



Five Blind People and an Elephant called ICS Supply Chain Security

Eric Byres, P.Eng, ISA Fellow
eric.byres@aDolus.com

Today's Talk

- The Problem: Understanding the issues in the firmware supply chain and all the different perspectives
- Possible Solutions: Existing solutions and their limitations for ICS and IIoT
- Our Research: Creating a secure trust ecosystem for firmware validation



Everyone Has a Different Perspective

Feels COUNTERFEIT

Is this a bad
CERTIFICATE
CHAIN?

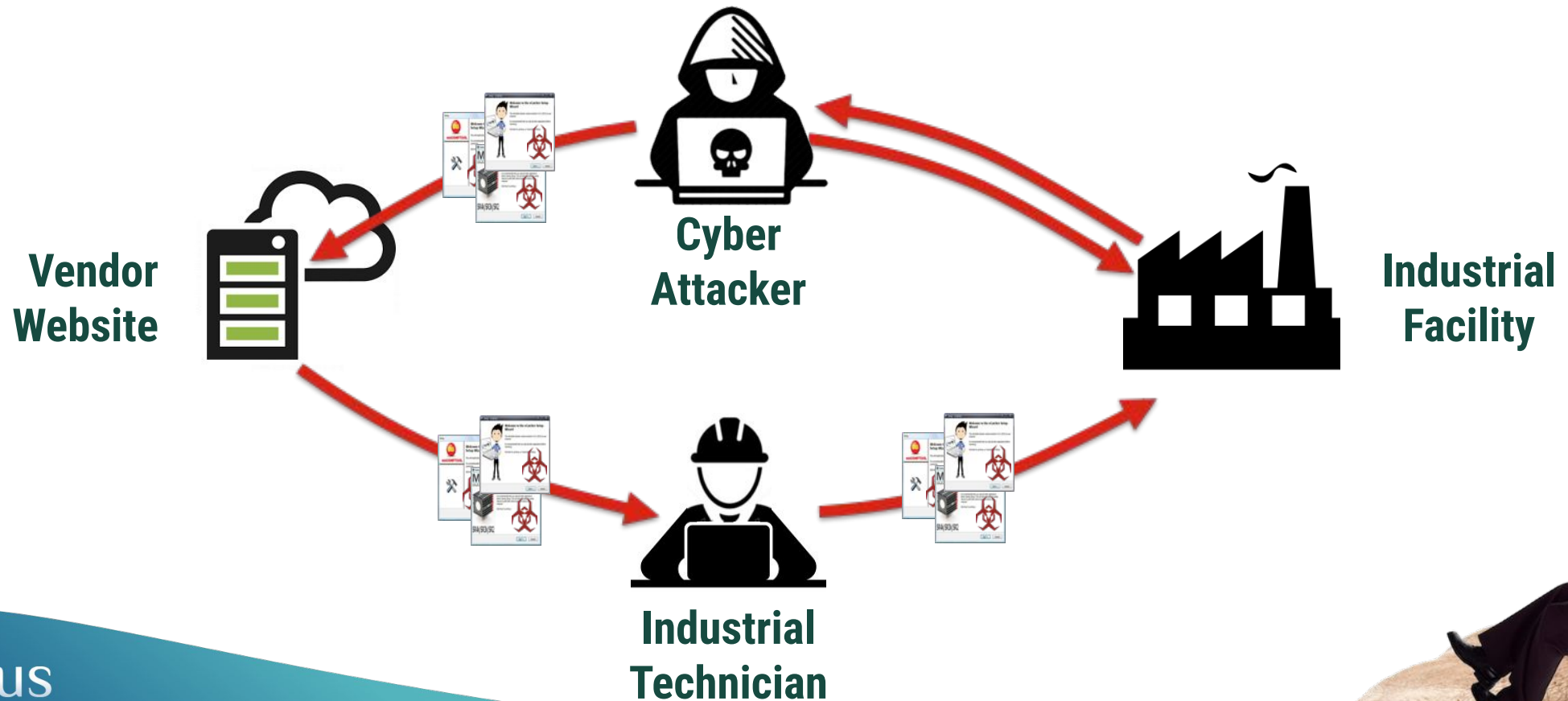
Isn't this
BANNED?

Seems to be
OBSOLETE

Is that a
MYSTERY
COMPONENT?

