The AhaBulb Party Game

STUFF EVERY SECURITY PRO SHOULD KNOW

How to play (30 seconds)

1. The reader reads a card and its three answers out loud.
2. Everyone says "One, two, three, Goldilocks!" and holds up 1, 2, or 3 fingers.
3. The reader flips the card and reads the answer and the Why.
4. Everyone who was right takes a point.
5. The reader reads the joke with a straight face. Anyone laughs or groans? The reader takes a point. Nobody got it right? The reader takes a point.
6. Pass the deck left. Most points when the points run out wins.

What you need

These cards and the point tokens on the last two pages. No tokens? Use coins, buttons, pebbles, or marshmallows. 3 to 10 players, ages 8 and up.

Expert rule: Bet It

Before the reader flips the card, you may put one of your points on your answer. Right: take your normal point plus one extra. Wrong: your bet goes back to the pile. That's it.

Printing

Print single-sided, on cardstock if you have it. Cut on the dashed lines. Each card is a 3.5 x 5 inch index card. The answer half is upside down on purpose, so the table can't peek.

Cards 1 to 50 of 100. More cards and the free daily online game at sesk.info. Built 2026-10-14.

SECURITY & PRIVACY

A file's hash value no longer matches after someone edits the file. Which CIA property was affected?

- A Confidentiality
- B Integrity
- C Availability

FLIP FOR THE ANSWER

B Integrity

WHY Integrity means information is not improperly modified or destroyed. A hash works like a fingerprint, so a changed file gives a different value.

STRAIGHT FACE
Why did the hash break up with the file? It could not handle any change.

SESK.INFO #5486

SECURITY & PRIVACY

Encrypting a laptop's files mainly protects which part of the CIA triad?

- A Confidentiality
- B Integrity
- C Availability

FLIP FOR THE ANSWER

A Confidentiality

WHY Confidentiality means only authorized people can read information. Encryption scrambles the data so a thief without the key sees nothing useful.

STRAIGHT FACE
Set your wifi password to 24446666688888888. So when someone asks for it, tell them it's 12345678.

SESK.INFO #5485

SECURITY & PRIVACY

Which assurance does a digital signature add so a signer cannot later deny signing?

- A Non-repudiation
- B Obfuscation
- C Redundancy

FLIP FOR THE ANSWER

A Non-repudiation

WHY A digital signature is made with the signer's private key. Anyone can verify it with the public key, which ties the data to the signer.

STRAIGHT FACE
Why can't a signer say 'it wasn't me'? The math says it was.

SESK.INFO #5488

SECURITY & PRIVACY

A flood of fake traffic knocks a website offline. Which CIA property does this attack target?

- A Confidentiality
- B Integrity
- C Availability

FLIP FOR THE ANSWER

C Availability

WHY Availability means timely, reliable access to information and services. Denial of service attacks prevent authorized users from getting in.

STRAIGHT FACE
Why was the server so stressed? Everyone wanted a connection and nobody wanted to wait.

SESK.INFO #5487

SECURITY & PRIVACY

You sign in, and then the system decides which folders you may open. What is that second step?

- **A** Authentication
- **B** Authorization
- **C** Accounting

FLIP FOR THE ANSWER

B Authorization

WHY Authentication proves who you are. Authorization grants access privileges. Accounting, the third A, records what you did.

STRAIGHT FACE
What is the biggest lie in the entire universe? "I have read and agree to the Terms & Conditions."

SESK.INFO #5489

SECURITY & PRIVACY

What is the core premise of zero trust architecture?

- **A** Everything inside the office network is trusted
- **B** A user is trusted for the day after one login
- **C** Trust is never granted implicitly and is continually evaluated

FLIP FOR THE ANSWER

C Trust is never granted implicitly and is continually evaluated

WHY Zero trust drops the idea of a safe inside network. Every request is checked using identity, device and context, and trust is re-evaluated continuously.

STRAIGHT FACE
A zero trust door asks for ID every time you enter. Even the door's mother gets checked.

SESK.INFO #5490

SECURITY & PRIVACY

In NIST's zero trust model, which component makes the final decision to grant access to a resource?

- **A** The policy engine
- **B** The policy enforcement point
- **C** The data plane switch

FLIP FOR THE ANSWER

A The policy engine

WHY The policy engine uses enterprise policy and outside inputs to approve or deny. The policy administrator sets up or tears down the session, and the enforcement point opens and closes the connection.

