adolus

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

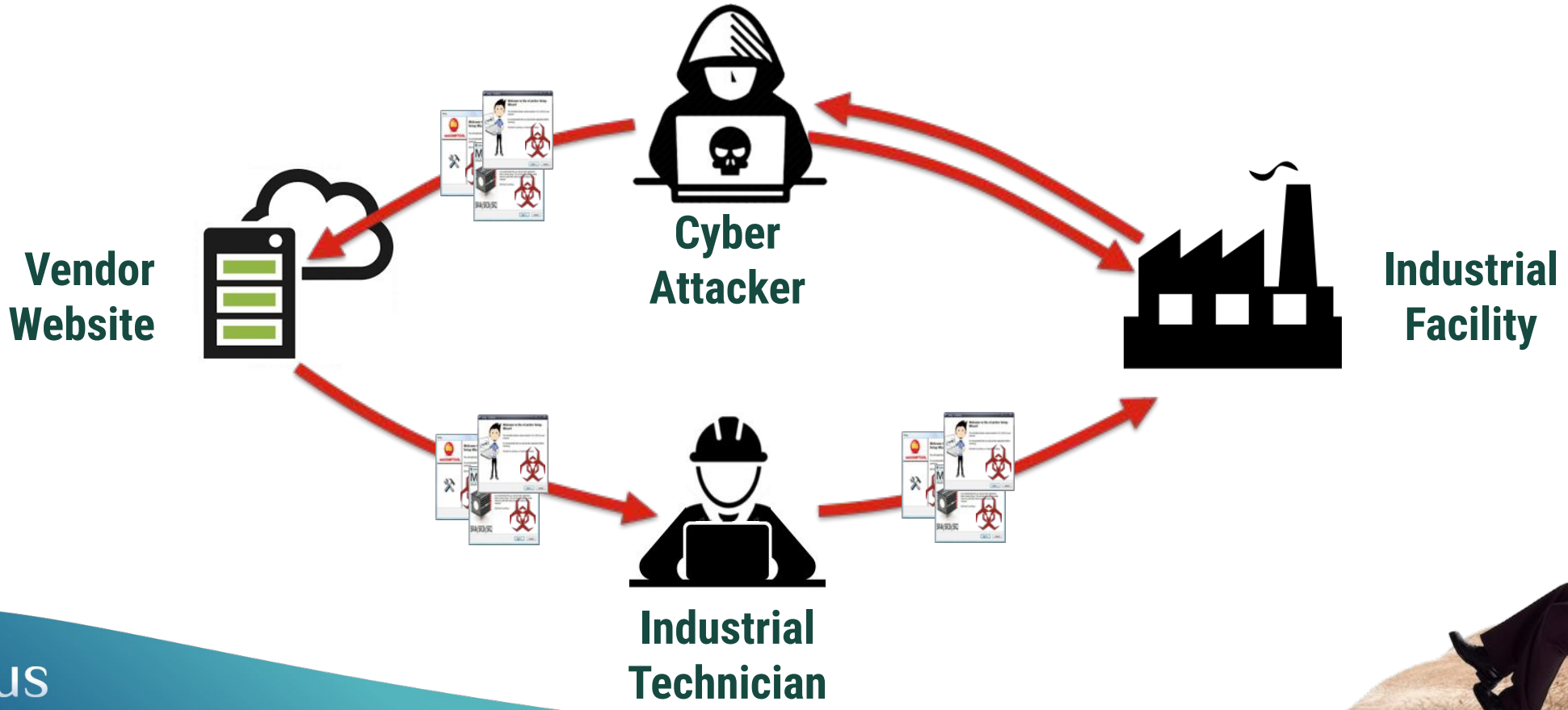
adolus

Everyone Has a Different Perspective

adolus

Critical Software Modified by Attackers

Dragonfly 2014: Exploiting Supplier-User Trust



adolus

Fake Software Updates

Allenbradleyupdate.zip

Rockwell Automation

Support Center

Claims of ransomware masquerading as an Allen-Bradley Update

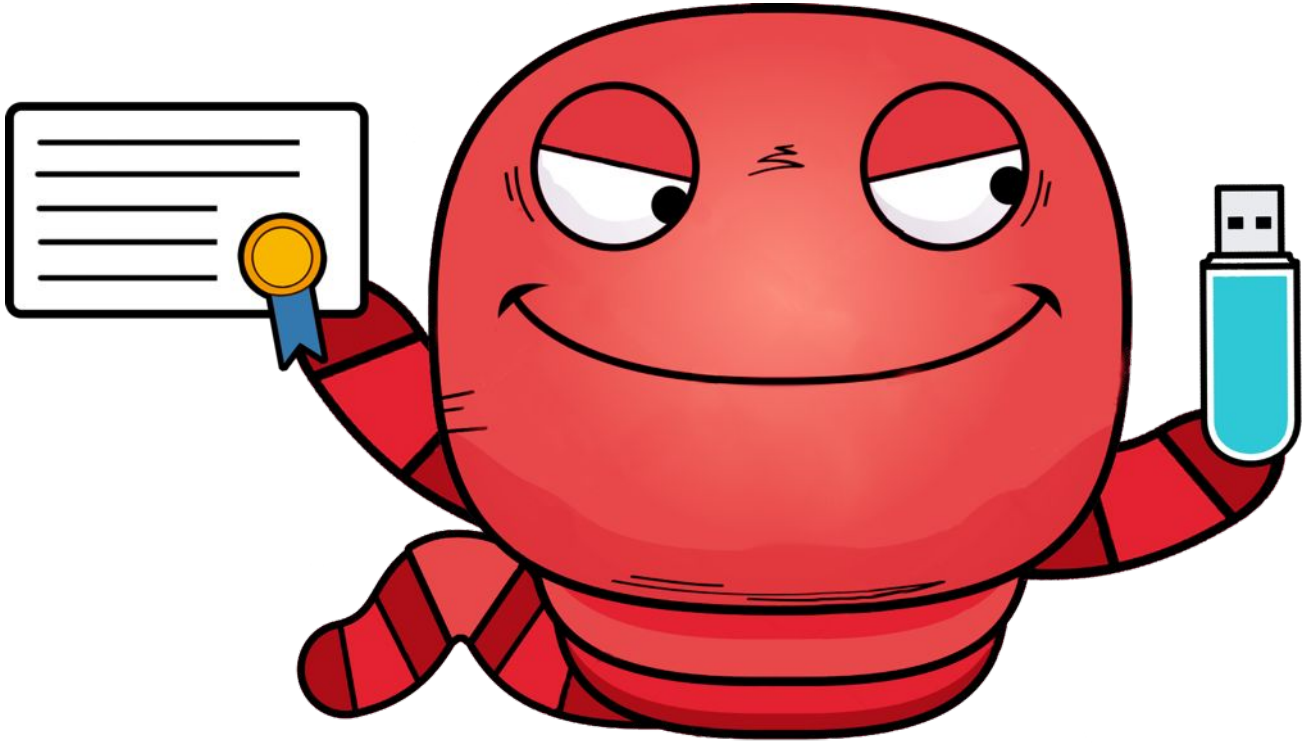
Version 2.0 - July 8th 2016

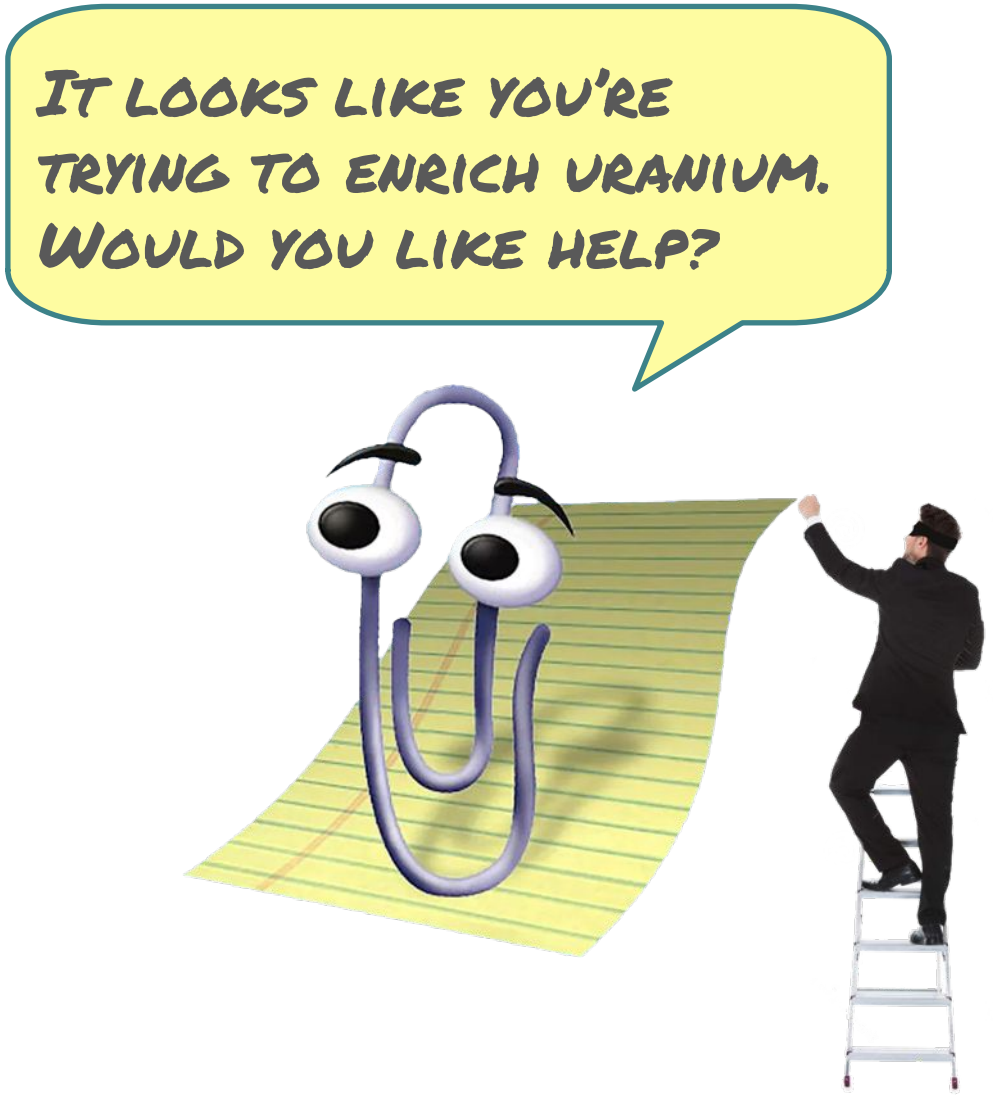
Rockwell Automation has learned about the existence of a malicious file called "Allenbradleyupload.zip" that is being distributed on the internet. **This file is NOT an official update from Rockwell Automation, and we have been informed that this**

