Patch me, if you can …

Dezernat 4
Bürgerservice, öffentliche Ordnung, Personal und IT

$ whoami

20+ Jahre Linux & OSS

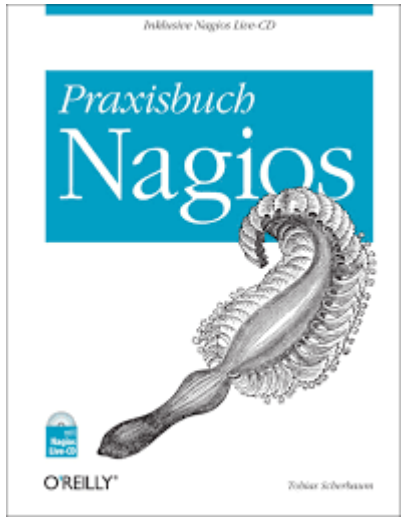
Monitoring

Admin

Sachgebietsleitung für Fachverfahren, Infrastruktur & IT-Sicherheit

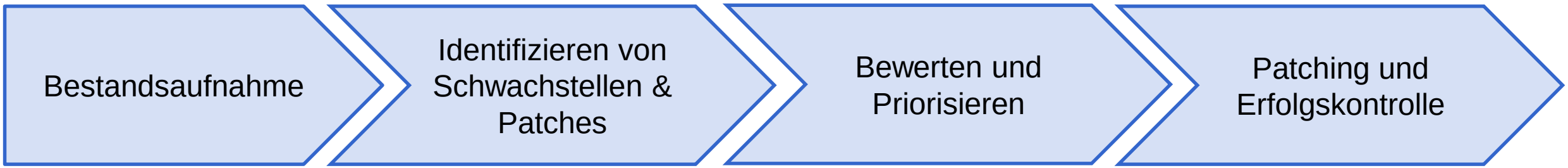
Seit 2021: IT-Sicherheit

gentoo linux

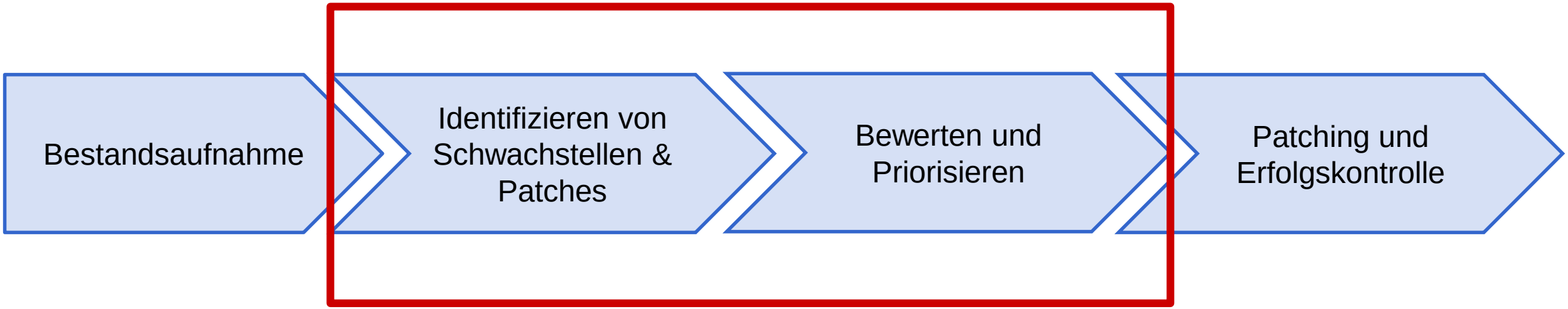


stadt
oberhausen

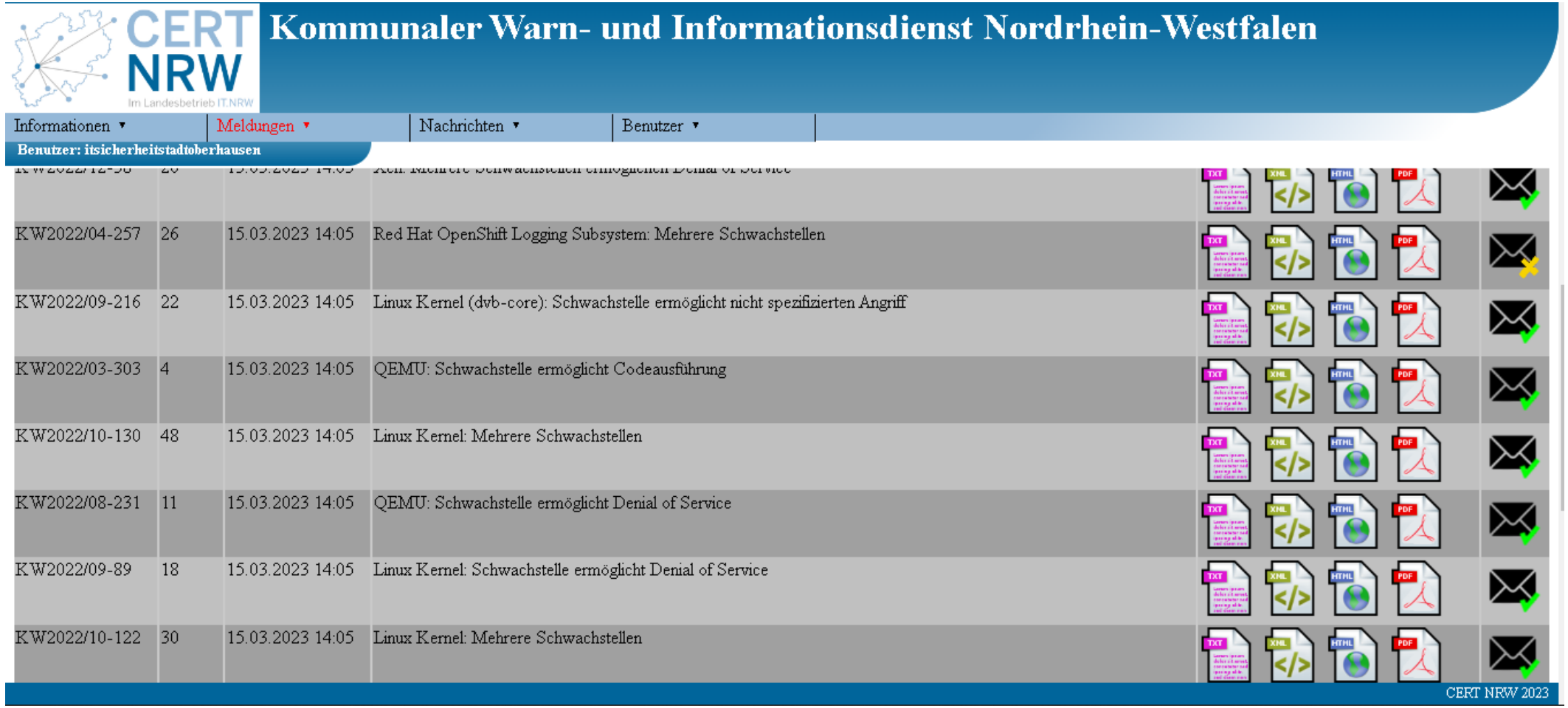
Patchmanagementprozess



Patchmanagementprozess



Kommunaler Warn- und Informationsdienst



Schwachstellen als App im Matrix42 Servicedesk

Ticket...	Zusammenfassung	Erstelldatu...	CVE	CPE Tags	CVE Risiko ...	Meldungsnummer
SEC01395	KW2023/03-149: Microsoft Azure Produ...	15.03.2023...	CVE-2023-23383,CVE-2023-23408	cpe:/a:microsoft:azure_hdinsights,cpe:...	Hoch	KW2023/03-149
SEC01394	KW2023/03-150: Microsoft Visual Studio...	15.03.2023...	CVE-2023-22490,CVE-2023-2274...	cpe:/a:microsoft:visual_studio_2017,c...	Hoch	KW2023/03-150
SEC01393	KW2023/03-126: Adobe Creative Cloud: ...	15.03.2023...	CVE-2023-25859,CVE-2023-2586...	cpe:/a:adobe:creative_cloud	Hoch	KW2023/03-126
SEC01391	KW2023/03-128: Zoom Video Communic...	15.03.2023...	CVE-2023-22880,CVE-2023-2288...	cpe:/a:zoom:zoom_client	Hoch	KW2023/03-128
SEC01390	KW2023/03-131: Lenovo BIOS: Mehrere ...	15.03.2023...	CVE-2022-3728,CVE-2022-4573,...	cpe:/h:lenovo:bios	Mittel	KW2023/03-131
SEC01389	KW2023/03-132: Adobe Photoshop: Sch...	15.03.2023...	CVE-2023-25908	cpe:/a:adobe:photoshop	Mittel	KW2023/03-132
SEC01388	KW2023/03-139: Microsoft Malware Pro...	15.03.2023...	CVE-2023-23389	cpe:/a:microsoft:malware_protection_...	Mittel	KW2023/03-139
SEC01387	KW2023/03-143: Microsoft Office: Mehr...	15.03.2023...	CVE-2023-23391,CVE-2023-2339...	cpe:/a:microsoft:365_apps,cpe:/a:micr...	Hoch	KW2023/03-143
SEC01386	KW2023/03-141: Microsoft Windows un...	15.03.2023...	CVE-2023-1017,CVE-2023-1018,...	cpe:/o:microsoft:windows_10,cpe:/o:m...	Hoch	KW2023/03-141
SEC01385	KW2023/03-145: Mozilla Firefox: Mehrer...	15.03.2023...	CVE-2023-25748,CVE-2023-2574...	cpe:/a:mozilla:firefox,cpe:/a:mozilla:fire...	Hoch	KW2023/03-145
SEC01384	KW2023/03-142: Linux Kernel: Schwach...	15.03.2023...	CVE-2023-1390	cpe:/o:linux:linux_kernel	Mittel	KW2023/03-142
SEC01383	KW2023/03-146: Microsoft OneDrive für ...	15.03.2023...	CVE-2023-24890	cpe:/a:microsoft:onedrive	Mittel	KW2023/03-146
SEC01382	KW2023/03-118: docker: Mehrere Schw...	14.03.2023...	CVE-2023-0628,CVE-2023-0629	cpe:/a:docker:docker	Mittel	KW2023/03-118
SEC01381	KW2023/03-120: Linux Kernel: Schwach...	14.03.2023...	CVE-2023-1380	cpe:/o:linux:linux_kernel	Mittel	KW2023/03-120
SEC01380	KW2023/03-122: Linux Kernel: Schwach...	14.03.2023...	CVE-2023-1032	cpe:/o:linux:linux_kernel	Mittel	KW2023/03-122
SEC01379	KW2023/03-113: Lexmark Drucker: Mehr...	13.03.2023...	CVE-2023-26063,CVE-2023-2606...	cpe:/h:lexmark:laser_printer,cpe:/h:lex...	Hoch	KW2023/03-113
SEC01378	KW2023/03-110: Linux Kernel: Mehrere ...	13.03.2023...		cpe:/o:linux:linux_kernel	Mittel	KW2023/03-110
SEC01377	KW2023/03-112: vim: Schwachstelle er...	13.03.2023...	CVE-2023-1355	cpe:/a:vim:vim	Mittel	KW2023/03-112
SEC01376	KW2023/03-104: ImageMagick: Schwac...	10.03.2023...	CVE-2023-1289	cpe:/a:imagemagick:imagemagick	Mittel	KW2023/03-104
SEC01372	KW2023/03-96: memcached: Schwachs...	09.03.2023...	CVE-2023-27478	cpe:/a:memcache_project:memcache	Mittel	KW2023/03-96