Critical Software Modified by Attackers

Dragonfly 2014: Exploiting Supplier-User Trust



Fake Software Updates

Allenbradleyupdate.zip

Rockwell
Automation

Support Center

Claims of ransomware masquerading as an Allen-Bradley Update

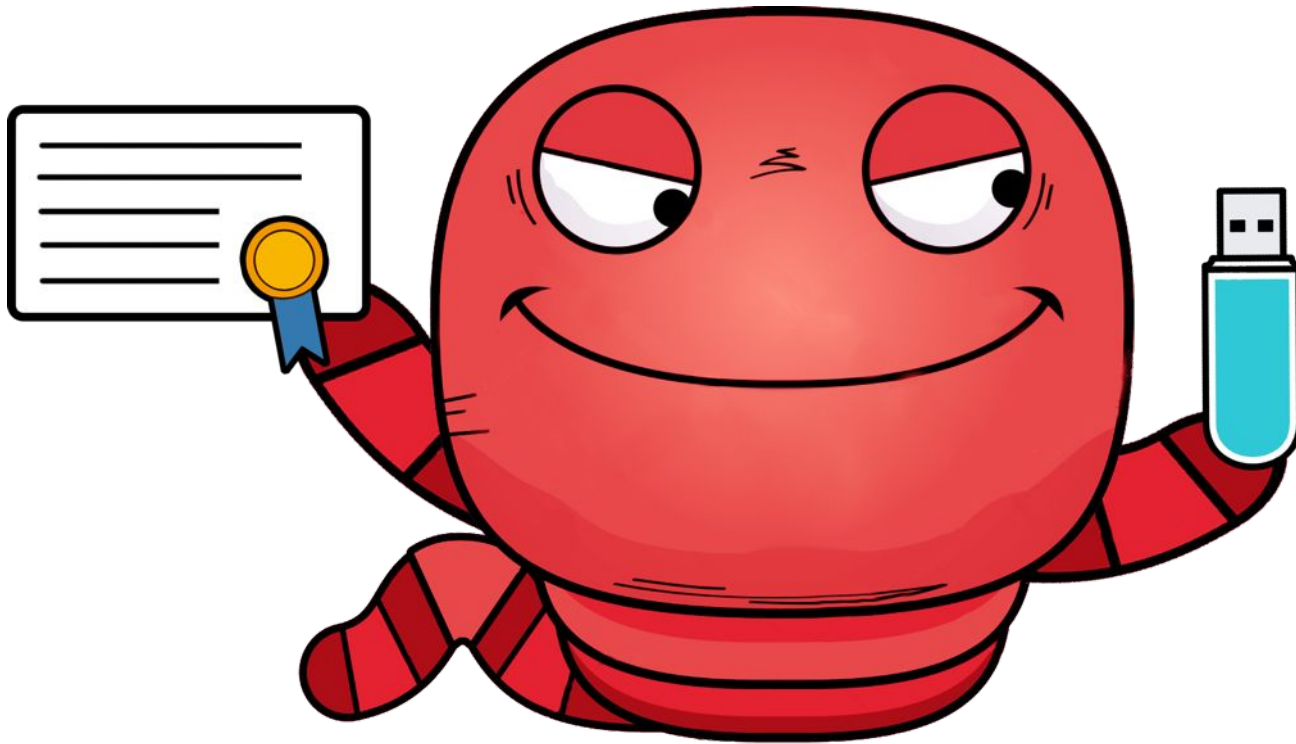
Version 2.0 - July 8th 2016

Rockwell Automation has learned about the existence of a malicious file called "Allenbradleyupload.zip" that is being distributed on the internet. **This file is NOT an official update from Rockwell Automation, and we have been informed that this**

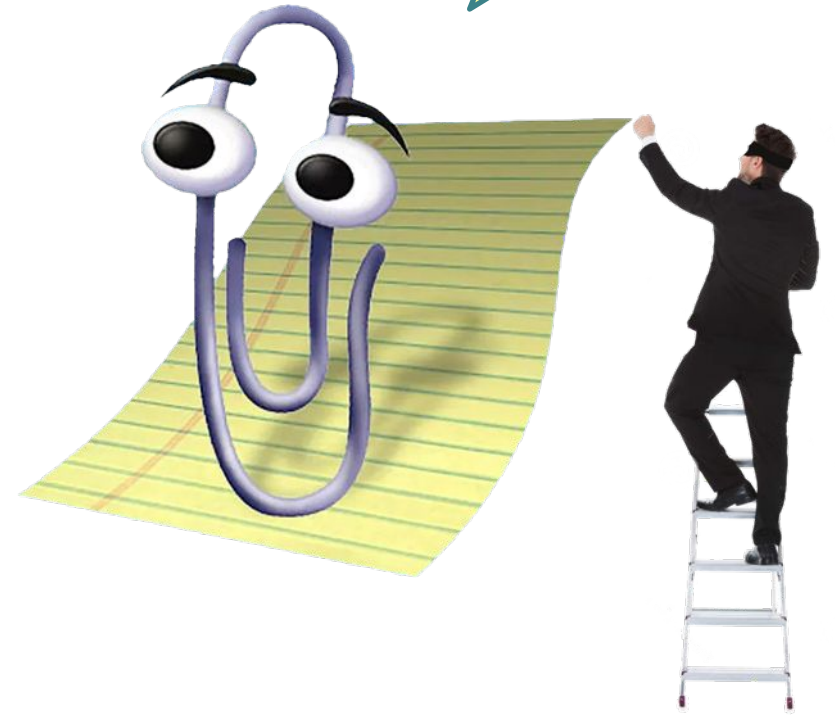


But Code Signing Will Fix Everything...