adolus

But Code Signing Will Fix Everything…

Stuxnet: Stolen Digital Certificates





adolus

Software with Hidden Vulnerabilities

Gemalto LMS 2017: Undisclosed 3rd-party Modules

SECURITY WEEK

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

Share G+ Tweet Recommend 25 RSS

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.

adolus

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

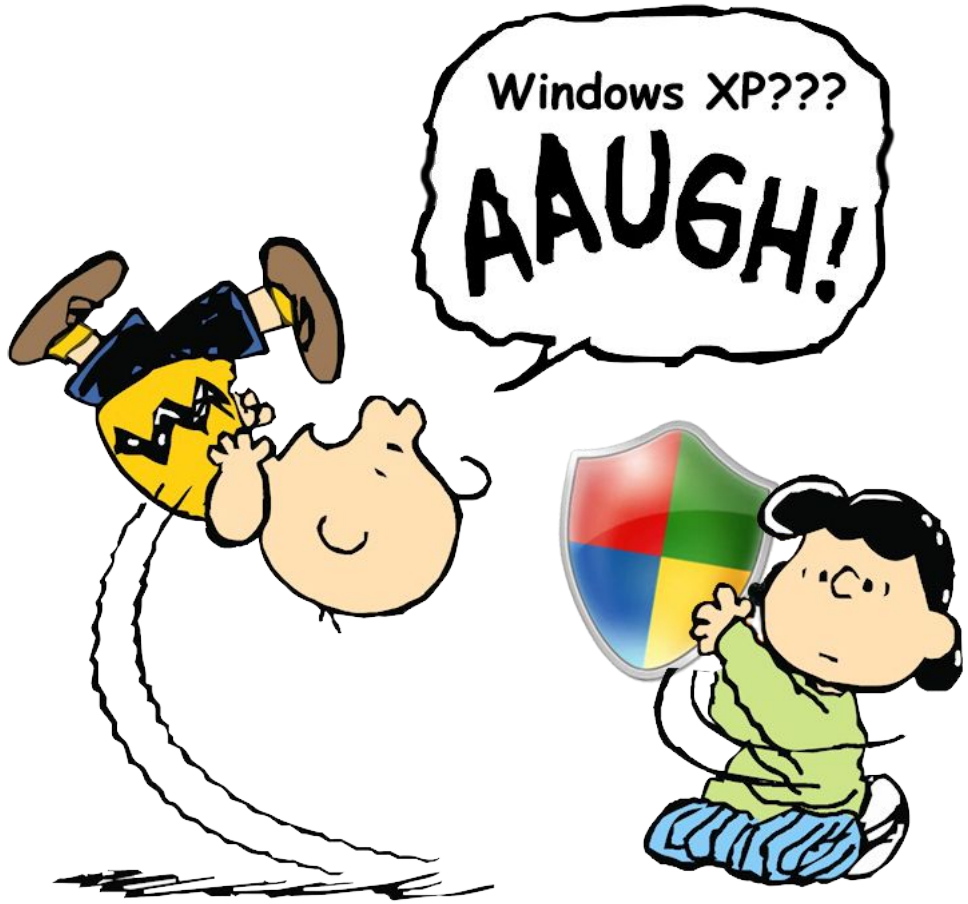
SEPTEMBER 10, 2018

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

adolus

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?

