

framatome

Actifs, Vulnérabilités,
Risques et
Remédiations,
comment gérer le
chaos ?

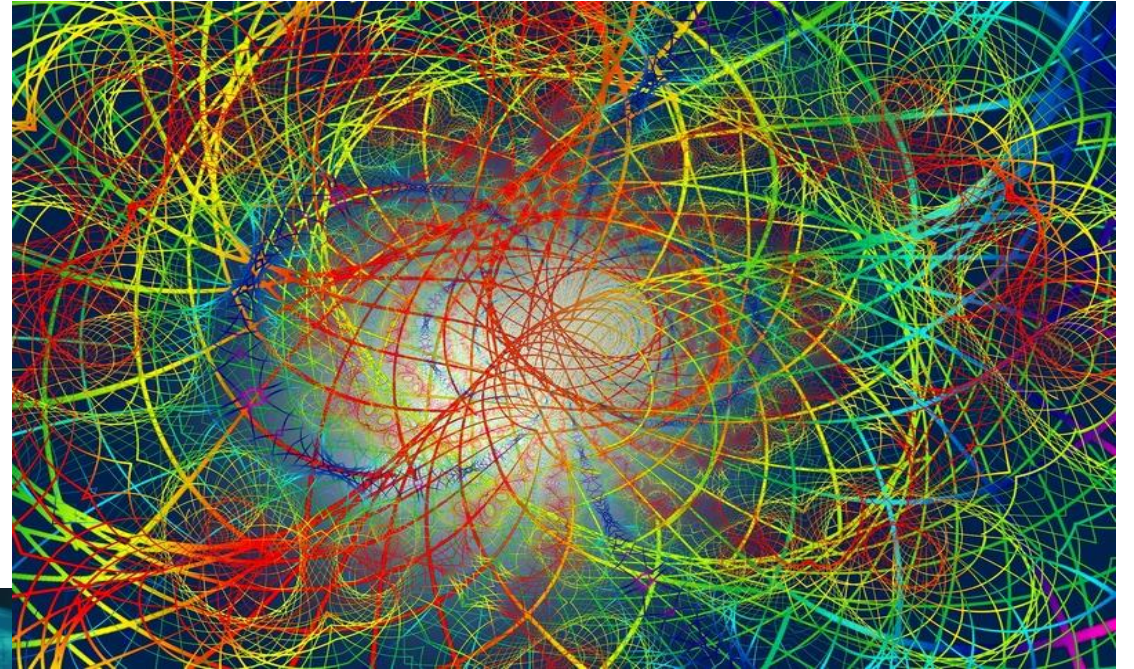
Framatome Cybersecurity

29 novembre 2023



Le Chaos - définition

- Grand désordre, confusion générale.
- Chaos déterministe, régis par des lois d'évolution parfaitement déterministes, devient imprévisible au bout d'un temps relativement court.

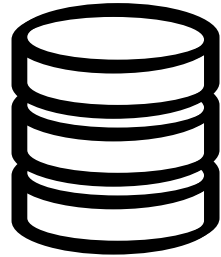


Inventaire des actifs IT, OT et IT for OT



Postes de travail

Postes fixes
Postes nomades



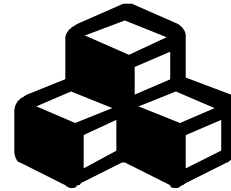
Serveurs

Machines virtuelles
Machines physiques
Hyperviseurs
Mainframes



Equipements réseaux

Routeurs
Switchs
Pare-feu



Conteneurs

Images
Instances



Sites web

URLs
Adresses IP



Equipements industriels

Firmwares
d'automates



Bibliothèques logicielles

Modules de
développement

NUTANIX™

CLAROTY



Microsoft
Azure

GitLab

vmware
ESXi

Google Cloud

OpenLDAP



docker

GLPI

SECKIOT

vmware®

servicenow

openstack.

