题目1：Fred的数据角色要求他维护系统安全计划，并确保系统用户和支持人员接受他们所需的有关安全实践和准用性的培训。Fred最可能在组织中担任什么角色？

Fred’s data role requires him to maintain system security plans and to ensure that system users and support staff get the training they need about security practices and acceptable use. What is the role that Fred is most likely to hold in the organization?

A：数据所有者

Data owner

B：系统所有者

System owner

C：用户

User

D：监管者

Custodian

答案:Fred的角色要求他维护系统安全计划，并确保系统用户和支持人员接受有关安全实践和准用性的培训。这些职责与系统所有者的角色最为吻合。系统所有者负责确保系统的安全性、可用性和完整性，并确保相关人员接受适当的培训。

因此，Fred最可能在组织中担任的角色是：

\*\*B：系统所有者\*\*

\*\*System owner\*\*

-------------------

题目2：Sally在传输模式下使用IPSec的ESP组件。她应该了解哪些关于传输模式的重要信息？

Sally is using IPsec’s ESP component in transport mode. What important information should she be aware of about transport mode?

A：传输模式提供整个IP数据包的完全加密

Transport mode provides full encryption of the entire IP packet.

B：传输模式添加一个新的未加密报头，以确保数据包到达其目的地

Transport mode adds a new, unencrypted header to ensure that packets reach their destination.

C：传输模式不加密数据包的头

Transport mode does not encrypt the header of the packet.

D：传输模式不提供加密，只有隧道模式提供加密

Transport mode provides no encryption; only tunnel mode provides encryption.

答案:在传输模式下使用IPSec的ESP（封装安全载荷）组件时，Sally应该了解以下重要信息：

C：传输模式不加密数据包的头

Transport mode does not encrypt the header of the packet.

解释：

- \*\*传输模式\*\*：在传输模式下，IPSec只加密IP数据包的\*\*有效载荷\*\*（即数据部分），而不加密IP头。这意味着IP头（包括源地址和目标地址）仍然是明文传输的。传输模式通常用于端到端的通信，例如在两个主机之间直接通信时使用。

- \*\*隧道模式\*\*：相比之下，隧道模式会加密整个IP数据包（包括IP头），并添加一个新的IP头。隧道模式通常用于在两个网络之间建立安全通道，例如在两个VPN网关之间通信时使用。

其他选项的解释：

- \*\*A\*\*：传输模式不提供整个IP数据包的完全加密，它只加密有效载荷部分。

- \*\*B\*\*：传输模式不会添加新的未加密报头，它只是保留原始的IP头。

- \*\*D\*\*：传输模式确实提供加密，但它只加密有效载荷部分，而不是整个数据包。

因此，正确答案是 \*\*C\*\*。

-------------------

题目3：以下哪一个不是软件能力成熟度模型（SW-CMM）的可重复阶段的关键过程？

Which one of the following is not an essential process area for the Repeatable phase of the Software Capability Maturity Model (SW-CMM)?

A：软件项目规划

Software Project Planning

B：软件质量管理

Software Quality Management

C：软件项目跟踪

Software Project Tracking

D：软件分包管理

Software Subcontract Management

答案:在软件能力成熟度模型（SW-CMM）中，可重复阶段（Repeatable Level）的关键过程包括：

A：软件项目规划（Software Project Planning）

C：软件项目跟踪（Software Project Tracking）

D：软件分包管理（Software Subcontract Management）

而选项 B：软件质量管理（Software Quality Management）并不是可重复阶段的关键过程。软件质量管理通常是在更高成熟度阶段（如已定义阶段或已管理阶段）中引入的。

因此，正确答案是：

\*\*B：软件质量管理（Software Quality Management）\*\*

-------------------

题目4：Ben希望自动提供关于其组织的风险暴露的预测信息，作为持续的组织风险管理计划的一部分。他应该怎么做？

Ben wants to provide predictive information about his organization’s risk exposure in an automated way as part of an ongoing organizational risk management plan. What should he use to do this?

A：KRI

KRIs

B：定量风险评估

Quantitative risk assessments

C：KPI

KPIs

D：渗透测试

Penetration tests

答案:题目4的正确答案是：

\*\*A：KRI (Key Risk Indicators) 关键风险指标\*\*

\*\*解释：\*\*

- \*\*KRI (Key Risk Indicators)\*\* 是关键风险指标，用于监控和预测组织可能面临的风险。它们可以帮助Ben自动提供关于组织风险暴露的预测信息，作为持续的风险管理计划的一部分。

- \*\*定量风险评估 (Quantitative risk assessments)\*\* 虽然也是风险管理的一部分，但它们通常用于评估特定风险的可能性和影响，而不是用于持续监控和预测。

- \*\*KPI (Key Performance Indicators)\*\* 是关键绩效指标，主要用于衡量组织的绩效，而不是风险。

- \*\*渗透测试 (Penetration tests)\*\* 是一种安全测试方法，用于评估系统的安全性，而不是用于预测风险暴露。

因此，\*\*KRI\*\* 是最适合用于自动提供关于组织风险暴露的预测信息的工具。

-------------------

题目5：在这里所示的图像中，系统B在三次TCP握手的步骤2处向系统A发送什么？

<div style="text-align:center"><img alt="" height="313" src="/file/100000/m/20210901/4ecbb83c8bcf47d3a1dcf47b9bb896be.png" width="609" /></div>

In the image shown here, what does system B send to system A at step 2 of the three-way TCP handshake?

<div style="text-align:center"><img alt="" height="313" src="/file/100000/m/20210901/bebc520ceb57447e8e7bda92d6ea2207.png" width="609" /></div>

A：SYN

SYN

B：ACK

ACK

C：FIN/ACK

FIN/ACK

D：SYN/ACK

SYN/ACK

答案:在三次TCP握手的步骤2中，系统B向系统A发送的是SYN/ACK。因此，正确答案是：

D：SYN/ACK

解释：

- 在三次TCP握手的步骤1中，系统A向系统B发送一个SYN（同步）包，请求建立连接。

- 在步骤2中，系统B收到SYN包后，会回复一个SYN/ACK（同步/确认）包，表示它已经收到了SYN包，并且同意建立连接。

- 在步骤3中，系统A再发送一个ACK（确认）包，确认连接已建立。

因此，步骤2中系统B发送的是SYN/ACK包。

-------------------

题目6：Chris在对远程目标执行侦查时发现目标网络的边界防火墙允许ping。通过ping来探测远程网络，Jim能够获得什么信息？

Chris is conducting reconnaissance on a remote target and discovers that pings are allowed through his target’s border firewall. What can he learn by using ping to probe the remote network?

A：哪些系统响应ping请求、网络拓扑的大致结构，以及可能存在的其他防火墙的位置

Which systems respond to ping, a rough network topology, and potentially the location of additional firewalls

B：目标防火墙后所有系统的列表

A list of all of the systems behind the target’s firewall

C：每个可以响应ping请求的系统的主机名和生存时间（TTL），以及防火墙允许通过的ICMP类型

The hostnames and time to live (TTL) for each pingable system, and the ICMP types allowed through the firewall

D：路由广播、请求响应，以及哪些主机可能具备限定攻击行为的安全配置

Router advertisements, echo request responses, and potentially which hosts are tarpitted

答案:正确答案是 \*\*A\*\*：哪些系统响应ping请求、网络拓扑的大致结构，以及可能存在的其他防火墙的位置。

### 解析：

通过使用ping（ICMP Echo请求）来探测远程网络，Chris可以获取以下信息：

1. \*\*哪些系统响应ping请求\*\*：

通过发送ping请求，Chris可以确定哪些主机或设备在目标网络中响应ICMP请求。这可以帮助他识别活跃的主机。

2. \*\*网络拓扑的大致结构\*\*：

通过分析ping的响应时间（TTL值）和路由路径，Chris可以推断出目标网络的大致拓扑结构。例如，TTL值的变化可以提示网络中可能存在多少跳（hop）。

3. \*\*可能存在的其他防火墙的位置\*\*：

如果某些ping请求被阻止或响应时间异常，Chris可以推测网络中可能存在其他防火墙或安全设备。

### 其他选项分析：

- \*\*B\*\*：ping无法提供目标防火墙后所有系统的完整列表，因为某些系统可能配置为不响应ping请求。

- \*\*C\*\*：虽然ping可以提供TTL值，但它无法直接提供主机名或ICMP类型的详细信息。

- \*\*D\*\*：ping主要用于检测主机是否在线，无法直接提供路由广播或安全配置的详细信息。

因此，\*\*A\*\*是最全面的正确答案。

-------------------

题目7：Jake正在对组织的身份和访问管理计划进行审查。在审查期间，他正在验证分配给每个用户的权限，并确保这些权限与符合业务需求。他正在审查该计划的哪些要素？

Jake is conducting a review of his organization&rsquo;s identity and access management program. During his review, he is verifying the privileges assigned to each user and ensuring that they match with business requirements. What element of the program is he reviewing?

A：身份

Identification

B：问责

Accountability

C：授权

Authorization

D：认证

Authentication

答案:Jake正在审查的是分配给每个用户的权限，并确保这些权限符合业务需求。这涉及到确定用户是否有权访问特定的资源或执行特定的操作，这是授权（Authorization）的核心内容。

因此，正确答案是：

C：授权

Authorization

-------------------

题目8：Faith正在查看使用了影子密码的/etc/passwd文件的系统配置。 当她检查文件中具有交互式登录权限用户这一行时，她希望在密码字段中应该看到什么？

Faith is looking at the /etc/passwd file on a system configured to use shadowed passwords. When she examines a line in the file for a user with interactive login permissions, what should she expect to see in the password field?

A：明文密码

Plaintext password

B：散列密码

Hashed password

C：x

x

D：\*

\*

答案:在使用了影子密码（shadowed passwords）的系统上，`/etc/passwd` 文件中的密码字段通常不会包含实际的密码信息。相反，密码信息会被存储在 `/etc/shadow` 文件中，以提高安全性。

因此，当 Faith 查看 `/etc/passwd` 文件中具有交互式登录权限用户的行时，她应该在密码字段中看到的是 `x`。这个 `x` 表示密码已经被转移到 `/etc/shadow` 文件中。

所以，正确答案是：

\*\*C：x\*\*

-------------------

题目9：Berta正在分析她的一台服务器上的Windows防火墙日志，看到了图中所示条目。这些条目表示了什么类型的攻击？

Berta is analyzing the logs of the Windows Firewall on one of her servers and comes across the entries shown in this figure. What type of attack do these entries indicate?

<div style="text-align:center"><img alt="" height="133" src="/file/100000/m/20210901/c548221d5dd149418574ce69c164ac12.png" width="625" /></div>

A：SQL注入

SQL injection

B：端口扫描

Port scan

C：Teardrop

Teardrop

D：Land

Land

答案:根据题目描述，Berta在分析Windows防火墙日志时看到的条目可能与某种网络攻击有关。虽然题目中没有提供具体的日志内容，但根据选项可以推测可能的攻击类型。

选项分析：

- \*\*A: SQL注入\*\* - SQL注入通常是通过Web应用程序进行的攻击，防火墙日志中不太可能直接记录这种攻击，除非是Web服务器防火墙。

- \*\*B: 端口扫描\*\* - 端口扫描是一种常见的网络攻击，攻击者通过扫描目标服务器的开放端口来寻找潜在的漏洞。防火墙日志中通常会记录大量的连接尝试，这可能表明正在进行端口扫描。

- \*\*C: Teardrop\*\* - Teardrop是一种利用IP分片漏洞的攻击，通常会导致目标系统崩溃。这种攻击在防火墙日志中可能会有特定的记录，但不如端口扫描常见。

- \*\*D: Land\*\* - Land攻击是一种利用伪造的IP地址和端口号来使目标系统陷入循环的攻击。这种攻击在防火墙日志中也可能有特定的记录，但同样不如端口扫描常见。

根据常见的防火墙日志分析，\*\*端口扫描\*\*是最有可能的攻击类型，因为防火墙日志中通常会记录大量的连接尝试，这些尝试可能是攻击者在寻找开放的端口。

\*\*正确答案：B：端口扫描 (Port scan)\*\*

-------------------

题目10：Danielle正在测试税务软件，测试过程中要求她输入各种实际税务表格，以验证软件生成正确的答案。Danielle正在执行什么类型的测试？

Danielle is testing tax software, and part of her testing process requires her to input a variety of actual tax forms to verify that the software produces the right answers. What type of testing is Danielle performing?

A：用例测试

Use case testing

B：动态测试

Dynamic testing

C：Fuzzing

Fuzzing

D：误用测试

Misuse testing

答案:Danielle正在执行的测试类型是 \*\*用例测试（Use case testing）\*\*。

用例测试是一种基于用户实际使用场景的测试方法，目的是验证软件在特定使用情境下是否能够正确工作。在这个例子中，Danielle通过输入各种实际的税务表格来验证软件是否能够正确生成结果，这正是用例测试的典型应用场景。

因此，正确答案是：

\*\*A：用例测试（Use case testing）\*\*

-------------------

题目11：Cassandra在一家机构工作了10年，现在是她第4个岗位，她是会计部的一名经理。假设该机构没有严格的账号维护习惯，那么在账户审查中可能出现下列哪类问题？

After 10 years working in her organization, Cassandra is moving into her fourth role, this time as a manager in the accounting department. What issue is likely to show up during an account review if her organization does not have strong account maintenance practices?

A：最小特权问题

An issue with least privilege

B：特权蠕变

Privilege creep

C：账号蠕变

Account creep

D：账号终止

Account termination

答案:在Cassandra的情况下，如果她的机构没有严格的账号维护习惯，那么在账户审查中最可能出现的问题是 \*\*B：特权蠕变\*\*（Privilege creep）。

\*\*特权蠕变\*\*指的是员工在组织内多次调动岗位后，逐渐积累过多的权限和访问权。由于Cassandra已经在机构工作了10年，并且现在是她的第4个岗位，她可能在每个岗位上都获得了新的权限，但旧的权限可能没有被及时撤销。这会导致她拥有超出当前岗位所需的权限，增加了安全风险。

其他选项的解释：

- \*\*A：最小特权问题\*\*（Least privilege）是指员工只应拥有完成工作所需的最低权限，但这与题目描述的情况不直接相关。

- \*\*C：账号蠕变\*\*（Account creep）通常指系统中存在大量未使用的或过期的账号，这与Cassandra的情况不完全吻合。

- \*\*D：账号终止\*\*（Account termination）是指员工离职后账号未被及时关闭，这也不是题目描述的重点。

因此，最合适的答案是 \*\*B：特权蠕变\*\*。

-------------------

题目12：IP 地址（如10.10.10.10和172.19.24.21）都是什么类型的IP地址例子？

IP addresses like 10.10.10.10 and 172.19.24.21 are both examples of what type of IP address?

A：公共IP 地址

Public IP addresses

B：禁止的IP 地址

Prohibited IP addresses

C：私有的IP 地址

Private IP addresses

D：B 类IP 范围

Class B IP ranges

答案:C：私有的IP 地址

Private IP addresses

解释：10.10.10.10 和 172.19.24.21 都是私有IP地址的例子。私有IP地址用于内部网络，不会在公共互联网上路由。10.0.0.0 到 10.255.255.255 是A类私有地址范围，172.16.0.0 到 172.31.255.255 是B类私有地址范围。因此，10.10.10.10 属于A类私有地址，172.19.24.21 属于B类私有地址。

-------------------

题目13：Ben正在审查其网站使用的密码恢复机制，并发现该方法通过使用安全问题来作为认知身份认证。这种方法的主要问题是什么？

Ben is reviewing the password recovery mechanism used by his website and discovers that the approach uses cognitive authentication through the use of security questions. What is the major issue with this approach?

A：它阻止使用令牌

It prevents the use of tokens.

B：问题的答案也许在互联网上很容易找到

The question’s answer may be easy to find on the internet.

C：认知密码需要用户思考来回答问题，并不是所有用户都能够知道所提出的问题

Cognitive passwords require users to think to answer the question, and not all users may be able to solve the problems presented.

D：认知密码不支持长密码

Cognitive passwords don’t support long passwords.

答案:题目13的正确答案是：

\*\*B：问题的答案也许在互联网上很容易找到\*\*

\*\*The question's answer may be easy to find on the internet.\*\*

### 解析：

使用安全问题作为认知身份认证的主要问题是，这些问题的答案通常很容易被猜测或通过互联网搜索找到。例如，常见的安全问题包括“你母亲的娘家姓是什么？”或“你出生在哪里？”，这些信息可能已经在社交媒体或其他公开渠道上被泄露。因此，攻击者可以通过简单的调查或社交工程手段获取这些信息，从而绕过密码恢复机制。

其他选项的解释：

- \*\*A：它阻止使用令牌\*\*

安全问题并不直接阻止使用令牌，两者可以共存，但安全问题本身存在安全隐患。

- \*\*C：认知密码需要用户思考来回答问题，并不是所有用户都能够知道所提出的问题\*\*

虽然认知密码需要用户思考，但这并不是主要问题。主要问题是答案容易被猜测或泄露。

- \*\*D：认知密码不支持长密码\*\*

认知密码与密码长度无关，这是一个无关的选项。

因此，\*\*B\*\* 是最合适的答案。

-------------------

题目14：Megan需要对调查中的一个硬盘进行取证拷贝。下列哪个工具最适用于这项任务？

Megan needs to create a forensic copy of a hard drive that will be used in an investigation. Which of the following tools is best suited to her work?

A：Xcopy

Xcopy

B：dd

dd

C：DBAN

DBAN

D：ImageMagik

ImageMagik

答案:在数字取证中，创建一个硬盘的取证拷贝（也称为镜像）是一个关键步骤。这个过程需要确保数据的完整性和准确性。以下是每个选项的简要分析：

A. \*\*Xcopy\*\*：这是一个Windows命令行工具，用于复制文件和目录。它不适合用于创建硬盘的取证拷贝，因为它无法处理硬盘的底层数据结构，也无法确保数据的完整性。

B. \*\*dd\*\*：这是一个Unix/Linux命令行工具，用于复制和转换文件。在数字取证中，`dd` 是一个非常常用的工具，因为它可以创建硬盘的逐位拷贝（bit-by-bit copy），并且可以确保数据的完整性。它还可以处理硬盘的底层数据结构，因此非常适合用于取证拷贝。

C. \*\*DBAN\*\*：这是一个用于安全擦除硬盘数据的工具。它不适合用于创建取证拷贝，因为它会销毁数据，而不是复制数据。

D. \*\*ImageMagik\*\*：这是一个用于图像处理的工具，主要用于处理图像文件。它不适合用于创建硬盘的取证拷贝。

因此，最适用于Megan任务的工具是 \*\*B. dd\*\*。

-------------------

题目15：Kay正为组织选择一种应用程序管理方法。员工需要灵活地在系统上安装软件，但Kay希望防止他们安装某些非法的软件包。她应该使用什么类型的方法？

Kay is selecting an application management approach for her organization. Employees need the flexibility to install software on their systems, but Kay wants to prevent them from installing certain prohibited packages. What type of approach should she use?

A：反病毒

Antivirus

B：白名单

Whitelist

C：黑名单

Blacklist

D：启发式

Heuristic

答案:Kay 面临的需求是允许员工在系统上安装软件，但同时要防止他们安装某些非法的软件包。这种情况下，最合适的方法是使用 \*\*黑名单（Blacklist）\*\*。

\*\*黑名单\*\* 是一种管理方法，它允许用户安装任何软件，除了那些明确列在禁止列表中的软件。这种方法提供了灵活性，同时也能有效阻止特定的非法或不受欢迎的软件包被安装。

其他选项的解释：

- \*\*反病毒（Antivirus）\*\*：主要用于检测和移除恶意软件，而不是管理软件的安装。

- \*\*白名单（Whitelist）\*\*：只允许安装列在白名单中的软件，其他软件一律禁止。这种方法过于严格，不符合员工需要灵活安装软件的需求。

- \*\*启发式（Heuristic）\*\*：通常用于检测未知的恶意软件，而不是管理软件的安装。

因此，\*\*C：黑名单（Blacklist）\*\* 是最合适的选项。

-------------------

题目16：Donna是一家位于美国的医疗保健提供商的安全管理员，正在审查他们的支付处理系统。该系统包含与过去、现在或将来为个人提供医疗保健付款相关的数据。这些信息根据HIPAA将如何进行分类？

Donna is a security administrator for a healthcare provider located in the United States and is reviewing their payment processing system. It contains data relating to the past, present, or future payment for the provision of healthcare to an individual. How would this information be classified under HIPAA?

