Operational Technology Assessment Report

Prepared For
Informata College

Prepared By
John Smith
Fortinet

Report Date
Aug 31, 2022

Executive Summary

We aggregated key findings from our OT assessment within the Executive Summary below. While the highlights are listed below, a more detailed view of each section follows. Be sure to review the Recommended Actions page at the end of this report for actionable steps your organization can take to protect your OT assets, validate industrial application usage, and identify potentially susceptible OT hosts.

Security

4,172
Application Vulnerability Attacks Detected

3
Malware and/or Botnets Discovered

6
OT Devices Attempting External Connection

Note that any threats observed within this report have potentially bypassed your existing network security controls, so they should be considered active risks until otherwise fully reconciled.

Applications

84
Total OT Applications Detected

8
Remote Access Applications Detected

32.0%
Percentage of OT Traffic

Applications in use within OT environments should be constrained and monitored. Understanding the industrial applications within your network can help define corporate use policies, set access controls on airgapped networks, and minimize unnecessary chatter.

Utilization

2.7GB
Total Bandwidth Used

13
Total OT Devices Detected

364.0MB
Average OT Bandwidth Per Day

Understanding overall utilization on your OT network can help with capacity planning and streamlining network traffic over time.

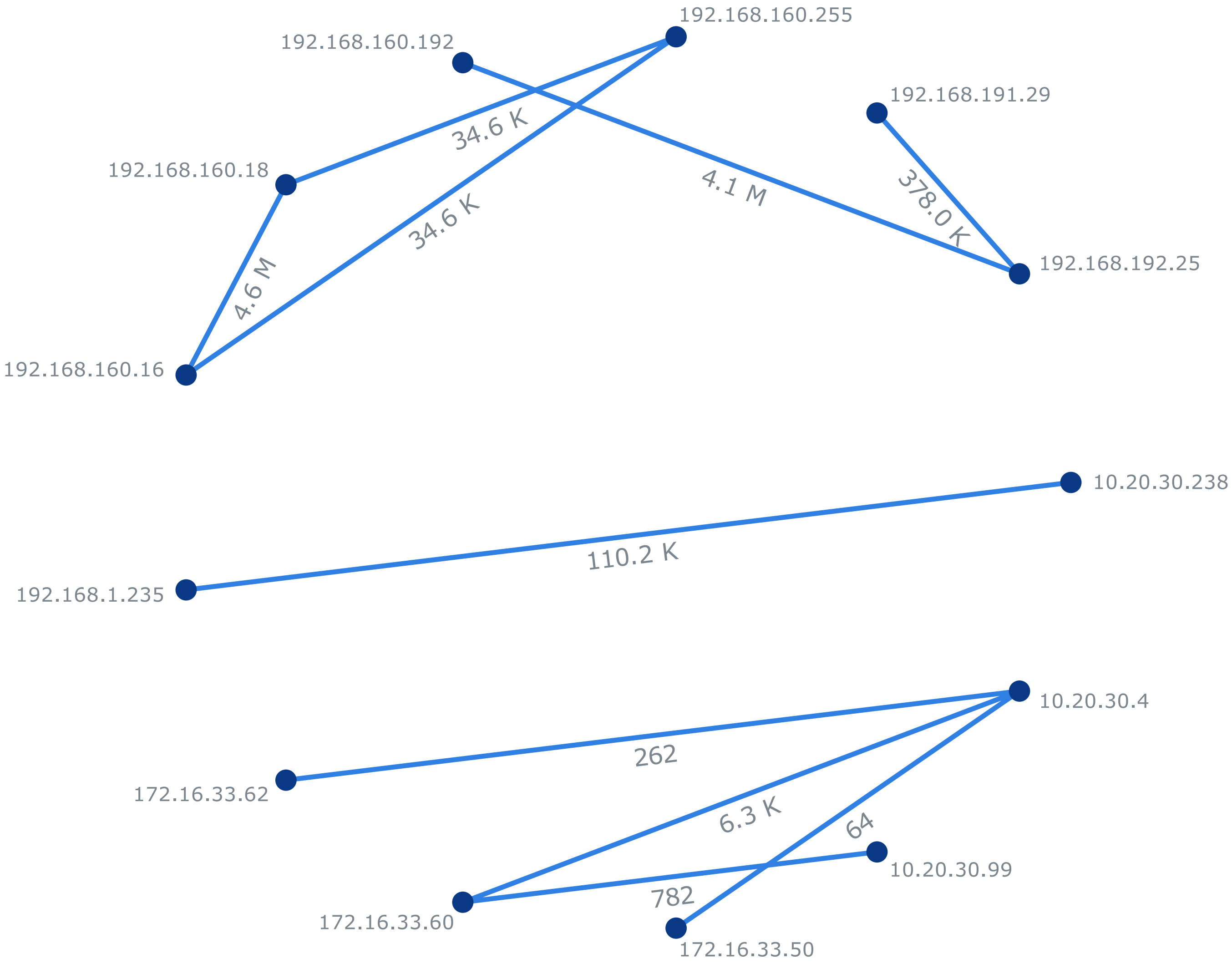
Security

Quick Stats

- **4,172** application vulnerability attacks detected
- **3** malware and/or botnets discovered
- **6** OT devices attempting external connection
- **6** OT application vulnerability attacks detected

