SOLUTION BRIEF

Operational Technology Cybersecurity Assurance With FortiDeceptor

Executive Summary

Industrial facility operational technology (OT) leaders reported a 20% increase in system intrusions from the previous year as network environments continue to transition away from closed to open systems.[1] This process led to the creation of a new threat vector for cyberattacks. Unfortunately, many of these organizations are ill-equipped to secure legacy supervisory control and data acquisition (SCADA) and industrial control system (ICS) devices found in the OT environment. The problems often relate to incompatible IT security controls and the complexity involved in building a holistic security infrastructure that encompasses both OT and IT environments.

FortiDeceptor provides simple-to-use, unintrusive, network-based early detection of threats that target OT and IT environments. Through the deployment of decoys and honeytokens, FortiDeceptor automates the containment of cyberattacks before serious damage occurs.

> *"Many, if not most, OT environments are like islands that have been isolated for eons. Interconnecting with an IT network opens up OT to the predatory world of cyberattacks and malware for which it is unprepared."*
>
> – Joe Robertson, "Securing Operational Technology in a Dynamic Landscape," Fortinet[2]

More OT Environments Are Vulnerable

As OT network environments are increasingly integrated with IT environments for external access, OT systems are more vulnerable to the types of intrusions typically found in IT (see Figure 1). Examples include:

- IT threats that have been recycled to target OT environments, such as EKANS ransomware
- Threats that specifically target OT, such as Stuxnet
- Attacks that can laterally move from IT networks to OT and vice versa
- Zero-day threats that target legacy OT systems that can't be patched

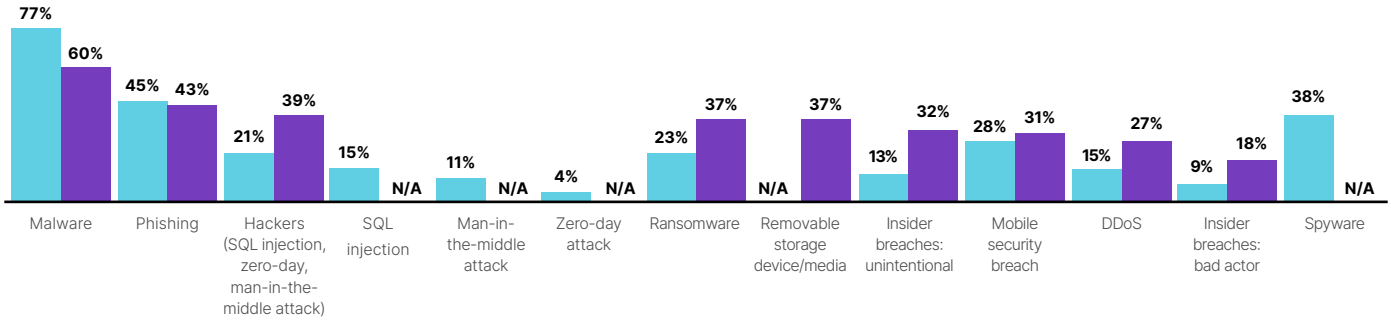

Figure 1: Types of intrusions reported.[3]

Organizations that design and build an OT infrastructure without considering cybersecurity will need to implement security controls later. They may need to mitigate production disruption from cyberattacks and comply with newer industry regulations to minimize noncompliance penalties. However, security adoption can be a difficult task because of legacy systems, downtime associated with security implementation, and a complex disjointed security approach with one approach for IT and another for OT.

Organizations could consider applying their IT-based security solutions for OT, but unfortunately, these solutions were not designed with OT systems in mind. Here are a few examples that showcase the problem:

- The latest antivirus software products are usually not compatible with legacy systems because of a lack of operating system (OS) support or a failure to meet the minimum hardware requirements.
- A typical firewall can detect threats within IT-based services and applications but isn't able to decode OT communications such as OPC, BACnet, and Modbus.
- Typical intrusion detection or prevention systems protect IT-based application vulnerabilities but not OT-based vulnerabilities.
- Most external threat feeds are applicable for IT but not OT.

