

The Impact of Cybersecurity & the CRA on Test Engineering

Márton Litkei
Sales Area Manager, NI

TechDay
2026 Slovenia



Software Ecosystem for Test

LabVIEW+ & SystemLink enable Test Engineers to use general purpose software alongside test-optimized software to meet their needs

Test-Optimized Software

General Purpose Software



Expansive T&M Ecosystem

Validated IP for measurement, signal processing, and control systems

Integrated T&M Expertise

Decades of T&M workflow expertise from system design to insights

Seamless Hardware Integration

Low-level control of measurement acquisition and timing

Software Community

Collaboration with broader software, data, and cloud teams

Trusted & Mission Ready

Professional software that prioritizes reliability, compliance, security, and maintainability

Purpose-built Data Platform

Integrated infrastructure to capture, manage, and analyze T&M data at scale

Performance Optimized

T&M systems require precise timing and deterministic execution

Open-Source Ecosystem

Access to IP and tools that enables rapid coding, including AI & Python

“Cybersecurity will drive
the largest investment in test and
measurement of our careers.”

Chief Engineer
Honeywell Aerospace
2019

Stuxnet - 2010

- Targeted SCADA systems
- Damaged nuclear program in Iran
- Nation state attack
- Caused centrifuges to vibrate apart
- Infected >200,000 systems
- Damaged 1,000 centrifuges
- Spread with USB drives on an air-gapped system



JLR – Cyber issues 2025

Jaguar Land Rover reveals shocking update in wake of cyberattack

The Jaguar Land Rover cyberattack: A manufacturing nightmare that could strike anyone

Share X f in



News and latest trends

JLR cyberattack: How one hack devastated Britain's Biggest carmaker

A sophisticated cyberattack has brought Jaguar Land Rover (JLR) to a complete standstill for over a month, creating one of the most devastating corporate cyber...

Panda Security | Oct 6, 2025 | 4 min read



September devastated the

s owns, had to shut down h.

t from Ford for \$2.23 billion

Rover

in the UK; largest UK auto

A sophisticated cyberattack has brought Jaguar Land Rover (JLR) to a complete standstill for over a month, creating one of the most devastating corporate cyber incidents in UK history. The attack demonstrates how modern manufacturers remain vulnerable to digital threats that can instantly halt multi-billion-dollar operations and threaten hundreds of thousands of jobs.

Key takeaways

- JLR has been shut down since August 31, losing up to £500 million per week
- Over 200,000 workers across the supply chain face job losses

It's the type of attack everybody fears and experts talk constantly about how devastating attacks seem rare. The recent example of an attack out of every IT

In this article

What happened in the JLR cyberattack?

How much is the cyberattack costing JLR?

Supply chain devastation

What is JLR doing to recover?

How did the UK Government respond?

What this means for British manufacturing

over to shut down key systems. Photograph:

er (JLR) returned to work on hoping to start making a limited a crippling cyber-attack.

action is at Wolverhampton in the s. Some workers are understood to

ok to restart limited production at ll in the West Midlands by the end h knowledge of the situation. Nitra

How production test is relevant?

Mocmex virus - 2008

- Designed to work around firewalls and security software
- Downloads files from remote locations
- Hides and randomly renames files
- Spreads through portable storage devices

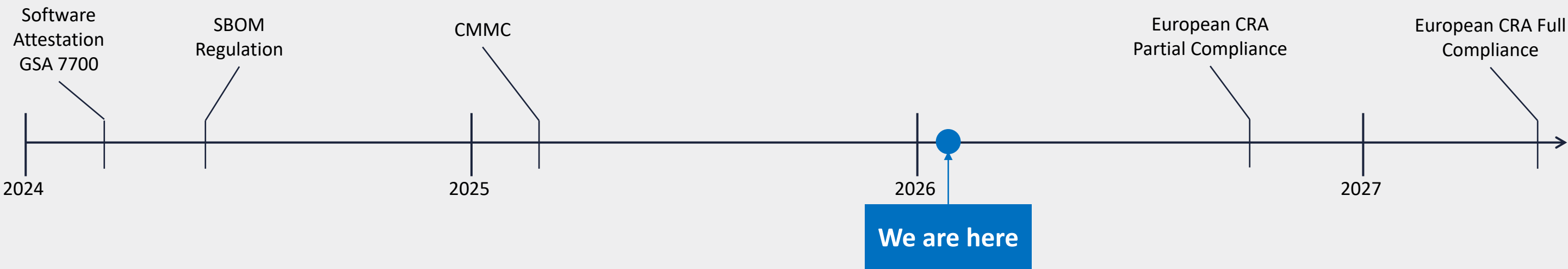
Hides on firmware in digital photoframes, spreads on home networks

How did this get into the photoframes?