STRAIGHT FACE
The policy engine never gets tired of saying no. It just calls it a decision.

SESK.INFO #5491

SECURITY & PRIVACY

Which one of these is a security control category, rather than a control type?

- **A** Preventive
- **B** Managerial
- **C** Deterrent

FLIP FOR THE ANSWER

B Managerial

WHY Categories describe what a control is made of: technical, managerial, operational or physical. Types describe what it does: preventive, deterrent, detective, corrective, compensating or directive.

STRAIGHT FACE
How many tech-support agents does it take to screw in a lightbulb? Press 1 to continue.

SESK.INFO #5492

SECURITY & PRIVACY

Which key lengths does the Advanced Encryption Standard (AES) support?

- **A** 56, 112 and 168 bits
- **B** 512, 1024 and 2048 bits
- **C** 128, 192 and 256 bits

FLIP FOR THE ANSWER

C 128, 192 and 256 bits

WHY AES is a symmetric cipher, so the same key encrypts and decrypts. Longer keys are harder to brute force, and every version works on 128-bit blocks.

STRAIGHT FACE
What form of digital payment does Superman avoid? Crypto-nite currency.

SESK.INFO #5496

SECURITY & PRIVACY

A server set up only to attract attackers so defenders can study them is called what?

- **A** A bastion host
- **B** A honeypot
- **C** A jump server

FLIP FOR THE ANSWER

B A honeypot

WHY Nobody legitimate has a reason to use a honeypot, so any traffic to it is suspicious. Defenders can watch what attackers try without risking real data.

STRAIGHT FACE
Why did the bear love the server? It smelled like honey.

SESK.INFO #5495

SECURITY & PRIVACY

Giving each user only the access needed for their assigned tasks follows which principle?

- **A** Least privilege
- **B** Separation of networks
- **C** Security through obscurity

FLIP FOR THE ANSWER

A Least privilege

WHY If an account is stolen or misused, least privilege limits the damage. Admin rights should go only to those who need them, and only when needed.

STRAIGHT FACE
Least privilege is why the intern can print but cannot delete the company.

SESK.INFO #5494

SECURITY & PRIVACY

A system cannot use the normal required control. What do you call the alternative that gives comparable protection?

- **A** A directive control
- **B** A deterrent control
- **C** A compensating control

FLIP FOR THE ANSWER

C A compensating control

WHY Sometimes a legacy system cannot run the standard control. A compensating control, such as network isolation, delivers equivalent or comparable protection another way.

STRAIGHT FACE
A compensating control is like using a ladder when the elevator is broken. You still reach the floor.

SESK.INFO #5493

SECURITY & PRIVACY

How long is a SHA-256 hash output, called the message digest?

- **A** 160 bits
- **B** 256 bits
- **C** 512 bits

FLIP FOR THE ANSWER

B 256 bits

WHY SHA-256 turns input of any size into a fixed 256-bit digest. SHA-1 gives 160 bits and SHA-512 gives 512 bits.

STRAIGHT FACE
Why did the hash fit every file? It is a one size fits all kind of function.

SESK.INFO #5498

SECURITY & PRIVACY

Which key does a recipient use to verify a digital signature?

- **A** The signer's public key
- **B** The signer's private key
- **C** The recipient's private key

FLIP FOR THE ANSWER

A The signer's public key

WHY The signer makes the signature with a private key nobody else has. Anyone can verify it with the matching public key, which is safe to share.

STRAIGHT FACE
What music genre has to do with computer commands? Algorithm and Blues.

SESK.INFO #5497

SECURITY & PRIVACY

Adding a unique random salt to each password before hashing mainly defends against what?

- **A** Precomputed lookup tables such as rainbow tables
- **B** Shoulder surfing
- **C** Phishing emails

FLIP FOR THE ANSWER

A Precomputed lookup tables such as rainbow tables

WHY Without a salt, two users with the same password get the same hash and attackers can use one table for everyone. A unique salt forces them to crack each hash separately.

STRAIGHT FACE
Salt makes every password hash different. Chefs and security teams agree it improves the dish.

SESK.INFO #5500

SECURITY & PRIVACY

Published attacks show MD5 is not prudent to use when you need which property?

- **A** Fast speed
- **B** Fixed-length output
- **C** Collision resistance

FLIP FOR THE ANSWER

C Collision resistance

WHY A collision is two different inputs with the same hash. If attackers can create collisions, they can swap a malicious file or certificate for a good one.

STRAIGHT FACE
MD5 and its twin walked in with the same hash. Nobody could tell them apart, which was the problem.

SESK.INFO #5499

SECURITY & PRIVACY

NIST's digital identity guidelines say a password salt must be at least how long?

- **A** 8 bits
- **B** 32 bits
- **C** 256 bits

FLIP FOR THE ANSWER

B 32 bits

WHY NIST SP 800-63B-4 requires a salt of at least 32 bits. The goal is that accounts almost never share a salt, so the same password rarely gives the same stored hash.

STRAIGHT FACE
My computer said my password is insecure. Well maybe if it wasn't forced to have such strict requirements it would be more confident.

SESK.INFO #5501

SECURITY & PRIVACY

Which of these is a poor choice for storing passwords because it is a fast hash?

- **A** Argon2id
- **B** bcrypt
- **C** Plain SHA-256

FLIP FOR THE ANSWER

C Plain SHA-256

WHY Password storage should use slow, tunable algorithms so each guess is costly. Argon2id, bcrypt and PBKDF2 do this, which is called key stretching.

STRAIGHT FACE
Password looks at itself in the mirror: "Don't listen to Google. You are a strong, confident password."

SESK.INFO #5502

SECURITY & PRIVACY

A tamper-resistant chip on a computer's motherboard that generates and stores cryptographic keys is called what?

- **A** A Trusted Platform Module (TPM)
- **B** A hardware load balancer
- **C** A smart card reader

FLIP FOR THE ANSWER

A A Trusted Platform Module (TPM)

WHY A TPM generates and protects keys inside hardware, so malware has a hard time stealing them. Disk encryption and device checks often use it.

STRAIGHT FACE
What is a computer geek's favorite snack? Microchips.

SESK.INFO #5503

SECURITY & PRIVACY

What do you send to a certificate authority to request a certificate?

- **A** Your private key
- **B** A certificate signing request (CSR)
- **C** A certificate revocation list

FLIP FOR THE ANSWER

B A certificate signing request (CSR)

WHY A CSR holds the public key and the name to be certified, and is signed with the matching private key. The private key itself never leaves your system.

STRAIGHT FACE
Why did the server sign its own request? It wanted to prove it had the key.

SESK.INFO #5504

SECURITY & PRIVACY

What is a certificate revocation list (CRL)?

- **A** A list of trusted root certificates
- **B** A list of users allowed to request certificates
- **C** A signed, time-stamped list of revoked certificates

FLIP FOR THE ANSWER

C A signed, time-stamped list of revoked certificates

WHY If a certificate is stolen or issued by mistake, the CA revokes it and publishes the serial number in a CRL. Clients check the list before trusting a certificate.

STRAIGHT FACE
My identity got stolen. They returned it with a note: "No thanks."

SESK.INFO #5505

SECURITY & PRIVACY

Which protocol lets software check the revocation status of a certificate online, more timely than CRLs?

- **A** Online Certificate Status Protocol (OCSP)
- **B** Simple Network Management Protocol (SNMP)
- **C** Lightweight Directory Access Protocol (LDAP)

FLIP FOR THE ANSWER

A Online Certificate Status Protocol (OCSP)

WHY Instead of downloading a whole CRL, a client asks an OCSP responder about one certificate. The answer is usually fresher than a periodically published list.

STRAIGHT FACE
OCSP is the only protocol that answers a question about someone's status without any drama.

SESK.INFO #5506

SECURITY & PRIVACY

A wildcard certificate for *.example.com is presented. Which name does it match?

- **A** www.example.org
- **B** www.example.com
- **C** a.b.example.com

FLIP FOR THE ANSWER

B www.example.com

WHY The wildcard can only be the whole left-most label and covers just one label. So a.b.example.com, with two labels, does not match.

STRAIGHT FACE
Why did the football team fumble the handoff? They didn't use a secure transfer method.

SESK.INFO #5507

SECURITY & PRIVACY

What did TLS 1.3 change about key exchange?

- **A** Static RSA key exchange became required
- **B** Key exchange moved to symmetric keys only
- **C** Every public-key key exchange now provides forward secrecy

FLIP FOR THE ANSWER

C Every public-key key exchange now provides forward secrecy

WHY With forward secrecy, a stolen server key cannot decrypt past recorded sessions, because each session uses fresh ephemeral keys. TLS 1.3 removed static RSA and static Diffie-Hellman.