Traffic Flows to OT Devices

Mapping out network traffic flows on industrial networks is useful when identifying high bandwidth pathways between hosts and identifying hosts which should not be communicating with each other. In the case of the former, high bandwidth flows could identify compromised hosts which are being used to exfiltrate data. Knowing how specific hosts/IPs on your OT network should be commmunicating can help you identify unknown traffic flows and can help improve network policies.



Top Application Vulnerability Exploits Detected

Application vulnerabilities can be exploited to compromise the security of your network. The FortiGuard research team analyzes these vulnerabilities and then develops signatures to detect them. FortiGuard currently leverages a database of more than 5,800 known application threats to detect attacks that evade traditional firewall systems. For more information on application vulnerabilities, please refer to FortiGuard at: http://www.fortiguard.com/intrusion.

#	Risk	Threat Name	Type	Victims	Sources	Count
1	5	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	38	2	2,493
2	5	MS.GDIPlus.JPEG.Buffer.Overflow	Buffer Errors	3	2	294
3	5	MS.IE.MSXML.Object.Handling.Code.Execution	Buffer Errors	1	1	130
4	5	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Code Execution	1	1	4
5	5	Honeywell.OPOS.Multiple.ActiveX.Open.Method.Buffer.Overflow	Buffer Errors	2	1	5
6	5	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Command Injection	2	1	2
7	5	Unitronics.VisiLogic.OPLC.TeeCommander.Memory.Corruption	Buffer Errors	1	1	2
8	5	IBM.Rational.ClearQuest.Username.Parameter.SQL.Injection	SQL Injection	1	1	1
9	4	LG.Smart.IP.Camera.Unauthenticated.Backup.File.Download	Permission/Privilege/Access Control	2	1	537
10	4	IISadmin.ISM.DLL.Access	Information Disclosure	29	1	169

Top Industrial Application Vulnerabilities Detected

Unless the industrial applications you're using are high volume, they may not appear on the list of top application vunlerabilities. This table helps identify application vulnerabilities that are specific to OT networks by using an enhanced set of industrial signatures. Any vulnerabiities within this table should be addressed immediately as they are known to specifically target your industrial infrastructure.

#	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

Top Malware, Botnets and Spyware/Adware Detected

There are numerous channels that cybercriminals use to distribute malware. Most common methods motivate users to open an infected file in an email attachment, download an infected file, or click on a link leading to a malicious site. During the security assessment, Fortinet identified a number of malware and botnet-related events which indicate malicious file downloads or connections to botnet command and control sites.

#	Malware Name	Type	Application	Victims	Sources	Count
1	Asprox.Botnet	Botnet C&C	Asprox.Botnet	5	1	6
2	W32/NGVCK	Virus	HTTP	1	1	3
3	W32/ForeignRansom.583D!tr	Virus	HTTP	1	1	1

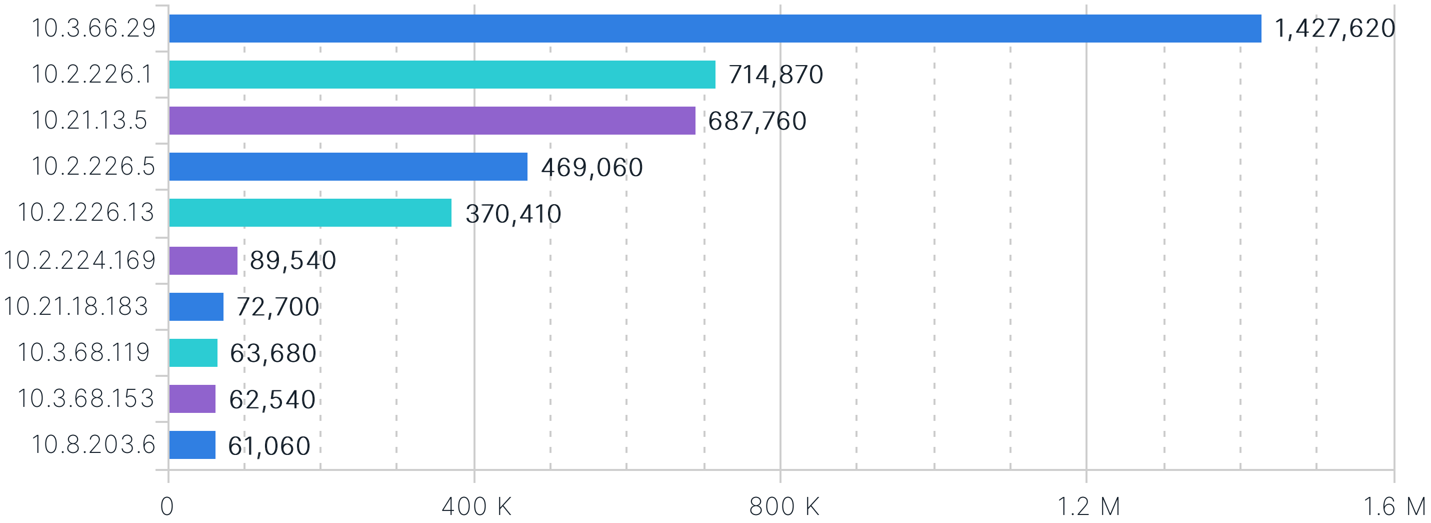
OT Devices Attempting External Connection