Installed from infected testers



Increasing Security Needs



GSA 7700	May 2024	Software attestation letter required for software sold to US government. Vendor must attest that software was developed using a secure development framework.
SBOM (FAR 2021-017)	Dec 2024	New FAR rule that requires an SBOM for any software sold to the US government (Cyberthreat and Incident Responding rule)
CMMC (48 CFR 204, 212, 217, 252)	July 2025	Requires that any system handling government data meet NIST 800-171 controls and be externally audited, impacting NI and our customers.
European CRA / Partial	Sep 2026	Reporting obligations. Report any security exploited vulnerabilities.
European CRA / Full	Dec 2027	New CE mark required for any software/hardware delivered to EU. Requires secure default installation and delivery with no exploitable vulnerabilities.

CRA Summary

- The European Union is concerned with cybersecurity of all products sold into the EU.
- New legislation in the EU will require a new CE mark that proves the product is secure.
- The Cyber Resilience Act (CRA) establishes a **baseline for product security requirements** of products with digital elements made available within Europe.
- The CRA was published on November 20, 2024.
- Companies will must fully comply by December 2027 to continue to sell any product into the EU.
- **Any non-secure product will not be available in the EU.**



September 2022:
Text Proposed

December 2023:
Political Agreement
Reached

March 2024:
European
Parliament Adopted
Text

November 20,
2024: Law takes
effect

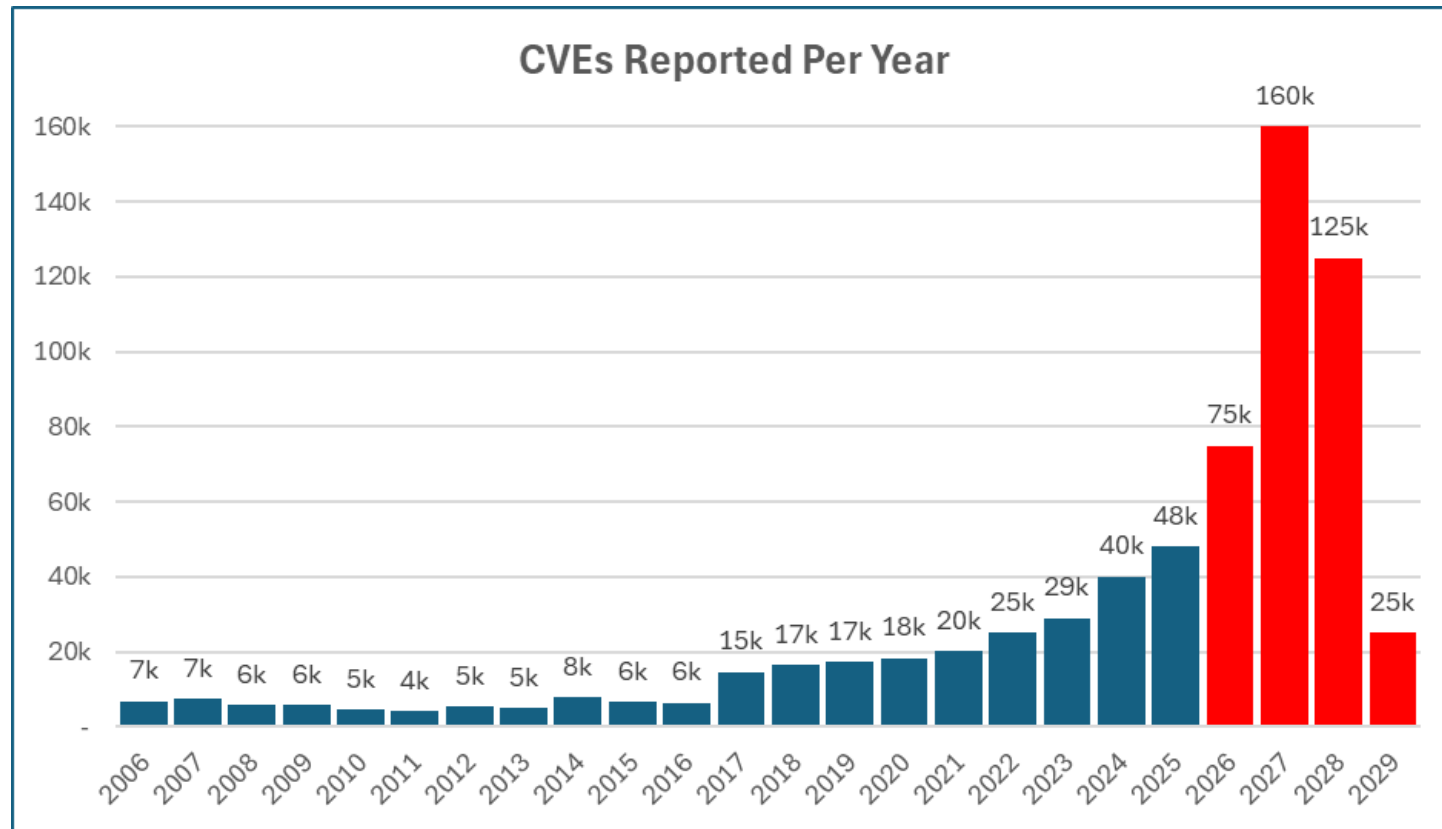
Sep 11, 2026:
Vulnerability & Incident
Reporting Obligations
Take Effect