Stuxnet: Stolen Digital Certificates



IT LOOKS LIKE YOU'RE
TRYING TO ENRICH URANIUM.
WOULD YOU LIKE HELP?



Software with Hidden Vulnerabilities

Gemalto LMS 2017: Undisclosed 3rd-party Modules



INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | CISO Foru



Gemalto Licensing Tool Exposes ICS, Corporate Systems to Attacks

By [Eduard Kovacs](#) on January 22, 2018



A significant number of industrial and corporate systems may be exposed to remote attacks due to the existence of more than a dozen vulnerabilities in a protection and licensing product from Gemalto.



Prohibited Software

Finding Kaspersky Code 2017: It's Everywhere

Nextgov

CYBERSECURITY

EMERGING TECH

ARTIFICIAL INTELLIGENCE

IT MODERNIZATION

As Kaspersky Deadline Approaches, Fears Loom That Contractors Aren't Prepared



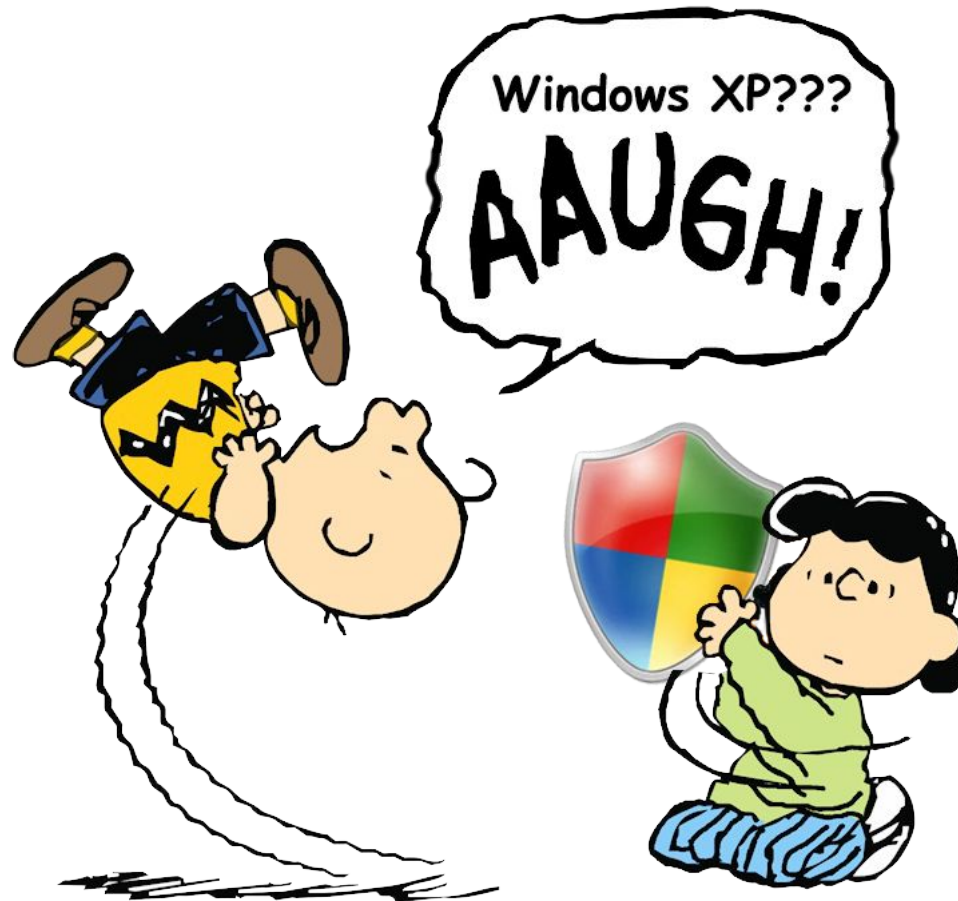
SEPTEMBER 10, 2018

Some contractors may not be aware the ban applies to them or that they're running Kasperksy in the first place. Others don't understand how complex removing



Version Validation

Tricking users into installing old updates with vulnerabilities



Existing Hash/Code Signing Solutions

- Vendor-published MD5/SHA file hashes
 - Are the hashes actually checked by the user?
 - Have the hashes been altered by attackers?
 - What do you do if a hash check fails?
- Code signing (e.g., Microsoft Authenticode)
 - What if you don't have an Internet connection?
 - Does your embedded O/S or device support signing?
 - It is signed but is anyone checking the certificate chain?
 - It is signed but what does it contain?

