

AUVESY Asset Inventory Service

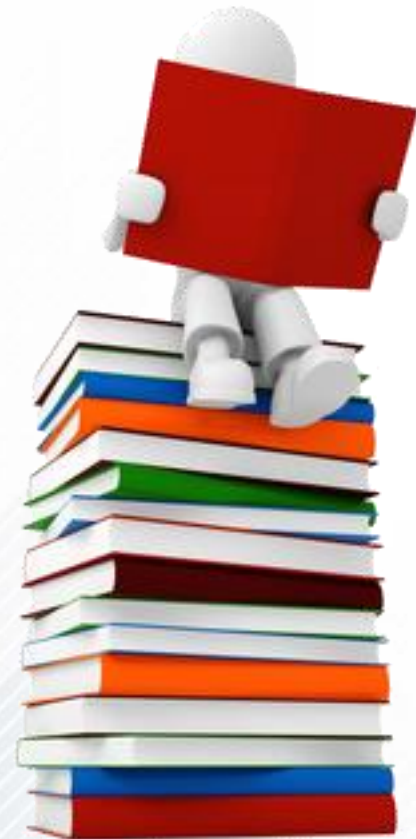
Detekce zařízení na síti a vyhodnocení bezpečnostních rizik

Lukáš Rejtek, David Školník

Pantek (CS) s.r.o.

Obsah prezentace

- ▶ VERSIONDOG – Připomenutí pozice Versiondogu
- ▶ AUVESY Asset Inventory Service - nové řešení pro detekci a správu zařízení na síti
- ▶ Vyhodnocení rizika a zranitelnosti z pohledu kybernetické bezpečnosti
- ▶ Hlavní přínosy
- ▶ Otázky ... a odpovědi



| Versiondog

Připomenutí pozice Versiondogu

Software pro automatizovanou správu, kontrolu a zálohování výrobních programů a dat

- ▶ **Automatizované archivování dat na centrální úložiště**
 - ▶ Dohledatelnost změn – Kdo, Kdy a Co změnil
 - ▶ Správa oprávnění pro přístup
- ▶ **Inteligentní porovnání změn (rozdílů) díky metodice Smart Compare**
 - ▶ Zobrazení rozdílů v přehledné (grafické / textové) podobě
 - ▶ Pro většinu zařízení není zapotřebí vývojové prostředí výrobce
- ▶ **Automatické průběžné kontroly on-line programů / dat**
 - ▶ Přehled nad skutečně provozovanými programy a provedenými změnami
- ▶ **Automatické průběžné zálohy programů / dat ve výrobě**
 - ▶ Pravidelné zálohování

Versiondog - s jakými soubory a programy pracuje?

PLC / CNC

- Siemens - Simatic S5 / S7, TIA Portal
- Rockwell Automation - RsLogix 5 / 500 / 5000
- Schneider Electric – Modsoft, Concept, Unity, EcoStruxure
- 3S CoDeSys, Beckhoff TwinCAT
- Phoenix Contact PC Worx, Omron
- Mitsubishi, B&R, GE Proficy Machine Edition
- Sinumerik 840D, Fanuc
- a další

HMI / DCS / ROBOT

- WinCC, ProTool
- WinCC-flexible, TIA Portal
- AVEVA InTouch, AVEVA System Platform
- GE iFix, Scheinder CitectSCADA
- Copa-data Zenon
- Siemens PCS 7, ABB Freelance
- ABB, KUKA, FANUC, Motoman, Adept
- a další

Inteligentní zařízení

- SEW
- Lenze, EPLAN
- Sick Scanner, Cognex
- Atlas Copco
- Kistler Maximos, Hirschmann, WAGO
- Siemens Scalance Switch
- a další

SOUBORY / DOKUMENTY

- MS Office Word, Excel
- PDF
- XML
- ASCII (.txt ...)
- INI soubory
- Binary, JSON
- a další