Dec 11, 2027:
Remainder of
Obligations take
effect

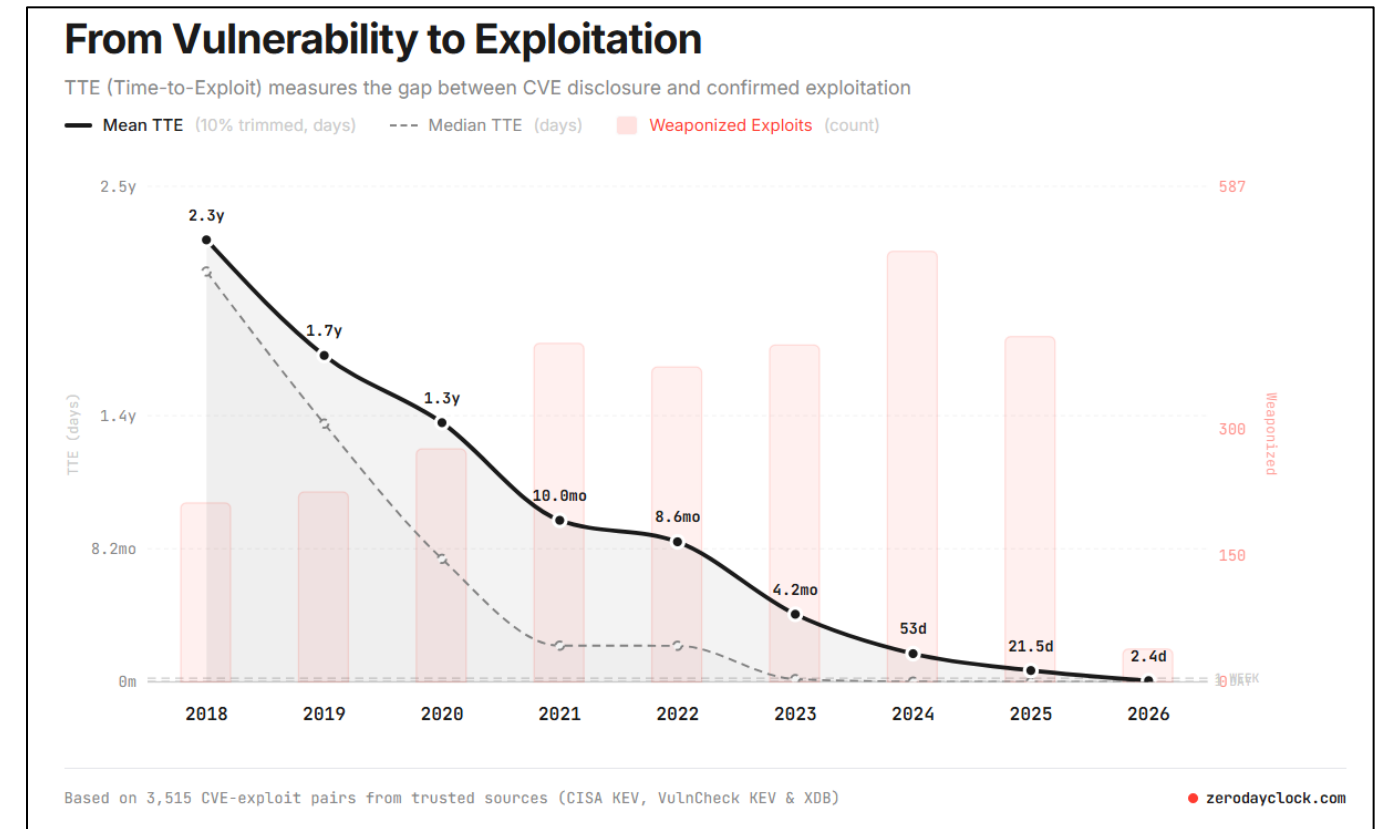
ATTORNEY CLIENT PRIVILEGED

We are here

The impact of AI on Cybersecurity

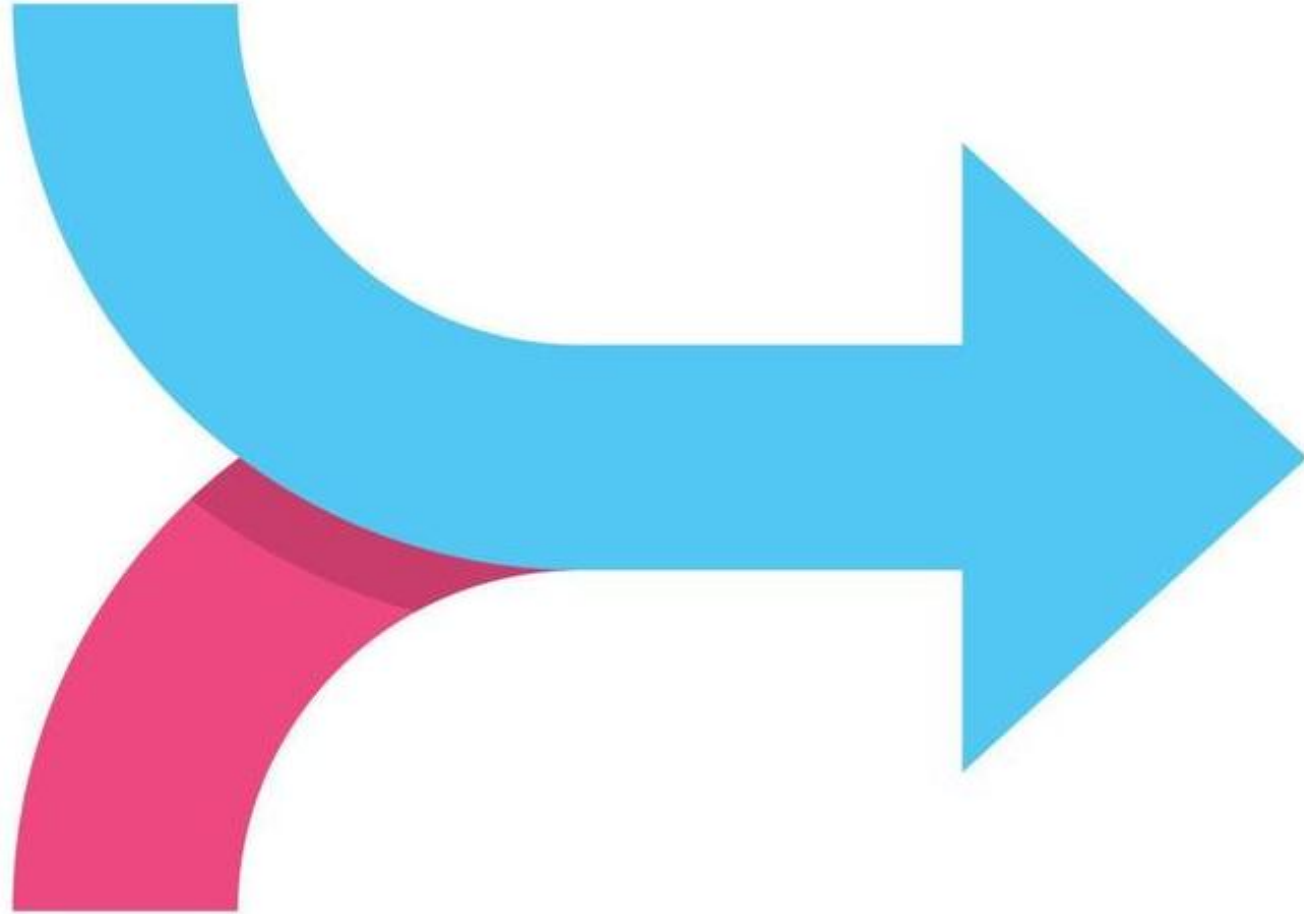


- New AI tools make finding, reporting vulnerabilities nearly effortless
- Hundreds of thousands of vulnerabilities will be found over the next few years
- Software companies will need to issue a large number of patches



- Near-future AI tools will simplify developing exploits, reducing the time end users have to update their systems
- Record break time: 27 seconds
- Users will not be able to wait years, months, or weeks to update systems

AI finding exponentially more vulnerabilities



CRA forcing “no vulnerability” software by Dec 2027

The Patch Wave:

- 2026-2027 will see a wave of patch updates from software vendors
- Plan now to update software by mid-2027 to secure systems
- Design systems to support frequent updates

Impact of security on test engineering teams

You will not be able to buy products that do not meet cybersecurity requirements.

- Test products
- Hardware and software
- Free software
- New and old versions

Check your supply chain

You will not be able to sell products if you do not meet the cybersecurity requirements.

