Trusted CI Operational Technology Procurement Vendor Matrix

Version:	1
Publish date:	2023-12-14
Authors:	Adams, Andrew; Arnold, Dan; Dopheide, Jeannette; Kiser, Ryan; Krenz, Mark; Paine, Drew; Peisert, Sean; Simpson, Michael M.; Zage, John
Licence:	This work is licensed under a Creative Commons Attribution-NonCommercial 3.0 Unported (CC BYNC 3.0) license.
Description:	Operational Technology (OT), when installed on an organization's network, becomes part of the overall cyber attack surface for an organization. When procuring this OT, it is important for the purchasing organization to understand how it will integrate with the existing network and security controls as well as understand what new risks it might introduce. This document provides a prioritized list of questions for organizations to send to manufacturers and suppliers to try to get as much of this information as possible.
Audience:	Organizational leadership, procurement department, IT, cybersecurity

How to use this document:

On the "Matrix" sheet of this spreadsheet document there is a list of questions for equipment vendors related to operational technology (OT). Read through the questions and familiarize yourself with them. During the procurement phase of any operational technology, you can send these questions to the OT manufacturer. It is expected that the manufacturer may take some time to get back all the information to you, so it wouldn't be unusual to have to wait a month. Make sure you plan for that in your procurement schedule. Once you receive answers from the manufacturer, it is strongly recommended that you share that information with your Cybersecurity and/or IT operations staff for a technical review and input. If you find the manufacturer's answers to be inadequate for your security needs, it is helpful to the community if you can provide the manufacturer that feedback so that they have a better understanding of the security needs of their customers.

ID #	Control	CIS Safeguards Reference	Implementation Group	Requirement	Vendor Question:	Tips & Examples	Threat Actor Examples	Reference Links	Reference Links, continued	Reference Links, continued
001	Inventory	1.1	1	Have an inventory that details network and computer hardware.	Does the product include a hardware manifest which details all computer and network hardware included?	An inventory should include physical computing assets which are components of the delivered system such as network switches, computers, or firewalls.	A physical inventory is the first step to understanding what devices exist that need to be secured, which can then lead to a prioritization of security and an assessment of how to secure devices at risk. A lack of such an inventory means that systems may be left unsecured or unpatched. An incomplete physical inventory can also lead to malicious, rogue devices [1] or a lack of understanding of interdependencies. For example, in the Target data breach [2], attackers entered through the HVAC system and leveraged the connectivity between that system and the broader network to compromise point-of-sale terminals	[1] https://darktrace.com/blog/smuggled-raspberry-pis-attempt-to-steal-passwords	[2] https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/	
002	Inventory	2.1	1	Provide a software bill of materials (SBOM) for the product.	Provide a software bill of materials (SBOM) for the product.	Ensure that no unauthorized software is used/enabled. Specifically identify and document software which accepts network connections.	"The 2022 annual report from Sonatype shows an average 742% annual increase in software supply chain attacks over the past three years. The impact of these attacks has been widespread, as shown by the Solarwinds, Codecov, and the log4j attacks." [3] Additional details are in the 12 May 2021 U.S. Executive Order 14028 [4] and from CISA [5].	[3] https://www.computer.org/csdl/magazine/sp/2023/06/10315778/1S2UxIIcU00	[4] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/	[5] https://www.cisa.gov/sbom
003	Inventory	2.2	1	Security vulnerabilities in vendor provided software must be patched.	Will the product receive software security patches throughout the product's intended lifecycle?	Describe the expected patching cycle for security vulnerabilities discovered in the product, the recommended patching timetable, and the patching method used.	WannaCry (one of the most well-known strains of ransomware) spread using the Windows vulnerability referred to as MS17-010, which hackers were able to take advantage of using the exploit EternalBlue….Microsoft actually became aware of EternalBlue and released a patch (a software update to fix the vulnerability). However, those who didn't apply the patch (which was most people) were still vulnerable to EternalBlue Link to article here [6].	[6] https://www.avast.com/c-wannacry?_ga=2.9088181.1861057657.1692136656-2079454395.1673559107		
004	Inventory	2.2	1	Software must run on supported versions of operating systems throughout the intended product lifecycle.	Will software components of the product be supported on operating systems supported by the operating system vendor throughout the product's intended lifecycle?	Do not use end-of-life operating systems such as Windows XP, Server 2003 or Vista. They no longer receive security patches and are vulnerable to compromise. Have a plan to migrate to a new OS version if the OS vendor will not support the deployed version throughout the intended operational life cycle of the product.	See J4 - use of end of life software leaves one vulnerable to attacks which are not easily patched			
005	Data Protection	3.3	1	The product must provide a mechanism to prevent unauthorized access to data.	Can access to data be restricted to prevent unauthorized access?	Filesystem permissions are a simple and widely supported mechanism for accomplishing this.	Chinese e-commerce giant Alibaba suffered a major data breach when it failed to apply sufficient forms of data protections which resulted in a non-malicious web crawler scraping up sensitive information from the service. Link [7].	[7] https://www.theregister.com/2021/06/16/alibaba_tabao_scraped_data_leak/		
006	Secure Configuration	4.6	1	Remote maintenance must use secure communication channels.	Are all communications methods used for remote maintenance using encryption?	Use secure communications methods such as SSH or HTTPS for remote maintenance activities.	The OT systems of the Maroochy Water Services, Australia, were compromised via its radio communication ability and maliciously commanded to create overflows of sewage waste. Link [8].	[8] https://www.mitre.org/sites/default/files/pdf/08_1145.pdf		

