THE STATE CYBER PROTECTION CENTRE OF THE STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE

2025

ANNUAL REPORT

VULNERABILITY DETECTION AND CYBER INCIDENT/CYBER ATTACK RESPONSE SYSTEM

TLP: CLEAR

VULNERABILITY DETECTION AND CYBER INCIDENT/CYBER ATTACK RESPONSE SYSTEM

Refers to a set of software and hardware tools that ensure 24/7 monitoring, analysis, and transmission of telemetry data on cyber incidents and cyber attacks that have occurred or are currently occurring at the protected entities and may have negative impact on their stable operation.

SUBSYSTEM OF CYBER INCIDENT RESPONSE OPERATIONS CENTRE

Refers to the central component of the Vulnerability Detection and Cyber Incident/Cyber Attack Response System that provides:

- Centralised management of all subsystems within the Vulnerability Detection and Cyber Incident/Cyber Attack Response System
- Centralised collection and accumulation of information about network security events
- Real-time monitoring and processing of cyber threats and cyber incidents.

The subsystem of Cyber Incident Response Operations Centre detects malicious activity as well as system and network anomalies at the protected entities by analysing the data obtained from network devices (active sensors, firewalls, vulnerability scanners), workstations, servers, authorisation systems, and internal/external sources of cyber threat intelligence.

MONITORING STATISTICS

OVERVIEW OF SUBSYSTEMS, TECHNOLOGIES, AND TOOLS

During 2025, 24 new organizations were added to the Subsystem of Collection of Telemetry Data from Information and Communication Systems (NDR), each receiving a set of network traffic monitoring equipment.

Also, 97 organizations are currently connected to the Endpoint Protection Subsystem (EDR), thus more than 46,5k workstations and servers are now monitored by the Vulnerability Detection and Cyber Incident/Cyber Attack Response System.

Technologies and tools

	Telemetry Collection Subsystem **NDR**	Endpoint Protection Subsystem **EDR**	Endpoint Protection Subsystem **MDR**
Cybersecurity tools	Organizations added: **92**	Organizations added: **97^{+39}**	
	Sensors installed: **93^{+24}**	Hosts protected (EDR): **~14.5k**	Hosts protected (MDR): **~32k**

The main efforts were focused on developing and scaling the functional capabilities of the Vulnerability Detection and Cyber Incident/Cyber Attack Response System, in particular on expanding the coverage of network and endpoint monitoring, improving the quality of telemetry collection, and enhancing the mechanisms for centralised analysis of information security events.

💡 **NOTE**

This report is based on the statistical data of the Cyber Incident Response Operations Centre of the Vulnerability Detection and Cyber Incident/Cyber Attack Response System from January 1, 2025 to December 31, 2025, inclusive.

CYBER INCIDENTS AND CYBER ATTACKS

QUANTITATIVE METRICS OF PROCESSED CYBER INCIDENTS

Cyber incidents and cyber attacks

17.3k
Security events

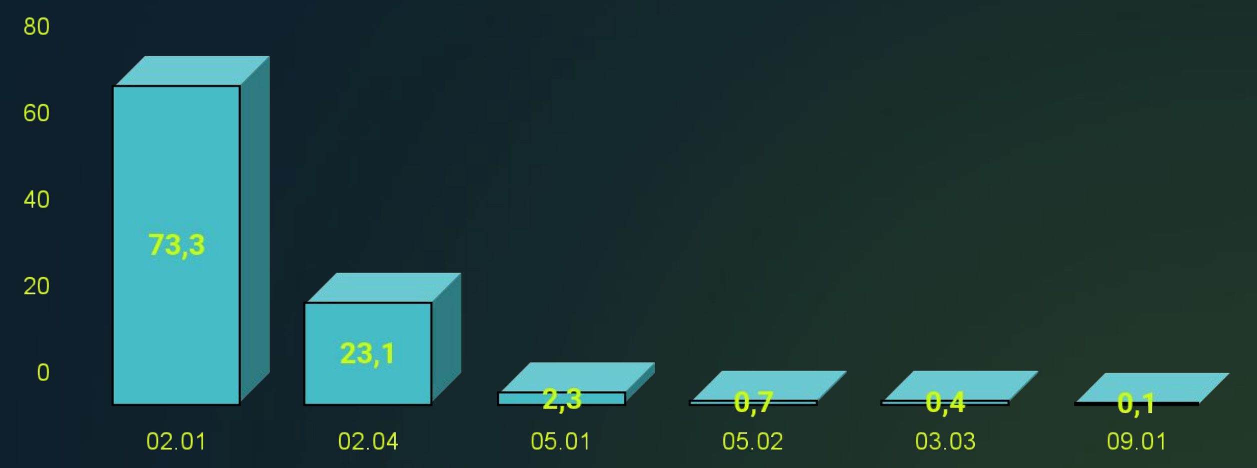
SIEM

730
Cyber incidents

During 2025, the Cyber Incident Response Operations Centre processed 17.3k security events and reported 730 cyber incidents of different severity. The majority of these cases involved malware. According to the analysis of the detected attacks, their primary objective was to gain concealed control over information systems and then use it for the purpose of cyber espionage or financial theft.

! It is worth noting that the vast majority of tactics and techniques used by attackers as an initial attack vector lose their effectiveness when unprivileged user accounts are used and basic security configurations are implemented on workstations.

Percentage breakdown by cyber incident type



02.01 – malware infection, 02.04 – malicious connection, 05.01 – account compromise, 05.02 – system compromise, 03.03 – phishing, 09.01 – vulnerability.

CYBER THREATS

ACTIVITY OF CYBER THREAT CLUSTERS

Cyber incidents and cyber attacks

730 Cyber incidents → **339** Cyber attacks

Among the cyber incidents and cyber attacks reported by the Cyber Incident Response Operations Centre, 339 were linked to known cyber threat clusters. According to the activity analysis, in 2025, clusters UAC-0010, UAC-0006, and UAC-0050 demonstrated the highest level of activity.

UAC-0010

Aliases:
Gamaredon, Primitive Bear, Trident Ursa, Aqua Blizzard

Tracked since:
2013

Motivation:
cyber espionage

Cyber attack targets:
government authorities, defence forces

UAC-0006

Aliases:
none

Tracked since:
2013

Motivation:
stealing money

Cyber attack targets:
financial departments of organizations

UAC-0050

Aliases:
none

Tracked since:
2020

Motivation:
cyber espionage, stealing money, PSYOPS

Cyber attack targets:
government authorities, defence forces, financial institutions

RECOMMENDATIONS

To enhance the level of cyber protection of your organization's ICS, we recommend utilizing the cybersecurity services available within the Vulnerability Detection and Cyber Incident/Cyber Attack Response System for real-time cyber threat detection and cyber incident management.

NDR	The service involves the installation and configuration of a network sensor to monitor network traffic and detect cyber incidents and cyber attacks. The sensor can be deployed either inside the network or at its perimeter.
EDR	The service provides comprehensive endpoint protection for your organization (personal computers, servers, virtual machines) through the installation and configuration of EDR technology.
MDR	The service provides the centralised collection, correlation, and analysis of event logs from the organization’s existing endpoint protection tools (EDR/AV) with the goal of timely detection of signs of compromise, response to cyber incidents, and enhancement of the overall security posture of endpoints.

To contact the State Cyber Protection Centre about gaining access to the services listed above:

Email: `info_scpc@cip.gov.ua`

Cyber Incident Response Operations Centre

State Cyber Protection Centre

State Service of Special Communications and Information Protection of Ukraine

State Cyber Protection Centre
https://scpc.gov.ua