A：PCI

PCI

B：个人计费数据

Personal billing data

C：PHI

PHI

D：个人身份信息(PII)

Personally identifiable information (PII)

答案:根据HIPAA（健康保险可携性和责任法案），与个人的医疗保健付款相关的数据通常被视为受保护的健康信息（Protected Health Information, PHI）。PHI 包括任何可以识别个人身份并与他们的健康状况、医疗保健服务或支付相关的信息。

因此，Donna 正在审查的支付处理系统中的数据应被分类为 PHI。

正确答案是：

C：PHI

-------------------

题目17：Harold的公司有严格的密码策略，要求长度至少为12个字符，并同时使用字母、数字和符号。攻击者破解Harold组织中的密码最有效方法是什么？

Harold’s company has a strong password policy that requires a minimum length of 12 characters and the use of both alphanumeric characters and symbols. What technique would be the most effective way for an attacker to compromise passwords in Harold’s organization?

A：蛮力攻击

Brute-force attack

B：字典攻击

Dictionary attack

C：彩虹表攻击

Rainbow table attack

D：社会工程学攻击

Social engineering attack

答案:在Harold的公司中，密码策略要求密码长度至少为12个字符，并且必须包含字母、数字和符号。这种策略使得密码的复杂性较高，从而增加了破解的难度。

- \*\*蛮力攻击（Brute-force attack）\*\*：这种方法会尝试所有可能的字符组合，直到找到正确的密码。对于长度为12个字符且包含字母、数字和符号的密码，蛮力攻击的计算量非常大，几乎不可行。

- \*\*字典攻击（Dictionary attack）\*\*：这种方法使用常见密码和单词列表进行尝试。由于密码策略要求使用字母、数字和符号，并且长度较长，字典攻击的成功率会大大降低。

- \*\*彩虹表攻击（Rainbow table attack）\*\*：这种方法使用预先计算的哈希表来破解密码。然而，如果密码策略要求使用盐值（salt）来增加哈希的复杂性，彩虹表攻击的效果会大打折扣。

- \*\*社会工程学攻击（Social engineering attack）\*\*：这种方法通过欺骗或操纵用户来获取密码。由于它不依赖于密码的复杂性，而是依赖于人的弱点，因此在这种情况下，社会工程学攻击可能是最有效的方法。

因此，\*\*D：社会工程学攻击（Social engineering attack）\*\* 是最有效的破解方法。

-------------------

题目18：James在出差中被人持刀逼迫登录笔记本电脑，这种场景叫做？

While traveling, James is held at knifepoint and forced to log into his laptop. What is this called?

A：胁迫

Duress

B：反社会工程

Antisocial engineering

C：危难

Distress

D：尖刀劫持

Knifepoint hacking

答案:这个场景描述的是James在出差时被人持刀逼迫登录笔记本电脑，这是一种胁迫行为。胁迫（Duress）是指通过威胁或使用暴力迫使某人做某事。因此，正确答案是：

A：胁迫

Duress

其他选项的解释如下：

- 反社会工程（Antisocial engineering）通常指的是利用社会工程学手段进行恶意行为，但这个词并不常见，也不是描述这种情况的准确术语。

- 危难（Distress）通常指的是心理或情感上的痛苦，而不是被胁迫的情况。

- 尖刀劫持（Knifepoint hacking）并不是一个标准的术语，虽然它描述了用刀威胁的情况，但不是一个正式的安全术语。

-------------------

题目19：Cameron负责备份公司的主文件服务器。他配置了一个备份计划，该计划在每个星期一晚上9:00执行完全备份，同时在一周的其他天执行增量备份。在星期三的备份中将复制多少个文件？

<div style="text-align:center"><img alt="" height="132" src="/file/100000/m/20210901/8df0b8bc9b33461883cff40db5798ada.png" width="132" /></div>

Cameron is responsible for backing up his company’s primary file server. He configured a backup schedule that performs full backups every Monday evening at 9 p.m. and incremental backups on other days of the week at that same time. How many files will be copied in Wednesday’s backup?

<div style="text-align:center"><img alt="" height="245" src="/file/100000/m/20210901/b362387b8dc44466b30d47582ddde32a.png" width="270" /></div>

A：1

1

B：2

2

C：5

5

D：6

6

答案:在这个备份计划中，Cameron在每个星期一晚上9:00执行完全备份，这意味着在星期一备份时，所有文件都会被复制。然后，在一周的其他天（星期二到星期日）执行增量备份，增量备份只会复制自上次备份以来发生变化的文件。

因此，在星期三的备份中，只会复制自星期二备份以来发生变化的文件。假设在星期二和星期三之间只有1个文件发生了变化，那么在星期三的备份中将复制1个文件。

所以，正确答案是：

A：1

-------------------

题目20：Susan使用span端口来监控其网站的流量，并使用监控工具来实时识别性能问题。她执行什么类型的监控？

Susan uses a span port to monitor traffic to her production website and uses a monitoring tool to identify performance issues in real time. What type of monitoring is she conducting?

A：被动监控

Passive monitoring

B：主动监控

Active monitoring

C：合成监控

Synthetic monitoring

D：基于签名的监控

Signature-based monitoring

答案:Susan 使用 span 端口来监控其生产网站的流量，并使用监控工具实时识别性能问题。她执行的是 \*\*被动监控\*\*。

\*\*解释：\*\*

- \*\*被动监控（Passive monitoring）\*\* 是指通过监听网络流量或系统活动来收集数据，而不主动向系统发送请求或注入流量。Susan 使用 span 端口来捕获网络流量，这种方式不会干扰正常的网络通信，因此属于被动监控。

- \*\*主动监控（Active monitoring）\*\* 是指通过主动向系统发送请求（如 ping、HTTP 请求等）来测试系统的响应时间和可用性。

- \*\*合成监控（Synthetic monitoring）\*\* 是一种主动监控的形式，通过模拟用户行为来测试系统的性能。

- \*\*基于签名的监控（Signature-based monitoring）\*\* 通常用于安全领域，通过匹配已知的攻击模式或恶意行为来检测威胁。

因此，正确答案是：

\*\*A：被动监控\*\*

\*\*Passive monitoring\*\*

-------------------

题目21：以下哪种类型的攻击中，攻击者会设法将自己插入到用户和合法网站之间的连接中？

In what type of attack do attackers manage to insert themselves into a connection between a user and a legitimate website?

A：中间人攻击

Man-in-the-middle attack

B：Fraggle攻击

Fraggle attack

C：战争驾驶攻击

Wardriving attack

D：中间相遇攻击

Meet-in-the-middle attack

答案:正确答案是：

A：中间人攻击

Man-in-the-middle attack

中间人攻击（Man-in-the-middle attack）是一种网络攻击方式，攻击者通过某种手段将自己插入到用户和合法网站之间的通信中，从而窃取或篡改传输的数据。这种攻击通常发生在不安全的网络环境中，如公共Wi-Fi。攻击者可以截获用户的登录信息、密码、信用卡信息等敏感数据。

其他选项的解释：

- B：Fraggle攻击是一种分布式拒绝服务攻击（DDoS），通过向目标系统发送大量UDP数据包来消耗带宽和资源。

- C：战争驾驶攻击（Wardriving attack）是指攻击者通过移动设备搜索并定位不安全的无线网络。

- D：中间相遇攻击（Meet-in-the-middle attack）是一种密码学攻击，通常用于破解加密算法。

因此，中间人攻击是唯一符合题目描述的选项。

-------------------

题目22：以下哪一项将被视为基础设施即服务的云计算的例子？

Which one of the following would be considered an example of infrastructure as a service cloud computing?

A：由供应商管理并通过网络传输数据的工资系统

Payroll system managed by a vendor and delivered over the web

B：由供应商管理的运行客户代码的应用程序平台

Application platform managed by a vendor that runs customer code

C：由客户在供应商管理的虚拟化平台上配置的服务器

Servers provisioned by customers on a vendor-managed virtualization platform

D：供应商提供的基于网络的电子邮件服务

Web-based email service provided by a vendor

答案:正确答案是 \*\*C\*\*：由客户在供应商管理的虚拟化平台上配置的服务器

\*\*Servers provisioned by customers on a vendor-managed virtualization platform\*\*

### 解析：

\*\*基础设施即服务（Infrastructure as a Service, IaaS）\*\* 是云计算的一种模式，供应商提供虚拟化的计算资源（如服务器、存储、网络等），客户可以根据需求配置和管理这些资源。选项C描述的是客户在供应商管理的虚拟化平台上配置服务器，这正是IaaS的核心特征。

其他选项的解释：

- \*\*A\*\*：工资系统由供应商管理并通过网络传输数据，这更像是\*\*软件即服务（SaaS）\*\*。

- \*\*B\*\*：由供应商管理的应用程序平台运行客户代码，这属于\*\*平台即服务（PaaS）\*\*。

- \*\*D\*\*：基于网络的电子邮件服务是典型的\*\*软件即服务（SaaS）\*\*。

因此，\*\*C\*\* 是正确答案。

-------------------

题目23-1：参考以下场景，回答3个问题。

Darcy是Roscommon农产品公司的信息安全风险分析师。她目前正在试图决定公司是否应为其主数据中心购买升级的灭火系统。数据中心设施的重置成本为200万美元。

与精算师、数据中心经理和消防专家协商后，Darcy了解到，如果发生一般火灾，那么可能需要更换建筑物内的所有设备，但不会导致重大的结构性损坏。他们一起估计，从火灾中恢复将需要75万美元。他们还确定，该公司每50年会发生一次这样的火灾。

For questions , please refer to the following scenario:

Darcy is an information security risk analyst for Roscommon Agricultural Products. She is currently trying to decide whether the company should purchase an upgraded fire suppression system for their primary data center. The data center facility has a replacement cost of $2 million.

After consulting with actuaries, data center managers, and fire subject-matter experts, Darcy determined that a typical fire would likely require the replacement of all equipment inside the building but not cause significant structural damage. Together, they estimated that recovering from the fire would cost $750,000. They also determined that the company can expect a fire of this magnitude once every 50 years.

根据上述信息，火灾对Roscommon农产品数据中心的影响的暴露因子是多少？

Based on the information in this scenario, what is the exposure factor for the effect of a fire on the Roscommon Agricultural Products data center?

A：7.5%

7.5 percent

B：15.0%

15.0 percent

C：27.5%

27.5 percent

D：37.5%

37.5 percent

答案:暴露因子（Exposure Factor, EF）是指特定风险事件发生时，资产可能遭受的损失比例。在这个场景中，火灾导致的恢复成本是75万美元，而数据中心设施的重置成本是200万美元。

暴露因子的计算公式是：

\[ \text{暴露因子} = \frac{\text{恢复成本}}{\text{重置成本}} \]

将给定的数值代入公式：

\[ \text{暴露因子} = \frac{750,000}{2,000,000} = 0.375 \]

将0.375转换为百分比：

\[ 0.375 \times 100 = 37.5\% \]

因此，火灾对Roscommon农产品数据中心的影响的暴露因子是37.5%。

正确答案是：

D：37.5%

37.5 percent

-------------------

题目23-1：参考以下场景，回答3个问题。

Darcy是Roscommon农产品公司的信息安全风险分析师。她目前正在试图决定公司是否应为其主数据中心购买升级的灭火系统。数据中心设施的重置成本为200万美元。

与精算师、数据中心经理和消防专家协商后，Darcy了解到，如果发生一般火灾，那么可能需要更换建筑物内的所有设备，但不会导致重大的结构性损坏。他们一起估计，从火灾中恢复将需要75万美元。他们还确定，该公司每50年会发生一次这样的火灾。

For questions , please refer to the following scenario:

Darcy is an information security risk analyst for Roscommon Agricultural Products. She is currently trying to decide whether the company should purchase an upgraded fire suppression system for their primary data center. The data center facility has a replacement cost of $2 million.

After consulting with actuaries, data center managers, and fire subject-matter experts, Darcy determined that a typical fire would likely require the replacement of all equipment inside the building but not cause significant structural damage. Together, they estimated that recovering from the fire would cost $750,000. They also determined that the company can expect a fire of this magnitude once every 50 years.

根据上述信息，Roscommon农产品数据中心的火灾年发生率是多少？

Based on the information in this scenario, what is the annualized rate of occurrence for a fire at the Roscommon Agricultural Products data center?

A：0.002

0.002

B：0.005

0.005

C：0.02

0.02

D：0.05

0.05

答案:要计算Roscommon农产品数据中心的火灾年发生率，我们需要使用以下公式：

\[ \text{年发生率} = \frac{1}{\text{事件发生的平均间隔时间}} \]

根据题目描述，火灾发生的平均间隔时间是50年。因此：

\[ \text{年发生率} = \frac{1}{50} = 0.02 \]

所以，正确答案是：

C：0.02

-------------------

题目23-1：参考以下场景，回答3个问题。

Darcy是Roscommon农产品公司的信息安全风险分析师。她目前正在试图决定公司是否应为其主数据中心购买升级的灭火系统。数据中心设施的重置成本为200万美元。

与精算师、数据中心经理和消防专家协商后，Darcy了解到，如果发生一般火灾，那么可能需要更换建筑物内的所有设备，但不会导致重大的结构性损坏。他们一起估计，从火灾中恢复将需要75万美元。他们还确定，该公司每50年会发生一次这样的火灾。

For questions , please refer to the following scenario:

Darcy is an information security risk analyst for Roscommon Agricultural Products. She is currently trying to decide whether the company should purchase an upgraded fire suppression system for their primary data center. The data center facility has a replacement cost of $2 million.

After consulting with actuaries, data center managers, and fire subject-matter experts, Darcy determined that a typical fire would likely require the replacement of all equipment inside the building but not cause significant structural damage. Together, they estimated that recovering from the fire would cost $750,000. They also determined that the company can expect a fire of this magnitude once every 50 years.

根据上述信息，Roscommon农产品数据中心的年度损失预期值是多少？

Based on the information in this scenario, what is the annualized loss expectancy for a fire at the Roscommon Agricultural Products data center?

A：15 000 美元

$15,000

B：25 000 美元

$25,000

C：75 000 美元

$75,000

D：750 000 美元

$750,000

答案:要计算年度损失预期值（Annualized Loss Expectancy, ALE），我们需要使用以下公式：

\[ \text{ALE} = \text{单次损失} \times \text{年度发生频率} \]

根据题目信息：

- 单次损失为 750,000 美元

- 每 50 年发生一次火灾，因此年度发生频率为 \( \frac{1}{50} = 0.02 \)

将这些值代入公式：

\[ \text{ALE} = 750,000 \times 0.02 = 15,000 \]

因此，Roscommon农产品数据中心的年度损失预期值是 \*\*15,000 美元\*\*。

正确答案是 \*\*A：15,000 美元\*\*。

-------------------

题目24：以下哪种技术使用统计方法从大池中选择少量日志记录进行进一步分析，目标是选择一组代表整个池的记录？

Which one of the following techniques uses statistical methods to select a small number of log records from a large pool for further analysis with the goal of choosing a set of records that is representative of the entire pool?

A：剪裁

Clipping

B：随机化

Randomization

C：抽样

Sampling

D：选择

Selection

答案:正确答案是 C：抽样 (Sampling)。

抽样是一种统计方法，通过从大量数据中选择一小部分记录来进行分析。抽样的目标是确保所选的记录能够代表整个数据集的特征。这种方法在数据分析和研究中非常常见，因为它可以显著减少处理的数据量，同时仍然能够提供对整体数据的准确估计。

其他选项的解释：

- A：剪裁 (Clipping) 通常指的是去除数据中的异常值或极端值，而不是选择代表性样本。

- B：随机化 (Randomization) 是一种确保数据选择过程无偏的方法，但它本身并不直接涉及选择代表性样本。

- D：选择 (Selection) 是一个更广泛的术语，可能包括多种选择方法，但不特指统计抽样。

-------------------

题目25：为防止API被滥用，Mike需要确保能够跟踪使用他的业务API的第三方用户。他需要实施下列哪项以达到目的？

Mike wants to ensure that third-party users of his service’s API can be tracked to prevent abuse of the API. What should he implement to help with this?

A：Session IDs

Session IDs

B：API防火墙

An API firewall

C：API密钥

API keys

D：API缓冲区

An API buffer

答案:为了防止API被滥用，Mike需要确保能够跟踪使用他的业务API的第三方用户。为了实现这一目标，最合适的措施是实施 \*\*API密钥（API keys）\*\*。

\*\*API密钥\*\* 是一种用于识别和验证API用户的机制。每个第三方用户在使用API时都需要提供一个唯一的API密钥，这样Mike就可以通过这个密钥来跟踪每个用户的使用情况，识别潜在的滥用行为，并采取相应的措施。

其他选项的解释如下：

- \*\*A: Session IDs\*\*：Session IDs 通常用于在用户会话期间保持用户的身份验证状态，但它们不适合用于跟踪第三方API用户。

- \*\*B: API防火墙\*\*：API防火墙可以用于保护API免受恶意攻击，但它本身并不能直接用于跟踪用户。

- \*\*D: API缓冲区\*\*：API缓冲区通常用于缓存API响应以提高性能，与跟踪用户无关。

因此，\*\*C: API密钥\*\* 是最合适的选项。

-------------------

题目26：Fran是一个网络开发人员，为一家在线零售商工作。老板要求她采用一种方式，使得客户可以轻松地和Fran公司的网站整合起来。他们需要能够实时检查库存、下订单以及以编程方式检查订单状态，而不必访问网页。Fran可通过什么方式来直接实现这种互动？

Fran is a web developer who works for an online retailer. Her boss asked her to create a way that customers can easily integrate themselves with Fran’s company’s site. They need to be able to check inventory in real time, place orders, and check order status programmatically without having to access the web page. What can Fran create to most directly facilitate this interaction?

A：API

API

B：Web Scraper

Web Scraper

C：数据字典

Data dictionary

D：呼叫中心

Call center

答案:为了满足客户能够实时检查库存、下订单以及以编程方式检查订单状态的需求，Fran应该创建一个API（应用程序编程接口）。API允许不同的软件应用程序之间进行交互，使得客户可以通过编程方式直接与公司的系统进行通信，而无需通过网页界面。

A：API - 这是正确的选择。API可以提供一个标准化的方法，让客户通过编程方式与公司的系统进行交互，执行如检查库存、下订单和查询订单状态等操作。

B：Web Scraper - 网页抓取器通常用于从网页中提取数据，但这种方法不适合实时交互和编程方式的订单管理，因为它依赖于网页的结构，且效率较低。

C：数据字典 - 数据字典主要用于描述数据的结构和含义，它不提供交互功能，因此不适合这个场景。

D：呼叫中心 - 呼叫中心主要用于通过电话进行客户服务，它不支持编程方式的交互，因此也不适合这个需求。

因此，最合适的答案是 A：API。

-------------------

题目27：Todd的数据中心设施最近经历了一系列涉及瞬间断电的事件。哪项术语最能描述这样的事件？

Todd’s data center facility recently experienced a series of events that involved the momentary loss of power. What term best describes these events?

A：故障

Fault

B：中断

Blackout

C：电压不足

Sag

D：降压

Brownout

答案:题目描述的是数据中心设施经历了一系列瞬间断电的事件。我们需要从选项中选择一个最能描述这种事件的术语。

A. 故障 (Fault) - 通常指的是设备或系统中的错误或问题，但不特指电力问题。

B. 中断 (Blackout) - 指的是电力完全中断，通常持续较长时间，而不是瞬间的。

C. 电压不足 (Sag) - 指的是电压暂时下降，但不一定导致完全断电。

D. 降压 (Brownout) - 指的是电压持续降低，通常是为了减少电力消耗，而不是瞬间断电。

瞬间断电的事件最符合的是 \*\*C. 电压不足 (Sag)\*\*，因为电压不足可能导致电力瞬间中断，但不会持续很长时间。

所以，正确答案是：

\boxed{C}

-------------------

题目28：Lauren 组织的每个系统管理员团队需要处理数百个具有不同安全级别要求的系统，由于这些系统具有大量用户名和密码，因此很难处理。为确保正确处理密码，同时实现日志记录和密码轮换等功能，她应该建议使用什么类型的解决方案？

Lauren’s team of system administrators each deal with hundreds of systems with varying levels of security requirements and find it difficult to handle the multitude of usernames and passwords they each have. What type of solution should she recommend to ensure that passwords are properly handled and that features like logging and password rotation occur?