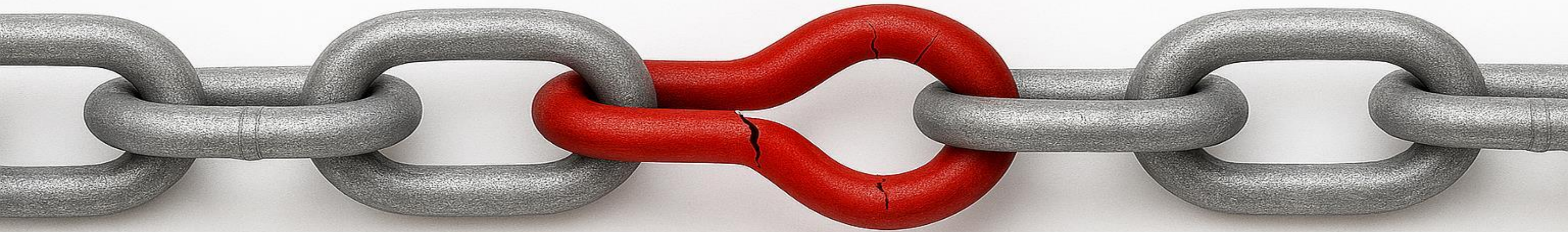
- Implement a secure development framework
- Document your product security
- Test for security

Establish secure development

Check your supply chain

Do Now:

Check your supply chain



Is your supplier working to be compliant with CRA?

What products will your supplier continue to support? Will CRA force EOL of some older components?

What versions will you be able to get, which will become unavailable?

Examples:

- A company may decide to EOL an older device rather than upgrade old components to comply with “zero vulnerabilities.”
- Companies will no longer be able to host older versions of software for download in Europe without updating those versions to comply



Do Now:

Establish Secure Development

Implement a secure development framework for test systems

- Adopt a zero-trust approach to security.
- Build a cybersecurity culture.
- Train your team on cybersecurity.
- Spend time on documentation, compliance, and architecture before building your test system.
- Build and document security through the project.
- Fund ongoing security updates.



**How NI
helps you meet
cyber-security
requirements?**

LabVIEW SBOM Generation

```
f{
  "$schema": "http://cyclonedx.org/schema/bom-1.5.schema.json",
  "bomFormat": "CycloneDX",
  "components": [
    {
      "bom-ref": "pkg:vipm/ni_lib_modbus_library@1.2.1.42",
      "description": "Modbus is a de facto standard for industrial communication which supports both serial- and TCP/IP-based communication. The core of the protocol consists of a function code (read or write) and data (what to read, what to write). Different packet forms are used, depending on the underlying bus, but that core set of information does not change.\r\n\r\nThis library allows for low-level access to that core function set and provides an API which includes both master (client) and slave device (server) functionality. ",
      "hashes": [
        {
          "alg": "MD5",
          "content": "cd7841a5d37a5c8cabd21adeba7d8ee5"
        },
        {
          "alg": "SHA-256",
          "content": "0e10bcc22fa54d8105eff690dc1b1d4d4ab14297ee74cd811de2c768e88b2a46"
        }
      ],
      "licenses": [
        {
          "license": {
            "name": "NI Sample Code License"
          }
        }
      ],
      "name": "ni_lib_modbus_library",
      "properties": [
        {
          "name": "vipm:display-name",
          "value": "NI Modbus Library"
        }
      ],
      "purl": "pkg:vipm/ni_lib_modbus_library@1.2.1.42",
      "supplier": {
        "name": "National Instruments"
      },
      "type": "library",
      "version": "1.2.1.42"
    },
    {
      "bom-ref": "pkg:vipm/oglib_time@6.0.1.6",
      "description": "The OpenG Time Library package contains several routines related to software time management.",
      "externalReferences": [
        {
          "type": "website",
          "url": "https://www.vipm.io/package/oglib_time/"
        }
      ],
      "hashes": [
        {
          "alg": "MD5",
          "content": "b7aabe378a358422d3646ce421f14829"
        },
        {
          "alg": "SHA-256",
          "content": "27b9c463cdae25c084c1336471afb2ffbbd3deddf7887278d7592a06e4c264e6"
        }
      ],
      "licenses": [
        {
          "license": {
            "id": "BSD-3-Clause"
          }
        }
      ],
      "name": "oglib_time",
      "properties": [
        {
          "name": "vipm:display-name",
          "value": "OpenG Time Library"
        }
      ]
    }
  ]
}
```

Shipping with LabVIEW 2026 Q3

- Generate SBOMs from LabVIEW Project
- Part of LabVIEW Pro
- LabVIEW menu option (File – Generation SBOM)
- Command line interface to integrate into automated workflows (CI/CD)
- Cyclone DX file generation

Sunshine - SBOM visualization tool

CycloneDX JSON file

Select a CycloneDX JSON file from your file system. All submitted data is processed locally within your browser, without being transmitted anywhere else.

Choose File

acme_modbus_slave.cdx.json

• If you do not have a CycloneDX JSON file available, but just want to see what output is produced by the tool see a sample HTML output [here with data enriched with EPSS and CISA KEY](#) or [here without enriched data](#).

• If your SBOM file is not in the CycloneDX JSON format, such as SPDX or CycloneDX XML, you can convert it using [CycloneDX Web Tool](#).

• If you prefer using a standalone CLI version [download it here](#).

