

A1

WithSecure delavnica

Predavatelj:
Vladimir Ban, CEH|OSCP

WithSecure Elements VM

Aktivno iskanje varnostnih nedoslednosti

WithSecure Elements VM

Iskanje lukenj
od zunaj

Iskanje lukenj
od znotraj

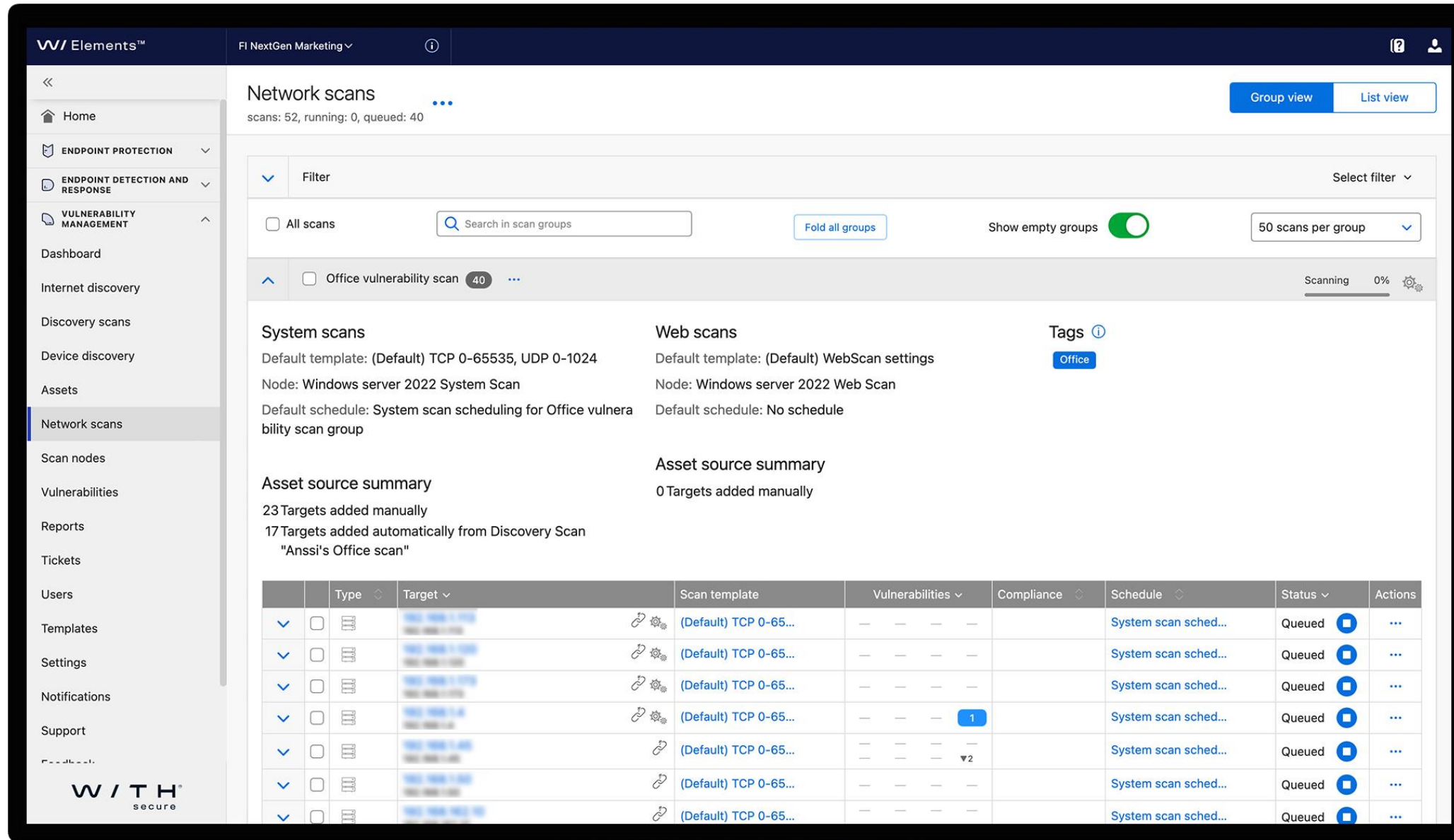
Iskanje lukenj
na elementih

WithSecure Elements VM

Enkratni
pregled

Periodični
pregled

WithSecure Elements VM – Vulnerability Scanner



- Discovery Scanner
- Internet network scanner
- Internet web application scanner
- Internal network scanner

