



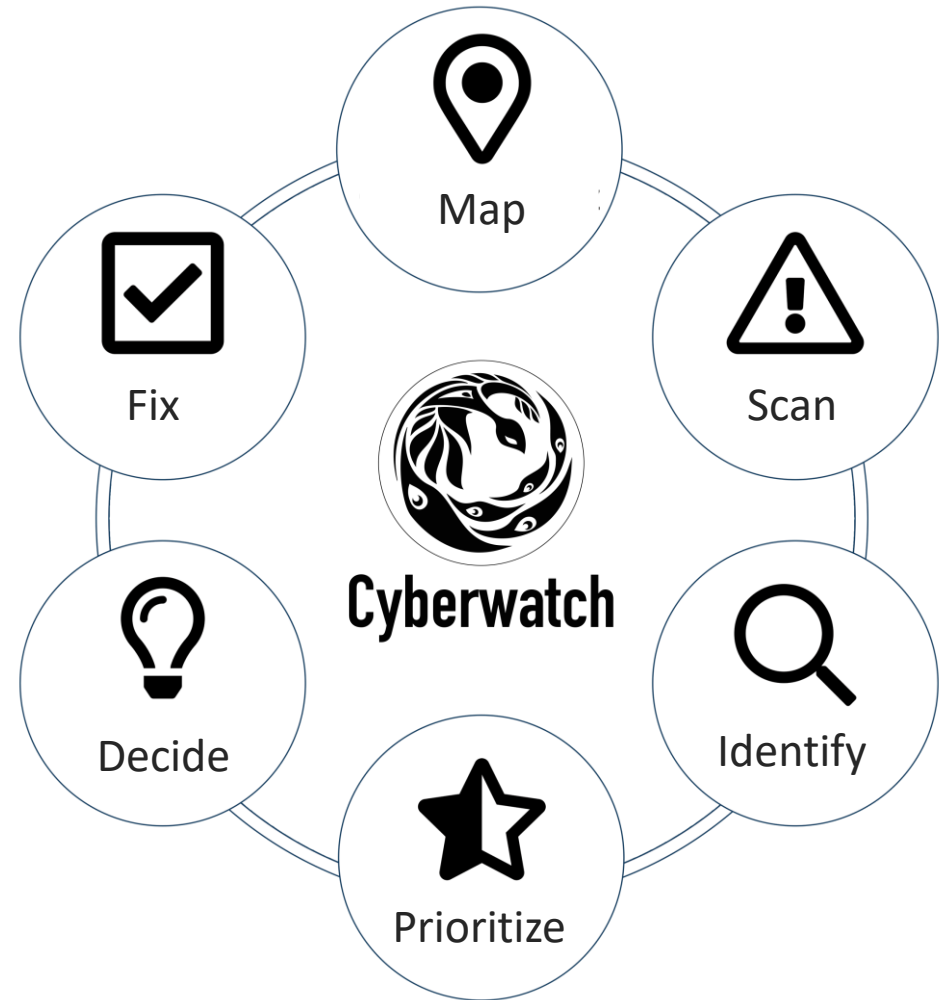
Cyberwatch

Vulnerability Management Software

Vulnerability Management Software

Cyberwatch **helps** you in your **Vulnerability Management**.

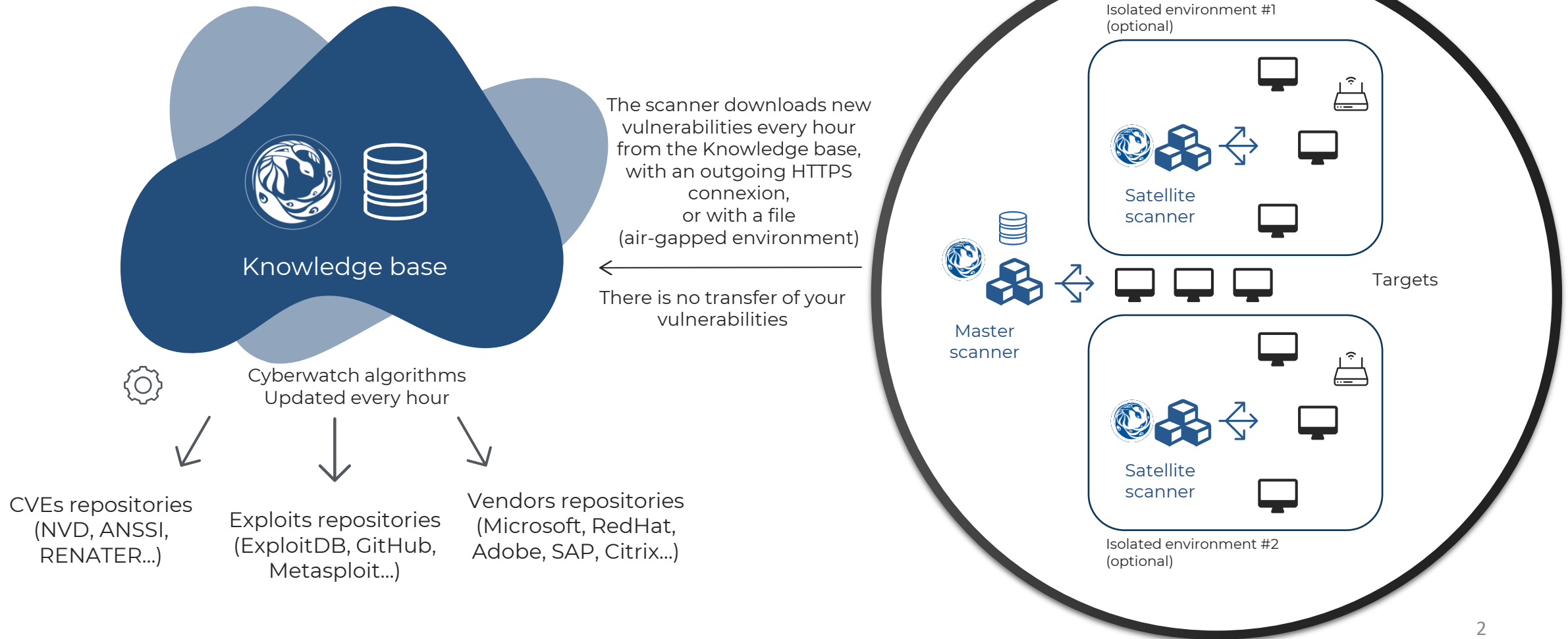
- ✓ Map your assets
- ✓ Scan your vulnerabilities continuously
- ✓ Identify most exposed assets
- ✓ Prioritize most dangerous vulnerabilities
- ✓ Decide the actions to implement
- ✓ Fix your vulnerabilities and control their remediation