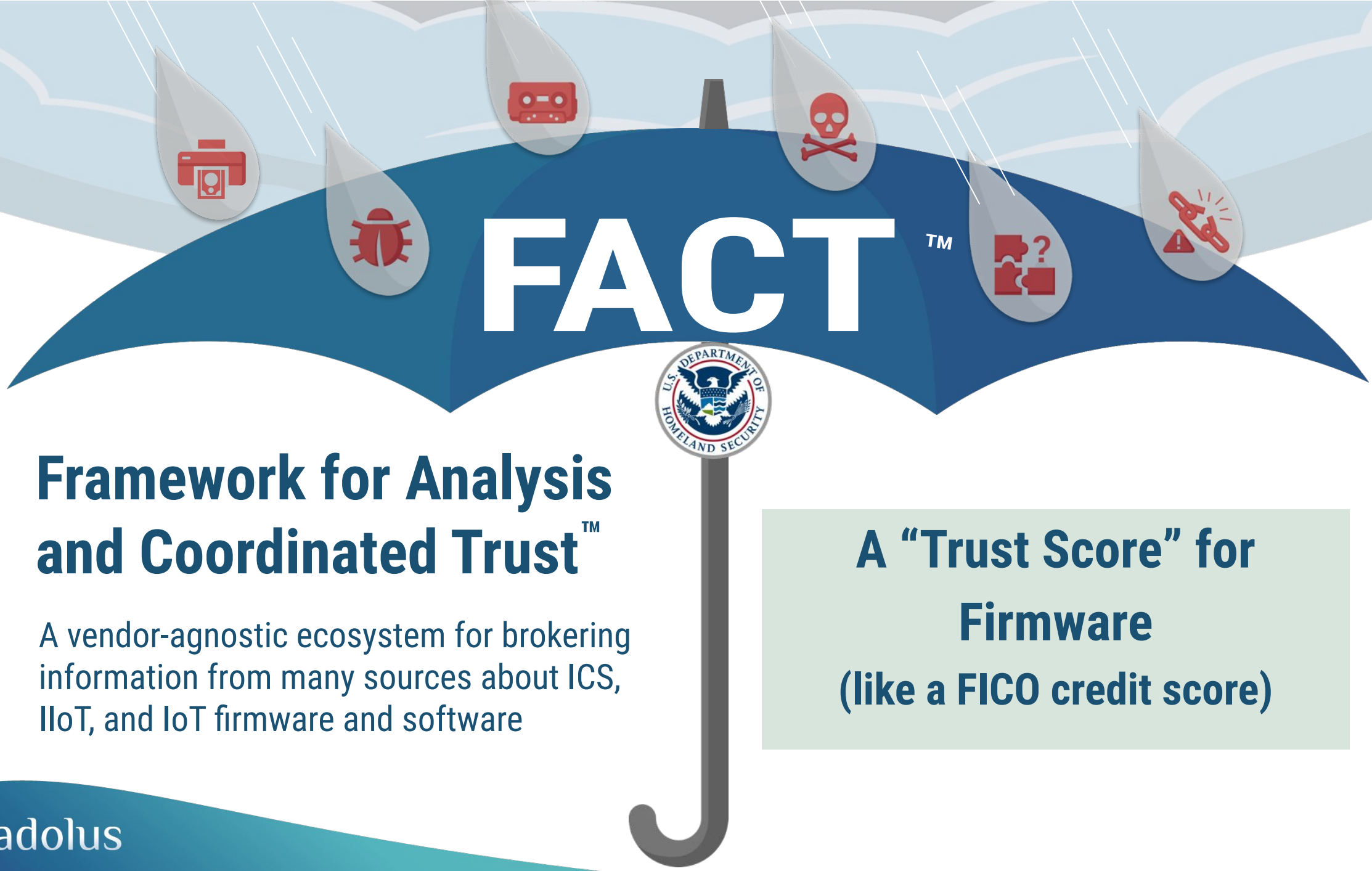
“The Truth is Out There”

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."*

adolus



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

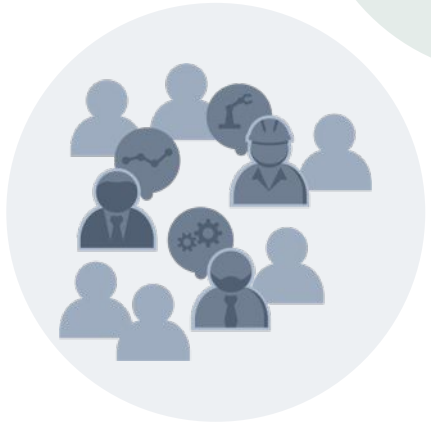
(like a FICO credit score)