WithSecure Elements VM – Vulnerability Scanner

- Enostaven za uporabo
- Omogoča pripravo preglednih, tehničnih in profesionalnih poročil
- Možnost skeniranja spletnih aplikacij
 - Tudi s prijavo v aplikacijo
- Možnost periodičnega skeniranja
- Možnost lokalnega skeniranja
 - Preko mrežnih skrbniških protokolov
 - Lokalno z agentom na strežniku

WithSecure Elements VM – Discovery scan

The screenshot shows the WithSecure Elements interface. The top navigation bar includes the logo, user information (A1 Slovenija, d.d.), and a notification bell. The left sidebar contains navigation options: Home, ENDPOINT PROTECTION, ENDPOINT DETECTION AND RESPONSE, VULNERABILITY MANAGEMENT, Dashboard, Internet discovery, Discovery scans (highlighted), Device discovery, Assets, Network scans, Scan nodes, Vulnerabilities, Reports, Tickets, Users, and Templates. The main content area displays 'Vulnerability Management / Discovery scans' with a notification banner about a breaking change. Below this, a red box highlights the IP address '91.209.150.0/24'. A 'Show changes' toggle is turned on. A table lists the results of the discovery scan, with columns for checkboxes, Operating system, Target (redacted), MAC address, Vulnerability scan, Ports, Change, and Status. All entries are marked as 'Scanned' and 'Online'.

<input type="checkbox"/>	Operating system	Target	MAC address	Vulnerability scan	Ports	Change	Status
<input type="checkbox"/>				Scanned	TCP/443	Many	Online
<input type="checkbox"/>				Scanned	TCP/443	Many	Online
<input type="checkbox"/>				Scanned	TCP/80 , TCP/135 , TCP/139 , TCP/445 , TCP/49154 , TCP/49156	Many	Online
<input type="checkbox"/>				Scanned	TCP/22 , TCP/53 , TCP/111 , TCP/10000	Many	Online
<input type="checkbox"/>				Scanned	TCP/21 , TCP/22 , TCP/80 , TCP/443 , TCP/10000 , TCP/10050	Many	Online
<input type="checkbox"/>				Scanned	TCP/22 , TCP/80 , TCP/443 , TCP/3306	Many	Online
<input type="checkbox"/>				Scanned	TCP/22 , TCP/80 , TCP/443 , TCP/3306 , TCP/10000 , TCP/10050	Many	Online
<input type="checkbox"/>				Scanned	TCP/443	Many	Online
<input type="checkbox"/>				Scanned	TCP/5000 , TCP/5001 , TCP/5090	Many	Online
<input type="checkbox"/>				Scanned	TCP/25	Many	Online
<input type="checkbox"/>				Scanned	TCP/443	Many	Online
<input type="checkbox"/>				Scanned	TCP/80 , TCP/443	Many	Online

WithSecure Elements VM – Network scan

AT Slovenija, d.d., NFR

Vulnerability Management / Assets

Home

ENDPOINT PROTECTION

ENDPOINT DETECTION AND RESPONSE

VULNERABILITY MANAGEMENT

Dashboard

Internet discovery

Discovery scans

Device discovery

Assets

Network scans

Scan nodes

Vulnerabilities

Reports

Tickets

Users

Templates

W / T H

61393

Port number

First discovered: 35 days ago | Last seen: 35 days ago | Last scanned: Not available | Last updated: 35 days ago | Risk last assessed: 4 hours ago

Vulnerabilities and findings 58

58 findings (41 vulnerabilities, 0 potential findings, 17 informative findings)

Select findings to update status.

