Cleopatra Hospitals Group

How Egypt's largest private healthcare network reduced high-severity investigation times by 75% with Kaspersky

kaspersky cybersecurity true to business

CHG CLEOPATRA HOSPITALS GROUP

16
medical entities across greater Cairo

2+ mln
patients annually

1,000
hospital beds

6,500
employees

3,000+
endpoints

500+
servers

7
SOC analysts

A defining force in Egyptian healthcare

In healthcare, cybersecurity is not only about protecting systems; it's about helping protect the continuity, quality and reliability of patient care. For Cleopatra Hospitals Group (CHG), stronger cybersecurity visibility supports the digital foundations behind faster workflows, trusted services and a better experience for the millions of patients it serves each year.

As Cleopatra Hospitals Group expanded into a highly connected, largely paperless and more sustainable healthcare environment, Kaspersky helped the organization strengthen cybersecurity visibility, improve threat detection and build a more mature security operations model across its hospitals, endpoints, servers and critical systems.

CHG is one of Egypt's most significant healthcare organizations. Founded in 2014 through the acquisition of some of the country's leading hospitals, the group has grown into the largest private healthcare provider in Egypt by number of beds, facilities and patients served. Listed on the Egyptian stock market since 2016, it is also the only healthcare provider represented in the EGX30 index.

Its scale is significant, but so is its role. CHG is leading the transformation of private healthcare in Egypt through clinical quality, strong governance, operational excellence and customer experience with a consistent focus on patient quality of life. With this scale comes responsibility: ensuring that digital healthcare operations remain secure, available and trusted across hospitals, medical centers, administrative teams, partners and patients.

Securing a highly digital healthcare model

CHG's technology environment is central to how the organization delivers care. Across its hospitals, 90-95% of workflows are automated, including medical, administrative, financial and back-office operations. A centralized private network connects its facilities, while consolidated servers support unified transactions and a single identity framework across the group. This helps create a more connected and standardized experience for patients, partners and internal teams across the organization's hospitals and medical entities.

However, that level of digital maturity also increases operational and cybersecurity risks. The group manages 3,000+ endpoints and more than 500 servers, alongside medical systems, finance platforms, patient engagement portals, AI-based patient engagement solutions, partner integrations and interoperability with major insurance providers. In this environment, cybersecurity is not a supporting function – it's part of the operational foundation of modern healthcare.

Results snapshot

75%
reduction in high-severity incident investigation time

83%
reduction in medium- and low-severity investigation time

Thousands of EPS
(events per second) processed by the SOC

50
incidents analyzed per day by the security team

Kaspersky Next XDR Expert

Kaspersky Next EDR Expert

The challenge: visibility across a growing digital estate

Before implementing Kaspersky solutions, CHG had antivirus protection in place but needed deeper visibility and a more mature approach to cybersecurity operations. Threat identification was limited, endpoint monitoring needed to improve and security data across the environment remained fragmented. As CHG became more digitized and connected, traditional protection alone was no longer enough. The organization needed a clearer understanding of activity across endpoints, servers, logs and transactions, brought together in a single operational model.

The strategy: building visibility, maturity and control

CHG conducted an intensive assessment of competing solutions, evaluating product maturity, vendor experience, ease of implementation, management capabilities, integration with its ecosystem, team enablement and value for money.

CHG chose Kaspersky to support the next stage of the group's cybersecurity journey.

Kaspersky Next XDR Expert, includes full-fledged EDR capabilities (Next EDR Expert) of CHG's security operations, helping the team monitor endpoint activity, correlate threats, analyze zero-day attack indicators and consolidate logs from across systems, networks, endpoints, servers and applications. Bringing this information into a more unified platform also helped improve issue resolution, operational efficiency and team productivity by reducing fragmentation across the security environment.

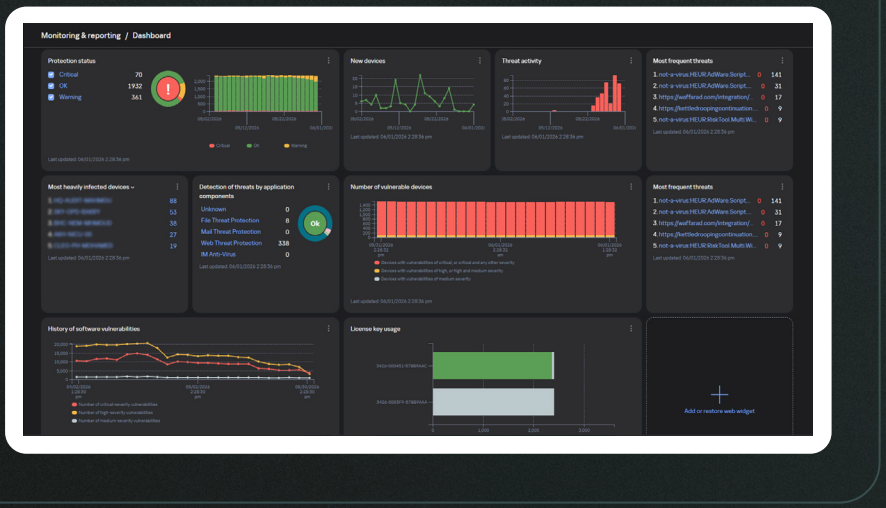
A collaborative implementation approach

The project went beyond a standard technology deployment. It was a wider operational integration involving CHG's internal infrastructure, cybersecurity operations and technology delivery teams, together with its implementation partner and Kaspersky specialists.

This kind of teamwork was critical to the deployment, which required correct log integration, optimization across the existing ecosystem, licensing alignment and interoperability with other security tools. Kaspersky supported – and continues to support – the process through technical guidance, health checks and best-practice implementation support.