"The Truth is Out There"

1000S OF
DEVICES

100S OF
DATABASES

HOW DO THEY
TRUST THEIR
SOFTWARE?

100S OF
VENDORS

100S OF
TOOLS

VALKYRIE
COMODO

VERACODE
refirm labs
BLACKDUCK
protecode
WhiteSource

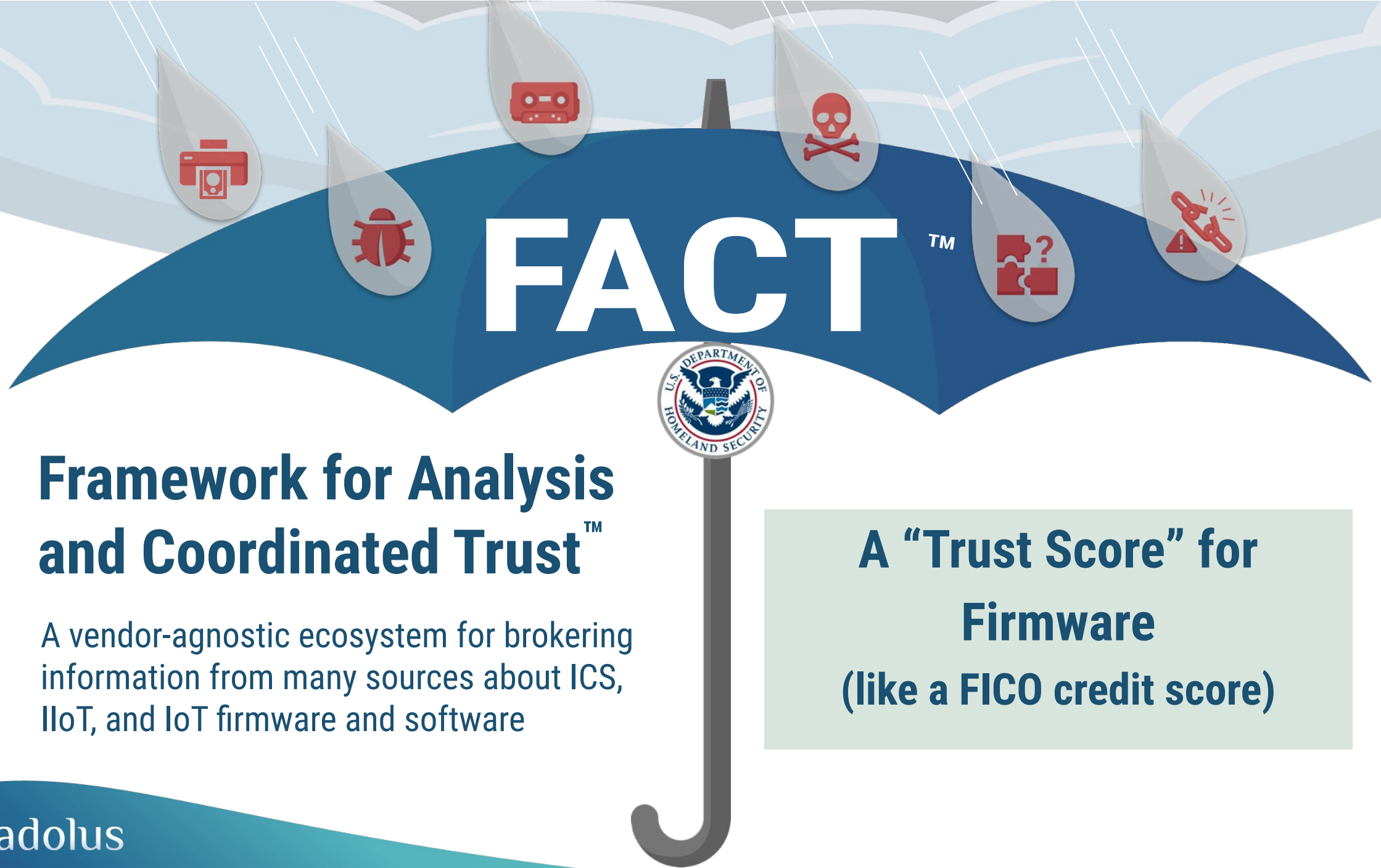
BOSCH
SIEMENS
EMERSON

In Search of a Comprehensive Solution

DHS SVIP funded research project:

“... to develop a robust, vendor agnostic solution for verifying and validating third-party firmware updates for IoT devices.”