Showing 58 records (41 vulnerabilities, 0 potential findings, 17 informative findings)

Group vulnerabilities

Filter	Flags	ID	Title	Severity	State	Status	Actions
	<input type="checkbox"/>	1064568	IBM Domino 9.0, 10.0 Buffer Overflow Vulnerability	9.8 CRITICAL	New	Unattended	
	<input type="checkbox"/>	1065029	IBM Domino before 10.0.1 FP4 Buffer Overflow Vulnerability	9.8 CRITICAL	New	Unattended	
	<input type="checkbox"/>	1065029	IBM Domino before 10.0.1 FP4 Buffer Overflow Vulnerability	9.8 CRITICAL	New	Unattended	
	<input type="checkbox"/>	1118671	IBM Domino 9.0 Micro Focus KeyView Multiple Vulnerabilities	9.8 CRITICAL	New	Unattended	
	<input type="checkbox"/>	1051008	IBM Domino 8.5 and 9.0 TLS server Diffie-Hellman key validation Vulnerability	9.8 CRITICAL	New	Unattended	

WithSecure Elements VM – Webscan

The screenshot displays the WithSecure Elements VM interface. The top navigation bar shows the user 'A1 Slovenija, d.d.' and the current page 'Vulnerability Management / Network scans'. A notification banner at the top right states: 'We want to inform you about an upcoming breaking change that will impact our service. Please read the following details carefully. Read more'. The main content area shows a scan for the URL 'http://213.157.243.57/cuenta/'. The scan is marked as 'Completed 2 days ago'. Below this, there are three summary cards: 'Vulnerabilities' showing 1 Critical, 3 High, 5 Medium, and 1 Low; 'Findings and changes' showing 0 New, 1 Fixed, 3 Unattended, 5 Ignored, and 1 Deleted; and 'Vulnerabilities by status' showing a large blue circle with '100% Unattended'. The left sidebar contains navigation options like 'Home', 'Endpoint Protection', 'Endpoint Detection and Response', 'Vulnerability Management', 'Dashboard', 'Asset Discovery', 'Discovery Scans', 'Service Discovery', 'Assets', 'Work Scans', 'Assets Nodes', 'Vulnerabilities', 'Reports', 'Alerts', and 'Updates'.

WithSecure Elements VM – Agent

The screenshot displays the 'Vulnerability Management / Assets' page for an asset named 'ICT2SERVER'. The interface includes a header with the asset name and a 'Show more asset details' link. Below this, there are several summary cards: 'Vulnerabilities' (3 Critical, 6 High, 3 Medium, 2 Low), 'Flags', 'Importance' (Normal), 'Internet exposure' (Not Exposed), and 'Asset risk' (Low, 40). The asset details section lists: Host name: ICT2SERVER, IP address: 10.10.10.41, Operating system: Windows Server 2012 R2 Essentials 6.3.9600, MAC: 00:0C:29:AB:48:D0, Domain name: ICT2.local, and Asset source: Endpoint Agent Scan. A 'Tags' section includes: Authenticated Check, Chrome, End of Life, Google, Third-party Software, and Tools. Below this is a 'Vulnerabilities and findings (14)' section with tabs for Software, Hardware, Description, Notes, and Activity log (3). The 'Scan summary' section shows 'Open ports' (Open TCP ports (32): 53, 80, 88, 135, 139 ...; Open UDP ports (5013): 53, 88, 123, 137, 138 ...) and 'Vulnerability tags (10)' (Authenticated Check, Chrome, End of Life, Google, Third-party Software, Tools).