Around 50% of FortiDeceptor deployments are in OT sectors such as energy and utilities, transportation, logistics, and several manufacturing sectors including chemical, food and beverage, automotive, aerospace, and defense.

Simulate Network Assets

Unlike other security solutions that require infrastructure changes or the need to take operations offline to implement cybersecurity, FortiDeceptor is easy to use and not intrusive. To lure threat actors away from critical assets, it creates a fake environment that simulates the network and assets. FortiDeceptor generates an early warning of an impending attack, so an automated response can protect both IT and OT segments.

In addition, FortiDeceptor automatically discovers network and assets in the environment and recommends appropriate decoys. Users can also centrally manage a distributed FortiDeceptor deployment from the primary node.

FortiDeceptor eliminates the need to take SCADA/ICS offline to install an agent. It creates a fake environment that simulates the actual environment. It uncovers threats using the concept of honeypots. As it passively monitors for activity across its network of decoys and honeytokens, FortiDeceptor doesn't cause delays.

In the first stage of the Cyber Kill Chain, it is typical for a threat actor to perform a reconnaissance to understand the environment and identify assets of interest before launching a full campaign.[4] Because the fake FortiDeceptor environment is indistinguishable from the real one, any interaction with the decoys during the reconnaissance phase will raise an immediate alert. These alerts are unambiguous because employees only interact with the real environment. FortiDeceptor also captures the tactics of threat actors, which can reveal how they entered the environment, their objectives, and the tools they used.

Threat Response Options That Protect OT and IT

FortiDeceptor correlates every action of the threat actor into a campaign timeline with contextual intelligence of their tactics, techniques, and procedures (TTPs), which provides options to mitigate a newly discovered threat. Organizations that have a large security operations center (SOC) may prefer to use deception to engage with threat actors so the activities can be studied. Then once the investigation is complete, the necessary mitigation and response can be performed. Other organizations may prefer to integrate deception into their automation framework supporting threat response and/or threat hunting.

Because FortiDeceptor is part of the Fortinet Security Fabric, it supports seamless integration with the following Fortinet products:

- **FortiGate** next-generation firewall (NGFW) integration enables instant quarantine, triggered by FortiDeceptor alerts of infected assets. In addition, deception decoys are visible through the network's physical and logical (decoys' network location) topology map.
- **FortiNAC** integration enables automated infected asset isolation (e.g., IoTs, third-party devices) based on FortiDeceptor threat detection alerts.
- **FortiSOAR** integration enriches playbooks with real-time threat intelligence data and enables automated incident response, triggered by FortiDeceptor alerts, to help accelerate time to resolution.
- **FortiSIEM** integration facilitates effective incident response processes by feeding the SIEM with high-fidelity alerts and threat intelligence data.
- **FortiAnalyzer** integration helps SOC analysts to identify and respond to evidence of attack activities shared by FortiDeceptor.
- **FortiSandbox** integration provides a complete static and dynamic analysis against malicious code captured by FortiDeceptor decoys. Analysis reports are available on the FortiDeceptor admin console.
- **FortiEDR** integration enables instant isolation of infected endpoints from the network based on FortiDeceptor's detection of suspicious activity.

FortiDeceptor also integrates with third-party security solutions via the Fortinet Security Fabric Connector.

It offers expansive SCADA/ICS support, including Rockwell Ethernet/IP, Siemens S7, and others. It also broadly covers the IT segment of an organization by simulating Windows and Linux clients and servers. Besides the devices themselves, deception supports various applications and services, such as Git repositories, virtual private networks (VPNs), Server Message Block (SMB), Structured Query Language (SQL), and others.

Organizations with mature security typically adopt security frameworks such as NIST or MITRE. Industrial facilities looking to modernize their ICS architecture also may consider the Purdue model as a systematic approach to applying security to each zone of the OT network that spans to the IT network. FortiDeceptor applies to the various Purdue zones, including process control, operations and control, and business and enterprise in the Purdue model.

