European Union Agency
for Cybersecurity
Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

RECORD NO: 76

CNW CENTRAL SERVICES TOOLS COLLECTION

Record 76 of processing operation "CNW Central Services Tools collection"	
Date of last update	22/09/2025
Name and contact details of controller	ENISA, Operational Cooperation Unit (CSIRTs Network Secretariat), cnw [at] enisa.europa.eu with the support of Operational Cooperation Unit, OCUTools [at] enisa.europa.eu
Name and contact details of DPO	dataprotection [at] enisa.europa.eu
Name and contact details of Joint Controller	European Union CSIRTs Network composed of EU Member States' appointed CSIRTs and CERT-EU.
Name and contact details of processor	• Simple Email Service of Amazon Web Services (Amazon SES), under a contract with ENISA from the Cloud II Framework Contract; used for sending automated outgoing emails that are generated by the operational tools like the identity provider and the chat messaging platform. Amazon SES only sends emails and it does not store any information for business use, apart from technical usage data that are necessary for the provision of the service (for example, emails bouncing back). Technical data storage at rest is within the EU only. • Microsoft Azure, under the same EU Cloud II Framework Contract as Amazon SES; used for hosting a website that provides ENISA-related services. As with SES, Azure is subject to the contractual terms established under this framework and has publicly affirmed alignment with EU data protection standards applicable to the contract. • Unisystems and EdW consortium who is responsible for the support and maintenance of the applications and infrastructure. • L-Soft: mailing list provider listserv (www.lsoft.com), based in Sweden under a contract with ENISA. Additional information are available under Record No 73 - Mailing List. • DFN-CERT Services GmbH: encrypted mailing list provider, based in Germany under a contract with ENISA. • Microsoft GitHub Enterprise Cloud: support tool offered optionally to the CNW members upon request and to ENISA staff, based in US (subscriptions purchased through EC DG DIGIT SIDE II Framework Contract to which ENISA is also a party).
Purpose of the processing	The purpose of this processing operation is to support the CSIRTs Network in the operational information exchange and incident response through provision of a collection of tools used under the CNW Central Services Facility (ex. MeliCERTes) that includes: • Team Management software (Cerebrate). Provisions users in IAM/SSO. Contains User and teams information, logs. • IAM/SSO (Identity and Access Management solution/Single Sign On) used for federated authentication. User accounts, user logs containing personal data are created and maintained. • Chat messaging platform. Users, logs, posts, files.

	• CSIRTs Network (CNW) Portal for files storage and online editing. Users, teams information, files. • CSIRT Network Minisite, hosts only publicly available informational content related to the activities of the CSIRT Network. The data presented on this minisite includes an interactive map displaying national CSIRTs, which is embedded and sourced from https://tools.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map Record No 33 - CSIRTs Network Secretariat provides additional information on the CNW processing operation. Regarding the Web Conferencing and the Events organization activities, more information are available under Record No 26 - Web Conferencing Tools and Record No 28 - Events Organization respectively. Further to this, monitoring and logging software on-prem e.g., Splunk and as service mechanism in the cloud are used for better visibility on the security status of the above mentioned tools e.g., Microsoft Defender and Redhat Insights. In SaaS services, diagnostic data is stored and further processed in pseudonymised form. Retention period in ENISA's tenant is configurable by ENISA (minimum 1 month). Additional information is available under Record No 58 - Server and Endpoint security. WEDOS is also used for providing advanced DDoS protection (up to L7) for all of on-prem CNW central services assets.Custom setup is used for termination of traffic within EU territory (for the decryption and re-encryption that is needed for the L7 protection). *The "MeliCERTes 2" project (SMART2018/1024 project, contract NUMBER - LC-0133746) was 100% EU−funded, for which the European Commission was the owner of its outcomes until 18/12/2022. Since then, the legal ownership was transferred to ENISA with the handover letter of 16/12/2022, Ref. Ares (2022)8749927.*
Description of data subjects	• Officially appointed CNW Members • ENISA appointed staff offering the CNW Secretariat • ENISA OCU staff members dealing with tools IT operations • ENISA/OCU contractors for the support and maintenance of the tools • For operational data (information exchange) potentially any individual whose personal data are processed in the context of an incident information sharing within the CSIRTs network (see data categories).
Description of data categories	The following personal data are collected: • User account information details for the use of CNW services collection such as First and Last name, Email address, telephone number, appointing authority etc. • Posts,chats, emails or any other activity performed by users within the CNW services collection • Personal data related to posting and/or sharing reports, data, events, alerts etc with the CNW *Note: ENISA does not generate itself operational data but rather supports the exchange of operational data between CSIRT network members.*
Time limits (for the erasure of data)	• Administrative data of the CNW Members personnel are kept for as long as personnel is appointed in the CNW plus a 6 months retention period since the disabling of the user. Operational data will be kept for as long as the information sharing on a particular incident is required, in accordance with rules and procedures of the CNW. Data related to incidents that are older than 3 years will be kept for operation needs but irrelevant personal information will be removed and the remaining data will be stored on the Cooperation Portal in a folder that is encrypted with the PGP keys of the CNW Members. Log data from the CNW systems and similar data will be stored for a maximum period of three years. Data that needs to be kept longer to allow investigating breaches that took place in the past will be stored according to the highest security standards. • For Microsoft GitHub Enterprise Cloud service: until 90 days after cancellation or termination of a user's account (though some information may remain in encrypted backups). • For the Microsoft Azure services: the retention period is 2 years from data generation. Platform logging and monitoring data are stored for the same time period as the contact data of the user that performed the relevant actions
Data recipients	• All beneficiaries of CNW Central Services can view certain personal data (depending on the tool) of the beneficiaries for team management purposes and

