How a Major Manufacturer is Fighting a New Wave of Cyberattacks

See how the company worked with a cybersecurity provider to develop an AI-driven defense system that met its needs for a major upgrade in protection.

FROM ARIA CYBERSECURITY SOLUTIONS

Keeping production lines running is the lifeblood of any manufacturing company. Disruption and unplanned downtime can lead to millions of dollars in revenue loss. Unlike in the IT environment, operational technology (OT) that controls production lines is expected to run for prolonged periods — often for several months — without maintenance shutdown windows. And devices aren't allowed access to the Internet for continuous updating.

In addition, OT devices often are in place for the production line's entire lifespan, running on legacy operating systems that can be decades old, thus allowing the manufacturer to sustain profitability and production targets.

Prior Mode of Operation (PMO): Production Protection

The manufacturer's PMO included these protections of their OT infrastructure: human-machine interface (HMI) devices, Engineering WorkStations (EWS) and data historians. It focused on creating

1339236035 ©CHIM / SHUTTERSTOCK.COM

limited access to where critical production applications run and are therefore most vulnerable, including:

- Passive network security focused on limiting corporate and Internet access to and from the plant floor to make it less accessible to attacks.
- Legacy signature-based antivirus (AV) systems, challenged by limited updates to annual maintenance windows and their lack of ability to stop modern polymorphic malware, which gets past signature detection.
- Vendors and contract services providers use of the Internet to get access during scheduled maintenance windows via virtual private network.
- Vendors and contract services asked to use AV-protected maintenance laptops to provide device application updates and troubleshooting during these windows.

- **Limited staff — typically one person — at a plant responsible for keeping the devices and applications working, providing asset management, reporting, and overseeing data security, and often responsible for multiple regional plants.**
- **Limited time for staff to learn and operate advanced security measures, and no time to continuously monitor and fine-tune cybersecurity tools.**

User's Challenges & Requirements

The PMO didn't meet the customer's requirements for protecting it from increasingly sophisticated attacks, including those that get through via the supply chain. The company identified these *new* requirements:

- **HMIs, EWSs, historians and other devices require their OS platform and applications to be protected from all forms of ransomware and malware, supply-chain attacks, and sophisticated breaches (such as an advanced persistent threat, or APT), under the following constraints:**
  - » Replace legacy, ineffective signature-based antivirus agents that don't detect today's malware.
  - » Do so without Internet-connected AV or Indicator of Compromise (IOC) updates or application patches.
  - » Be able to work fully air-gapped for up to a year and retain efficacy of protection.
  - » Stop all attacks automatically without human involvement, before production is impacted.
  - » Be able to lock down certain devices so no unapproved application nor existing application updates will run until approved.
  - » Run on a variety of platforms, from current Windows server/Windows desktop OS, back to Windows XP SP2.
  - » Provide reports to help verify insurance policy and U.S. Securities Exchange Commission (SEC) rule compliance.

- **Environment-related requirements:**
  - » Deploy factory-wide, coming up fully protected within a four-hour window for all site devices.
  - » Be simple to deploy and operate with no need for formal training due to limited time for onboarding.
  - » For IT, the ability to automatically export the appropriate reports for compliance purposes, and securely send forensic syslog information formatted for the IT organization's security information and event management (SIEM).

Selecting the Solution to Meet Requirements

A number of solutions were analyzed for their ability to meet these requirements. Some solutions that were considered lock down systems to assure only approved applications run, but they only run at the time the OS or the applications are started or restarted. They don't provide protection from attacks to the approved applications while they are running.

To counter this, the vendor recommended continuous patching to mitigate application vulnerabilities. However, this technique requires rebooting the production environment continuously.

The Application Allow Listing didn't stop fileless malware nor sophisticated attacks by the contracted Red Team, a group of people authorized by the user to pretend to be cyberattackers to expose vulnerabilities.

In addition, some solutions proved difficult to run out-of-the-gate and had to be tuned by skilled, trained staff to allow the applications to continue to run with every patch update, or when rarely run

1332808136 ©CHIM / SHUTTERSTOCK.COM

The upgraded solution continuously monitors how applications execute in memory, to provide continuous protection from any form of attempted adulteration to the running applications.

applications were activated for the first time.

Next-Generation Antivirus

The IT side of the organization used the industry's leading next-generation antivirus (NGAV) and endpoint detection and response (EDR) solutions, and proposed these be deployed for the OT organization.

Instead of relying on signatures, these solutions use known patterns of attacks (IOCs) that have been seen before in other customer environments.

However, the challenge for the OT organization was that the solution required the OT devices to be continuously connected to the Internet for monitoring and to receive updates from the vendor's cloud.

Also, updates could be queued and tested on lab devices, but couldn't be loaded to production devices until the annual maintenance window. And, the solutions didn't run on the older windows OS, which would leave critical devices unprotected.

The Red Team could use standard techniques to bypass the protections, similar to those techniques used in the SolarWinds and other supply chain attacks.

Artificial Intelligence-Driven Defense

The manufacturer then analyzed and decided to use a comprehensive AI-driven defense system designed to protect all OT endpoints from all cybersecurity threats. This solution, AZT PROTECT from Rockwell Automation Technology Partner ARIA Cybersecurity, can lock down applications and the OS, preventing malware and ransomware from running.

It also continuously monitors how applications execute in memory, to provide continuous protection from any form of attempted adulteration to the running applications. In addition, it provides additional measures that stop the common techniques used by sophisticated attacks, including misuse of OS processes, shellcode, injections and privilege escalations.

The combination was intended to stop sophisticated attacks, such as those coming in via supply chains, that commonly have access to OT environments.

Results

The AI-driven defense system met the manufacturer's requirements with positive results. The solution was able to learn the applications on the device and prevent new unapproved applications from running — out of the box. It blocked all ransomware and malware, including fileless malware attacks launched by the Red Team. It also defended against the Red Team attempts to misuse OS processes, shellcode, injections and privilege escalations as seen in sophisticated supply-chain attacks.

It prevented code adulteration attacks on the applications with unpatched vulnerabilities while running. The solution defended all attacks while being fully air gapped, and it didn't need updates to stop new attacks.

The cyber defense system supported all legacy operating systems and didn't negatively affect production application performance.

And, it provided reporting required for SEC and other compliance in addition to exporting syslog formatted alert data into IT's SIEM for further analysis.

Additional benefits included:

- **A complete inventory of all applications and versions running and their status on each device and in each device group.**
- **Stopping unknown vulnerabilities — such as the Pool Party novel process thread attacks discovered in December of 2023.**
- **The ability to be loaded on running devices without reboot.**
- **Ease of use for OT staff to deploy and operate with minimal training.** ●

ARIA CYBERSECURITY SOLUTIONS

ARIA Cybersecurity Solutions, based in Lowell, Massachusetts, is a Rockwell Automation Technology Partner that offers complete network and data security solutions. Its ARIA Zero Trust PROTECT (AZT PROTECT™) AI-driven defense system is designed to protect OT endpoints from all cybersecurity threats.