adolus

FACT™

ASSET OWNERS

SECURITY PARTNERS

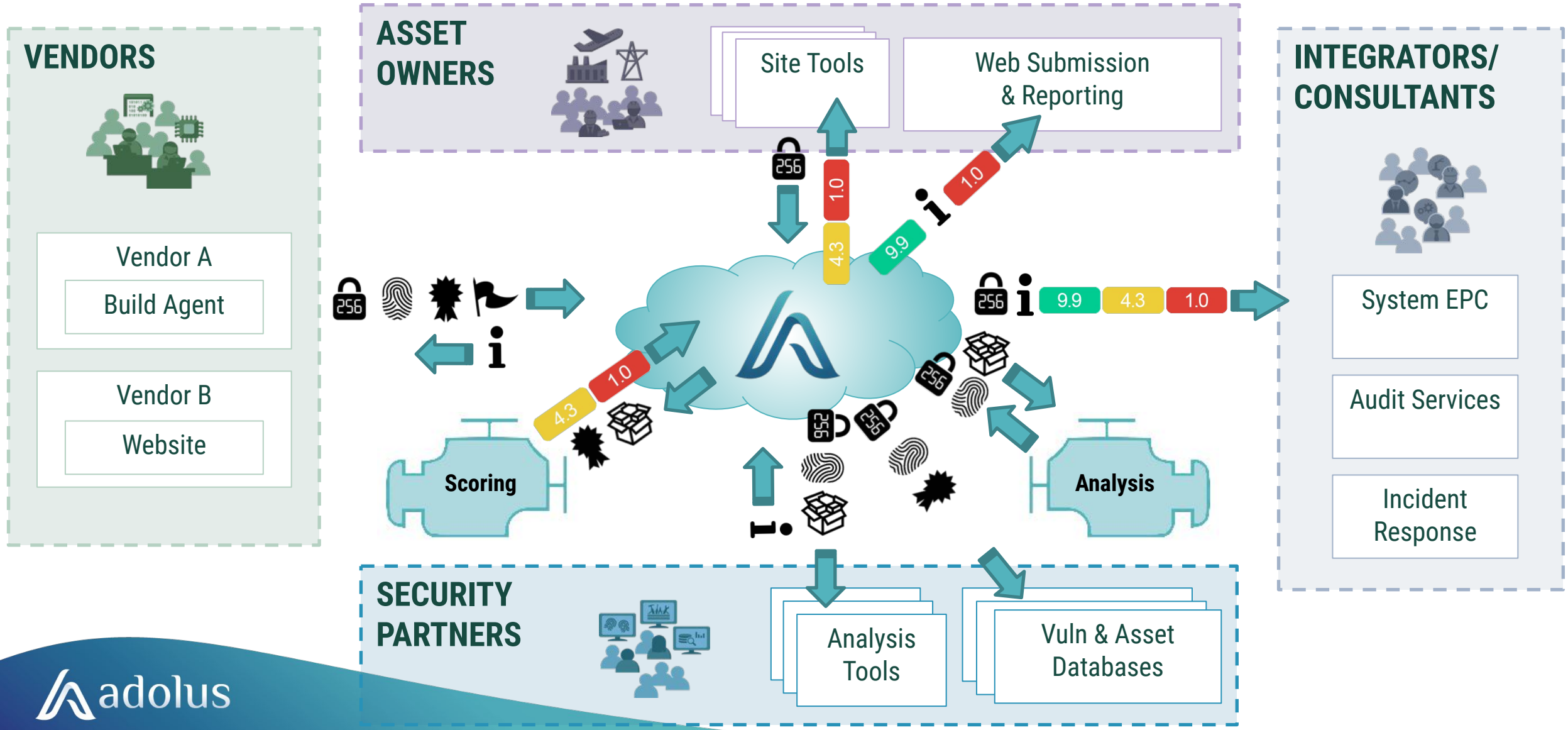


INTEGRATORS & CONSULTANTS

VENDORS

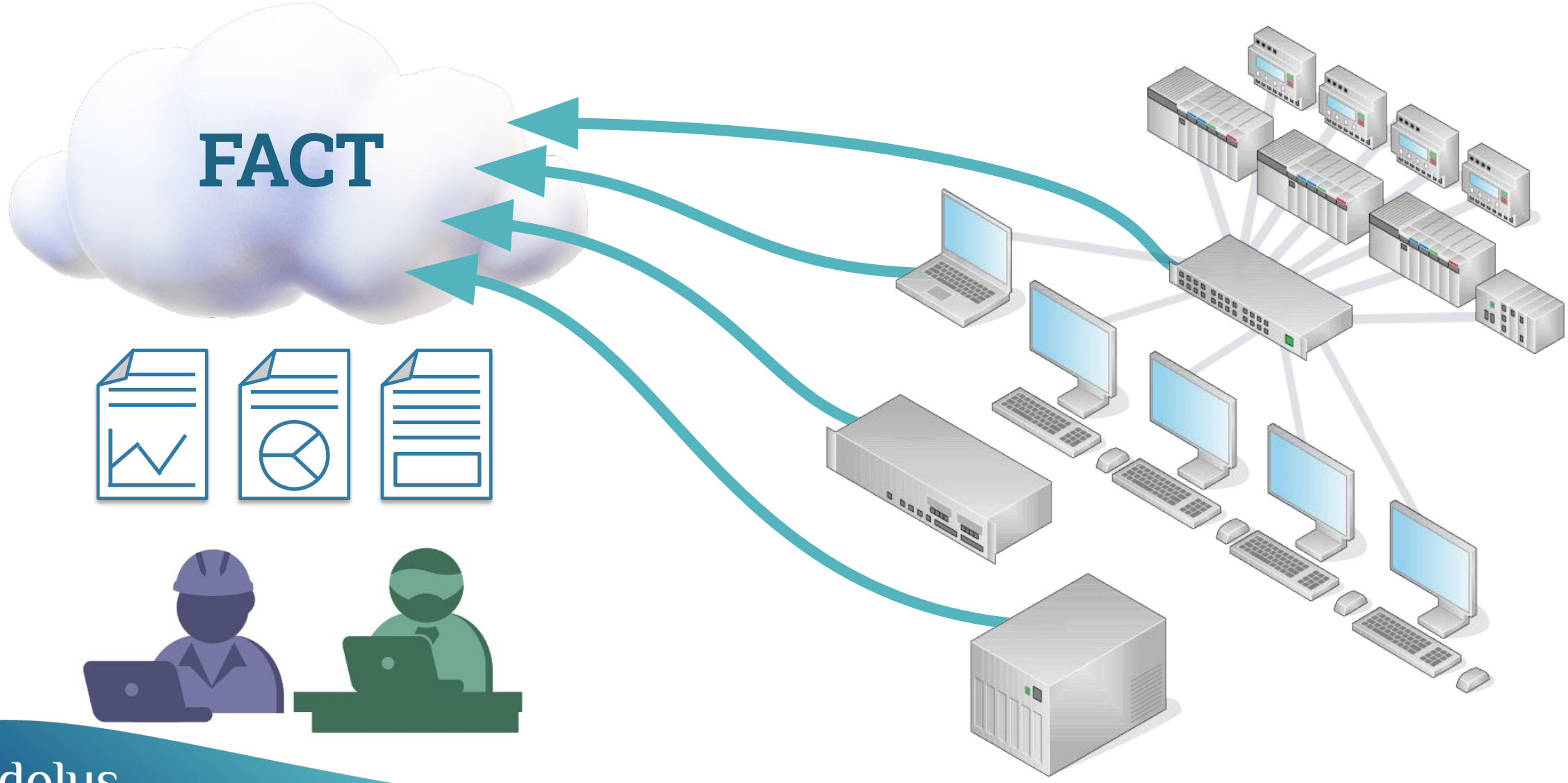
adolus

FACT™ Architecture