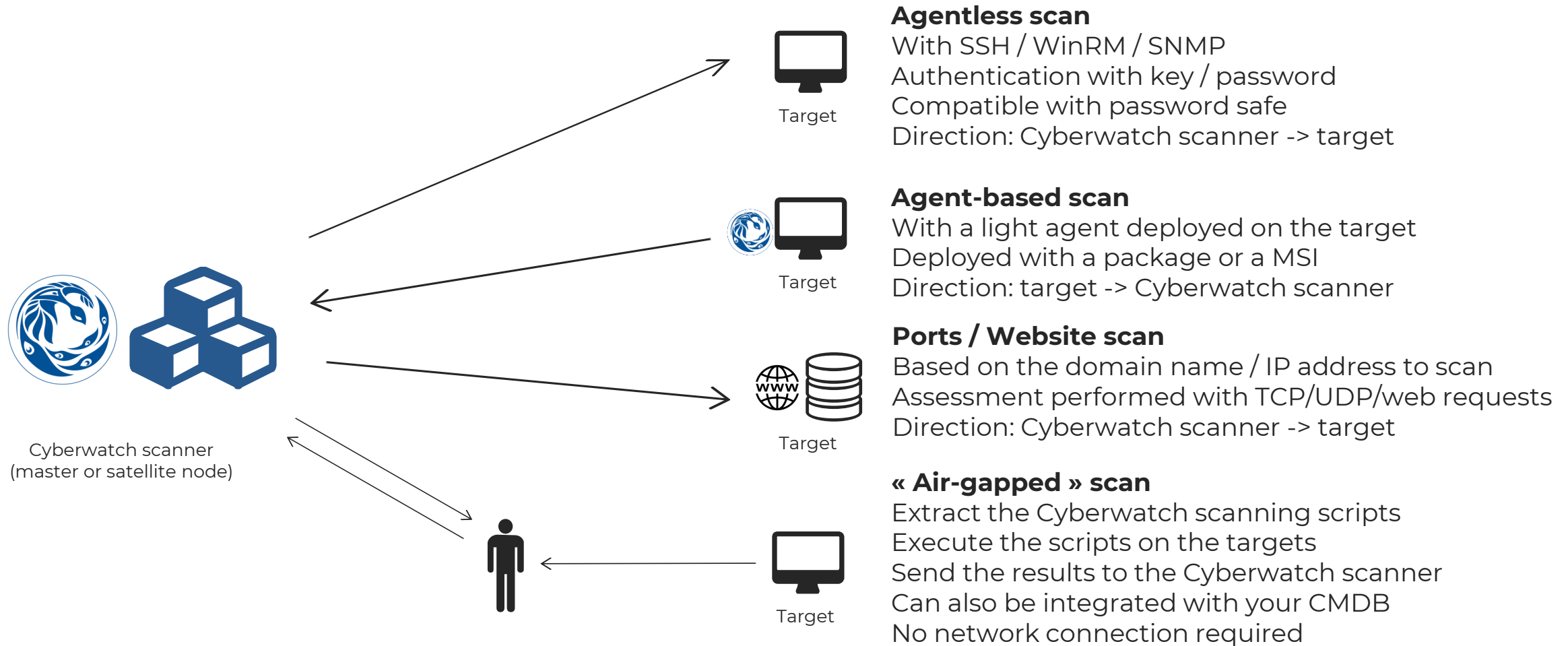
Software architecture

Cyberwatch Cloud (OVH)

Customer's infrastructure



Flexible scanning options



These scanning modes can coexist

Scope



Desktops

PCs
Laptops

*Debian / Ubuntu Desktop
Windows XP / Windows 7
Windows 8 / 10...*



Servers

Virtual Machines
Physical Machines
Hypervisors
Mainframes

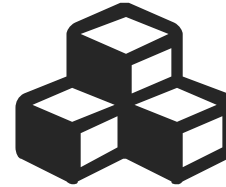
*Debian / Ubuntu
CentOS / RedHat
ArchLinux / Manjaro
SUSE
Windows Server 2003/2008
Windows Server
2012/2016/2019
ESXi, AIX...*