A：凭据管理系统

A credential management system

B：强密码策略

A strong password policy

C：职责分离

Separation of duties

D：单点登录

Single sign-on

答案:Lauren 面临的挑战是管理大量具有不同安全级别要求的系统，并且每个系统都有不同的用户名和密码。为了确保密码得到正确处理，并且实现日志记录和密码轮换等功能，她应该推荐使用 \*\*凭据管理系统\*\*（Credential Management System）。

\*\*凭据管理系统\*\* 是一种专门用于存储、管理和保护用户名和密码等敏感信息的工具。它可以帮助系统管理员集中管理凭据，自动执行密码轮换，记录访问日志，并提供安全的访问控制。这种系统可以显著减少手动管理凭据的复杂性，并提高安全性。

其他选项的分析：

- \*\*强密码策略\*\*（B）虽然有助于提高密码的安全性，但并不能解决管理大量凭据的问题。

- \*\*职责分离\*\*（C）是一种安全实践，但它主要关注的是权限分配和防止内部威胁，而不是直接解决凭据管理问题。

- \*\*单点登录\*\*（D）可以简化用户的登录过程，但它并不直接解决系统管理员管理大量凭据的需求。

因此，\*\*A：凭据管理系统\*\* 是最合适的解决方案。

-------------------

题目29：Ed的Windows系统无法连接到网络，ipconfig显示以下内容：系统发生了什么？

<div style="text-align:center"><img alt="" height="79" src="/file/100000/m/20210901/f18d75d7171c46ff94a1febcab8f8cd8.png" width="454" /></div>

Ed’s Windows system can’t connect to the network and ipconfig shows the following: What has occurred on the system?

<div style="text-align:center"><img alt="" height="113" src="/file/100000/m/20210901/0b1adfeab90747bb86bbc89d61a0ce51.png" width="513" /></div>

A：系统被其DHCP服务器分配了无效的IP地址

The system has been assigned an invalid IP address by its DHCP server.

B：系统具有手动分配的IP地址

The system has a manually assigned IP address.

C：系统未能获取DHCP地址，并为自己分配了一个地址

The system has failed to get a DHCP address and has assigned itself an address.

D：子网掩码设置不正确，系统无法与网关通信

The subnet mask is set incorrectly, and the system cannot communicate with the gateway.

答案:根据题目描述和图片内容，Ed的Windows系统无法连接到网络，并且`ipconfig`显示的内容表明系统未能从DHCP服务器获取有效的IP地址。系统自动分配了一个以`169.254`开头的IP地址，这是Windows操作系统在无法从DHCP服务器获取IP地址时自动分配的APIPA（Automatic Private IP Addressing）地址。

因此，最可能的情况是：

\*\*C：系统未能获取DHCP地址，并为自己分配了一个地址\*\*

The system has failed to get a DHCP address and has assigned itself an address.

这种情况通常发生在DHCP服务器不可用、网络配置问题或网络连接故障时。

-------------------

题目30：Gina正在为一批新员工创建用户帐户。她正在执行配置过程的哪个阶段？

Gina is performing the initial creation of user accounts for a batch of new employees. What phase of the provisioning process is she conducting?

A：注册

Enrollment

B：清除验证

Clearance verification

C：背景调查

Background checks

D：初始化

Initialization

答案:Gina正在为一批新员工创建用户帐户，这属于用户帐户配置过程的初始阶段。因此，她正在执行的阶段是：

D：初始化

Initialization

这个阶段通常包括创建用户帐户、分配初始权限和设置基本配置等步骤。

-------------------

题目31：Ravi正在为其组织进行的调查取证制定流程，并希望根据每种调查类型常用的证据标准进行区分。什么类型的调查取证通常具有最高的证据标准？

Ravi is developing procedures for forensic investigations conducted by his organization and would like to differentiate based upon the evidentiary standards commonly used for each type of investigation. What type of forensic investigation typically has the highest evidentiary standards?

A：行政性的

Administrative

B：刑事的

Criminal

C：民事的

Civil

D：行业的

Industry

答案:在调查取证中，不同类型的调查通常会有不同的证据标准。证据标准的高低通常取决于调查的严重性和可能产生的后果。以下是各个选项的简要分析：

A. 行政性的 (Administrative)：行政调查通常涉及组织内部的违规行为或政策违反，证据标准相对较低，通常以“优势证据”或“合理怀疑”为标准。

B. 刑事的 (Criminal)：刑事调查涉及犯罪行为，通常由执法机构进行。刑事调查的证据标准最高，通常要求“排除合理怀疑”（beyond a reasonable doubt），这是最高的证据标准，因为刑事定罪可能导致严重的后果，如监禁。

C. 民事的 (Civil)：民事调查通常涉及个人或组织之间的纠纷，证据标准为“优势证据”（preponderance of the evidence），即证据显示某一方的主张更有可能是真实的。这个标准比刑事调查低，但比行政调查高。

D. 行业的 (Industry)：行业调查通常涉及行业标准或规范的遵守情况，证据标准因行业和具体情况而异，但通常不会高于民事调查的标准。

因此，\*\*刑事调查\*\*通常具有最高的证据标准。

正确答案是：\*\*B：刑事的 (Criminal)\*\*

-------------------

题目32：美国有哪些法律保护可以防止执法机构在没有合理理由或未经同意的情况下，搜查美国设施或电子系统？

What U.S. legal protection prevents law enforcement agencies from searching an American facility or electronic system without either probable cause or consent?

A：第一修正案

First Amendment

B：第四修正案

Fourth Amendment

C：第五修正案

Fifth Amendment

D：第十五修正案

Fifteenth Amendment

答案:正确答案是 B：第四修正案 (Fourth Amendment)。

第四修正案保护公民免受不合理的搜查和扣押。它规定，执法机构在没有合理理由（probable cause）或未经当事人同意的情况下，不得进行搜查或扣押。这一修正案旨在保护个人隐私权，防止政府滥用权力。

其他选项的解释：

- A：第一修正案 (First Amendment) 保护言论自由、宗教自由、新闻自由等权利。

- C：第五修正案 (Fifth Amendment) 保护公民免受自证其罪、双重危险等权利。

- D：第十五修正案 (Fifteenth Amendment) 保护公民的投票权，不论种族、肤色或以前的奴役状态。

-------------------

题目33：Tom认为其互联网服务提供商的客户已经利用他系统中的漏洞来读取其他客户的电子邮件。如果是真的，该客户最可能违反什么法律？

Tom believes that a customer of his internet service provider has been exploiting a vulnerability in his system to read the email messages of other customers. If true, what law did the customer most likely violate?

A：ECPA

ECPA

B：CAREA

CAREA

C：HITECH

HITECH

D：隐私法

Privacy Act

答案:题目中描述的情况涉及到未经授权访问他人的电子邮件，这通常被视为侵犯隐私和未经授权的数据访问。在美国，电子通信隐私法（Electronic Communications Privacy Act, ECPA）是主要的相关法律，它规定了电子通信的隐私保护，包括电子邮件。ECPA禁止未经授权的访问、拦截或披露电子通信。

选项A：ECPA（电子通信隐私法）是正确的，因为它直接涉及到电子通信的隐私保护，包括电子邮件。

选项B：CAREA（计算机滥用和滥用法案）虽然涉及到计算机系统的滥用，但它更侧重于计算机欺诈和滥用，而不是特别针对电子邮件的隐私保护。

选项C：HITECH（健康信息技术经济和临床健康法案）主要涉及健康信息的隐私和安全，与电子邮件隐私无直接关联。

选项D：隐私法（Privacy Act）是一个广义的术语，通常指的是保护个人隐私的法律，但在美国，具体到电子邮件的隐私保护，ECPA是更直接相关的法律。

因此，最可能违反的法律是ECPA。答案是A：ECPA。

-------------------

题目34：在这里所示的环保护模型中，哪个环包含用户程序和应用程序？

In the ring protection model shown here, what ring contains user programs and applications?

<div style="text-align:center"><img alt="" height="382" src="/file/100000/m/20210901/35b1d2ce3c3f4a1aa299062706026aed.png" width="412" /></div>

A：环0

Ring 0

B：环1

Ring 1

C：环2

Ring 2

D：环3

Ring 3

答案:在环保护模型（Ring Protection Model）中，通常有四个环，编号从0到3。每个环具有不同的权限级别：

- \*\*环0（Ring 0）\*\*：这是最高权限级别，通常用于操作系统内核。它可以直接访问硬件和执行特权指令。

- \*\*环1（Ring 1）\*\* 和 \*\*环2（Ring 2）\*\*：这些环通常用于设备驱动程序或其他系统服务，权限低于环0，但高于环3。

- \*\*环3（Ring 3）\*\*：这是最低权限级别，通常用于用户程序和应用程序。它只能访问有限的系统资源，并且不能直接执行特权指令。

因此，\*\*用户程序和应用程序\*\*通常运行在\*\*环3\*\*中。

\*\*正确答案是：D：环3（Ring 3）\*\*

-------------------

题目35：在虚拟化平台中，负责控制虚拟资源对物理资源的访问的模块叫什么名字？

In virtualization platforms, what name is given to the module that is responsible for controlling access to physical resources by virtual resources?

A：客户机

Guest machine

B：SDN

SDN

C：内核

Kernel

D：虚拟机管理程序

Hypervisor

答案:在虚拟化平台中，负责控制虚拟资源对物理资源的访问的模块叫做\*\*虚拟机管理程序\*\*，英文是\*\*Hypervisor\*\*。

因此，正确答案是：

D：虚拟机管理程序

Hypervisor

-------------------

题目36：在以下哪种云计算模型中，客户与云供应商的其他客户共享计算基础设施，其中一个客户可能不知道另一个客户的身份？

In which cloud computing model does a customer share computing infrastructure with other customers of the cloud vendor where one customer may not know the other’s identity?

A：公有云

Public cloud

B：私有云

Private cloud

C：社区云

Community cloud

D：共享云

Shared cloud

答案:正确答案是 A：公有云 (Public cloud)。

在公有云模型中，客户与云供应商的其他客户共享计算基础设施。这种模型允许多个客户使用相同的硬件、存储和网络设备，而这些客户通常不知道彼此的身份。公有云服务提供商负责管理和维护基础设施，客户则通过互联网访问这些资源。这种模型提供了高度的可扩展性和成本效益，因为资源是按需分配和计费的。

-------------------

题目37：Justin最近参加了一个灾难恢复计划的测试，团队坐在一起讨论对场景的响应，但实际上并没有激活任何灾难恢复控制。他参加了什么类型的测试？

Justin recently participated in a disaster recovery plan test where the team sat together and discussed the response to a scenario but did not actually activate any disaster recovery controls. What type of test did he participate in?

A：清单审核

Checklist review

B：完全中断测试

Full interruption test

C：并行测试

Parallel test

D：桌面练习

Tabletop exercise

答案:Justin参加的测试类型是 \*\*D：桌面练习（Tabletop exercise）\*\*。

\*\*桌面练习\*\*是一种模拟灾难恢复计划的测试形式，团队成员坐在一起讨论对特定场景的响应，但并不实际激活任何灾难恢复控制。这种测试的目的是通过讨论和模拟来评估计划的可行性和完整性，发现潜在的问题或改进点，而不影响实际的生产环境。

-------------------

题目38：Susan想整合她的网站，以允许用户使用Google等网站的账户。她应该采用什么技术？

Susan wants to integrate her website to allow users to use accounts from sites like Google. What technology should she adopt?

A：Kerberos

Kerberos

B：LDAP

LDAP

C：OpenID

OpenID

D：SESAME

SESAME

答案:题目38的正确答案是：

C：OpenID

OpenID 是一种开放标准，允许用户使用单一的数字身份（如Google账户）登录多个网站。通过OpenID，Susan可以让用户使用他们在Google等网站上的账户来登录她的网站，而不需要为每个网站创建新的账户。这简化了用户的登录过程，并提高了用户体验。

其他选项的解释：

- A：Kerberos 是一种网络认证协议，主要用于企业内部的单点登录（SSO），不适用于跨网站的账户整合。

- B：LDAP（轻量级目录访问协议）通常用于管理和查询目录服务，如企业内部的用户目录，不适用于跨网站的账户整合。

- D：SESAME 是一种安全系统，用于分布式环境中的认证和授权，也不适用于跨网站的账户整合。

-------------------

题目39：Tom正在为位于佛罗里达州中部的Orange Blossoms开展业务连续性规划工作。在评估过程中，委员会确定该地区存在降雪风险，但没有多余资金来实施控制措施以降低该风险的影响。他们选择不采取任何具体行动来应对风险。Orange Blossoms追求什么风险管理策略？

Tom is conducting a business continuity planning effort for Orange Blossoms, a fruit orchard located in Central Florida. During the assessment process, the committee determined that there is a small risk of snow in the region but that the cost of implementing controls to reduce the impact of that risk is not warranted. They elect to not take any specific action in response to the risk. What risk management strategy is Orange Blossoms pursuing?

A：风险缓解

Risk mitigation

B：风险转移

Risk transference

C：风险规避

Risk avoidance

D：风险接受

Risk acceptance

答案:在题目描述的情况下，Orange Blossoms的委员会评估了降雪风险，并认为实施控制措施的成本不值得，因此决定不采取任何具体行动来应对这一风险。这种决策表明他们选择接受这一风险，而不是试图减少、转移或避免它。

因此，Orange Blossoms追求的风险管理策略是：

D：风险接受

Risk acceptance

这种策略意味着组织认识到风险的存在，但决定不采取任何措施来改变风险的潜在影响或发生概率，可能是因为他们认为风险的影响较小，或者控制措施的成本超过了潜在损失。

-------------------

题目40：Paul正在审查一份审计报告的内容，并发现会计部门的一名经理拥有执行财务系统中所有职能的全部权限。以下哪些安全原则最有可能被违反？（选择所有符合条件的）

Paul is reviewing the contents of an audit report and discovers a finding that a manager in the accounting department has full access to perform every function in the financial system. What security principles have most likely been violated? (Select all that apply.)

A：职责分离

Separation of duties

B：工作轮换

Job rotation

C：管理审查

Management review

D：最小特权

Least privilege

答案:在审计过程中，如果发现会计部门的一名经理拥有执行财务系统中所有职能的全部权限，这通常违反了以下安全原则：

A：职责分离 (Separation of duties) - 这是指将关键任务和责任分配给不同的个人或团队，以防止欺诈和错误。如果一个经理可以执行所有职能，那么就没有有效的职责分离。

D：最小特权 (Least privilege) - 这是指用户应该只拥有完成其工作所必需的最小权限。如果一个经理拥有执行所有职能的权限，这显然超出了最小特权的原则。

因此，最有可能被违反的安全原则是 A 和 D。选项 B（工作轮换）和 C（管理审查）虽然也是重要的安全措施，但它们与描述的情况没有直接关联。

-------------------

题目41：Jack的组织是一个多国非营利组织，在世界各地许多发展中国家设有小型办事处。他们需要实现一个访问控制系统，灵活性要求高，尽管在他们的位置的互联网连接性较差，但是它们仍然可以正常工作，Jack的组织采用的最佳访问控制设计类型是什么？

Jack’s organization is a multinational nonprofit that has small offices in many developing countries throughout the world. They need to implement an access control system that allows flexibility and that can work despite poor internet connectivity at their locations. What is the best type of access control design for Jack’s organization?

A：集中访问控制

Centralized access control

B：强制访问控制’

Mandatory access control

C：非集中访问控制

Decentralized access control

D：基于规则的访问控制

Rule-based access control

答案:题目描述中提到Jack的组织是一个多国非营利组织，在许多发展中国家设有小型办事处。这些地方的互联网连接性较差，但组织仍然需要一个灵活性高的访问控制系统。基于这些信息，我们可以分析各个选项的适用性：

A. 集中访问控制（Centralized access control）：集中访问控制通常依赖于一个中央服务器来管理所有的访问权限。由于题目中提到互联网连接性较差，集中访问控制可能无法在断网或网络不稳定的情况下正常工作，因此不太适合。

B. 强制访问控制（Mandatory access control）：强制访问控制是一种严格的访问控制方式，通常用于高安全性的环境，如军事或政府机构。它不太适合需要高灵活性的组织，因此也不符合题目的要求。

C. 非集中访问控制（Decentralized access control）：非集中访问控制允许各个办事处或节点独立管理访问权限，不需要依赖中央服务器。这种设计在互联网连接性较差的情况下仍然可以正常工作，并且提供了较高的灵活性，因此非常适合Jack的组织。

D. 基于规则的访问控制（Rule-based access control）：基于规则的访问控制依赖于预定义的规则来决定访问权限。虽然它具有一定的灵活性，但在互联网连接性较差的情况下，可能无法及时更新或应用规则，因此不如非集中访问控制适合。

综上所述，最佳的选择是：

\*\*C. 非集中访问控制（Decentralized access control）\*\*

-------------------

题目42：哪类美国政府信息分类标签对应这样的信息：&quot;未授权披露通常可能会对国家安全带来可以由原分类组织识别或描述的严重损害&quot;?

What U.S. government classification label is applied to information that, if disclosed, could cause serious damage to national security and also requires that the damage that would be caused is able to be described or identified by the classification authority?

A：分类

Classified

B：秘密

Secret

C：机密

Confidential

D：绝密

Top Secret

答案:题目问的是美国政府信息分类标签中，哪一类对应的是“未授权披露通常可能会对国家安全带来可以由原分类组织识别或描述的严重损害”的信息。这个描述符合“绝密”（Top Secret）的定义。

“绝密”是最高级别的分类，适用于那些如果未经授权披露，可能会对国家安全造成极其严重损害的信息。这种损害的程度和性质必须能够由分类机构识别和描述。

因此，正确答案是：

D：绝密

Top Secret

-------------------

题目43-1：参考以下场景，回答4个问题：

Mike和Renee想使用非对称密码系统来相互通信。它们位于该国的不同地区，但是通过使用由相互信任的证书机构签名的数字证书来交换加密密钥。

For questions , please refer to the following scenario:

Mike and Renee would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.

当证书颁发机构(CA)创建Renee 的数字证书时，证书正文中包含什么密钥？

When the certificate authority (CA) created Renee’s digital certificate, what key was contained within the body of the certificate?

A：Renee的公钥

Renee’s public key

B：Renee的私钥

Renee’s private key

C：CA的公钥

CA’s public key

D：CA的私钥

CA’s private key

答案:在数字证书中，证书颁发机构（CA）会将证书持有者的公钥包含在证书的正文中。因此，Renee的数字证书中包含的是Renee的公钥。

正确答案是：

A：Renee的公钥

Renee's public key

-------------------

题目43-1：参考以下场景，回答4个问题：

Mike和Renee想使用非对称密码系统来相互通信。它们位于该国的不同地区，但是通过使用由相互信任的证书机构签名的数字证书来交换加密密钥。

For questions , please refer to the following scenario:

Mike and Renee would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.

当证书颁发机构创建Renee的数字证书时，它使用什么密钥对完成的证书进行数字签名？

When the certificate authority created Renee’s digital certificate, what key did it use to digitally sign the completed certificate?

A：Renee的公钥

Renee’s public key

B：Renee的私钥

Renee’s private key

C：CA的公钥

CA’s public key

D：CA的私钥

CA’s private key

答案:当证书颁发机构（CA）创建Renee的数字证书时，它使用自己的私钥对证书进行数字签名。因此，正确的答案是：

D：CA的私钥

CA's private key

解释：数字证书的目的是证明某个公钥确实属于某个实体（在这个例子中是Renee）。为了确保证书的真实性和完整性，CA使用自己的私钥对证书进行签名。这样，任何拥有CA公钥的人都可以验证证书的签名，从而确认证书是由可信的CA颁发的。

-------------------

题目43-1：参考以下场景，回答4个问题：

Mike和Renee想使用非对称密码系统来相互通信。它们位于该国的不同地区，但是通过使用由相互信任的证书机构签名的数字证书来交换加密密钥。

For questions , please refer to the following scenario:

Mike and Renee would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.

