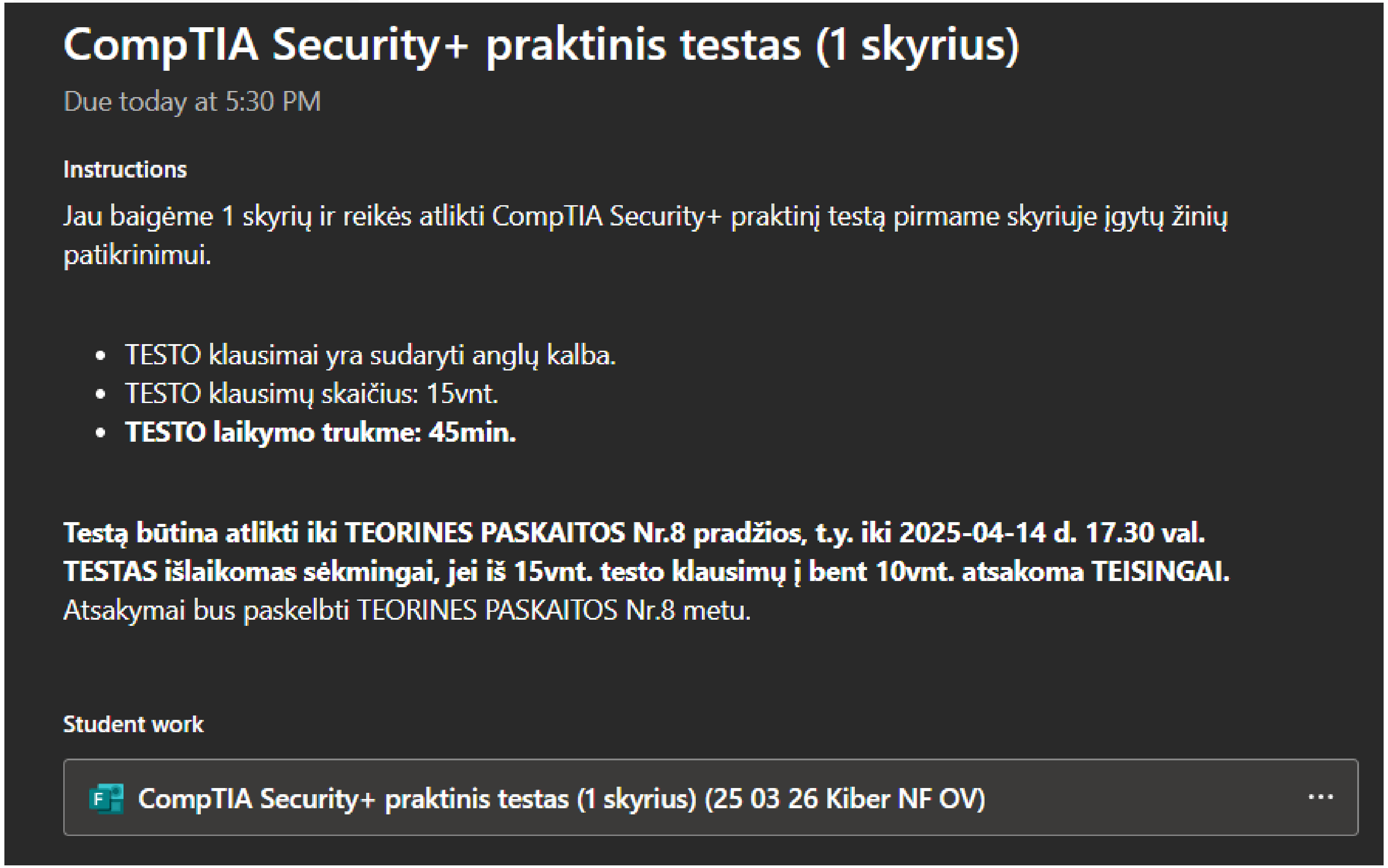
Cyber Security
Lession 8

Quiz

Assignments



CompTIA Security+ praktinis testas (1 skyrius)

Due today at 5:30 PM

Instructions

Jau baigėme 1 skyrių ir reikės atlikti CompTIA Security+ praktinį testą pirmame skyriuje įgytų žinių patikrinimui.

- TESTO klausimai yra sudaryti anglų kalba.
- TESTO klausimų skaičius: 15vnt.
- **TESTO laikymo trukme: 45min.**

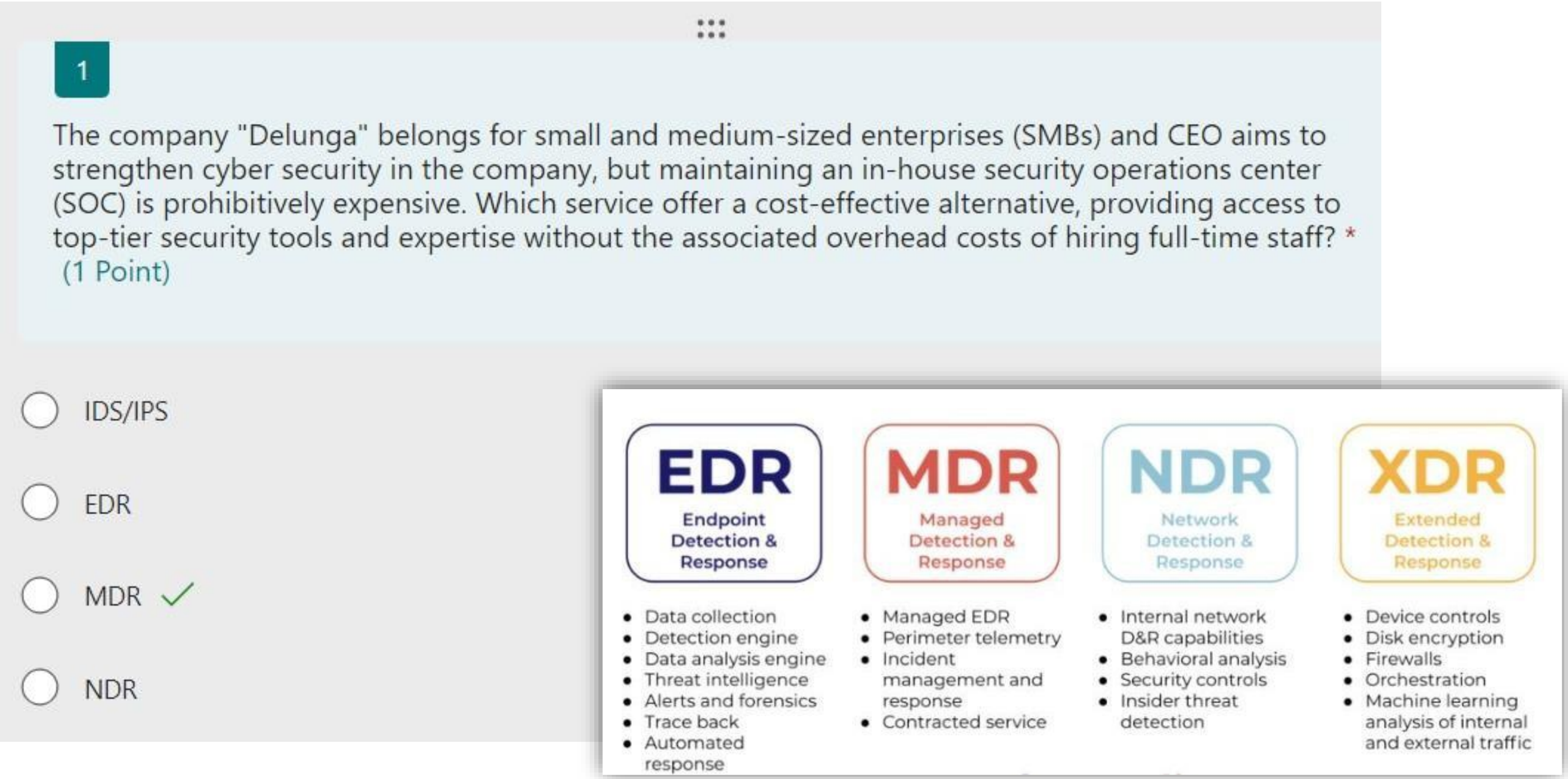
Testą būtina atlikti iki TEORINES PASKAITOS Nr.8 pradžios, t.y. iki 2025-04-14 d. 17.30 val. TESTAS išlaikomas sėkmingai, jei iš 15vnt. testo klausimų į bent 10vnt. atsakoma TEISINGAI. Atsakymai bus paskelbti TEORINES PASKAITOS Nr.8 metu.

Student work

CompTIA Security+ praktinis testas (1 skyrius) (25 03 26 Kiber NF OV) ···

11 Students – Turned in
0 Students – Viewed
0 Student – Not turned in

Quiz



1

The company "Delunga" belongs for small and medium-sized enterprises (SMBs) and CEO aims to strengthen cyber security in the company, but maintaining an in-house security operations center (SOC) is prohibitively expensive. Which service offer a cost-effective alternative, providing access to top-tier security tools and expertise without the associated overhead costs of hiring full-time staff? *
(1 Point)

○ IDS/IPS

○ EDR

○ MDR ✓

○ NDR

EDR Endpoint Detection & Response

- Data collection
- Detection engine
- Data analysis engine
- Threat intelligence
- Alerts and forensics
- Trace back
- Automated response

MDR Managed Detection & Response

- Managed EDR
- Perimeter telemetry
- Incident management and response
- Contracted service

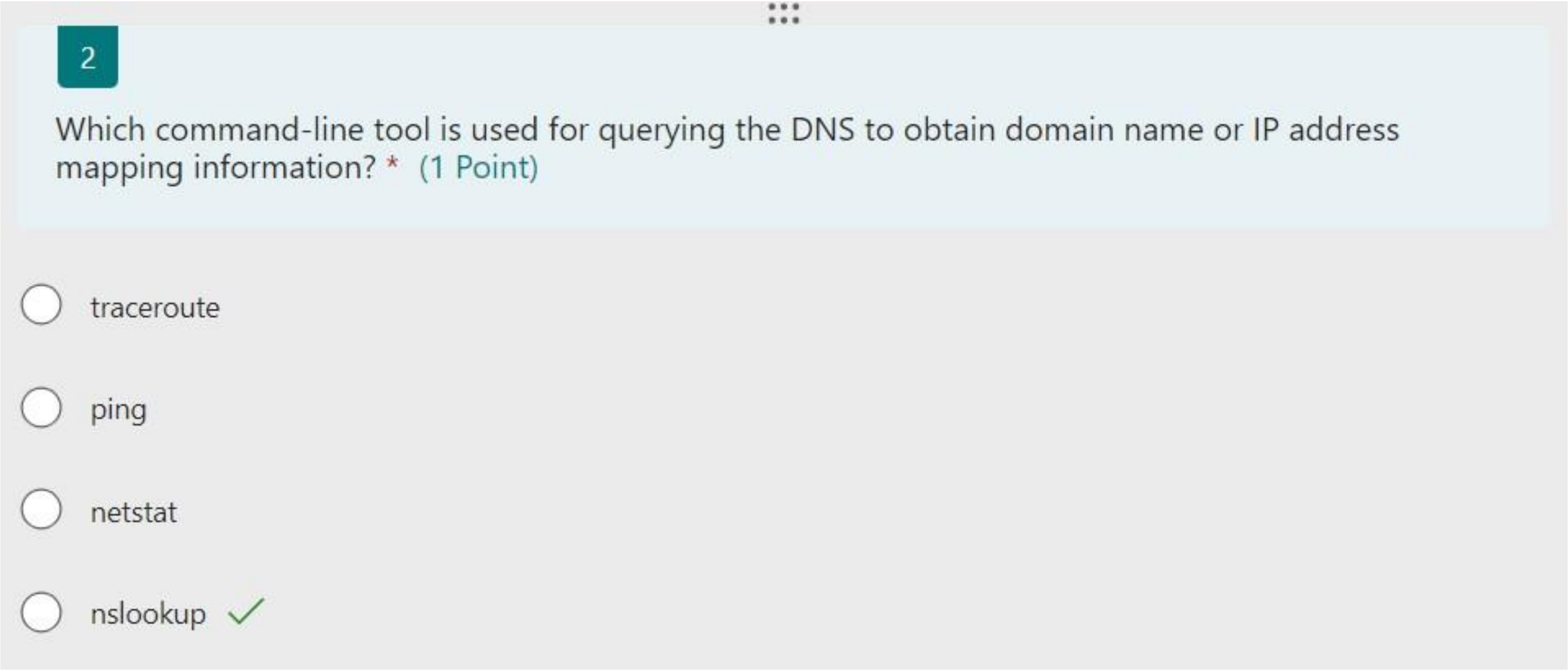
NDR Network Detection & Response

- Internal network D&R capabilities
- Behavioral analysis
- Security controls
- Insider threat detection

XDR Extended Detection & Response

- Device controls
- Disk encryption
- Firewalls
- Orchestration
- Machine learning analysis of internal and external traffic

Quiz



2

Which command-line tool is used for querying the DNS to obtain domain name or IP address mapping information? * (1 Point)