Network devices

Routers
Switches
Firewalls

*Cisco IOS
Palo Alto
Fortinet
Stormshield...*



Containers

Images
Instances

*Docker
Alpine Linux...*



Web applications

URLs
IP addresses

*Technology
fingerprinting
SSL/TLS configuration
review
OWASP analysis...*



Industrial devices

Firmwares

*Siemens
Schneider Electric
Wago
Endress Hauser
Pepperl+Fuchs...*

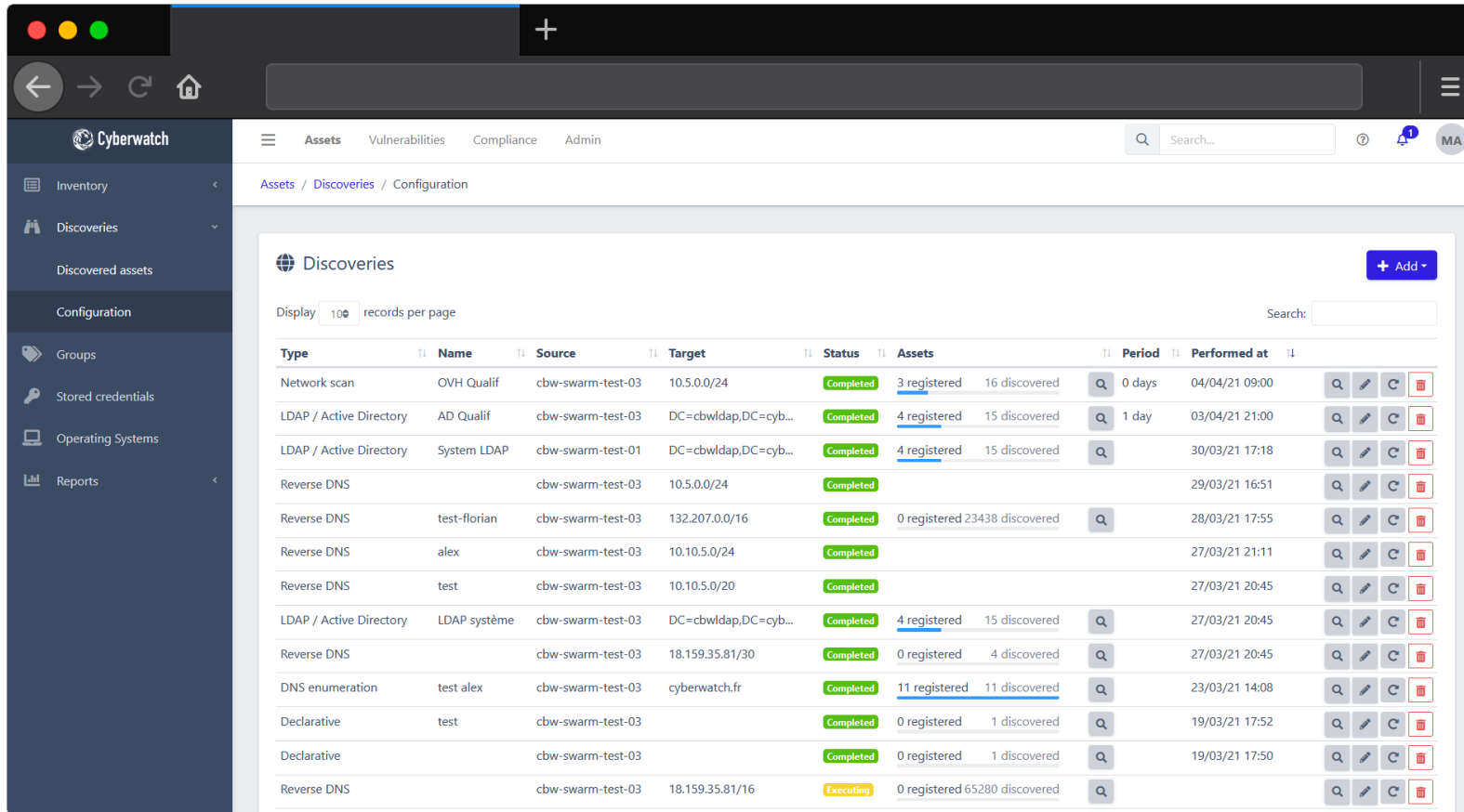


Software libraries

Development
modules

*PIP
Gems
NPM...*

Automated assets discovery



The screenshot displays the Cyberwatch web interface. The left sidebar contains navigation options: Inventory, Discoveries, Discovered assets, Configuration, Groups, Stored credentials, Operating Systems, and Reports. The main content area is titled 'Discoveries' and shows a table of discovered assets. The table has columns for Type, Name, Source, Target, Status, Assets (with registered and discovered counts), Period, and Performed at. Each row includes action icons for search, edit, delete, and refresh.

Type	Name	Source	Target	Status	Assets	Period	Performed at
Network scan	OVH Qualif	cbw-swarm-test-03	10.5.0.0/24	Completed	3 registered 16 discovered	0 days	04/04/21 09:00
LDAP / Active Directory	AD Qualif	cbw-swarm-test-03	DC=cbwldap,DC=cyb...	Completed	4 registered 15 discovered	1 day	03/04/21 21:00
LDAP / Active Directory	System LDAP	cbw-swarm-test-01	DC=cbwldap,DC=cyb...	Completed	4 registered 15 discovered		30/03/21 17:18
Reverse DNS		cbw-swarm-test-03	10.5.0.0/24	Completed			29/03/21 16:51
Reverse DNS	test-florian	cbw-swarm-test-03	132.207.0.0/16	Completed	0 registered 23438 discovered		28/03/21 17:55
Reverse DNS	alex	cbw-swarm-test-03	10.10.5.0/24	Completed			27/03/21 21:11
Reverse DNS	test	cbw-swarm-test-03	10.10.5.0/20	Completed			27/03/21 20:45
LDAP / Active Directory	LDAP système	cbw-swarm-test-03	DC=cbwldap,DC=cyb...	Completed	4 registered 15 discovered		27/03/21 20:45
Reverse DNS		cbw-swarm-test-03	18.159.35.81/30	Completed	0 registered 4 discovered		27/03/21 20:45
DNS enumeration	test alex	cbw-swarm-test-03	cyberwatch.fr	Completed	11 registered 11 discovered		23/03/21 14:08
Declarative	test	cbw-swarm-test-03		Completed	0 registered 1 discovered		19/03/21 17:52
Declarative		cbw-swarm-test-03		Completed	0 registered 1 discovered		19/03/21 17:50
Reverse DNS		cbw-swarm-test-03	18.159.35.81/16	Executing	0 registered 65280 discovered		

Automated assets identification on your Information System, with un-scanned assets auto-tagging

How many desktops do I have in my Active Directory?

What are the virtualized servers on my VMWare environment?

What are the “Shadow IT” elements related to my web domains?

How many assets are on my 192.168.1.1/24 VLAN?