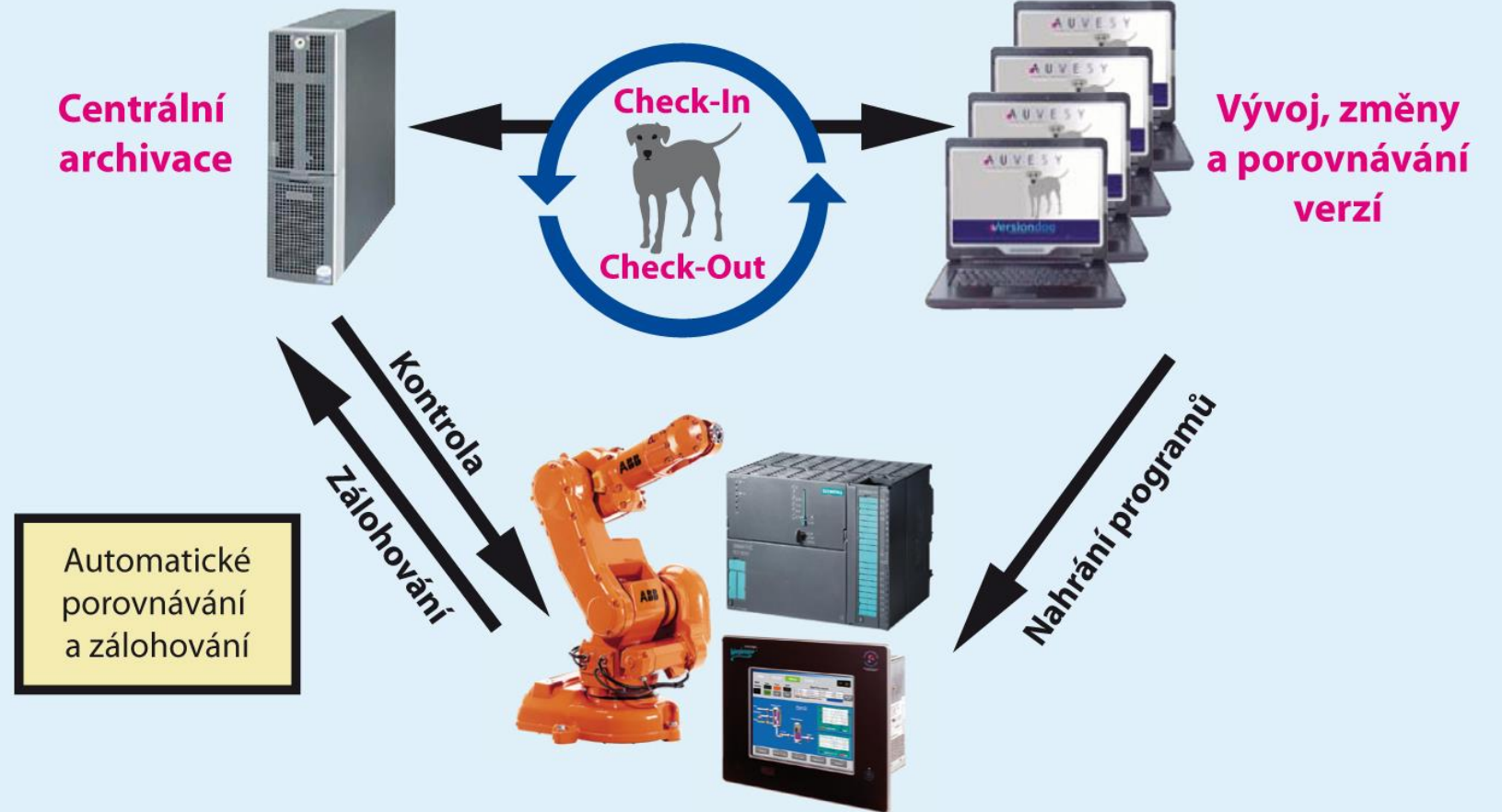
Versiondog

Versiondog server

Versiondog klienti

**Centrální
archivace**

**Vývoj, změny
a porovnávání
verzí**



Výrobní zařízení (PLC, PC, roboty aj.)

Versiondog - speciálně pro průmyslové využití – reference v ČR/SR



**MANN+
HUMMEL**

Continental

vitesc
TECHNOLOGIES



**FEDERAL
MOGUL**



SIEMENS

Nemak

starcam::S::

Miele



★ Heineken

Pilsner Urquell

STAROPRAMEN

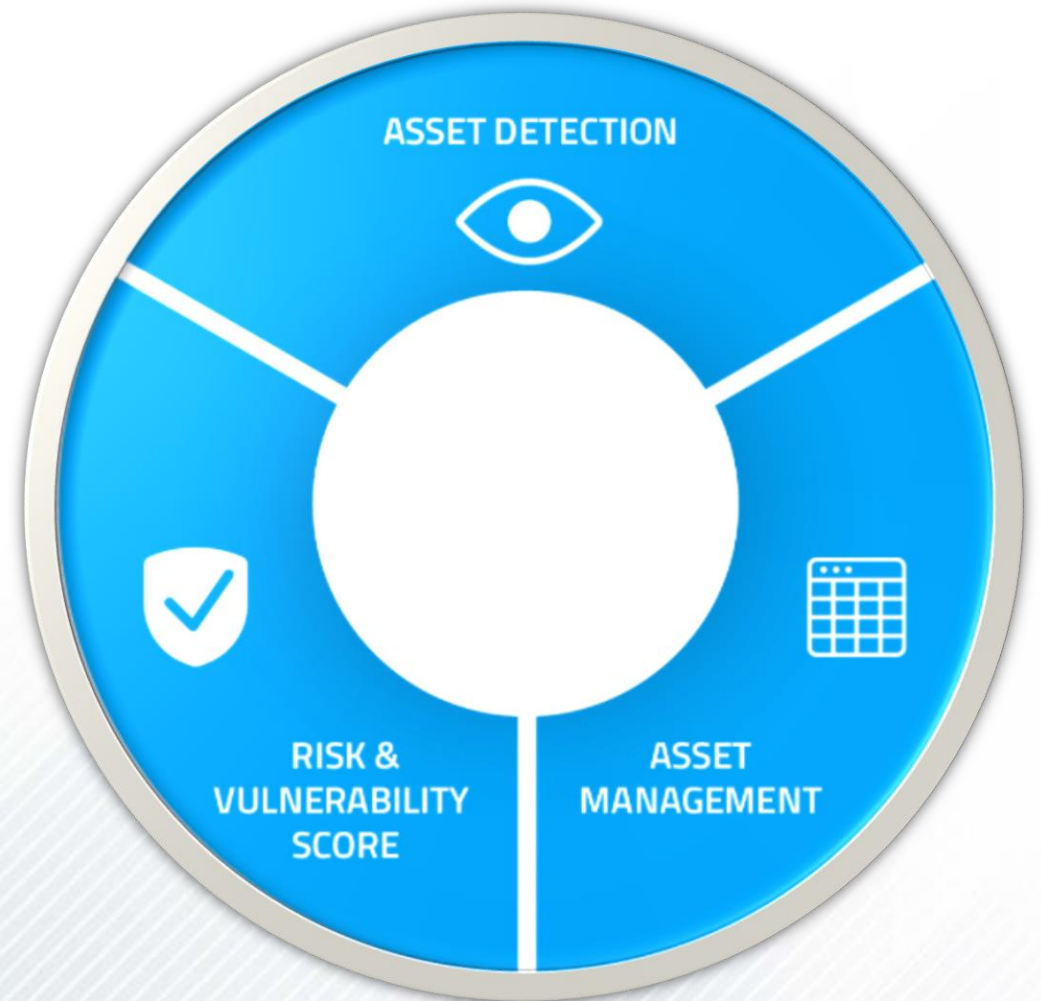
LEGO

BONATRANS

| Nové řešení pro detekci
a správu zařízení na síti

Nové řešení pro detekci a správu zařízení na síti

- ▶ Monitoring sítě a vyhodnocení rizik přináší vyšší bezpečnost výrobního prostředí
- ▶ Základní principy Asset Inventory Service
 - ▶ Detekce zařízení na síti
 - ▶ Správa zařízení
 - ▶ Vyhodnocení rizika a zranitelnosti z pohledu kybernetické bezpečnosti