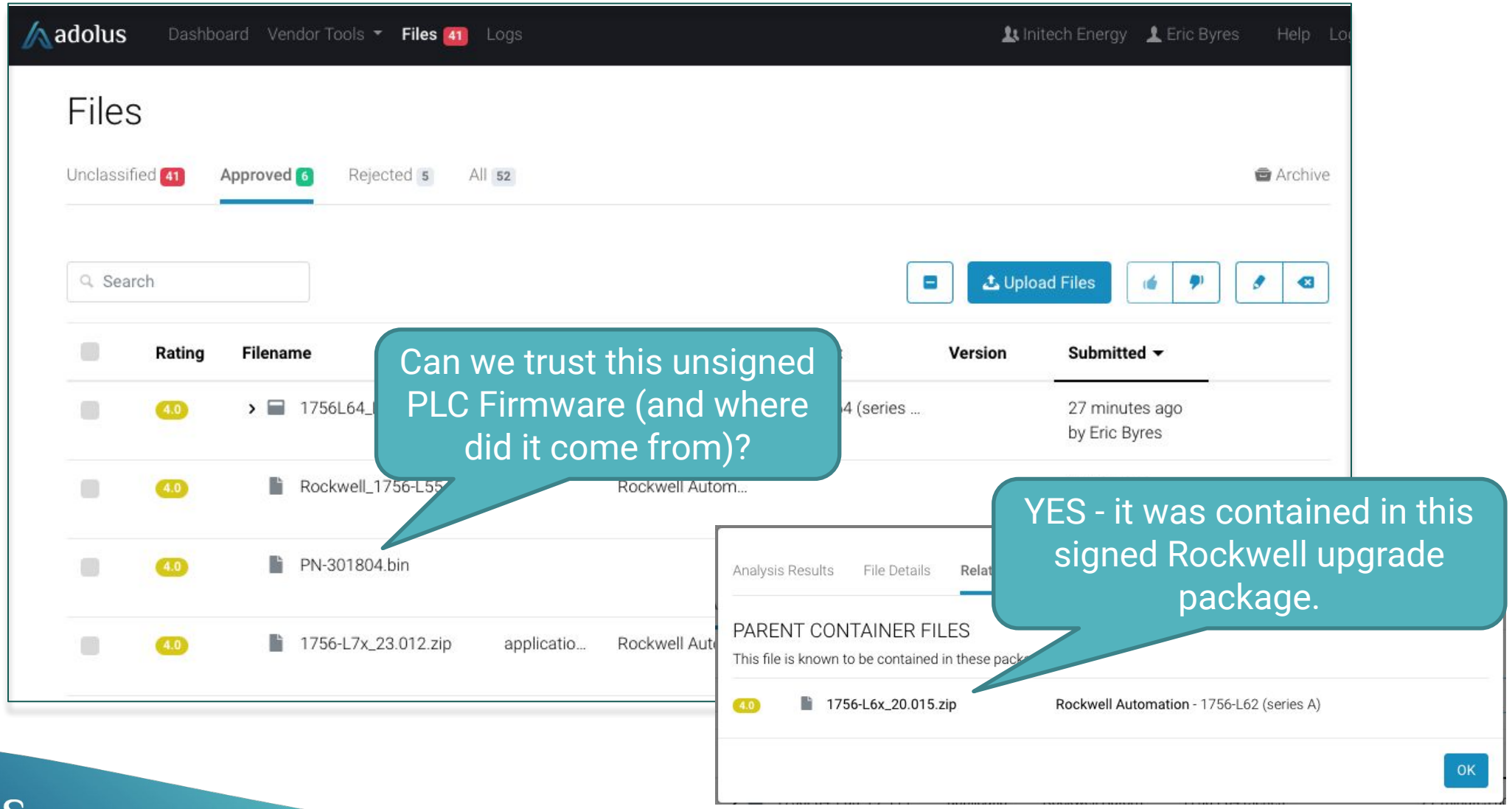
adolus

Plant Floor Software Discovery Reporting

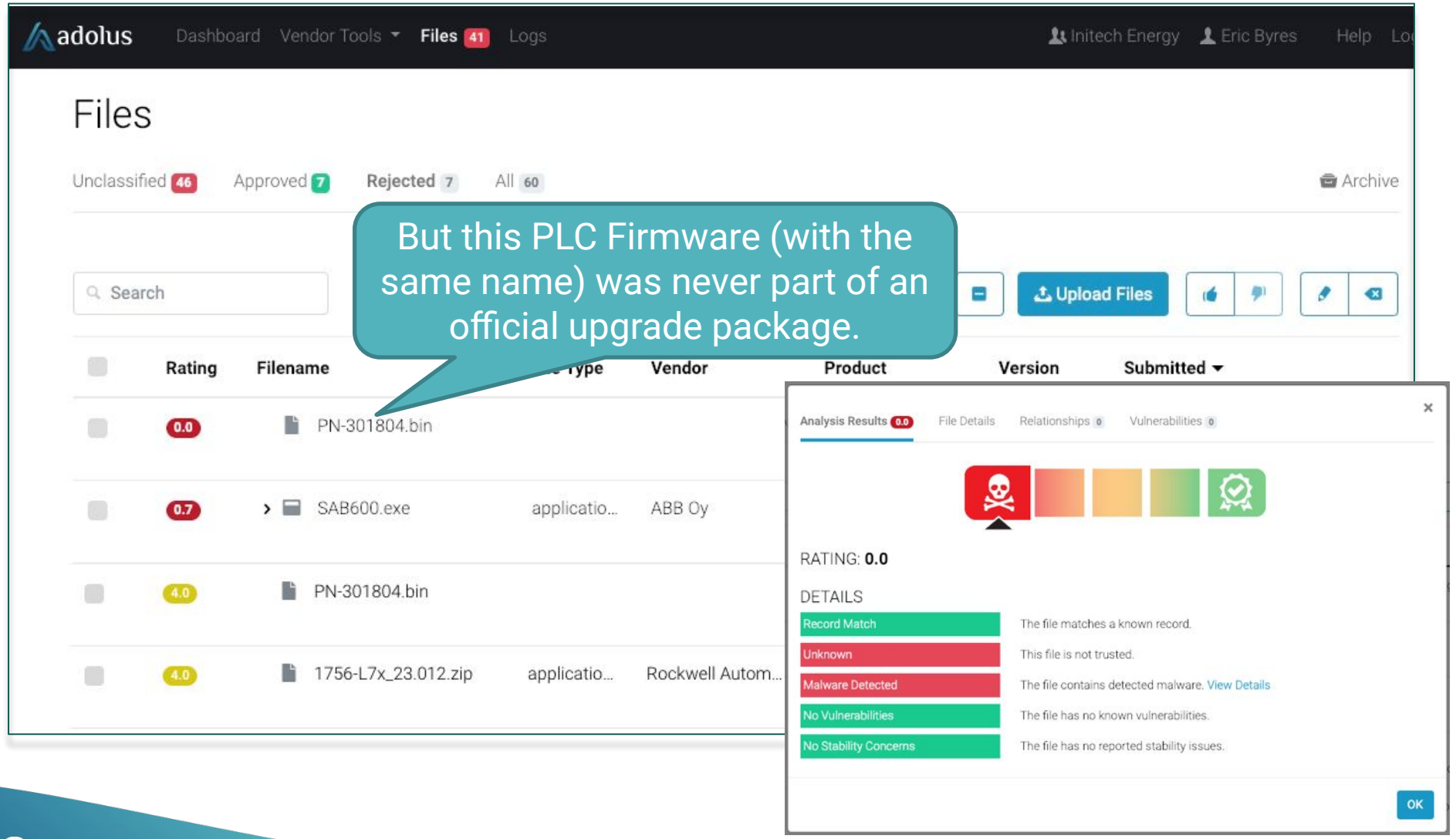


adolus

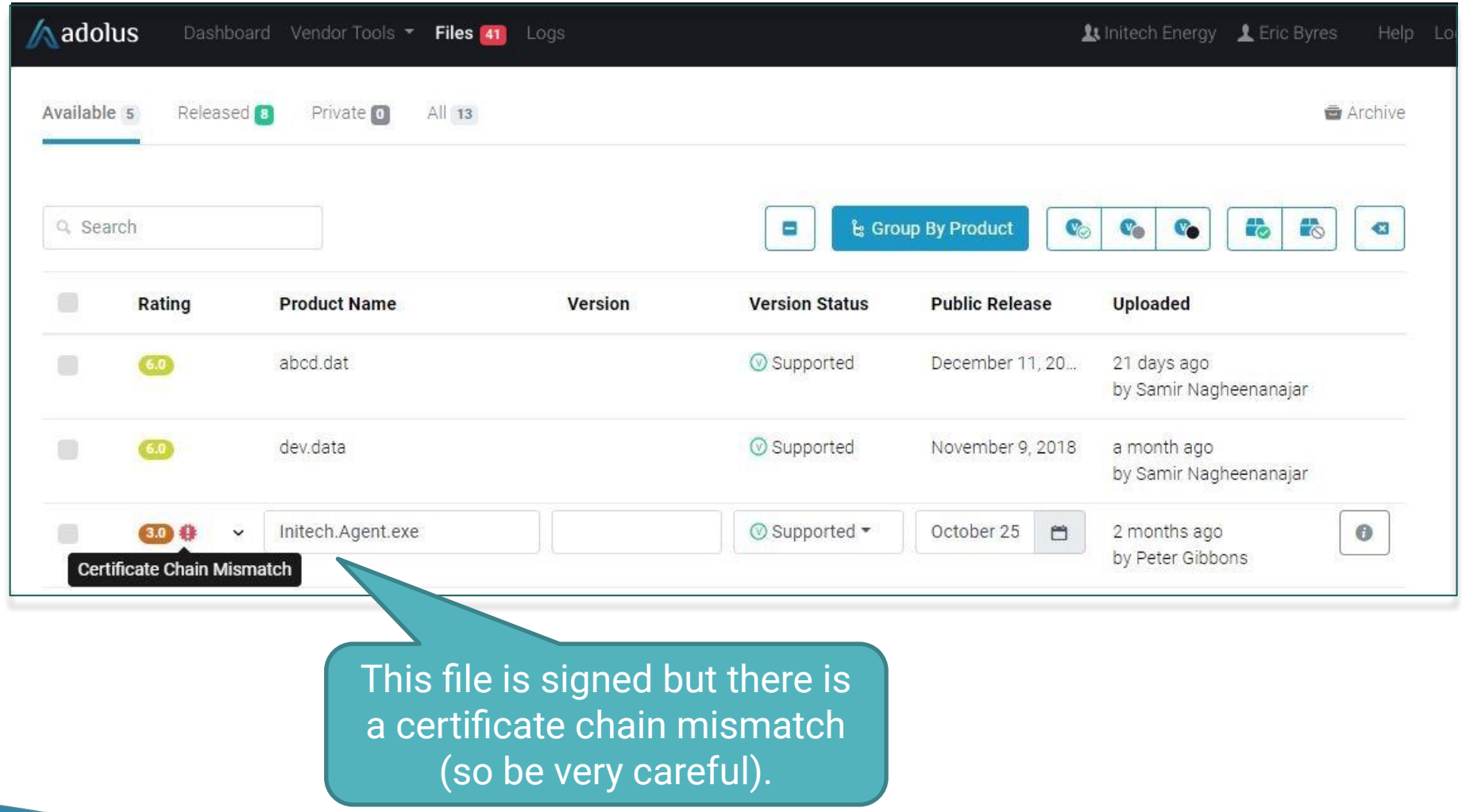
Checking Firmware Trustworthiness