ID #	Control	CIS Safeguards Reference	Implementation Group	Requirement	Vendor Question:	Tips & Examples	Threat Actor Examples	Reference Links	Reference Links, continued	Reference Links, continued
007	Secure Configuration	4.7	1	It must be possible to either change credentials of or disable any default accounts.	Can default accounts be disabled or their credentials changed, including encryption keys?	For operating system accounts such as Windows accounts, the built-in password change mechanisms are sufficient to qualify. Other accounts such as web application accounts should also be possible to change.	Stuxnet infected WinCC machines via a hardcoded database server password. Link [9].	[9] https://www.cisa.gov/news-events/ics-advisories/icsa-10-272-01		
008	Secure Configuration	4.8	2	It must be possible to disable services or functionality which is not necessary for the proper functionality of the product in its installed application.	Can unused functionality be disabled such that it is unavailable?	This can be achieved by a variety of means, including disabling services, uninstalling software, disabling software which listens on network ports, or explicitly blocking port numbers using host firewall rules.	Stuxnet, malware specifically created to damage OT propagates using the MS10-061 Print Spooler and MS08-067 Windows Server Service (SMB) vulnerabilities, neither of which are necessary on all machines. Link [10], Link [11].	[10] https://www.cisa.gov/news-events/ics-advisories/icsa-10-272-01	[11] https://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf	
009	Account Management	5.2	1	Accounts must use unique credentials or it must be possible to configure them to use unique credentials.	Can all accounts be configured to use different credentials?	Use unique passphrases or keys for each account.	Threat group Chimera uses passwords obtained from previous breaches to compromise new victims. Link [12].	[12] https://research.nccgroup.com/2021/01/12/abusing-cloud-services-to-fly-under-the-radar/		
010	Account Management	5.3	1	Disable unused accounts	Can accounts be disabled, including unused default accounts?	This should apply to operating system accounts as well as other accounts on the system. Built-in mechanisms for disabling Windows or Linux accounts can be used to meet this requirement. For example: - Windows command prompt: net user <username> /active:no - Red Hat Enterprise Linux: ipa user-disable <username> - Generic Linux environments: usermod --lock --expiredate 1970-01-02 <username>	One of the oldest exploited issues. At LBNL in 1987, Markus Hess used the unused account of Colonel Abrens in order to evade detection by system administrators. This was documented in The Cuckoo's Egg on page 152			
011	Account management	5.4	1	Users of the system must use accounts with limited privileges when logging in.	Can user accounts have their privileges restricted?	"Administrator" or "root" accounts should not be used as day-to-day user accounts on computer systems. Windows and Linux systems provide the ability to operate with reduced privileges via UAC and sudo mechanisms respectively. These mechanisms provide the ability to limit privileges during normal use, but escalate privileges via authentication prompt when required.	Many examples here, but a notable one is the Sony Pictures breach of 2014, where the attacker's data mangling tool would wipe out the host's MBR if the tool had administrative rights. Link [13]	[13] https://www.secureops.com/wp-content/uploads/2021/06/Sony-Breach-Analysis-v4.pdf		
012	Access Control Management	6.4	1	Remote network access requires multifactor authentication.	Does the product support multifactor authentication for remote access?	Institutional policy and procedures may define specific allowed or required multifactor authentication mechanisms. Some common ones include Duo, Time Based One Time Passwords (TOTP), or hardware U2F tokens.	Ukraine's power grid OT was affected by a malicious actor (SandWorm) through their ability to 'brute force' the utility's exposed RPC service. Link [14], Link [15].	[14] https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine	[15] https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf	
013	Access Control Management	6.5	1	Administrative access must use multifactor authentication	Does the product require multifactor authentication for administrative access or can it be configured to require it?		See J13 - this is an additional layer of security that can prevent improper access			

