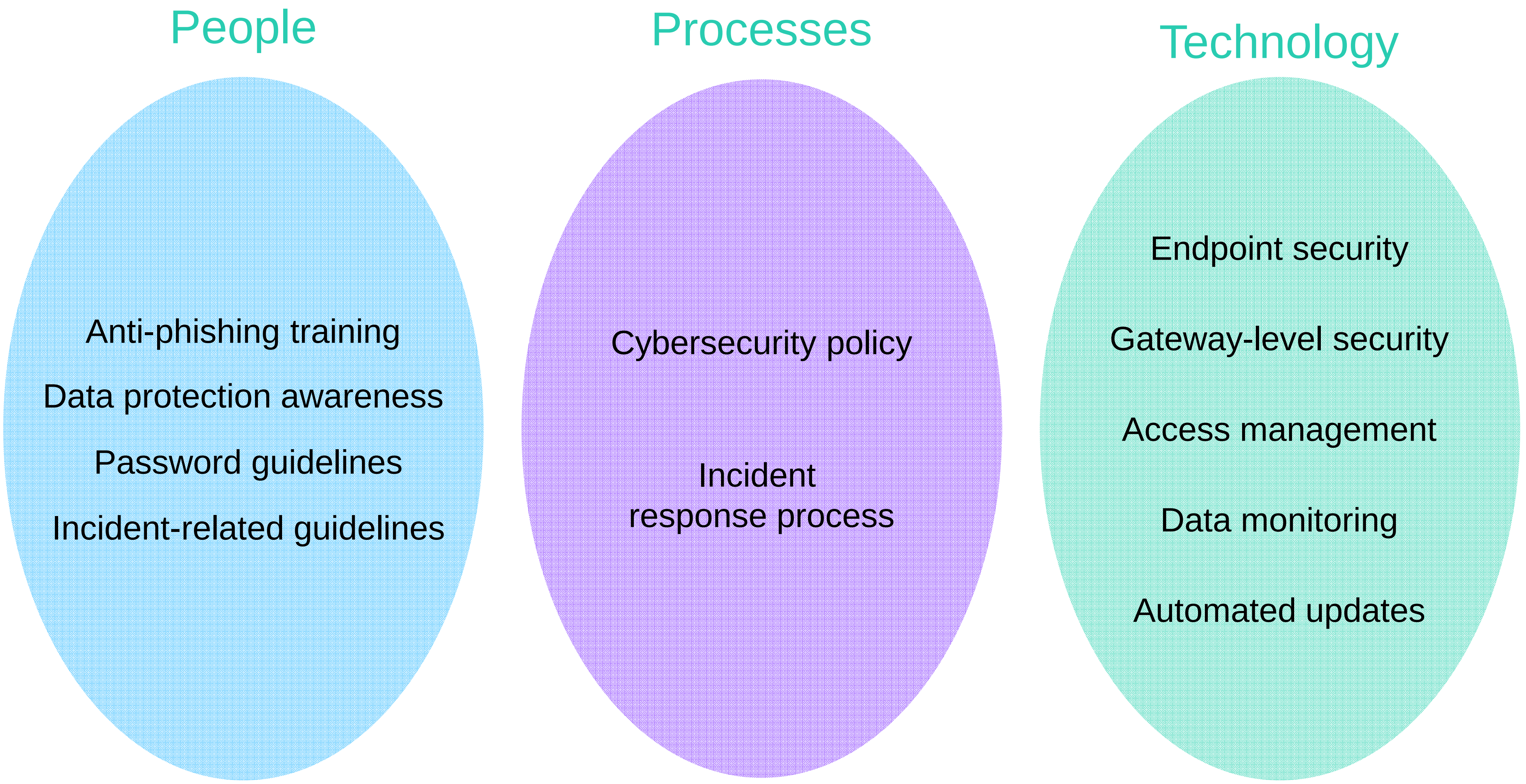
Cyber Resilience in Compliance with EU Directives

