Evaluate Your Industrial Controls Network Risk with the Fortinet Cyber Threat Assessment Program

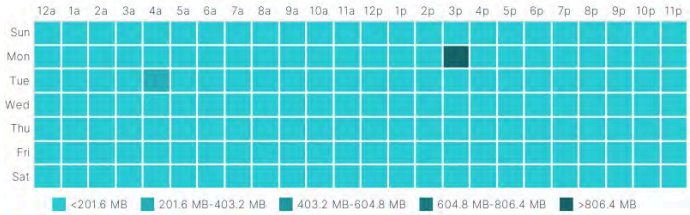
Gauge Current Security, Applications, and Utilization of your Operational Technology (OT) Network

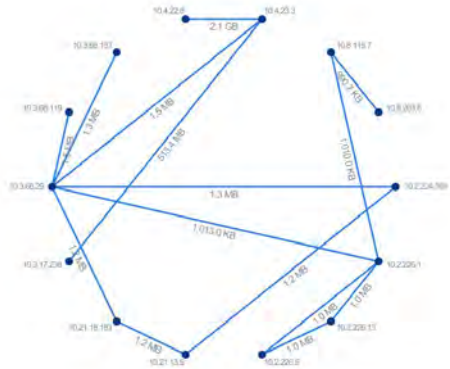
As industrial environments increase connectivity with internet-based corporate networks and adopt Internet of Things (IoT) or industrial IoT (IIoT) technologies, security becomes a critical priority for operational technology (OT). Accurate detection of today's advanced threats and full visibility of the users, data, devices and applications used in OT is a must. If you are concerned about ensuring safe, available and secure operations while protecting the legacy and modern industrial equipment, an OT assessment is a recommended next step.

Validate your OT network's security effectiveness, application flows, and utilization by enlisting expert guidance. A Fortinet expert will use a FortiGate to monitor key indicators within your OT network. After several days of gathering information, you will receive an OT Assessment Report which is divided into three primary sections:

- **Security and Threat Prevention –** How effective is your current network security solution? Learn more about application vulnerabilities are attacking your network, which malware/botnets were detected and even pinpoint "at risk" devices within your network. Make sure your existing security solution isn't letting anything slip through the cracks by leveraging FortiGuard Labs' award-winning content security.
- **OT/IT Application Usage –** What steps are you taking to monitor traffic flows in your network? Improve your visibility to traffic and most used applications within your OT environment. Monitor traffic patterns to identify network anomalies whether accessing on-site or via remote access.
- **Network Utilization and Performance –** How should your network security solution be optimized for performance?Find out more about your throughput, session and bandwidth requirements during peak hours. Ensure your security solution is sized and optimized properly based on your actual usage.

#	Risk	Threat Name	Type	Victims	Sources	Count
1	5	Honeywell.OPOS.Multiple.ActiveX.Open.Method.Buffer.Overflow	Buffer Errors	2	1	5
2	5	Unitronics.VisiLogic.OPLC.TeeCommander.Memory.Corruption	Buffer Errors	1	1	2
3	3	Schneider.Electric.GP-Pro.EX.ParseAPI.Heap.Buffer.Overflow	Buffer Errors	3	1	112
4	2	Siemens.SIMATIC.WinCC.Flexible.Runtime.Stack.Buffer.Overflow	Buffer Errors	1	1	98
5	2	Trihedral.VTScada.WAP.Directory.Traversal	Path Traversal	3	1	14
6	1	Modbus.TCP.Report.Server.Info	Permission/Privilege/Access Control	1	1	12





Obtaining an OT Assessment Report will give you a critical and quantified view into your current industrial security posture. Find out if you qualify for your own assessment today!

Terms and Conditions: All Fortinet Products provided to you under this promotion are subject to Fortinet's End User License Agreement (EULA), located at: http://www.fortinet.com/doc/legal/EULA.pdf.
By using Fortinet Products under this promotion, you acknowledge that you understand the EULA and agree to be bound by the EULA.

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet.