Vulnerability Services

Efficient handling of vulnerabilities

SIEMENS

Neglecting vulnerabilities means taking risks

Operative challenges

- Companies need to reduce their exposure to vulnerabilities in the face of a growing number of cyberthreats. Identifying new vulnerabilities as soon as possible is crucial. But they are reported daily. How do I know if I am affected? And how to keep track of it?
- Manufacturers and operators of automation technology use a multitude of different software components and, thus, are also affected. Plus, the industrial security standard IEC 62443 2-3 recommends a broad patch management process. How can I implement a comprehensive and efficient solution?

Already known security vulnerabilities are one of the main entry points for cyber attacks. You need to keep on track with the vulnerabilities and react promptly.

Possible consequences

High manual effort and consequently neglecting already officially reported vulnerabilities

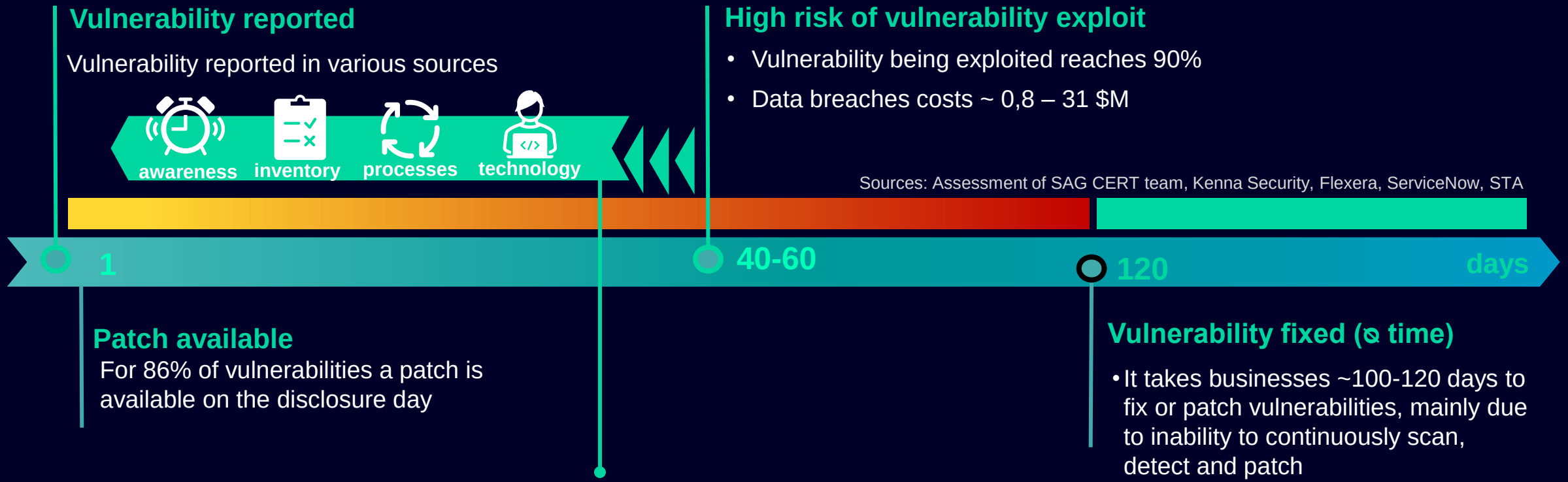
Stay unaware of real threats and consequently not trigger proactive measures (e.g. patching)

Significant financial loss due to cyber attacks exploiting existing vulnerabilities

SIEMENS

Companies need to reduce their exposure to vulnerabilities in the face of a growing number of cyberthreats

Typical timeframe of vulnerability remediation



SIEMENS

The increasing threat of manufacturing OT attacks

61%

of smart factories have experienced a **cybersecurity incident**.[1]

33%

of **cyber incidents** occur in manufacturing.[2]

65%

of **ransomware attacks** occur in manufacturing.[3]

75%

of IT architectures had **external connections to OT** in 2021.[4]

1 Manufacturing Automation – Growing cybersecurity risks for smart factories | **2** PMMI 2021 Assess your risk white paper |
3 Dragos 2021 ICS/OT Cybersecurity year in review | **4** Dragos 2021 ICS/OT Cybersecurity year in review

SIEMENS

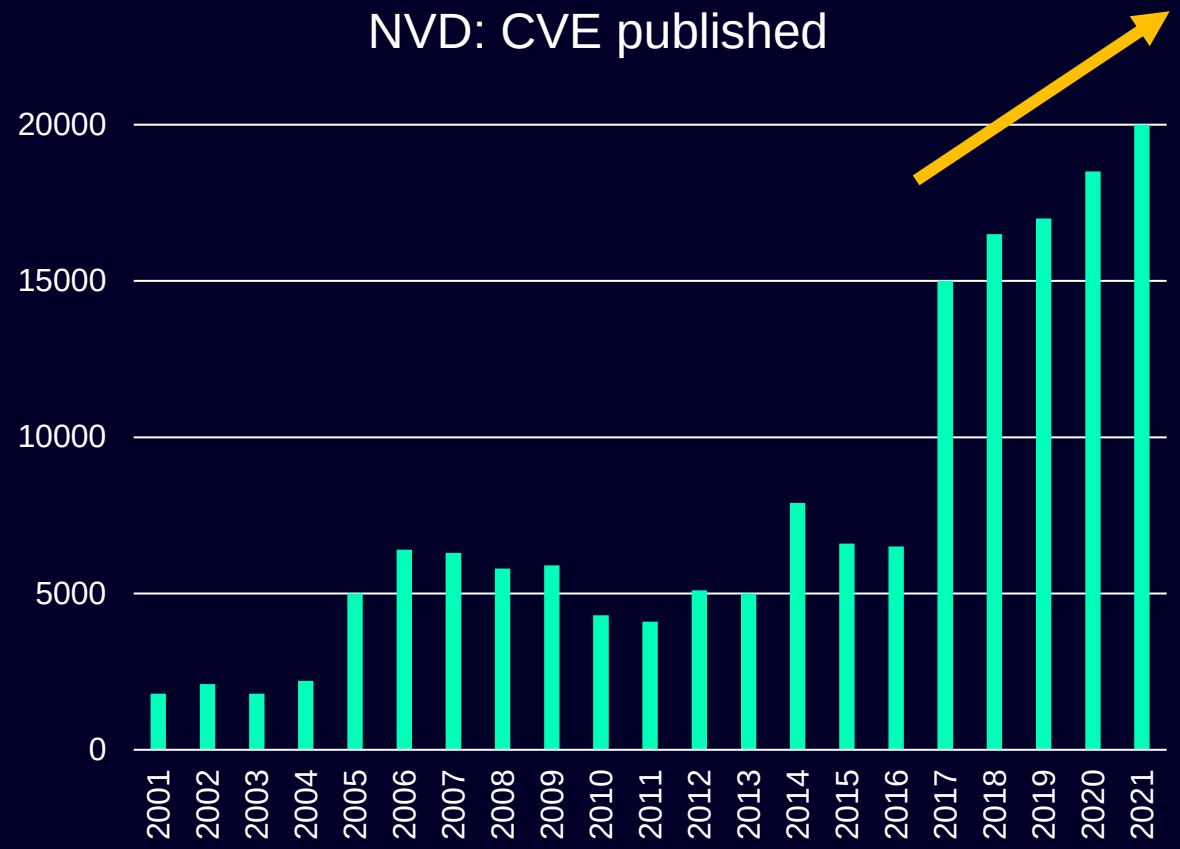
Cybersecurity challenges of industrial manufacturers: stay on top of the growing number of vulnerabilities

49%

ICS-related vulnerability growth rate, 2019-2020

Industrial control systems (ICS)-related vulnerabilities discovered in 2020 were 49% higher year-over-year from 2019.

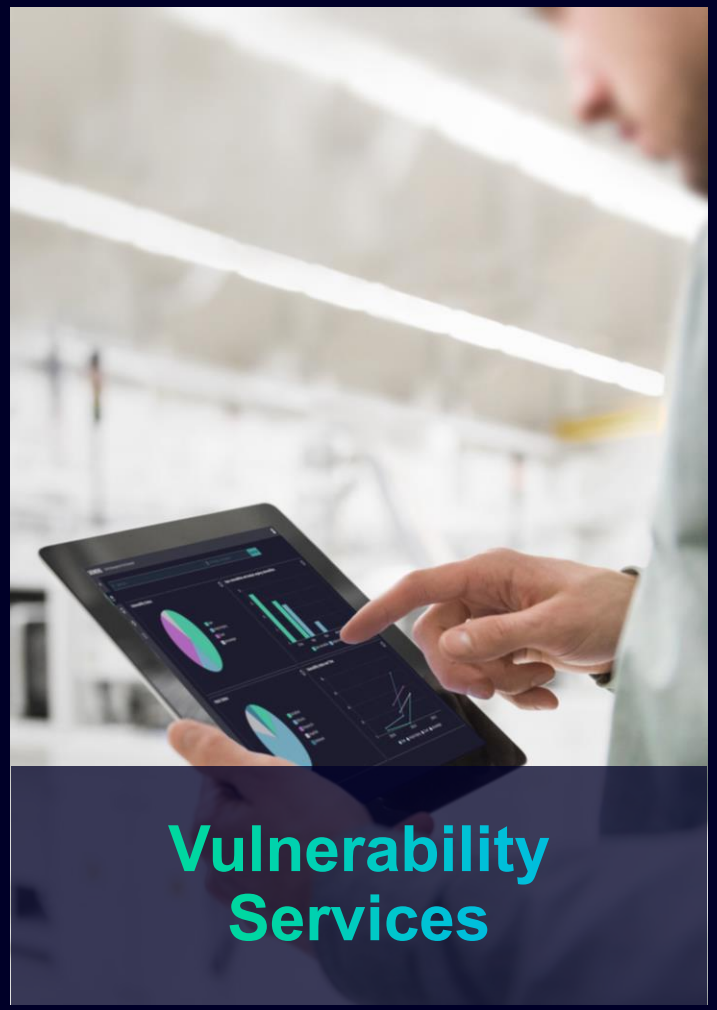
IBM X-Force 2021



How will your defense team handle the workload?

SIEMENS

Efficient handling of vulnerabilities with Vulnerability Services



Solution

Vulnerability Services empower you to secure your full stack product development, infrastructure and product portfolio by providing relevant, actionable vulnerability intelligence.

How does it work?

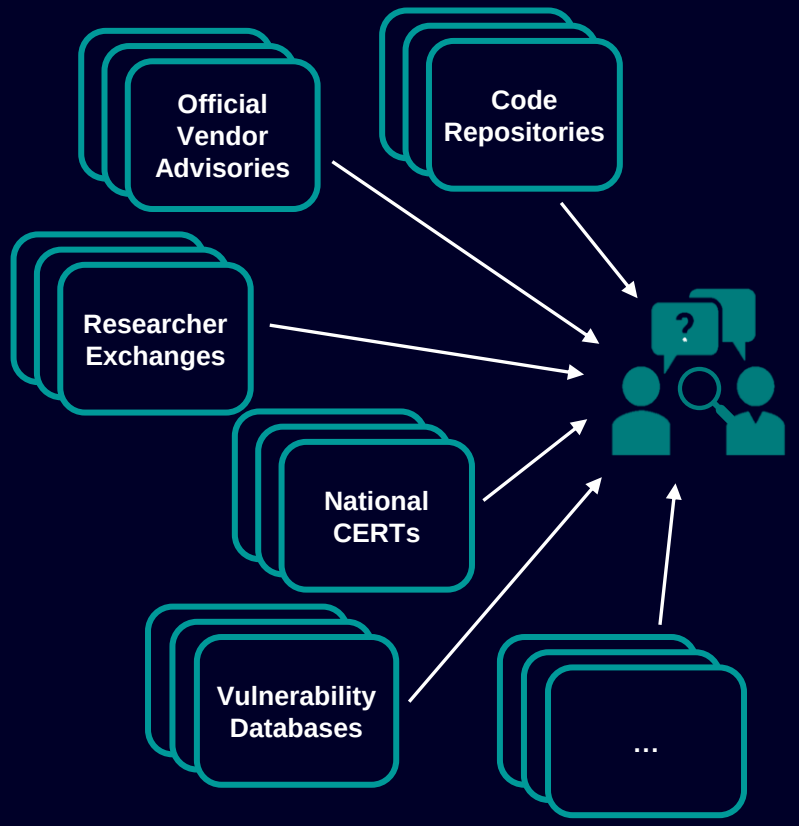
The basis of Vulnerability Services is a **unique monitoring approach** with thousands of security sources using advanced technologies in combination with in-depth analysis by acknowledged cybersecurity experts. As a result, you **receive alerts** about vulnerabilities affecting your individual system, enabling you to proactively manage your cyber risks. There are different options to receive these alerts:

- The **Management Portal** is a web-based tool offering a structured overview of relevant vulnerabilities for your components – with asset import functions as well as integrated reporting, dashboarding and notification features.
- With the **Application Programming Interface (API)** we offer a seamless interface to integrate the vulnerability intelligence into your existing vulnerability management tools and processes.
- You don’t have the personnel resources and look for a trustful partner to handle the monitoring and management of vulnerabilities? Then ask for our **Managed Service**.

SIEMENS

Vulnerability Intelligence – a sophisticated system

Vulnerability Services are based on a **unique monitoring infrastructure** using thousands of information sources, merged by security experts into consumable and actionable information.



Expert Analysis

1. Monitor information sources
2. Analyze new vulnerabilities
3. Aggregate patch/fix information
4. (Contact provider for clarifications)
5. Review risk score (CVSS) for each vulnerability
6. Compile consolidated vulnerability report

Data Basis

Highlights

- **Proven technology** on high Siemens quality standards to detect and patch vulnerabilities
- **Existing internal and external business** with major corporate customers
- **20 years of experience** protecting the world's most critical products and infrastructure

Asset facts:

- **1000+** of vulnerability information sources
- **200,000+ third-party** components in database, constantly growing as any component can be requested
- **1000+ active new users** per month (internal/external)

SIEMENS

Vulnerability Services offer a unique service that supports all types of components and a component-driven vulnerability mitigation intelligence

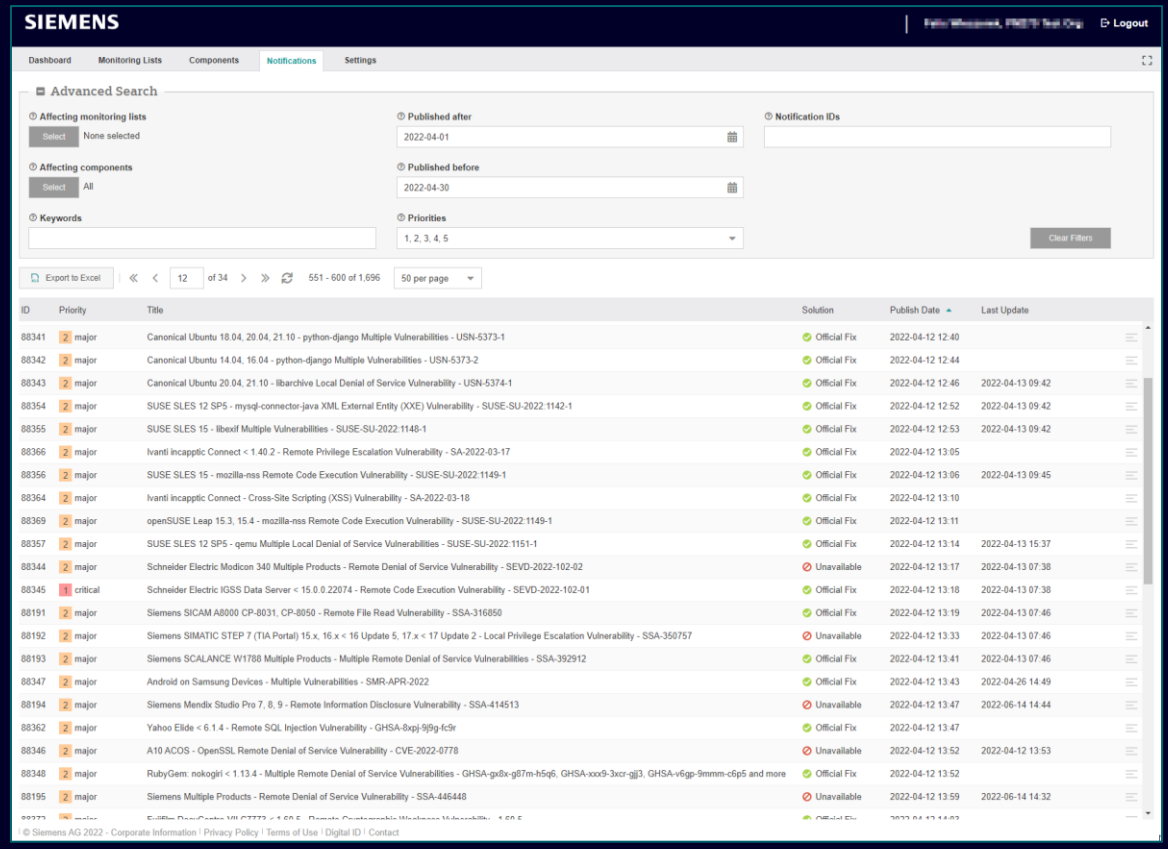
Coverage – most flexible component database

Hardware (Firmware) | Proprietary SW | Open Source SW | Legacy HW / SW | …

- Only vulnerability database on the market with **no component limitation** and **lifecycle information** (i.e. when component runs out of patch support)
- Components can range from **open source to proprietary SW** to **legacy HW** - as long as there is usable data input - service will be provided

Patch orientation – component-driven vulnerability monitoring

- Vulnerability monitoring starts once a component is added to our database. Starting from that point **vulnerabilities** are **matched to** the corresponding **fix**.
- **Minimize time to patch** with fast, comprehensive and solution-oriented alerts, allowing you **to quickly apply necessary mitigations**



SIEMENS

Vulnerability Services – the right fit solution for every use case

I need a tool for a structured overview of relevant vulnerabilities for my components. I also need to manage my components, track the mitigation process and report to my boss.

We already have vulnerability management tools set up in our plant. We now want to integrate sophisticated vulnerability intelligence into our processes.

I don’t have the resources for vulnerability management and look for a trustful partner to handle the monitoring and management of vulnerabilities.

Vulnerability Management...

SIEMENS

… the right fit solution for every use case.

Management Portal

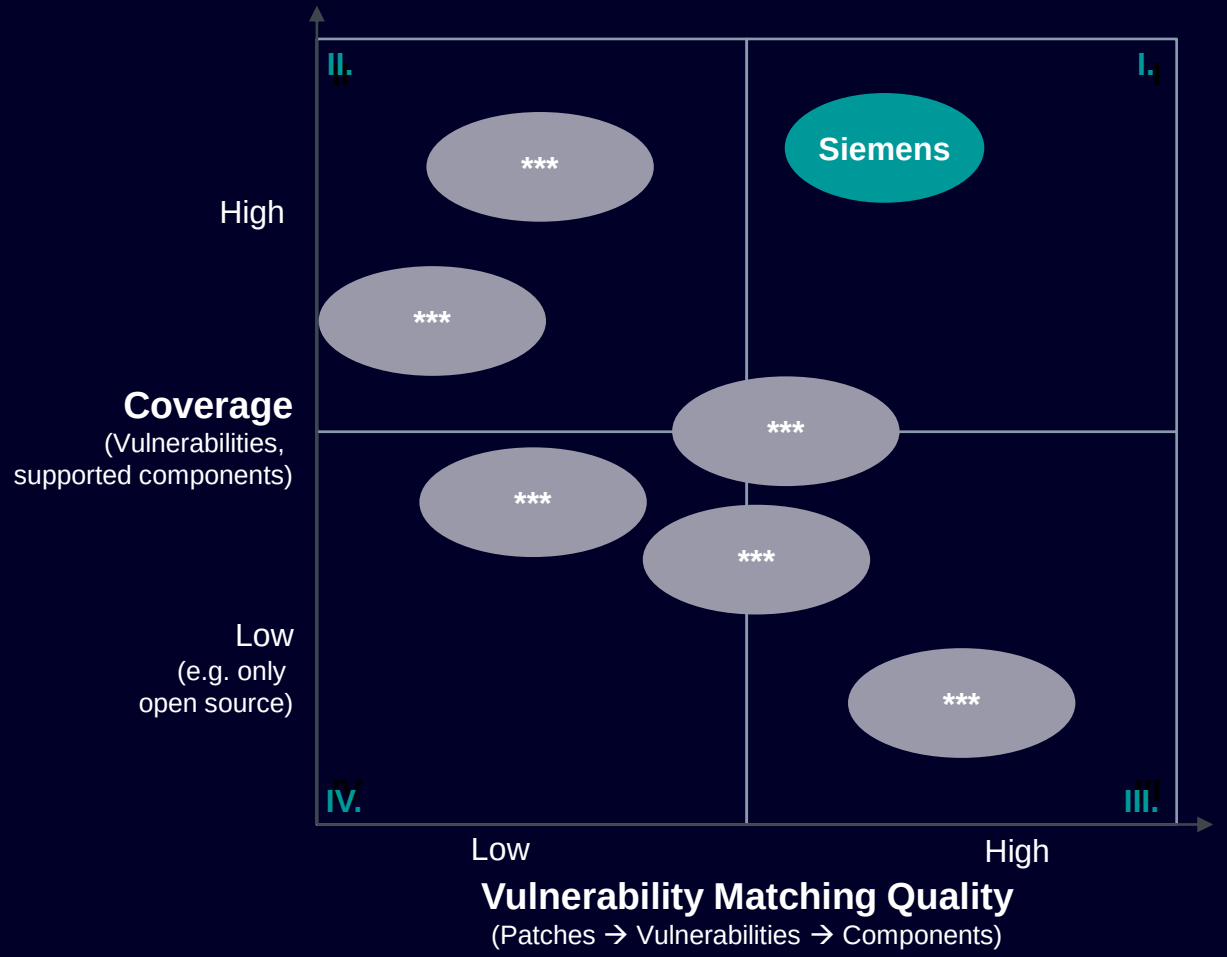
Data Service (API)

Managed Service

SIEMENS

Unique positioning in the market combining high vulnerability and supported component coverage as well as patch management quality

Competitive landscape



Rationale

I. **Siemens Vulnerability Services** is the only service providing high coverage and matching of vulnerabilities to patches for components as a one-stop shop

II. *** has a high coverage of vulnerabilities but has users to do heavy lifting of complex component matching. Notifications aren't solution oriented

III. *** has strong matching capabilities but limits scope of components on Open-Source frameworks

IV. *** has limited Vulnerability Intelligence solutions and focus on license compliance

SIEMENS

Vulnerability Services include application and infrastructure security as well as lifecycle intelligence

Your Product Security

- ✓ Supporting all platforms and package management systems
- ✓ Covering all OSS and COTS dependencies
- ✓ Comprehensive details including mitigating factors, workarounds, and more

Your Infrastructure Security

- ✓ Solution-oriented alerting simplifies patching
- ✓ Full asset coverage modelling entire IT/OT infrastructure
- ✓ Receive access-restricted vulnerability information

Lifecycle intelligence from suppliers

- ✓ Precise and reliable end-of-life (EOL) dates
- ✓ Know in advance about upcoming EOL events
- ✓ Guidance on required updates

SIEMENS

Best-in-class actionable vulnerability intelligence with Vulnerability Services

Broad component coverage applications and infrastructure

Faster patch management with solution-oriented alerts

Lifecycle information to plan ahead with replacements

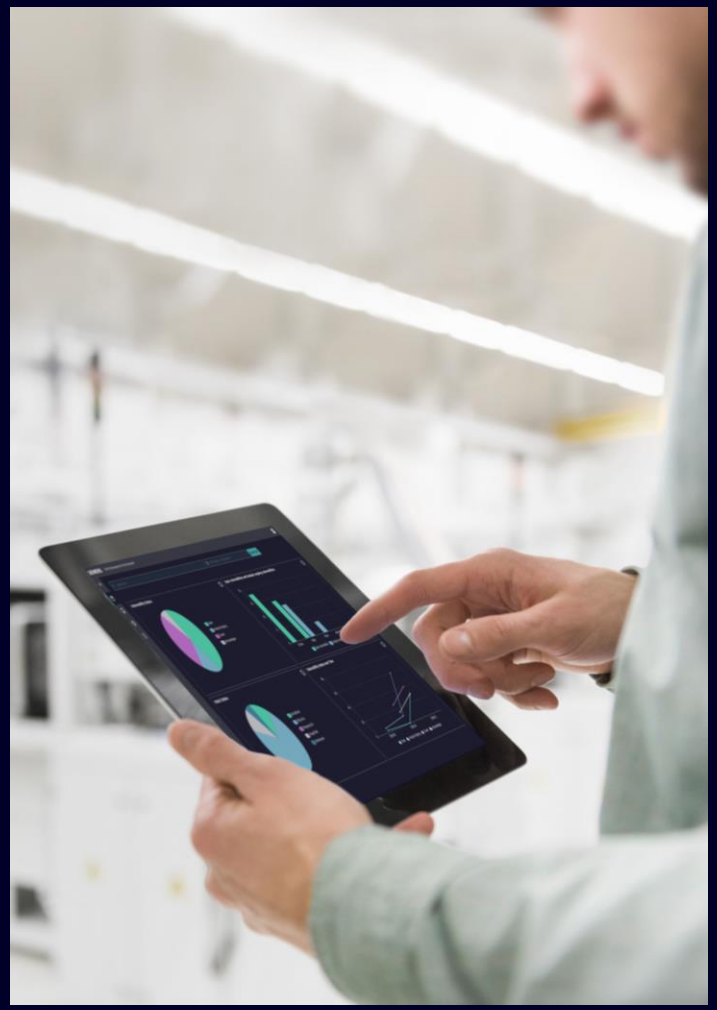
Easy integration into existing workflows or access via Web Portal