Generally, OT devices should not be communicating with IPs external to the organization. This table lists any OT devices which are communicating with external IPs sorted by last communication date. Be sure to review these hosts and verify that any external connections are sanctioned.

#	Host/IP	Session Count	Last External Application	Last External Connection
1	10.3.66.29	272,300	Proxy.HTTP	Jan 11, 2022 5:07 PM
2	10.2.226.1	77,091	Splashtop	Jan 10, 2022 7:34 PM
3	10.2.226.5	353,514	VNC	Jan 9, 2022 10:08 PM
4	10.21.13.5	6,902	Windows.Powershell	Jan 8, 2022 7:38 PM
5	10.2.224.169	6,900	VNC	Jan 6, 2022 9:12 AM
6	10.8.203.6	13,803	Proxy.HTTP	Jan 5, 2022 11:22 AM

At-Risk Devices and Hosts

Based on the types of activity exhibited by an individual host, we can approximate the trustworthiness of each individual client. This client reputation is based on key factors such as websites browsed, applications used and inbound/outbound destinations utilized. Ultimately, we can create an overall threat score by looking at the aggregated activity used by each individual host.



Applications

Quick Stats

- **84** total OT applications detected
- **8** remote access applications detected
- **32.0%** percentage of OT traffic

- **69%:31%** IT vs. OT Application Mix
- **185** IT applications detected
- **269** total applications detected

High Risk Applications

The FortiGuard research team assigns a risk rating of 1 to 5 to an application based on the application behavioral characteristics. The risk rating can help administrators to identify the high risk applications quickly and make a better decision on the application control policy. Applications listed below were assigned a risk rating of 4 or higher.

#	Risk	Application	Category	Technology	Users	Bandwidth	Sessions
1	5	Proxy.HTTP	Proxy	Network-Protocol	26	332.08 MB	93,688
2	4	Citrix.Receiver	Remote.Access	Client-Server	11	8.25 MB	2,945
3	4	RDP	Remote.Access	Client-Server	4	41.83 MB	200
4	4	VNC	Remote.Access	Client-Server	1	25.53 KB	180
5	4	Splashtop	Remote.Access	Client-Server	1	306.63 KB	18
6	4	Windows.Powershell	Remote.Access	Client-Server	1	9.81 KB	2

High Risk Industrial Applications

Industrial applications which are classified as high risk should be investigated. This table shows the highest risk industrial applications detected on your OT network sorted by risk rating. Typically, industrial applications by their very nature are lower risk, but if there are industrial applications with risk ratings 4+, you should investigate further.

#	Risk	Application	Category	Technology	Bandwidth	Sessions
1	3	IEC.60870.5.104_Control.Functions.Unnumbered	Industrial	Client-Server	6.31 MB	3,688
2	3	Vedeer-Root.ATG.Access	Industrial	Client-Server	5.25 MB	2,475

Applications

Industrial Applications In Use By Bandwidth

Industrial application use can sometimes be buried in a sea of common IT traffic. This table highlights industrial specific traffic based on bandwidth usage. Sometimes abnormal bandwidth usage can indicate data exfiltration; be sure to review the application protocol being used by the highest bandwidth industrial applications.