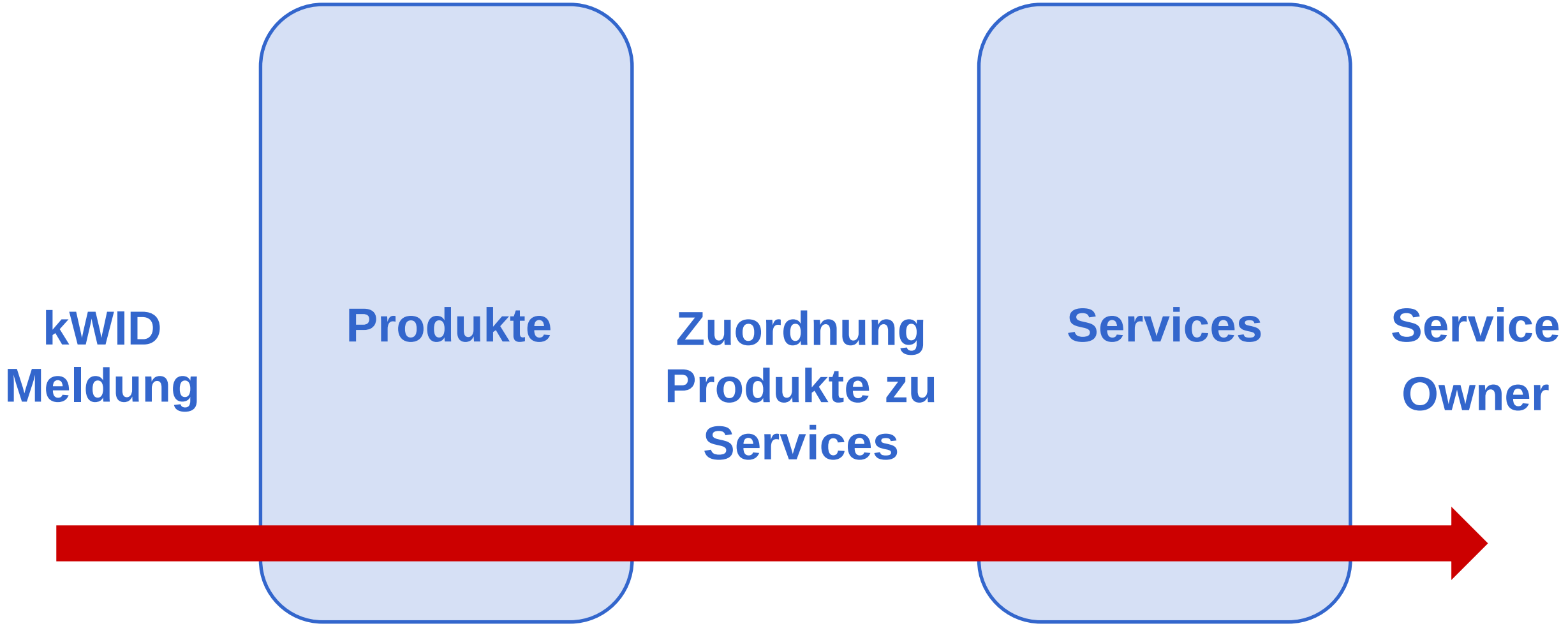
CVE: https://de.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures
CPE: https://de.wikipedia.org/wiki/Common_Platform_Enumeration

