infopulse

Implementing Long-Term Security Strategy to Protect Infopulse's and Our Clients' Assets in a War_

Future-proof security strategy to enable ultimate protection

Client: Infopulse **Industry:** Software & Hi-Tech **Location:** Ukraine

Specialists: 2,300+ **Website:** www.infopulse.com

Client Background

Infopulse, part of the leading Nordic digital services company Tietoevry, is an international vendor of services in the areas of Software R&D, Application Management, Cloud & Infrastructure, and Cybersecurity to SMEs and Fortune 100 companies across the globe.

Business Challenge

At Infopulse, we believe that in order to deliver quality, cutting-edge, and secure services, our company should apply the same principles to all internal processes. We strive to build and support a robust infrastructure that meets the needs of our clients in terms of security and resilience, ensuring the protection of the company's data assets. To achieve this, Infopulse has developed and implemented a company-wide security strategy that has been gradually improved and adjusted to the changing threat landscape since 2017.

Objectives set for the Infopulse security team were as follows:

- Ensure the utmost protection of sensitive data and clients' assets within the Infopulse IT ecosystem.
- Achieve a great understanding of the new types of cyberattacks aimed at companies and governmental facilities.
- Enhance Infopulse infrastructure with advanced security tools and approaches to counter modern, more sophisticated attacks.
- Adopt a proactive approach to cybersecurity to timely address detected threats and vulnerabilities.
- Regularly assess and audit the state of the company's security perimeter.
- Design and improve processes and operations to their perfection for the Infopulse cybersecurity team.
- Ensure a 360-degree view of the company's security landscape.

Solution

The implementation of Infopulse's security strategy was tightly intertwined with the events that occurred through the years and marked new chapters in the development of the threat landscape. Our specialists responded to the events in a way that would ensure these new threats and relevant approaches could be effectively countered.

2017-2021

The year 2017 is infamous for the global spread of the NotPetya malware, which primarily targeted Ukraine-based organizations. It raised the priority to defend against large-scale destructive attacks and strengthen our security stance. Infopulse security team responded in the following way:

- Implemented a QRadar SIEM system. The solution was fine-tuned and enriched with new rules in the course of several years.
- Considering the new types of attacks, the team worked on approaches that would significantly reduce the chances of a successful attack.
- Improved segmentation of the corporate network by means of an additional internal firewall and a protected jump host to administrate corporate systems.
- Strengthened cooperation with the internal IT team to align efforts on achieving high security for the launched services.
- Adopted industry best practices in secure administration of corporate systems.
- In partnership with Microsoft, Infopulse successfully switched to the next-gen security solutions:
    - When the pandemic, and later the war, disrupted established processes, the cloud hosting allowed for extensive support for Infopulse specialists during relocation and maintained the required level of control over workplaces and corporate data. It also enabled unique services that addressed clients' security concerns, such as remote data wipes.
    - Infopulse corporate services, including a Microsoft 365 suite, were migrated to a protected cloud configuration. The entire company is now covered by one of the most advanced complexes of security licenses provided by Microsoft.
- Designed and ran a company-wide security awareness campaign with an online phishing simulator kindly provided by Tietoevry, our parent company.
- Initiated the next stage of improving the maturity level of security processes:
    - Formalized numerous security processes, e.g., incident management, vulnerability management, security event management, etc.
    - Developed criteria to measure the effectiveness and performance of the team, based on the analytics of their existing activities.
    - As a result, it allowed for fast, efficient, and well-coordinated work within the team when the war started.