#	Risk	Application	Category	Technology	Hosts	Bandwidth	Sessions
1	2	OPC.UA_Close.Secure.Channel.Request	Industrial	Client-Server	1	1.21 GB	4,322
2	2	OPC.UA_Publish.Request	Industrial	Client-Server	1	842.05 MB	309
3	2	EtherNet.IP_Unregister.Session	Industrial	Client-Server	1	249.81 MB	1
4	2	CIP_Response.Success	Industrial	Client-Server	1	159.15 MB	1
5	2	CIP.CM.ForwardClose	Industrial	Client-Server	1	104.49 MB	2
6	2	OPC.UA_Secure.Conversation.Message	Industrial	Client-Server	1	39.90 MB	1
7	2	BACnet_Who.Is	Industrial	Client-Server	2	3.04 MB	8,653
8	2	OPC.UA_Read.Request	Industrial	Client-Server	1	37.07 KB	1
9	2	Modbus_Report.Slave.ID	Industrial	Client-Server	1	31.97 KB	246
10	2	OPC.UA_Error.Message	Industrial	Client-Server	1	13.12 KB	15

Industrial Applications In Use By Sessions

High session use amongst industrial applications can be indicative of security or (more commonly) issues related to retransmission. Keep in mind that industrial application sessions by their very nature can establish connections for extended periods of time.

#	Risk	Application	Category	Technology	Hosts	Bandwidth	Sessions
1	2	OPC.UA_Close.Secure.Channel.Request	Industrial	Client-Server	1	1.21 GB	43,399
2	2	BACnet_Who.Is	Industrial	Client-Server	2	3.04 MB	8,653
3	2	Modbus_Report.Slave.ID	Industrial	Client-Server	1	31.97 KB	246
4	2	OPC.UA_Error.Message	Industrial	Client-Server	1	13.12 KB	15
5	2	OPC.UA_Publish.Request	Industrial	Client-Server	1	842.05 MB	3
6	2	CIP.CM.ForwardClose	Industrial	Client-Server	1	104.49 MB	2
7	2	OPC.UA_Open.Secure.Channel.Request	Industrial	Client-Server	1	1.03 KB	2
8	2	EtherNet.IP_Unregister.Session	Industrial	Client-Server	1	249.81 MB	1
9	2	OPC.UA_Hello.Message	Industrial	Client-Server	1	287 B	1
10	2	OPC.UA_Get.Endpoints.Request	Industrial	Client-Server	1	842 B	1

Applications

IT Applications In Use By Bandwidth

This table highlights IT specific traffic based on bandwidth usage. Sometimes abnormal bandwidth usage can indicate data exfiltration; be sure to review the application protocol being used by the highest bandwidth IT applications.

#	Risk	Application	Category	Technology	Hosts	Bandwidth	Sessions
1	2	HTTP.Video	Video/Audio	Browser-Based	2	109.24 GB	307
2	5	Proxy.HTTP	Proxy	Network-Protocol	26	66.08 GB	393,688
3	2	RTSP	Video/Audio	Network-Protocol	1	56.53 GB	24
4	2	MS.Windows.Update	Update	Client-Server	24	53.15 GB	40,025
5	2	Stream.Media	Video/Audio	Browser-Based	1	47.10 GB	357
6	2	Citrix.Services	Collaboration	Browser-Based,Client-Server	14	17.52 GB	600
7	2	LDAP	Network.Service	Network-Protocol	103	10.56 GB	168,555
8	3	HTTPS.BROWSER	Web.Client	Browser-Based	161	10.50 GB	122,309
9	2	Facebook_Video.Play	Video/Audio	Browser-Based	4	8.60 GB	448
10	2	SMB.v3	Network.Service	Client-Server	95	4.38 GB	72,615

IT Applications In Use By Sessions

High session use amongst IT applications can be indicative of security or (more commonly) issues related to retransmission. Keep in mind that IT application sessions by their very nature can establish connections for extended periods of time.

#	Risk	Application	Category	Technology	Hosts	Bandwidth	Sessions
1	2	NTP	Network.Service	Network-Protocol	101	978.88 MB	1,661,146
2	2	DNS	Network.Service	Network-Protocol	36	435.78 MB	1,414,697
3	2	Kerberos	Network.Service	Network-Protocol	92	3.64 GB	760,060
4	2	UPnP	Network.Service	Network-Protocol	86	452.71 MB	725,464
5	5	Proxy.HTTP	Proxy	Network-Protocol	26	66.08 GB	393,688
6	2	LDAP	Network.Service	Network-Protocol	103	10.56 GB	168,555
7	2	MS.RPC	Network.Service	Client-Server	94	1.77 GB	135,248
8	3	HTTPS.BROWSER	Web.Client	Browser-Based	161	10.50 GB	122,309
9	2	LLMNR	Network.Service	Network-Protocol	81	15.77 MB	108,977
10	2	ICMP	Network.Service	Network-Protocol	75	141.58 MB	78,192

Applications

Industrial Applications Communications Details

It is not uncommon for OT protocols to encapsulate files during day to day communications. This table renders any files that are traversing via OT protocols. Potentially malicious code could exfiltrate files from your OT network and this visualization helps you ensure any files being transported are authorized.