Checking Firmware Trustworthiness

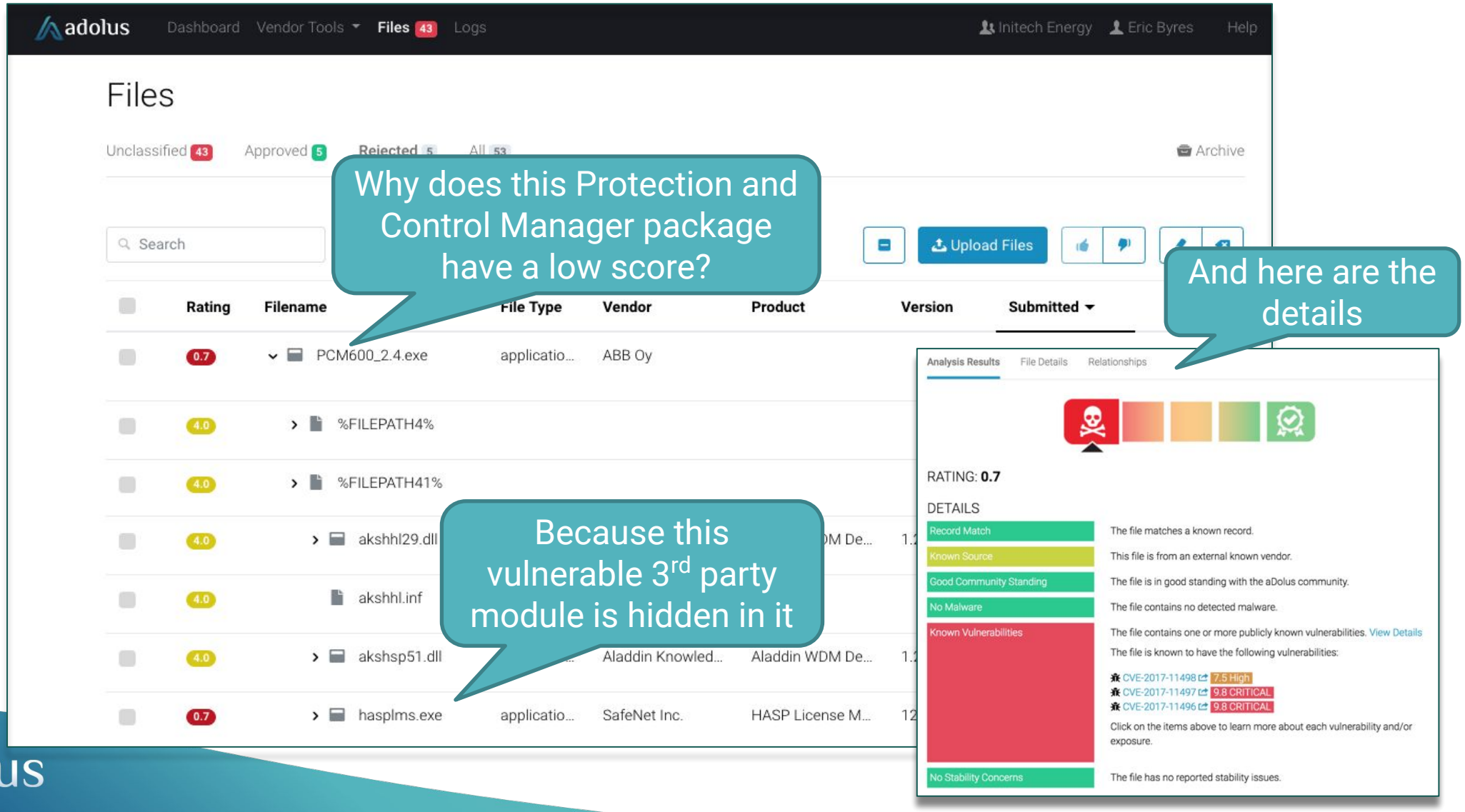


Validating Certificate Signing



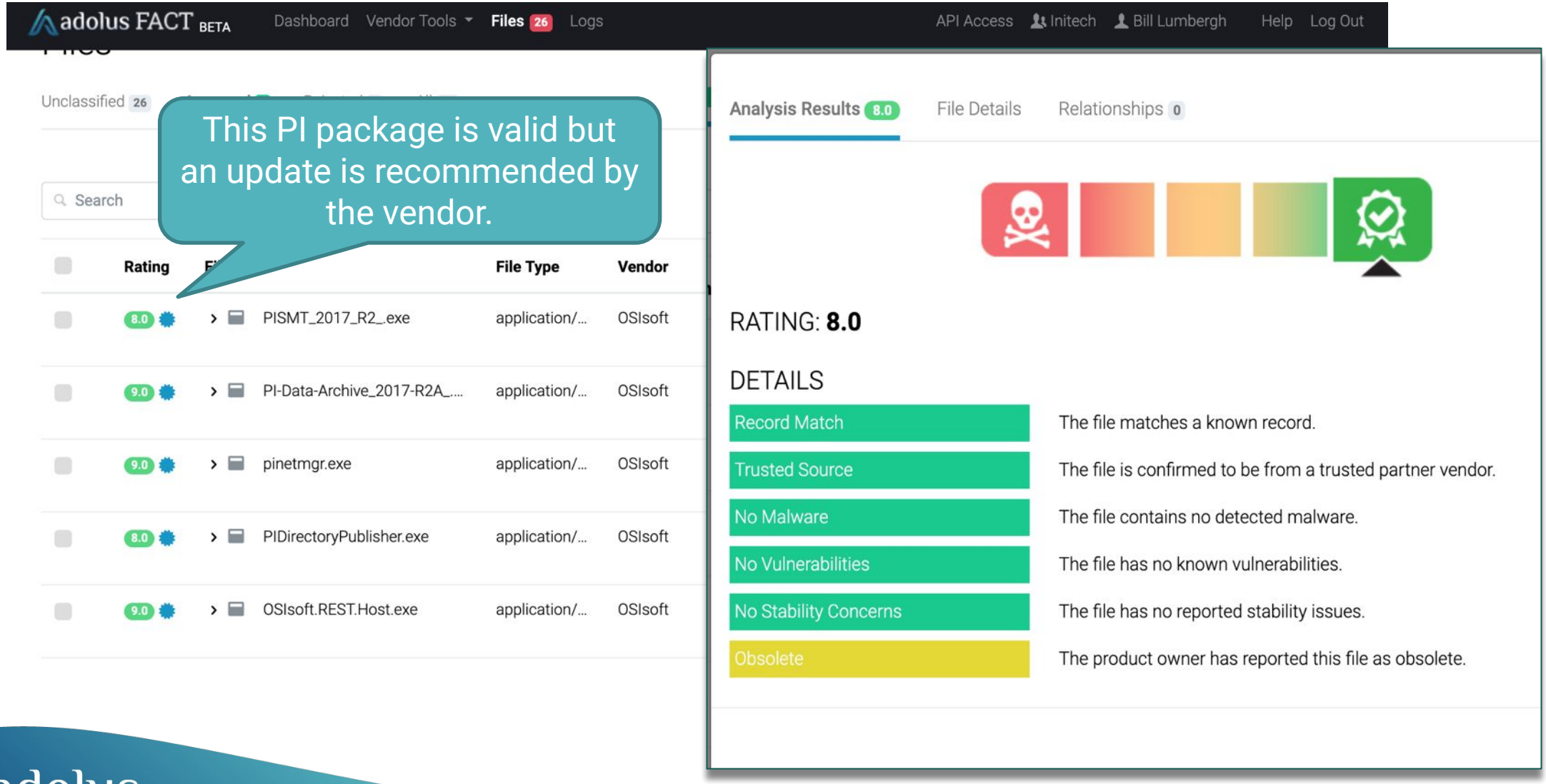
adolus

Finding Hidden Vulnerabilities