18 iunie
2025



People

Anti-phishing training

Data protection awareness

Password guidelines

Incident-related guidelines

Processes

Cybersecurity policy

Incident
response process

Technology

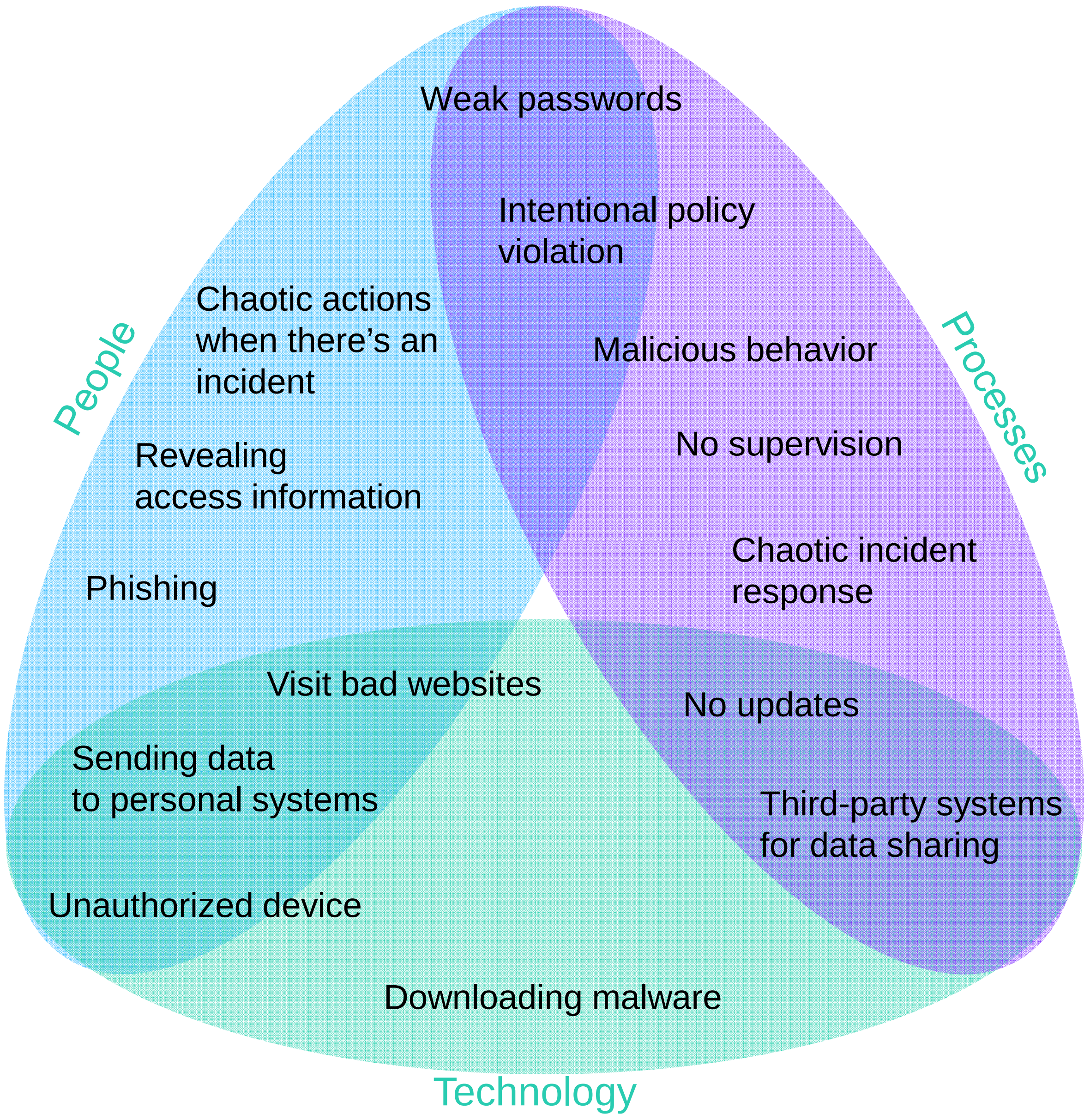
Endpoint security

Gateway-level security

Access management

Data monitoring

Automated updates



People

Processes

Technology

Weak passwords

Intentional policy violation

Chaotic actions when there’s an incident

Malicious behavior

Revealing access information

No supervision

Phishing

Chaotic incident response

Visit bad websites

No updates

Sending data to personal systems

Third-party systems for data sharing

Unauthorized device

Downloading malware

Approach

People

- Conduct regular safe conduct assessments
- Carry out training
- Encourage responsible, diligent behaviour
- Watch for insider risks
- Grow in-house expertise

Processes

- Limit rights to absolutely necessary only
- Establish processes for all critical situations
- Check against business processes
- Exercise regularly
- Be proactive, plan for continuous security buildup

JP6
OG23

Technology

- Prevent exposure by blocking threats earlier and automatically
- Aim for across-infrastructure visibility
- Make key ITSec tasks (such as incident response) simpler to carry out

Slide 4

JP6 Exercise regularly? I mean, this is good advice, but not sure it fits here - unless there's a word or two missing?
Janet Paterson; 16.07.2024

OG23 Practice useful processes regularly - such is doing thing at the time of an incident. Please suggest a better phrasing that would be short enough but would tell the story in a better way!
Oleg Gorobets; 16.07.2024

From Security to Offense: Redefining Cyber Defense Strategy

Evolving cybersecurity challenges

Struggling to identify cybersecurity risks based on the threat landscape of a particular organization

Poor prioritization of security alerts emanating from disparate security technologies

Inefficient incident response, leading to high recovery costs and offending business continuity and growth

Undiscovered threats lurking inside your infrastructure

Skilled professionals shortage

Regulatory compliance and privacy

Kaspersky Threat Intelligence

2. Detection & Investigation

- Kaspersky CyberTrace
- Kaspersky Threat Data Feeds
- Kaspersky Threat Lookup

5. Investigation & Response

- Kaspersky Intelligence Reporting
- Kaspersky Threat Lookup
- Kaspersky Threat Analysis