#	Application	Message	Source IP	Destination IP	Input/Output	Bandwidth
1	Modbus_Encapsulated. Interface.Transport	0e 01 81 00 00 03 00 12 53 63 68 6e 65 69 64 65 72 20 45 6c 65 63 74 72 69 63 01 0a 54 4d 32 32 31 43 45 31 36 54 02 04 56 31 2e 30	10.3.66.29	10.2.224.169	others	63 B
2	Modbus_Encapsulated. Interface.Transport	0e 01 81 00 00 03 00 12 53 63 68 6e 65 69 64 65 72 20 45 6c 65 63 74 72 69 63 01 0a 54 4d 32 32 31 43 45 31 36 54 02 04 56 31 2e 30	10.3.17.238	10.4.23.3	others	44 B
3	Modbus_Encapsulated. Interface.Transport	0e 01 81 00 00 03 00 12 53 63 68 6e 65 69 64 65 72 20 45 6c 65 63 74 72 69 63 01 0a 54 4d 32 32 31 43 45 31 36 54 02 04 56 31 2e 30	10.3.66.29	10.2.226.1	others	42 B
4	Modbus_Encapsulated. Interface.Transport.Read. Device.Info	01 81 00 00 03 00 12 53 63 68 6e 65 69 64 65 72 20 45 6c 65 63 74 72 69 63 01 0a 54 4d 32 32 31 43 45 31 36 54 02 04 56 31 2e 30	10.2.226.5	10.2.226.1	others	115 B
5	Modbus_Encapsulated. Interface.Transport.Read. Device.Info	01 81 00 00 03 00 12 53 63 68 6e 65 69 64 65 72 20 45 6c 65 63 74 72 69 63 01 0a 54 4d 32 32 31 43 45 31 36 54 02 04 56 31 2e 30	10.8.203.6	10.8.115.7	others	293 B
6	Modbus_Encapsulated. Interface.Transport.Read. Device.Info	01 81 00 00 03 00 12 53 63 68 6e 65 69 64 65 72 20 45 6c 65 63 74 72 69 63 01 0a 54 4d 32 32 31 43 45 31 36 54 02 04 56 31 2e 30	10.3.68.153	10.3.17.238	others	88 B
7	Modbus_Read.Input.Registers	14 00 47 00 54 00 47 00 54 16 9d 00 00 00 00 00 00 00 00 00 00	10.21.18.183	10.3.66.29	others	163 B
8	Modbus_Read.Input.Registers	14 00 46 00 58 00 46 00 58 16 9d 00 00 00 00 00 00 00 00 00 00	10.3.66.29	10.4.23.3	others	228 B

Remote Access Traffic to OT Devices

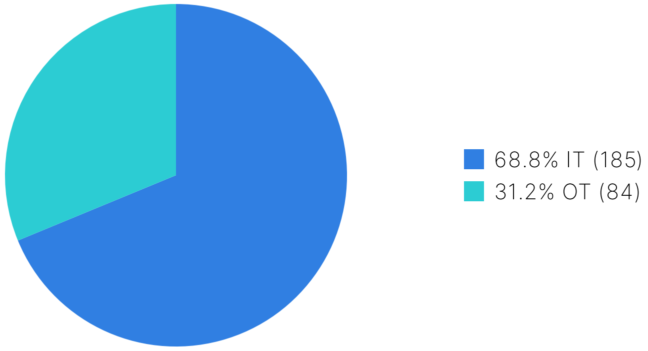
Hosts which are establishing remote access connections with OT devices should be scrutinized. This table lists remote applications detected which have been communicating with OT devices. Be sure to audit whether or not remote access is allowed to these OT devices and from whom the requests are originating.

#	Host/IP	Application	Bandwidth	Sessions	Source IP	Last Session
1	10.3.66.29	Proxy.HTTP	145.99 MB	83	18.33.48.117	Jan 9, 2022 6:11 PM
2	10.2.226.1	Splashtop	130.62 MB	14	226.15.77.181	Jan 8, 2022 9:51 PM
3	10.21.13.5	Windows.Powershell	113.10 MB	11	12.44.18.62	Jan 6, 2022 3:51 AM
4	10.8.203.6	Proxy.HTTP	104.27 MB	8	173.73.39.119	Jan 5, 2022 12:39 PM
5	10.2.226.5	VNC	92.26 MB	3	28.116.195.94	Jan 4, 2022 8:23 AM
6	10.21.18.183	VNC	73.09 MB	2	10.3.66.29	Jan 3, 2022 6:08 PM
7	10.3.66.29	VNC	64.19 MB	2	10.21.18.183	Jan 2, 2022 6:07 PM
8	10.2.226.1	Windows.Powershell	62.93 MB	1	105.28.224.228	Jan 2, 2022 11:05 AM
9	10.2.224.169	Splashtop	59.09 MB	1	226.15.77.181	Dec 30, 2021 10:04 PM
10	10.2.226.5	Windows.Powershell	56.08 MB	1	10.33.48.117	Dec 26, 2021 3:05 PM

Applications

IT vs. OT Applications

While OT networks are primarily dedicated for industrial traffic, the amount of common IT applications running on them is usually high. This pie chart visualization shows the percentage of OT versus IT applications (as measured by a distinct application count). In full hybrid environments, it's not uncommon for OT traffic to be overshadowed entirely by IT traffic.