Settings:

Enrich data with EPSS and CISA KEY

Show only vulnerabilities in CISA KEY

Note this setting can be used any when data enrichment is enabled

Show only vulnerabilities with severity:

Any

Critical

High or above

Medium or above

Low or above

Show only vulnerabilities with CVSS equal to or greater than:

Selected CVSS: 0.0

Show only vulnerabilities with EPSS equal to or greater than:

Selected EPSS: 0.00

Note this setting can be used any when data enrichment is enabled

Apply settings

Summary

No. of Components

Vulnerabilities

Main Component

Spec Version

Serial Number

Version

Tool

3

Max EPSS → 0.0

Vulnerabilities in CISA KEY → 0

Type → application

Name → Acme Modbus Slave

Version → 1.0.0.0

1.5

urn:uuid:85870216-2ae4-4249-bf21-5ad1d8b8b309

1

Component Type → application

Component Name → vipm-cli

Component Version → 2026.3.0

Components table

Show 10 entries

Copy

CSV

Excel

Print

Component	Depth	Depends on	Dependency of	Direct vulnerabilities	Transitive vulnerabilities	License
Search Component	Search Depth	Search Depends on	Search Dependency of	Search Direct vulnerabiliti	Search Transitive vulnerat	Search License
ni_lib_modbus_library 1.2.1.42	1	-	pkg:vipm/project_with_modbus@1.0.0.0	-	-	NI Sample Code License
oglib_time 6.0.1.6	1	-	pkg:vipm/project_with_modbus@1.0.0.0	-	-	BSD-3-Clause
pkg:vipm/project_with_modbus@1.0.0.0	root	oglib_time 6.0.1.6 ni_lib_modbus_library 1.2.1.42	-	-	-	-