ID #	Control	CIS Safeguards Reference	Implementation Group	Requirement	Vendor Question:	Tips & Examples	Threat Actor Examples	Reference Links	Reference Links, continued	Reference Links, continued
014	Patching	7.3	1	For systems connected to the internet, operating systems must be capable of being configured to automatically apply updates.	When connected to the internet, can the product software be configured to automatically apply security updates?	For operational systems, it may be undesireable to take the risk of configuring a system to do so, however the capability should exist and vendor requirements should not prevent this.	WannaCry (one of the most well-known strains of ransomware) spread using the Windows vulnerability referred to as MS17-010, which hackers were able to take advantage of using the exploit EternalBlue….Microsoft actually became aware of EternalBlue and released a patch (a software update to fix the vulnerability). However, those who didn't apply the patch (which was most people) were still vulnerable to EternalBlue Link to article here [16].	[16] https://www.avast.com/c-wannacry?_ga=2.9088181.1861057657.1692136656-2079454395.1673559107		
015	Patching	7.7	2	Security patches for vendor software must be available promptly upon discovery of a vulnerability.	Does the vendor have a vulnerability management and disclosure process which details patch release timelines?	A common practice is to have a vulnerability disclosure statement which provides these details. Vendors may simply provide reference to this document.	See J15 - disclosure of vulnerabilities and a patch release timeline is critical for ensuring relevant software is up to date			
016	Audit log management	8.2	1	The product must produce logs which provide necessary information for event analysis and incident investigations. At minimum, these must include system logins and usage of elevated privileges.	Does the product keep a record of important events, particularly login activity and usage of elevated privileges?	Minimally, events indicating successful/failed authentication attempts and usage of elevated privileges must be collected. It may also be important to collect additional items such as DNS lookups, command line execution logs, URL request logs, encryption certificate details, or API request details.	The UK's National Cyber Security Centre has stated that many investigations have been hindered due to lack of sufficient logging. Link to article here [17].	[17] https://www.ncsc.gov.uk/collection/incident-management/technical-response-capabilities#logs		
017	Audit log management	8.9	2	Logs from the system must be able to be forwarded to a central logging system.	Does the product store logs in a way that allows them to be forwarded to log aggregation systems?	Sending logs and alerts to a central repository enables faster detection of issues and ensures records are available after an incident has occurred. Common logging formats such as syslog provide a standardized way to consume, manage, send, and retain logs programmatically both on and off of the source hosts. Non-standard or application-specific logging formats can still provide this, however they will often require additional processing.	Sophos: "Cybercriminals Disabled or Wiped Out Logs in 82% of Attacks with Missing Telemetry in Cases Analyzed for Sophos Active Adversary Report " Link to article here [18].	[18] https://www.sophos.com/en-us/press/press-releases/2023/11/cybercriminals-disabled-or-wiped-out-logs-82-attacks-missing-telemetry		
018	Malware defenses	10.1	1	Deploy anti-malware software and enable it.	Does the product allow for the installation of anti-malware software on common operating systems which are network connected?	Built-in offerings such as Windows Defender qualify for this requirement.	Several examples at this link [19]. Ransomware example: the city of Baltimore was hit by a type of ransomware named RobbinHood, which halted all city activities, including tax collection, property transfers, and government email for weeks. This attack has cost the city more than $18 million so far, and costs continue to accrue. The same type of malware was used against the city of Atlanta in 2018, resulting in costs of $17 million.	[19] https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/		
019	Malware defenses	10.2	1	Configure automatic updates for anti-malware software	Can malware definitions be updated automatically where applicable?	As malware techniques change over time, anti-malware defenses must change as well. Definition updates must be enabled in order for the defenses to remain effective.	See J19 - keeping anti-malware up to date to maximize its effectiveness			
020	Malware defenses	10.3	1	Disable autorun and autoplay for removeable media	Do any computer systems which are components of the product have autorun or autoplay enabled for removeable media?	There are multiple "autorun" and "autoplay" mechanisms in modern operating systems that are important to take account of. For example, Microsoft sysinternals includes the "autoruns" utility, which is a useful way to check these on Windows systems: Link [20]	See J19 - disabling autorun prevents malware from being automatically run when media is connected	[20] https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns		