Utilization

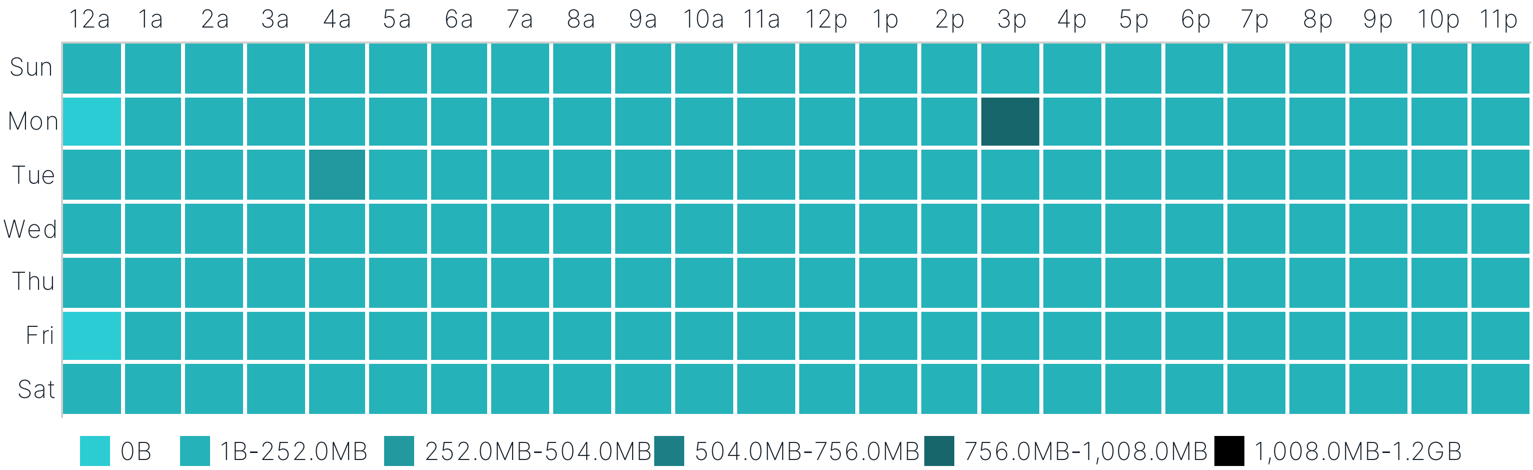
Quick Stats

- **2.7GB** total bandwidth used
- **13** total OT devices detected
- **364.0MB** average OT bandwidth per day