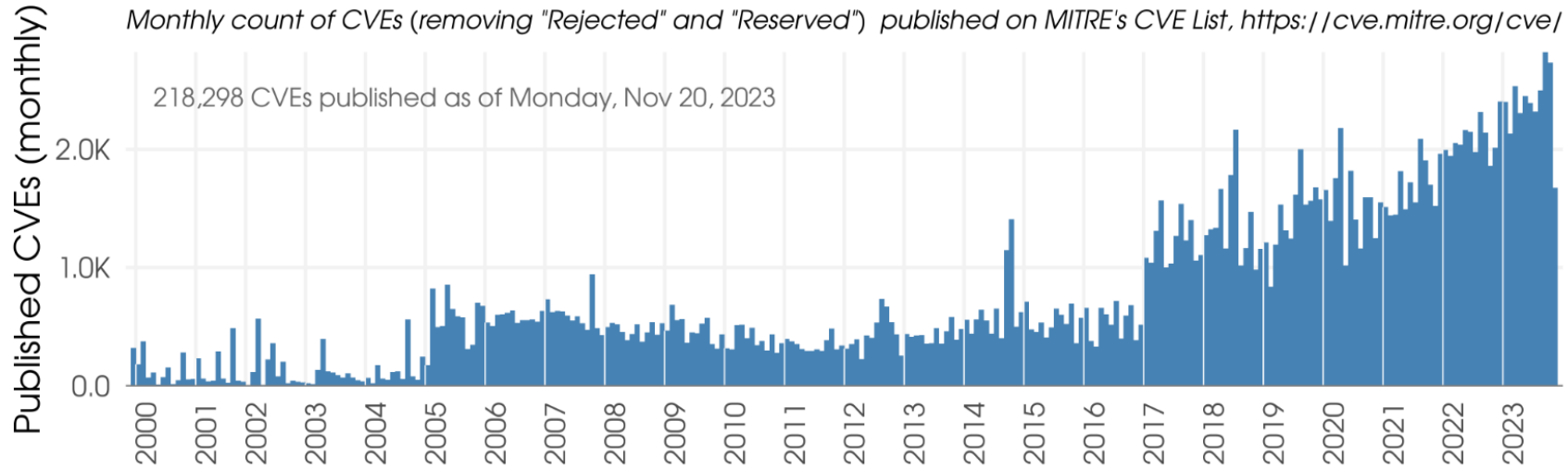
aws

Active Directory

Chaos sur les vulnérabilités

Monthly counts of CVE publications (MITRE CVE List)

Monthly count of CVEs (removing "Rejected" and "Reserved") published on MITRE's CVE List, <https://cve.mitre.org/cve/>