- Deluje znotraj agent klienta
- Preverja varnostne nedoslednosti lokalno
 - Nedoslednosti programske opreme
 - Nedoslednosti OS

WithSecure Elements VM – Assets pregled

The screenshot shows the 'Assets' page in the WithSecure Elements VM interface. The page includes a navigation sidebar on the left, a top header with the company name 'A1 Slovenija, d.d.', and a main content area. A notification banner at the top of the main area states: 'We want to inform you about an upcoming breaking change that will impact our service. Please read the following details carefully. Read more'. Below the notification, the 'Assets' section is displayed with a table of asset data. The table has columns for Name, Vulnerabilities, Importance, Flags, Risk score, and Last seen. A large red rectangle obscures the names of the assets in the first three rows. The table data is as follows:

Name	Vulnerabilities	Importance	Flags	Risk score	Last seen
[Redacted]	2, 36, 9, 4, 2	Normal	Shield icon	Serious 84	3 hours ago
[Redacted]	3, 6, 3, —, 2	Normal		Low 40	10 hours ago
[Redacted]	2, 3, —, 1, 2	Normal		Minimum 27	19 hours ago
[Redacted]	—, 1, 5, 3, 12	Normal	Shield, Globe icons	Minimum 34	4 days ago
[Redacted]	5, —, 35, 13, 27	Normal	Shield, Globe icons	Minimum 26	35 days ago
[Redacted]	8, 13, 16, 4, 17	Normal	Shield, Globe icons	Moderate 71	35 days ago
[Redacted]	—, 1, 9, 5, 10	Normal	Shield, Globe icons	Low 45	35 days ago
[Redacted]	—, 1, 10, 7, 25	Normal	Shield, Globe icons	Low 39	35 days ago
[Redacted]	—, —, —, —, 5	Normal	Globe icon	Minimum 5	35 days ago

WithSecure Elements VM – Reports

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

Navigation ×

Search document 🔍

Findings Pages Results

- 1. Executive summary
 - 1.1. Conclusion
 - 1.2. Scope
 - 1.3. Statistics
- 2. Findings – eti8 (91.223....)
 - 2.1. Service enumeration
 - 2.2. Platform scan findi...
 - 2.2.1.1 Critical ris...
 - 2.2.1.2 High risk...
 - 2.2.1.3 Medium ri...
- 3. Findings – eti9 (91.223....)
 - 3.1. Service enumeration
 - 3.2. Platform scan findi...
 - 3.2.1.1 Critical ris...
- 4. Findings – eti2 (94.75.8...)
 - 4.1. Service enumeration
 - 4.2. Platform scan findi...
 - 4.2.1.1 High risk...
 - 4.2.1.2 Medium ri...

1. Executive summary

1.1. Conclusion

Based on the selected scan targets and the below described summary report configuration, the overall security level¹ for the systems in scope of the assessment is: **Low**

1.2. Scope

The following 14 targets and 0 sites have been scanned.

Targets	Risk score	Importance	Scan date	Findings			
				Critical	High	Medium	Low
			18-07-2023	3	17	6	-
			18-07-2023	1	0	0	-
			18-07-2023	0	3	8	-
			18-07-2023	0	2	4	-
			18-07-2023	0	1	6	-
			18-07-2023	0	1	4	-



Posebna akcija:

WithSecure elements VM – 25ip
990,00€ + DDV

Dodatek: Profesionalne storitve svetovanja

Naročila: do 31.12.2023

HEK Delavnica

Torek 14.11 ob 9h
Ljubljana

250€ + DDV

WithSecure Elements
Collaboration protection

M-365

Email protection

Share point

One Drive

Teams

Microsoft 365 E3
\$32.00 user/month
 (annual commitment)

Microsoft 365 E5
\$57.00 user/month
 (annual commitment)

Microsoft 365 F3
\$8.00 user/month
 (annual commitment)

[Contact sales >](#)

[Contact sales >](#)

[Contact sales >](#)

— **Threat protection**

Detect and investigate advanced threats, compromised identities, and malicious actions across your on-premises and cloud environments. Protect your organization with adaptive, built-in intelligence.