Framework for Analysis and Coordinated Trust™

A vendor-agnostic ecosystem for brokering information from many sources about ICS, IIoT, and IoT firmware and software

A “Trust Score” for
Firmware
(like a FICO credit score)

FACTTM



**ASSET
OWNERS**



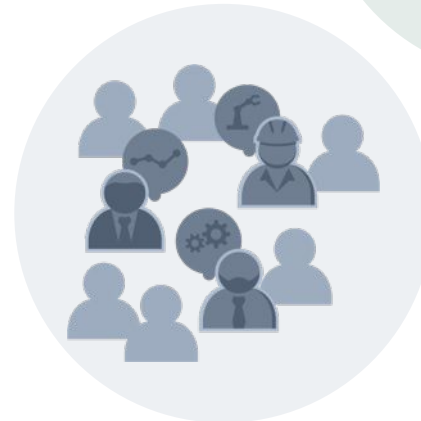
**SECURITY
PARTNERS**



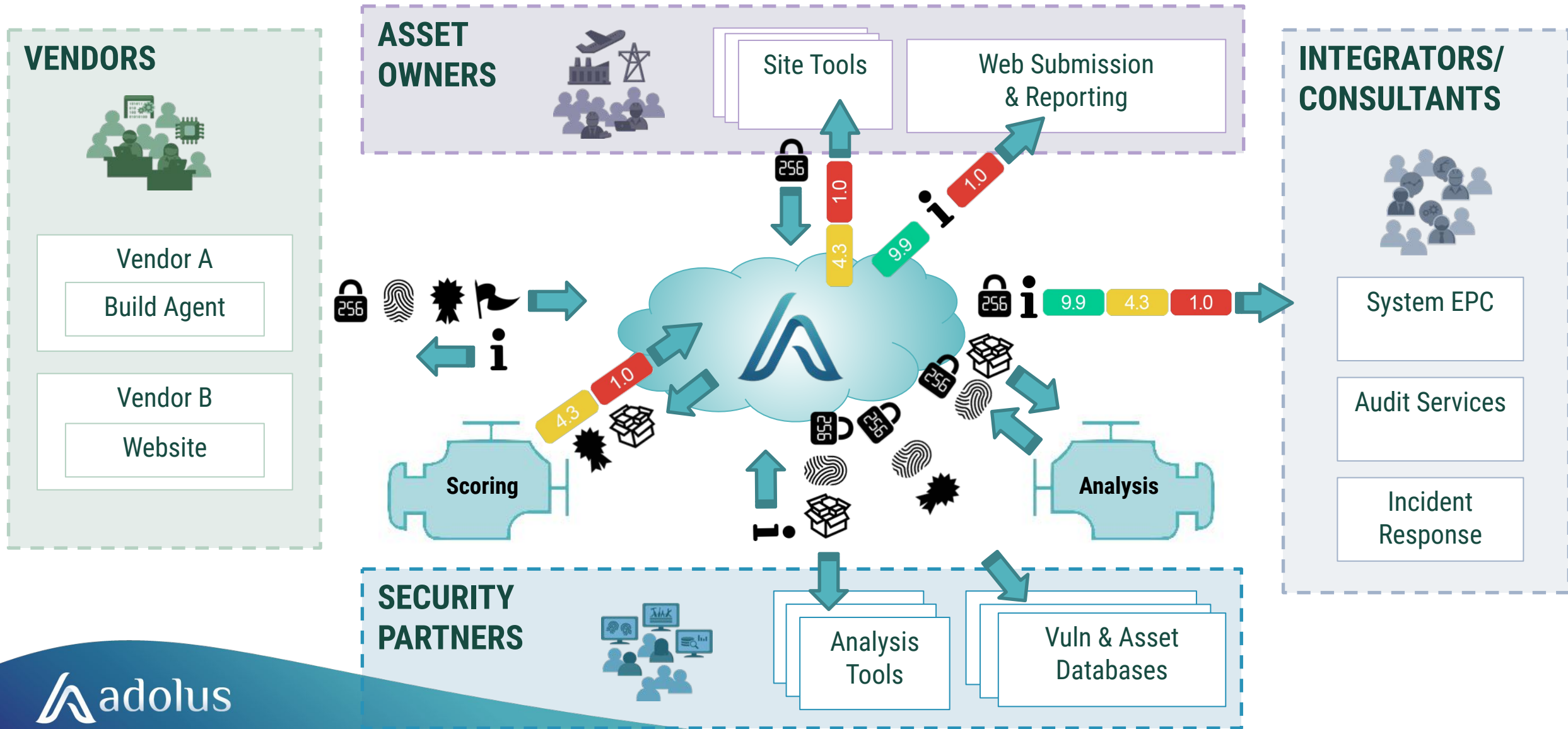
VENDORS



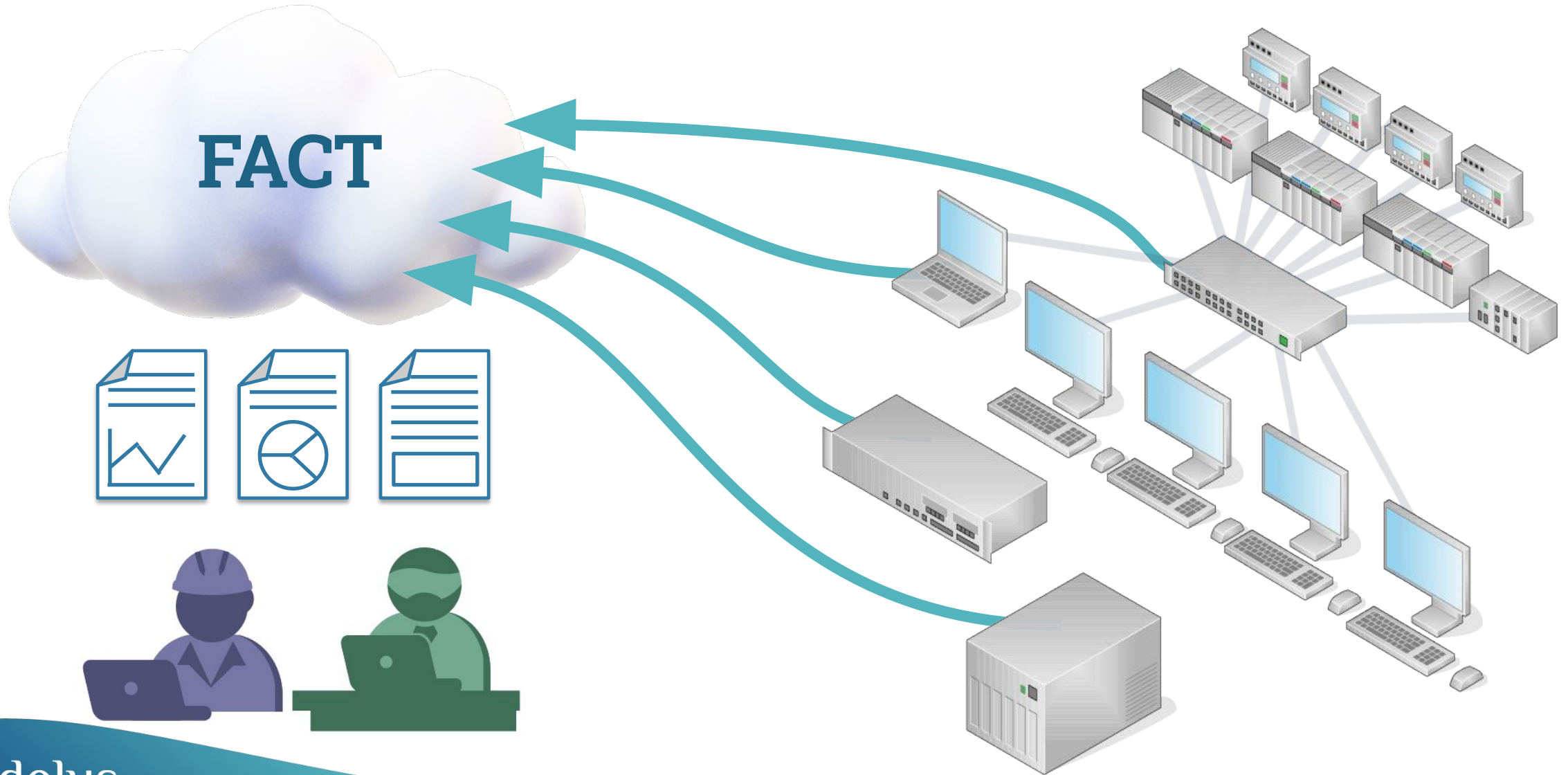
**INTEGRATORS &
CONSULTANTS**



FACT™ Architecture



Plant Floor Software Discovery Reporting



Checking Firmware Trustworthiness

The screenshot shows the Adolus Files interface. The top navigation bar includes the Adolus logo, a dashboard menu, and user information for Initech Energy and Eric Byres. The main section is titled 'Files' and shows a list of files with columns for Rating, Filename, Version, and Submitted. A search bar and an 'Upload Files' button are also visible. A modal window is open, displaying 'PARENT CONTAINER FILES' and a list of files known to be contained in the package.

Can we trust this unsigned PLC Firmware (and where did it come from)?

