Securing Spaces

AP Cybersecurity · Vocabulary in context

Word	Example
CIA triad /ˌsiː aɪ ˈeɪ ˈtraɪæd/	The **CIA triad** is confidentiality, integrity and availability.
Confidentiality /ˌkɒnfɪˌdenʃiˈæləti/	**Confidentiality** means only the right people can read the data.
Integrity /ɪnˈtegrɪti/	**Integrity** means nobody has changed the data without permission.
Availability /əˌveɪləˈbɪlɪti/	**Availability** means users can get to the service when they need it.
script kiddie /skrɪpt ˈkɪdi/	A **script kiddie** uses attack tools made by others.
hacktivist /ˈhæktɪvɪst/	A **hacktivist** attacks websites for a political cause.
insider /ɪnˈsaɪdə/	An **insider** already has access, so can do a lot of harm.
cyberterrorist /ˈsaɪbətərərɪst/	A **cyberterrorist** attacks computers to cause fear.
transnational criminal organisations /trænˈsnæʃənl ˈkrɪmɪnl ˌɔːgənaɪˈzeɪʃnz/	**Transnational criminal organisations** run online scams across many countries.
phases /ˈfeɪzɪz/	An attack has several **phases**, from planning to stealing data.
reconnaissance /rɪˈkɒnɪsəns/	**Reconnaissance** means collecting information about the target first.
OSINT /ˈəʊsɪnt/	**OSINT** uses public information, like social media posts.

exercises.lol exercises.com.cn

Word	Example
lateral movement /ˈlætərəl ˈmuːvmənt/	**Lateral movement** means moving from one hacked computer to others.
social engineering /ˈsəʊʃl ˌendʒɪˈnɪərɪŋ/	**Social engineering** tricks people into giving away secrets.
Pretexting /ˈpriːtekstɪŋ/	**Pretexting** uses a made-up story: “Hi, I’m from IT support.”
Authority /əˈθɒrɪti/	Attackers use **authority** by pretending to be the boss.
Intimidation /ɪnˌtɪmɪˈdeɪʃn/	**Intimidation** uses threats: “Do this now or lose your job!”
Consensus /kənˈsensəs/	**Consensus** makes people follow others: “Everyone has already signed up.”
Scarcity /ˈskeəsɪti/	**Scarcity** pressures people: “Only two left!”
Familiarity /fəˌmɪliˈærɪti/	**Familiarity** makes a fake email look like it is from a friend.
Urgency /ˈɜːdʒənsi/	**Urgency** makes people act fast without checking.
risk /rɪsk/	Known probabilities help a manager estimate **risk**.
threat /θret/	A **threat** is anything that could harm the system.
vulnerability /ˌvʌlnərəˈbɪlɪti/	An old password is a **vulnerability**.
asset /ˈæset/	A delivery van is an **asset**.
likelihood /ˈlaɪklihʊd/	The **likelihood** of an attack is how probable it is.

Word	Example
severity /səˈverɪti/	The **severity** of a risk is how bad the harm would be.
quantitative /ˈkwɒntɪteɪtɪv/	A **quantitative** risk score uses numbers.
qualitative /ˈkwɒlɪteɪtɪv/	A **qualitative** risk rating uses words like low, medium and high.
risk assessment /rɪsk əˈsesmənt/	A **risk assessment** lists threats and how serious they are.
Avoid /əˈvɔɪd/	**Avoid** a risk by not doing the risky thing at all.
Transfer /ˈtrænsfɜː/	**Transfer** a risk by buying insurance.
Mitigate /ˈmɪtɪgeɪt/	**Mitigate** a risk by adding a firewall.
Accept /əkˈsept/	**Accept** a small risk when fixing it costs too much.
residual risk /rɪˈsɪdʒuːəl rɪsk/	The **residual risk** is the risk left after all your protections.
physical /ˈfɪzɪkl/	The **physical** layer sends bits as electrical or light signals.
technical /ˈteknɪkl/	A firewall is a **technical** control.
managerial /ˌmænəˈdʒɪərɪəl/	A security policy is a **managerial** control.
preventative /prɪˈventətɪv/	A lock is a **preventative** control: it stops the attack.
detective /dɪˈtektɪv/	A camera is a **detective** control: it shows what happened.
corrective /kəˈrektɪv/	Restoring a backup is a **corrective** action.

exercises.lol exercises.com.cn

Word	Example
defense-in-depth /dɪˈfens ɪn depθ/	**Defense-in-depth** uses many layers of protection.
physical attacks /ˈfɪzɪkl əˈtæks/	Stealing a laptop is one of many **physical attacks**.
Piggybacking /ˈpɪgɪbækɪŋ/	**Piggybacking** is when a worker lets a stranger through the door.
Tailgating /ˈteɪlgeɪtɪŋ/	**Tailgating** is when a stranger slips in behind a worker unnoticed.
Shoulder surfing /ˈʃəʊldə ˈsɜːfɪŋ/	**Shoulder surfing** means watching someone type their PIN. PIN
Dumpster diving /ˈdʌmpstə ˈdaɪvɪŋ/	**Dumpster diving** means searching rubbish for secret papers.
Card cloning /kɑːd ˈkləʊnɪŋ/	**Card cloning** copies the data on an access card.
keylogger /ˈkiːlɒgə/	A **keylogger** records everything you type.
foothold /ˈfʊthəʊld/	The attacker gained a **foothold** on one computer.
clean desk policy /kliːn desk ˈpɒlɪsi/	A **clean desk policy** means no papers left on desks.
bollards /ˈbɒlɑːdz/	**Bollards** stop cars from driving into the building.
card readers /kɑːd ˈriːdəz/	**Card readers** check staff cards at the door.
access control vestibule /ˈækses kənˈtrəʊl ˈvestɪbjuːl/	An **access control vestibule** has two doors: the second opens only after the first closes.

Word	Example
uninterruptible power supply (UPS) /ˌʌˌnɪntəˈrʌptɪbl ˈpaʊə səˈplaɪ/	An **uninterruptible power supply (UPS)** keeps computers on during a power cut.
motion sensors /ˈməʊʃn ˈsensəz/	**Motion sensors** turn on the alarm when someone moves.
points of ingress and egress /pɔɪnts ɒv ˈɪŋgres ænd iːˈgres/	Guard the **points of ingress and egress**: all ways in and out.
command and control (C2)	Infected computers get orders from a **command and control (C2)** server.
privileges	Give each user only the **privileges** they need.
exfiltration	**Exfiltration** means secretly copying data out of a network.
cost-effective	A control is **cost-effective** if it costs less than the loss it prevents.
expected loss	The **expected loss** is the chance of the event times its cost.
turnstile	A **turnstile** lets one person through at a time.
surge protector	A **surge protector** guards devices against sudden power spikes.

exercises.lol exercises.com.cn