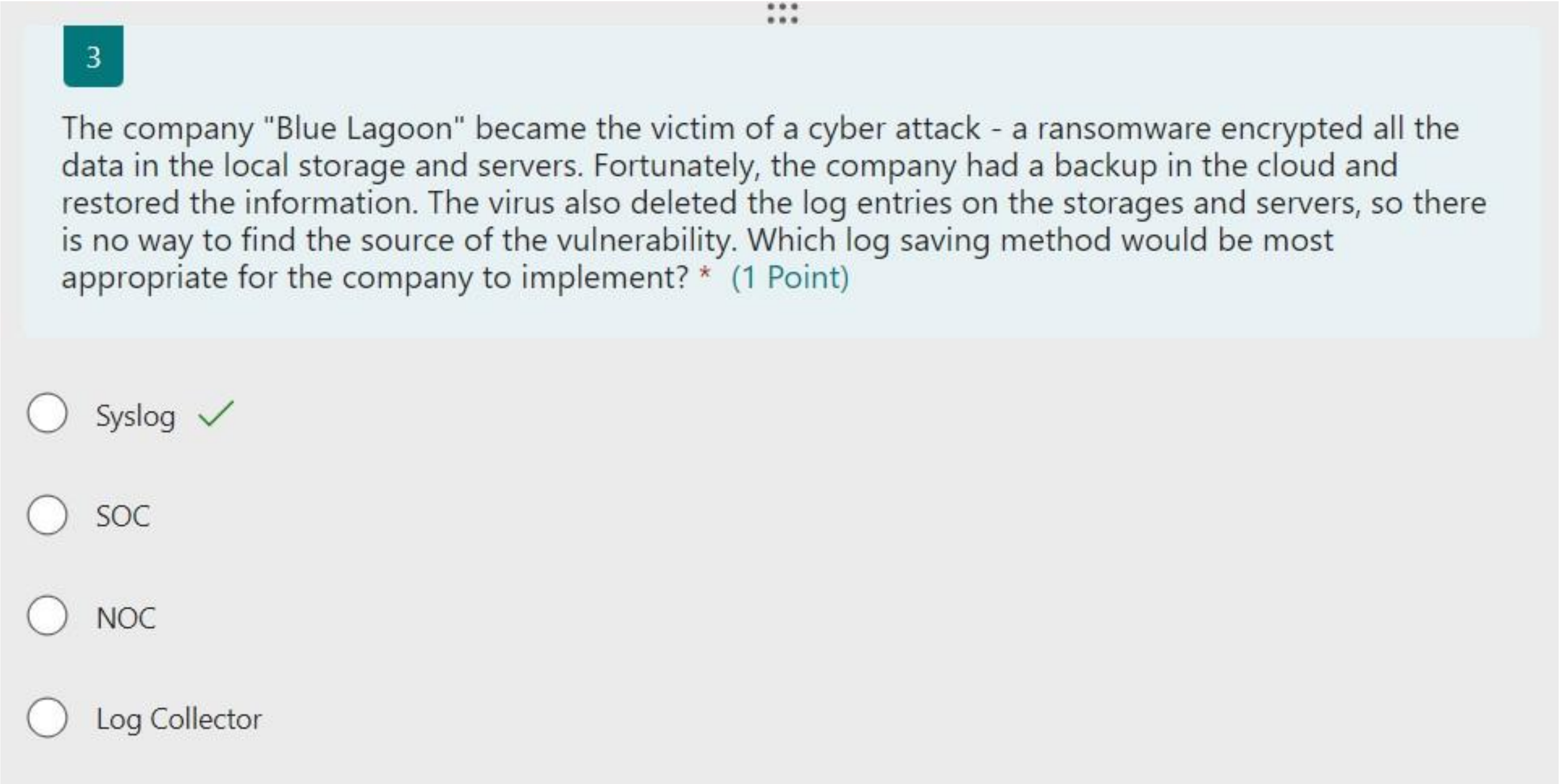
○ traceroute

○ ping

○ netstat

○ nslookup ✓

Quiz



3

The company "Blue Lagoon" became the victim of a cyber attack - a ransomware encrypted all the data in the local storage and servers. Fortunately, the company had a backup in the cloud and restored the information. The virus also deleted the log entries on the storages and servers, so there is no way to find the source of the vulnerability. Which log saving method would be most appropriate for the company to implement? * (1 Point)

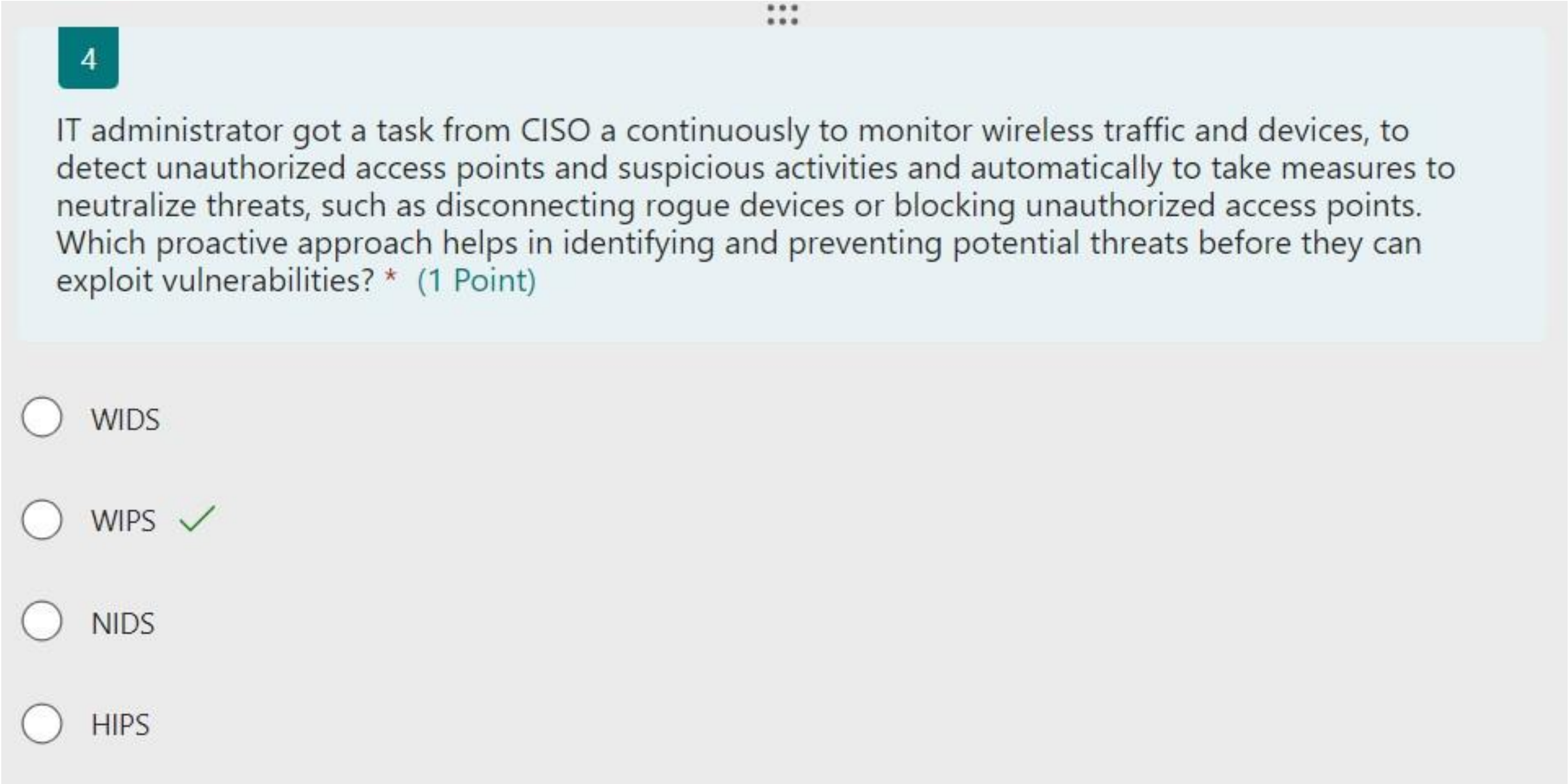
○ Syslog ✓

○ SOC

○ NOC

○ Log Collector

Quiz



4

IT administrator got a task from CISO a continuously to monitor wireless traffic and devices, to detect unauthorized access points and suspicious activities and automatically to take measures to neutralize threats, such as disconnecting rogue devices or blocking unauthorized access points. Which proactive approach helps in identifying and preventing potential threats before they can exploit vulnerabilities? * (1 Point)

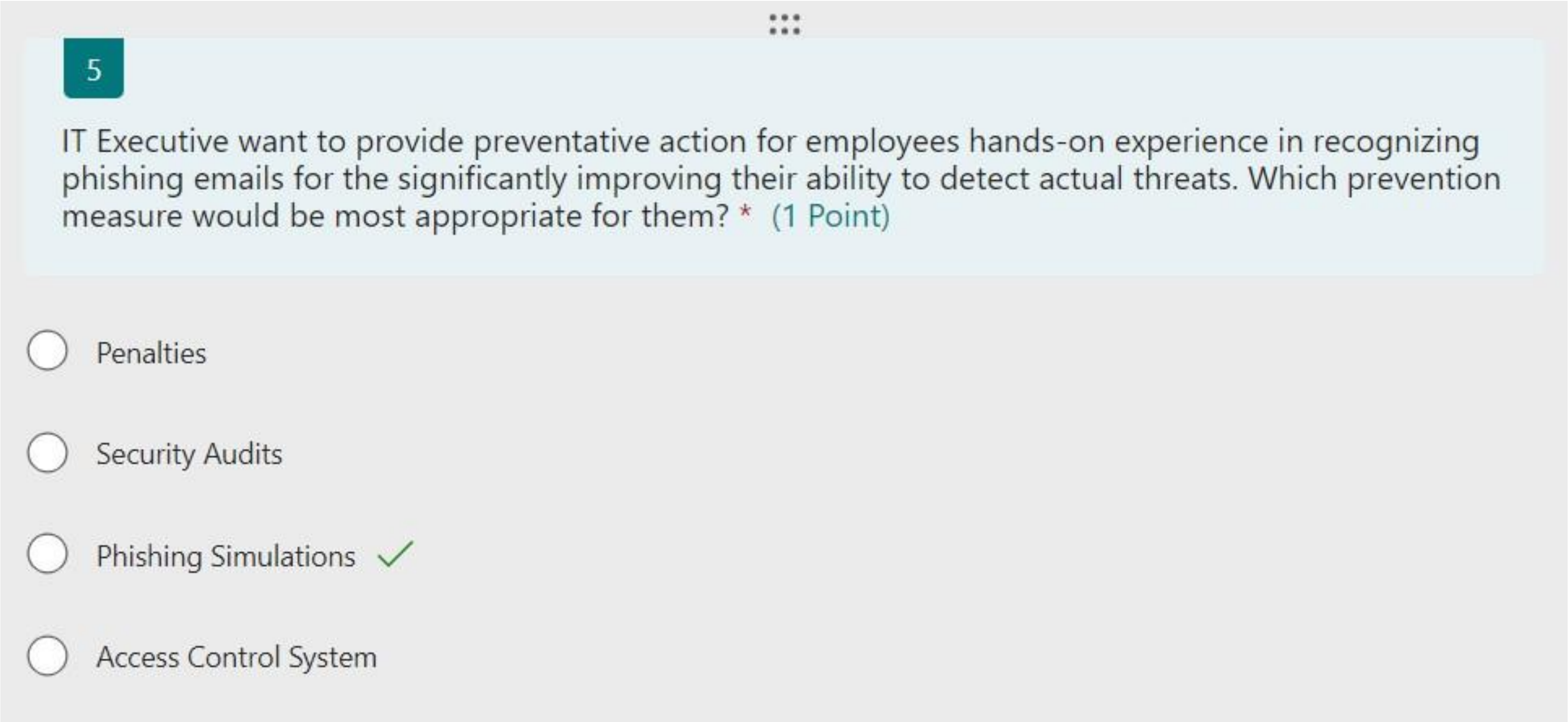
○ WIDS

○ WIPS ✓

○ NIDS

○ HIPS

Quiz



5

IT Executive want to provide preventative action for employees hands-on experience in recognizing phishing emails for the significantly improving their ability to detect actual threats. Which prevention measure would be most appropriate for them? * (1 Point)

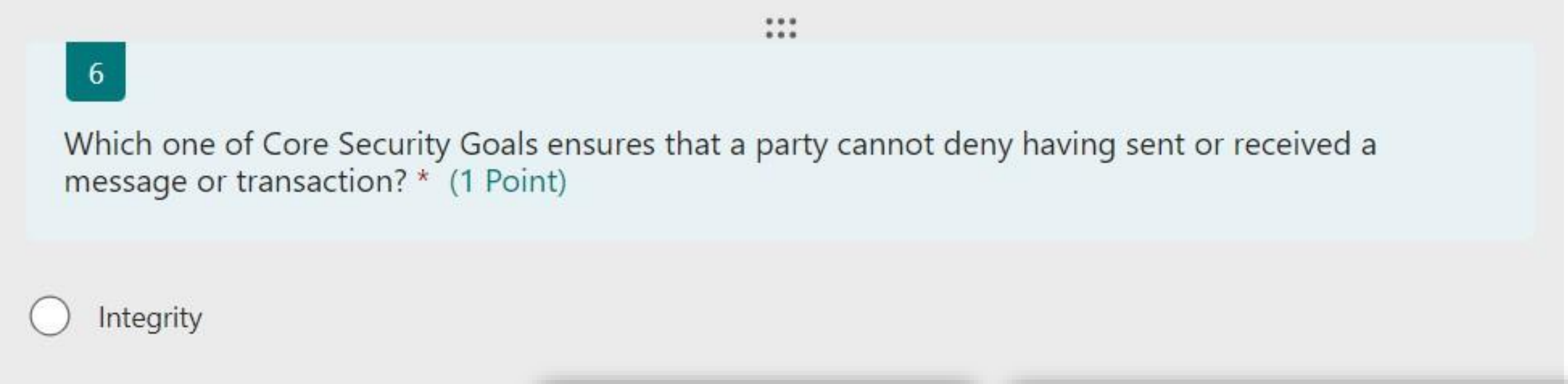
○ Penalties

○ Security Audits

○ Phishing Simulations ✓

○ Access Control System

Quiz



6

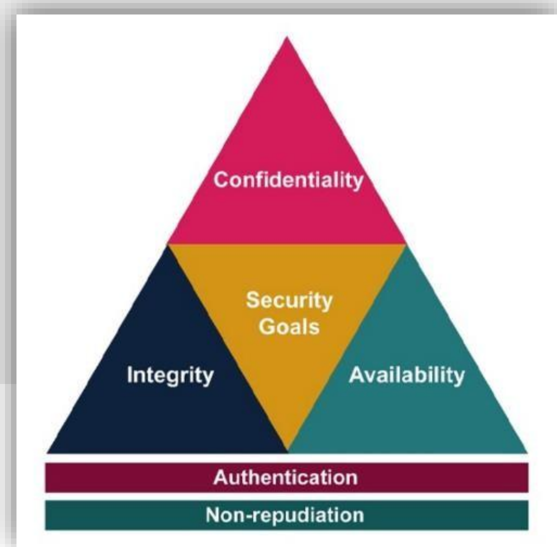
Which one of Core Security Goals ensures that a party cannot deny having sent or received a message or transaction? * (1 Point)

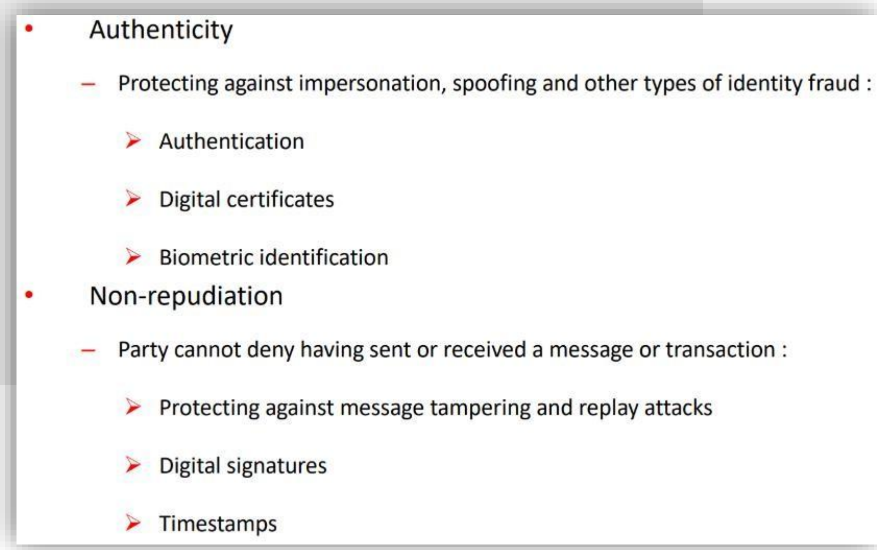
○ Integrity

○ Authenticity

○ Availability

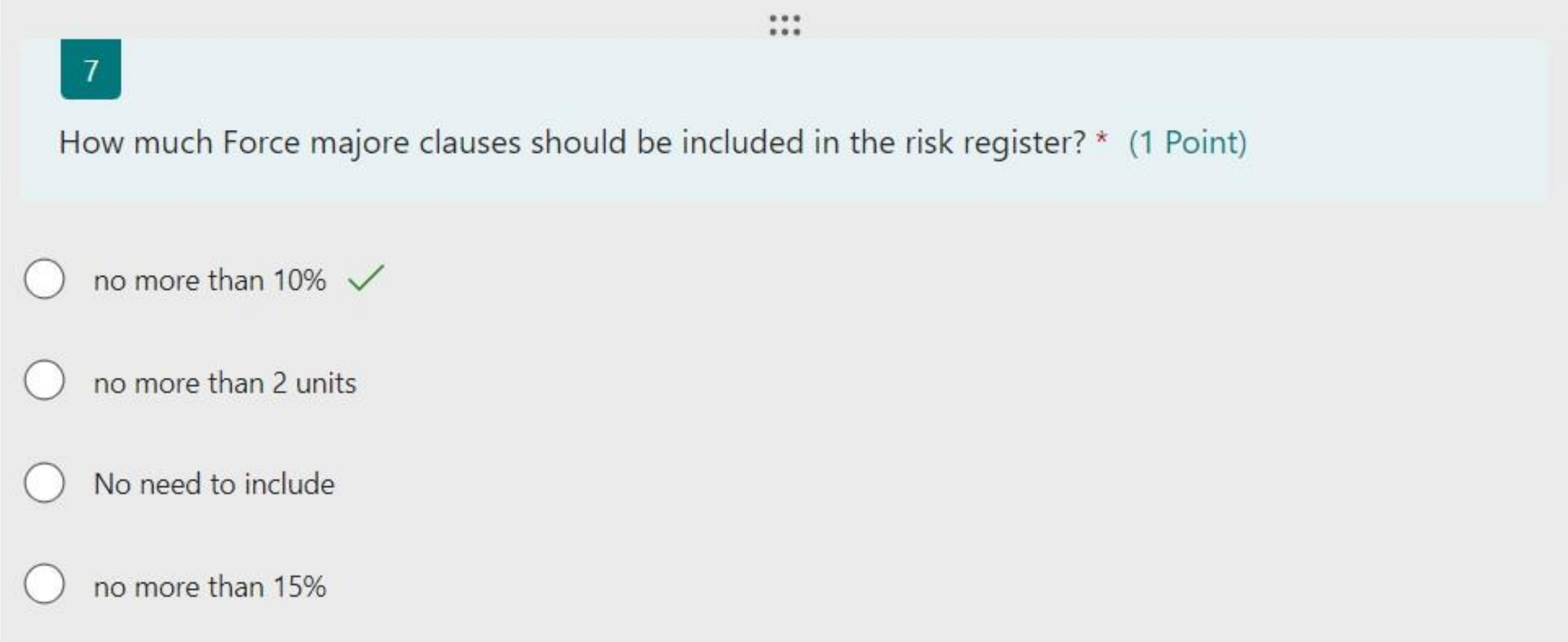
○ Non-repudiation ✓





- Authenticity
  - Protecting against impersonation, spoofing and other types of identity fraud :
    - Authentication
    - Digital certificates
    - Biometric identification
- Non-repudiation
  - Party cannot deny having sent or received a message or transaction :
    - Protecting against message tampering and replay attacks
    - Digital signatures
    - Timestamps

Quiz



7

How much Force majore clauses should be included in the risk register? * (1 Point)

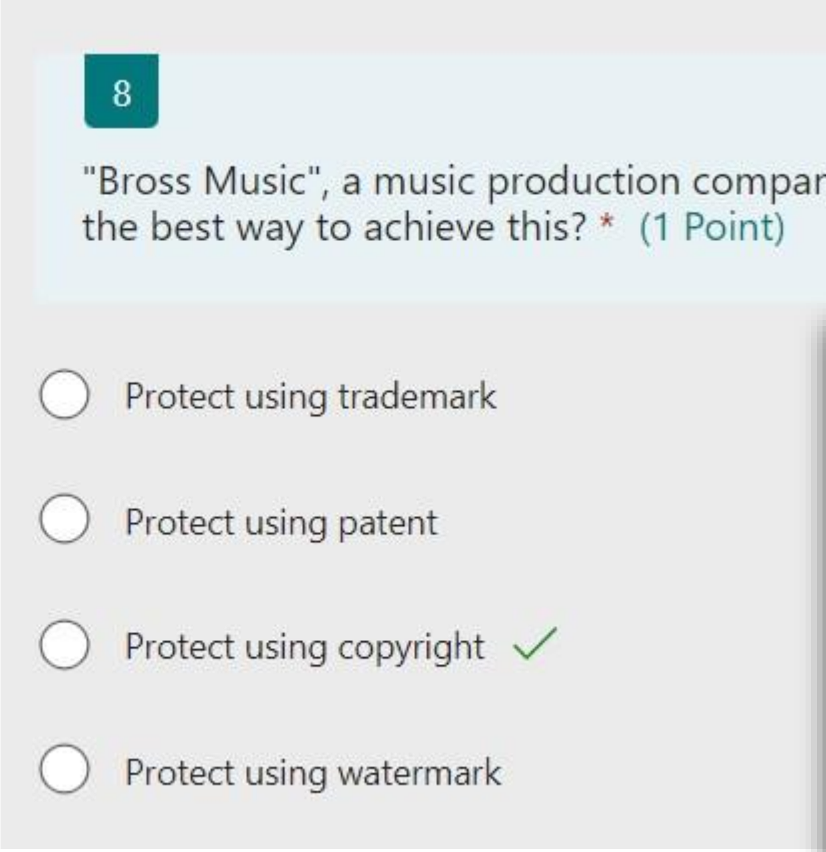
○ no more than 10% ✓

○ no more than 2 units

○ No need to include

○ no more than 15%

Quiz



8

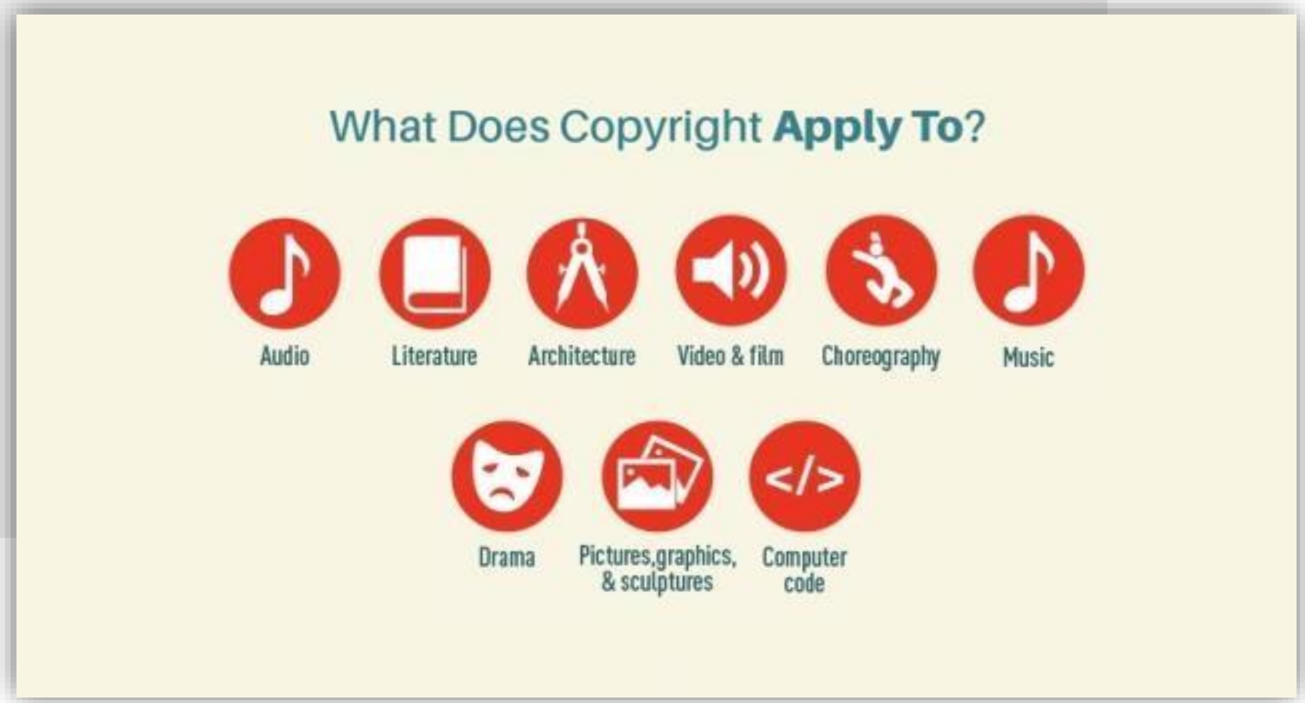
"Bross Music", a music production company, want to protect its intellectual property. What would be the best way to achieve this? * (1 Point)

○ Protect using trademark

○ Protect using patent

○ Protect using copyright ✓

○ Protect using watermark

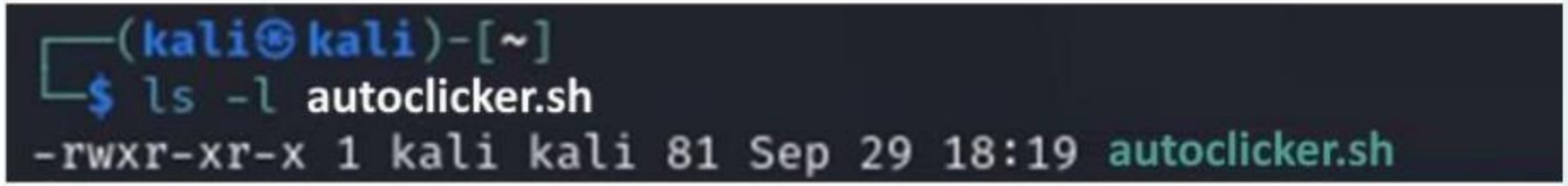


What Does Copyright **Apply To**?

Quiz

9

IT administrator created autoclicker.sh script and set different permissions for a file and control who can read it. Based on the picture, what permissions are set for the group? * (1 Point)



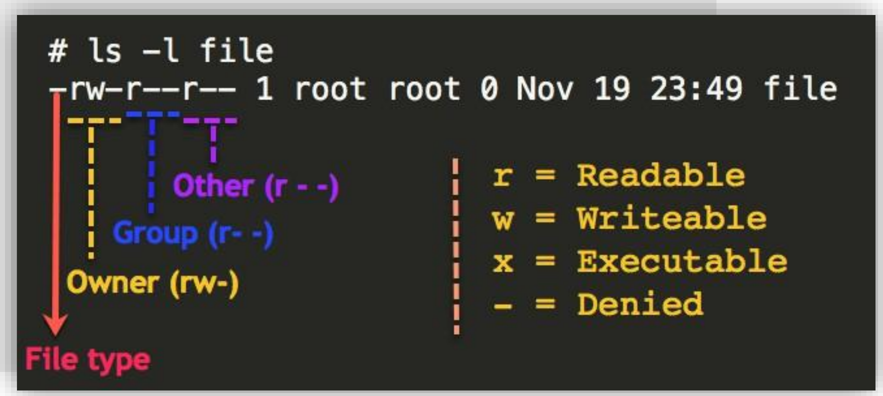
```
┌──(kali㉿kali)-[~]
└─$ ls -l autoclicker.sh
-rwxr-xr-x 1 kali kali 81 Sep 29 18:19 autoclicker.sh
```

○ Readable, Writeable, Executable

○ Readable and Executable ✓

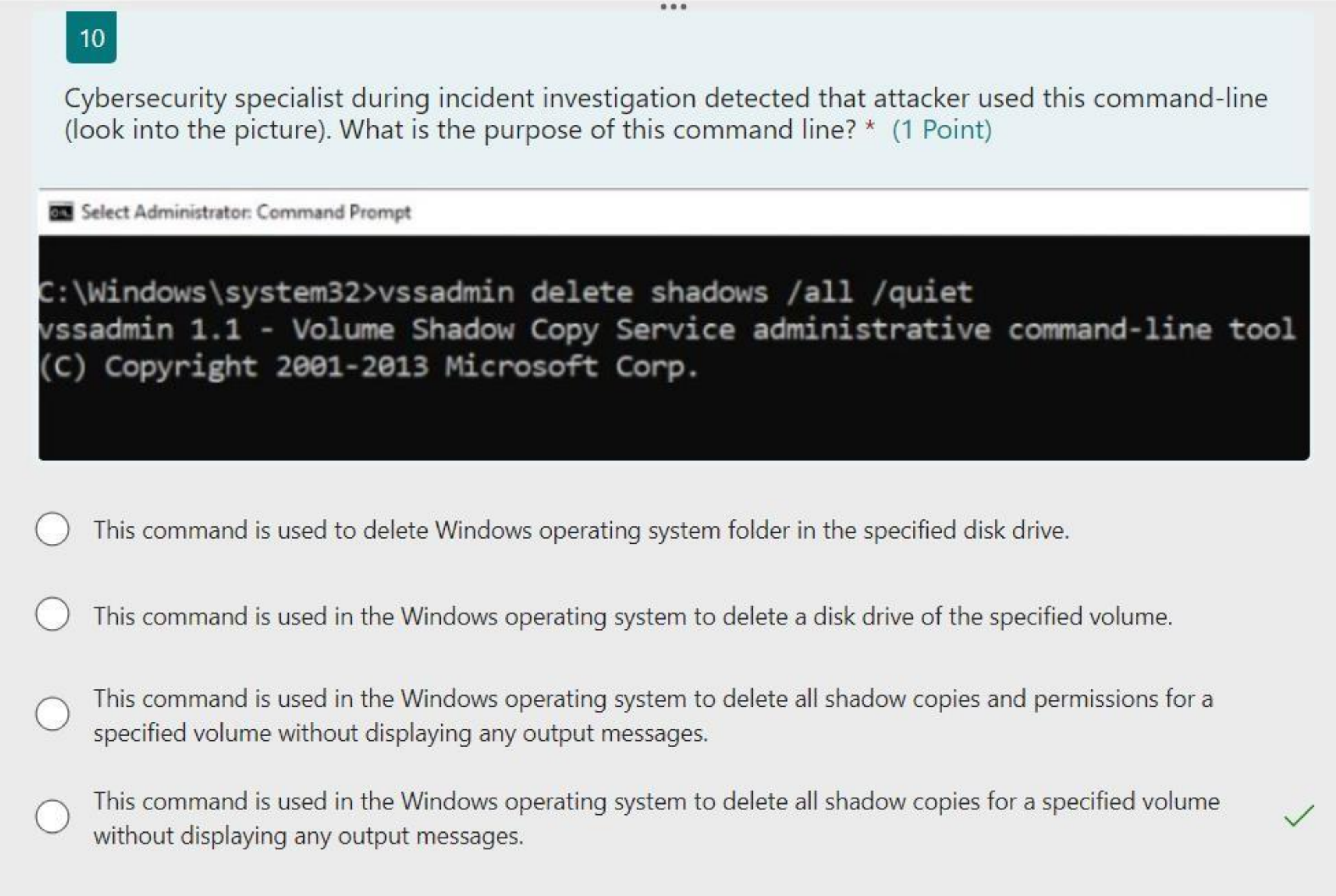
○ Writeable, Executable

○ Only Executable



```
# ls -l file
-rw-r--r-- 1 root root 0 Nov 19 23:49 file
```

Quiz



10

Cybersecurity specialist during incident investigation detected that attacker used this command-line (look into the picture). What is the purpose of this command line? * (1 Point)

Select Administrator: Command Prompt

```
C:\Windows\system32>vssadmin delete shadows /all /quiet
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.
```

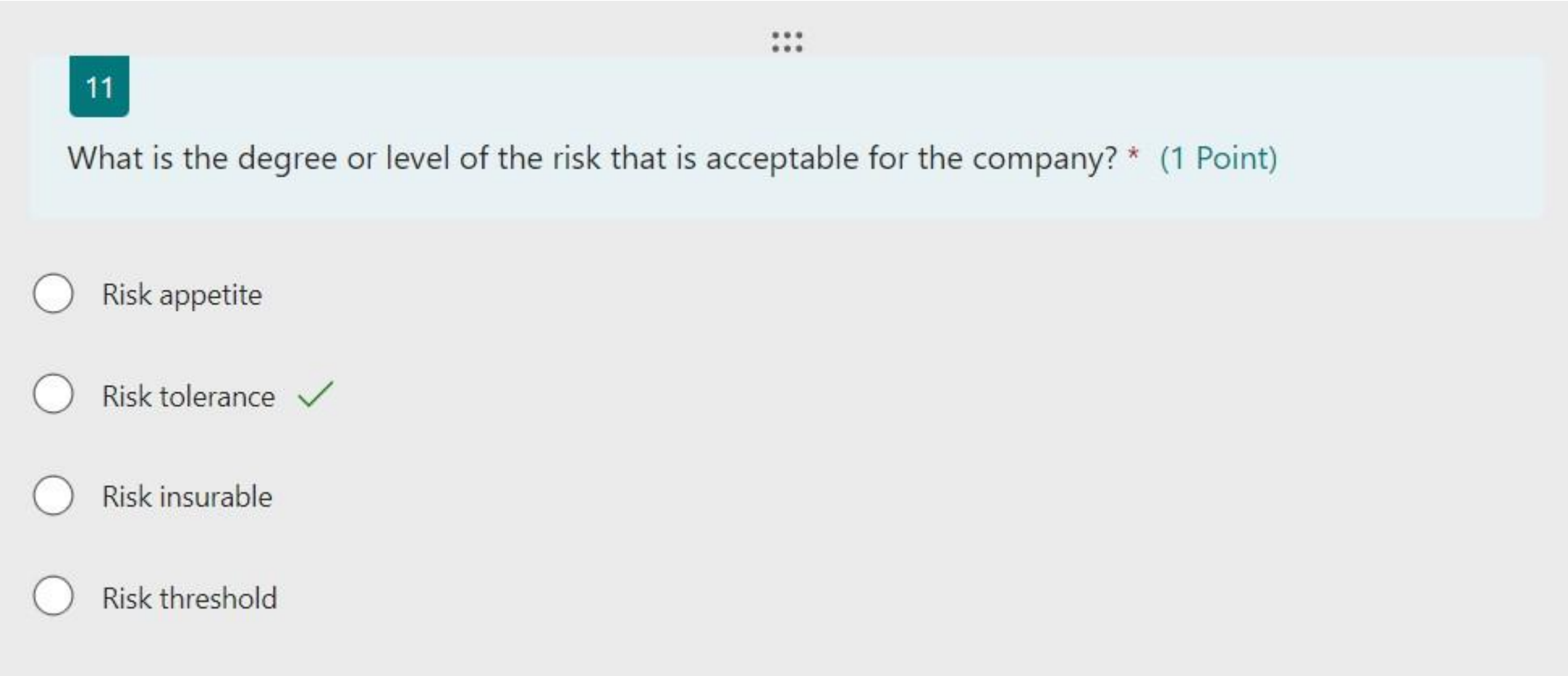
○ This command is used to delete Windows operating system folder in the specified disk drive.

○ This command is used in the Windows operating system to delete a disk drive of the specified volume.

○ This command is used in the Windows operating system to delete all shadow copies and permissions for a specified volume without displaying any output messages.

○ This command is used in the Windows operating system to delete all shadow copies for a specified volume without displaying any output messages. ✓

Quiz



11

What is the degree or level of the risk that is acceptable for the company? * (1 Point)

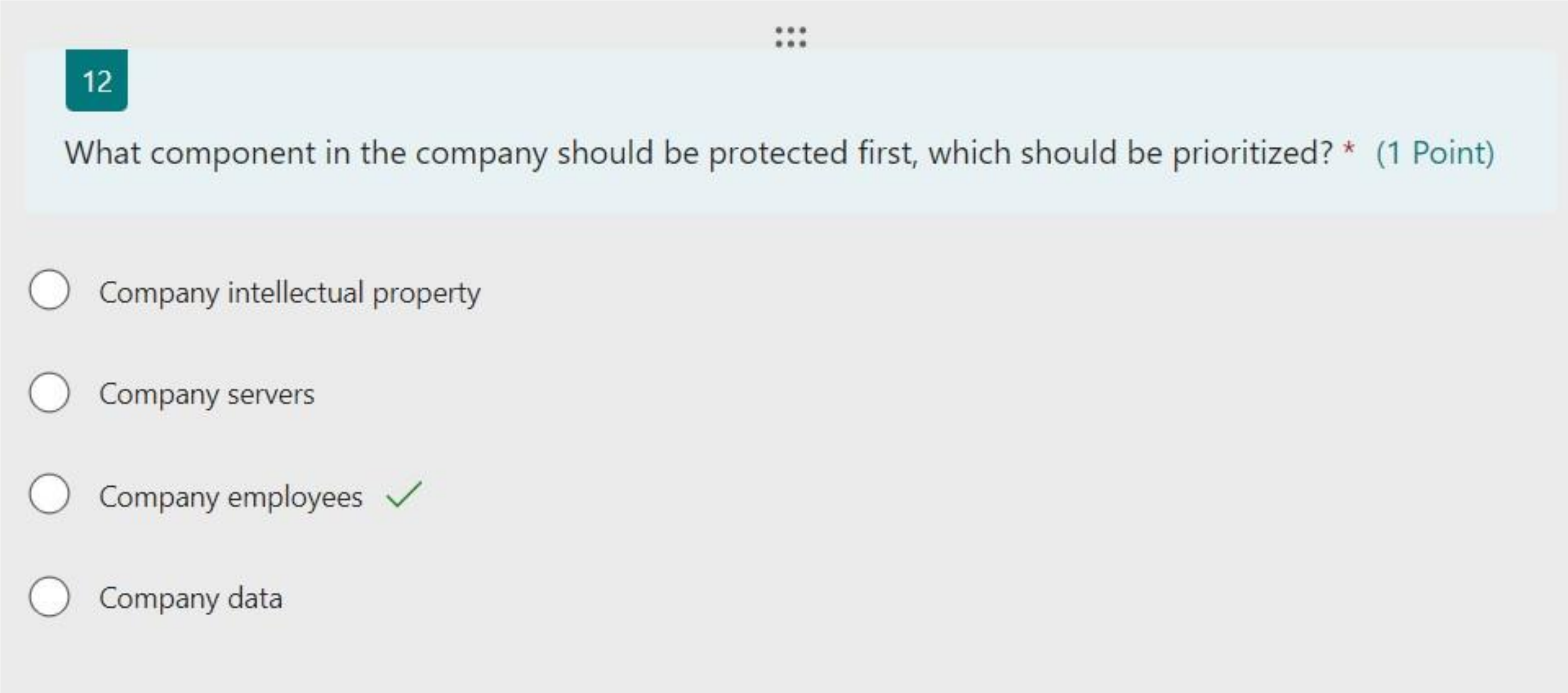
○ Risk appetite

○ Risk tolerance ✓

○ Risk insurable

○ Risk threshold

Quiz



12

What component in the company should be protected first, which should be prioritized? * (1 Point)

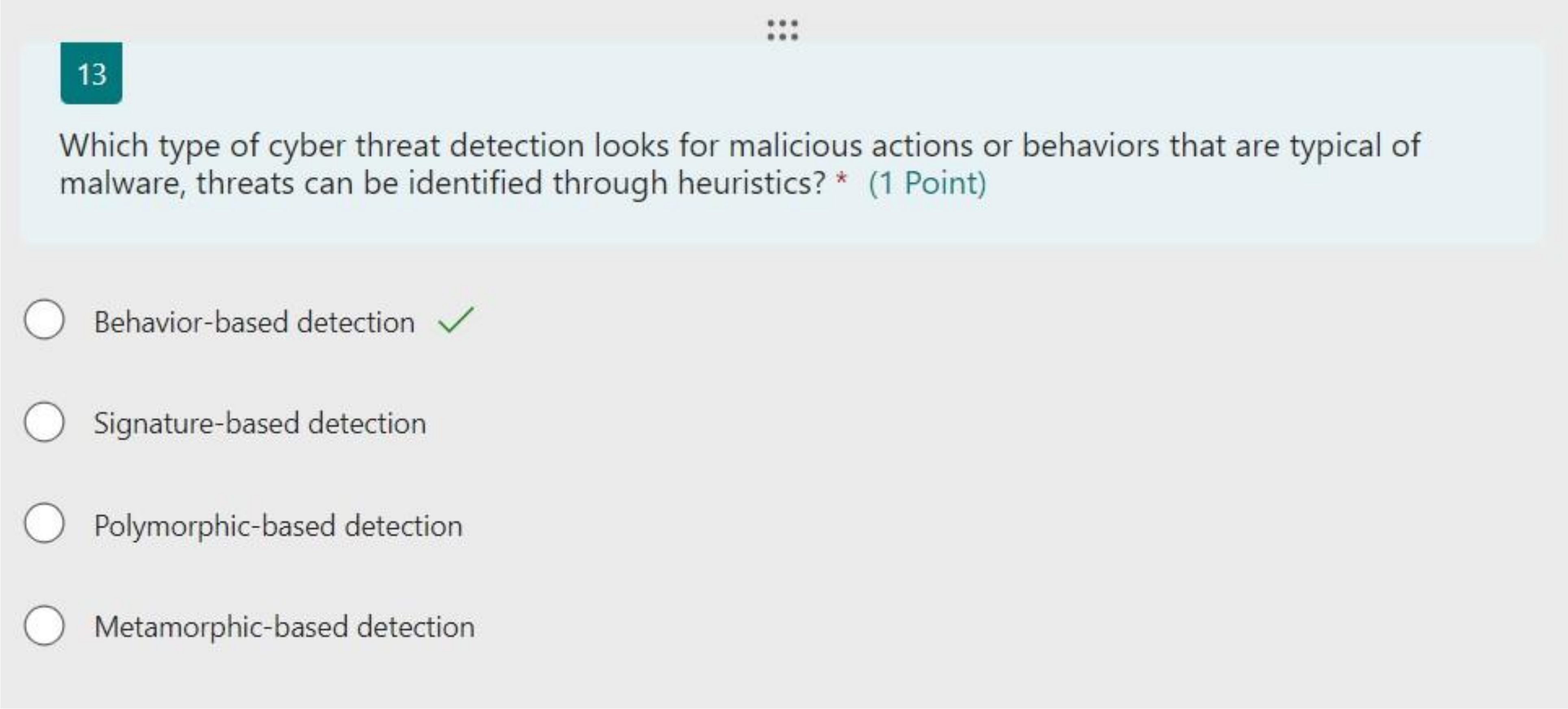
○ Company intellectual property

○ Company servers

○ Company employees ✓

○ Company data

Quiz



13

Which type of cyber threat detection looks for malicious actions or behaviors that are typical of malware, threats can be identified through heuristics? * (1 Point)

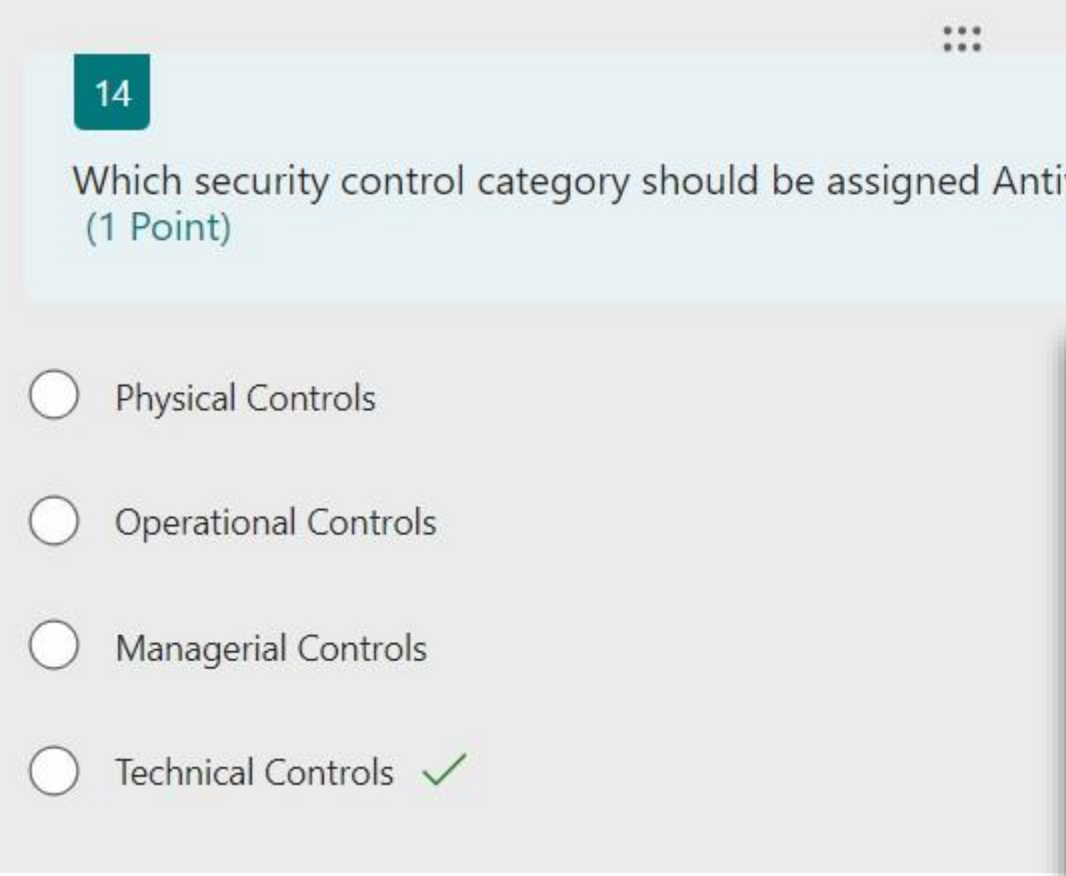
○ Behavior-based detection ✓

○ Signature-based detection

○ Polymorphic-based detection

○ Metamorphic-based detection

Quiz



14

Which security control category should be assigned Antivirus software, Firewall and IDS/IPS? *
(1 Point)

○ Physical Controls

○ Operational Controls

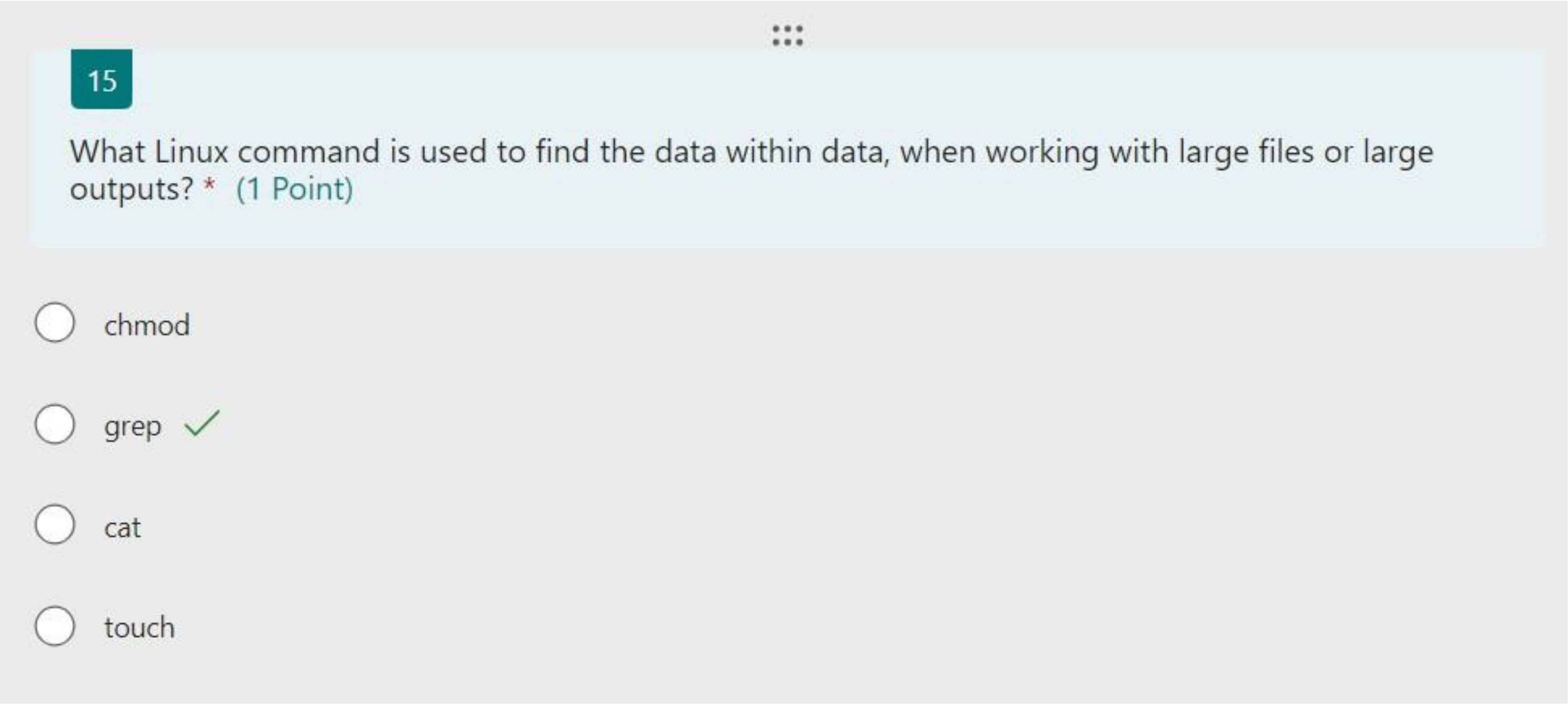
○ Managerial Controls

○ Technical Controls ✓

Technical Security Controls

- ✓ Firewalls
- ✓ Endpoint Detection and Response systems
- ✓ Data encryption
- ✓ Access Control Lists
- ✓ Network segmentation
- ✓ Patch management systems

Quiz



15

What Linux command is used to find the data within data, when working with large files or large outputs? * (1 Point)

○ chmod

○ grep ✓

○ cat

○ touch

Quiz best results

10+ correct – passed

<10 correct – not passed

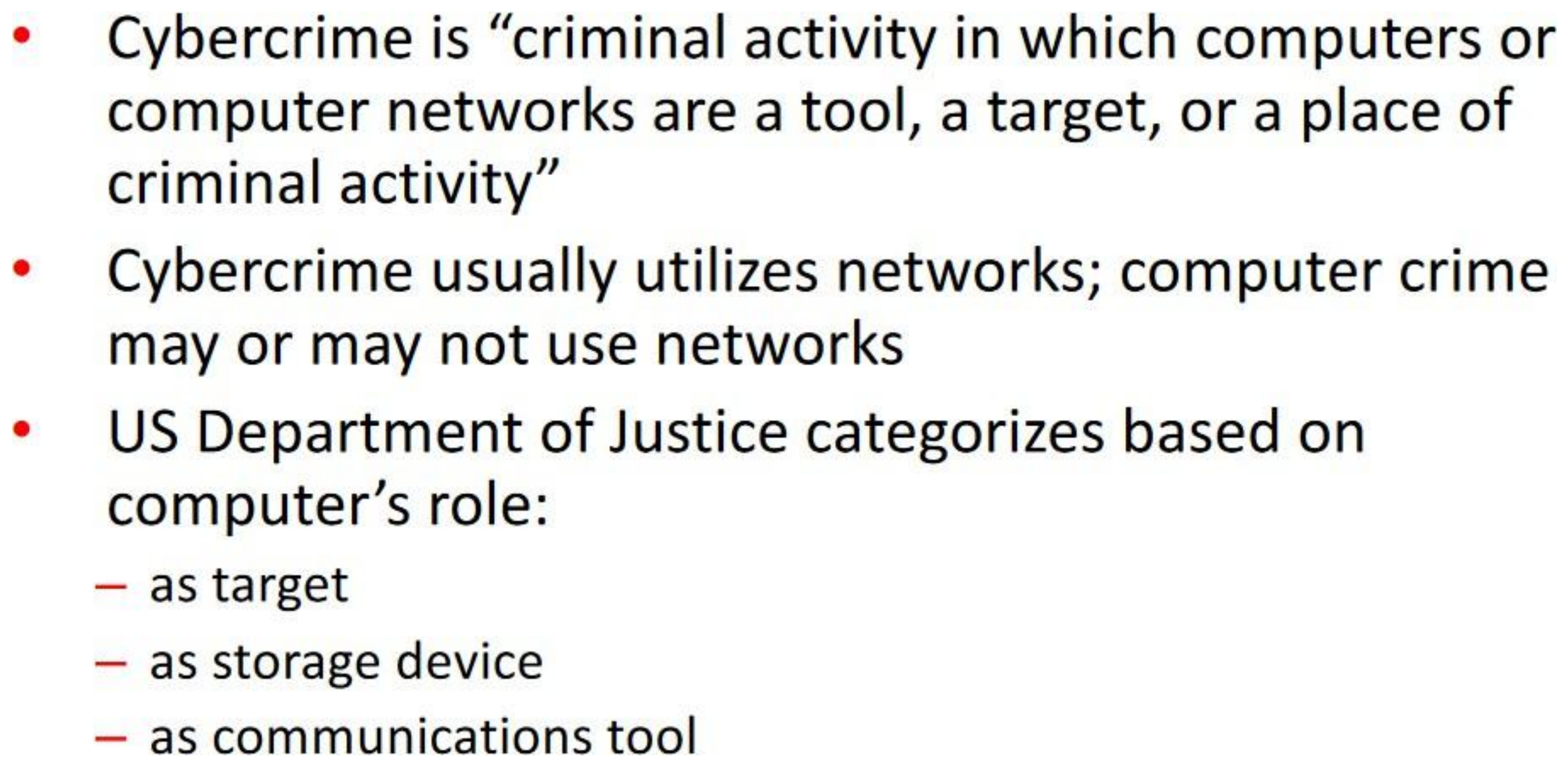
In the previous lession…

Legal aspects of cyber security

Overview

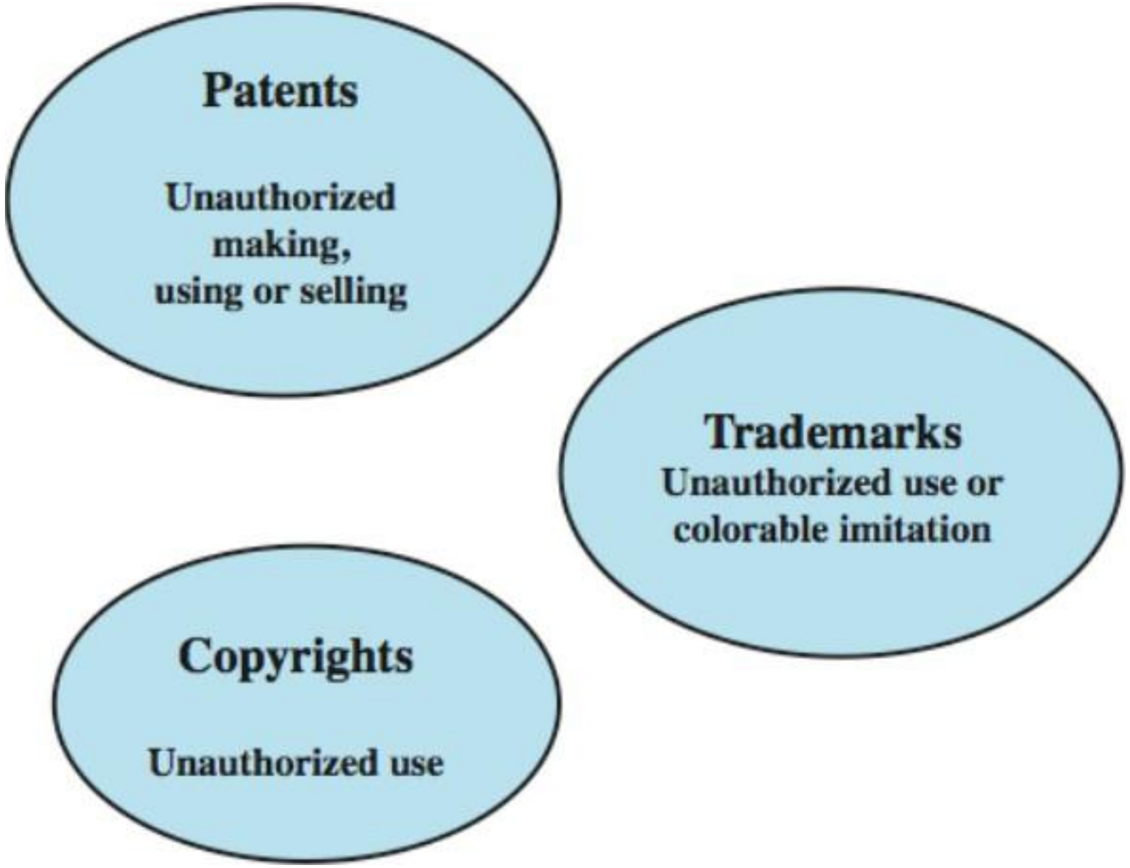
- Cybercrime and computer crime
- Intellectual property issues
- Privacy
- Ethical issues

Cybercrime / Computer Crime



- Cybercrime is “criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity”
- Cybercrime usually utilizes networks; computer crime may or may not use networks
- US Department of Justice categorizes based on computer’s role:
  - as target
  - as storage device
  - as communications tool