YES - it was contained in this signed Rockwell upgrade package.

Rating	Filename	Version	Submitted
4.0	1756L64...	4 (series ...	27 minutes ago by Eric Byres
4.0	Rockwell_1756-L55...	Rockwell Autom...	
4.0	PN-301804.bin		
4.0	1756-L7x_23.012.zip	applicatio...	Rockwell Aut...

PARENT CONTAINER FILES

This file is known to be contained in these packages:

Rating	Filename	Version
4.0	1756-L6x_20.015.zip	Rockwell Automation - 1756-L62 (series A)

Checking Firmware Trustworthiness

The screenshot shows the Adolus Files interface. The top navigation bar includes the Adolus logo, a dashboard menu, and user information for Initech Energy and Eric Byres. The main section is titled 'Files' and shows a list of files with columns for Rating, Filename, Type, Vendor, Product, Version, and Submitted. A search bar is available. A callout box points to a file named 'PN-301804.bin' with a rating of 0.0, stating: 'But this PLC Firmware (with the same name) was never part of an official upgrade package.'

The detailed analysis window for 'PN-301804.bin' shows a rating of 0.0 and the following details:

Category	Status	Description
Record Match	Green	The file matches a known record.
Unknown	Red	This file is not trusted.
Malware Detected	Red	The file contains detected malware. View Details
No Vulnerabilities	Green	The file has no known vulnerabilities.
No Stability Concerns	Green	The file has no reported stability issues.

Validating Certificate Signing

The screenshot shows the adolus web interface. At the top, there's a navigation bar with 'Dashboard', 'Vendor Tools', 'Files 41', and 'Logs'. On the right, user information for 'Initech Energy' and 'Eric Byres' is displayed. Below the navigation bar, there are filters for 'Available 5', 'Released 8', 'Private 0', and 'All 13'. A search bar and a 'Group By Product' button are also present. The main content is a table with columns: Rating, Product Name, Version, Version Status, Public Release, and Uploaded. The table lists three files: 'abcd.dat', 'dev.data', and 'Initech.Agent.exe'. The 'Initech.Agent.exe' file has a rating of 3.0, a red gear icon, and a 'Certificate Chain Mismatch' warning. A callout bubble points to this warning.

Rating	Product Name	Version	Version Status	Public Release	Uploaded
6.0	abcd.dat		Supported	December 11, 20...	21 days ago by Samir Nagheenanajar
6.0	dev.data		Supported	November 9, 2018	a month ago by Samir Nagheenanajar
3.0	Initech.Agent.exe		Supported	October 25	2 months ago by Peter Gibbons

This file is signed but there is a certificate chain mismatch (so be very careful).

Finding Hidden Vulnerabilities

Files

Unclassified 43 Approved 5 Rejected 5 All 53

Search

Why does this Protection and Control Manager package have a low score?

Rating	Filename	File Type	Vendor	Product	Version	Submitted
0.7	PCM600_2.4.exe	applicatio...	ABB Oy			
4.0	%FILEPATH4%					
4.0	%FILEPATH41%					
4.0	akshhl29.dll			DM De...	1.2	
4.0	akshhl.inf					
4.0	akshsp51.dll		Aladdin Knowled...	Aladdin WDM De...	1.2	
0.7	hasplms.exe	applicatio...	SafeNet Inc.	HASP License M...	12	

And here are the details

Because this vulnerable 3rd party module is hidden in it

Analysis Results File Details Relationships

RATING: 0.7

DETAILS

- Record Match: The file matches a known record.
- Known Source: This file is from an external known vendor.
- Good Community Standing: The file is in good standing with the aDolus community.
- No Malware: The file contains no detected malware.
- Known Vulnerabilities: The file contains one or more publicly known vulnerabilities. [View Details](#)
The file is known to have the following vulnerabilities:
 - CVE-2017-11498 7.5 High
 - CVE-2017-11497 9.8 CRITICAL
 - CVE-2017-11496 9.8 CRITICALClick on the items above to learn more about each vulnerability and/or exposure.
- No Stability Concerns: The file has no reported stability issues.

Firmware/Software Version Management

adolus FACT BETA

Dashboard Vendor Tools Files 26 Logs

API Access Initech Bill Lumbergh Help Log Out

Unclassified 26

Search

Rating	File	File Type	Vendor
8.0	PISMT_2017_R2_exe	application/...	OSIsoft
9.0	PI-Data-Archive_2017-R2A_...	application/...	OSIsoft
9.0	pinetmgr.exe	application/...	OSIsoft
8.0	PIDirectoryPublisher.exe	application/...	OSIsoft
9.0	OSIsoft.REST.Host.exe	application/...	OSIsoft

This PI package is valid but an update is recommended by the vendor.