Dashboard with KPIs

Overview of your risk level with Key Performance Indicators

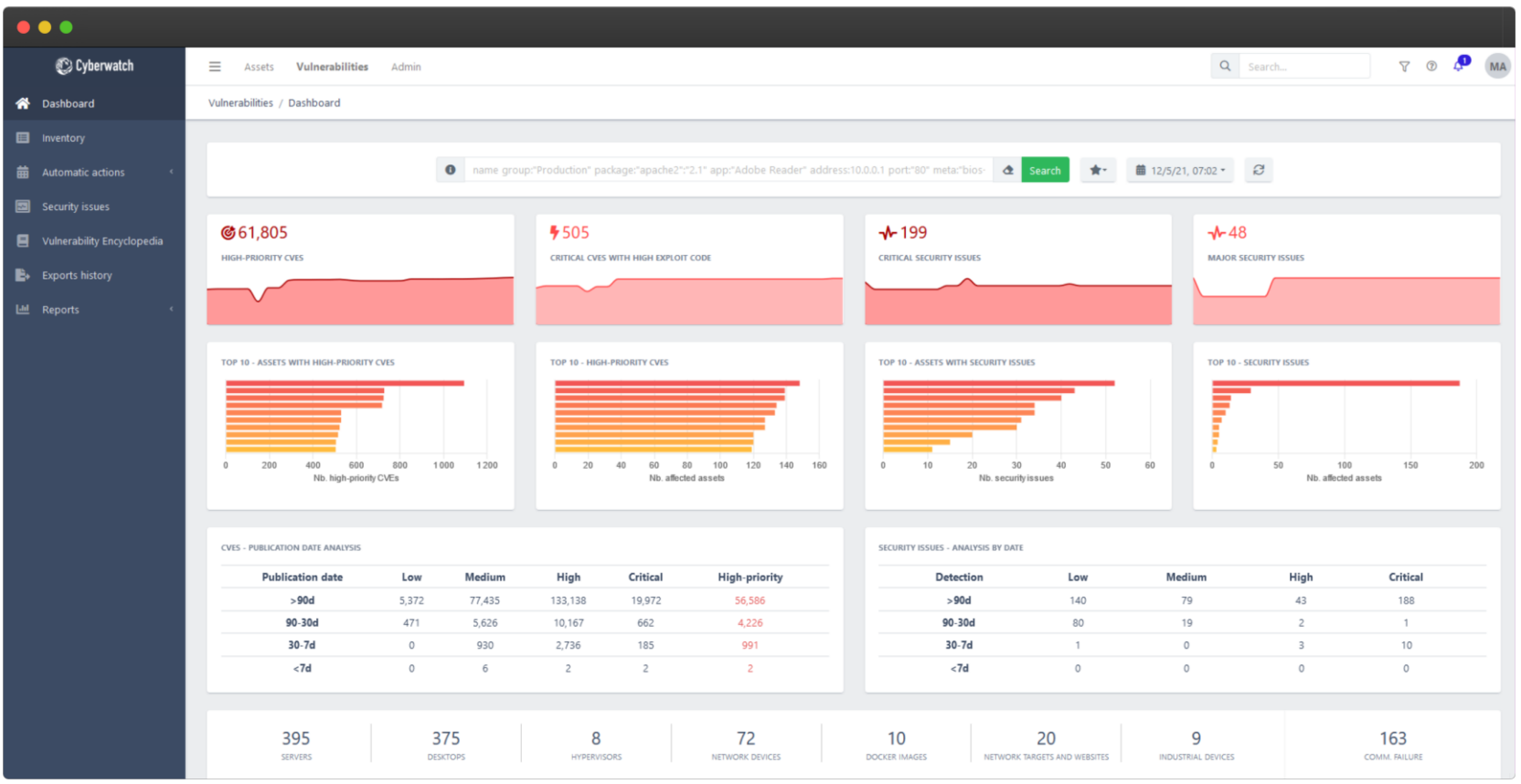
How many CVEs require my attention today?

How many assets require to reboot?

How many assets have obsoletes OS?

What are the assets with the most dangerous vulnerabilities?

Do I have very old and dangerous vulnerabilities?



Overview of your information system

The screenshot displays the Cyberwatch interface for the 'Vulnerabilities / Inventory' section. A search bar at the top contains the query: `name group:"Production" cve:"CVE-2015-0739" package:"apache2:*2.1" app:"Adobe Reader" address:10.0.0.1 port:"80" meta:"bios-version":"1004"`. The interface includes several filter panels:

- Category:** Desktop (3), Docker Image (0), Hypervisor (1), Network Device (1), Network Target or website (3), None (0), Server (18).
- Operating Systems:** Debian 10 (Buster) (1), Debian 9 (Stretch) (3), Mac OS X (1), Ruby on Rails (1), Stormshield (1), Ubuntu 14.04 LTS (1), Ubuntu 18.04 LTS (4), Ubuntu 20.04 LTS (1).
- Criticality:** bdd (0), Collaborateurs (0), Haute dispo (0), High (3), Low (13), Medium (10), Privacy (0), RGD (0).
- Groups:** O_Compliance (4), AmazonWebServices (2), APP_Apache (2), APP_BaseDeDonnees (2), auditeur (1), Cloud (3), Direction_Comm (1), ENV_PRODUCTION (2).
- Statuses:** Compliant (3), Outdated system (2), Vulnerable (21).
- Maximal severity:** Low, Medium, High, Critical.
- Public exploit:** Available.

At the bottom, a table lists assets with the following columns: Name, System, Criticality, Groups, Status, CVEs, and a search icon. The table shows several entries, including Windows Server 2012 and Ubuntu machines, with their respective criticality levels and associated CVEs.

Complete overview of your information system with facets (groups, criticality, name, operating system...)

What are the most exposed critical systems?

What is the risk level of the Production environment?

Which machines have Adobe Flash?

Where is the CVE-2020-0601?

Asset analysis with vulnerability tracking

Complete analysis of the vulnerabilities of your assets, with automated priority, and the ability to ignore or track the status of the remediations

How many vulnerabilities require my immediate attention on this asset?

Was this asset affected by CVE-2017-0143 2 months ago?

*Has CVE-2020-0601 been fixed?
In how much time?*

The screenshot displays the Cyberwatch web interface for asset management. The main dashboard shows a 'Vulnerable' status with a red warning icon and a summary: 'Number of vulnerabilities detected: 2572 including 5 high-priority vulnerabilities'. Below this, a table lists individual vulnerabilities with columns for Reference, Score, CWE, Technology, Corrective action, Comment, and Detected at. The table shows several entries for CVE-2019-11708, CVE-2020-12388, CVE-2020-12389, CVE-2020-17095, CVE-2020-11112, CVE-2021-24094, CVE-2021-24077, CVE-2021-24074, CVE-2021-1722, and CVE-2021-1694, all with scores of 10.0 or 9.8. The interface also includes a sidebar with navigation options like Dashboard, Inventory, and Reports, and a top navigation bar with Assets, Vulnerabilities, Compliance, and Admin.

Reference	Score	CWE	Technology	Corrective action	Comment	Detected at
<input type="checkbox"/> CVE-2019-11708	10.0	CWE-20	Firefox	87		29/01/2021 09:27
<input type="checkbox"/> CVE-2020-12388	10.0	CWE-20	Firefox	87		29/01/2021 09:28
<input type="checkbox"/> CVE-2020-12389	10.0	CWE-20	Firefox	87		29/01/2021 09:28
<input type="checkbox"/> CVE-2020-17095	9.9	NVD-CWE-...	KB5000822	2021-03 Cumulative Update for...		29/01/2021 09:27
<input type="checkbox"/> CVE-2020-11112	9.9	CWE-434	KB5000822	2021-03 Cumulative Update for...		29/01/2021 09:27
<input type="checkbox"/> CVE-2021-24094	9.8	NVD-CWE-...	KB5000822	2021-03 Cumulative Update for...		10/02/2021 03:07
<input type="checkbox"/> CVE-2021-24077	9.8	NVD-CWE-...	KB5000822	2021-03 Cumulative Update for...		10/02/2021 03:07
<input type="checkbox"/> CVE-2021-24074	9.8	NVD-CWE-...	KB5000822	2021-03 Cumulative Update for...		10/02/2021 03:07
<input type="checkbox"/> CVE-2021-1722	9.8	NVD-CWE-...	KB5000822	2021-03 Cumulative Update for...		10/02/2021 03:07
<input type="checkbox"/> CVE-2021-1694	9.8	CWE-269	KB5000822	2021-03 Cumulative Update for...		29/01/2021 09:27

Vulnerability analysis with detailed information

Description
Insufficient vetting of parameters passed with the Prompt:Open IPC message between child and parent processes can result in the non-sandboxed parent process opening web content chosen by a compromised child process. When combined with additional vulnerabilities this could result in executing arbitrary code on the user's computer. This vulnerability affects Firefox ESR < 60.7.2, Firefox < 67.0.4, and Thunderbird < 60.7.2.