STRAIGHT FACE
Forward secrecy means yesterday's secrets stay secret, even if today's key is stolen.

SESK.INFO #5508

SECURITY & PRIVACY

What cryptographically links each block in a blockchain to the one before it?

- **A** The previous block header's hash
- **B** The miner's password
- **C** A shared symmetric session key

FLIP FOR THE ANSWER

A **The previous block header's hash**

WHY Each block header includes a hash of the previous block. Change an old block and its hash changes, which breaks every link after it, so tampering is easy to spot.

STRAIGHT FACE
Why was the blockchain so well organized? Every block knew exactly who came before it.

SESK.INFO #5509

SECURITY & PRIVACY

Which threat actor already has authorized access to an organization's systems?

- **A** A nation-state outsider
- **B** An insider threat
- **C** An unskilled external attacker

FLIP FOR THE ANSWER

B **An insider threat**

WHY Insiders can harm systems on purpose or by accident because they already hold valid accounts. That makes access limits and monitoring just as important as the perimeter.

STRAIGHT FACE
What do you get when you cross people who break into computers with a caramel-coated popcorn snack? Hacker Jacks.

SESK.INFO #5510

SECURITY & PRIVACY

Tricking a person into revealing information or taking a harmful action is called what?

- **A** Key stretching
- **B** Port scanning
- **C** Social engineering

FLIP FOR THE ANSWER

C **Social engineering**

WHY Attackers exploit trust, urgency and helpfulness. Phishing, pretexting, impersonation and baiting are all forms, which is why training matters.

STRAIGHT FACE
The best exploit in IT needs no code. It is a friendly voice saying, can you hold the door?

SESK.INFO #5511

SECURITY & PRIVACY

What is phishing called when it targets a specific person, company or industry?

- **A** Spearphishing
- **B** Smishing
- **C** Pharming

FLIP FOR THE ANSWER

A **Spearphishing**

WHY Mass phishing casts a wide net. Spearphishing uses real names, roles and projects to look believable, so it is harder to spot.

STRAIGHT FACE
Spearphishing is when the email knows your name, your boss and your lunch order.

SESK.INFO #5512

SECURITY & PRIVACY

Phishing carried out over a phone call is commonly called what?

- **A** Smishing
- **B** Vishing
- **C** Whaling

FLIP FOR THE ANSWER

B Vishing

WHY Attackers call pretending to be a bank, vendor or help desk and press you to act fast. Hang up and call back using a number you know is real.

STRAIGHT FACE
The scammer called to say my car warranty had a problem. My phone said the problem was his number.

SESK.INFO #5513

SECURITY & PRIVACY

Compromising a website that a target group often visits, to infect them, is called what?

- **A** A typosquatting attack
- **B** A replay attack
- **C** A watering hole attack

FLIP FOR THE ANSWER

C A watering hole attack

WHY Instead of attacking a hardened target directly, attackers infect a trusted site its users visit. Visitors get infected just by browsing.

STRAIGHT FACE
The antelope avoided the watering hole. Too many crocodiles in the comments.

SESK.INFO #5514

SECURITY & PRIVACY

Registering a domain that looks like a real one, such as exmple.com, is called what?

- **A** Typosquatting
- **B** Cache poisoning
- **C** Domain hijacking

FLIP FOR THE ANSWER

A Typosquatting

WHY Attackers register near-miss domains, such as swapped letters or a different top-level domain, to catch typos or fool readers. Always check the exact address.

STRAIGHT FACE
Typosquatters make a living from our typing. They really have a way with errors.

SESK.INFO #5515

SECURITY & PRIVACY

Which malware spreads by inserting copies of itself into host programs or data files?

- **A** A worm
- **B** A virus
- **C** A rootkit

FLIP FOR THE ANSWER

B A virus

WHY Viruses are often triggered when you open a file or run a program. A worm, by contrast, is self-contained and spreads on its own.

STRAIGHT FACE
What is a computer virus? A terminal illness!

SESK.INFO #5516

SECURITY & PRIVACY

Which malware is self-contained and spreads across a network on its own, without user action?

- **A** A virus
- **B** A Trojan horse
- **C** A worm

FLIP FOR THE ANSWER

C A worm

WHY A worm does not need a host file or a person to click anything. Network service worms exploit a vulnerable service to jump to the next host.