| Detekce zařízení na síti

Detekce zařízení na síti

▶ Aktivní a pasivní SCAN

- ▶ Zařízení na síti jsou detekována pomocí aktivních a pasivních scanů
- ▶ Vytváří celkový seznam všech zařízení
- ▶ Nalézá „nedostatky“ pro doplnění plánu záloh a automatických kontrol pro Versiondog
 - ▶ Nové zařízení je možné automaticky importovat do Versiondogu

▶ Integrace s Versiondogem

- ▶ Automaticky zálohovaná zařízení jsou převzata z Versiondogu
- ▶ Při provedení každé zálohy dochází k aktualizaci informací o jednotlivém zařízení
- ▶ Všechny změny v konfiguraci provedené v rámci nových verzí jsou zaznamenány a vyhodnocovány
- ▶ Každé nové zařízení ve Versiondogu je automaticky přidáno do Asset Inventory Service

Aktivní a pasivní SCAN

▶ Pasivní SCAN

- ▶ Sleduje chování na síti
- ▶ Vyhodnocuje „nestandardní“ komunikaci
- ▶ Nedochozí k zatěžování komunikace
- ▶ Lze použít pro více sítí současně

▶ Aktivní SCAN

- ▶ Pokročilá metoda používající aktivní dotazování koncových zařízení
- ▶ Dotazování využívá jak standardní tak vlastní pokročilé detekční metody

▶ Jaké informace jsou poskytovány

- ▶ IP adresa (MAC adresa), Výrobce, Firmware, Hardware (Modelová řada, Rack/Slot) ...

| Správa zařízení

- ▶ **Centrální část systému**

- ▶ Zařízení převzatá z Versiondogu
- ▶ Zařízení detekovaná pomocí aktivních a pasivních scanů

- ▶ **Vytváří o všech zařízeních komplexní přehled, který je:**

- ▶ Plně automatizovaný
- ▶ Centralizovaný
- ▶ Pravidelně aktualizovaný
- ▶ Poskytuje i dodatečné informace o projektech přebírané z Versiondogu, což umožňuje lepší orientaci
- ▶ Čitelný

Správa zařízení

- ▶ Nevytváří pouze jednoduchý přehled o IP adresách, ale seznam zařízení
 - ▶ Typ zařízení, výrobce, verze firmware ...

The screenshot displays a web interface for device management. It is divided into two main sections: 'DEVICE INFORMATION' and 'RACK SLOTS'.

DEVICE INFORMATION


NETWORK		HARDWARE		SOFTWARE
IP	Host name	Vendor	Model	Parsed Asset
10.0.0.221	SIMATIC 400(1)	Siemens	CPU 4 16-2 DP	Yes
Purdue Level	First Seen	Order Number (MFR)		
Level 1 <input checked="" type="checkbox"/>	27/02/2021 12:29	6ES7 416-20002...		
Last Seen	Class			
27/02/2021 12:29	DT			

RACK SLOTS

The rack slots section shows a horizontal row of four slots. Slots 0, 1, and 2 are labeled 'Empty'. Slot 3 is highlighted in blue and contains a Siemens CPU 4 16-2 DP with firmware version V1.2. Slot 4 is also highlighted in blue and contains a Siemens CP443-1IT. Slots 5 and 6 are not visible.

Správa zařízení

ASSETS

Presets Custom  Reset

Filter By

Class: Select Class... Type: Select Type... Vendor: Select Vendor... Protocol: Select Protocol... Criticality: Select Criticality... Search By: Name, IP, Version, Model, Mac ...