ID #	Control	CIS Safeguards Reference	Implementation Group	Requirement	Vendor Question:	Tips & Examples	Threat Actor Examples	Reference Links	Reference Links, continued	Reference Links, continued
021	Data Recovery	11.2	1	There must be a mechanism available to automatically back up and restore data necessary for the product to function. This restoration mechanism should be available to the responsible staff without third-party intervention under degraded operating conditions.	Are there backup mechanisms in place which can be used to automatically back up and restore data necessary for the product to function? Can this mechanism be used to restore functionality by authorized staff without outside intervention?	Software configuration files are a common example of data necessary for products to function. Standard backup and recovery mechanisms such as Windows backup or rsync can often be configured to suffice for this requirement.	1. T-Mobile's Sidekick phone's servers operators (Danger) did not have functioning backups/restore strategy, and the servers failed; customers lost all data if they turned their phones off or the battery expired prior to the system being restored: Link [21]. 2. Even though Colonial Pipeline paid the ransom after their cyberattack, the decryptor key/app they received from the ransomware gang was performing too slowly to get operations back online, hence they were forced to resort to restoring from their own backups: Link [22].	[21] https://techcrunch.com/2009/10/10/t-mobile-sidekick-disaster-microsofts-servers-crashed-and-they-dont-have-a-backup/	[22] https://www.bleepingcomputer.com/news/security/ransomware-gangs-slow-decryptors-prompt-victims-to-seek-alternatives/	
022	Network Infrastructure Management	12.1	1	Network devices which are included as components of the product should be capable of being patched to fix security vulnerabilities.	Do all network devices included with the product provide a mechanism of patching security vulnerabilities?	i.e., vpn, router and/or switch firmware	Toyota Financial Services (TFS) was breached by the Medusa ransomware gang in November, 2023; security analysts following the incident noted that the Citrix Gateway endpoint used by TFS's German office was public and had not been updated since August 2023, making it exploitable to the critical Citrix Bleed (CVE-2023-4966) vulnerability. Link [23].	[23] https://www.bleepingcomputer.com/news/security/toyota-confirms-breach-after-medusa-ransomware-threatens-to-leak-data/		
023	Network Infrastructure Management	12.4	2	Provide a network diagram describing the system components and their interaction mechanisms.	Does the product documentation include a network diagram describing key networked components and their interactions?	Documentation is important to ensuring all aspects of the network are properly configured. This documentation would prove invaluable when upgrading/repalcing components. Ideally this would reference port numbers and protocols used for network communications.	Improper setup of network infrastructure can lead to improper function of relevant cybersecurity controls, leading to increased cyber risk. See J24 and J22 for examples of the effects of ransomware attacks.			
	Version: 2023-12-14									

ID #	Control	CIS Safeguards Reference	Implementation Group	Requirement	Vendor Question:	Tips & Examples	Threat Actor Examples	Reference Links	Reference Links, continued	Reference Links, continued
	Deploy and maintain anti-malware software	10.1	IG1							
	Configure automatic updates for anti-malware software	10.2	IG1							
	Disable autorun and autoplay for removeable media	10.3	IG1							

ID #	Control	CIS Safeguards Reference	Implementation Group	Requirement	Vendor Question:	Tips & Examples	Threat Actor Examples	Reference Links	Reference Links, continued	Reference Links, continued
	Configure automatic malware scans for removable media.	10.4	IG2							