Supporting long-term SOC maturity

CHG also began mapping detection capabilities against the MITRE ATT&CK framework as part of its broader SOC maturity journey, helping the organization measure improvements in visibility, detection coverage and operational readiness over time.



CHG's SOC team uses advanced monitoring and threat detection capabilities to strengthen operational resilience

From fragmented signals to stronger security insight

One of the most significant improvements was gaining clearer visibility into activity across the environment. By consolidating logs and security information from different parts of the environment into a unified platform, CHG boosted its ability to understand what was happening across its infrastructure. The team gained better insight into endpoint activity, system logs, transactions, email communications, file exchanges and media transfers.

This improved threat correlation, accelerated issue resolution and supported more automated actions across the environment. It also enhanced operational efficiency and productivity for the security team, while creating a stronger foundation for threat intelligence analysis and future SOC maturity.

In the first half of 2025, CHG established its own SOC team, responsible for monitoring and managing cybersecurity operations. Today, Kaspersky plays an important role in that operating model, supporting technology deployment, monitoring, threat hunting, threat intelligence, IOC management and broader SOC operations.

Expanded detection and SOC capabilities

Kaspersky Next XDR Expert provides IR, EDR and SIEM capabilities integrated into SOC monitoring and correlation, CHG's expanded detection capabilities include:

- IOC-based threat hunting and IOC matching
- Suspicious PowerShell execution detection
- Remote administration tool misuse monitoring
- Unauthorized access attempt detection
- Abnormal user and insider activity monitoring
- Suspicious network scanning and reconnaissance detection
- YARA- and Sigma-based threat detection

Planned next steps include additional MITRE ATT&CK mapping, rule tuning and detection coverage optimization.

The outcome: a resilient foundation for continuous improvement

For CHG, the value of the project lies not only in what has been implemented, but in the foundation it creates for what comes next.

Kaspersky currently covers all endpoints and servers Kaspersky Next XDR Expert, including monitoring of additional system logs and transactions.

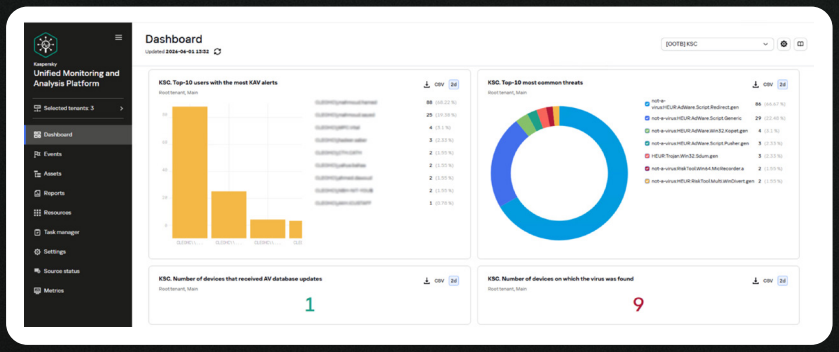
The project has helped CHG:

- Improve visibility across endpoints, servers, logs and transactions
- Strengthen threat detection, correlation and zero-day investigation
- Consolidate security information from multiple systems into a more unified platform
- Accelerate issue resolution and support more automated actions

Incident investigation time improvement

Severity	Before implementation	After implementation	Improvement
High	8 hours	2 hours	75% reduction
Medium	1 day	4 hours	83% reduction
Low	2 days	8 hours	83% reduction

- Improve security team efficiency and productivity
- Build a stronger foundation for threat intelligence, SOC maturity and future enhancements



Unified threat detection and analysis support more efficient cybersecurity operations across the healthcare network.

Kaspersky
Threat Intelligence

Looking ahead

The partnership continues to evolve through ongoing workshops and planned enhancements, including integrations with Kaspersky Threat Intelligence, additional intelligence feeds, XDR capability upgrades, cybersecurity awareness tools and future service improvements. These initiatives support CHG's continued journey toward stronger visibility, richer threat context and more mature cybersecurity operations.

Future priorities include continued SOC maturity development, enhanced threat intelligence integration, proactive threat hunting, expanded XDR coverage across healthcare applications and critical systems, advanced automation and orchestration, stronger GRC capabilities, progress toward a Zero Trust security model, broader cyber resilience, continuous workforce readiness and ongoing optimization of MITRE ATT&CK coverage, detection engineering and threat analytics.

Key takeaways

For a healthcare organization operating at national scale, cybersecurity visibility is essential to resilience. CHG's experience shows how Kaspersky Next XDR Expert helps mature security operations by bringing endpoint activity, system data, logs and threat intelligence into a more unified model.

It also demonstrates that successful cybersecurity transformation depends on more than technology. Product maturity matters, but so do integration, implementation support, internal readiness and long-term partnership.

For CHG, this also matters because every improvement in cybersecurity supports the patient experience. When systems are more visible, better monitored and more resilient, clinical, administrative and partner workflows can run with greater confidence. This helps the group continue delivering standardized, well-managed and responsive care across its network while reinforcing the trust patients place in its services.

Kaspersky has helped us strengthen visibility across our environment, from endpoint activity and threat correlation to log analysis and zero-day investigation. For a healthcare organization operating at this scale, that visibility is essential to maintaining resilient operations and supporting patient care. The product capabilities, implementation expertise and ongoing support have been critical to the success of the project.

Dr. Amr AlAshkar

Chief Information Officer, Cleopatra Hospitals Group

Kaspersky Next XDR Expert

Learn more

Kaspersky Next EDR Expert

Learn more

www.kaspersky.com

#kaspersky
#truetobusiness