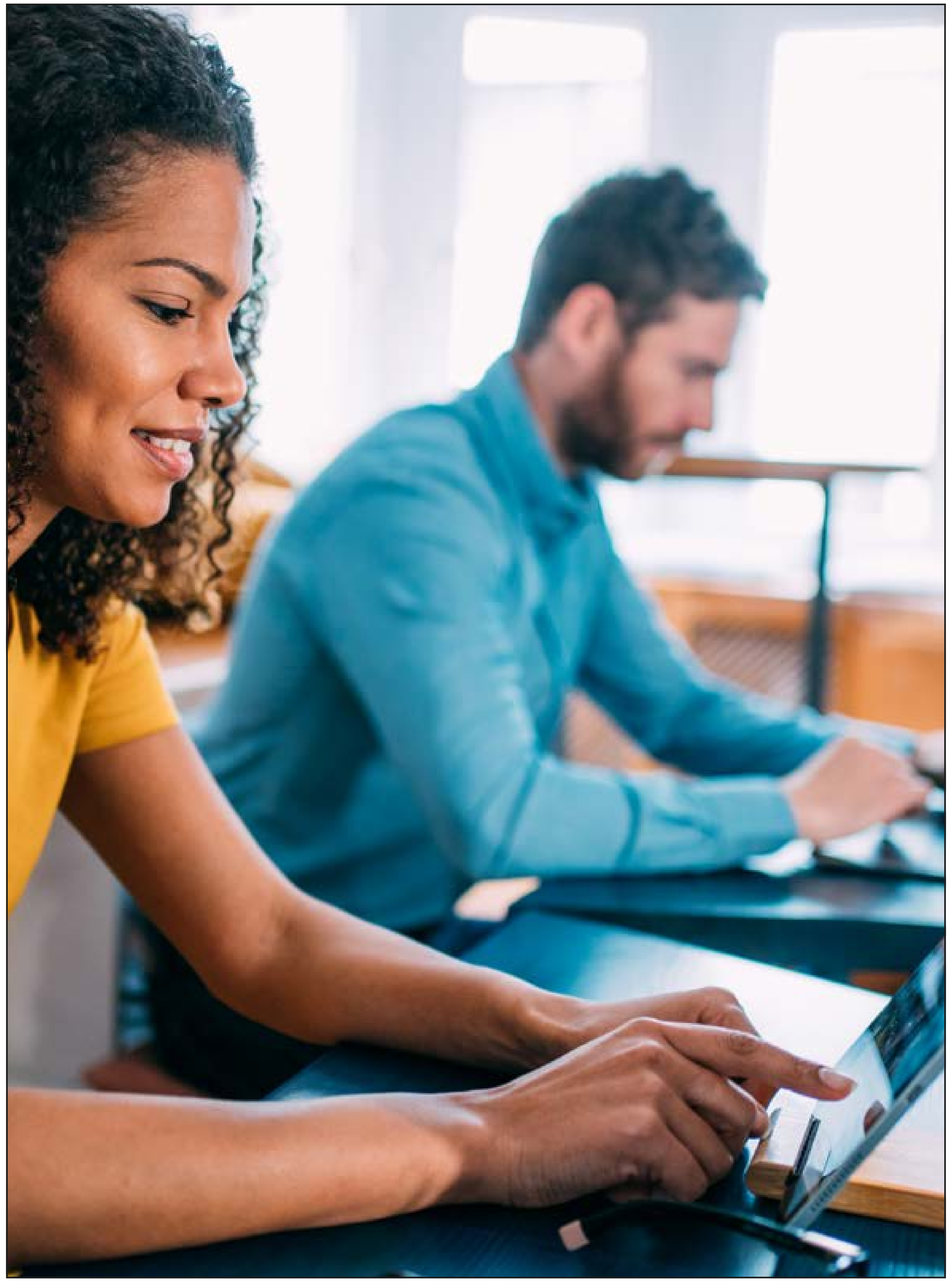
- Formalized and configured the vulnerability management process to timely discover vulnerabilities in IT services and eliminate them, in cooperation with the IT team:
  - Achieved a minimal vulnerability profile.
  - In December 2021, migrated the vulnerability management system to the cloud, which created the opportunity for fast and straightforward migration to the EU platform once required.

January 2022 "Final preparations"

A January 2022 cyberattack on the Ukrainian enterprise and government websites marked the beginning of the cyberwar that was unfolding in the background.

