POINT OF VIEW

Use Cyberdeception To Lure Attackers From Critical Assets

Proactive Cybersecurity for Operational Technology

Executive Summary

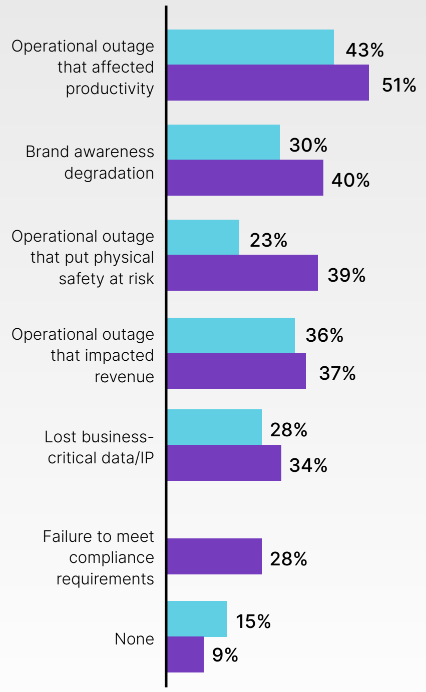
Today, many operational technology (OT) leaders are struggling with business resilience and the reality that security must be embedded within their environment and operational processes. But many security solutions don't make sense in an OT environment, which has significant challenges that aren't found in a typical information technology (IT) environment. Deception technology is a passive network-based security solution that lures attackers to decoy devices that appear indistinguishable from real IT and OT assets. Deception is an effective tool in the security arsenal that offers a compelling advantage for OT because it can be deployed without the need to rearchitect or change OT systems at all.

The Challenges Involved in Protecting OT Environments

With the convergence of OT and IT networks, security threats against industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems have increased for a number of reasons. In fact, as more OT networks transition away from closed environments, the number of intrusions has increased by around 20% since 2019.[2]

In the past, most OT solutions were protected because they were air gapped from the corporate IT and public networks. Even though industrial sensors used Internet Protocol (IP) networks to communicate, threat actors were more focused on the IT infrastructure, where they could get a bigger and faster return on their investment in malware. Going after a basic sensor deployed in an OT network was extra work with little return. And ransomware, which is now used by attackers to hold critical OT systems and Internet-of-Things (IoT) devices for ransom, primarily targeted end-user devices for years. In fact, there was still little interest in targeting SCADA or ICS systems until Stuxnet hit in 2010.

The Impact of System Intrusions[1]



Because OT sensor and early IoT device functionality was so simple, there was little to exploit. Protecting the devices primarily involved air gapping the OT environment from the internet and putting a firewall in front of the OT network to block IT. Today however, basic sensors have evolved into "smart sensors," which provide a wider variety of capabilities. IoT devices or Industrial IoT (IIoT) in some environments have also become more sophisticated. At the same time, IT and OT networks and devices converged to generate more efficiencies in asset utilization and to facilitate the move from calendar-based maintenance to condition-based maintenance. These changes have made the OT attack surface significantly more complicated to protect.

OT leaders are increasingly tasked with evaluating cybersecurity solutions as OT networks become more and more challenging to protect. In many cases, remote access is now the norm for third-party vendor visibility, operational efficiency, and troubleshooting. Because of the pandemic, remote access has been required for internal employees as well.

OT Is Different Than IT

Because they operate on a much longer update and replacement cycle than IT systems do, OT systems are more vulnerable than IT systems. Many OT leaders are concerned about security and maintaining business resiliency because an operational outage can affect productivity, revenue, and brand perception. OT intrusions may include malware, phishing, hacking, and ransomware from either external or internal bad actors. The theft of critical data can lead to lost business and the failure to meet compliance requirements. Even worse, depending on the system, a breach could even risk physical safety. Suppose a bad actor disabled the cooling stations in a nuclear power plant, for example.

One of the biggest issues facing OT leaders is that many security solutions are designed for IT, but few are applicable for OT. A suitable security solution for OT needs to be able to work with legacy systems, including ones that can no longer be patched. The solution needs to have no impact on critical production environments, and of course, it needs to be effective in defending against attacks.

Exposing Cyber Crime Using Deception Technology

It's clear that a proactive security approach is essential to address the threats facing OT systems, and deception technology is gaining traction and support. Analysts such as Gartner are recommending using deception tools within OT networks, and MITRE has endorsed this type of approach as well.

Deception technology is a method of uncovering the bad actors and their tactics by redirecting both external and internal threats away from critical assets. The theory behind deception technology is simple: It mines a network with trip-wired decoys disguised as data assets that alert an organization when they have been accessed. Deception technology lures criminals away from actual valuable data, while exposing their presence—often without their knowledge, which allows security professionals to engage in forensic analysis in real time by closely monitoring patterns, activities, and techniques to discover breached devices and exploited vulnerabilities.

With deception technology, the IT/OT team can deploy these virtual fake assets over the infrastructure, which then emulate IT devices and OT control system elements. This decoy network tricks malicious actors, luring them away from critical assets. More importantly, since all of the organization's legitimate devices and workflows recognize that these assets are a decoy, only unauthorized users, devices, and applications will trigger them. In this respect, deception provides clear, unambiguous detection of an impending threat, which means it generates high-fidelity alerts and a low number of false positives when compared to other security solutions.

Protect Against External and Internal Threats

Deception techniques don't just protect against outside attacks; they are also powerful tools for discovering internal threats. If rogue employees start poking around a network for information they are not authorized to access, deception technology is one of the most effective ways to catch them. Next-generation deception differs from detection-based honeypots because it also includes tools such as threat analytics, as well as integration with security controls, to proactively block attacks before any real damage can be inflicted.

Deception solutions provide valuable intelligence because they determine how attackers got in, their objectives, and the tools they used. Although deception is a passive security solution, it is a valuable tool for converged IT and OT environments that improves security posture by targeting the source of these attacks.

Slowing Down Attacks

Whether they're looking for profit or trying to make a political statement, cyber criminals are always looking for accessible targets. They recognize that the convergence of IT and OT networks typically can reveal attack surface gaps they can use to accomplish their goals.

By creating decoys that are dispersed throughout the environment, deception technology can slow down attacks. If attackers are unable to determine which assets are fake and which are real, their time advantage is reduced or eliminated altogether. Cyber criminals are forced to waste time on fake assets while inadvertently tipping off a security administrator to their presence. Even if they become aware of the deception, attackers need to exercise caution, and in some cases, they may consider retreating to avoid risking further exposure.

Deceive, Expose, and Eliminate Cyber Crime

Integrating deception technology into the security stack allows OT organizations to be more proactive and use attackers' techniques and tactics against them. The best deception technologies not only protect against advanced IT-based threats but they also are able to detect, analyze, and defend against advanced OT/IoT attacks. Deception technology enables a more proactive security posture by deceiving the attackers, exposing their actions, and then eliminating these threats with appropriate threat mitigation and response, so the enterprise can return to normal operations.

73% of attacks launched against the manufacturing sector were motivated by financial reasons, with the balance involving espionage. Additionally, Verizon found that 75% of attacks involved external forces, while internal threats accounted for the remainder.[3]

[1] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, June 30, 2020.

[2] Ibid.

[3] "2020 Data Breach Investigations Report," Verizon, May 2020.

www.fortinet.com

April 28, 2021 6:27 AM

D:\Fortinet\2021 Rebranded templates\POV\April\FortiDeceptor OT\pov-FA-fortideceptor-ot-4282021\pov-FA-fortideceptor-ot-4282021

979401-0-0-EN