Category: Input Validation Error
CWE-20 (Input Validation)
The product does not validate or incorrectly validates input that can affect the control flow or data flow of a program.

Security Notices

- NVD** CVE-2019-11708
- ANSSI** CERTFR-2019-AVI-287
- MITRE** MFSAs2019-19, MFSAs2019-20
- ORACLE** ELSA-2019-1603, ELSA-2019-1604, ELSA-2019-1623, ELSA-2019-1624, ELSA-2019-1626, ELSA-2019-1696

Exploits

- Wiki** EDB-47752
- GitHub**

Related technologies

Vendor	Product
mozilla	firefox
mozilla	firefox_esr
mozilla	thunderbird

Related assets

Name	OS	Criticality	Groups	Comment	Technology	Corrective action	Status
DESKTOP-00NN1BR	Windows10	Low			Firefox	87	1
MacBook-Pro.local	macOS	Low	Direction_Comm		Firefox	87	1

Embedded Vulnerability Encyclopedia, with technical details, links to security advisories, ability to filter by CVE code, exploitability, CVSS score...

What are the critical and exploitable vulnerabilities in my Information System?

What do the authorities and the vendors say on CVE-2019-0708?

What are the public exploits available for CVE-2017-0143?

Am I affected by BlueKeep?

Website analysis based on the OWASP

Website analysis with spidering and tests based on the OWASP Web Security Testing Guide, technologies fingerprinting, and SSL / TLS hardening level assessment

Is there any potential SQL or XSS injection on my website?

Are my JavaScript libraries related to known CVE?

Do I still have SSLv3 or TLS 1.0 on my frontal web server ?

Cyberwatch

Assets Vulnerabilities Compliance Admin

Vulnerabilities / Security issues / SQL Injection

SQL Injection

Description

An SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the data input or transmitted from the client (browser) to the web application.

A successful SQL injection attack can read sensitive data from the database, modify database data (insert/update/delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file existing on the DBMS file system or write files into the file system, and, in some cases, issue commands to the operating system.

SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.

General

Reference: WSTG-INPV-05

Severity: **CRITICAL**

Max CVEs score: -

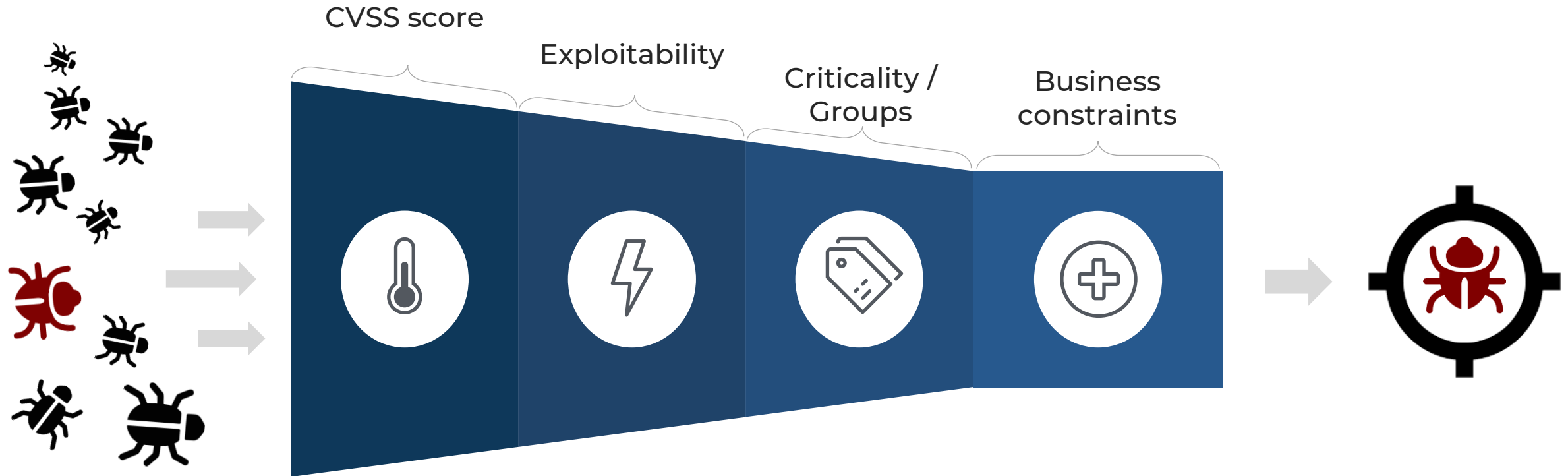
Max CVEs exploit code maturity: -

Published on 02/03/21 - Updated on 01/04/21

Related assets 17 Related CVEs 0 Tracked changes 0

Name	OS	Criticality	Groups	Payload	Comment	Detected at	Status
testphp.vulnweb.com		Medium		SQL Injection (DMBS: ...	Q	03/03/2021 11:54	Detected
testphp.vulnweb.com		Medium		SQL Injection (DMBS: ...	Q	03/03/2021 11:54	Detected
testphp.vulnweb.com		Medium		SQL Injection (DMBS: ...	Q	03/03/2021 11:54	Detected
testphp.vulnweb.com		Medium		SQL Injection (DMBS: ...	Q	03/03/2021 11:54	Detected
testphp.vulnweb.com		Medium		SQL Injection (DMBS: ...	Q	03/03/2021 11:54	Detected
testphp.vulnweb.com		Medium		SQL Injection (DMBS: ...	Q	03/03/2021 11:54	Detected
testphp.vulnweb.com		Medium		SQL Injection via inject...	Q	22/05/2021 17:53	Detected