Showing 1 to 3 of 3 entries

Previous

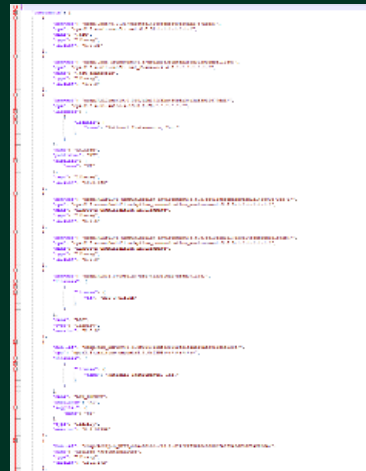
1

Next

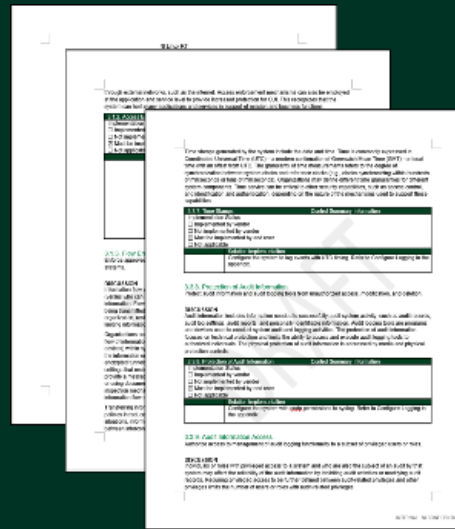
Vulnerabilities table



Letters of Volatility



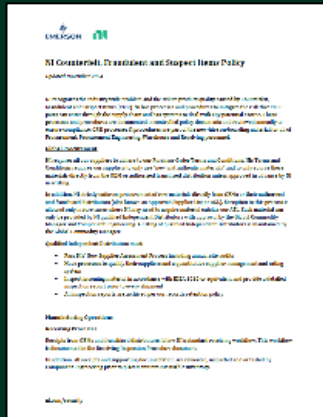
SBOMs



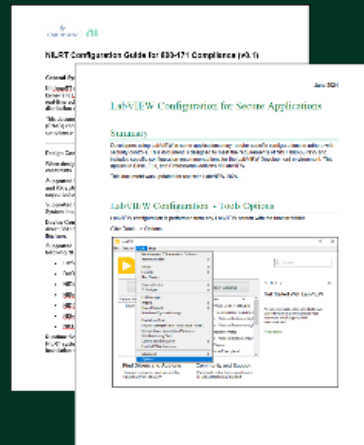
Compliance Documents



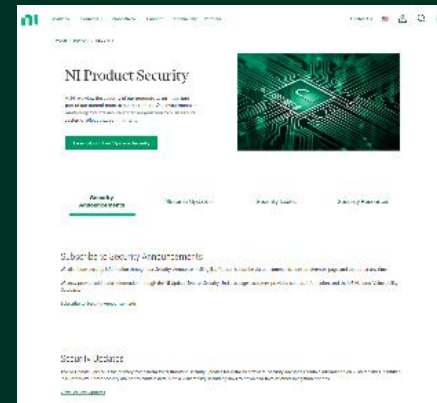
Security resources



Anti-counterfeit Measures



Configuration Guides



ni.com/security



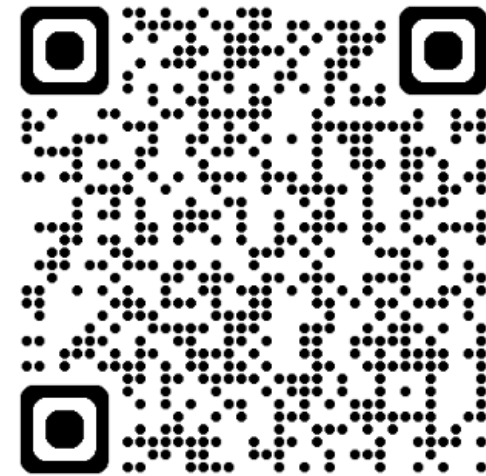
Security Forum



NI SSDF

Test System Security Forum

- Test developers must meet customer/company expectations to protect sensitive data.
- Test developers must meet government security regulations.
- Security teams force requirements on to test teams, but do not understand test.



*Join the Test
System Security
Forum*

AI is More Than Large Language Models



AI Agents



Cyber Security



LLMs



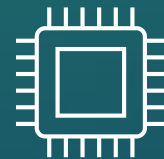
AI Inferencing



Virtual Test



Cloud Compute



GPU & NPU



System
Synchronization



High Speed
Networking



Big Data

Where do AI models run?

SaaS/Public Cloud



The LLM runs is hosted by a 3rd party provider. They pay all the hosting and GPU costs, and you pay them a usage-based fee.

Private Cloud



Your Company

The LLM runs in a cloud instance that is leased by your company. While a 3rd party hosts it, anything running in this cloud is only accessible to you.

On Premises



Your IT department owns and operates a farm of servers and GPUs inside your physical walls. The model and any AI applications run there.

What to ask your IT Dept about AI

Practical Recommendations

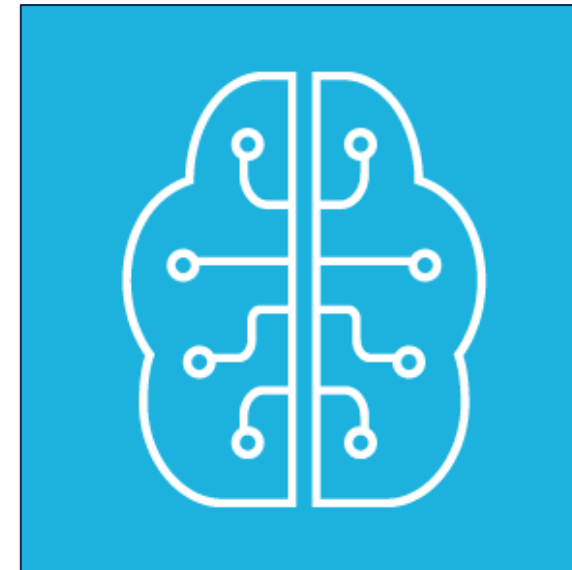
Is SaaS a possibility?

- Can you access SaaS (Software as a Service) applications in the cloud? Can you access SaaS beyond Microsoft 365?
- If the general answer is no, is there an exemption process?



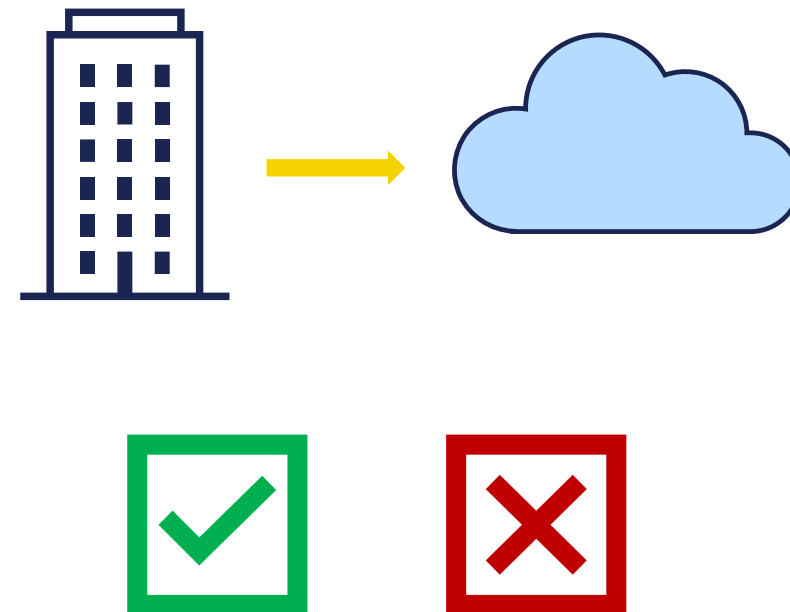
Can you use AI?

- Does your company let you use AI?
- Do you have a special AI that your company hosts, or can you use third-party tools such as ChatGPT by Open AI, Claude by Anthropic, or CoPilot by Microsoft?