Automatisierte Aufgabenerstellung und Weiterleitung in Matrix 42

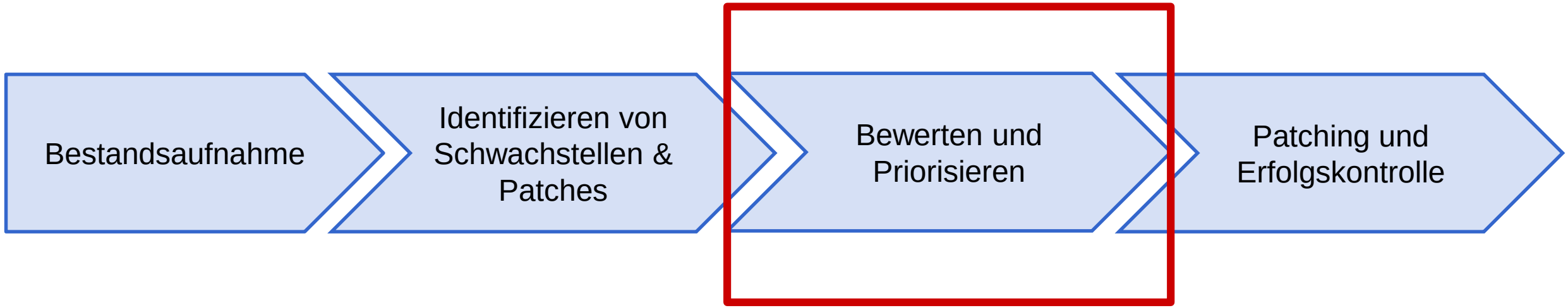
Produkte

Services

Automatisierte Aufgabenerstellung und Weiterleitung in Matrix 42



Patchmanagementprozess



2022

4595

Schwachstellen

1015

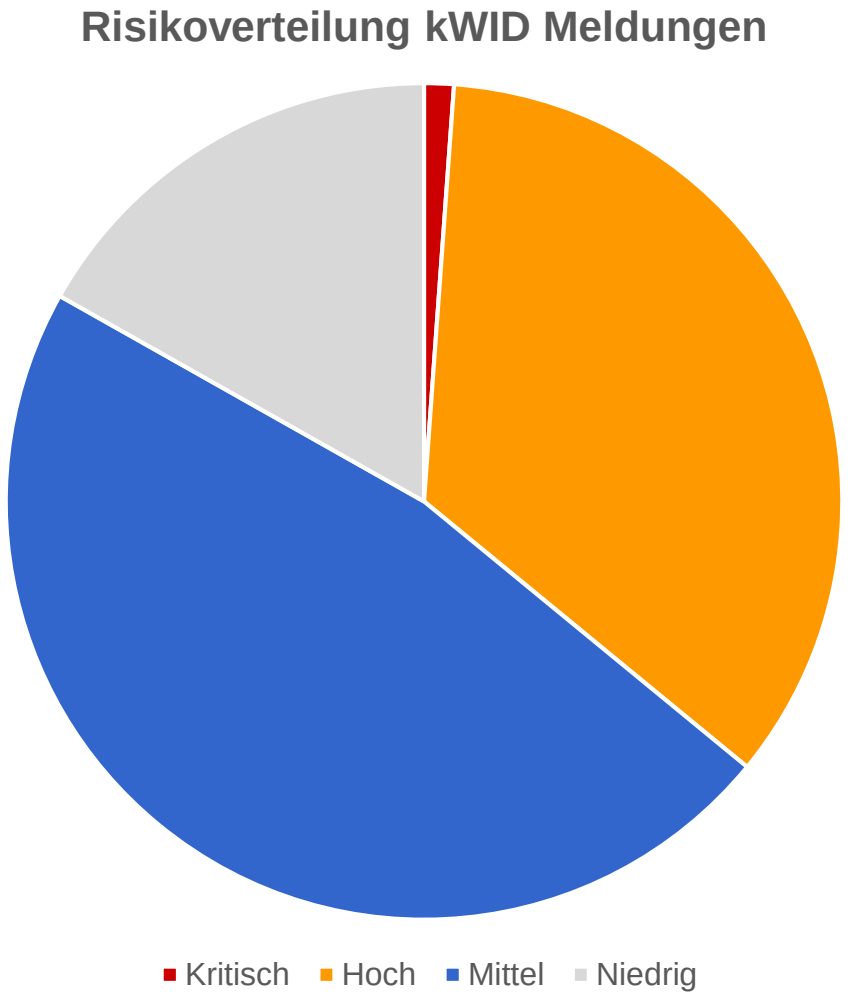
… davon in Microsoft Produkten

1046

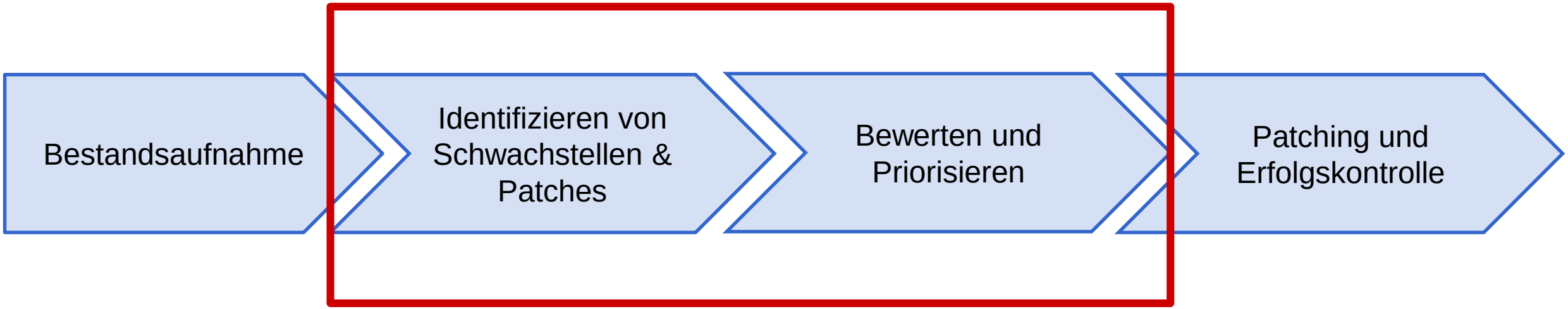
kWID Meldungen

72