Microsoft Advanced Threat Analytics ¹⁰



Microsoft Defender Antivirus and Device Guard ⁹



Microsoft 365 Defender



Microsoft Defender for Endpoint

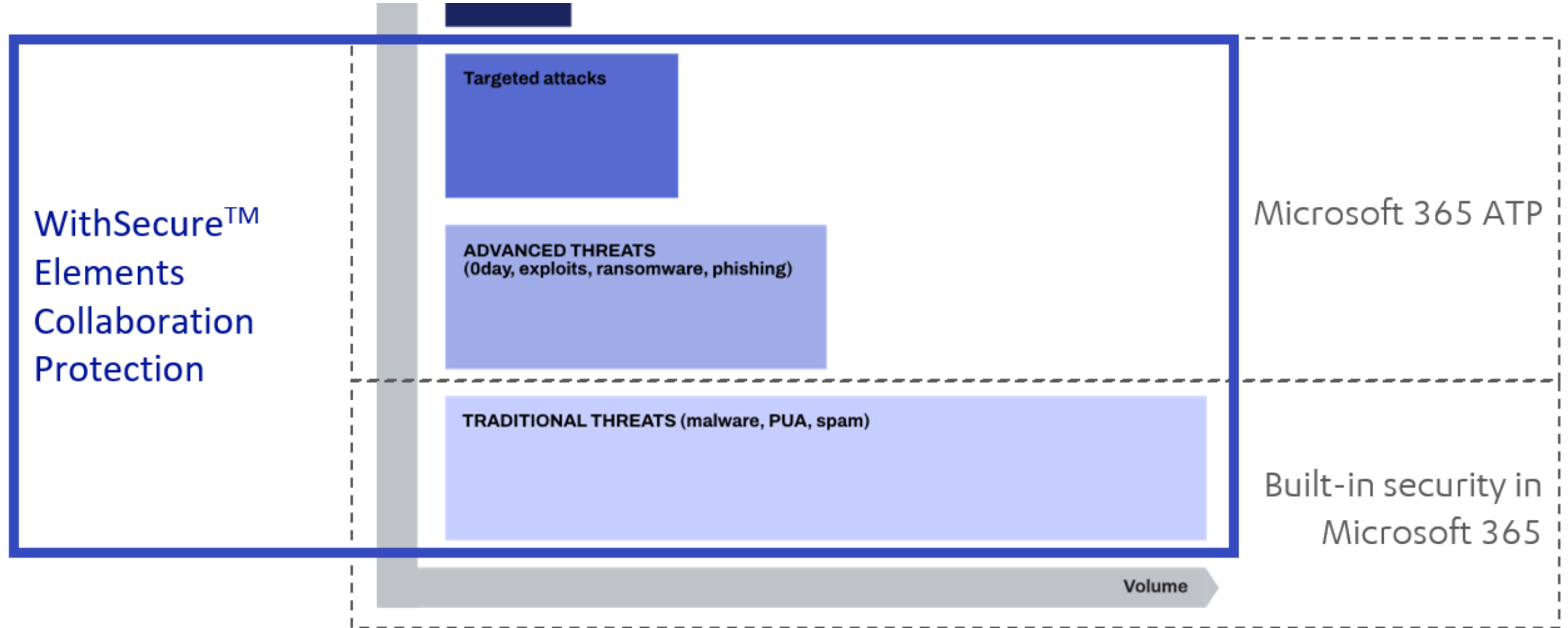


Microsoft Defender for Office 365



Microsoft Defender for Identity





WithSecure Elements CP – Dashboard pregled

The screenshot displays the WithSecure Elements CP Dashboard for 'A1 Slovenija, d.d.'. The dashboard is divided into four main sections:

- Current detections:** Shows 'No detections' for the last month.
- Item status:** Shows a total of 2 items, all of which are 'Protected'. The status breakdown is: Protected (2), Unprotected (0), Error (0), and Unavailable (0).
- Top affected items:** Shows 'No affected items' for the last month.
- Inbox rules:** Shows 'No inbox rules' for the last month.