当Mike收到Renee的数字证书时，他使用什么密钥来验证证书的真实性？

When Mike receives Renee’s digital certificate, what key does he use to verify the authenticity of the certificate?

A：Renee的公钥

Renee’s public key

B：Renee的私钥

Renee’s private key

C：CA的公钥

CA’s public key

D：CA的私钥

CA’s private key

答案:当Mike收到Renee的数字证书时，他需要使用\*\*CA的公钥\*\*来验证证书的真实性。

解释：

- 数字证书是由证书颁发机构（CA）签发的，证书中包含了Renee的公钥以及CA的签名。

- 为了验证证书的真实性，Mike需要使用CA的公钥来解密证书中的签名，并验证签名是否与证书内容匹配。

- 如果验证通过，说明证书确实是由可信的CA签发的，从而可以信任证书中包含的Renee的公钥。

因此，正确答案是：

C：CA的公钥

CA's public key

-------------------

题目43-1：参考以下场景，回答4个问题：

Mike和Renee想使用非对称密码系统来相互通信。它们位于该国的不同地区，但是通过使用由相互信任的证书机构签名的数字证书来交换加密密钥。

For questions , please refer to the following scenario:

Mike and Renee would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificates signed by a mutually trusted certificate authority.

Mike想使用在此交换过程中获得的信息向Renee发送私人消息。他应该使用什么密钥来加密消息？

Mike would like to send Renee a private message using the information gained during this exchange. What key should he use to encrypt the message?

A：Renee的公钥

Renee’s public key

B：Renee的私钥

Renee’s private key

C：CA的公钥

CA’s public key

D：CA的私钥

CA’s private key

答案:在非对称密码系统中，公钥用于加密数据，私钥用于解密数据。Mike想要向Renee发送一条私人消息，确保只有Renee能够解密并阅读该消息。因此，Mike应该使用Renee的公钥来加密消息。这样，只有Renee的私钥才能解密该消息，确保消息的机密性。

因此，正确答案是：

A：Renee的公钥 (Renee's public key)

-------------------

题目44：以下哪个工具可能直接违反未加密的VoIP网络通信的机密性？

Which one of the following tools may be used to directly violate the confidentiality of communications on an unencrypted VoIP network?

A：Nmap

Nmap

B：Nessus

Nessus

C：Wireshark

Wireshark

D：Nikto

Nikto

答案:题目44的正确答案是：

C：Wireshark

\*\*解释：\*\*

- \*\*Nmap\*\* 是一个网络扫描工具，主要用于发现网络上的主机和服务，但它不直接用于捕获或分析网络流量。

- \*\*Nessus\*\* 是一个漏洞扫描工具，用于检测系统中的安全漏洞，但它也不直接用于捕获或分析网络流量。

- \*\*Wireshark\*\* 是一个网络协议分析工具，可以捕获和分析网络流量。对于未加密的VoIP通信，Wireshark可以直接捕获并解析这些通信内容，从而违反通信的机密性。

- \*\*Nikto\*\* 是一个Web服务器漏洞扫描工具，主要用于检测Web应用程序的安全问题，但它不直接用于捕获或分析网络流量。

因此，\*\*Wireshark\*\* 是可能直接违反未加密VoIP网络通信机密性的工具。

-------------------

题目45：关于(ISC)2道德规范，以下哪项是不正确的？

Which of the following is not true about the (ISC)2 Code of Ethics?

A：遵守规范是获得证书的一个条件

Adherence to the code is a condition of certification.

B：不遵守规范可能会导致证书被撤销

Failure to comply with the code may result in revocation of certification.

C：该守则适用于信息安全行业的所有成员

The code applies to all members of the information security profession.

D：发现违反守则的会员必须报告可能的违规行为

Members who observe a breach of the code are required to report the possible violation.

答案:(ISC)² 道德规范是专门为持有 (ISC)² 认证的专业人士制定的，而不是适用于信息安全行业的所有成员。因此，选项 C 是不正确的。

正确答案是：

C：该守则适用于信息安全行业的所有成员

The code applies to all members of the information security profession.

其他选项是正确的：

- A：遵守规范是获得证书的一个条件

- B：不遵守规范可能会导致证书被撤销

- D：发现违反守则的会员必须报告可能的违规行为

-------------------

题目46：下列哪一种加密算法支持不可否认的目标？

Which one of the following cryptographic algorithms supports the goal of nonrepudiation?

A：Blowfish

Blowfish

B：DES

DES

C：AES

AES

D：RSA

RSA

答案:题目46的正确答案是：

\*\*D：RSA\*\*

\*\*解释：\*\*

不可否认性（Nonrepudiation）是指确保消息的发送者无法否认其发送过该消息。RSA 是一种非对称加密算法，广泛用于数字签名，而数字签名是实现不可否认性的关键技术。通过使用发送者的私钥对消息进行签名，接收者可以使用发送者的公钥验证签名的真实性，从而确保消息确实来自发送者。

其他选项：

- \*\*A：Blowfish\*\* 是一种对称加密算法，主要用于加密数据，不支持不可否认性。

- \*\*B：DES\*\* 也是一种对称加密算法，同样不支持不可否认性。

- \*\*C：AES\*\* 是另一种对称加密算法，也不支持不可否认性。

因此，只有 \*\*RSA\*\* 支持不可否认的目标。

-------------------

题目47：Microsoft的STRIDE威胁评估框架使用六种类别的威胁：欺骗、篡改、否认、信息泄露、拒绝服务和特权提升。如果渗透测试人员能够修改审核日志，哪两个STRIDE类别最能描述这个问题？

Microsoft’s STRIDE threat assessment framework uses six categories for threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. If a penetration tester is able to modify audit logs, what STRIDE categories best describe this issue?

A：篡改和信息泄露

Tampering and information disclosure

B：特权提升和篡改

Elevation of privilege and tampering

C：否认和拒绝服务

Repudiation and denial of service

D：否认和篡改

Repudiation and tampering

答案:题目47的正确答案是：

D：否认和篡改

Repudiation and tampering

解析：

- \*\*篡改（Tampering）\*\*：渗透测试人员能够修改审核日志，这直接涉及到篡改数据的行为。

- \*\*否认（Repudiation）\*\*：通过修改审核日志，攻击者可以掩盖其行为，使得系统无法追踪到他们的操作，从而导致否认的可能性增加。

因此，选项D最能描述这个问题。

-------------------

题目48：Carmen正在审查其组织的Web架构，并意识到Web服务器经常要承受来自世界不同地区用户的沉重负载。这种负载出现在不可预测的时间。她希望找到一种解决方案，最大限度地减轻组织服务器的负担，并将内容放置在地理位置更靠近用户的位置以减少加载时间。满足 Carmen需求的最佳解决方案是什么？

Carmen is reviewing her organization’s web architecture and realizes that the web server is often under heavy load from users in different regions of the world. This load comes at unpredictable times. She would like to find a solution that minimizes the burden on her organization’s servers and places content geographically closer to the user to decrease load time. What would be the best solution to Carmen’s requirements?

A：负载均衡器

Load balancer

B：内容交付网络

Content delivery network

C：TLS 加速

TLS acceleration

D：Web应用防火墙

Web application firewall

答案:Carmen 的需求是减轻服务器负担并将内容放置在更靠近用户的地理位置以减少加载时间。最佳解决方案是使用内容交付网络（Content Delivery Network, CDN）。

\*\*内容交付网络（CDN）\*\* 是一种分布式服务器系统，能够将网站内容缓存到全球多个地理位置的服务器上。当用户请求内容时，CDN 会将内容从离用户最近的服务器上提供，从而减少延迟并加快加载时间。此外，CDN 还可以分担原始服务器的负载，因为它可以处理大量的用户请求，而不需要每次都访问原始服务器。

其他选项的解释：

- \*\*负载均衡器（Load balancer）\*\*：虽然负载均衡器可以分配流量到多个服务器以减轻单个服务器的负担，但它并不能将内容放置在更靠近用户的地理位置。

- \*\*TLS 加速（TLS acceleration）\*\*：TLS 加速主要用于加速加密和解密过程，减少 SSL/TLS 握手的时间，但它不直接解决内容分发和地理位置的问题。

- \*\*Web应用防火墙（Web application firewall）\*\*：Web 应用防火墙主要用于保护 Web 应用免受攻击，而不是优化内容分发或减轻服务器负载。

因此，\*\*B：内容交付网络（Content delivery network）\*\* 是最佳解决方案。

-------------------

题目49：Brian最近加入了一个组织，该组织在自己的数据中心虚拟化平台上运行了大部分服务，但也利用IaaS提供商来托管其Web服务和SaaS电子邮件系统。什么术语最好的描述该组织使用的云环境类型？

Brian recently joined an organization that runs the majority of its services on a virtualization platform located in its own data center but also leverages an IaaS provider for hosting its web services and a SaaS email system. What term best describes the type of cloud environment this organization uses?

A：公共云

Public cloud

B：专用云

Dedicated cloud

C：私有云

Private cloud

D：混合云

Hybrid cloud

答案:题目描述的组织使用了两种不同的云环境：一种是在自己的数据中心运行的虚拟化平台，这通常被视为私有云（Private Cloud）；另一种是利用IaaS（基础设施即服务）提供商托管的Web服务和SaaS（软件即服务）电子邮件系统，这通常被视为公共云（Public Cloud）。因此，这个组织使用的云环境类型是混合了私有云和公共云的混合云（Hybrid Cloud）。

正确答案是：

D：混合云

Hybrid cloud

-------------------

题目50：Ben工作的政府机构安装了一个新的门禁系统。系统使用Ben的身份、部门、正常工作时间、工作类别和位置等信息进行授权。Ben的雇主采用什么类型的访问控制系统？

The government agency that Ben works at installed a new access control system. The system uses information such as Ben’s identity, department, normal working hours, job category, and location to make authorization. What type of access control system did Ben’s employer adopt?

A：基于角色的访问控制

Role-based access control

B：基于属性的访问控制

Attribute-based access control

C：管理访问控制

Administrative access control

D：系统自由访问控制

System discretionary access control

答案:题目描述的系统使用了Ben的身份、部门、正常工作时间、工作类别和位置等信息来进行授权。这种类型的访问控制系统是根据用户的属性（如身份、部门、工作时间等）来决定访问权限的，因此它属于基于属性的访问控制（Attribute-based access control, ABAC）。

正确答案是：

B：基于属性的访问控制

Attribute-based access control

-------------------

题目51：Ben正在建立他的组织的安全意识和培训计划，并希望包括更好地吸引用户的互动活动。什么方法最能有助于他实现这个目标？Ben is building his organization’s security awareness and training program and would like to include interactive activities that better engage users. What techniques would best help him meet this goal?

A：策略审查

Policy reviews

B：游戏化

Gamification

C：课堂培训

Classroom training

D：网络钓鱼模拟

Phishing simulations

答案:题目51是关于Ben在建立他的组织的安全意识和培训计划时，希望包括更好地吸引用户的互动活动。我们需要选择一个最能帮助他实现这个目标的方法。

选项分析：

A：策略审查 - 这通常涉及审查和更新组织的安全策略，虽然重要，但不是直接吸引用户参与的方法。

B：游戏化 - 游戏化是一种将游戏设计元素应用于非游戏环境的方法，可以显著提高用户的参与度和兴趣。

C：课堂培训 - 这是一种传统的培训方法，虽然有效，但可能不如游戏化那样吸引用户。

D：网络钓鱼模拟 - 这是一种模拟网络钓鱼攻击的培训方法，虽然有助于提高安全意识，但主要是被动接受信息，互动性较低。

综合考虑，游戏化（B）是最能吸引用户参与并提高他们安全意识的方法。因此，最佳答案是：

B：游戏化

Gamification

-------------------

题目52：Andrew认为属于他的组织的数字证书已被盗用，并希望将其添加到证书吊销列表（CRL）中。谁必须将证书添加到CRL？

Andrew believes that a digital certificate belonging to his organization was compromised and would like to add it to a certificate revocation list (CRL). Who must add the certificate to the CRL?

A：Andrew

Andrew

B：顶级域的根官方

The root authority for the top-level domain

C：颁发证书的CA

The CA that issued the certificate

D：顶级域的撤销授权官方

The revocation authority for the top-level domain

答案:正确答案是 C：颁发证书的CA（The CA that issued the certificate）。

证书吊销列表（CRL）是由颁发数字证书的证书颁发机构（CA）维护和更新的。当证书被认为不再安全或有效时，例如在证书被盗用的情况下，颁发该证书的CA负责将其添加到CRL中。这样，依赖方（如浏览器或其他客户端）可以检查CRL以确认证书的有效性。Andrew作为证书的持有者，可以请求CA吊销证书，但实际将证书添加到CRL的操作必须由颁发证书的CA执行。

-------------------

题目53：Amanda正在考虑实施一名顾问建议的数据库恢复机制。在推荐的方法中，自动过程将按小时将事务的记录从主站点移动到备份站点。顾问描述什么类型的数据库恢复技术？

Amanda is considering the implementation of a database recovery mechanism recommended by a consultant. In the recommended approach, an automated process will move records of transactions from the primary site to a backup site on an hourly basis. What type of database recovery technique is the consultant describing?

A：电子仓库

Electronic vaulting

B：事务日志

Transaction logging

C：远程镜像

Remote mirroring

D：远程日志

Remote journaling

答案:题目中描述的是一种数据库恢复技术，其中自动过程按小时将事务的记录从主站点移动到备份站点。这种技术最符合的是远程日志（Remote journaling）。

远程日志是一种数据库恢复技术，它通过将事务日志实时或定期传输到远程站点来确保数据的安全性和可恢复性。这种方法可以在主站点发生故障时，使用备份站点上的日志来恢复数据。

因此，正确答案是：

D：远程日志

Remote journaling

-------------------

题目54：Ron正在努力对其组织使用的信息进行分类，并希望在他的分类方案中包括可能触发美国州数据泄露通知法的所有信息。假设这些信息与特定个人有关，他应该包括以下哪些类别的信息？ （选择所有符合条件的。）

Ron is working to classify information used by his organization and would like to include all information that might trigger a U.S. state data breach notification law in his classification scheme. Which of the following categories of information should he include, assuming that they are connected to a specific individual? (Select all that apply.)

A：银行帐号和PIN

Bank account number and PIN

B：驾照号码

Driver’s license number

C：婚姻状况

Marital status

D：社会安全号码

Social Security number

答案:在美国，各州的数据泄露通知法通常要求组织在发生数据泄露事件时通知受影响的个人，特别是当泄露的信息可能被用于身份盗窃或其他欺诈行为时。这些法律通常涵盖与个人身份密切相关的敏感信息。根据这些法律，Ron应该包括以下类别的信息：

A：银行帐号和PIN

银行帐号和PIN是与个人财务安全直接相关的敏感信息，泄露这些信息可能导致财务损失或身份盗窃。

B：驾照号码

驾照号码是个人身份的重要标识符，泄露这些信息可能被用于身份盗窃或其他欺诈行为。

D：社会安全号码

社会安全号码是美国公民和居民的重要身份标识符，泄露这些信息可能导致严重的身份盗窃问题。

C：婚姻状况

婚姻状况通常不被视为触发数据泄露通知法的敏感信息，因为它通常不会直接导致身份盗窃或财务损失。

因此，Ron应该选择A、B和D作为可能触发美国州数据泄露通知法的信息类别。

-------------------

题目55：以下哪种调查类型对收集和保存信息的标准最为宽松？

Which one of the following investigation types has the loosest standards for the collection and preservation of information?

A：民事调查

Civil investigation

B：业务调查

Operational investigation

C：刑事调查

Criminal investigation

D：监管调查

Regulatory investigation

答案:在收集和保存信息的标准方面，不同类型的调查有不同的严格程度。刑事调查通常有最严格的标准，因为它们涉及法律程序和可能的刑事指控，需要确保证据的完整性和合法性。监管调查也有相对严格的标准，因为它们通常由政府机构进行，以确保遵守法律法规。

民事调查和业务调查的标准相对较为宽松。民事调查通常涉及个人或公司之间的纠纷，而业务调查则可能涉及公司内部的审计或效率评估。这些调查的目的通常不是为了刑事起诉，因此对证据的收集和保存要求不如刑事或监管调查严格。

因此，选项 \*\*B：业务调查 (Operational investigation)\*\* 对收集和保存信息的标准最为宽松。

-------------------

题目56：当Sue在她的新公司工作时，她需要签署NDA。为什么公司要求她签署NDA？

Sue was required to sign an NDA when she took a job at her new company. Why did the company require her to sign it?

A：保护其数据的保密性

To protect the confidentiality of their data

B：确保Sue没有删除他们的数据

To ensure that Sue did not delete their data

C：防止Sue将来与他们直接竞争

To prevent Sue from directly competing with them in the future

D：要求Sue确保数据的可用性

To require Sue to ensure the availability for their data as part of her job

答案:题目56的正确答案是：

A：保护其数据的保密性

To protect the confidentiality of their data

解释：NDA（Non-Disclosure Agreement，保密协议）的主要目的是确保签署方不会泄露公司的机密信息。因此，公司要求Sue签署NDA是为了保护其数据的保密性，防止敏感信息被泄露给外部人员或竞争对手。其他选项（如防止数据删除、防止竞争或确保数据可用性）并不是NDA的主要目的。

-------------------

题目57：Susan担心她所使用的生物识别技术的错误接受率(FAR)。什么是处理错误接受率的最好方法？

Susan is concerned about the FAR associated with her biometric technology. What is the best method to deal with the FAR?

A：调整交叉错误率(CER)

Adjust the CER.

B：改变系统的灵敏度以降低错误拒绝率(FRR)

Change the sensitivity of the system to lower the FRR.

C：添加第二个因素

Add a second factor.

D：更换生物识别系统

Replace the biometric system.

答案:错误接受率（FAR，False Acceptance Rate）是指生物识别系统错误地将未授权用户识别为授权用户的比率。处理错误接受率的最好方法通常涉及调整系统的安全性和准确性，以确保只有真正的授权用户被接受。

选项分析：

A：调整交叉错误率（CER） - 交叉错误率是错误接受率（FAR）和错误拒绝率（FRR）的平衡点。调整CER可能会影响FAR，但这并不是直接处理FAR的方法。

B：改变系统的灵敏度以降低错误拒绝率（FRR） - 降低FRR可能会间接影响FAR，但这并不是直接处理FAR的方法。

C：添加第二个因素 - 添加第二个因素（如密码、智能卡等）可以显著提高系统的安全性，减少FAR。这是一种有效的多因素认证方法，可以大大降低错误接受的风险。

D：更换生物识别系统 - 虽然更换系统可能解决FAR问题，但这通常是一个成本高昂且复杂的过程，并不是最直接或最有效的方法。

因此，处理错误接受率的最好方法是 \*\*C：添加第二个因素\*\*。

-------------------

题目58：组织中的哪种数据处理角色最有可能授予用户日常访问信息的权限？

Which data processing role in an organization is most likely to grant users access to information on a day-to-day basis?

A：企业所有者

Business owners

B：数据处理者

Data processors

C：数据所有者

Data owners

D：数据管理员

Data stewards

答案:在组织中，最有可能授予用户日常访问信息权限的角色是 \*\*D：数据管理员（Data stewards）\*\*。

\*\*数据管理员\*\*通常负责管理和维护数据的日常使用，确保数据的准确性、一致性和安全性。他们的职责包括为用户分配访问权限，确保用户能够访问他们需要的数据，同时遵守组织的政策和法规。

其他选项的解释：

- \*\*A：企业所有者（Business owners）\*\*：通常负责业务战略和决策，而不是日常的数据访问管理。

- \*\*B：数据处理者（Data processors）\*\*：负责处理数据，但不一定负责访问权限的管理。

- \*\*C：数据所有者（Data owners）\*\*：负责数据的整体管理和策略，但通常不直接处理日常的访问权限分配。

因此，\*\*数据管理员\*\*是最合适的答案。

-------------------

题目59：Ron是一家美国公司的首席信息安全官，该公司正在与一家欧洲公司建立业务合作伙伴关系。 这家欧洲公司将通过Ron公司的专有信用评分算法，来发送公司客户记录。在GDPR下，Ron 的公司将在客户数据方面扮演什么角色？

Ron is the CISO of a U.S. company that is entering into a business partnership with a European firm. The European firm will be sending his company customer records to run through Ron’s firm’s proprietary credit scoring algorithm. Under GDPR, what role will Ron’s company have relative to the customer data?

