Stairwell for OT & Manufacturing

OT & manufacturing environments are being targeted

It is a fact that attackers continue to identify weaknesses that they can exploit for their own financial gain or to cause as much disruption as possible to a targeted organization's operations. This fact has taken on a new sense of urgency as more than half of industrial firms (54%) have suffered a ransomware attack that has impacted their operational technology, whether directly or because a linked IT system had been attacked.

These figures prove organizations across numerous sectors are now under pressure to detect the latest threats on systems and within environments often unsupported by traditional security tools. This is because attackers are gaining access to OT environments where they target Industrial Control Systems (ICS) or Supervisory Control and Data Acquisition (SCADA) systems, so they can cause the greatest amount of disruption.

How Stairwell helps manufacturing & processing organizations:

- **OT Support:** Rapidly deploy within operation based environments and identify unknown threats and variants that EDR misses
- **Proactive Deployment:** Deploy advanced analysis, even on systems not covered by other security tools
- **Automation:** Streamline manual processes via automation, such as automated threat intelligence and prebuilt YARA queries for vulnerability identification at 10x the speed
- **Fast Detection:** Identify exposed assets within seconds of an IOC / exploit notification
- **Comprehensive Assessment:** Facilitate quick and comprehensive reviews, allowing timely responses to management/regulators without retention concerns for a threat or 3rd party vulnerability

Minimize disruption: before and during production

The attacks pointed at manufacturing and operations-based organizations are different from those directed at retailers, financial services, or healthcare providers as they rely on types of systems that are not easily monitored. Attackers are targeting production by gaining unauthorized access to the network the OT systems reside on and leveraging vulnerabilities to exploit them.

Stairwell for OT & Manufacturing

Stairwell helps manufacturing and OT-based organizations ensure their operational systems are safe from attacks, protecting their production lines from being disrupted or altogether stopped. With near real-time analysis, security teams can provide a clean bill of health before production begins as well as on a continuous basis, ensuring production is not disrupted.

The latest malware or 3rd-party vulnerability - Am I impacted?

Stairwell is able to swiftly identify emerging threats and active exploits, often before the security/IT team is aware of a potential exposure within their organization. Our manufacturing clients leverage Stairwell to make sure their operation systems are safe and in the "clear" before kicking off their production lines.

Within minutes, Stairwell is able to conduct a comprehensive environment assessment – a task that traditionally consumes days or even weeks through manual audits, enabling our operations-based customers to respond promptly to management and regulators regarding third-party vulnerabilities like the Log4j exploit, showcasing a rapid and effective security posture.

Continuous analysis - finding unknowns and variants

What might be known today was not known yesterday, a week ago, or even months ago. Stairwell is able to continuously and automatically analyze every executable or executable-like file at the binary level for every file that has ever been ingested since becoming a customer, as there are no retention limits.

Stairwell automatically identifies malware files and their variants within manufacturing-based organizations that were previously not identified as malicious based on the latest threat intelligence received. The security team is able to know exactly which file is malicious, where it was located, and provide detailed analysis of the malware identified, allowing both the security and operations teams to assess risk and respond accordingly.

Summary

Stairwell understands manufacturing and OT based organizations need to take extra measures to ensure their operations are safe and not impacted by the latest threats targeting their unique applications and systems. Stairwell is here to help our customers take immediate action against threats or exploits and is switching up the game by taking a whole new approach to detecting threats missed by others. If you would like to learn more, please reach out, as we'd be more than happy to have a chat and discuss how Stairwell can help protect your organization from the latest threats.