Advanced Options»

RESULTS (70)

	NAME	IP	MAC	CLASS	TYPE	CRITICALITY	RISK LEVEL	VENDOR	NETWORK	LAST SEEN
<input type="checkbox"/>	Switch	10.0.220.17	00:0E:8C:B7:E8:02	IT	Endpoint	● Low	● Medium	Siemens	Default	14/04/2021 17:01
<input type="checkbox"/>	10.0.220.143	10.0.220.143		OT	PLC	● High	● Medium	Rockwell Automation	Default	14/04/2021 17:01
<input type="checkbox"/>	10.0.220.145	10.0.220.145		OT	PLC	● High	● Medium	Rockwell Automation	Default	14/04/2021 17:01
<input type="checkbox"/>	10.0.220.67	10.0.220.67		IT	Endpoint	● Low	● Medium	Omron	Default	14/04/2021 17:01
<input type="checkbox"/>	10.0.220.144	10.0.220.144		OT	PLC	● High	● Medium	Rockwell Automation	Default	14/04/2021 17:01
<input type="checkbox"/>	10.0.220.41	10.0.220.41		OT	PLC	● High	● Medium	Rockwell Automation	Default	14/04/2021 17:01
<input type="checkbox"/>	10.0.220.142	10.0.220.142		OT	PLC	● High	● Medium	Rockwell Automation	Default	14/04/2021 17:01

Vyhodnocení rizika a zranitelnosti z pohledu kybernetické bezpečnosti

Vyhodnocení rizika a zranitelnosti

- ▶ Detailní informace o rizicích a zranitelnosti pro všechna zařízení
- ▶ Údaje o každém zařízení se porovnávají s databází známých rizik a zranitelností (CVE – common vulnerabilities and exposures)
 - ▶ Znalostní databáze je průběžně aktualizována
- ▶ **Provádí se i kontrola**
 - ▶ Nezabezpečených komunikačních protokolů
 - ▶ Chybných konfigurací
 - ▶ Další bezpečnostních slabin
- ▶ **Vlastní detekční metody v rámci aktivních a pasivních scanů**

Vyhodnocení rizika a zranitelnosti

- ▶ Každé riziko pro jednotlivá zařízení je posouzeno a vyhodnoceno napříč celou průmyslovou sítí
- ▶ Riziko je vyhodnoceno prostřednictvím skóre pro jednotlivá zařízení
- ▶ Vyhodnocována jsou i komunikační rizika po síti

Vyhodnocení rizika a zranitelnosti

► Komplexní přehled nalezených hrozeb a rizik

The screenshot displays the 'INSIGHTS' dashboard interface. On the left is a navigation sidebar with categories like Dashboard, Visibility, Risk & Vulnerabilities (selected), Attack Vector, Threat Detection, Investigation, and Reports. The main area features a search bar, filter options (Class, Type, Vendor, Protocol, Criticality), and a search field. Below the filters, there are tabs for 'Advanced Options' and 'Insights Options'. The main content area shows a list of six insights, each with a lightbulb icon and a dropdown arrow. The insights are:

- 29 assets have 127 unpatched vulnerabilities - Full Match
- 4 assets are using 1 unsecured protocol: TELNET
- 5 assets have 30 unpatched vulnerabilities - Vendor and Model Match
- 2 PLCs are exposed to remote program changes or have stopped
- 2 assets have unpatched vulnerabilities - Windows Match
- 3 assets have unpatched vulnerabilities - Vendor Match (highlighted in green)

Vyhodnocení rizika a zranitelnosti

► CVE – zobrazení skóre všech identifikovaných rizik pro zařízení

The screenshot displays the 'INSIGHTS' section of a security dashboard. The left sidebar contains navigation options: Dashboard, Visibility, Risk & Vulnerabilities (selected), Risk & Vulnerabilities Overview, Insights, Attack Vector, Threat Detection, Investigation, and Reports. The main content area shows a filter for 'Insight Name: Full Match CVEs'. Below the filter are dropdown menus for Class, Type, Vendor, Protocol, and Criticality, along with a search box. A summary card indicates '13 assets have 12 unpatched vulnerabilities - Full Match'. Below this, a table lists 12 results with columns for CVE-ID, SCORE (CVSS), TITLE, PUBLISHED, MODIFIED, AFFECTED ASSETS, and ACTIONS. The table shows four rows of vulnerabilities with scores ranging from 7.5 to 7.8.