A：数据控制者

Data controller

B：数据所有者

Data owner

C：数据主体

Data subject

D：数据处理者

Data processor

答案:在GDPR（通用数据保护条例）下，Ron的公司将扮演的角色是 \*\*D：数据处理者（Data processor）\*\*。

解释如下：

- \*\*数据控制者（Data controller）\*\* 是指决定数据处理目的和方式的实体。在这个场景中，欧洲公司是数据控制者，因为他们决定将客户数据发送给Ron的公司进行处理。

- \*\*数据处理者（Data processor）\*\* 是指代表数据控制者处理数据的实体。Ron的公司接收欧洲公司的客户数据并运行其专有信用评分算法，因此是数据处理者。

- \*\*数据所有者（Data owner）\*\* 不是GDPR中的正式术语。

- \*\*数据主体（Data subject）\*\* 是指数据所涉及的个人，即客户。

因此，Ron的公司在GDPR下的角色是数据处理者。

-------------------

题目60：Tonya最近在她的组织中引入了一种新的安全控制作为紧急访问系统管理权限。在此过程中，必须两名合格的管理员一起去检索紧急凭据。什么术语最能描述这个过程？

Tonya recently introduced a new security control in her organization for emergency access to system administrator privileges. Under this procedure, two qualified administrators must agree to retrieve emergency credentials. What term best describes this process?

A：职责分离

Separation of duties

B：最小特权

Least privilege

C：双人控制

Two-person control

D：多因素认证

Multifactor authentication

答案:这个问题的答案应该是 C：双人控制（Two-person control）。

双人控制是一种安全措施，要求至少两个人在场才能执行某些关键操作，如访问敏感信息或执行高权限任务。这种方法有助于防止内部威胁和错误操作，因为需要两个人的同意和参与才能完成操作。在这个例子中，Tonya 引入的安全控制要求两名合格的管理员一起检索紧急凭据，这正符合双人控制的概念。

其他选项的解释如下：

- A：职责分离（Separation of duties）是指将任务和责任分配给不同的人，以防止一个人拥有过多的权力或控制。

- B：最小特权（Least privilege）是指用户或系统只拥有完成其任务所需的最小权限。

- D：多因素认证（Multifactor authentication）是指使用两种或更多种不同的认证方法来验证用户的身份。

这些选项虽然都是重要的安全控制措施，但它们并不直接描述题目中提到的需要两名管理员共同操作的过程。

-------------------

题目61：侵害网站的攻击者经常获取散列密码的数据库。什么技术可以最好地保护这些密码免受使用预先计算值的自动密码破解攻击？

Attackers who compromise websites often acquire databases of hashed passwords. What technique can best protect these passwords against automated password cracking attacks that use precomputed values?

A：使用MD5 散列算法

Using the MD5 hashing algorithm

B：使用SHA-1 散列算法

Using the SHA-1 hashing algorithm

C：盐

Salting

D：双散列

Double-hashing

答案:正确答案是 \*\*C：盐 (Salting)\*\*。

### 解释：

- \*\*盐 (Salting)\*\*：盐是一种随机数据，它在密码散列过程中被添加到密码中。每个用户的密码都会使用不同的盐值进行散列，即使两个用户使用相同的密码，最终的散列值也会不同。这可以有效地防止攻击者使用预先计算的彩虹表（rainbow tables）进行密码破解。

- \*\*MD5 和 SHA-1\*\*：这些散列算法已经被证明是不安全的，容易受到碰撞攻击和彩虹表攻击。因此，它们不适合用于保护密码。

- \*\*双散列 (Double-hashing)\*\*：虽然双散列可以增加破解的难度，但它并不能有效防止使用预先计算值的攻击（如彩虹表攻击）。盐的使用是更有效的防护措施。

因此，\*\*盐 (Salting)\*\* 是保护密码免受预先计算值攻击的最佳技术。

-------------------

题目62：Jim开始了一个系统工程师的新工作，他正在审查一份题为&ldquo;调查取证响应指南&rdquo;的文件。下列哪项陈述是不正确的？

Jim starts a new job as a system engineer, and he is reviewing a team document entitled &quot;Forensic Response Guidelines.&quot;Which one of the following statements is not true?

A：Jim必须遵守本文档中的信息

Jim must comply with the information in this document.

B：该文件包含有关取证检查的信息

The document contains information about forensic examinations.

C：Jim应该彻底阅读文件

Jim should read the document thoroughly.

D：该文件可能是基于行业的最佳实践

The document is likely based on industry best practices.

答案:题目要求找出不正确的陈述。我们来逐一分析每个选项：

A：Jim必须遵守本文档中的信息

- 作为一个系统工程师，Jim通常需要遵守公司或团队的政策和指南，因此这个陈述是正确的。

B：该文件包含有关取证检查的信息

- 文件标题是“调查取证响应指南”，因此可以合理推断文件内容涉及取证检查，这个陈述也是正确的。

C：Jim应该彻底阅读文件

- 作为新员工，Jim应该彻底阅读和理解相关的工作指南和文档，以确保他能够正确执行工作职责，这个陈述也是正确的。

D：该文件可能是基于行业的最佳实践

- 通常，这类指南会基于行业的最佳实践来制定，因此这个陈述也是合理的。

综上所述，所有选项看起来都是正确的。然而，题目要求找出不正确的陈述。在这种情况下，可能需要重新审视选项A。虽然Jim通常需要遵守公司或团队的指南，但“必须遵守”可能有些绝对，因为有时可能会有例外情况或需要根据具体情况进行调整。因此，选项A可能是最不正确的陈述。

最终答案是：

A：Jim必须遵守本文档中的信息

Jim must comply with the information in this document.

-------------------

题目63：Evan正在审查他的访问控制系统，以确保没有任何用户能够读取超出其安全许可级别的信息。他正在执行什么安全模型？

Evan is reviewing his access control system to ensure that no user is able to read information that is above their security clearance level. What security model is he enforcing?

A：Bell-LaPadula

Bell-LaPadula

B：\*安全属性

Star security property

C：自主安全属性

Discretionary security property

D：Biba

Biba

答案:Evan正在审查他的访问控制系统，以确保没有任何用户能够读取超出其安全许可级别的信息。他正在执行的安全模型是 \*\*Bell-LaPadula\*\* 模型。

\*\*Bell-LaPadula\*\* 模型是一种强制访问控制（MAC）模型，主要用于保护信息的机密性。它的核心原则是“不能向上读，不能向下写”（no read up, no write down），即用户不能读取高于其安全级别的信息，也不能将信息写入低于其安全级别的区域。

因此，正确答案是：

\*\*A：Bell-LaPadula\*\*

-------------------

题目64：Ben需要验证他组织的关键应用程序的最新补丁没有在其他地方引入问题。Ben需要进行什么类型的测试以确保这一点？

Ben needs to verify that the most recent patch for his organization&rsquo;s critical application did not introduce issues elsewhere. What type of testing does Ben need to conduct to ensure this?

A：单元测试

Unit testing

B：白盒测试

White box

C：回归测试

Regression testing

D：黑盒测试

Black box

答案:题目64的正确答案是：

C：回归测试

Regression testing

解析：

回归测试（Regression testing）是一种软件测试方法，用于验证在软件修改或更新后，原有的功能是否仍然正常工作。Ben需要确保最新的补丁没有引入新的问题或破坏现有的功能，因此回归测试是最合适的测试类型。通过回归测试，可以检查应用程序的各个部分是否仍然按预期工作，从而确保补丁没有在其他地方引入问题。

其他选项的解释：

- 单元测试（Unit testing）：主要用于测试单个代码单元或模块的功能，通常由开发人员在编写代码时进行。

- 白盒测试（White box testing）：关注代码的内部结构和逻辑，通常需要了解代码的实现细节。

- 黑盒测试（Black box testing）：关注软件的功能和输出，而不考虑内部代码结构。

回归测试是确保补丁没有引入新问题的关键测试类型。

-------------------

题目65：Tamara最近决定购买网络安全保险，以便在发生数据泄露时支付公司的费用。她追求什么风险管理策略？

Tamara recently decided to purchase cyberliability insurance to cover her company’s costs in the event of a data breach. What risk management strategy is she pursuing?

A：风险接受

Risk acceptance

B：风险缓解

Risk mitigation

C：风险转移

Risk transference

D：风险规避

Risk avoidance

答案:Tamara决定购买网络安全保险，这是一种将潜在的财务风险转移给保险公司的策略。通过购买保险，她将因数据泄露可能产生的费用转移给了保险公司，而不是由自己的公司承担。因此，她追求的风险管理策略是风险转移。

正确答案是：

C：风险转移

Risk transference

-------------------

题目66：下列哪一项不是(ISC)2道德守则的四个规范之一？

Which of the following is not one of the four canons of the (ISC)2 Code of Ethics?

A：避免可能危及公正性的利益冲突

Avoid conflicts of interest that may jeopardize impartiality.

B：保护社会公共利益和维持必要的公众信任

Protect society, the common good, necessary public trust and confidence, and the infrastructure.

C：正直、诚实、公正、负责任和合法地行事

Act honorably, honestly, justly, responsibly, and legally.

D：为负责人提供高效优质的服务

Provide diligent and competent service to principals.

答案:(ISC)² 道德守则的四个规范包括：

1. 保护社会公共利益和维持必要的公众信任（Protect society, the common good, necessary public trust and confidence, and the infrastructure）。

2. 正直、诚实、公正、负责任和合法地行事（Act honorably, honestly, justly, responsibly, and legally）。

3. 为负责人提供高效优质的服务（Provide diligent and competent service to principals）。

4. 发展和保护职业（Advance and protect the profession）。

选项 A 中的“避免可能危及公正性的利益冲突”并不是 (ISC)² 道德守则的四个规范之一。因此，正确答案是：

\*\*A：避免可能危及公正性的利益冲突\*\*

Avoid conflicts of interest that may jeopardize impartiality.

-------------------

题目67：Jim希望允许合作组织的Active Directory森林(B)访问他的域森林(A)的资源，但不希望允许其域中的用户访问B的资源。他也不希望信任在形成时通过域树向上流动。他应该怎么做？

Jim wants to allow a partner organization’s Active Directory forest (B) to access his domain forest’s (A)’s resources but doesn’t want to allow users in his domain to access B’s resources. He also does not want the trust to flow upward through the domain tree as it is formed. What should he do?

A：建立一个双向传递信任

Set up a two-way transitive trust.

B：建立单向传递信任

Set up a one-way transitive trust.

C：建立单向不可转移信任

Set up a one-way nontransitive trust.

D：建立双向不可转移信任

Set up a two-way nontransitive trust.

答案:Jim 的需求是允许合作组织的 Active Directory 森林（B）访问他的域森林（A）的资源，但不希望允许其域中的用户访问 B 的资源。此外，他也不希望信任在形成时通过域树向上流动。

根据这些需求，Jim 应该选择 \*\*C：建立单向不可转移信任\*\*（Set up a one-way nontransitive trust）。

### 解释：

- \*\*单向信任\*\*：单向信任意味着只有一方（B）可以访问另一方的资源（A），而另一方（A）不能访问 B 的资源。这符合 Jim 的需求，即允许 B 访问 A 的资源，但不允许 A 的用户访问 B 的资源。

- \*\*不可转移信任\*\*：不可转移信任意味着信任关系不会自动扩展到其他域或森林。这符合 Jim 的需求，即不希望信任通过域树向上流动。

因此，\*\*C：建立单向不可转移信任\*\* 是最符合 Jim 需求的选项。

-------------------

题目68：Susan的团队通过手动审查缺陷代码来执行代码分析。他们执行什么类型的分析？

Susan’s team is performing code analysis by manually reviewing the code for flaws. What type of analysis are they performing?

A：灰盒

Gray box

B：静态

Static

C：动态

Dynamic

D：模糊

Fuzzing

答案:Susan的团队通过手动审查缺陷代码来执行代码分析，这种分析属于\*\*静态分析\*\*。静态分析是指在代码不运行的情况下，通过检查源代码或编译后的代码来发现潜在的错误、漏洞或不符合编码规范的地方。

因此，正确答案是：

\*\*B：静态\*\*

Static

-------------------

题目69：Kevin的组织最近遭受了勒索软件攻击，他正在考虑支付赎金。关于支付赎金，以下哪些描述是正确的？（选择所有符合条件的）

Kevin’s organization recently suffered a ransomware attack, and he is considering paying the ransom. Which of the following statements are true about paying the ransom? (Select all that apply.)

A：不能保证他会收到解密密钥

There is no guarantee that he will receive the decryption key.

B：攻击者加密了他的数据，但无法访问数据本身

The attackers have encrypted his data but do not have access to the data itself.

C：从备份中恢复将无法还原信息

Restoring from backup will not recover information.

D：支付赎金可能是非法的

Paying ransoms may be illegal.

答案:在考虑支付勒索软件赎金时，以下描述是正确的：

A：不能保证他会收到解密密钥

There is no guarantee that he will receive the decryption key.

- 这是正确的。支付赎金后，攻击者并不总是会提供解密密钥，或者提供的密钥可能无法正常工作。

B：攻击者加密了他的数据，但无法访问数据本身

The attackers have encrypted his data but do not have access to the data itself.

- 这是正确的。勒索软件通常只是加密数据，而攻击者本身并不一定访问或窃取数据内容。

D：支付赎金可能是非法的

Paying ransoms may be illegal.

- 这是正确的。在某些国家或地区，支付赎金可能是非法的，尤其是当涉及到某些类型的攻击者（如恐怖组织）时。

C：从备份中恢复将无法还原信息

Restoring from backup will not recover information.

- 这是不正确的。从备份中恢复通常是解决勒索软件攻击的有效方法，前提是备份是最近的且未被加密。

因此，正确的选项是 A、B 和 D。

-------------------

题目70：可信平台模块（TPM）的哪些功能会创建系统配置的散列摘要来验证未进行过修改？

What feature of a Trusted Platform Module (TPM) creates a hash summary of the system configuration to verify that changes have not been made?

A：远程证明

Remote attestation

B：绑定

Binding

C：密封

Sealing

D：RNG

RNG

答案:可信平台模块（TPM）的功能中，用于创建系统配置的散列摘要以验证系统未被修改的功能是 \*\*远程证明（Remote Attestation）\*\*。

\*\*远程证明\*\* 允许系统向外部实体证明其当前状态（如系统配置、软件状态等）未被篡改。TPM 会生成系统配置的散列摘要，并将其与预期的值进行比较，以验证系统的完整性。

因此，正确答案是：

\*\*A：远程证明\*\*

\*\*Remote attestation\*\*

-------------------

题目71：Gary担心其组织数据中心的环境控制措施可能无法有效控制湿度。以下哪种情况可能由湿度问题引起？（选择所有符合条件的）

Gary is concerned that the environmental controls in his organization’s data center may not be effectively controlling humidity. Which of the following circumstances may result from humidity issues? (Select all that apply.)

A：静电损坏设备

Static electricity damaging equipment

B：电源起火

Fires in power supplies

C：设备腐蚀

Corrosion of equipment

D：物理访问控制失效

Physical access control failures

答案:题目71是关于数据中心环境控制中湿度问题可能引起的后果。湿度问题在数据中心中是一个重要的环境因素，因为它可以影响设备的性能和寿命。让我们逐一分析每个选项：

A：静电损坏设备

高湿度可以减少静电的积累，而低湿度则可能导致静电积累增加。静电放电（ESD）可以损坏敏感的电子设备。因此，湿度控制不当（特别是湿度过低）可能导致静电损坏设备。

B：电源起火

虽然湿度过高可能导致电气设备短路，从而引发火灾，但这种情况相对较少见。电源起火更多与电气故障、过载或设备老化有关，而不是直接由湿度问题引起。

C：设备腐蚀

高湿度环境可能导致金属部件的腐蚀，特别是如果湿度控制不当，导致冷凝水形成。腐蚀会损害设备的物理结构和电气连接，从而影响设备的性能和可靠性。

D：物理访问控制失效

物理访问控制通常涉及门禁系统、锁具等安全措施，这些措施不太可能直接受到湿度问题的影响。因此，湿度问题不太可能导致物理访问控制失效。

综上所述，湿度问题可能引起的情况包括静电损坏设备（A）和设备腐蚀（C）。因此，正确答案是A和C。

-------------------

题目72：Evan最近建立了一个备用处理设施，其中包括在几分钟或几秒钟内恢复运行所需的所有硬件和数据。他建造了什么类型的设施？

Evan recently built an alternate processing facility that includes all of the hardware and data necessary to restore operations in a matter of minutes or seconds. What type of facility has he built?

A：热站点

Hot site

B：温站点

Warm site

C：冷站点

Cold site

D：移动站点

Mobile site

答案:Evan建立的备用处理设施能够在几分钟或几秒钟内恢复运行，这意味着该设施已经具备了所有必要的硬件和数据，并且可以立即投入使用。这种类型的设施被称为“热站点”（Hot site）。

热站点是一种完全配置好的备用设施，通常与主站点保持实时同步，确保在主站点发生故障时能够迅速接管并继续运行。因此，正确答案是：

A：热站点

Hot site

-------------------

题目73：Hadley正在查看网络流量日志，并在其网络上搜索系统日志活动。当他创建一个过滤器来搜索该流量时，他应该包括哪个UDP端口？

Hadley is reviewing network traffic logs and is searching for syslog activity on his network. When he creates a filter to look for this traffic, which UDP port should he include?

A：443

443

B：514

514

C：515

515

D：445

445

答案:正确答案是 B：514。

系统日志（syslog）通常使用UDP端口514来传输日志信息。因此，如果Hadley想要过滤出与系统日志相关的网络流量，他应该在过滤器中包含UDP端口514。其他选项中的端口号分别用于不同的协议：

- 443：通常用于HTTPS（加密的HTTP）通信。

- 515：通常用于LPD（Line Printer Daemon）协议，用于打印服务。

- 445：通常用于Microsoft-DS（Microsoft Directory Services）协议，用于文件共享和网络服务。

-------------------

题目74：Fred发现一个数据包，他的协议分析器显示PSH和URG都被设置了。他正在看什么类型的包，这两个标志是什么意思？

Fred finds a packet that his protocol analyzer shows with both PSH and URG set. What type of packet is he looking at, and what do the flags mean?

A：UDP数据包；PSH和URG用于指示数据应当以高速发送

A UDP packet; PSH and URG are used to indicate that the data should be sent at high speed.

B：TCP数据包；PSH和URG用于清除缓冲区并指示数据是紧急的

A TCP packet; PSH and URG are used to clear the buffer and indicate that the data is urgent.

C：TCP数据包；PSH和URG用于预置报头并指示网络的速度不受监管

A TCP packet; PSH and URG are used to preset the header and indicate that the speed of the network is unregulated.

D：UDP数据包；PSH和URG用于指示应该清除UDP缓冲区，并指示数据是紧急的

A UDP packet; PSH and URG are used to indicate that the UDP buffer should be cleared and that the data is urgent.

答案:正确答案是 B：TCP数据包；PSH和URG用于清除缓冲区并指示数据是紧急的。

解释：

- \*\*PSH (Push) 标志\*\*：在TCP协议中，PSH标志用于指示接收方应立即将数据传递给应用程序，而不是等待缓冲区填满。这通常用于需要立即处理的数据，例如实时通信或交互式应用。

- \*\*URG (Urgent) 标志\*\*：URG标志用于指示数据包中包含紧急数据。紧急数据通常需要优先处理，TCP协议中的紧急指针字段会指向紧急数据的末尾。

UDP协议中没有PSH和URG标志，因此选项A和D是错误的。选项C中的描述也不正确，因为PSH和URG标志并不用于预置报头或指示网络速度不受监管。

因此，Fred正在查看的是一个TCP数据包，PSH和URG标志分别用于清除缓冲区和指示数据是紧急的。

-------------------

题目75：这里显示了什么代码审查流程？

<div style="text-align:center"><img alt="" height="370" src="/file/100000/m/20210901/f2215b00f88343e69e5f14c58118a624.png" width="312" /></div>

What code review process is shown here?

