
Protecting Your
Digital World.
Infosec
Powered by TeleGroup

Infosec
Powered by TeleGroup

Aleksandar Vratonjić Gligorijević
Chief Marketing Officer, TeleGroup


1.0 What you need to know?

# Key Cybersecurity Trends for 2025

Infosec
Powered by TeleGroup

- Increased Adoption of Zero Trust Architecture
- Growth of Cloud Security
- Rise of AI and Machine Learning
- Emphasis on Cyber Resilience
- Expansion of IoT Security
- Zero Trust Security

# Key Cybersecurity Trends for 2025

Infosec
Powered by TeleGroup

Increased Adoption of Zero Trust Architecture

Growth of Cloud Security

Rise of AI and Machine Learning

Emphasis on Cyber Resilience

Expansion of IoT Security

Zero Trust Security

That means... .

# OT security is undergoing a significant transformation.

- New technologies like Industrial Internet of Things (IoT), cloud computing, and AI are boosting productivity and efficiency. However, they're also expanding the threat landscape, creating more entry points for cyberattacks.

- The growing number of connected devices, estimated to reach 25 billion by 2025, combined with the convergence of IT and OT systems and the rise of remote work, has significantly increased the attack surface for OT.

# OT security is undergoing a significant transformation.

- New technologies like Industrial Internet of Things (IoT), cloud computing, and AI are boosting productivity and efficiency. However, they're also expanding the threat landscape, creating more entry points for cyberattacks.

## That leads to… .

- The growing number of connected devices, estimated to reach 25 billion by 2025, combined with the convergence of IT and OT systems and the rise of remote work, has significantly increased the attack surface for OT.

# Top 10 cyber threats in 2024

## 1 Social Engineering

Any network is hackable if an employee can be duped into sharing access.

## 2 Third-Party Exposure

Vendors, clients and app integrations with poor security can provide access to an otherwise well-protected network.

## 3 Configuration Mistakes

Even the most cutting-edge security software only works if its's installed correctly.

## 4 Poor Cyber Hygiene


Employee training is essential to ensure those with network access maintain safe cyber practice.

## 5 Cloud Vulnerabilities

Online data storage and transfer provides increased opportunities for a potential hack.

## 6 Ransomware

Hackers can capture sensitive data or take down networks and demand payment for restored access.

## 7 Mobile Device Vulnerabilities

Devices that connect to multiple networks are exposed to more potential security threats.

## 8 Internet of Things

Smart technology users may not realize that any IoT device can be hacked to obtain network access.

## 9 Poor Data Management

When massive amount of unnecessary data are kept, it's easier to lose and expose essential information.

## 10 Inadequate Post-Attack Procedures

Security patches must be as strong as the rest of your cybersecurity protections.

Infosec
Powered by TeleGroup

420 millions cyberattacks between January 2023-January 2024 in critical infrastructure

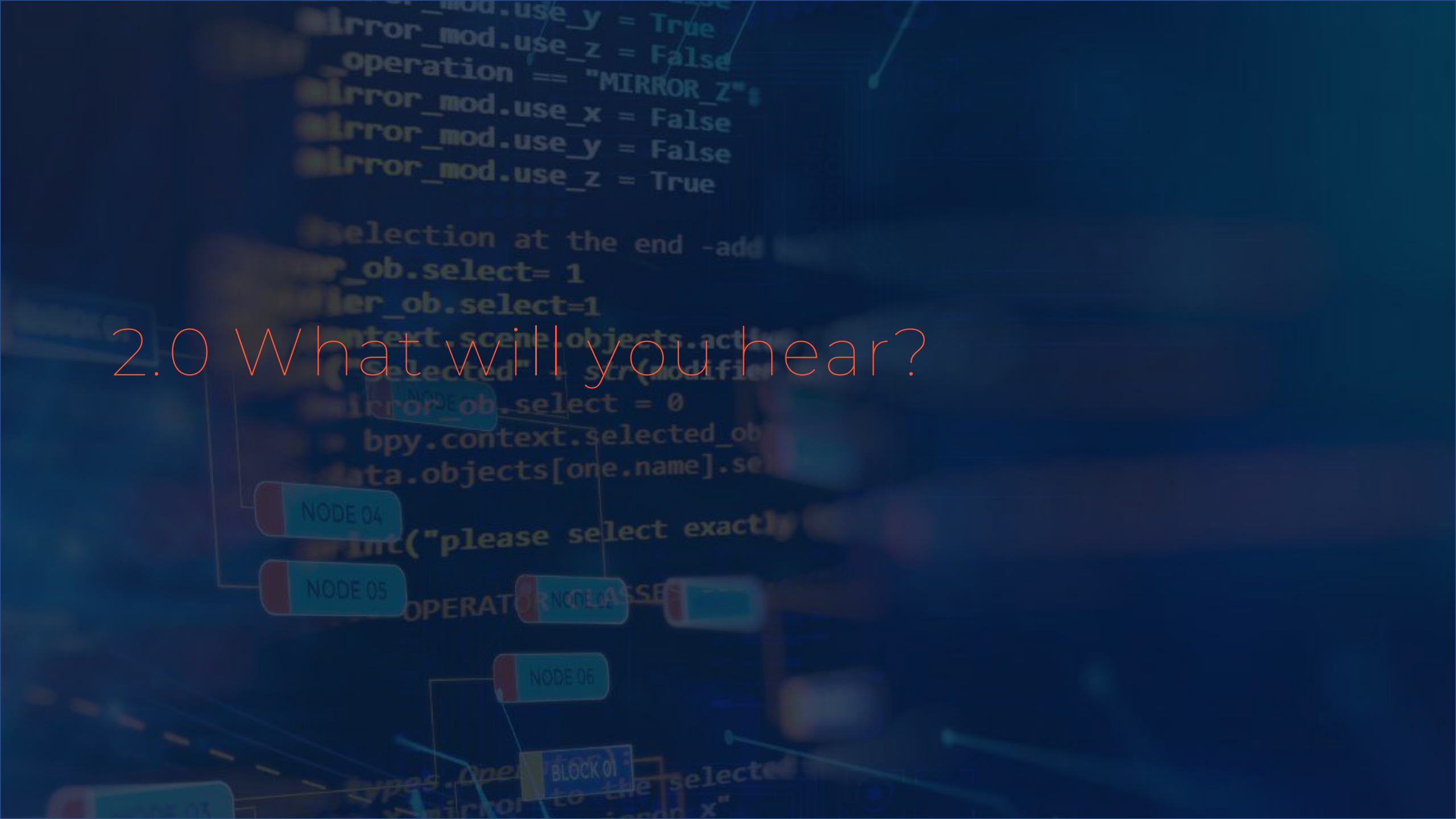
41% of incidents identified phishing as the leading infection vector