STRAIGHT FACE
What eats laptops? Computer worms.

SESK.INFO #5517

SECURITY & PRIVACY

Which malware looks like a useful program but has a hidden malicious purpose and does not replicate?

- **A** A Trojan horse
- **B** A worm
- **C** A virus

FLIP FOR THE ANSWER

A A Trojan horse

WHY Like the ancient story, it gets in by looking harmless. Unlike viruses and worms, a Trojan does not replicate; the victim installs it.

STRAIGHT FACE
The Trojan said, I come bearing gifts. The firewall said, I will take that in the sandbox.

SESK.INFO #5518

SECURITY & PRIVACY

Malware that hides its own presence by modifying operating system functions is called what?

- **A** A keylogger
- **B** A rootkit
- **C** Adware

FLIP FOR THE ANSWER

B A rootkit

WHY Rootkits intercept and change operating system calls to hide files, processes and connections. That makes them very hard to find and remove.

STRAIGHT FACE
The rootkit won hide and seek. It even hid from the scoreboard.

SESK.INFO #5519

SECURITY & PRIVACY

Code intentionally hidden in software that triggers a malicious action when conditions are met is called what?

- **A** A keylogger
- **B** A botnet
- **C** A logic bomb

FLIP FOR THE ANSWER

C A logic bomb

WHY The trigger could be a date, a missing employee record or a certain command. Because it hides inside normal code, code review and change control help catch it.

STRAIGHT FACE
A logic bomb is patient. It has all the time in the world and a calendar.

SESK.INFO #5520

SECURITY & PRIVACY

Which web attack inserts a database query into an input field that the application then runs?

- **A** Cross-site scripting
- **B** SQL injection
- **C** Directory traversal

FLIP FOR THE ANSWER

B SQL injection

WHY If an app builds queries by pasting in user text, attackers can add their own SQL. Successful attacks can read, change or delete data.

STRAIGHT FACE
An SQL statement walks into a bar and sees two tables. It asks, "May I join you?"

SESK.INFO #5522

SECURITY & PRIVACY

Malware that encrypts your files and demands payment for the decryption key is called what?

- **A** Ransomware
- **B** Spyware
- **C** Bloatware

FLIP FOR THE ANSWER

A Ransomware

WHY Ransomware makes files unusable until a ransom is paid. Tested offline backups let you restore your data without paying.

STRAIGHT FACE
Ransomware sent a note: pay up or your files stay locked. My backups replied, we are good, thanks.

SESK.INFO #5521

SECURITY & PRIVACY

Which attack forces a logged-in user's browser to perform an action they did not intend?

- **A** Cross-site request forgery (CSRF)
- **B** Cross-site scripting
- **C** Session replay

FLIP FOR THE ANSWER

A Cross-site request forgery (CSRF)

WHY The victim is already authenticated, so the web app trusts the request. A link or page tricks their browser into sending an unwanted action.

STRAIGHT FACE
CSRF is when your browser does a favor for a stranger without asking you first.

SESK.INFO #5524

SECURITY & PRIVACY

Which web attack injects malicious scripts into otherwise trusted websites so they run in other users' browsers?

- **A** SQL injection
- **B** Buffer overflow
- **C** Cross-site scripting (XSS)

FLIP FOR THE ANSWER

C Cross-site scripting (XSS)

WHY The site fails to clean user input and sends it back to other visitors, whose browsers run it. Attackers can steal session tokens or change what the page shows.

STRAIGHT FACE
The website trusted all user input. The browsers ran everything. The scripts took a vacation.

SESK.INFO #5523

SECURITY & PRIVACY

Capturing valid login data and sending it again later to impersonate a user is called what?

- **A** A birthday attack
- **B** A downgrade attack
- **C** A replay attack

FLIP FOR THE ANSWER

C A replay attack

WHY The attacker does not need to break the encryption, only to reuse a valid message. Nonces, timestamps and one-time values make old messages useless.

STRAIGHT FACE
A replay attack is just a rerun. The attacker needs a new episode, but got the same one.

SESK.INFO #5526

SECURITY & PRIVACY

Using sequences like ../ to reach files outside a web application's folder is called what?

- **A** Buffer overflow
- **B** Directory (path) traversal
- **C** Credential stuffing

FLIP FOR THE ANSWER

B Directory (path) traversal

WHY The attacker manipulates file path variables to read files the app never meant to share, such as configuration files or source code.