- **68%:32%** IT vs. OT bandwidth mix
- **99%:1%** IT vs. OT session mix

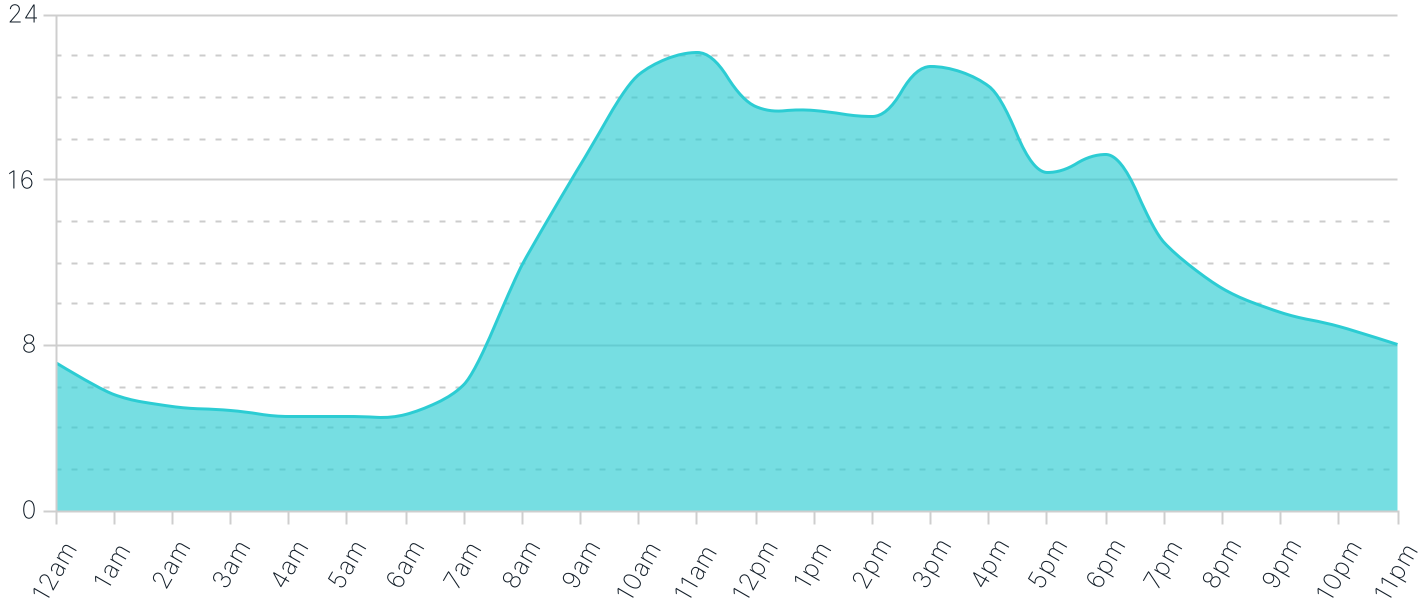
OT Application Bandwidth Utilization

By looking at OT bandwidth usage when distributed over an average day, administrators can better understand their organizational ISP connection and interface speed requirements. Bandwidth can also be optimized on an application basis (using throttling), specific hosts can be prioritized during peak traffic times, and firmware updates can be rescheduled outside of working hours.



Average Log Rate by Hour

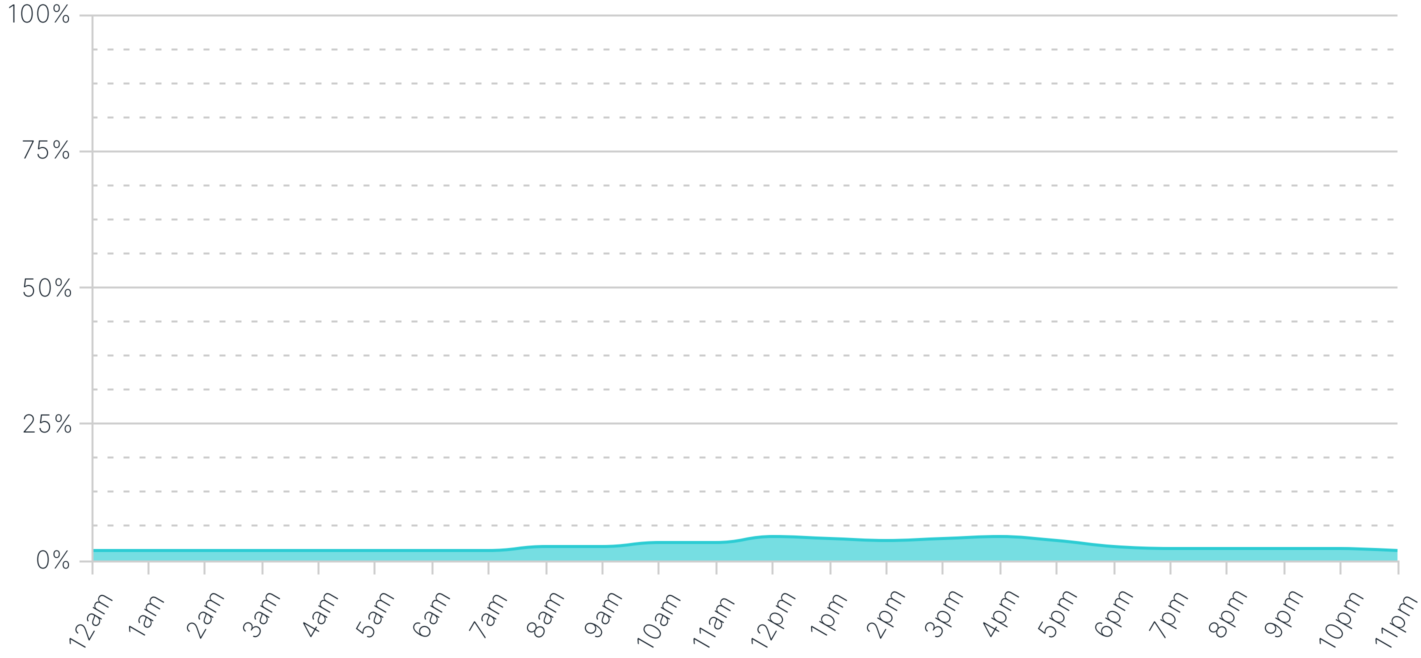
Understanding average log rates is extremely beneficial when sizing a security environment from a performance standpoint. Higher average log rates applied to specific hours usually indicate peak traffic usage and throughput. Calculating enterprise-wide log rates can also help when sizing for upstream logging/analytics devices such as FortiAnalyzer. Keep in mind, the log rates presented here are with the full logging capabilities of the FortiGate enabled and will include all log types (traffic, anti-virus, application, IPS, web and system events).