<div style="text-align:center"><img alt="" height="484" src="/file/100000/m/20210901/7e047ee171df4463b9e47b4eecaf35ed.png" width="524" /></div>

A：静态检查

Static inspection

B：Fagan检查

Fagan inspection

C：动态检查

Dynamic inspection

D：接口测试

Interface testing

答案:根据提供的图片描述，代码审查流程显示的是Fagan检查（Fagan inspection）。Fagan检查是一种正式的代码审查方法，由Michael Fagan在1970年代开发，旨在通过结构化的流程来提高代码质量。这种方法通常包括以下几个步骤：

1. \*\*规划\*\*：确定审查的目标和范围。

2. \*\*概述\*\*：向审查团队介绍代码的背景和目标。

3. \*\*准备\*\*：审查团队成员独立审查代码，准备问题和建议。

4. \*\*审查会议\*\*：团队成员集体讨论代码，提出问题并记录缺陷。

5. \*\*返工\*\*：开发人员根据审查结果修改代码。

6. \*\*跟进\*\*：确保所有问题都已解决，并且代码符合质量标准。

因此，正确答案是：

\*\*B：Fagan检查\*\*

Fagan inspection

-------------------

题目76：在日志审查期间，Karen发现她收集日志的系统需要具有如图所示的日志设置。Karen可能遇到什么问题？

<div style="text-align:center"><img alt="" height="333" src="/file/100000/m/20210901/2c0dd09d1eb841a7b57b9a480b66cd29.png" width="373" /></div>

During a log review, Karen discovers that the system she needs to gather logs from has the log setting shown here. What problem is Karen likely to encounter?

<div style="text-align:center"><img alt="" src="/file/100000/m/20210901/950d45441f2548c6b9c8313aca85fdab.png" /></div>

A：系统中存储了过多日志数据

Too much log data will be stored on the system.

B：系统自动清除归档日志

The system is automatically purging archived logs.

C：日志将不包含所需的信息

The logs will not contain the information needed.

D：日志将仅包含最近的20MB日志数据

The logs will only contain the most recent 20 MB of log data.

答案:根据题目描述和提供的图片信息，Karen在审查日志时发现系统设置了日志的存储限制。具体来说，系统可能设置了日志文件的大小限制为20MB，并且当日志文件达到这个大小后，旧的日志数据可能会被覆盖或删除。

因此，Karen可能会遇到的问题是日志数据只包含最近的20MB内容，而旧的日志数据可能会丢失。这可能会导致她无法获取到完整的日志信息，特别是如果需要审查较早的日志数据时。

所以，正确答案是：

\*\*D：日志将仅包含最近的20MB日志数据\*\*

The logs will only contain the most recent 20 MB of log data.

-------------------

题目77：在调查一起大范围的分布式拒绝服务攻击时，Matt在他的浏览器中输入一个攻击系统的IP，他看到了如下界面。该僵尸网络很可能是由什么类型的设备组成的？

While investigating a widespread distributed denial-of-service attack, Matt types in the IP address of one of the attacking systems into his browser and sees the following page. What type of devices is the botnet likely composed of?

<div style="text-align:center"><img alt="" height="676" src="/file/100000/m/20210901/0203309206a3492c88d1e85c2c79eede.png" width="739" /></div>

A：SCADA

SCADA

B：云基础设施

Cloud infrastructure

C：Web服务器

Web servers

D：IoT

IoT

答案:在调查分布式拒绝服务攻击（DDoS）时，Matt通过浏览器访问攻击系统的IP地址并看到了一个特定的界面。根据这个界面的特征，我们可以推测出僵尸网络（Botnet）的组成设备类型。

选项分析：

- \*\*A：SCADA\*\* - SCADA系统通常用于工业控制系统，不太可能被用于大规模的DDoS攻击。

- \*\*B：云基础设施\*\* - 云基础设施通常由大型服务提供商管理，安全性较高，不太可能被轻易用于DDoS攻击。

- \*\*C：Web服务器\*\* - Web服务器虽然可能被攻击，但通常不会大规模组成僵尸网络。

- \*\*D：IoT\*\* - 物联网设备（如智能摄像头、路由器等）由于数量庞大且安全性较低，常被用于组成僵尸网络进行DDoS攻击。

根据题目描述和界面特征，最可能的设备类型是物联网设备（IoT）。

\*\*正确答案：D：IoT\*\*

-------------------

题目78-1：参考以下场景，回答3个问题 ：

Alejandro是一家大型公司的事故响应分析师。他的上班时间是午夜，一个入侵检测系统发出警报，公司的一个关键信息系统可能遭受暴力密码攻击。他在采取任何其他行动之前执行事件的初步分类。

For questions , please refer to the following scenario:

Alejandro is an incident response analyst for a large corporation. He is on the midnight shift when an intrusion detection system alerts him to a potential brute-force password attack against one of the company’s critical information systems. He performs an initial triage of the event before taking any additional action.

Alejandro 目前正在执行的事件响应过程的哪个阶段？

What stage of the incident response process is Alejandro currently conducting?

A：检测

Detection

B：反应

Response

C：恢复

Recovery

D：缓解

Mitigation

答案:Alejandro 目前正在执行的事件响应过程的阶段是 \*\*A：检测 (Detection)\*\*。

在这个阶段，Alejandro 通过入侵检测系统（IDS）发现了一个潜在的暴力密码攻击，并正在进行初步的事件分类。检测阶段的主要任务是识别和确认潜在的安全事件，以便进一步分析和响应。

-------------------

题目78-1：参考以下场景，回答3个问题 ：

Alejandro是一家大型公司的事故响应分析师。他的上班时间是午夜，一个入侵检测系统发出警报，公司的一个关键信息系统可能遭受暴力密码攻击。他在采取任何其他行动之前执行事件的初步分类。

For questions , please refer to the following scenario:

Alejandro is an incident response analyst for a large corporation. He is on the midnight shift when an intrusion detection system alerts him to a potential brute-force password attack against one of the company’s critical information systems. He performs an initial triage of the event before taking any additional action.

如果Alejandro 的初步调查确定可能发生安全事件，那么下一步应该是什么？

If Alejandro’s initial investigation determines that a security incident is likely taking place, what should be his next step?

A：调查根本原因

Investigate the root cause.

B：提交书面报告

File a written report.

C：激活事件响应小组

Activate the incident response team.

D：尝试将系统恢复到正常操作

Attempt to restore the system to normal operations.

答案:如果Alejandro的初步调查确定可能发生安全事件，那么他的下一步应该是 \*\*C：激活事件响应小组\*\*。

在确认安全事件后，激活事件响应小组是标准操作程序的一部分。事件响应小组通常由多个部门的专家组成，他们可以共同协作，进一步调查事件、评估影响、制定应对策略，并采取必要的措施来控制和缓解事件的影响。只有在事件响应小组的指导下，才能有效地进行根本原因调查、提交报告或尝试恢复系统操作。因此，激活事件响应小组是确保事件得到妥善处理的关键步骤。

-------------------

题目78-1：参考以下场景，回答3个问题 ：

Alejandro是一家大型公司的事故响应分析师。他的上班时间是午夜，一个入侵检测系统发出警报，公司的一个关键信息系统可能遭受暴力密码攻击。他在采取任何其他行动之前执行事件的初步分类。

For questions , please refer to the following scenario:

Alejandro is an incident response analyst for a large corporation. He is on the midnight shift when an intrusion detection system alerts him to a potential brute-force password attack against one of the company’s critical information systems. He performs an initial triage of the event before taking any additional action.

随着事件响应的进展，团队在哪个阶段进行根本原因分析？

As the incident response progresses, during which stage should the team conduct a rootcause analysis?

A：响应

Response

B：报告

Reporting

C：补救

Remediation

D：经验教训

Lessons learned

答案:在事件响应的过程中，根本原因分析通常在\*\*补救（Remediation）\*\*阶段进行。这个阶段的目标是识别并解决导致事件发生的根本原因，以防止类似事件再次发生。因此，正确答案是：

\*\*C：补救\*\*

\*\*Remediation\*\*

-------------------

题目79：Barry最近收到Melody的消息，Melody使用对称加密法加密。Barry使用什么密钥来解密消息？

Barry recently received a message from Melody that Melody encrypted using symmetric cryptography. What key should Barry use to decrypt the message?

A：Barry的公钥

Barry’s public key

B：Barry的私钥

Barry’s private key

C：Melody的公钥

Melody’s public key

D：共享密钥

Shared secret key

答案:在对称加密法中，加密和解密使用的是同一个密钥。因此，Barry需要使用的密钥是Melody用来加密消息的那个密钥。这个密钥是双方事先共享的，所以被称为共享密钥。

正确答案是：

D：共享密钥

Shared secret key

-------------------

题目80：在对应用程序进行100%覆盖的自动功能测试后，最可能存在哪种类型的错误？

After you do automated functional testing with 100 percent coverage of an application, what type of error is most likely to remain?

A：业务逻辑错误

Business logic errors

B：输入验证错误

Input validation errors

C：运行时错误

Runtime errors

D：错误处理错误

Error handling errors

答案:在对应用程序进行100%覆盖的自动功能测试后，最可能存在的错误类型是 \*\*A：业务逻辑错误\*\*（Business logic errors）。

### 原因分析：

- \*\*功能测试\*\*主要关注的是应用程序的功能是否符合预期，通常是通过模拟用户操作来验证系统的行为。

- \*\*100%覆盖\*\*意味着所有的功能路径和输入组合都被测试到了，但这并不意味着所有的业务逻辑都被正确实现。

- \*\*业务逻辑错误\*\*通常涉及复杂的规则和条件，可能在功能测试中被遗漏，尤其是当测试用例没有覆盖所有可能的业务场景时。

- 其他选项（如输入验证错误、运行时错误、错误处理错误）通常在功能测试中更容易被发现，因为它们往往会导致明显的异常或错误行为。

因此，即使功能测试覆盖率达到100%，业务逻辑错误仍然可能隐藏在复杂的业务规则中，难以被发现。

-------------------

题目81：在事件响应过程的哪个阶段，安全专业人员对过程本身进行分析，以确定是否需要作出任何改进？

During what phase of the incident response process would security professionals analyze the process itself to determine whether any improvements are warranted?

A：经验教训

Lessons learned

B：修复

Remediation

C：恢复

Recovery

D：报告

Reporting

答案:在事件响应过程中，安全专业人员会在“经验教训”（Lessons learned）阶段对过程本身进行分析，以确定是否需要作出任何改进。这个阶段通常是在事件处理完毕后进行的，目的是回顾整个事件响应过程，识别其中的不足和成功之处，以便在未来的事件响应中提高效率和效果。

因此，正确答案是：

A：经验教训

Lessons learned

-------------------

题目82：哪项美国法律禁止删除版权所有者对受版权保护作品的保护机制？

What U.S. law prevents the removal of protection mechanisms placed on a copyrighted work by the copyright holder?

A：HIPAA

HIPAA

B：DMCA

DMCA

C：GLBA

GLBA

D：ECPA

ECPA

答案:正确答案是 B：DMCA。

DMCA（Digital Millennium Copyright Act，数字千年版权法）是美国的一项法律，旨在保护数字内容的版权。该法律特别禁止删除或绕过版权所有者对受版权保护作品所设置的保护机制（如数字版权管理，DRM）。因此，DMCA 是防止删除版权保护机制的法律。

其他选项：

- A：HIPAA（Health Insurance Portability and Accountability Act，健康保险可携性和责任法案）是关于健康信息隐私和安全的法律。

- C：GLBA（Gramm-Leach-Bliley Act，格雷姆-里奇-布莱利法案）是关于金融机构隐私保护的法律。

- D：ECPA（Electronic Communications Privacy Act，电子通信隐私法）是关于电子通信隐私保护的法律。

-------------------

题目83：Linda 正在为她的组织选择灾难恢复设施，她希望尽可能保持与其他组织的独立性。她想选择一个平衡成本和恢复时间的设施，允许在宣布灾难后大约一周内激活。她应该选择什么类型的设施？

Linda is selecting a disaster recovery facility for her organization, and she wants to retain independence from other organizations as much as possible. She would like to choose a facility that balances cost and recovery time, allowing activation in about one week after a disaster is declared. What type of facility should she choose?

A：冷站点

Cold site

B：温站点

Warm site

C：互惠协议

Mutual assistance agreement

D：热站点

Hot site

答案:Linda 正在为她的组织选择灾难恢复设施，她希望尽可能保持与其他组织的独立性，并且希望选择一个平衡成本和恢复时间的设施，允许在宣布灾难后大约一周内激活。根据这些要求，她应该选择 \*\*温站点（Warm site）\*\*。

### 选项分析：

- \*\*A：冷站点（Cold site）\*\*

冷站点是一个基本的设施，通常只有电源、网络和物理空间，但没有预先配置的硬件或软件。恢复时间较长，可能需要几天到几周的时间来完全恢复运营。虽然成本较低，但恢复时间不符合 Linda 的要求。

- \*\*B：温站点（Warm site）\*\*

温站点介于冷站点和热站点之间，具备部分预先配置的硬件和软件，但可能没有实时数据同步。恢复时间通常在几小时到几天之间，成本适中。这符合 Linda 对恢复时间（大约一周内）和成本平衡的需求。

- \*\*C：互惠协议（Mutual assistance agreement）\*\*

互惠协议是与其他组织达成的协议，在灾难发生时共享资源。这种方式依赖于其他组织的可用性和合作，无法保证独立性，也不符合 Linda 的需求。

- \*\*D：热站点（Hot site）\*\*

热站点是完全配置好的设施，具备实时数据同步和即时恢复能力。恢复时间最短（通常在几小时内），但成本最高。这超出了 Linda 对成本和恢复时间的平衡要求。

### 结论：

\*\*B：温站点（Warm site）\*\* 是最适合 Linda 的选择，因为它提供了适中的成本和合理的恢复时间，同时保持了组织的独立性。

-------------------

题目84：Helen的组织处理了大量高度敏感的信息。为了帮助解决这一风险，她购买了网络责任保险单。海伦正在采取什么类型的风险处置措施？

Helen’s organization handles large quantities of highly sensitive information. To help address this risk, she purchased a cyberliability insurance policy. What type of risk response action is Helen taking?

A：转移

Transfer

B：规避

Avoid

C：缓解

Mitigate

D：接受

Accept

答案:题目84的正确答案是：

A：转移

Transfer

解析：Helen通过购买网络责任保险单，将潜在的财务风险转移给了保险公司。这是一种风险转移的策略，因为她并没有试图完全避免风险（规避），也没有采取措施减少风险发生的可能性或影响（缓解），而是选择通过保险来分担可能的经济损失。因此，她采取的是风险转移措施。

-------------------

题目85：什么类型的渗透测试提供渗透测试范围的详细信息(包括测试选用的系统)，但是测试者不能掌握系统或者网络的配置等全部信息？

What type of penetration testing provides detail on the scope of a penetration testincluding items like what systems would be targeted-but does not provide full visibility into the configuration or other details of the systems or networks the penetration tester must test?

A：晶盒测试

Crystal box

B：白盒测试

White box

C：黑盒测试

Black box

D：灰盒测试

Gray box

答案:正确答案是：D：灰盒测试（Gray box）

灰盒测试是一种介于白盒测试和黑盒测试之间的渗透测试方法。在这种测试中，测试者会获得一些关于目标系统的信息，例如系统的部分配置、网络结构或某些特定的系统细节，但不会获得系统的完整信息。这种测试方法模拟了一个攻击者可能已经获得了一些内部信息的情况，但并没有完全掌握系统的所有细节。

- \*\*白盒测试（White box）\*\*：测试者拥有系统的完整信息，包括配置、源代码、网络架构等。

- \*\*黑盒测试（Black box）\*\*：测试者没有任何关于系统的内部信息，完全模拟外部攻击者的视角。

- \*\*灰盒测试（Gray box）\*\*：测试者拥有部分信息，介于白盒和黑盒之间。

因此，灰盒测试最符合题目描述的情况。

-------------------

题目86：Joanna想实施多因素身份认证，以限制进入其建筑内的工作区。以下哪对控制最能满足她的要求？

Joanna would like to implement multifactor authentication for access to a restricted work area in her building. Which pairing of controls would best meet her requirement?

A：ID卡和PIN

ID card and PIN

B：密码和视网膜扫描

Password and retinal scan

C：ID卡和访问令牌

ID card and access token

D：视网膜扫描和指纹扫描

Retinal scan and fingerprint scan

答案:多因素身份认证（Multifactor Authentication, MFA）通常要求用户提供两种或以上的认证因素，这些因素通常分为以下几类：

1. \*\*知识因素\*\*（Something you know）：如密码、PIN码等。

2. \*\*持有因素\*\*（Something you have）：如ID卡、访问令牌、手机等。

3. \*\*生物特征因素\*\*（Something you are）：如指纹、视网膜扫描、面部识别等。

为了满足多因素身份认证的要求，Joanna需要选择来自不同类别的认证因素。让我们分析一下每个选项：

- \*\*A：ID卡和PIN\*\*

- ID卡属于“持有因素”，PIN属于“知识因素”。这两个因素来自不同的类别，因此符合多因素身份认证的要求。

- \*\*B：密码和视网膜扫描\*\*

- 密码属于“知识因素”，视网膜扫描属于“生物特征因素”。这两个因素也来自不同的类别，符合多因素身份认证的要求。

- \*\*C：ID卡和访问令牌\*\*

- ID卡和访问令牌都属于“持有因素”。这两个因素来自同一类别，因此不符合多因素身份认证的要求。

- \*\*D：视网膜扫描和指纹扫描\*\*

- 视网膜扫描和指纹扫描都属于“生物特征因素”。这两个因素来自同一类别，因此不符合多因素身份认证的要求。

因此，\*\*选项A和选项B\*\*都符合多因素身份认证的要求。但是，通常在实际应用中，\*\*选项B（密码和视网膜扫描）\*\*被认为是更安全的组合，因为生物特征因素（如视网膜扫描）比持有因素（如ID卡）更难伪造或窃取。

\*\*最终答案：B：密码和视网膜扫描\*\*

-------------------

题目87：现代以太网使用什么样的网络拓扑？

What network topology is used by modern-day Ethernet networks?

A：星型

Star

B：网状

Mesh

C：环型

Ring

D：总线

Bus

答案:现代以太网通常使用星型拓扑（Star Topology）。在星型拓扑中，所有的网络设备都连接到一个中央集线器或交换机上。这种拓扑结构简化了网络的维护和故障排除，因为每个设备都独立连接到中央节点，单个设备的故障不会影响整个网络的运行。

因此，正确答案是：

A：星型

Star

-------------------

题目88：Reed希望在他的网络中添加功能，使他能够对远程Web服务器上隐藏其用户的身份。以下哪种工具最能满足他的需求？

Reed would like to add capabilities to his network that allow him to hide the identities of his users from remote web servers. Which one of the following tools would best meet his needs?

A：代理服务器

Proxy server

B：内容过滤器

Content filter

C：恶意软件过滤器

Malware filter

D：缓存服务器

Caching server

答案:Reed希望在他的网络中添加功能，使他能够对远程Web服务器上隐藏其用户的身份。以下哪种工具最能满足他的需求？

答案是：\*\*A：代理服务器 (Proxy server)\*\*

代理服务器可以隐藏用户的真实IP地址，使得远程Web服务器只能看到代理服务器的IP地址，从而保护用户的身份不被暴露。其他选项如内容过滤器、恶意软件过滤器和缓存服务器主要用于不同的目的，如过滤内容、防止恶意软件或提高访问速度，但它们并不直接用于隐藏用户身份。

-------------------

题目89：Evelyn正在准备一项培训计划，该计划将为经常出国旅行的用户提供网络安全建议。以下哪个主题需要特殊培训，以确保用户不会违反美国出口管制法律？

Evelyn is preparing a training program that will provide cybersecurity advice to users who often travel internationally. Which of the following topics requires special training to ensure that users do not run afoul of U.S. export control laws?