80%

des cyberattaques
auraient pu être évité en
appliquant un patch

SOURCE: Microsoft

Des objectifs difficilement conciliables



**RSSI
CISO**



**Directeur
Site**



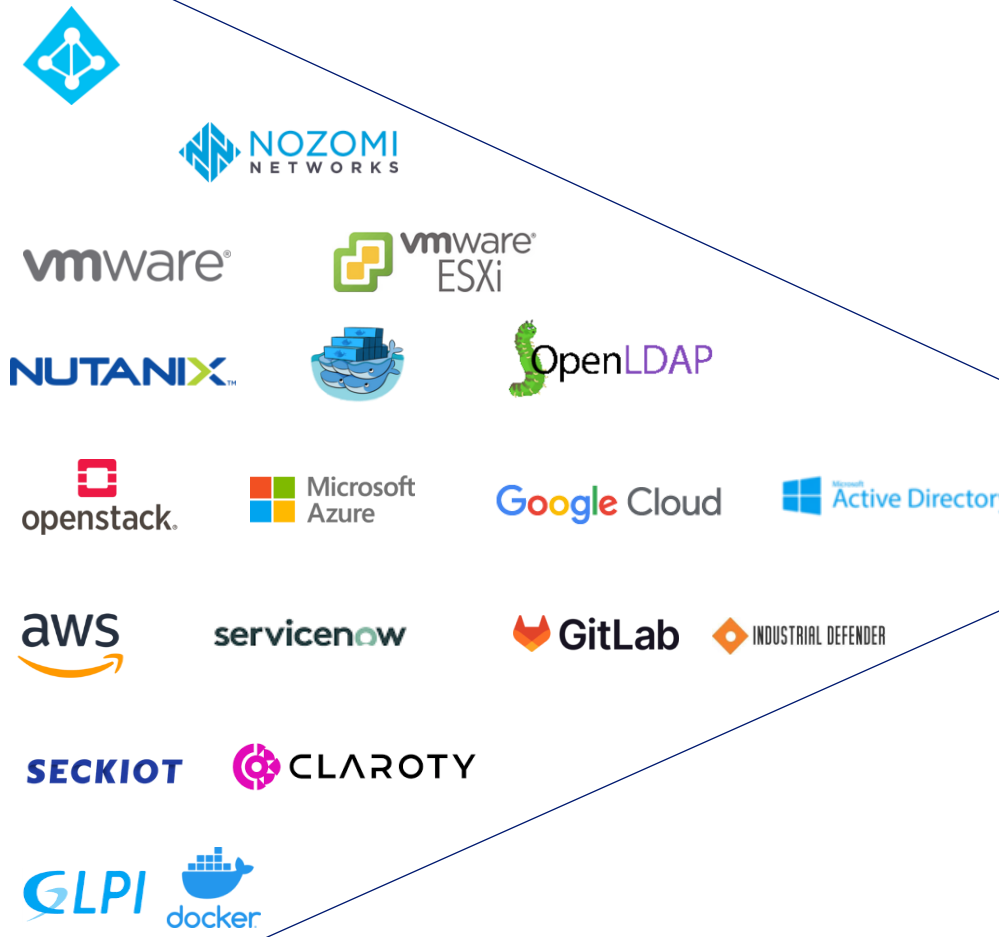
**Responsable
Production**



Comment organiser le chaos ?



Consolider l'inventaire

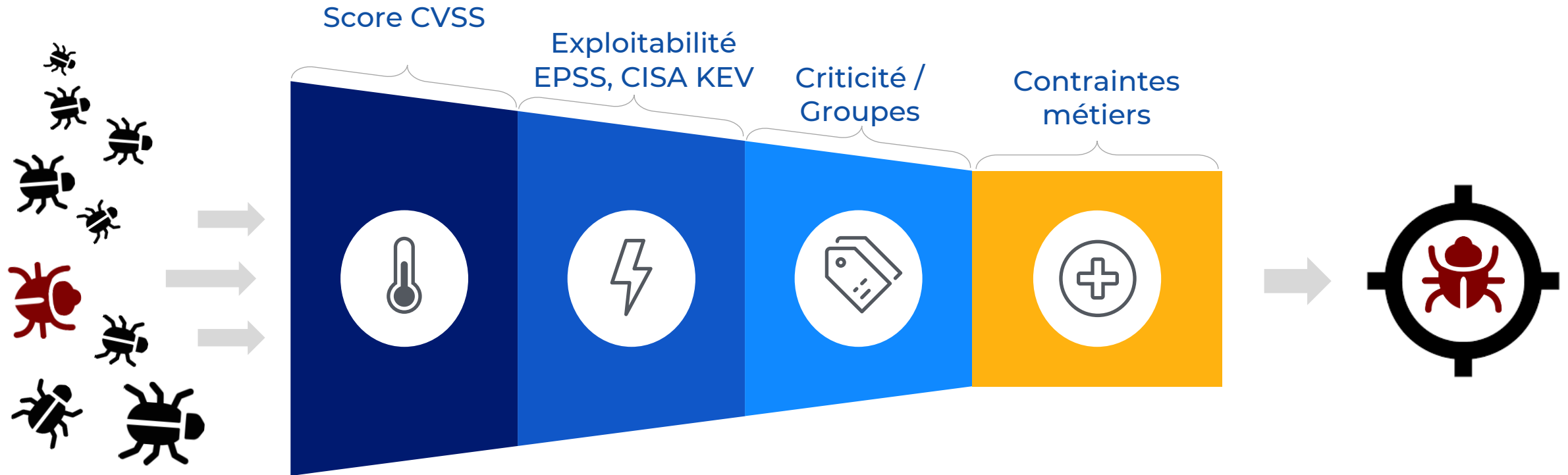


The screenshot shows a dashboard with a sidebar menu on the left and a main content area on the right. The sidebar menu includes sections like ASSETS, ENCycLOPEDIAS, and REPORTS. The main content area displays a table of assets with the following columns: Category, Operating system, Criticality, and Group. Below the table, there are pagination controls and buttons for Export, Bulk edits, and Bulk actions.