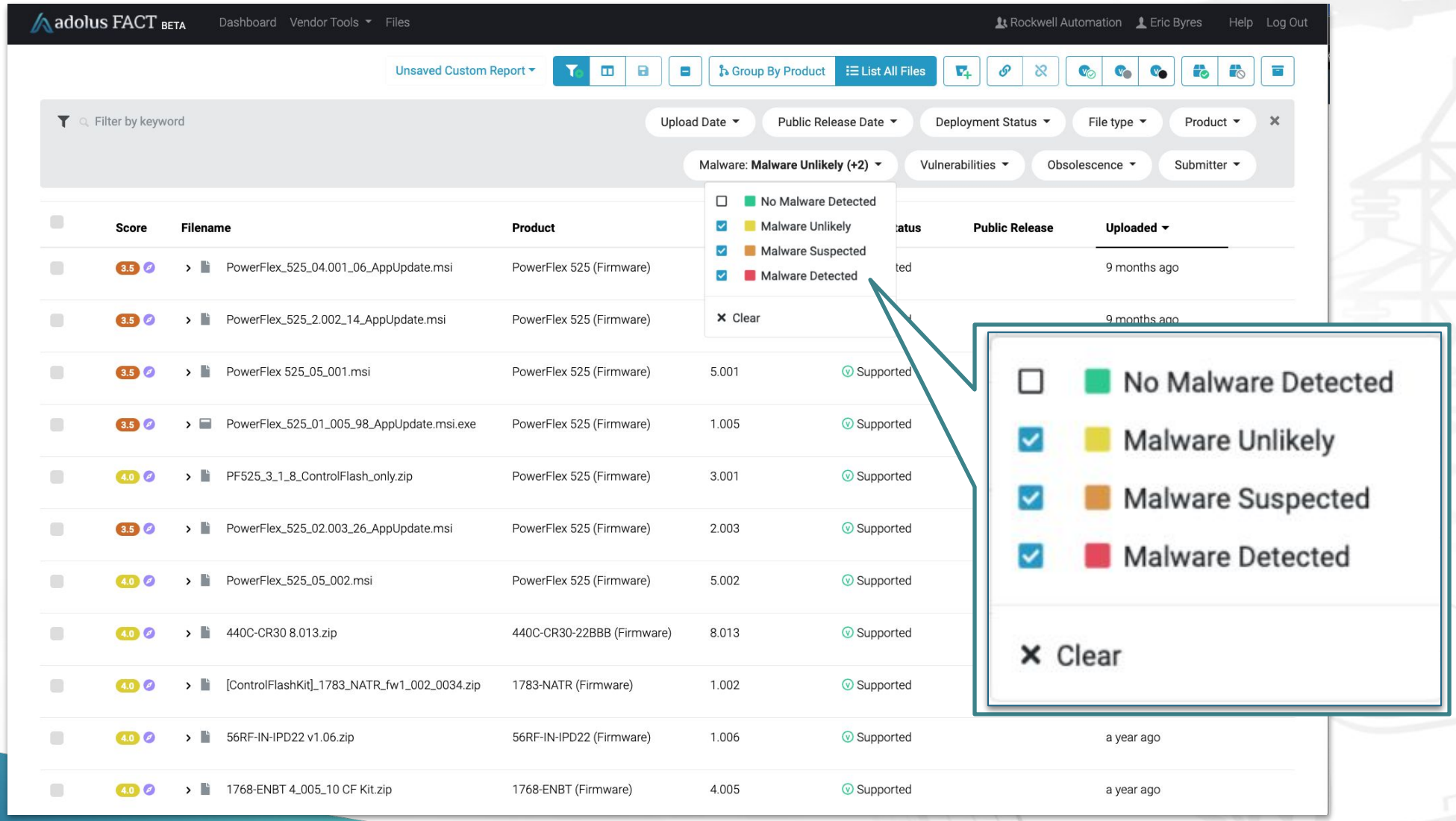
adolus

Firmware/Software Version Management



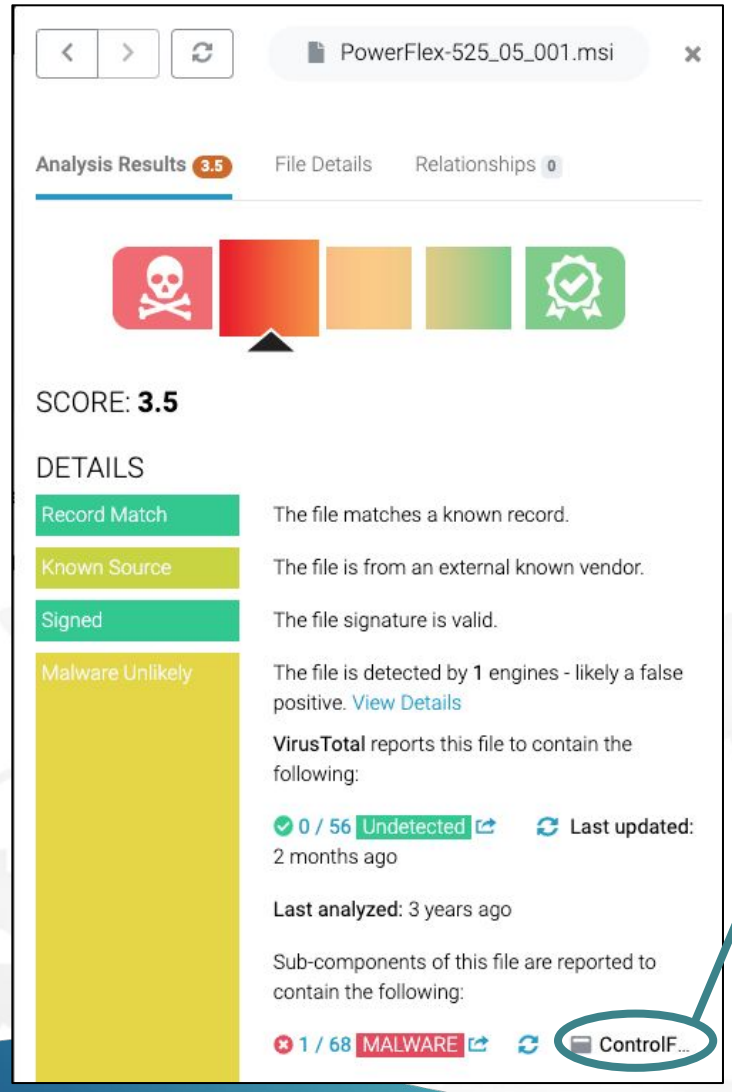
adolus

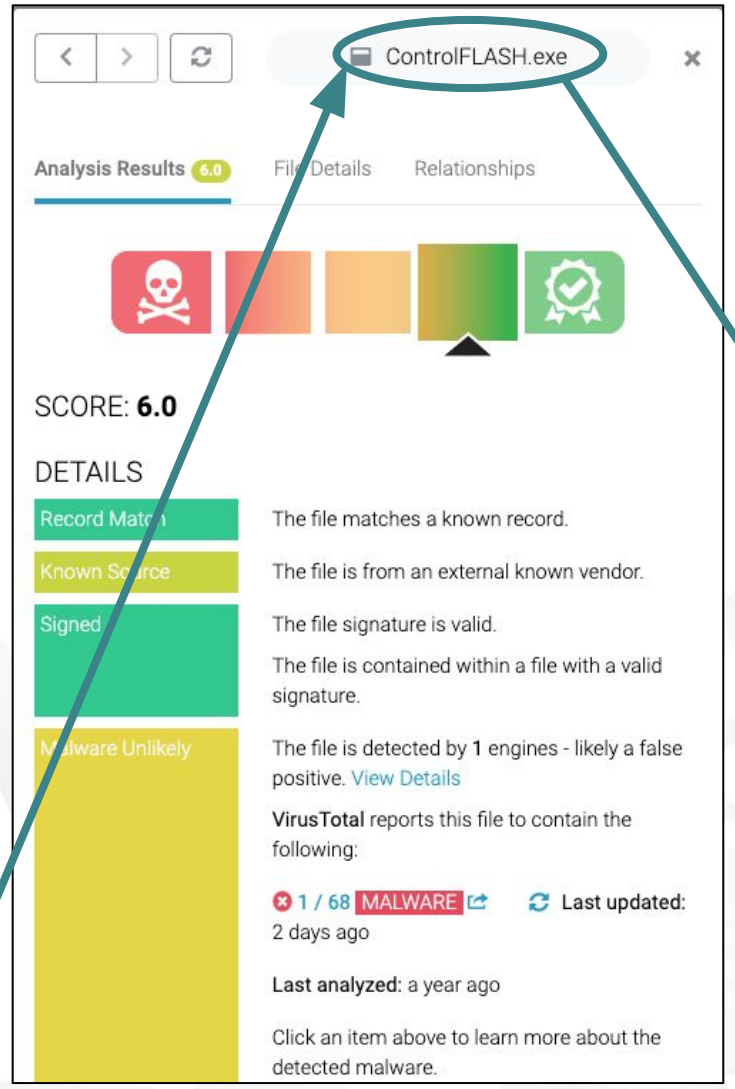
Helping Vendors Find Malware False Positives