Intellectual Property



Patents

Unauthorized making, using or selling

Trademarks

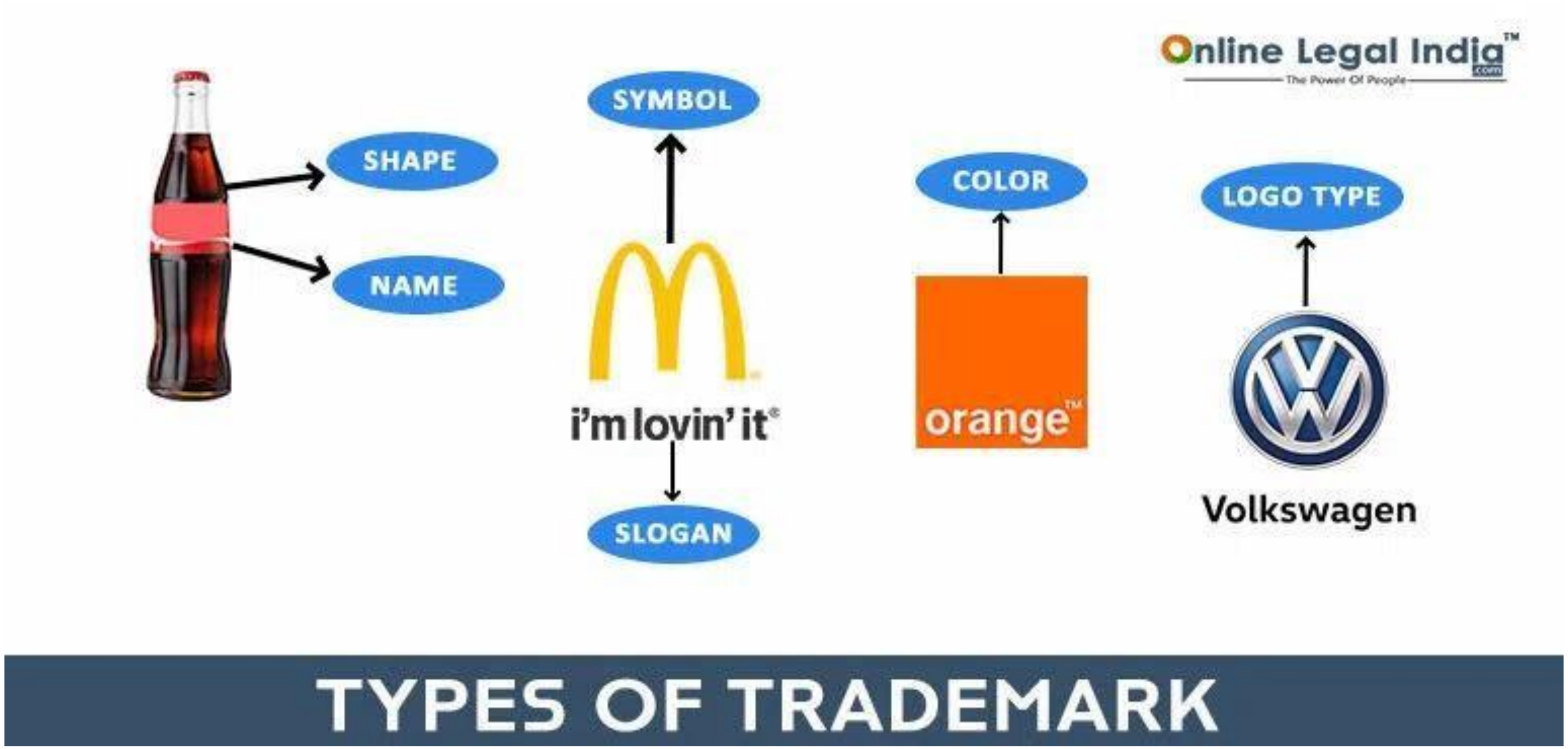
Unauthorized use or colorable imitation

Copyrights

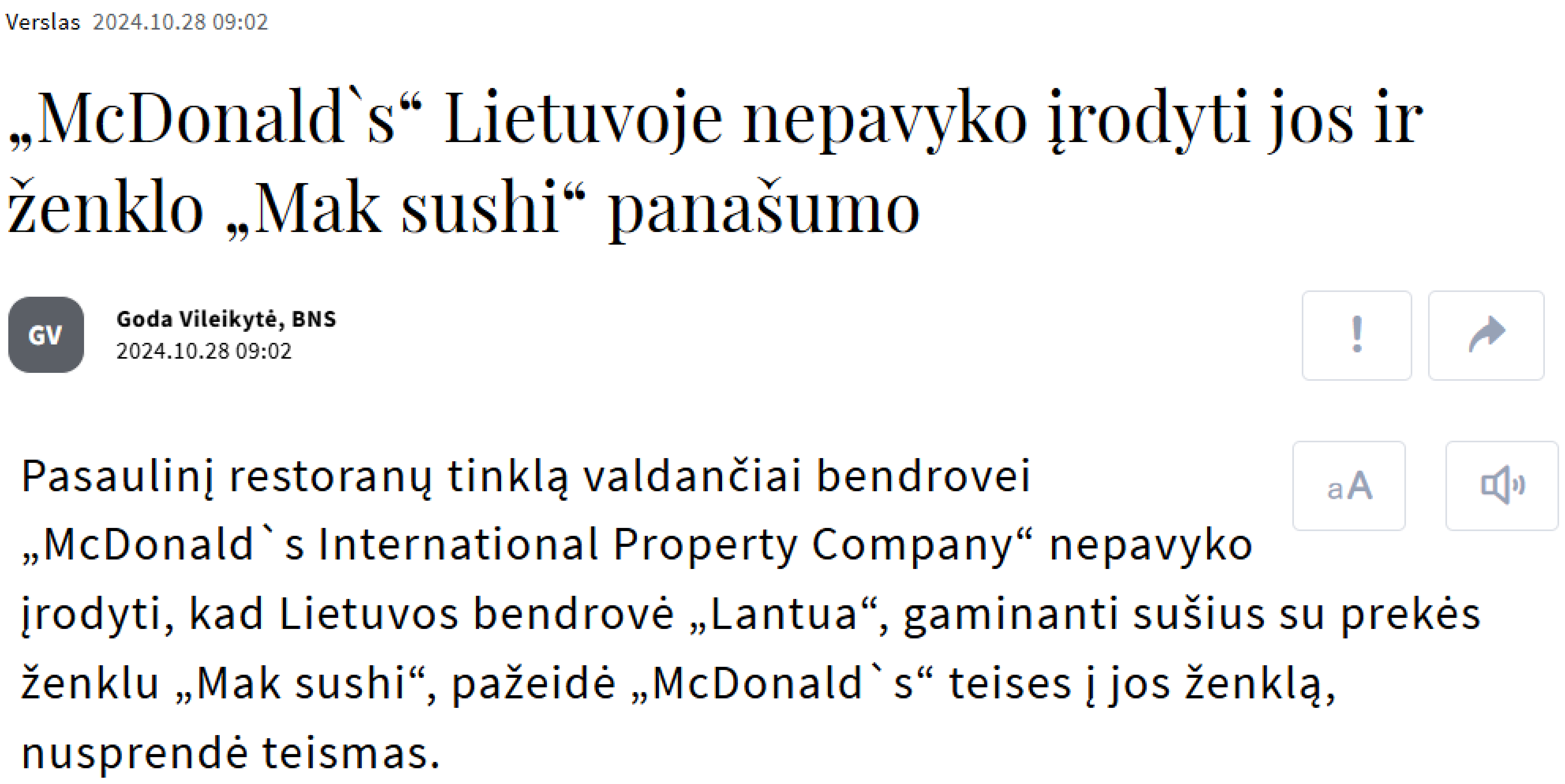
Unauthorized use

Copyright Rights

Trademarks


Online Legal India™
The Power Of People
SHAPE
NAME
SYMBOL
i'm lovin' it®
SLOGAN
COLOR
orange™
LOGO TYPE
Volkswagen
TYPES OF TRADEMARK

Trademarks



Verslas 2024.10.28 09:02

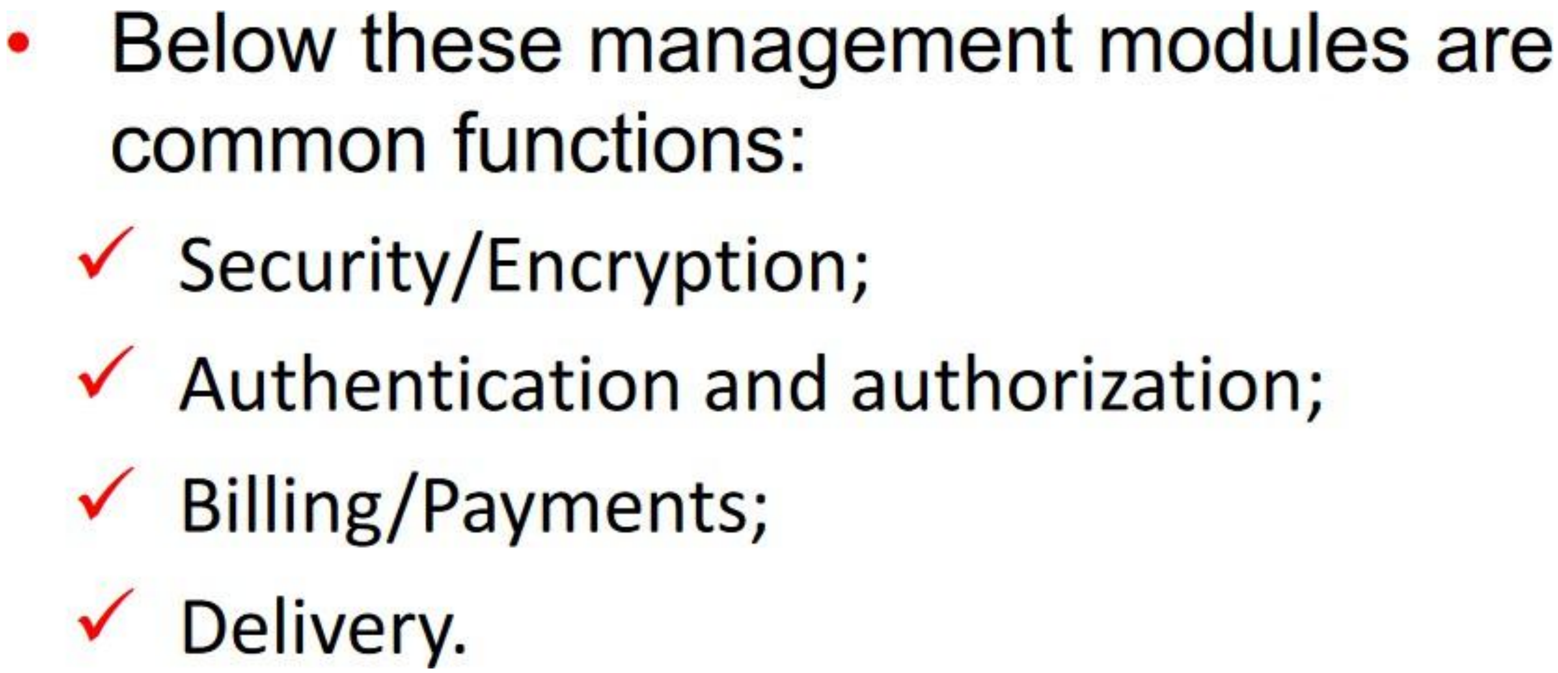
„McDonald`s“ Lietuvoje nepavyko įrodyti jos ir ženklo „Mak sushi“ panašumo

Goda Vileikytė, BNS
2024.10.28 09:02

Pasaulinį restoranų tinklą valdančiai bendrovei „McDonald`s International Property Company“ nepavyko įrodyti, kad Lietuvos bendrovė „Lantua“, gaminanti sušius su prekės ženklu „Mak sushi“, pažeidė „McDonald`s“ teises į jos ženklą, nusprendė teismas.

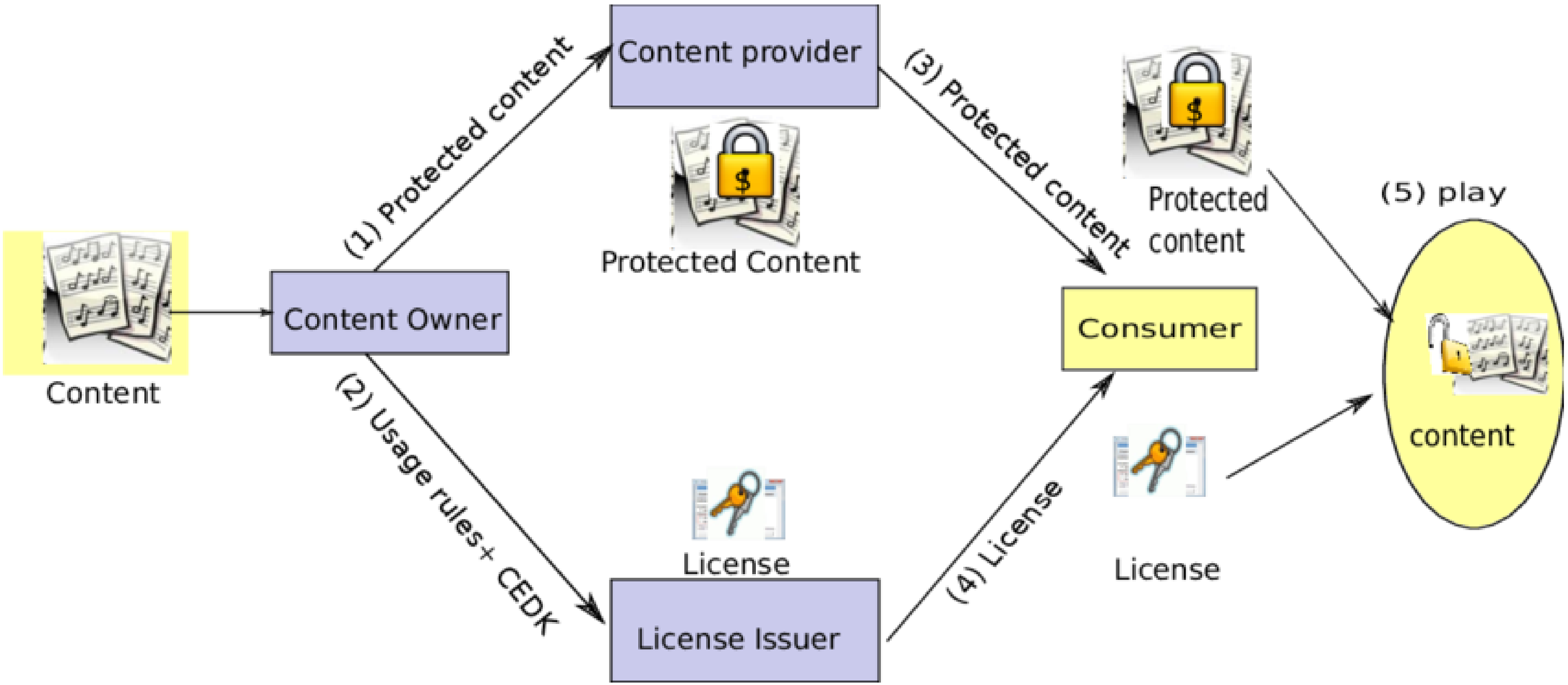
Lesson 8

DRM System Architecture



- Below these management modules are common functions:
  - ✓ Security/Encryption;
  - ✓ Authentication and authorization;
  - ✓ Billing/Payments;
  - ✓ Delivery.

DRM System Architecture



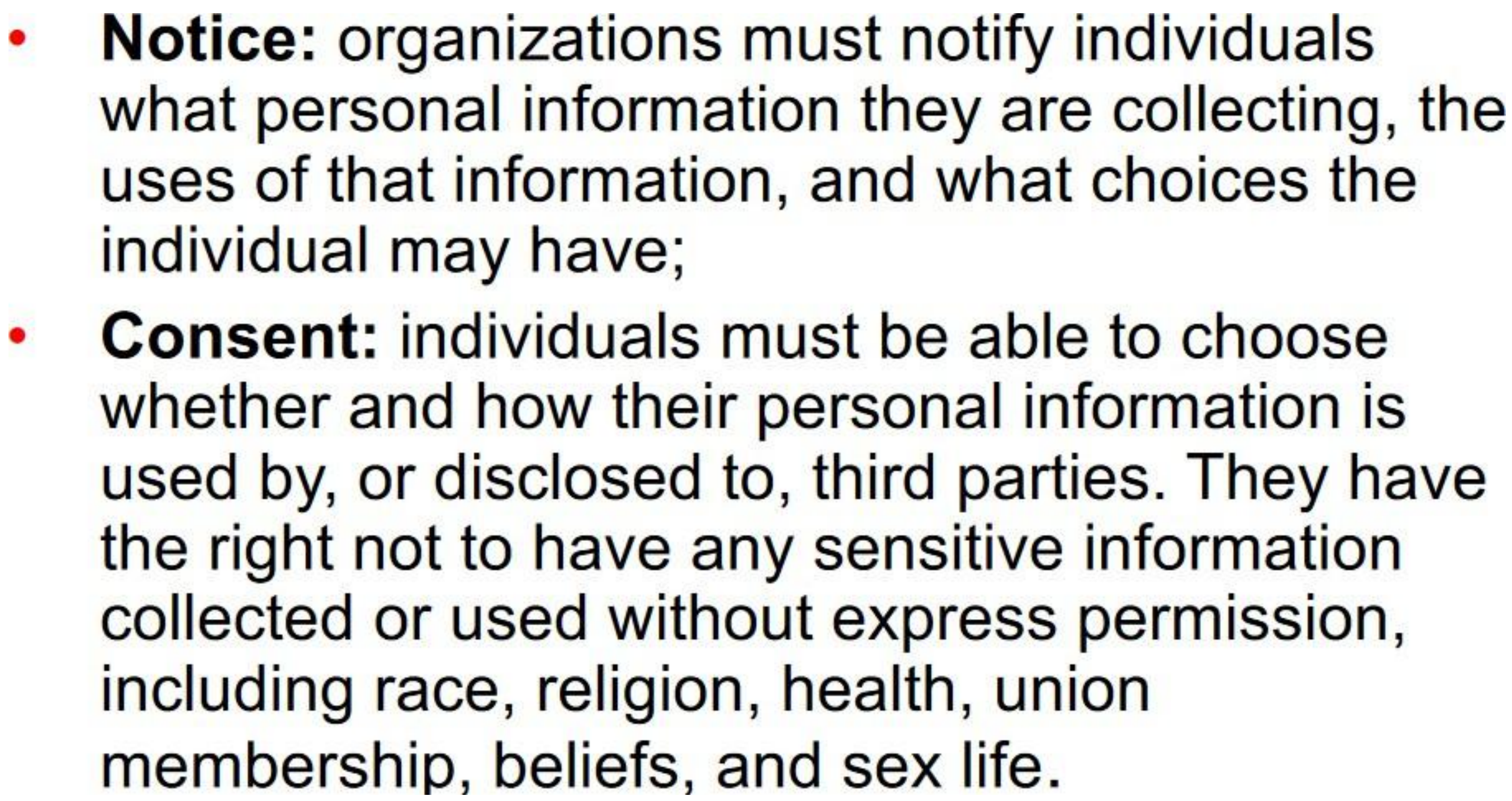
Privacy

- Overlaps with computer security;
- Has dramatic increase in scale of info collected and stored :
  - ✓ motivated by law enforcement, national security, economic incentives;
- Individuals increasingly aware of access and use of personal / private info;
- Concerns about the extent to which privacy has been compromised has resulted in a range of responses and legal and technical approaches and to reinforcing privacy rights.