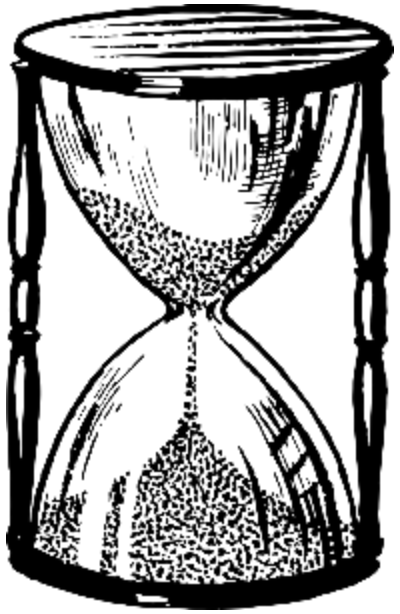
Texteditor

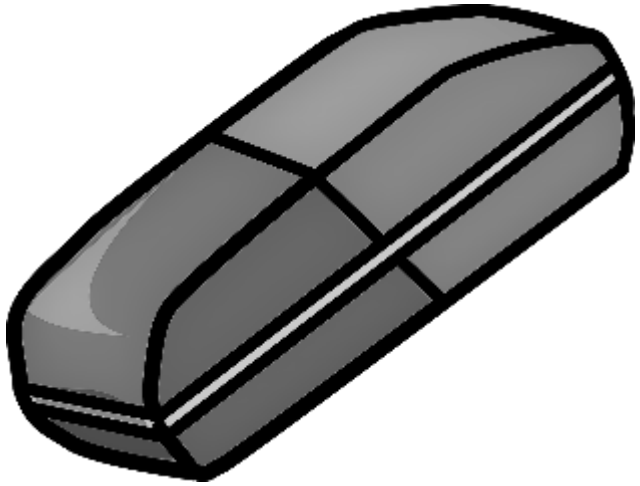


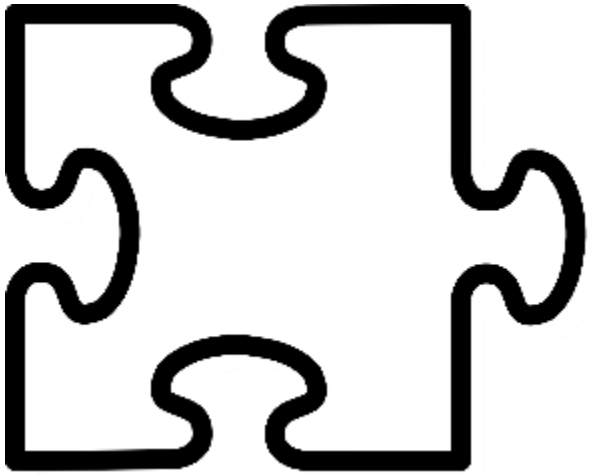
Patchmanagementprozess



Erfahrungen mit dem kWID





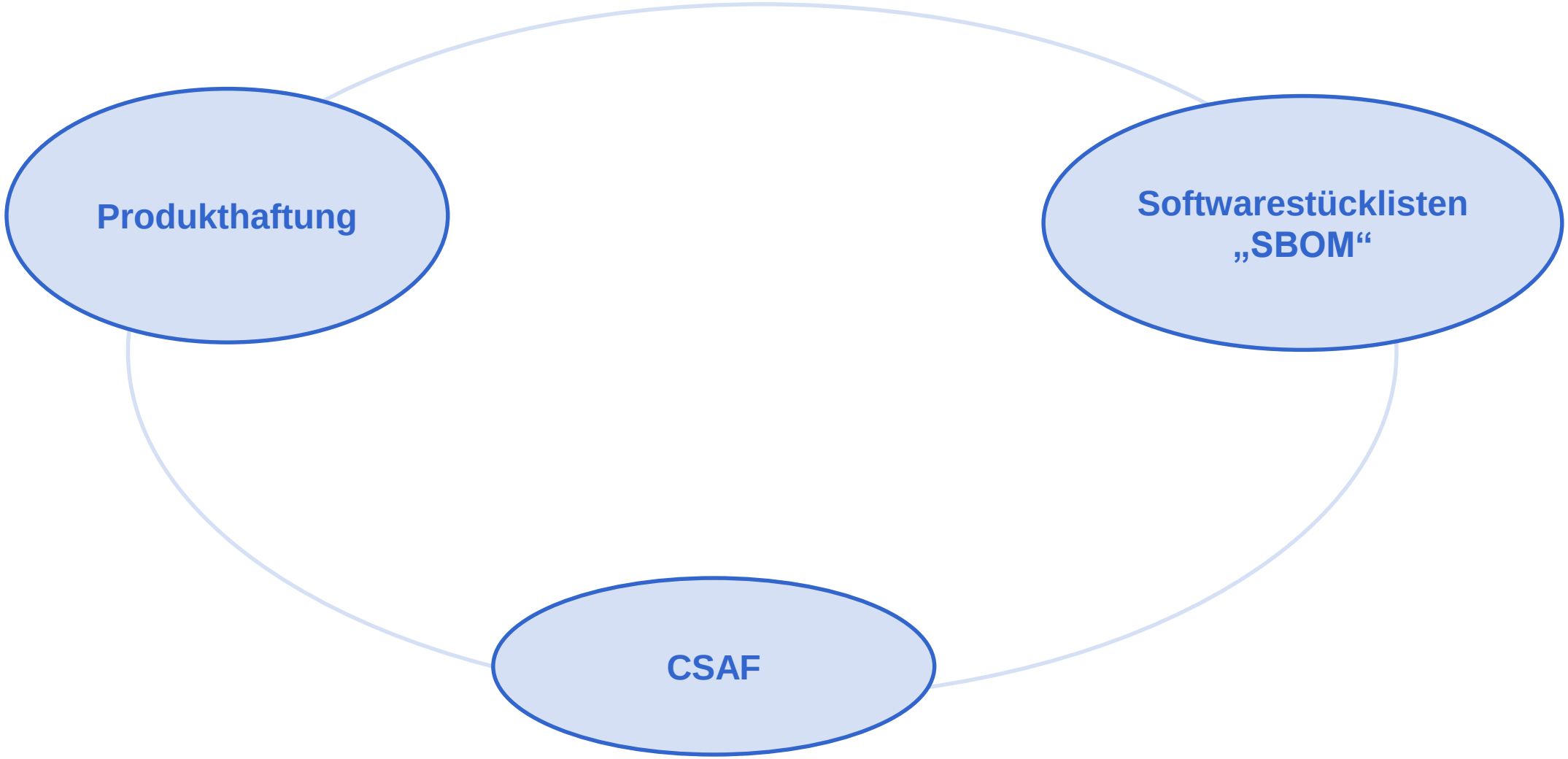


CISA, Cybersecurity & Infrastructure Security Agency https://www.cisa.gov
Known Exploited DB: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Grafiken: Pixabay, lizenzfrei.

Was wir wissen, was wir nicht wissen ….

Ein Blick in die Zukunft …



SBOM: Software Bill of Materials, Softwarestückliste https://de.wikipedia.org/wiki/St%C3%BCckliste
CSAF: Common Security Advisory Framework https://csaf.io/

… und jetzt viel Erfolg beim Patchen ;)

Kontaktdaten

Stadt Oberhausen
Bereich 4-4 / IT
Bahnhofstr. 66
46145 Oberhausen

tobias.scherbaum@oberhausen.de
0208 / 825-7536