CVE-ID	SCORE (CVSS)	TITLE	PUBLISHED	MODIFIED	AFFECTED ASSETS	ACTIONS
SSA-501073	7.8	Vulnerabilities in Controllers CPU 1518 MFP using Intel CPUs (November 2020)	11/05/21	11/05/21	12 assets - click to filter	Mark All as Completed
SSA-180635	7.5	Denial-of-Service Vulnerabilities in S7-1500 CPU	08/01/19	08/01/19	1 asset - click to filter	Mark All as Completed
SSA-307392	7.5	Denial-of-Service in OPC UA in Industrial Products	09/04/19	14/05/19	2 assets - click to filter	Mark All as Completed
SSA-780073	7.5	Denial-of-Service Vulnerability in PROFINET	11/02/20	11/02/20	4 assets - click to filter	Mark All as Completed

Vyhodnocení rizika a zranitelnosti

► CVE – detailní pohled

INSIGHTS Presets Custom [Upload] Reset

Filter By Insight Name: Full Match CVEs x Insights: Full Match CVEs; CVE-ID: SSA-501073 x Insight Name: Full Match CVEs x Clear all Query V

Class: Select Class... Type: Select Type... Vendor: Select Vendor... Protocol: Select Protocol... Criticality: Select Criticality... Search By: Name, IP, Version, Model, Mac ...

Advanced Options» Insights Options»

INSIGHTS (1)
RESULTS (12)

CVE-ID	SCORE (CVSS)	TITLE	PUBLISHED	MODIFIED	AFFECTED ASSETS	ACTIONS
SSA-501073	7.8	Vulnerabilities in Controllers CPU 1518 MFP using Intel CPUs (November 2020)	11/05/21	11/05/21	12 assets - click to filter	Mark All as Completed

Access Type: Local

Intel has published information on vulnerabilities in Intel products in November 2020. Some Siemens Controllers are affected by these vulnerabilities due to the use in Intel products.

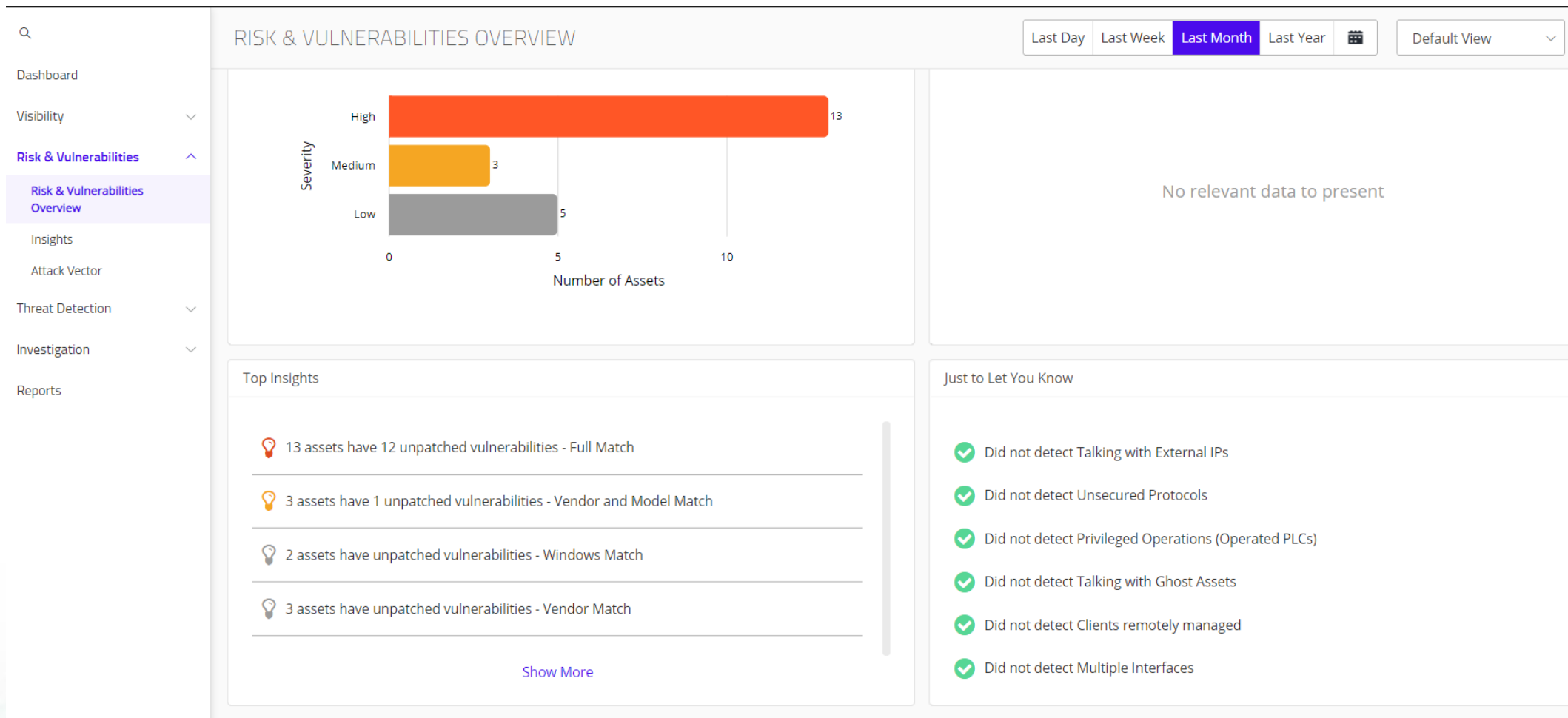
Related CVEs: CVE-2020-8744, CVE-2020-0591