EU Privacy Law

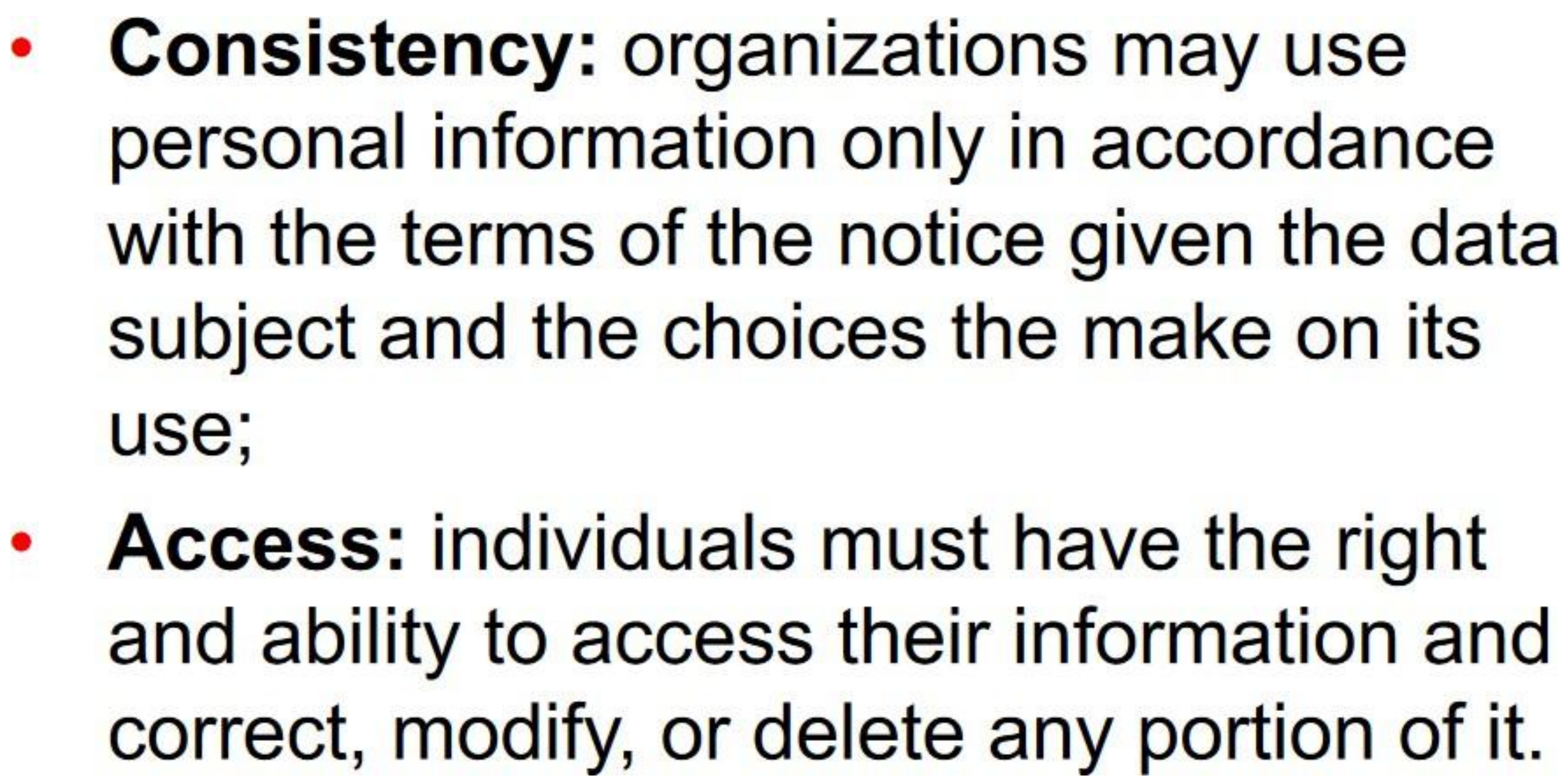
- European Union Data Protection Directive was adopted in 1998 to:
  - ✓ ensure member states protect fundamental privacy rights when processing personal info;
  - ✓ prevent member states from restricting the free flow of personal info within EU;
- Organized around principles of:
  - ✓ notice, consent, consistency, access, security, onward transfer, enforcement.

EU Privacy Law Principles



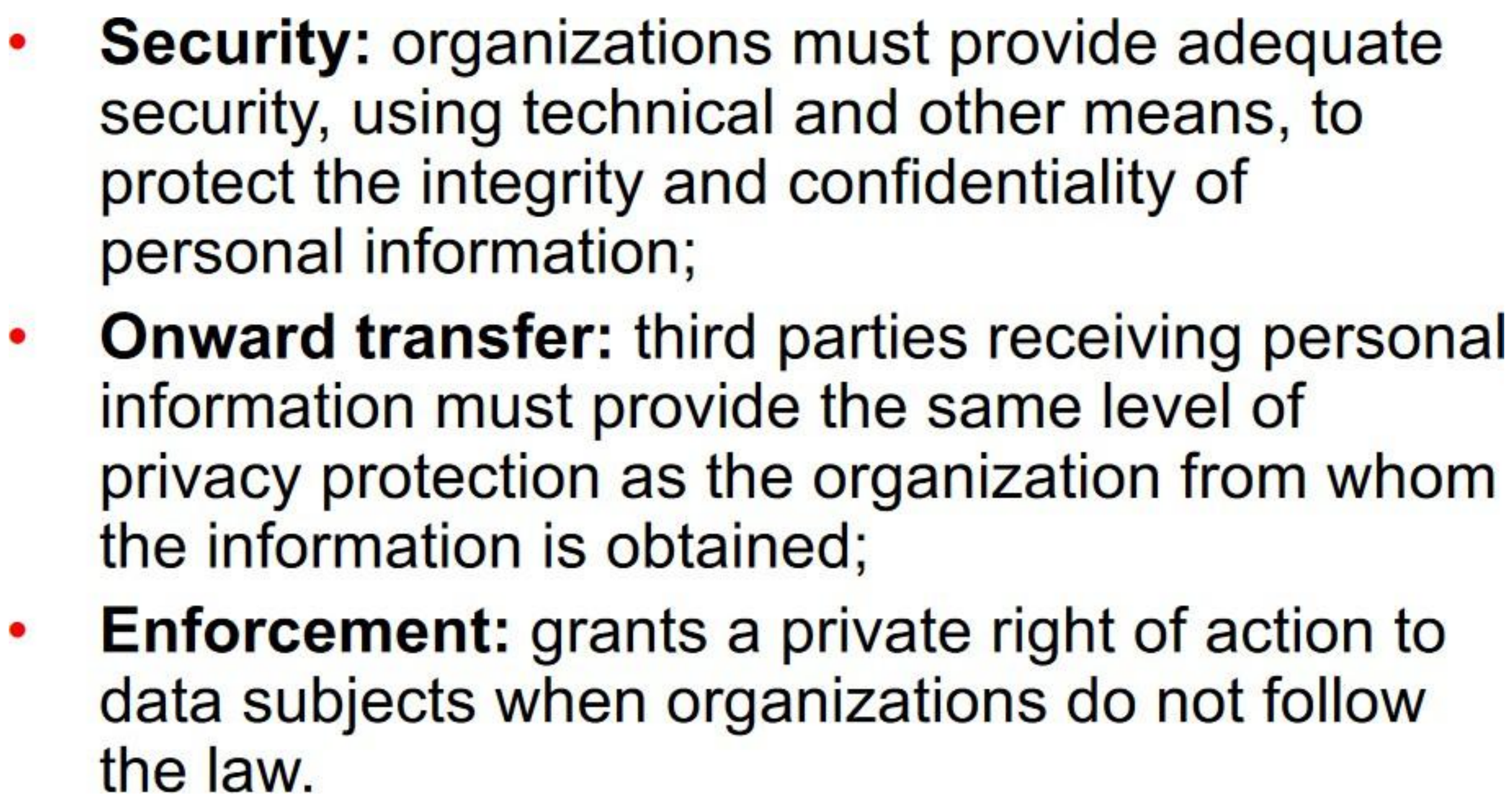
- **Notice:** organizations must notify individuals what personal information they are collecting, the uses of that information, and what choices the individual may have;
- **Consent:** individuals must be able to choose whether and how their personal information is used by, or disclosed to, third parties. They have the right not to have any sensitive information collected or used without express permission, including race, religion, health, union membership, beliefs, and sex life.

EU Privacy Law Principles



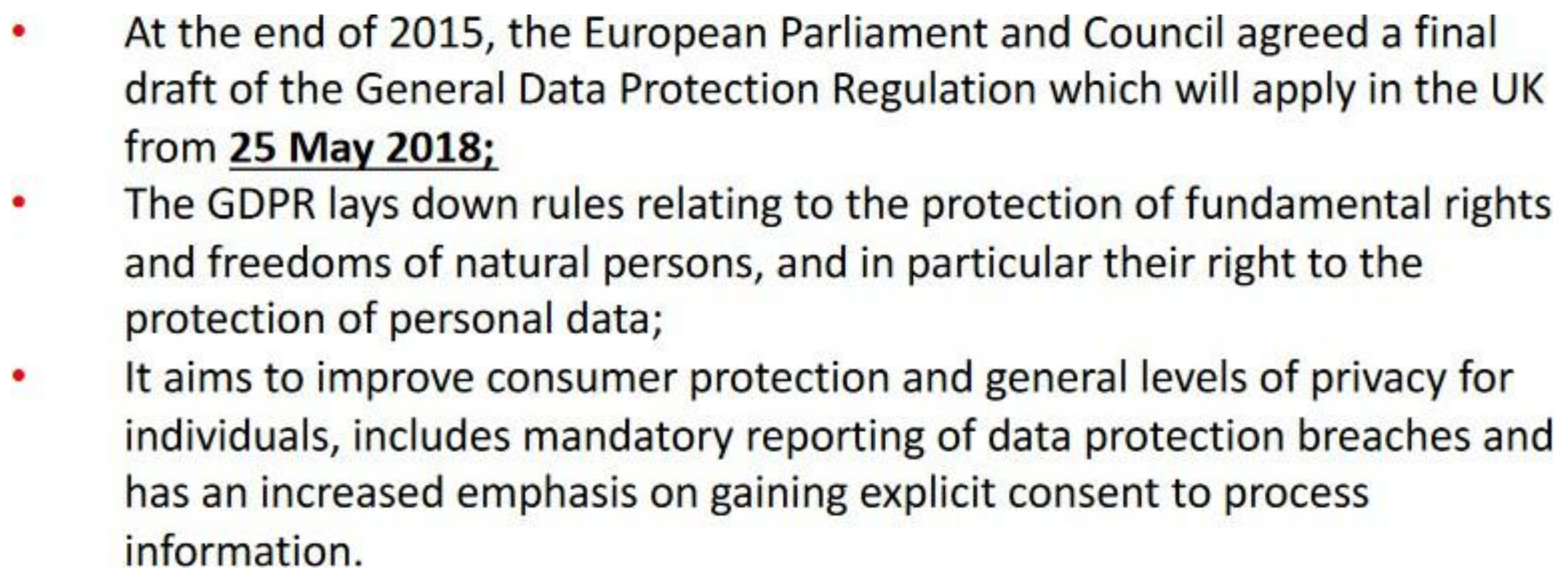
- **Consistency:** organizations may use personal information only in accordance with the terms of the notice given the data subject and the choices the make on its use;
- **Access:** individuals must have the right and ability to access their information and correct, modify, or delete any portion of it.

EU Privacy Law Principles

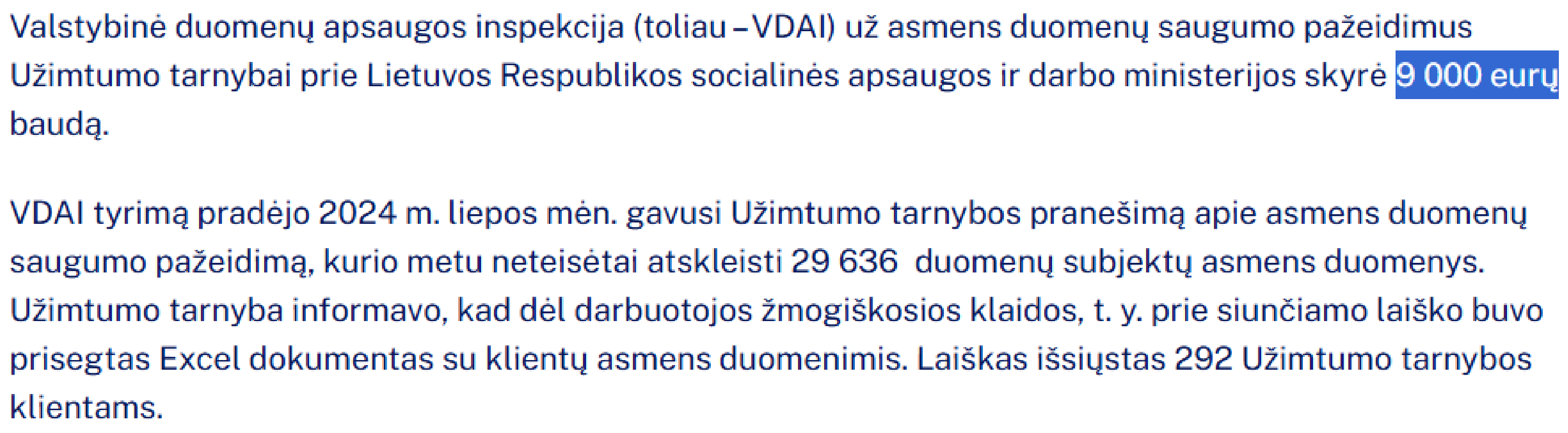


- **Security:** organizations must provide adequate security, using technical and other means, to protect the integrity and confidentiality of personal information;
- **Onward transfer:** third parties receiving personal information must provide the same level of privacy protection as the organization from whom the information is obtained;
- **Enforcement:** grants a private right of action to data subjects when organizations do not follow the law.

