies have decided to put a firewall in front of each critical system. While this architecture may provide an additional layer of security, it comes at great cost. This could involve the deployment of thousands of firewalls, requiring hardware costs, configuration and implementation resource costs and downtime costs for implementation. The addition of so many pieces of hardware could require additional full-time resources to manage and maintain the devices, monitor and analyze traffic and ensure uptime of the critical systems these firewalls were protecting. The total costs can be high with only a moderate increase in threat protection.

On top of firewalls, many manufacturers are turning to IDS solutions that monitor network traffic and look for suspicious or malicious activity. These systems monitor the behavior of a network, looking for anomalies that can be suspicious traffic. Unfortunately, these tools alone have numerous shortcomings:

- First and foremost, they will not Prevent the execution of malware attacks on your endpoints which is the ultimate target
- They do not provide needed visibility into your operating systems and related applications which must be manage and protected. If you don't know what's in your environment, you cannot defend and protect it.
- They lack forensic artifacts in context required to analyze potential malware attacks
- They require experienced security engineers to configure and administer them. Experienced security engineers are in short supply and can be costly to procure. According to Ponemon, only 39% of OT organizations surveyed had adequate staffing in their security function to scan vulnerabilities in a timely manner.

- An IDS is only as good as its signature library. They require constant updates to be effective and systems are vulnerable until updates are applied.
- They create frequent false positives, creating resource strain and churn. In fact, false positives are more frequent than actual threats. Engineers must spend time investigating them to ensure that real attacks can't slip through the cracks.
- IP packets can be spoofed, rendering IDS solutions ineffective, making the threat more difficult to detect and assess.
- They are susceptible to protocol attacks, which can crash the device itself.

Network-level security is an important layer in a defense-in-depth strategy, but can be expensive and, by itself, cannot provide complete protection and prevention required to keep OT systems productive and secure.

2. Intrusion Detection is Too Late

Intrusion Detection Systems (IDS) contain all the tools to identify assets, detect threats and alert engineers to suspicious or malicious activity on the network so that they can respond accordingly. IDS solutions have become an integral part of OT cybersecurity because they increase visibility into systems and network traffic in an unobtrusive way that does not impact production. Unfortunately, IDS alerting can be too late to stop an attack from happening or stop it from proliferating across critical OT systems.

IDS solutions deployed in OT are passive monitoring solutions; detecting and alerting engineers as opposed to taking preventive action. As a result, an IDS-based approach to defense has limited value in forward-leaning, hunting-oriented defense, and is of almost no value whatsoever in catching 'new' intrusions not previously observed.

While IDS solutions are an important part of a defense-in-depth strategy, the alerting they provide are often too late, as quite often the attacks that are reported have already occurred. You're in reactive mode rather than proactive prevention mode. As we've seen in recent attacks, proliferation of malware can happen very quickly, meaning that by the time you are alerted to the presence of malware, it's too late. It's like having a laser radar detector in your car. While it will alert you to the presence of a radar detector, you may have, unfortunately, already been caught speeding. The alert means you should pull over, not slow down!

3. Malware Proliferation Happens Faster Than You Can Respond

The volume of malware continues to grow and become more sophisticated in nature with file-less attacks launched in memory becoming more popular, and attacks are more targeted, persistent, and complex. Depending on the nature of the attack, the speed with which malware can proliferate across an environment far exceeds the alerting capability of passive monitoring systems and, in many cases, it appears as valid traffic between systems. APT's may be lurking on your network for months without being detected by IDS solutions. Zero-day attacks are real and increasing. Phishing and spear-phishing are still primary attack vectors used by hackers to gain a foothold into an environment. From there, hackers move laterally from system to system, stealing credentials and data, ultimately gaining administrative credentials and access to vital systems and proprietary data.

This lateral movement can happen in minutes. In the case of the Moller-Maersk attack in June of 2017, the NotPetya malware that began its attack that morning spread so quickly that by mid-afternoon employees were told to go home with no idea when they would return. One IT administrator whose PC screen had just gone black looked up to see "a wave of screens turning black."

Today's malware is designed to fly under the radar, using techniques that are not blocked because they use tools built into Microsoft Windows platforms. These tools extract credentials from memory and when administrator credentials are compromised, the speed of proliferation increases. File-less malware sneaks in without using traditional executable files as a first level of attack.