[Link 1](#)

NAME	IP	TYPE	VENDOR	MODEL	FIRMWARE	IDENTIFIED ON	STATUS	UPDATED BY	COMMENT	ACTIONS
SIMATIC 400	10.0.0.222	PLC	Siemens	CPU 416F-2	V5.3.1	31/05/21	Open			Mark as Completed

Vyhodnocení rizika a zranitelnosti

► Komplexní vyhodnocení rizika



| Hlavní přínosy

Hlavní přínosy

- ▶ **Komplexní přehled o zařízeních na síti**

- ▶ Automatické sestavení přehledu všech zařízení s detailními informacemi (adresa, typ, výrobce)

- ▶ **Zvýšení bezpečnosti a monitoring sítě**

- ▶ Detekce případných hrozeb a známých rizik

- ▶ **Rozšíření plánu automatických záloh**

- ▶ Detekce zařízení, pro která není v rámci Versiondogu naplánována automatická kontrola a zálohování

- ▶ **Snížení nákladů**

- ▶ Zvýšení efektivity a předcházení riziku, které může mít zásadní dopad na výrobu

AUVESY Asset Inventory Service

▶ Jak je možné Asset Inventory Service získat?

- ▶ Asset Inventory Service verze 1.0 je součástí Versiondogu od verze 9.0
- ▶ Jako samostatné řešení bude nabízeno od verze 2.0 (první pololetí 2022)
 - ▶ Bude dostupné i pro zákazníky, kteří Versiondog nepoužívají

▶ Další informace na:

- ▶ www.auvesy.com/en/asset-inventory-service/

Vy ještě nemáte Versiondog?

- ▶ Riziko hrozeb / útoků na výrobní zařízení se stále zvyšuje, a tím i tlak na automatizované kontroly a zálohy výrobních zařízení pro zajištění rychlé obnovy
- ▶ Versiondog díky nové funkci Easy Asset Integrator nabízí možnost importu zařízení do Versiondogu včetně importu projektů, což umožňuje zásadně rychlejší nasazení
- ▶ Stále je nabízena možnost testovací licence včetně nasazení u zákazníka



| Děkuji za pozornost

Otázky, odpovědi



Váš partner ve světě digitální transformace

Sušilova 1528/1
500 02 Hradec Králové
Česká republika

www.pantek.cz