88% of cybersecurity breaches are caused by human error.

$4.88 million The average cost of a data breach in 2024, the highest average on record

94% of malware is delivered by email

$24 trillion is the expected global cost of cybercrime by 2027, as these costs continue to rise


2.0 What will you hear?

# Thursday, September 26th

Infosec
Powered by TeleGroup

Dejan Vukšić
Advisor to the President for Security and Defense, Cabinet of the President of Montenegro

KeyNote
Cisco Challenges and Solutions for Effective Cyber Attack Protection

Aleksandar Pavlović
Regional Sales Manager for Cisco Cybersecurity Solutions, CEE

Check Point
Connecting Securely: Cyber Security solutions for Protecting Distributed Traffic Network Infrastructure

Ivan Štrbac
Lead Security Engineer

---

Panel Discussion
OT Security Challenges and Solutions in Critical Infrastructure

Ljubomir Dujović — Security Department Manager, ONE

Marko Krstić — Head of the Information Security Department and National CERT Affairs, Ratel

Predrag Raković – Chief of Telecommunications Service, CEDIS

Ivan Mladenović– Channel Manager Serbia, Check Point

Igor Vujačić– Advisor to the Chief of Staff for modernization of Armed Forces, Armed Forces of Montenegro

Cognyte
The global threat landscape: trends, attacks, and threats

Omree Wechsler
Cyber Threat Intelligence Analyst

4Sec
WatchGuard ORION – Security Operation Center

Goran Obradović
Network engineer, 4Sec

Irena Djaković Oštro
Network engineer, 4Sec

---

TeleGroup
DORA & NIS2 Regulations: What You Need to Know

Aleksandar Obradović
Security Specialist
TeleGroup

Fireside Chat
GRC: Key Insights You Were Afraid to Ask

Aleksandar Obradović
Security Specialist
TeleGroup

Branko Džakula
Information Security Advisor, Entrepreneur and Educator

Fireside Chat
Designing Secure Systems: Best Practices and Strategies

Đorđe Ćirić
Product Manager, TeleGroup

Dragan Novaković
Security Solutions Engineer, Cisco

# Friday, September 27th

Infosec
Powered by TeleGroup

Cisco
Cisco Zero Trust Solutions
Dragan Novaković
Security Solutions Engineer

IBM
How Much is Your Data Worth?
Siniša Krstić
Security Sales Representative

TC2
How to build a secure and future-proof environment in AWS?
Károly Sepsy
Chief Technology Officer

---

Horizon projects: Support in Securing Funding for Innovative Projects
Miloš Kostić
Project Manager and Business Developer, Tecnalia Research & Innovation

Hitachi
A Japanese Fortress for Your Data
Andrej Gursky
Solution Consultant CEE

Critical Infrastructure Protection – Does AI Help or Hurt?
Branko Primetica
Partner at Cedars International

# 3.0 What you need to do?

Infosec
Powered by TeleGroup

# 8 steps to creating a cybersecurity plan:

1. Conduct a security risk assessment
2. Set your security goals
3. Evaluate your technology
4. Select a security framework
5. Review security polices
6. Create a risk management plan
7. Implement your security strategy
8. Evaluate your security strategy

Infosec
Powered by TeleGroup

8 steps to creating a cybersecurity plan:

1 Conduct a security risk assessment

2 Set your security goals

3 Evaluate your technology

4 Select a security framework

5 Review security polices

6 Create a risk management plan

7 Implement your security strategy

8 Evaluate your security strategy

# Protect Your Digital World with TeleGroup.

Infosec
Powered by TeleGroup