A：加密软件

Encryption software

B：内容过滤

Content filtering

C：防火墙规则

Firewall rules

D：网络钓鱼模拟

Phishing simulations

答案:题目中提到的美国出口管制法律主要涉及对某些技术和产品的出口进行限制，以防止这些技术和产品被用于军事或其他可能威胁美国国家安全的目的。加密软件（选项A）通常受到这些法律的严格管制，因为强大的加密技术可以被视为一种“双重用途”技术，既可用于民用也可用于军事目的。

因此，对于经常出国旅行的用户来说，了解如何合法地携带和使用加密软件是非常重要的，以避免无意中违反美国的出口管制法律。其他选项（内容过滤、防火墙规则、网络钓鱼模拟）虽然也是网络安全的重要方面，但它们通常不涉及出口管制法律的问题。

所以，正确答案是：

A：加密软件

Encryption software

-------------------

题目90：Skip需要将文件从他的PC传输到远程服务器。他应该使用什么协议，而不是FTP？

Skip needs to transfer files from his PC to a remote server. What protocol should he use instead of FTP?

A：SCP

SCP

B：SSH

SSH

C：HTTP

HTTP

D：Telnet

Telnet

答案:Skip 需要将文件从他的 PC 传输到远程服务器，而不使用 FTP。在这种情况下，最合适的协议是 \*\*SCP\*\*（Secure Copy Protocol）。

\*\*SCP\*\* 是一种基于 SSH（Secure Shell）的文件传输协议，它提供了加密的文件传输功能，比 FTP 更安全。FTP 传输数据时是明文的，容易被拦截和窃取，而 SCP 通过 SSH 加密传输数据，确保了数据的安全性。

其他选项的解释：

- \*\*SSH\*\*：虽然 SSH 可以用于远程登录和命令执行，但它本身并不是专门用于文件传输的协议。

- \*\*HTTP\*\*：HTTP 主要用于网页浏览，不适合用于文件传输。

- \*\*Telnet\*\*：Telnet 是一种不安全的远程登录协议，不适合用于文件传输。

因此，正确答案是：

\*\*A：SCP\*\*

-------------------

题目91：Ben在纽约的商业网络服务收集来自加利福尼亚州居民的个人信息。加州在线隐私保护法案要求Ben做什么？

Ben’s New York-based commercial web service collects personal information from California residents. What does the California Online Privacy Protection Act require Ben to do to be compliant?

A：Ben必须加密他收到的所有个人数据

Ben must encrypt all personal data he receives.

B：Ben必须遵守欧盟DPD

Ben must comply with the EU GDPR.

C：Ben必须在他的网站上发布一个显眼的隐私政策

Ben must have a conspicuously posted privacy policy on his site.

D：Ben必须为其网站的用户提供通知和选择

Ben must provide notice and choice for users of his website.

答案:加州在线隐私保护法案（California Online Privacy Protection Act，简称CalOPPA）要求任何收集加州居民个人信息的商业网站或在线服务必须在其网站上发布一个显眼的隐私政策。这个隐私政策需要详细说明收集的个人信息的类型、如何使用这些信息、以及这些信息是否会与第三方共享等内容。

因此，正确答案是：

C：Ben必须在他的网站上发布一个显眼的隐私政策

Ben must have a conspicuously posted privacy policy on his site.

其他选项虽然也涉及隐私保护，但并不直接对应CalOPPA的具体要求。A选项提到的加密数据是数据安全的一部分，但不是CalOPPA的明确要求；B选项提到的欧盟DPD（数据保护指令）是欧盟的法律，与加州的法律无关；D选项提到的通知和选择是隐私保护的一部分，但CalOPPA更具体地要求的是隐私政策的发布。

-------------------

题目92：Grayson正在审查其组织的密码策略，并希望遵循流行的最佳实践。密码的建议有效期是多久？

Grayson is reviewing his organization’s password policies and would like to follow modern best practices. What is the recommended expiration period for passwords?

A：30天

30 days

B：90天

90 days

C：180天

180 days

D：无

None

答案:根据现代密码安全最佳实践，频繁强制更改密码可能会导致用户选择较弱的密码或重复使用旧密码，从而降低安全性。因此，许多安全专家和组织（如美国国家标准与技术研究院，NIST）建议取消定期强制更改密码的要求，除非有证据表明密码已经泄露。

因此，最合适的答案是：

\*\*D：无\*\*

\*\*None\*\*

-------------------

题目93：一个学院和大学联盟最近致力于整合他们的认证系统，以便在一个机构注册的学生可以使用他们的证书访问其他机构的服务。什么术语最能描述这种安排？

A consortium of colleges and universities recently worked to integrate their authentication systems so that students registered at one institution may use their credentials to access services at other institutions. What term best describes this arrangement?

A：联合

Federation

B：身份证明

Identity proofing

C：注册

Enrollment

D：配置

Provisioning

答案:题目描述的是一个学院和大学联盟整合他们的认证系统，使得在一个机构注册的学生可以使用他们的证书访问其他机构的服务。这种安排最符合“联合”（Federation）的概念。在信息技术和网络安全领域，联合身份认证（Federated Identity）允许多个组织共享身份认证系统，用户在一个组织中的身份认证可以在其他组织中也被认可和使用。

因此，正确答案是：

A：联合

Federation

-------------------

题目94：Olivia正在选择一种新的生物特征认证技术，并正在考虑购买虹膜扫描仪。与大多数其他类型的生物识别因素相比，虹膜扫描有什么优势？

Olivia is selecting a new biometric authentication technology and is considering purchasing iris scanners. What advantage do iris scans have over most other types of biometric factors?

A：虹膜扫描仪更难以欺骗

Iris scanners are harder to deceive.

B：虹膜的变化没有其他因素那么大

Irises don’t change as much as other factors.

C：虹膜扫描仪比其他因素更便宜

Iris scanners are cheaper than other factors.

D：虹膜不容易轻易复制

Iris scans cannot be easily replicated.

答案:题目94的正确答案是：A：虹膜扫描仪更难以欺骗 (Iris scanners are harder to deceive.)

解析：

虹膜扫描技术是一种高度精确的生物特征认证方法。虹膜是人眼中彩色的环形区域，其图案在每个人出生后的早期就固定下来，并且在一生中几乎不会改变。这种独特性使得虹膜扫描成为一种非常安全的认证方式。以下是虹膜扫描的一些优势：

1. \*\*高独特性\*\*：每个人的虹膜图案都是独一无二的，即使是双胞胎的虹膜也不相同。

2. \*\*难以伪造\*\*：虹膜图案复杂且难以复制，因此虹膜扫描仪更难以被欺骗或伪造。

3. \*\*非接触式\*\*：虹膜扫描通常是非接触式的，用户不需要触摸设备，这提高了卫生性和用户体验。

4. \*\*高精度\*\*：虹膜扫描的误识率极低，通常比其他生物特征认证技术（如指纹或面部识别）更精确。

选项B（虹膜的变化没有其他因素那么大）虽然正确，但不是虹膜扫描的主要优势。选项C（虹膜扫描仪比其他因素更便宜）不正确，因为虹膜扫描仪通常比其他生物识别设备更昂贵。选项D（虹膜不容易轻易复制）虽然正确，但不如选项A全面。

因此，最合适的答案是A：虹膜扫描仪更难以欺骗。

-------------------

题目95：Matthew、Richard和Christopher想要使用对称加密技术相互交换信息。他们希望确保每个人都可以私下向另一个人发送消息，而第三人无法阅读消息。他们需要多少个密钥？

Matthew, Richard, and Christopher would like to exchange messages with each other using symmetric cryptography. They want to ensure that each individual can privately send a message to another individual without the third person being able to read the message. How many keys do they need?

A：1

1

B：2

2

C：3

3

D：6

6

答案:在对称加密技术中，每对通信双方需要共享一个唯一的密钥，以确保他们之间的通信是私密的，而第三方无法解密。对于三个人（Matthew、Richard和Christopher）来说，他们之间可以形成以下通信对：

1. Matthew 和 Richard

2. Matthew 和 Christopher

3. Richard 和 Christopher

因此，他们需要为每一对通信双方生成一个独立的密钥。这意味着总共需要3个密钥。

所以，正确答案是：

C：3

-------------------

题目96：Colleen负责保护信用卡号，这是她所在组织努力遵守PCI DSS的一部分。她想选择适当的控制，来保护通过网络传输的这些号码。以下哪种控制最能满足这种需求？

Colleen is responsible for protecting credit card numbers as part of her organization’s efforts to comply with PCI DSS. She would like to select an appropriate control to protect those numbers while in transit over the network. Which of the following controls would best meet this need?

A：FDE

FDE

B：SSL

SSL

C：TPM

TPM

D：TLS

TLS

答案:题目是关于选择适当的控制来保护通过网络传输的信用卡号，以符合PCI DSS（支付卡行业数据安全标准）的要求。PCI DSS要求保护持卡人数据在传输过程中的安全，通常通过加密来实现。

选项分析：

A. FDE（全盘加密）：FDE主要用于加密存储在设备上的数据，而不是在传输过程中的数据。因此，FDE不符合保护网络传输数据的需求。

B. SSL（安全套接字层）：SSL是一种早期的加密协议，用于保护网络传输中的数据。然而，SSL已经被认为是不安全的，并且已经被TLS（传输层安全）所取代。

C. TPM（可信平台模块）：TPM是一种硬件安全模块，用于存储加密密钥和保护设备上的数据。它不直接用于保护网络传输中的数据。

D. TLS（传输层安全）：TLS是SSL的继任者，是一种广泛使用的加密协议，用于保护网络传输中的数据。TLS提供了强大的加密和认证机制，非常适合用于保护信用卡号等敏感数据在传输过程中的安全。

因此，最能满足保护通过网络传输的信用卡号需求的选项是D：TLS。

-------------------

题目97：Joe担心电子邮件消息的机密性，因为他们将使用互联网将信息从组织的服务器传输到最终目的地。Joe确保电子邮件机密性的最佳方法是什么？

Joe is concerned about the confidentiality of email messages as they are transiting the internet from his organization’s servers to their final destination. What is the best way that Joe can ensure email confidentiality in motion?

A：在客户端和服务器之间使用TLS

Use TLS between the client and server.

B：在客户端和服务器之间使用SSL

Use SSL between the client and server.

C：加密电子邮件内容

Encrypt the email content.

D：使用数字签名

Use a digital signature.

答案:Joe 担心电子邮件在传输过程中的机密性，确保电子邮件在传输过程中机密性的最佳方法是加密电子邮件内容。虽然使用 TLS（传输层安全性协议）可以在客户端和服务器之间提供加密的通信通道，但它主要保护的是传输过程中的数据，而不是电子邮件内容本身。SSL（安全套接字层）是 TLS 的前身，现在已经被 TLS 取代，因此选项 B 不是最佳选择。数字签名主要用于验证电子邮件的来源和完整性，而不是保护其机密性。

因此，最佳方法是 \*\*C：加密电子邮件内容\*\*。通过加密电子邮件内容，即使电子邮件在传输过程中被截获，内容也无法被读取，从而确保其机密性。

-------------------

题目98：Brenda组织的订单处理应用程序是基于Web的，在数据泄露后，她分析了Web服务器日志。她在日志文件中找到一个条目，用户在下订单时输入了以下信息作为他的姓氏：Smith&rsquo;; DROP TABLE orders; -- 该用户在尝试什么类型的攻击？

Brenda is analyzing the web server logs after a successful compromise of her organization’s web-based order processing application. She finds an entry in the log file showing that a user entered the following information as his last name when placing an order: Smith’;DROP TABLE orders;-- What type of attack was attempted?

A：缓冲区溢出

Buffer overflow

B：跨站点脚本

Cross-site scripting

C：跨站点请求伪造

Cross-site request forgery

D：SQL 注入

SQL injection

答案:正确答案是 D：SQL 注入（SQL injection）。

解释：

用户在姓氏字段中输入的内容 `Smith'; DROP TABLE orders; --` 是一个典型的 SQL 注入攻击尝试。这个输入的目的是通过在 SQL 查询中插入恶意代码来操纵数据库。具体来说：

- `Smith'` 是用户输入的姓氏。

- `;` 用于结束当前的 SQL 语句。

- `DROP TABLE orders;` 是一个 SQL 命令，用于删除名为 `orders` 的表。

- `--` 是 SQL 中的注释符号，用于注释掉后续的 SQL 代码，以防止语法错误。

如果应用程序没有对用户输入进行适当的验证和过滤，这个输入可能会导致数据库执行 `DROP TABLE orders;` 命令，从而删除 `orders` 表，造成数据丢失。

其他选项的解释：

- A：缓冲区溢出（Buffer overflow）是指向程序的缓冲区写入超过其容量的数据，导致内存溢出，通常与 SQL 注入无关。

- B：跨站点脚本（Cross-site scripting, XSS）是一种攻击方式，攻击者通过在网页中注入恶意脚本，从而在用户浏览器中执行这些脚本，通常与 SQL 注入无关。

- C：跨站点请求伪造（Cross-site request forgery, CSRF）是一种攻击方式，攻击者诱使用户在不知情的情况下执行某些操作，通常与 SQL 注入无关。

因此，正确答案是 D：SQL 注入。

-------------------

题目99：Hannah的组织正在实施一种依赖SAML的新用户身份认证方法。她希望防止流量被窃听，并确保SAML流量不会被攻击者伪造。她应该做什么才能防止这两种类型的攻击？

Hannah’s organization is implementing a new approach to user authentication that relies upon SAML. She would like to protect against eavesdropping on this traffic and also ensure that SAML traffic is not forged by an attacker. What should she do to protect against both types of attack?

A：使用SAML的安全模式提供安全身份验证

Use SAML’s secure mode to provide secure authentication.

B：使用一个强大的密码套件实现TLS，这将防止这两种类型的攻击

Implement TLS using a strong cipher suite, which will protect against both types of attacks.

C：使用强密码套件实现TLS，并使用数字签名

Implement TLS using a strong cipher suite and use digital signatures.

D：使用强密码套件和消息散列实现TLS

Implement TLS using a strong cipher suite and message hashing.

答案:为了确保SAML流量不被窃听和伪造，Hannah需要采取以下措施：

1. \*\*防止窃听\*\*：通过使用TLS（传输层安全性协议）来加密通信，可以防止流量被窃听。TLS使用强大的密码套件来确保数据在传输过程中的机密性和完整性。

2. \*\*防止伪造\*\*：通过使用数字签名来验证SAML消息的真实性和完整性，可以防止攻击者伪造SAML流量。数字签名确保消息在传输过程中没有被篡改，并且确实来自预期的发送者。

因此，正确的做法是结合使用TLS和数字签名来保护SAML流量。

\*\*正确答案是：\*\*

C：使用强密码套件实现TLS，并使用数字签名

Implement TLS using a strong cipher suite and use digital signatures.

-------------------

题目100：BCP流程的目标是什么？

What is the goal of the BCP process?

A：RTO &lt; MTD

RTO &lt; MTD

B：MTD &lt; RTO

MTD &lt; RTO

C：RPO &lt; MTD

RPO &lt; MTD

D：MTD &lt; RPO

MTD &lt; RPO

答案:BCP（业务连续性计划，Business Continuity Planning）流程的主要目标是确保在发生灾难或重大中断事件时，企业能够迅速恢复关键业务功能，并尽量减少对业务运营的影响。BCP的核心目标包括确定恢复时间目标（RTO，Recovery Time Objective）和最大容忍中断时间（MTD，Maximum Tolerable Downtime）。

- \*\*RTO\*\* 是指从灾难发生到业务功能恢复所需的时间。

- \*\*MTD\*\* 是指业务能够承受的最长中断时间，超过这个时间可能会导致严重的业务影响。

因此，BCP流程的目标是确保 \*\*RTO < MTD\*\*，即恢复时间目标应小于最大容忍中断时间，以确保业务能够在可接受的时间内恢复。

所以，正确答案是：

\*\*A：RTO < MTD\*\*

-------------------

题目101：在事故响应过程的哪个阶段，管理员设计新的安全控制来防止事故再次发生？

During which phase of the incident response process would administrators design new security controls intended to prevent a recurrence of the incident?

A：报告

Reporting

B：恢复

Recovery

C：修复

Remediation

D：经验教训

Lessons learned

答案:在事故响应过程中，管理员设计新的安全控制来防止事故再次发生的阶段是 \*\*D：经验教训（Lessons learned）\*\*。

在这个阶段，团队会回顾整个事故响应过程，分析事故的原因和响应措施的有效性，并从中吸取教训。基于这些分析，管理员会设计新的安全控制措施或改进现有的控制措施，以防止类似的事故再次发生。

因此，正确答案是 \*\*D：经验教训（Lessons learned）\*\*。

-------------------

题目102：Bethany收到了一个同事的电子邮件，其中有一个不寻常的附件，名为smime.p7s，她没见过该附件，也不知道该怎么办。该附件最可能是什么？

Bethany received an email from one of her colleagues with an unusual attachment named smime.p7s. She does not recognize the attachment and is unsure what to do. What is the most likely scenario?

A：这是一封加密的电子邮件

This is an encrypted email message.

B：这是一个网络钓鱼攻击

This is a phishing attack.

C：这是嵌入式恶意软件

This is embedded malware.

D：这是一个欺骗攻击

This is a spoofing attack.

答案:题目102的正确答案是：

A：这是一封加密的电子邮件

This is an encrypted email message.

解释：

- \*\*smime.p7s\*\* 是 S/MIME（Secure/Multipurpose Internet Mail Extensions）加密邮件的附件格式。S/MIME 是一种用于加密和签名电子邮件的标准，通常用于确保邮件的机密性和完整性。

- 这种附件通常包含加密的邮件内容或数字签名，而不是恶意软件或钓鱼攻击的一部分。

- 如果 Bethany 不确定如何处理这个附件，她可以联系发件人确认邮件的真实性，或者使用支持 S/MIME 的邮件客户端来解密和查看邮件内容。

其他选项（B、C、D）虽然也是网络安全中的常见威胁，但与 \*\*smime.p7s\*\* 附件的性质不符。

-------------------

题目103-1：参考以下场景，回答3个问题：

Kim是飞机系统公司(ASI)的数据库安全管理员。ASI是从事飞机航空电子系统设计和分析的军事承包商，代表政府和其他政府承包商定期处理分类信息。Kim关注确保ASI数据库中存储的信息的安全性。

Kim的数据库是一个多级安全数据库，不同的ASI员工有不同的安全许可。数据库包含关于使用ASI系统的军用飞机的位置的信息，以允许ASI工作人员监控这些系统。

For questions , please refer to the following scenario:

Kim is the database security administrator for Aircraft Systems, Inc. (ASI). ASI is a military contractor engaged in the design and analysis of aircraft avionics systems and regularly handles classified information on behalf of the government and other government contractors. Kim is concerned about ensuring the security of information stored in ASI databases.

Kim’s database is a multilevel security database, and different ASI employees have different security clearances. The database contains information on the location of military aircraft containing ASI systems to allow ASI staff to monitor those systems.

Kim得知，军方正在计划一个涉及ASI飞机的机密任务。她担心未获准执行任务的员工可能会通过注意到许多飞机前往该地区而得知此事。个别员工有权了解某个飞机的运动，但他们无权了解整体任务。Kim担心什么类型的攻击？

Kim learned that the military is planning a classified mission that involves some ASI aircraft. She is concerned that employees not cleared for the mission may learn of it by noticing the movement of many aircraft to the region. Individual employees are cleared to know about the movement of an individual aircraft, but they are not cleared to know about the overall mission. What type of attack is Kim concerned about?