As part of its business continuity plan, Infopulse developed a security strategy to counteract potential attacks and prepare for the upcoming war, which included:

- Meetings with Tietoevry, our parent company, to align efforts and share relevant experiences.
- More comprehensive testing of the backup data center in the EU.
- Comprehensive analytics of large-scale cyberattacks within the cyberwar frame.
- The emergency security action plan to enable the most crucial processes was focused on:
  - Enhanced protection of endpoints and external web services.
  - Migration of technical security solutions to the EU data center.
  - Identification of cyber security risks for projects working for critical infrastructure.
  - Tuned additional policies for cloud security.
- Preparing backup communication channels, such as satellite links.



February-April 2022 “Effective response”

When russia invaded Ukraine on February 24 and started an atrocious war, it unfolded both on physical and digital planes. Many Ukrainian sites were under attack, which signalized it was high time to adopt a new approach and a new security plan to be able to withstand the unraveling chaos:

- Infopulse activated a ban on implementing any significant changes, except for critical activities for IT and security infrastructure.
- Relocated security solutions to the EU data center.
- Reconsidered current activities and focused on the most important operations:
  - Handling security events
  - Analysis of risk locations
  - Blocking corporate accounts on devices in risk locations.
- Supported secure development of the ‘Infopulse Connect’ application to efficiently collect the required data from all the company’s specialists.
- Created awareness recommendations for the specialists to warn them against phishing attacks.
- Supported regular and comprehensive communication with clients and Tietoevry on the safety of our people and protection of the equipment and information.
- Enabled emergency relocation of Infopulsers and their families, equipment, and tangibles.
- Performed conservation of offices in risk locations and prepared other offices for possible conservation as well.
- Evacuated equipment from the Kyiv data center to a safe location in the most effective and reliable way.
- Minimized the perimeter for attacks by turning off services that could be potentially attacked and were not required at the moment.

Technologies

- IBM QRadar SIEM
- Microsoft 365
- Cloud security solutions
- Anti-phishing solutions
- WAF (Web Application Firewall)
- Azure AD Identity Protection
- EDR (Endpoint Detection and Response)
- SOC

Business Value

A steady and well-thought security strategy provided Infopulse with an unprecedented level of protection. Thanks to the proactive approach and informed decision-making, Infopulse withstood the dangerous times with little to no damage caused by cyberattacks. Here is our effort and success in numbers:

Business Continuity

- Prepared **30+** informational materials for clients on service continuity and cybersecurity.
- Performed **20+** trips to relocate and evacuate people and equipment.
- Transported **270+** company specialists with the help of the relocation team.
- Moved **2** archives of physical documentation with a total volume of **3** cubic meters (**106** cubic feet).
- Processed **60+** events on the location of specialists in risk areas.

Corporate Security

- Analyzed **5** nationwide cyberattacks.
- Blocked **800+** phishing emails.
- Expanded the protection of external web services by **110%**.
- Implemented **3** new cybersecurity controls.
- Reinforced the implementation of **5** information services from the security point of view.
- Achieved **100%** coverage of corporate information systems with an effective vulnerability management process.
- Updated approx. **260** connections of the security event monitoring systems.
- Processed **40%** more cybersecurity events and incidents than during peacetime.
- Handled **5** information security incidents.
- Published **6** specialized security announcements.

About Infopulse

Infopulse, part of the leading Nordic digital services company Tietoevry, is an international vendor of services in the areas of Software R&D, Application Management, Cloud & IT Operations, and Cybersecurity to SMEs and Fortune 100 companies across the globe. Founded in 1991, the company has a team of over 2,300 professionals and is represented in 7 countries across Europe and the Americas.

Infopulse is trusted by many established brands, such as BICS, Bosch, British American Tobacco, Credit Agricole, Delta Wilmar, ING Bank, Microsoft, Norwegian Oil and Gas Association, OLX Group, OTP Bank, SAP, UkrSibbank BNP Paribas Group, Vodafone, Zeppelin Group, and others.

For more information, please visit **www.infopulse.com**

Contact us

PL	+48 (221) 032-442
DE	+49 (69) 505-060-4719
US	+1 (888) 339-75-56
UK	+44 (8455) 280-080
UA	+38 (044) 585-25-00
BG	+359 (876) 92-30-90
BR	+55 (21) 99298-3389

✉ info@infopulse.com