Access to external applications

- When running applications on your premises or in your private cloud, can those applications access resources “outside your walls?”
- If no, is there an exemption process to open specific ports or traffic types?



NI Nigel AI Design Principles

Enterprise-Grade Security

Nigel is built on a secure cloud platform with enterprise-grade compliance and encryption safeguards.

Data Privacy and Anonymization

Uses anonymized data; no customer data is stored or included in training datasets.

Encrypted User Communications

User prompts are encrypted in transit and discarded immediately after response generation.

Transparency and Compliance

Full compliance with global privacy laws and transparency through source-linked responses.

Secure Software Development

NI adheres to ISO 9001 and integrates secure development lifecycle principles ensuring rigorous quality and security.

Controlled User Access

Access to Nigel requires ni.com login and active service entitlement, with regional restrictions for embargoed areas.

Data Protection and Privacy

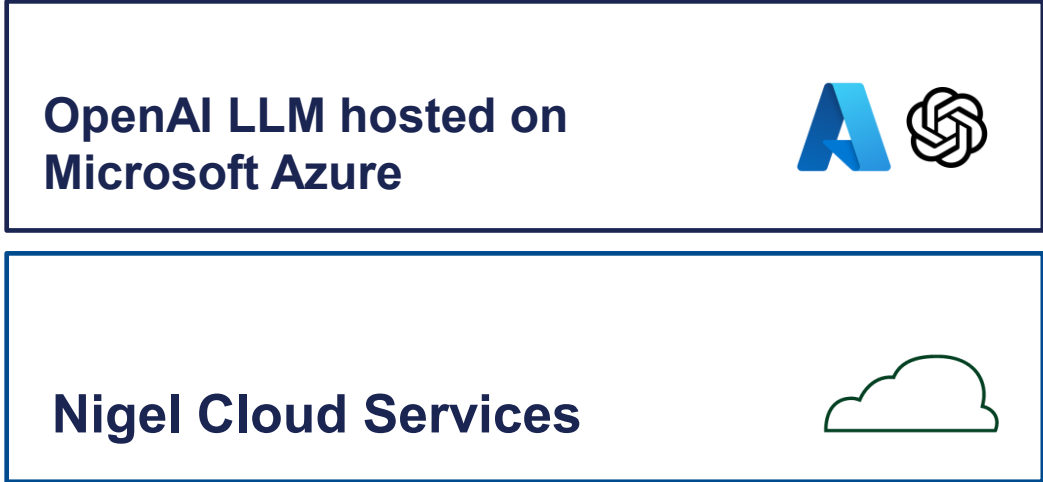
Nigel does not share data with third parties, and customer search data is excluded from cloud backups to ensure privacy.

Operational Resilience and Control

Organizations can disable Nigel via registry keys or installation options, maintaining control over AI availability.

Architected for Security At Every Level

Cloud

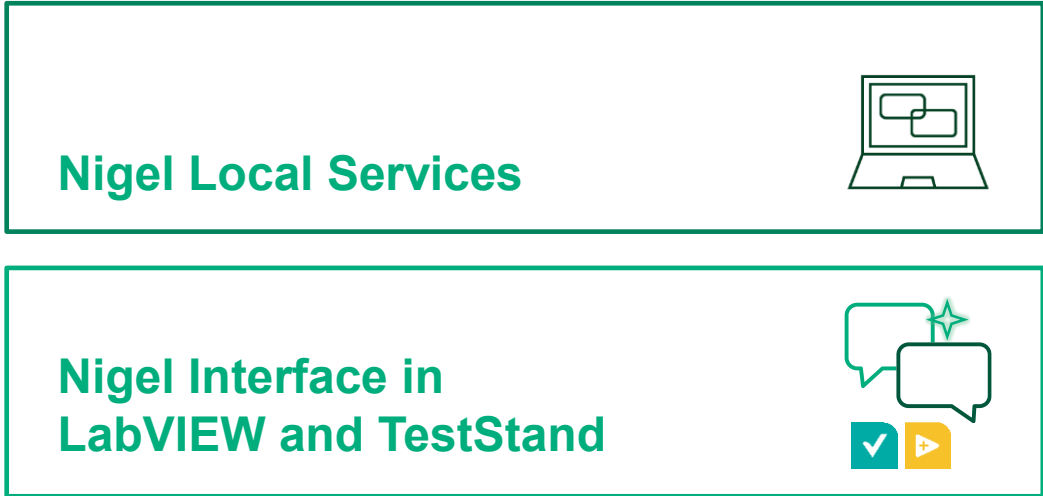


- Industry-leading OpenAI Models
- Enterprise reliability and security with Microsoft Azure

----- Encrypted TLS -----

- Encrypted communication (TLS)

Local



- Nigel stores only prompt data locally
- Nigel does not store customer data or train models on data



Q&A

Thank you for your participation!