STRAIGHT FACE
A hacker walked up the directory tree and said, I'm just going to take the long way home.

SESK.INFO #5525

SECURITY & PRIVACY

Trying stolen username and password pairs from one breach against other websites is called what?

- **A** Password spraying
- **B** Credential stuffing
- **C** Pass the hash

FLIP FOR THE ANSWER

B Credential stuffing

WHY Attackers automate logins with breached pairs. It works because many people use the same password on several sites; unique passwords and MFA stop it.

STRAIGHT FACE
My email password has been hacked. That's the third time I've had to rename the cat.

SESK.INFO #5528

SECURITY & PRIVACY

An attacker secretly positions themselves between two devices to sniff or change their traffic. What is this attack called?

- **A** An on-path attack
- **B** A birthday attack
- **C** A reflected DDoS

FLIP FOR THE ANSWER

A An on-path attack

WHY Everything flows through the attacker. TLS and certificate checks help, because the attacker cannot read or change protected traffic without being noticed.

STRAIGHT FACE
The on-path attacker said, I am just here for the traffic. The packets said, we are not.

SESK.INFO #5527

SECURITY & PRIVACY

Trying one common password against many different accounts is called what?

- **A** Credential stuffing
- **B** A dictionary pass
- **C** Password spraying

FLIP FOR THE ANSWER

C Password spraying

WHY Spreading attempts across many accounts helps attackers avoid lockouts that trip after repeated failures on a single account.

STRAIGHT FACE
Yesterday I decided to change my WiFi name to "Hack me if you can" and when I woke up this morning I saw the name changed to "Challenge accepted" somebody help.

SESK.INFO #5529

SECURITY & PRIVACY

In a reflection DDoS attack, what do attackers send to third-party servers?

- **A** Packets with the victim's spoofed source address
- **B** Packets with the reflector's real password
- **C** Encrypted copies of the victim's data

FLIP FOR THE ANSWER

A Packets with the victim's spoofed source address

WHY Reflectors answer requests, so replies flood the victim instead of the attacker. With amplification, a small request triggers a much larger reply.

STRAIGHT FACE
What do you get when you cross a dog and a computer? A machine that has a bark worse than its byte.

SESK.INFO #5530

SECURITY & PRIVACY

A user signs in from Nashville and, ten minutes later, from Tokyo. Which indicator of compromise is this?

- **A** Resource consumption
- **B** Impossible travel
- **C** Out-of-cycle logging

FLIP FOR THE ANSWER

B Impossible travel

WHY No one can move that far in that time, so the account is probably being used by someone else. Security tools raise an alert to investigate.

STRAIGHT FACE
Why didn't the IT team set up their remote office from the beach? It was too cloudy.

SESK.INFO #5531

SECURITY & PRIVACY

Which hardening step reduces the attack surface by removing what a system does not need?

- **A** Enabling every available service
- **B** Sharing admin passwords across servers
- **C** Disabling unnecessary services, ports and protocols

FLIP FOR THE ANSWER

C Disabling unnecessary services, ports and protocols

WHY Every running service is a possible vulnerability. Turning off unneeded services, applications and protocols leaves fewer ways in.

STRAIGHT FACE
An open port is like a window left unlocked. Close the ones you are not using.

SESK.INFO #5532

SECURITY & PRIVACY

Which control limits how many failed login attempts can be made on an account?

- **A** Key escrow
- **B** Rate limiting or throttling
- **C** Data masking

FLIP FOR THE ANSWER

B Rate limiting or throttling

WHY Online guessing needs many tries. Throttling or lockout slows brute force and keeps attackers from testing millions of passwords.

STRAIGHT FACE
A rate limiter is polite but firm. It says, one at a time, please.

SESK.INFO #5534

SECURITY & PRIVACY

A list of applications authorized to run, with everything else blocked by default, is called what?

- **A** An application allow list
- **B** A certificate revocation list
- **C** A deny list of known malware

FLIP FOR THE ANSWER

A An application allow list

WHY Default-deny stops unknown programs, including new malware, from running at all. It works best on managed machines where users cannot install software.

STRAIGHT FACE
The allow list is the bouncer who only lets in people with names on the sheet.

SESK.INFO #5533

1
AhaBulb POINT

1
AhaBulb POINT