Rather than using malicious software or downloads of executable files as the primary entry point onto corporate networks, file-less malware often hides in memory or other difficult-to-detect locations. From there, it is written directly to RAM rather than to disk to execute a series of events or is coupled with other attack vectors such as ransomware to accomplish its malicious intent. Traditional anti-virus tools can't detect file-less attacks, or by definition, zero-days, and recent ransomware has been designed to make sure that the signature does not get detected by anti-virus tools.

In a manufacturing company, the target is often the OT environment. In the case of the Triton malware that targeted safety systems in critical infrastructure organizations, the hacker was able to gain a foothold in the corporate network and use that to gain access to the OT environment.

How to Keep OT/ICS Systems Productive and Secure

A true Defense-in-Depth strategy consists of multiple layers of security controls that include technical, physical and administrative controls. Process and procedure are equally as important as the tools that are used for monitoring and enforcement.

Where cyber-security is concerned, layers and controls are important to protect critical digital assets and resources. Monitoring and alerting on suspicious network activity is a vital component of a layer security strategy, but they do not provide the proactive cyber-attack prevention needed in OT. Malware, as we've discussed, attacks at the system level, and moves from system to system using valid tools and traffic patterns. Malware that cannot execute cannot spread, cannot steal data and cannot impact system performance. Malware must be prevented from executing at the system level, with no load or latency, to provide real risk reduction.

What if you could implement real cyber-threat prevention on all critical OT workstations and servers, eliminating the need for costly emergency security patching, allowing you to patch after you test and analyze on your timetable?

What if you could implement real cyber-threat prevention on all critical legacy OT workstations and servers ensuring they are protected regardless of security patch level, with no impact to system resources or production, no load or latency, maintaining uptime and keeping you productive?

What if you could implement real cyber-threat prevention on all critical OT workstations and servers that reduced night, weekend and holiday resource churn, reducing resource costs and improving employee morale?

What if you could have a local security control center allowing you to proactively manage risk, enable the appropriate security polices based on risk, provide forensic, reporting and audit capabilities?

Now you can! DI PROTECT™ is the only OT cyber-threat prevention solution that CONVERGES security and productivity!

Digital Immunity's patented approach to protecting Windows-based operating systems and related applications, provides OT engineers with an option that, before now, was not available: the full-scale immunization of a workstation or server that will prevent the execution of file-based and file-less malware attacks without disrupting trusted processes from executing. In addition, and perhaps equally important, Digital Immunity has architected the solution to use nominal resources on OT devices. This is critical to maintaining the performance objectives of a production operation.

Digital Immunity PROTECT™ is different because Zero Days and known vulnerabilities will be rendered ineffective in taking control of the Windows server or workstation, including devices such as HMI, MES, Data Historian, SCADA and other servers. This is accomplished by what we call Digital DNA Mapping. DI PROTECT™ will map the operation of an OS and related Applications verifying the integrity of execution code in memory, at runtime. This is far superior to whitelisting approaches employed by other vendors such as file identification and hashing. DI PROTECT™ maps at a deeper level, hardening the OS and related applications, and thus recognizes and prevents an attempted deviation to the normal state and blocks this action. It will prevent against tampering of trusted code or the introduction of foreign or malicious code.

This is the Digital Immunity difference: full protection regardless of security patch level, and a device sensor that is so light your systems can continue to perform at a high-level. The ability to be protected between patch cycles is invaluable. You no longer need to worry about the 'emergency' patch cycle, and you can run systems securely and patch in your own timeline, during scheduled downtime.

Now you can implement robust threat prevention that:

- Protects critical devices with a lightweight Sensor that runs in the kernel and requires less than 1% CPU utilization on critical systems without the need for system rebooting or downtime,
- Protects against file, file-less, known and unknown threats in memory, at run-time when applications are most vulnerable without pre-existing threat or vulnerability knowledge,
- Complete visibility into operating systems and related applications

- Requires no signature updates, behavioral/AI algorithms, or external connections,
- Prevents zero-day attacks,
- Provides deep forensic data in context for Incident Response, and
- Centralizes operational control through an intuitive console that gives you complete visibility across your OT and IT environment.

Now you don't have to sacrifice security on the altar of productivity. Contact Digital Immunity today to see how we can help you Stay Productive, Stay Secure!

Digital Immunity: Stay Productive, Stay Secure!

About Digital Immunity

Digital Immunity, Inc., 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. 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 DI PROTECT™, our flagship solution. DI PROTECT™ will also capture forensic artifacts in context and present them in the DI Control Center for further analysis.

For more information, visit **http://www.digitalimmunity.com**.