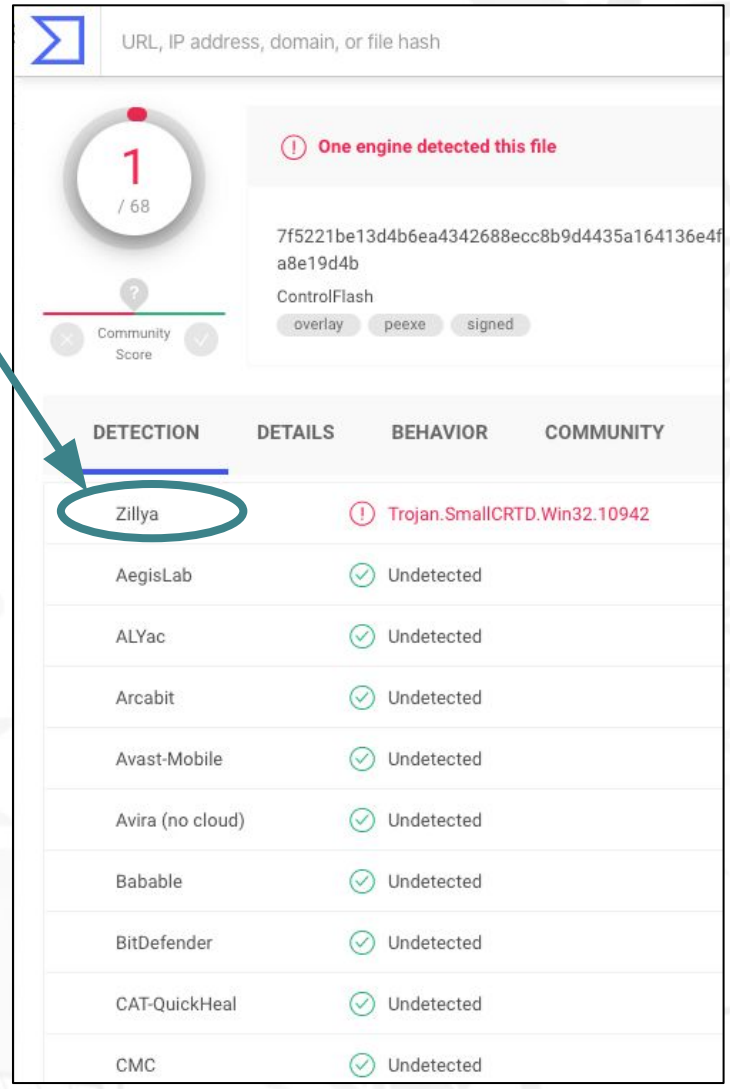


adolus

Helping Vendors Find Malware False Positives







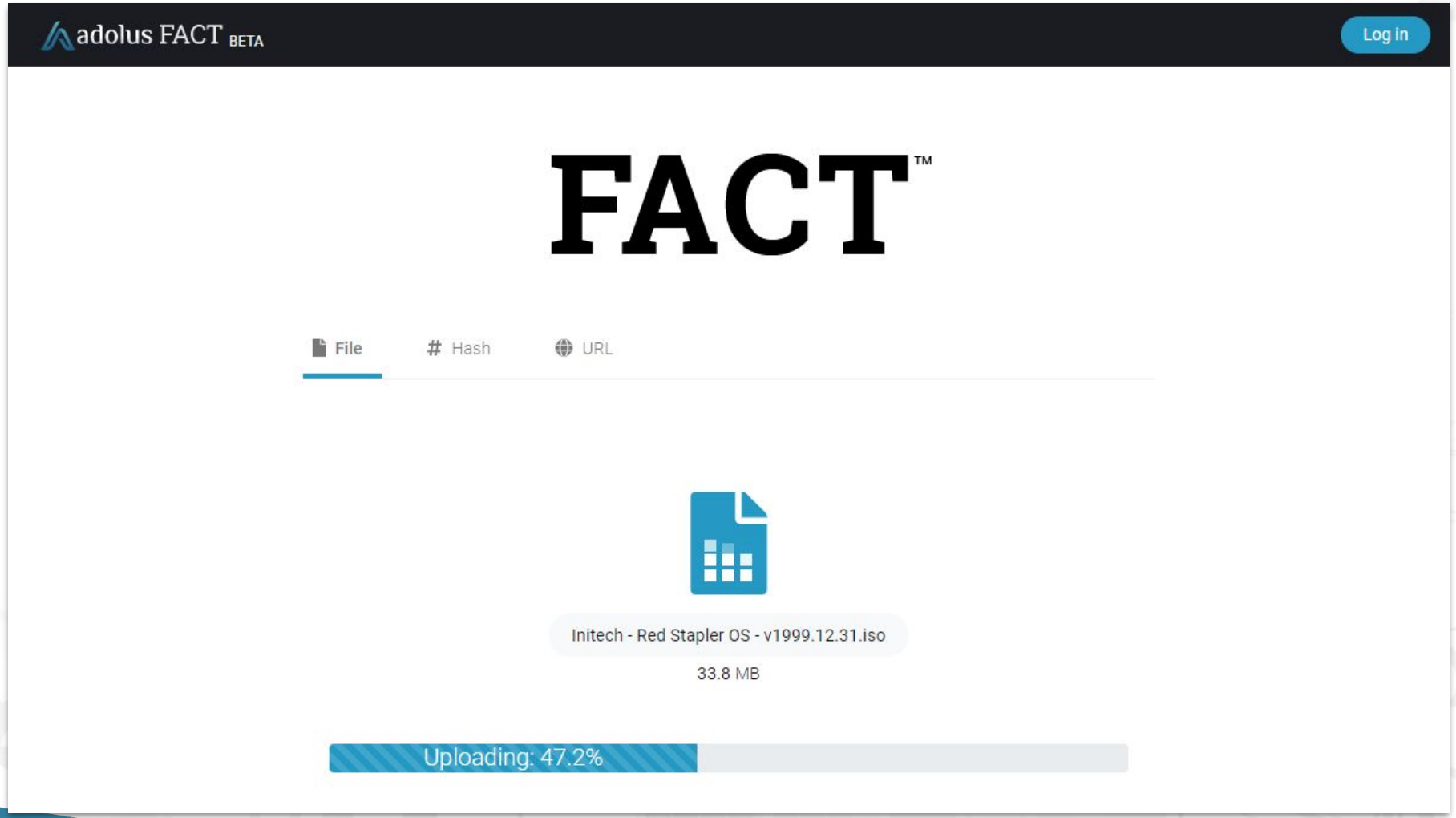
adolus

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

adolus

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



adolus


adolus
Contact us to become a member
www.adolus.com
info@adolus.com
1-866-423-6587
adolus