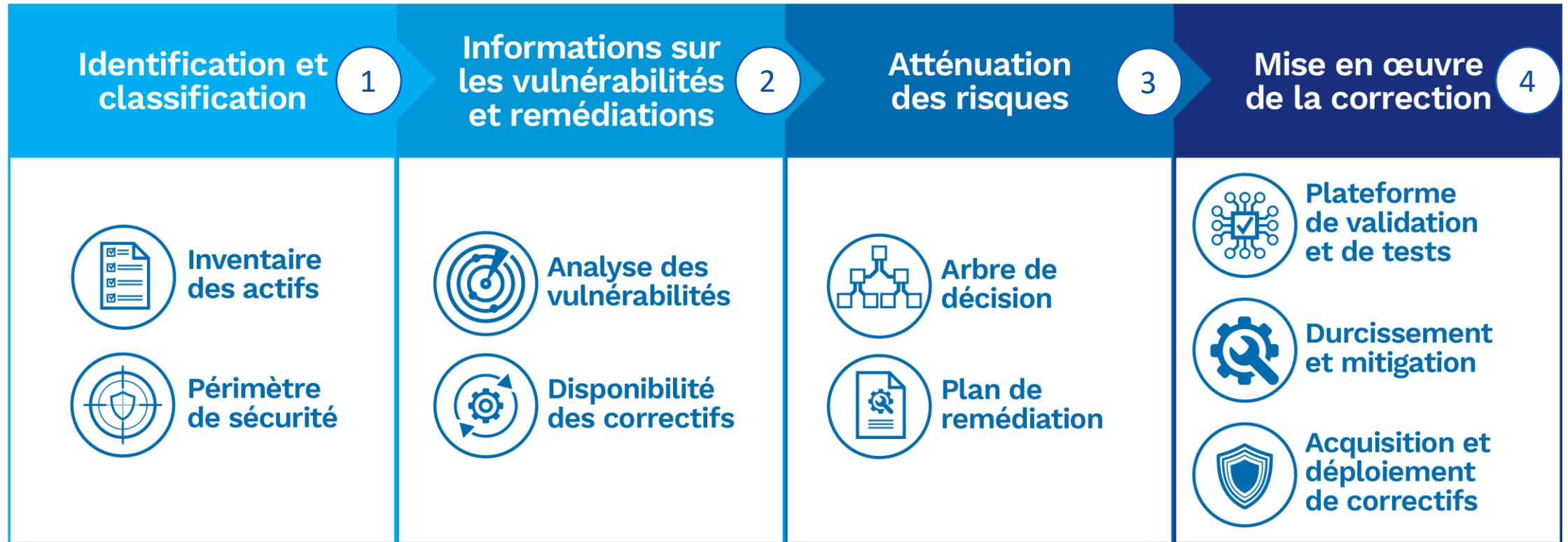
Category	Operating system	Criticality	Group
Cloud	Hirschmann	High	Network
Desktop	Juniper	Low	Operator-Engineering
Docker Image	pfsense	Medium	PLC
Hypervisor	RHEL 8	Medium (CVSS)	
Industrial Device	Siemens		
Mobile	Stormshield		
Network Device	Ubuntu 22.04		
Network Target or website	Ubuntu 22.04		
None	Windows 7		
Server	Windows 10 21H2		
	Windows 2012 R2		

Name	System	Criticality	Groups	CVES
pfsense.localdomain	pfsense	Medium (CVSS)	Network	6
rhel8-2	redhat	Medium (CVSS)		14
rhel8-2	redhat	Medium (CVSS)		14
VMSNSX00C1212A9	stormshield	Medium (CVSS)		48
172.20.12.13	SIEMENS	Medium (CVSS)	PLC	
BRS-A0B0867BB8E3	HIRSCHMANN	Medium (CVSS)	Network	
S71500/ET200MP station_1	SIEMENS	Medium (CVSS)	PLC	
WIN-HNS1KQDU9NS-HMI1-a...	Windows7	Medium (CVSS)	Operator-Engineer...	

Prioriser les vulnérabilités



Maintien en Condition de Sécurité



Un parcours de l'inventaire à la remédiation

Apprenez à surfer sur la vague !



**Pour plus d'informations et échanges,
rencontrons-nous au stand N° 12**

<https://framatomecybersecurity.com/>

framato**me**

Merci