Cost effective consumption-based solution

Strong experience in protecting world’s most critical assets

SIEMENS

Why should you choose Vulnerability Services?



Instant transparency on vulnerabilities and minimized patch-times

Proactive management of cyber risks – easily integrated into your workflow

Reduced risk of costly exploits

SIEMENS

Siemens as reliable partner for Industrial Cybersecurity

We are the automation experts

We drive digitalization

We understand industrial security

We have specific industry know-how

We offer state-of-the-art technology and end-to-end services from a single source

“We make sure that you can focus on your core business.”

SIEMENS

Nokia Solutions and Networks Oy, Finland
Reduced risks with Vulnerability Services

Customer profile	Nokia Solutions and Networks Oy (Nokia) is a multinational data networks and telecommunications solution supplier headquartered in Espoo, Finland and a wholly owned subsidiary of Nokia corporation.
Customer objectives	As part of a broad security concept, Nokia needed a solution to stay informed about security vulnerabilities and end-of-life announcements affecting their software and hardware components as well as integrated applications.
Siemens solution	**Vulnerability Services – Data Service (API)** • Nokia receives complete vulnerability data in a timely way, specifically tailored to the customer's solution landscape. • Data aggregation from thousands of vulnerability information sources and continuous update of the centralized database. • Released security notifications contain key information such as CVSS V3 score, vendor web-link, patch status/hotfixes that shall be considered as part of a vulnerability management process. • More than 280,000 monitored software and hardware components and more than 30,000 security notifications per year for Siemens, third-party and open-source communities.
Customer value	• Reducing security risks by continuously monitoring a predefined list of applications, hardware and software components concerning security vulnerabilities within the portfolio. • Fully automatic notification feeds as soon as new security notifications are published. • Vulnerability information requests for new components can be directly integrated into the R&D process with the API option. • The digital service scales as the vulnerability database continues to grow, benefiting all users with more comprehensive vulnerability coverage.
Why Siemens?	• Trusted partner of Nokia since 2016.

Reference ID: 9856

“Nokia has been using the Siemens vulnerability services for years, by feeding its data into our security vulnerability management process. This enabled our R&D teams to keep track of existing patches and improving the security of our products.”
Fabio Vignoli, Head of Product Security

Customer quotes

Enlighted, Inc.
Sam Negron, Chief Security Officer

“Vulnerability Services allow us to easily keep on top of security vulnerabilities in all of our third-party components without having to do all of the work of constantly looking for new vulnerability disclosures.”

Siemens Healthineers
Dr. Hans-Martin von Stockhausen, Chief Product Security Office

“Our customers deal with highly sensitive data that necessarily deserves the highest level of protection. Vulnerability Services thought-out service enable us to meet critical security demands and foster a trustful relationship with our customers while allowing us to comply with regulatory requirements.”

Siemens Technology Intellectual Properties
Thomas Bauer, Senior Key Expert M&A Software Due Diligence at Siemens

“In M&A projects, fast fact-finding is mission critical. When conducting software due diligence, integration with the Data Services portal helps us navigate through the jungle of hundreds of cybersecurity vulnerability reports found in a product software codebase of a company being acquired. By using the Vulnerability Services API, mitigation information for Common Vulnerability and Exposures (CVE) is directly integrated into software scan reports. The reports are submitted to the company for implementation of cybersecurity remediation measures. Decisions on necessary actions to make software products more secure are accelerated from weeks to a few days.”

SIEMENS

Let us know if there is anything we can support you with!

You want to find out more?

You can find more information:
www.siemens.com/vvs

or contact the Siemens partner near you

Siemens Contact Database

SIEMENS

Disclaimer

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

SIEMENS

Security Information

Siemens provides products and solutions with industrial security functions
that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats,
it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept.
Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks.
Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent
such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
https://www.siemens.com/industrialsecurity

SIEMENS