What is GDPR?

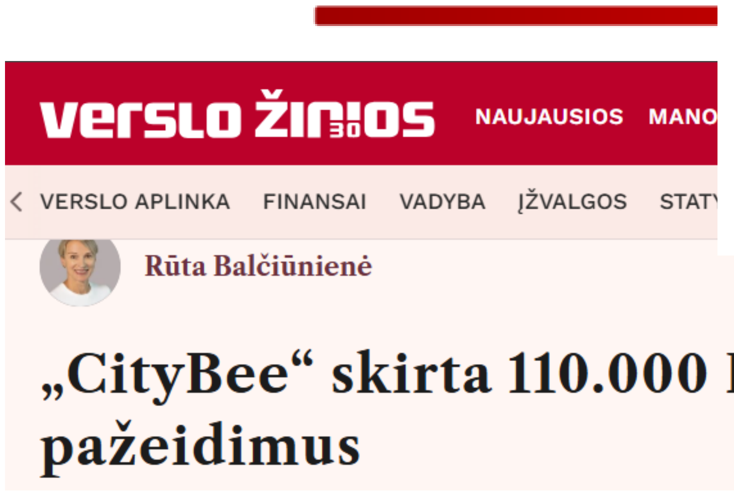


- At the end of 2015, the European Parliament and Council agreed a final draft of the General Data Protection Regulation which will apply in the UK from **25 May 2018;**
- The GDPR lays down rules relating to the protection of fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data;
- It aims to improve consumer protection and general levels of privacy for individuals, includes mandatory reporting of data protection breaches and has an increased emphasis on gaining explicit consent to process information.



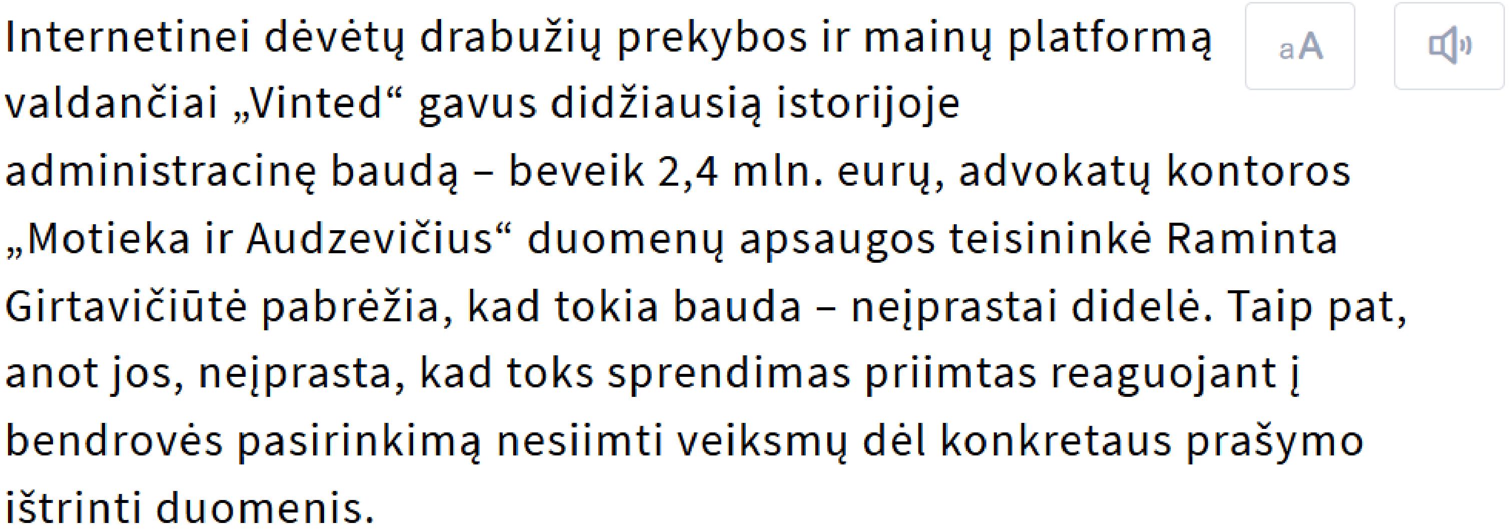
Valstybinė duomenų apsaugos inspekcija (toliau – VDAI) už asmens duomenų saugumo pažeidimus Užimtumo tarnybai prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos skyrė 9 000 eurų baudą.

VDAI tyrimą pradėjo 2024 m. liepos mėn. gavusi Užimtumo tarnybos pranešimą apie asmens duomenų saugumo pažeidimą, kurio metu neteisėtai atskleisti 29 636 duomenų subjektų asmens duomenys. Užimtumo tarnyba informavo, kad dėl darbuotojos žmogiškosios klaidos, t. y. prie siunčiamo laiško buvo prisegtas Excel dokumentas su klientų asmens duomenimis. Laiškas išsiųstas 292 Užimtumo tarnybos klientams.



Rūta Balčiūnienė

„CityBee“ skirta 110.000 Eur bauda už BDAR pažeidimus

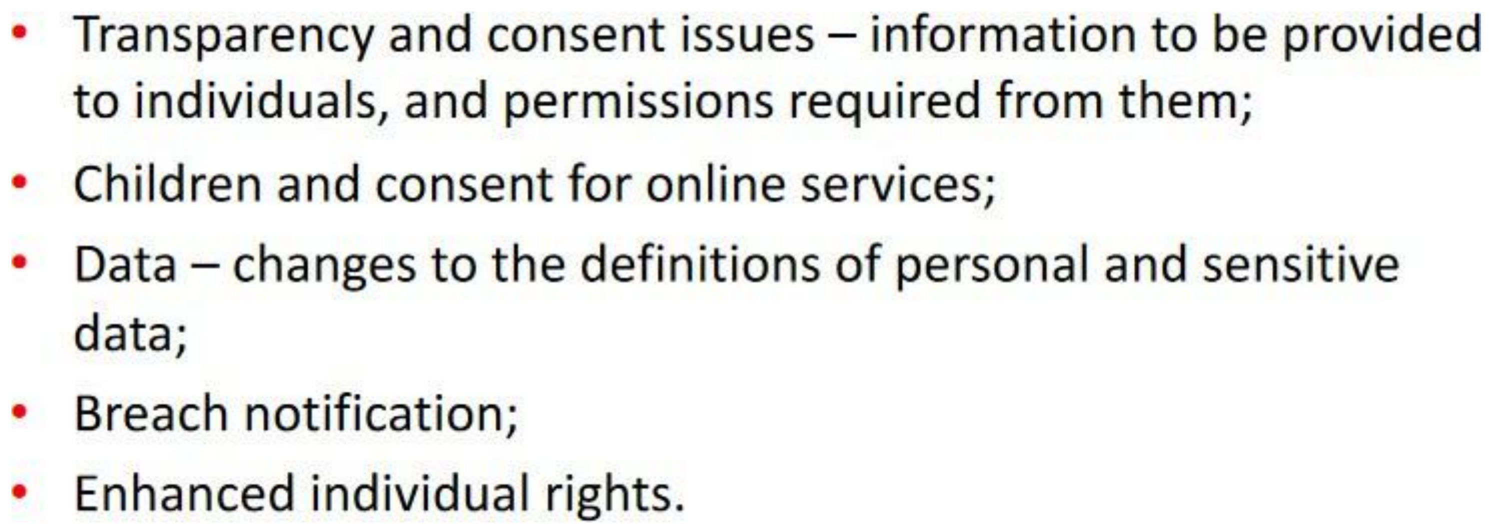


Internetinei dėvėtų drabužių prekybos ir mainų platformą valdančiai „Vinted“ gavus didžiausią istorijoje administracinę baudą – beveik 2,4 mln. eurų, advokatų kontoros „Motieka ir Audzevičius“ duomenų apsaugos teisininkė Raminta Girtavičiūtė pabrėžia, kad tokia bauda – neįprastai didelė. Taip pat, anot jos, neįprasta, kad toks sprendimas priimtas reaguojant į bendrovės pasirinkimą nesiimti veiksmų dėl konkretaus prašymo ištrinti duomenis.

Data Protection Bill

- The UK will also replace its current Data Protection Act (1998) in the next few months, incorporating the GDPR requirements. The Data Protection Bill is currently going through the relevant parliamentary processes (it has gone through the House of Lords and is currently in the House of Commons on its 2nd reading);
- The advice from the Information Commissioner's Office is that many of the GDPR's main concepts and principles are much the same as those in the current Act, and therefore if we are complying properly with the current law then most of our approach to compliance will remain valid under the GDPR and the new Bill, and will give us a starting point to build from.

The GDPR – new and changed concepts from Data Protection Act 1998



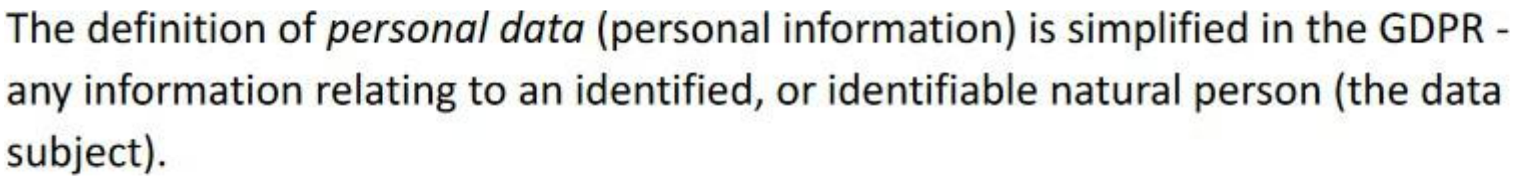
- Transparency and consent issues – information to be provided to individuals, and permissions required from them;
- Children and consent for online services;
- Data – changes to the definitions of personal and sensitive data;
- Breach notification;
- Enhanced individual rights.

Scope of the GDPR

Any / all information relating to an identified or identifiable individual e.g.

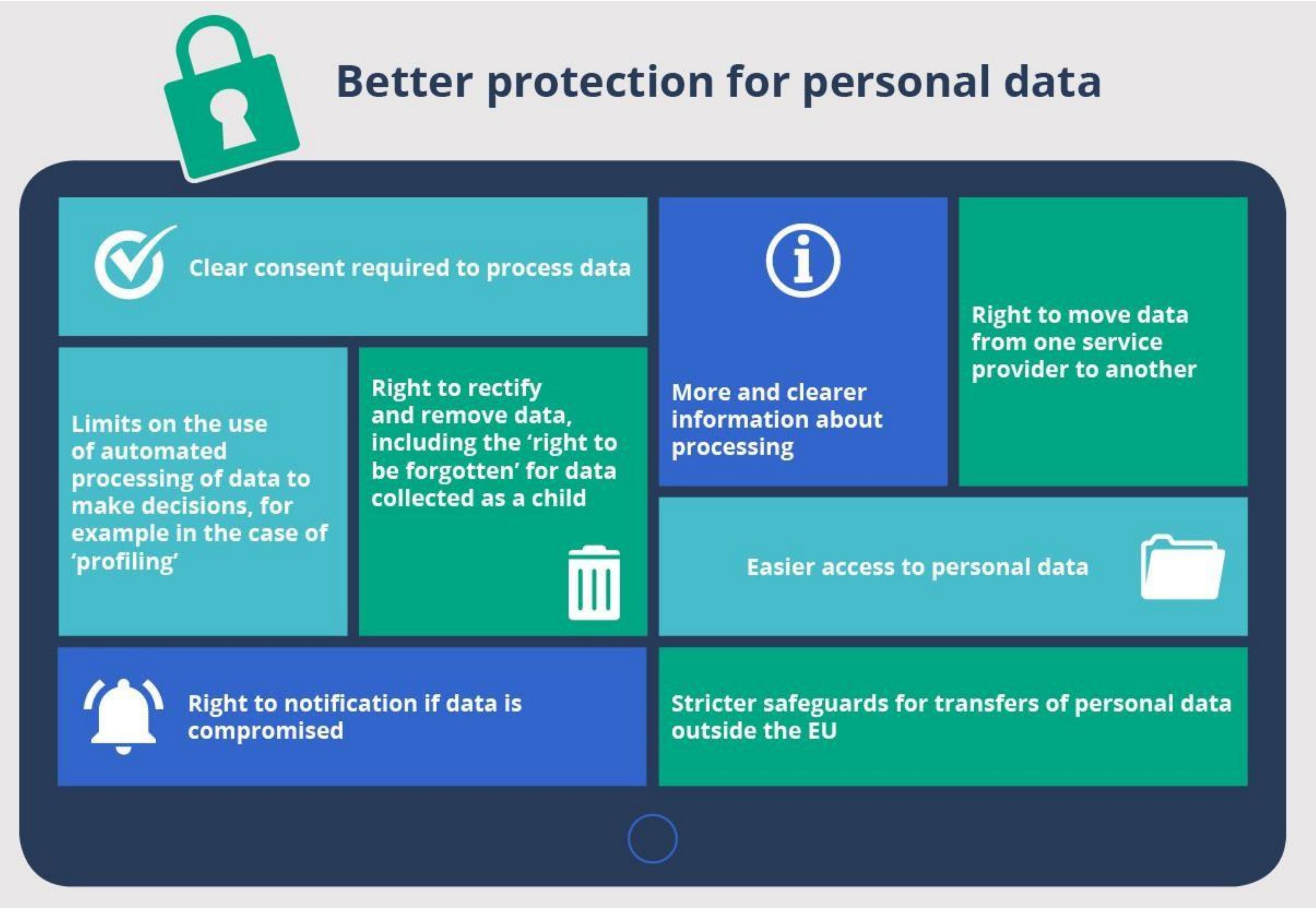
- Information held in manual form or printed out;
- Emails, databases, spreadsheets etc.;
- Photographs on web sites, marketing photographs, ID Cards and Passes;
- CCTV images (both central CCTV system and any localised systems / webcams);
- Web pages;
- Information which may be associated with online identifiers provided by devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers.

Definition of Personal Data



The definition of *personal data* (personal information) is simplified in the GDPR - any information relating to an identified, or identifiable natural person (the data subject).

Legitimate Grounds for Processing Personal Data



Better protection for personal data

Clear consent required to process data

Limits on the use of automated processing of data to make decisions, for example in the case of 'profiling'

Right to rectify and remove data, including the 'right to be forgotten' for data collected as a child

More and clearer information about processing

Right to move data from one service provider to another

Easier access to personal data

Right to notification if data is compromised

Stricter safeguards for transfers of personal data outside the EU

Legitimate Grounds for Processing Personal Data

More opportunities for business

- Level playing field for all EU and non-EU businesses offering goods and services to persons in the EU
- One set of rules for the whole EU
- Rules that allow businesses, especially SMEs, to get the most out of the Digital Single Market
- Risk-based approach, matching obligations of controllers to the level of risk of the processing