Why Deploy FortiDeceptor?

FortiDeceptor offers three key business benefits: powerful security, broad coverage, and automated protection. It is a powerful addition to an organization's security strategy because it focuses on the source of threats: threat actors. Incorporating deception's early detection and response characteristics as a proactive defense strategy elevates an organization's existing security posture and reduces business disruption from external or internal threats.

Deploying security in an OT environment is complex; however, FortiDeceptor removes that obstacle by being unintrusive and also does not add delay to OT operations before, during, and after its deployment. FortiDeceptor isn't just for OT environments; it works for IT as well, so security operations staff can close gaps with comprehensive coverage of the dynamic attack surface. Most importantly, FortiDeceptor is part of the Fortinet Security Fabric, so it easily integrates with Fortinet and third-party security solutions that enable automated threat response and contextual threat hunting, thus improving efficiencies within SOC processes, and allows SecOps to scale even further.

FortiDeceptor Supported Decoys	
Windows Server Decoys	■ Windows Server 2016 ■ Windows Server 2019
Windows Desktop Decoy	■ Windows 7 ■ Windows 10
Custom Decoy ("golden images") Import your custom OS image for the decoy into FortiDeceptor. Decoys can be cloned and deployed across the environment.	■ Windows Server 2016 ■ Windows Server 2019 ■ Windows Server 10
Windows Services	■ SMB ■ RDP ■ TCP Port Listener ■ SQL Server ■ FTP ■ MSSQL IIS (HTTP/HTTPS) ■ NBNS SpoofSpotter (responder attack) ■ ICMP
Windows Deception Tokens	■ RDP (fake credentials) ■ SAMBA/SMB (fake credentials) ■ Fake Network Connection ■ HoneyDocs (Office & PDF) ■ SQL ODBC ■ Cache Credentials ■ SAP Connector ■ SSH (fake credentials)

FortiDeceptor Supported Decoys (contd.)	
VPN Decoy	■ FortiOS ■ Fortinet SSL-VPN (HTTPS)
Linux Decoy	■ Ubuntu ■ CentOS
Linux Services	■ SSH ■ SAMBA ■ GIT ■ FTP ■ ESXi ■ ELK ■ TCPListener ■ ICMP ■ HTTP/S
Linux Deception Tokens	■ SAMBA ■ SSH
Application Decoys	■ POS-WEB ■ ERP-WEP ■ SAP (Dispatcher, SAP WEB UI and SAP Router)
On-premises/Cloud-base Active Directory Decoys	■ AD domain decoy ■ AD server decoy ■ Fake credentials/Cached credentials
Cloud Decoys	■ AWS ■ Azure ■ GCP
OT/IoT Decoys and Lures	
IoT Decoys	■ Cisco Routers ■ IP Camera ■ Printers (HP, Lexmark, Brother) ■ UPS ■ TPLink Router Modem
IoT Decoy Services	■ Jetdirect ■ UPnP ■ RTSP ■ CDP ■ HTTP/S ■ CWMP ■ SNMP ■ TELNET

OT/IoT Decoys and Lures (contd.)	
OT Decoy Services	■ MODBUS ■ S7COMM ■ BACNET ■ IPMI ■ GUARDIAN-AST ■ IEC 60870-5-104 ■ EtherNet/IP (Rockwell ENIP) ■ DNP3 ■ TRICONEX (Schneider Electric) ■ HTTP ■ FTP ■ TFTP ■ SNMP
Medical IoT Decoys	■ Infusion Pump TELNET, FTP ■ PACS-WEB ■ PACS ■ DICOM server ■ Braun infusomat (HTTP/S, CAN Bus Protocol)

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

[2] Rick Peters, "Looking Back and Forward: Critical Takeaways for Operational Technology Security," Fortinet, December 2, 2020.

[3] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, June 30, 2020.

[4] "The Cyber Kill Chain," Lockheed Martin, accessed April 28, 2021.

FORTINET

www.fortinet.com

June 25, 2022 1:10 AM
988459-0-0-EN