Utilization

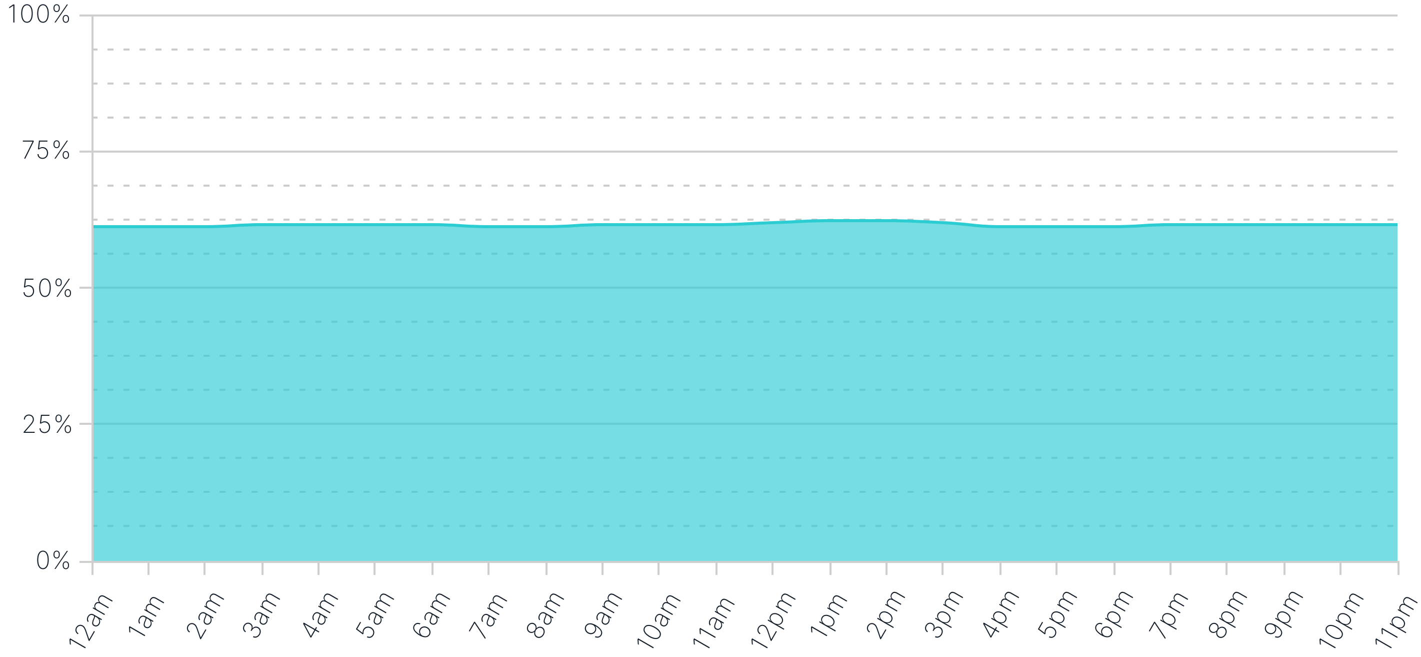
Average FortiGate CPU Usage by Hour

CPU usage of a FortiGate is often used to size a final solution properly. By looking at an hourly breakdown of CPU utlilization statistics, it's easy to get a good idea about how FortiGates will perform in the target network. Typically, with higher throughput, more logs are generated. If 75% or more utilization is sustained over a long period of time, either a more powerful model or revised architecture may be required for final implementation.



Average FortiGate Memory Usage by Hour

Similarly, memory usage over time is an indicator of the FortiGate's sustainability in the target network environment. Memory usage may remain high even when throughput is relatively low due to logging activity (or queued logging activity) over time.



Recommendations

☑ **1. Quarantine Botnet Hosts**

Botnet activity was detected on at least one host within your network. You should immediate quarantine any botnet hosts (e.g. remove them from the network) and investigate any associated breach activity.

☑ **2. Reconcile External Remote Access**

Based on your corporate use policies, determine whether or not external users should be accessing OT devices remotely. If remote access isn't allowed, investigate these as potential breaches.

☑ **3. Audit OT Devices Communicating Externally**

OT devices are normally airgapped or isolated into specific industrial segments on the network. We detected some OT devices attempting to communicate externally however; this may indicate malicious C&C activity and is worthy of additional investigation.

☑ **4. Verify Firmware on OT Devices**

We detected OT specific application attacks on your network. Verify that potentially affected devices are running the latest firmware and are not an exposure risk to application vulnerabilities.

☑ **5. Audit High Risk Hosts for Attack Susceptibility**

Some hosts on your network are exhibiting a high degree of suspicious behavior (which could include originating lateral attacks, potential malware installation, or botnet activity detected). Review the hosts most at risk, and quarantine those devices until you can determine the root cause of the suspicious behavior.