The left sidebar contains navigation options: Home, ENDPOINT PROTECTION, ENDPOINT DETECTION AND RESPONSE, VULNERABILITY MANAGEMENT (No access), CLOUD SECURITY POSTURE MANAGEMENT (No subscription), COLLABORATION PROTECTION (selected), Dashboard, Cloud services, Detections, Compromised accounts, Policies, Quarantine, System events, Reports, Support, and Management -.

The URL at the bottom of the browser is `elements.withsecure.com/apps/cloudprotection/.../dashboard`.

WithSecure Elements CP – Pregled po servisih

The screenshot shows the WithSecure Elements CP interface. The top navigation bar includes the logo, user information (A1 Slovenija, d.d.), and notification icons. The left sidebar contains a menu with categories like ENDPOINT PROTECTION, ENDPOINT DETECTION AND RESPONSE, and VULNERABILITY MANAGEMENT. The main content area is titled 'Cloud services' and features a table with columns for Name, Exchange, SharePoint, OneDrive, Teams, and Policy. A table with one row is visible, showing a service named 'Varnostne rešitve' with counts of 2 for Exchange, 1 for SharePoint, 1 for OneDrive, and 2 for Teams, all under the 'WithSecure Policy3'.

<input type="checkbox"/>	Name	Exchange	SharePoint	OneDrive i	Teams	Policy
<input type="checkbox"/>	Varnostne rešitve	2	1	1	2	WithSecure Policy3

WithSecure Elements CP – Pregled detekcij

- Home
- ENDPOINT PROTECTION
- ENDPOINT DETECTION AND RESPONSE
- VULNERABILITY MANAGEMENT
No access
- CLOUD SECURITY POSTURE MANAGEMENT
No subscription
- COLLABORATION PROTECTION**
- Dashboard
- Cloud services
- Detections**
- Compromised accounts
- Policies
- Quarantine
- System events
- Reports
- Support
- Management -

Collaboration Protection / Detections

Detections

Status

Select one or more values

Refresh

Clear all

All

Items: 20

<input type="checkbox"/>	Description	Affected ass... i	Sever... i	Date and time	Affected user	Location	Action taken	Status	Cloud service	Comments	ID
<input type="checkbox"/>	Harmful content: 1 attachment	TEST	MEDIUM	7 months ago Apr 17, 2023 12:39:11	vladimir.ban@varnostne-...	Inbox	Quarantined	New	E Varnost...	0	
<input type="checkbox"/>	Harmful content: 1 URL	ef	MEDIUM	a year ago Nov 04, 2022 05:04:57	vladimir.ban@varnostne-...	Inbox	Quarantined	New	E Varnost...	0	
<input type="checkbox"/>	Harmful content: 1 URL	Fwd: Poštni ...	MEDIUM	a year ago May 24, 2022 02:16:05	vladimir.ban@varnostne-...	Inbox	Quarantined	New	E Varnost...	0	
<input type="checkbox"/>	Harmful content: 1 URL	DHL posiljka	MEDIUM	2 years ago Jul 09, 2021 00:49:53	vladimir.ban@varnostne-...	Deletions	Quarantined	New	E Varnost...	0	
<input type="checkbox"/>	Harmful content: 1 URL	DHL posiljka	MEDIUM	2 years ago Jul 09, 2021 00:49:53	vladimir.ban@varnostne-...	Deletions	Quarantined	New	E Varnost...	0	
<input type="checkbox"/>	Harmful content: 1 URL	DHL posiljka	MEDIUM	2 years ago Jul 09, 2021 00:49:52	vladimir.ban@varnostne-...	Deletions	Quarantined	New	E Varnost...	0	
<input type="checkbox"/>	Harmful content: 1 URL	DHL posiljka	MEDIUM	2 years ago Jul 09, 2021 00:49:52	vladimir.ban@varnostne-...	Deletions	Quarantined	New	E Varnost...	0	



WithSecure Elements CP – Compromised accounts

The screenshot shows the 'Compromised accounts' page in the WithSecure Elements CP interface. The top navigation bar includes the 'WI Elements™' logo, the user 'A1 Slovenija, d.d.', and the organization 'A1 Slovenija, d.d._NFR'. The left sidebar contains navigation options: Home, ENDPOINT PROTECTION, ENDPOINT DETECTION AND RESPONSE, VULNERABILITY MANAGEMENT (No access), CLOUD SECURITY POSTURE MANAGEMENT (No subscription), COLLABORATION PROTECTION (selected), Dashboard, Cloud services, Detections, Compromised accounts, Policies, Quarantine, System events, Reports, Support, and Management.