Vulnerability prioritization



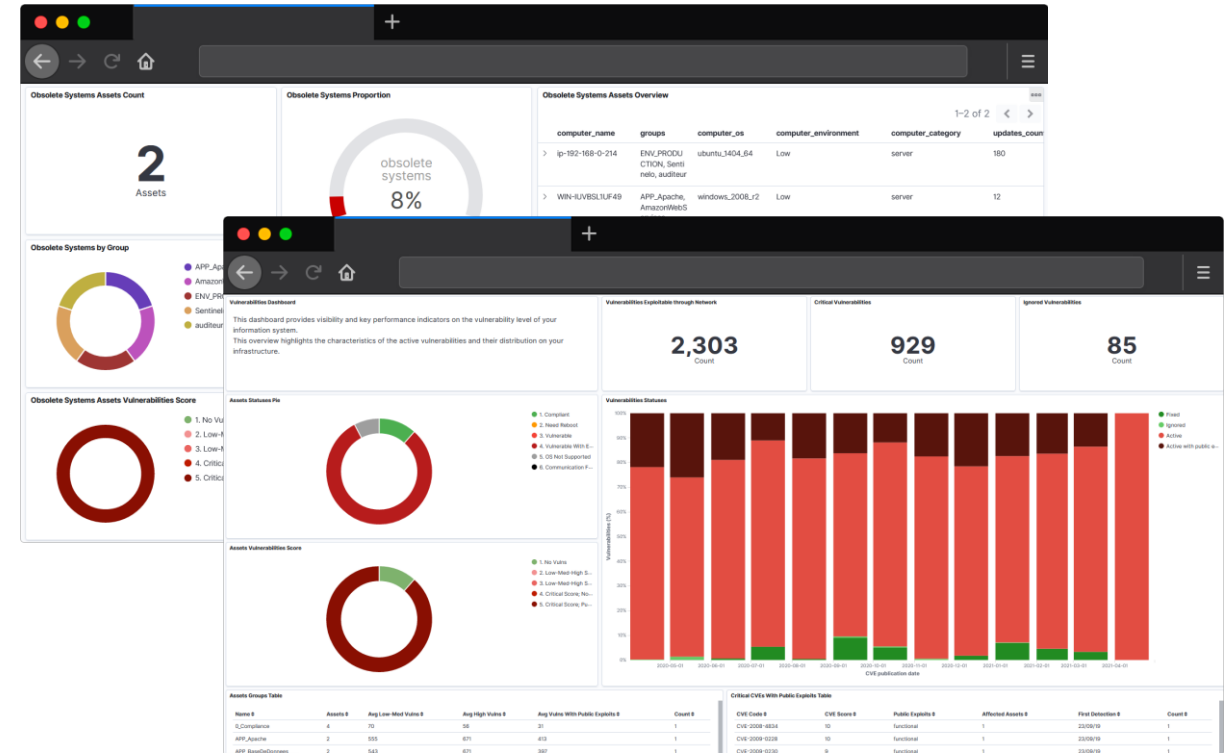
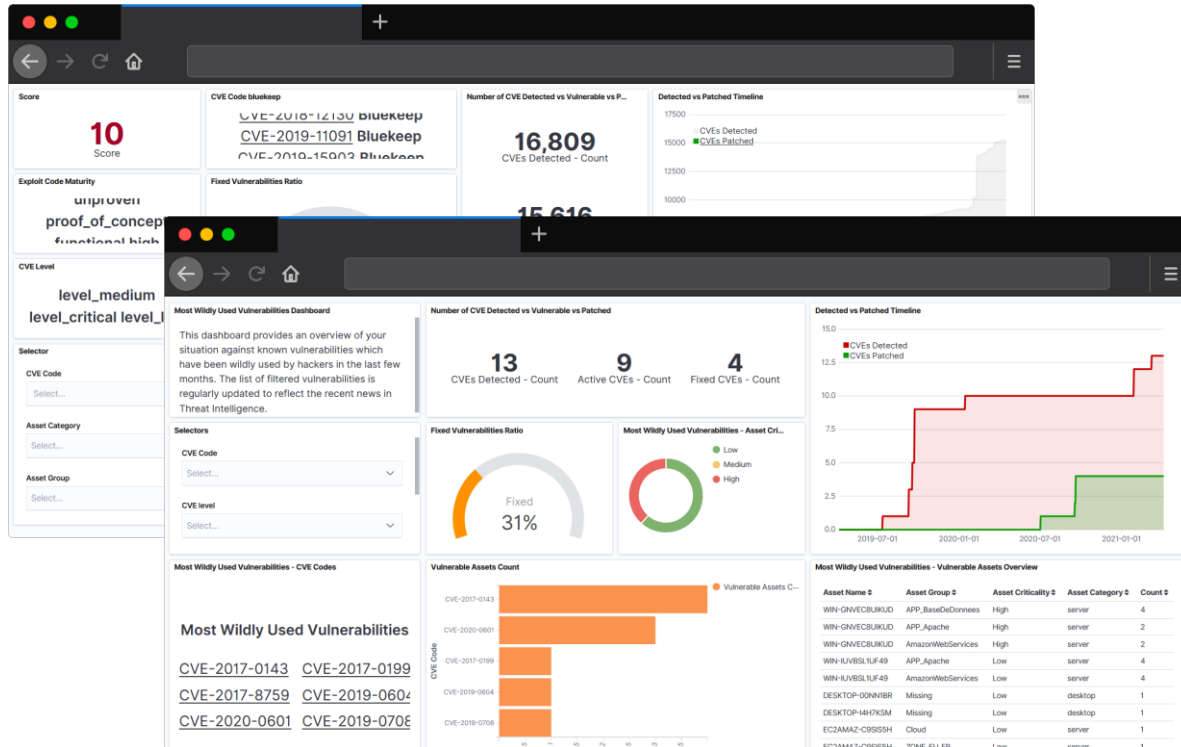
Cyberwatch helps you to **identify** the **most important risks** in your Information System
Cyberwatch provides you with a **default configuration**, that you can **adapt to your needs**