Analysis Results 8.0 File Details Relationships 0

RATING: 8.0

DETAILS

Record Match

The file matches a known record.

Trusted Source

The file is confirmed to be from a trusted partner vendor.

No Malware

The file contains no detected malware.

No Vulnerabilities

The file has no known vulnerabilities.

No Stability Concerns

The file has no reported stability issues.

Obsolete

The product owner has reported this file as obsolete.

Helping Vendors Find Malware False Positives

adolus FACT BETA Dashboard Vendor Tools Files Rockwell Automation Eric Byres Help Log Out

Unsaved Custom Report Group By Product List All Files

Filter by keyword Upload Date Public Release Date Deployment Status File type Product

Malware: Malware Unlikely (+2) Vulnerabilities Obsolescence Submitter

	Score	Filename	Product	Status	Public Release	Uploaded
	3.5	> PowerFlex_525_04.001_06_AppUpdate.msi	PowerFlex 525 (Firmware)			9 months ago
	3.5	> PowerFlex_525_2.002_14_AppUpdate.msi	PowerFlex 525 (Firmware)			9 months ago
	3.5	> PowerFlex_525_05.001.msi	PowerFlex 525 (Firmware)	5.001	Supported	
	3.5	> PowerFlex_525_01.005_98_AppUpdate.msi.exe	PowerFlex 525 (Firmware)	1.005	Supported	
	4.0	> PF525_3_1_8_ControlFlash_only.zip	PowerFlex 525 (Firmware)	3.001	Supported	
	3.5	> PowerFlex_525_02.003_26_AppUpdate.msi	PowerFlex 525 (Firmware)	2.003	Supported	
	4.0	> PowerFlex_525_05.002.msi	PowerFlex 525 (Firmware)	5.002	Supported	
	4.0	> 440C-CR30 8.013.zip	440C-CR30-22BBB (Firmware)	8.013	Supported	
	4.0	> [ControlFlashKit]_1783_NATR_fw1_002_0034.zip	1783-NATR (Firmware)	1.002	Supported	
	4.0	> 56RF-IN-IPD22 v1.06.zip	56RF-IN-IPD22 (Firmware)	1.006	Supported	a year ago
	4.0	> 1768-ENBT 4.005_10 CF Kit.zip	1768-ENBT (Firmware)	4.005	Supported	a year ago

☐ No Malware Detected
☒ Malware Unlikely
☒ Malware Suspected
☒ Malware Detected
X Clear

☐ No Malware Detected
☒ Malware Unlikely
☒ Malware Suspected
☒ Malware Detected
X Clear

Helping Vendors Find Malware False Positives

PowerFlex-525_05_001.msi

Analysis Results **3.5** File Details Relationships 0

SCORE: **3.5**

DETAILS

- Record Match: The file matches a known record.
- Known Source: The file is from an external known vendor.
- Signed: The file signature is valid.
- Malware Unlikely: The file is detected by 1 engines - likely a false positive. [View Details](#)

VirusTotal reports this file to contain the following:

0 / 56 Undetected Last updated: 2 months ago

Last analyzed: 3 years ago

Sub-components of this file are reported to contain the following:

1 / 68 MALWARE ControlF...

ControlFLASH.exe

Analysis Results **6.0** File Details Relationships

SCORE: **6.0**

DETAILS

- Record Match: The file matches a known record.
- Known Source: The file is from an external known vendor.
- Signed: The file signature is valid.
- Malware Unlikely: The file is detected by 1 engines - likely a false positive. [View Details](#)

VirusTotal reports this file to contain the following:

1 / 68 MALWARE Last updated: 2 days ago

Last analyzed: a year ago

Click an item above to learn more about the detected malware.

URL, IP address, domain, or file hash

1 / 68

7f5221be13d4b6ea4342688ecc8b9d4435a164136e4fa8e19d4b

ControlFlash

overlay peexe signed

DETECTION DETAILS BEHAVIOR COMMUNITY

Zillya	Trojan.SmallCRTD.Win32.10942
AegisLab	Undetected
ALYac	Undetected
Arcabit	Undetected
Avast-Mobile	Undetected
Avira (no cloud)	Undetected
Babable	Undetected
BitDefender	Undetected
CAT-QuickHeal	Undetected
CMC	Undetected

Benefits of FACT Validation Model

- Vendor and platform independent solution for securing the last mile of your supply chain
- Validation using proven cryptographic technology
- Fits into existing asset-owner processes
- Vendors and asset owners maintain control of their software
- Provides compliance with acquisition requirements for validation of software

Validation



Deconstruction



Obsolescence



Reputation



Try It – It's Free! (portal/adolus.com)





adolus

Contact us to become a member

www.adolus.com

info@adolus.com

1-866-423-6587