The main content area is titled 'Compromised accounts' and features a search filter: 'Domain name' includes 'Enter a value and then press Enter'. There are 'Refresh' and 'Clear all' buttons. Below the search filter, a section titled 'Varnostne rešitve' (Security fixes) indicates the last check for compromised accounts was on 09.11.2023 at 02:23:04.

Email account	Domain name	Breaches	Last password change ⓘ	MFA ⓘ
No compromised accounts were detected				

WithSecure Elements CP – Karantene

The screenshot shows the 'Quarantine' section of the WithSecure Elements CP interface. The sidebar on the left contains navigation items: Home, ENDPOINT PROTECTION, ENDPOINT DETECTION AND RESPONSE, VULNERABILITY MANAGEMENT (No access), CLOUD SECURITY POSTURE MANAGEMENT (No subscription), and COLLABORATION PROTECTION (expanded). Under COLLABORATION PROTECTION, there are links for Dashboard, Cloud services, Detections, Compromised accounts, Policies, Quarantine (highlighted), System events, Reports, and Support. A Management - dropdown is at the bottom.

The main content area is titled 'Quarantine' and shows 'Total size: 1.55 MB'. It includes a search bar for 'Quarantine ID' with a 'Refresh' button and a 'Clear all' link. A filter dropdown is set to 'All'. A status filter shows 'Status: Quarantined, Failed, Recoverable failure'. Below this, it says 'Showing 22' items.

	<input type="checkbox"/>	Status	Quarantine ID	Cloud service	Date and time	Reason	Action
<input checked="" type="checkbox"/>	<input type="checkbox"/>	✉	0546505e-34ca-4293-a40f-c30adb5d7c00	Exchange	17.04.2023 12:39:11	Harmful content	View detection
<input checked="" type="checkbox"/>	<input type="checkbox"/>	✉	19ae0fc2-d3a5-4398-95c9-ce5f168ed40a	Exchange	04.11.2022 05:04:57	Harmful URL	View detection
<input checked="" type="checkbox"/>	<input type="checkbox"/>	✉	b4b18081-4da3-40df-917d-0d16b793c2f1	Exchange	24.05.2022 02:16:05	Harmful URL	View detection
<input checked="" type="checkbox"/>	<input type="checkbox"/>	✉	ed2daf18-d492-492c-8567-f2575d6e935b	Exchange	09.07.2021 00:49:53	Harmful URL	View detection
<input checked="" type="checkbox"/>	<input type="checkbox"/>	✉	3c2456ef-b9fa-424c-988e-07853ac55e8c	Exchange	09.07.2021 00:49:53	Harmful URL	View detection
<input checked="" type="checkbox"/>	<input type="checkbox"/>	✉	cc858316-8d9e-4a26-abd8-1d5a2ae6e9dc	Exchange	09.07.2021 00:49:51	Harmful URL	View detection
<input checked="" type="checkbox"/>	<input type="checkbox"/>	✉	dcd04846-865c-4ebe-a196-37948e5d07ac	Exchange	09.07.2021 00:49:51	Harmful URL	View detection
<input checked="" type="checkbox"/>	<input type="checkbox"/>	✉	552b5e67-ce95-4eb2-a40d-8906d644f84e	Exchange	09.07.2021 00:49:51	Harmful URL	View detection
<input checked="" type="checkbox"/>	<input type="checkbox"/>	✉	2291bd7b-1e65-4e8e-946f-e826d223381e	Exchange	09.07.2021 00:49:51	Harmful URL	View detection



A1

**Thank
you**

Vladimir Ban

vladimir.ban@a1.si