Risk analysis with MITRE ATT&CK®

Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 24 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 16 techniques	Exfiltration 8 techniques	Impact 13 techniques
External Remote Services	Remote Desktop Protocol	Boot or Logon Autostart Execution (2/14)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Man-in-the-Middle (0/2)	File and Directory Discovery	Remote Services (1/6)	Man-in-the-Middle (0/2)	Ingress Tool Transfer	Exfiltration (0/1)	Service Denial of Service (3/4)
Drive-by Compromise	Command and Scripting Interpreter (0/8)	Boot or Logon Initialization Scripts (0/5)	Access Token Manipulation (2/5)	Access Token Manipulation (2/5)	Steal or Forge Kerberos Tickets (1/4)	Account Discovery (0/3)	Remote Service Session Hijacking (0/2)	Data from Local System	Application Layer Protocol (0/4)	Data Transfer Size Limits	Account Access Removal
Exploit Public-Facing Application	Container Administration Command	Account Manipulation (0/2)	Create or Modify System Process (4/4)	Masquerading (0/6)	Brute Force (4/4)	Browser Bookmark Discovery	Taint Shared Content	Automated Collection	Communication Through Removable Media	Exfiltration Over Alternative Protocol (0/2)	Data Destruction
Hardware Additions	Deploy Container	BITS Jobs	Boot or Logon Autostart Execution (2/14)	Rootkit	Network Sniffing	Network Service Scanning	Software Deployment Tools	Data from Network Shared Drive	Data Encoding (0/2)	Exfiltration Over C2 Channel	Data Encrypted for Impact
Phishing (0/3)	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	BITS Jobs	Credentials from Password Stores (0/5)	Peripheral Device Discovery	Exploitation of Remote Services	Archive Collected Data (0/3)	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Data Manipulation (0/3)
Replication Through Removable Media	Inter-Process Communication (0/2)	Compromise Client Software Binaries	Escape to Host	Deobfuscate/Decode Files or Information	Exploitation for Credential Access	Permission Groups Discovery (0/2)	Internal Spearphishing	Audio Capture	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)	Defacement (0/2)
Supply Chain Compromise (0/3)	Native API	Create Account (0/2)	Domain Policy Modification (0/2)	Deploy Container	Focused Authentication	Process Discovery	Lateral Tool Transfer	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Trusted Relationship	Scheduled Task/Job (0/7)	Hijack Execution Flow (0/11)	Event Triggered Execution (3/15)	Direct Volume Access	Forge Web Credentials (0/2)	Remote System Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Fallback Channels	Exfiltration Over Web Service (0/2)	Firmware Corruption
Valid Accounts (3/3)	Shared Modules	Create or Modify System Process (4/4)	Event Triggered Execution (3/15)	Domain Policy Modification (0/2)	Input Capture (0/4)	System Information Discovery	Use Alternate Authentication Material (2/2)	Data from Information Repositories (0/1)	Multi-Stage Channels	Scheduled Transfer	Inhibit System Recovery
	System Services (0/2)	External Remote Services	Hijack Execution Flow (0/11)	Execution Guardrails (0/1)	Modify Authentication Process (0/4)	System Network Configuration Discovery (0/1)		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2/2)
	User Execution (0/3)	Event Triggered Execution (3/15)	Process Injection (0/11)	Exploitation for Defense Evasion	OS Credential Dumping (0/8)	System Owner/User Discovery		Data Stage (0/2)	Non-Standard Port		Resource Hijacking
	Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (0/7)	File and Directory Permissions Modification (0/2)	Steal Web Session Cookie	System Service Discovery		Email Collection (1/3)	Protocol Tunneling		Service Stop
		Modify Authentication Process (0/4)	Valid Accounts (3/3)	Hide Artifacts (0/7)	Two-Factor Authentication Interception	System Time Discovery		Man in the Browser	Proxy (0/4)		System Shutdown/Reboot
		Office Application Startup (0/6)		Hijack Execution Flow (0/11)	Unsecured Credentials (3/6)	Network Sniffing		Host Capture (0/4)	Remote Access Software		
		Pre-OS Boot (1/5)		Impair Defenses (2/5)		Application Window Discovery		Screen Capture	Traffic Signaling (0/1)		
		Scheduled Task/Job (0/7)		Indicator Removal on Host (0/6)		Container and Resource Discovery		Video Capture	Web Service (0/3)		
		Server Software Component (1/3)		Indirect Command Execution		Domain Trust Discovery					
		Traffic Signaling (0/1)		Modify Authentication Process (0/4)		Password Policy Discovery					
		Valid Accounts (3/3)		Modify Registry		Query Registry					
				Modify System Image (0/2)		Software Discovery (0/1)					

Cyberwatch generates the **MITRE ATT&CK® framework** based on your vulnerabilities. You can then **identify your killchain** and **compare it against known APT**.

Customizable reports



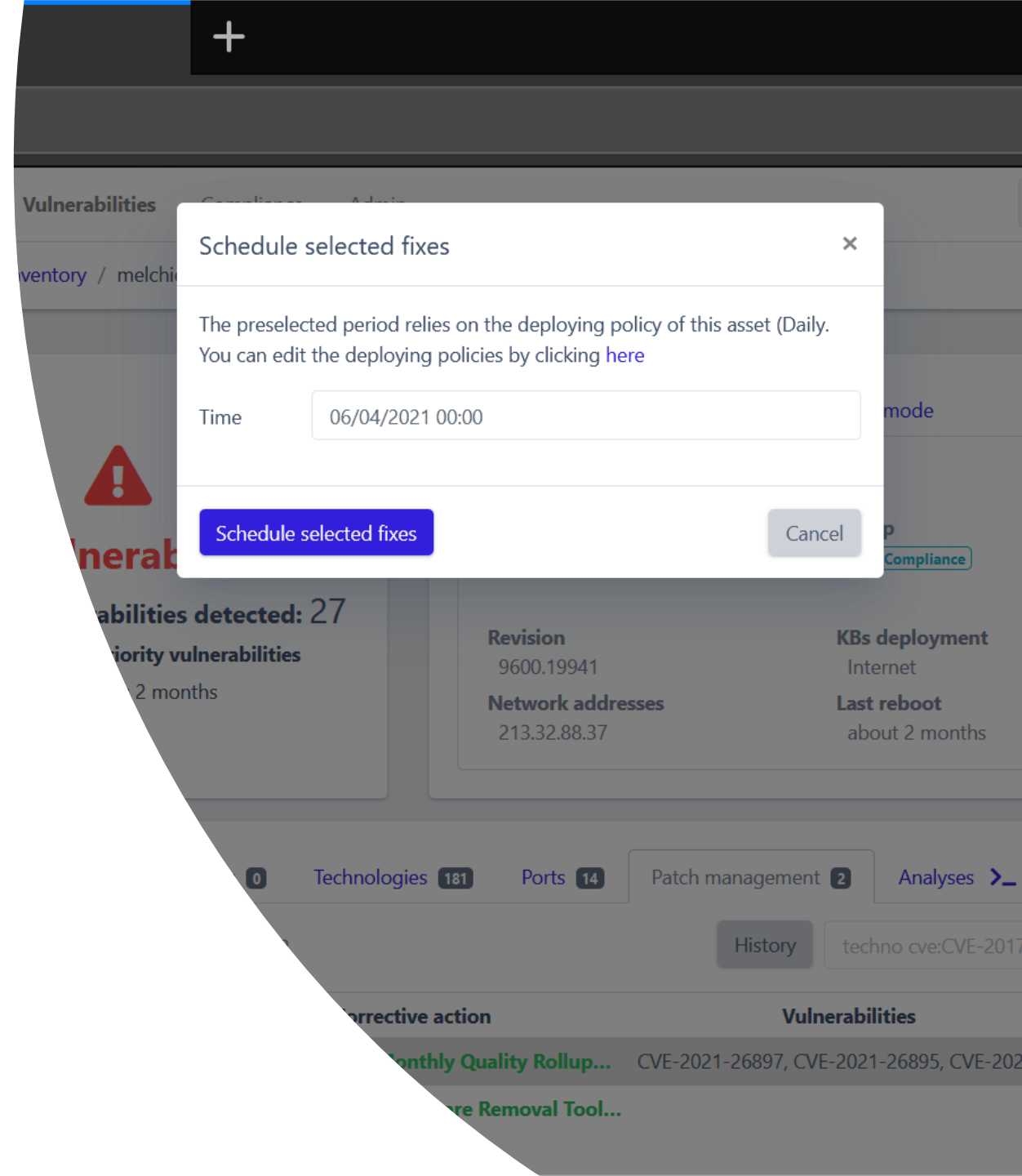
Cyberwatch provides you with **reports** with several **default templates**
Cyberwatch lets you **choose / edit** the **visualizations** and the **data to analyze**