	information exchange. (e.g., email addresses, ASCII-armored OpenPGP public keys, documents uploaded by other users of the systems, etc). • All admin users in the tools, this means ENISA/ OCU staff and ENISA/OCU contractors that deal with the support and maintenance of the tools • The data may also be available to EU bodies charged with monitoring or inspection tasks in application of EU law (e.g. internal audits, European Anti-fraud Office – OLAF).
Transfers to third countries	All CNW Central Services tools and backups are hosted on ENISA premises with the exception of the Simple Email Service (SES) of Amazon Web Services , MS Defender, RH Insights (used to especially support the operation of the CNW Central Services tools collection) and other services maintained by our contractors L-Soft, DFN-CERT, Microsoft Github Enteprise Cloud, Microsoft Azure Services, WEDOS DDoS protection based in EU. Following the SES service specification, the service is used for sending emails only and it does not store any information for business use, apart from technical usage data that are necessary for the provision of the service (for example, emails bouncing back). Technical data storage at rest is within the EU only. Any transfer of personal data outside the EU/EEA is performed in line with Chapter V Regulation 1725/2018 (EUDPR). MS Defender Microsoft Defender is a cloud service that offers: • Security posture management • Antimalware • Endpoint detection and response (EDR) • Extended detection and response (XDR) • Virtual machine behavioral analytics and security alerts • Threat detection for OS-level and Network-level • Security Policy and Regulatory Compliance • Qualys vulnerability assessment • File integrity monitoring and more. It keeps diagnostic (pseudonymised) data in EU. (Microsoft 365 Defender data security and privacy | Microsoft Learn) MS Defender for Cloud uses Azure Arc to protect non-Azure machines. (Plan Defender for Servers agents and extensions deployment | Microsoft Learn) Redhat insights is a SaaS (US located) which offers value in our environment, proactively identifying and remediating threats, assessing vulnerabilities, analyzing compliance, creating inventories, determining missing patches, identifying configuration risks. By default, no personal information is collected: The design principle with Insights is the following: collect only the minimum data that is needed for analysis, issue identification, and remediation. Complete volumes of system information such as core dumps or full log files are not collected. Insights, by default, does not collect personal information. Red Hat Insights for Red Hat Enterprise Linux Technical FAQ - Red Hat Customer Portal WEDOS can apply DDoS mitigation policies effectively at both the network and application layers, identifying and blocking attacks without compromising SSL security. This architecture enables WEDOS to inspect packets and HTTP header metadata, to identify and filter malicious traffic. This happens by analyzing the encrypted traffic without affecting end-user privacy, as the traffic is re-encrypted before reaching the origin server or user. Decryption is performed exclusively within EU borders. Sensitive data is never stored. WEDOS.protection - WEDOS.com - WE DO Security
Security measures - General description	Security policy and technical/organisational measures applicable to ENISA's IT systems. More specifically, • Enabled Multi-Factor Authentication (MFA) • Deployment of Hardened Operating System images • Implementation of referenced Security Baselines • Utilization of Red Hat Insights for Vulnerability Monitoring • Utilization of Microsoft Defender Cloud service • Enabled auditing and logging

	• Centralized Log collection to ENISA Splunk and Microsoft Sentinel • Continuous Log monitoring and analysis • Established Incident Response procedures
Privacy statement	Available to the CSIRT network members under the portal.