A：聚合

Aggregation

B：SQL注入

SQL injection

C：推理

Inference

D：多级安全

Multilevel security

答案:Kim担心的攻击类型是 \*\*A：聚合（Aggregation）\*\*。

### 解释：

- \*\*聚合攻击（Aggregation Attack）\*\*：这种攻击发生在用户通过访问多个低级别的信息片段，间接推断出更高级别的敏感信息。在Kim的场景中，个别员工有权了解单个飞机的运动信息，但如果他们注意到多个飞机都前往同一地区，可能会推断出存在一个更高级别的机密任务。这种通过组合多个低级别信息来推断出高级别信息的行为就是聚合攻击。

- \*\*SQL注入（SQL Injection）\*\*：这是一种通过恶意SQL代码操纵数据库的攻击方式，与Kim的场景无关。

- \*\*推理攻击（Inference Attack）\*\*：推理攻击通常是指通过已知的信息推断出未知的敏感信息。虽然Kim的场景中也有一定的推理成分，但更准确地说，这是通过聚合多个信息片段来推断出更高级别的信息，因此聚合攻击更为贴切。

- \*\*多级安全（Multilevel Security）\*\*：这是数据库的一种安全机制，用于控制不同安全级别的用户访问不同级别的信息。它本身不是一种攻击类型。

因此，Kim最担心的是 \*\*聚合攻击\*\*。

-------------------

题目103-1：参考以下场景，回答3个问题：

Kim是飞机系统公司(ASI)的数据库安全管理员。ASI是从事飞机航空电子系统设计和分析的军事承包商，代表政府和其他政府承包商定期处理分类信息。Kim关注确保ASI数据库中存储的信息的安全性。

Kim的数据库是一个多级安全数据库，不同的ASI员工有不同的安全许可。数据库包含关于使用ASI系统的军用飞机的位置的信息，以允许ASI工作人员监控这些系统。

For questions , please refer to the following scenario:

Kim is the database security administrator for Aircraft Systems, Inc. (ASI). ASI is a military contractor engaged in the design and analysis of aircraft avionics systems and regularly handles classified information on behalf of the government and other government contractors. Kim is concerned about ensuring the security of information stored in ASI databases.

Kim’s database is a multilevel security database, and different ASI employees have different security clearances. The database contains information on the location of military aircraft containing ASI systems to allow ASI staff to monitor those systems.

Kim可使用什么技术来防止没有任务许可的员工了解飞机的真实位置？

What technique can Kim employ to prevent employees not cleared for the mission from learning the true location of the aircraft?

A：输入验证

Input validation

B：多实例化

Polyinstantiation

C：参数化

Parameterization

D：服务器端验证

Server-side validation

答案:Kim可以使用多实例化（Polyinstantiation）技术来防止没有任务许可的员工了解飞机的真实位置。

多实例化是一种数据库安全技术，它允许在同一数据库中存储多个版本的相同数据，每个版本对应不同的安全级别或用户权限。通过这种方式，不同安全级别的用户只能访问与其权限相匹配的数据版本。例如，对于没有任务许可的员工，数据库可以显示一个虚假的或模糊的飞机位置信息，而不是真实的精确位置。

因此，正确答案是：

B：多实例化

Polyinstantiation

-------------------

题目103-1：参考以下场景，回答3个问题：

Kim是飞机系统公司(ASI)的数据库安全管理员。ASI是从事飞机航空电子系统设计和分析的军事承包商，代表政府和其他政府承包商定期处理分类信息。Kim关注确保ASI数据库中存储的信息的安全性。

Kim的数据库是一个多级安全数据库，不同的ASI员工有不同的安全许可。数据库包含关于使用ASI系统的军用飞机的位置的信息，以允许ASI工作人员监控这些系统。

For questions , please refer to the following scenario:

Kim is the database security administrator for Aircraft Systems, Inc. (ASI). ASI is a military contractor engaged in the design and analysis of aircraft avionics systems and regularly handles classified information on behalf of the government and other government contractors. Kim is concerned about ensuring the security of information stored in ASI databases.

Kim’s database is a multilevel security database, and different ASI employees have different security clearances. The database contains information on the location of military aircraft containing ASI systems to allow ASI staff to monitor those systems.

Kim的数据库通过使用其尾号唯一地标识飞机。以下哪一个术语不一定能够准确描述尾号？

Kim’s database uniquely identifies aircraft by using their tail number. Which one of the following terms would not necessarily accurately describe the tail number?

A：数据库字段

Database field

B：外键

Foreign key

C：主键

Primary key

D：候选键

Candidate key

答案:在数据库中，尾号（tail number）被用来唯一标识飞机，这意味着尾号在数据库表中具有唯一性。根据数据库设计的基本原则，我们可以分析每个选项：

A. \*\*数据库字段（Database field）\*\*：尾号是数据库中的一个字段，用来存储飞机的尾号信息。这个描述是准确的。

B. \*\*外键（Foreign key）\*\*：外键是用来建立和强制两个表之间的链接的字段。它通常指向另一个表中的主键。尾号在这个场景中是用来唯一标识飞机的，而不是用来建立表之间的关系，因此尾号不一定是外键。

C. \*\*主键（Primary key）\*\*：主键是用来唯一标识表中每一行的字段。由于尾号被用来唯一标识飞机，它很可能是主键。

D. \*\*候选键（Candidate key）\*\*：候选键是能够唯一标识表中每一行的字段或字段组合。尾号具有唯一性，因此它是一个候选键。

综上所述，尾号不一定是\*\*外键（Foreign key）\*\*，因为外键的作用是建立表之间的关系，而不是唯一标识表中的记录。因此，正确答案是：

\*\*B：外键（Foreign key）\*\*

-------------------

题目104：Kim希望创建一个强制实施数据库参照完整性的密钥。她需要创建什么类型的密钥？

Kim would like to create a key that enforces referential integrity for the database. What type of key does she need to create?

A：主键

Primary key

B：外键

Foreign key

C：候选键

Candidate key

D：主密钥

Master key

答案:Kim希望创建一个强制实施数据库参照完整性的密钥。她需要创建的是 \*\*B：外键\*\*（Foreign key）。

外键用于建立和强制实施表与表之间的关系，确保一个表中的数据与另一个表中的数据保持一致。外键通常指向另一个表的主键，从而保证参照完整性。

-------------------

题目105：Doug正在选择一个软件开发生命周期模型，用于开发新业务应用程序。他有非常明确的要求，并希望选择一种早期强调开发全面文件的方法。他不需要生产快速原型或迭代改进。哪种模型最适合这种情况？

Doug is choosing a software development lifecycle model for use in a project he is leading to develop a new business application. He has clearly defined requirements and would like to choose an approach that places an early emphasis on developing comprehensive documentation. He does not have a need for the production of rapid prototypes or iterative improvement. Which model is most appropriate for this scenario?

A：敏捷

Agile

B：瀑布

Waterfall

C：螺旋

Spiral

D：DevOps

DevOps

答案:在这种情况下，最适合Doug选择的软件开发生命周期模型是 \*\*B：瀑布模型（Waterfall）\*\*。

### 原因：

1. \*\*明确的需求\*\*：Doug有非常明确的需求，瀑布模型适用于需求明确且不太可能发生变化的项目。

2. \*\*早期强调全面文档\*\*：瀑布模型在项目初期就强调详细的规划和文档编制，这与Doug的需求相符。

3. \*\*不需要快速原型或迭代改进\*\*：瀑布模型是线性的，每个阶段完成后才进入下一个阶段，不强调快速原型或迭代开发，因此符合Doug不需要这些特性的要求。

### 其他选项的分析：

- \*\*A：敏捷（Agile）\*\*：敏捷模型强调迭代开发和快速原型，适合需求不明确或可能变化的项目，与Doug的需求不符。

- \*\*C：螺旋（Spiral）\*\*：螺旋模型结合了瀑布模型和迭代开发的优点，适合高风险项目，但同样强调迭代和原型开发，不符合Doug的需求。

- \*\*D：DevOps\*\*：DevOps主要关注开发和运维的集成，强调持续交付和自动化，与Doug的需求不相关。

因此，\*\*瀑布模型（Waterfall）\*\*是最适合Doug的选择。

-------------------

题目106：哪些个人承担数据保护任务的最终责任？

Which individual bears the ultimate responsibility for data protection tasks?

A：数据所有者

Data owner

B：数据监管者

Data custodian

C：用户

User

D：审计员

Auditor

答案:在数据保护任务中，最终责任通常由数据所有者（Data Owner）承担。数据所有者是指对数据的收集、存储、处理和使用的目的和方式有最终决策权的个人或组织。他们负责确保数据的安全性、完整性和隐私性，并确保遵守相关的法律法规。

选项A：数据所有者（Data Owner）是正确的答案。

其他选项的角色如下：

- 数据监管者（Data Custodian）：负责数据的技术管理和维护，确保数据的安全性和可用性，但最终责任不在他们。

- 用户（User）：使用数据的人员，通常不承担数据保护的最终责任。

- 审计员（Auditor）：负责审查和评估数据保护措施的有效性，但不承担最终责任。

因此，正确答案是A：数据所有者（Data Owner）。

-------------------

题目107：Carla正在进行Web应用程序安全测试，并希望自动生成用于测试应用程序的输入。以下哪项工具最适合此目的？

Carla is conducting a web application security test and would like to automatically generate input that is used to test the application. Which of the following tools would be best suited for this purpose?

A：静态应用测试工具

Static application testing tool

B：白盒测试工具

White-box testing tool

C：蛮力测试工具

Brute-force testing tool

D：模糊测试工具

Fuzz testing tool

答案:Carla希望自动生成用于测试Web应用程序的输入，这种需求最适合使用模糊测试工具（Fuzz testing tool）。

\*\*解释：\*\*

- \*\*A：静态应用测试工具\*\* - 静态应用测试工具主要用于分析源代码或编译后的代码，而不涉及生成输入或执行应用程序。

- \*\*B：白盒测试工具\*\* - 白盒测试工具通常用于测试应用程序的内部结构或代码逻辑，通常需要访问源代码，并且不专注于生成输入。

- \*\*C：蛮力测试工具\*\* - 蛮力测试工具通常用于尝试所有可能的输入组合，通常用于破解密码或暴力破解，而不是生成用于安全测试的输入。

- \*\*D：模糊测试工具\*\* - 模糊测试工具专门用于生成随机、异常或无效的输入数据，以测试应用程序的鲁棒性和安全性。这种工具非常适合用于自动生成输入以测试Web应用程序的安全性。

因此，\*\*D：模糊测试工具\*\* 是最适合Carla需求的工具。

-------------------

题目108：Warren的组织最近完成了一场大规模的网络钓鱼宣传活动，他想衡量其有效性。以下哪种工具最能提供这种测量？

Warren’s organization recently completed a massive phishing awareness campaign, and he would like to measure its effectiveness. Which of the following tools would best provide this measurement?

A：调查

Survey

B：模拟

Simulation

C：代码审查

Code review

D：第三方评估

Third-party assessment

答案:要衡量网络钓鱼宣传活动的有效性，最合适的工具是 \*\*B：模拟 (Simulation)\*\*。

\*\*解释：\*\*

- \*\*A：调查 (Survey)\*\*：虽然调查可以提供员工对网络钓鱼活动的认知和态度，但它不能直接衡量员工在实际网络钓鱼攻击中的反应。

- \*\*B：模拟 (Simulation)\*\*：通过模拟真实的网络钓鱼攻击，可以测试员工在实际情境中的反应，从而直接衡量宣传活动的有效性。例如，可以发送模拟的钓鱼邮件，观察有多少员工点击了链接或提供了敏感信息。

- \*\*C：代码审查 (Code review)\*\*：代码审查主要用于检查代码的质量和安全性，与衡量网络钓鱼宣传活动的有效性无关。

- \*\*D：第三方评估 (Third-party assessment)\*\*：虽然第三方评估可以提供客观的反馈，但它通常用于评估整体安全态势，而不是专门针对网络钓鱼宣传活动的有效性。

因此，\*\*B：模拟 (Simulation)\*\* 是最能提供这种测量的工具。

-------------------

题目109：以下哪项控制在检测零日攻击方面最有效？

Which one of the following controls would be most effective in detecting zero-day attack attempts?

A：基于签名的入侵检测

Signature-based intrusion detection

B：基于异常的入侵检测

Anomaly-based intrusion detection

C：强大的补丁管理

Strong patch management

D：全盘加密

Full-disk encryption

答案:题目109的正确答案是：

\*\*B：基于异常的入侵检测 (Anomaly-based intrusion detection)\*\*

\*\*解析：\*\*

- \*\*A：基于签名的入侵检测 (Signature-based intrusion detection)\*\*：这种方法依赖于已知攻击的特征库来检测攻击。对于零日攻击（即尚未被发现或没有已知签名的攻击），基于签名的检测方法无法有效识别。

- \*\*B：基于异常的入侵检测 (Anomaly-based intrusion detection)\*\*：这种方法通过分析系统的正常行为模式，检测出与正常行为不符的异常活动。由于零日攻击通常表现出与正常行为不同的特征，基于异常的检测方法更有可能发现这些未知的攻击。

- \*\*C：强大的补丁管理 (Strong patch management)\*\*：虽然补丁管理对于防止已知漏洞被利用非常重要，但它无法直接检测零日攻击，因为零日攻击利用的是尚未被发现或修补的漏洞。

- \*\*D：全盘加密 (Full-disk encryption)\*\*：全盘加密主要用于保护数据在存储时的安全性，防止未经授权的访问。它与检测零日攻击无关。

因此，\*\*基于异常的入侵检测\*\*是最有效的控制措施，用于检测零日攻击。

-------------------

题目110：以下哪项不是(ISC)2道德规范的准则？

Which one of the following is not a canon of the (ISC)2 Code of Ethics?

A：保护社会、公共利益、必要的公众信任和信心以及基础设施

Protect society, the common good, necessary public trust and confidence, and the infra- structure.

B：及时向有关部门报告安全漏洞

Promptly report security vulnerabilities to relevant authorities.

C：以正直、诚实、公正、尽责和合法的方式行事

Act honorably, honestly, justly, responsibly, and legally.

D：为雇主提供勤勉和称职的服务

Provide diligent and competent service to principals.

答案:(ISC)² 是一个全球性的非营利组织，专注于信息安全领域的教育和认证。其道德规范（Code of Ethics）是认证专业人士必须遵守的行为准则。根据 (ISC)² 的道德规范，以下是其准则：

1. \*\*保护社会、公共利益、必要的公众信任和信心以及基础设施\*\*（Protect society, the common good, necessary public trust and confidence, and the infrastructure）。

2. \*\*以正直、诚实、公正、尽责和合法的方式行事\*\*（Act honorably, honestly, justly, responsibly, and legally）。

3. \*\*为雇主提供勤勉和称职的服务\*\*（Provide diligent and competent service to principals）。

选项 B \*\*“及时向有关部门报告安全漏洞”\*\*（Promptly report security vulnerabilities to relevant authorities）并不是 (ISC)² 道德规范的正式准则之一。虽然报告安全漏洞是信息安全专业人士的常见职责，但它并未被明确列为 (ISC)² 道德规范的准则之一。

因此，正确答案是 \*\*B\*\*。

-------------------

题目111：组织的应急响应指南应包括以下哪项？

Which one of the following components should be included in an organization’s emergency response guidelines?

A：对于事件响应者的后续响应流程

Secondary response procedures for incident responders

B：长期业务连续性协议

Long-term business continuity protocols

C：组织冷站点的激活程序

Activation procedures for the organization’s cold sites

D：订购设备的联系方式

Contact information for ordering equipment

答案:组织的应急响应指南是为了在紧急情况下提供明确的指导和步骤，以确保组织能够有效地应对和管理突发事件。这些指南通常包括立即响应措施、资源分配、沟通策略和恢复计划等。

选项A：“对于事件响应者的后续响应流程”是应急响应指南中非常重要的一部分。它确保了在初步响应之后，有明确的步骤和流程来进一步处理事件，包括评估、控制和恢复等。

选项B：“长期业务连续性协议”虽然重要，但通常属于业务连续性计划的一部分，而不是应急响应指南的主要内容。

选项C：“组织冷站点的激活程序”是灾难恢复计划的一部分，用于在主要设施不可用时启用备用设施，这通常是在应急响应之后进行的。

选项D：“订购设备的联系方式”虽然在某些情况下可能有用，但不是应急响应指南的核心内容。

因此，最合适的答案是A：“对于事件响应者的后续响应流程”。

-------------------

题目112：当Jim进入其组织的数据中心时，他必须使用智能卡和密码进入，先通过第一组门，接着第一组门关闭，然后他必须再次使用他的卡通过第二组门。这是什么类型的控制，它叫什么？

When Jim enters his organization’s data center, he has to use a smart card and code to enter and is allowed through one set of doors. The first set of doors closes, and he must then use his card again to get through a second set, which locks behind him. What type of control is this, and what is it called?

A：物理控制；单向活板门

A physical control; a one-way trapdoor

B：逻辑控制；双刷卡授权

A logical control; a dual-swipe authorization

C：指令控制；单向通道走廊

A directive control; a one-way access corridor

D：预防性访问控制；陷门

A preventive access control; a mantrap

答案:这个问题的正确答案是：

D：预防性访问控制；陷门

A preventive access control; a mantrap

解释：

Jim进入数据中心时使用的安全措施被称为“陷门”（mantrap）。这是一种物理安全控制措施，旨在通过设置两个独立的门来限制和监控进入高安全区域的人员。用户必须通过第一道门，然后第一道门关闭后才能打开第二道门。这种设计确保只有经过授权的人员才能进入，同时防止尾随（piggybacking）或未经授权的人员进入。这种控制属于预防性访问控制，因为它旨在防止未经授权的访问。

-------------------

题目113：Bill在一台总共有3个磁盘的服务器上实施了RAID 5。在不丢失数据的情况下，有多少磁盘可以发生故障？

Bill implemented RAID level 5 on a server that he operates using a total of three disks. How many disks may fail without the loss of data?

A：0

0

B：1

1

C：2

2

D：3

3

答案:在RAID 5配置中，数据被分布在多个磁盘上，并且每个磁盘上存储了奇偶校验信息。这种配置允许在其中一个磁盘发生故障时，通过其他磁盘上的数据和奇偶校验信息来重建丢失的数据。

因此，对于总共有3个磁盘的RAID 5配置，最多可以有1个磁盘发生故障而不丢失数据。如果超过1个磁盘发生故障，数据将无法完全恢复。

所以，正确答案是：

B：1

-------------------

题目114：请为下列数字标记的服务组织控制（SOC）等级，匹配与之对应SOC报告定义SOC等级：

1. SOC 1，Type 1

2. SOC 1, Type 2

3. SOC 2

4. SOC 3

SOC报表描述：

A. 一般性报告，包括与合规性和/或运营相关的控制措施有效性

B. 报告为机密性、可用性、完整性、系统隐私性，及系统所含信息的相关控制提供了预配的标准基准；一般用于限制使用；

C. 报告针对受服务组织流程影响的财务报表方面的重大错报提供风险评估，并包含服务审计员内控测试的描述、结果，及其有效性。

D．报告提供了审计员对于服务组织控制的财务声明的意见，并包含包括对服务组织系统的表述意见以及控制的适宜性的报告

Match the following numbered Service Organization Control (SOC) levels to their matching lettered SOC report descriptions:

SOC levels

1.SOC 1, Type 1

2. SOC 1, Type 2

3. SOC 2

4. SOC 3

SOC report descriptions

A.A general use report that reports on controls related to compliance and/or operations

B.A report that provides predefined, standard benchmarks for controls involving confidentiality, availability, integrity, and privacy of a system and the information it contains, generally for restricted use

C.A report that provides an assessment of the risk of material misstatement of financial statement assertions affected by the service organization’s processing and that includes a description of the service auditor’s tests of the controls and the results of the tests and their effectiveness

D.A report that provides the auditor’s opinions of financial statements about controls at the service organization and that includes a report on the opinion on the presentation of the service organization’s system as well as suitability of the controls

答案:根据题目要求，以下是SOC等级与SOC报告描述的匹配：

1. SOC 1, Type 1 - \*\*C\*\*

- 描述：报告针对受服务组织流程影响的财务报表方面的重大错报提供风险评估，并包含服务审计员内控测试的描述、结果，及其有效性。

2. SOC 1, Type 2 - \*\*D\*\*

- 描述：报告提供了审计员对于服务组织控制的财务声明的意见，并包含包括对服务组织系统的表述意见以及控制的适宜性的报告。

3. SOC 2 - \*\*B\*\*

- 描述：报告为机密性、可用性、完整性、系统隐私性，及系统所含信息的相关控制提供了预配的标准基准；一般用于限制使用。

4. SOC 3 - \*\*A\*\*

- 描述：一般性报告，包括与合规性和/或运营相关的控制措施有效性。

因此，匹配结果为：

1 - C

2 - D

3 - B

4 - A

-------------------