Patch Management module (optional)

Cyberwatch embeds an optional **Patch Management** module

Cyberwatch helps you to identify the vulnerabilities and to **deploy** the appropriate **security fixes**

The security fixes are deployed in **compliance with your settings** (internal repositories, WSUS...)



The screenshot shows a web interface for creating a security issue. At the top, there are navigation tabs for 'Vulnerabilities', 'Compliance', and 'Admin'. Below this is a breadcrumb trail 'Security issues / Creation'. The main heading is 'Security issue Creation'. The form contains several fields: 'Reference' with the value 'Pentest ref CBW-2021-XXX-PENTEST'; 'Title' with the value 'HTTP Headers verification issue in XXXX'; 'Description' with the text 'The 443 port of the target exposes a web service with a form that does'; 'Severity' with the value 'Critical'; 'Assets' with a tag 'WIN-GNVEC8UIKUD'; and 'CVEs' with a search input 'Search for a CVE'. A blue 'Save' button is located at the bottom of the form.

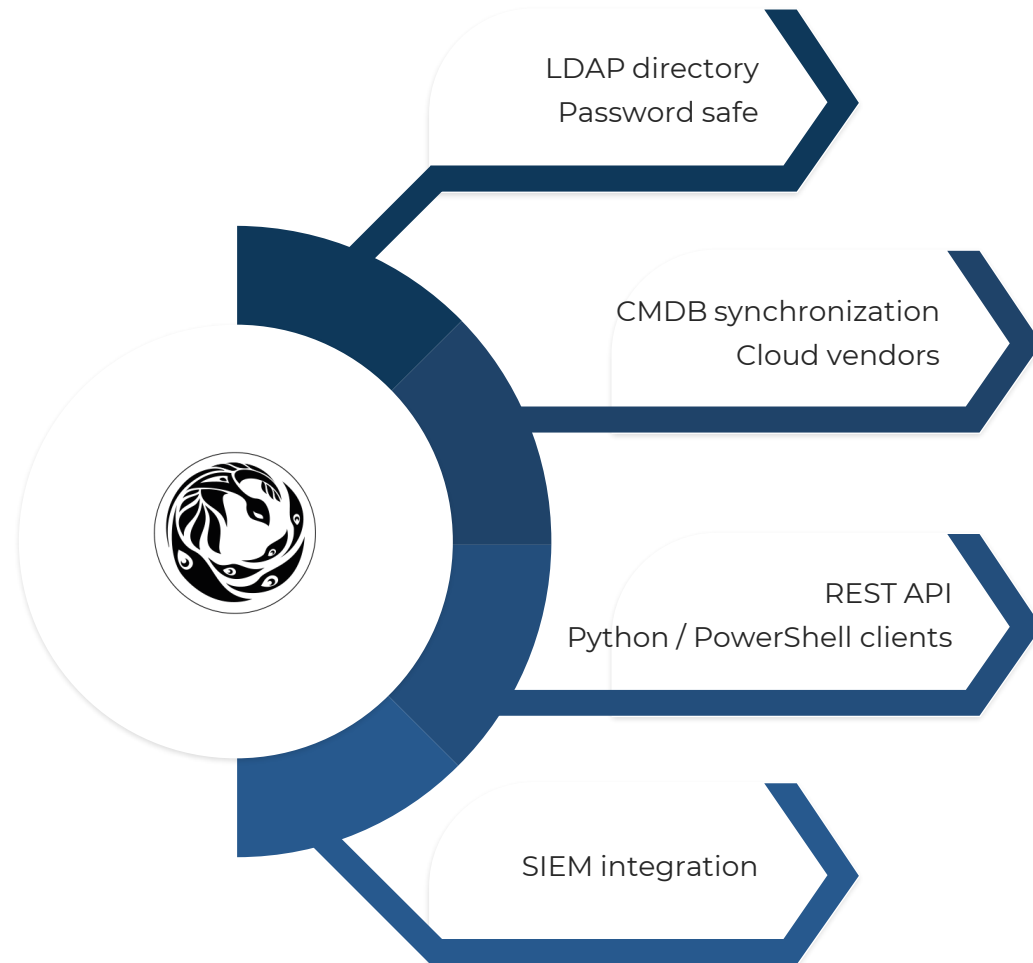
Option – Penetration testing data import

Cyberwatch provides an optional module to **import data from Pentest reports**

Cyberwatch allows you to **enrich** and **centralize** data from your security audits services, on a unique interface

Imported data can then be marked by your team, as fixed or accepted

Integrations with other tools



Cyberwatch offers a REST API to:

- Automate the tickets creation;
- Send information for human review;
- Trigger an action in a third-party tool (WAPT, Chocolatey, SUSE Manager...);
- Compare the scanning scope with a third-party repository (ActiveDirectory, CMDB, Public Cloud...);
- Import results from third-party sources.

Cyberwatch also has native integrations with LDAP, SAML, Syslog, Wallix...

For more information

www.cyberwatch.fr
contact@cyberwatch.fr

+33 1 85 08 69 79



French company

Selected by



H E X A T R U S T

CLOUD CONFIDENCE & CYBERSECURITY