6. Vulnerability Management

- Kaspersky Vulnerability Feed

3. Investigation & Response

Kaspersky Threat Intelligence Portal

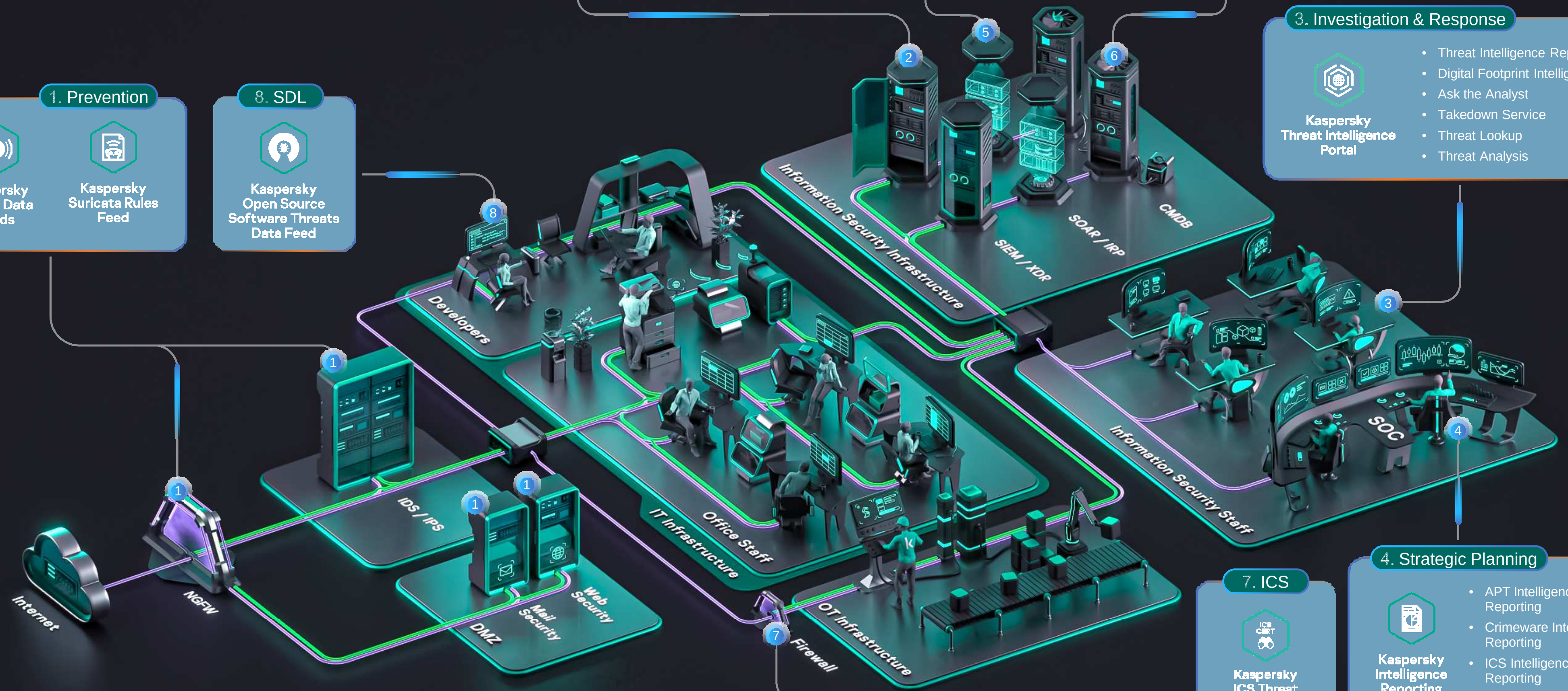
- Threat Intelligence Reporting
- Digital Footprint Intelligence
- Ask the Analyst
- Takedown Service
- Threat Lookup
- Threat Analysis

1. Prevention

- Kaspersky Threat Data Feeds
- Kaspersky Suricata Rules Feed

8. SDL

- Kaspersky Open Source Software Threats Data Feed



7. ICS

- Kaspersky ICS Threat Intelligence

4. Strategic Planning

Kaspersky Intelligence Reporting

- APT Intelligence Reporting
- Crimeware Intelligence Reporting
- ICS Intelligence Reporting
- DFI Analytical Report

— Network traffic — Telemetry

Threat Landscape on Kaspersky Threat Intelligence Portal

Region- and industry-specific threat intelligence to understand the exact threats facing your organization

- MITRE ATT&CK alignment
- Real-time updates based on ongoing Kaspersky researches
- Enhanced adversary profiles

400 000+

Malicious files detected daily by Kaspersky

Feedback on the EU Cybersecurity Act Revision

- Supports simplification of cybersecurity certification schemes and reducing administrative burdens

- Recommends strengthening ENISA’s role for better coordination and capacity

- Emphasizes harmonizing reporting obligations across NIS2, DORA, GDPR

- Encourages international mutual recognition to reduce compliance costs

Stay safe out there!

And let's talk!

Bogdan.Albu@kaspersky.com

Territory Manager

in @bogdanalbu

kaspersky