

CySA+

Exam Review

The whole exam in one pass. Every term CompTIA lists, grouped the way it is tested, defined in a single sentence, with the distinctions that separate look-alike answers called out in place.

EXAM SNAPSHOT

Exam code	CS0-004 (V4)	Questions	Max. 85
Question types	Multiple choice + PBQ	Time	165 minutes
Passing score	750 of 100–900	Experience	4 years, SOC level 2

OBJECTIVE DOMAIN MAP

1.0	Security Operations		34%
2.0	Vulnerability Management		26%
3.0	Incident Response and Management		24%
4.0	Reporting and Communication		16%

WHAT IS INSIDE

All four domains as grouped reference tables • one-line definitions you can scan • tool and flag cheat sheets • ports, CVSS v4.0, frameworks and acronyms • designed for the last two weeks before the exam.

Contents

How to use this review	iii
Who it is for	iii
How it is organised	iii
A suggested schedule	iii
1.0 Security Operations	1
1.1 System and network architecture	1
1.2 Indicators of potential malicious activity	6
1.3 Tools to determine malicious activity	8
1.4 Threat intelligence and threat hunting	11
1.5 Efficiency and process improvement	13
1.6 Artificial intelligence in security operations	14
2.0 Vulnerability Management	16
2.1 Vulnerability scanning methods	16
2.2 Vulnerability assessment tool output	18
2.3 Prioritising and mitigating vulnerabilities	20
2.4 Control types, risk and vulnerability management	22
3.0 Incident Response and Management	24
3.1 Attack methodology frameworks	24
3.2 The incident response process	26
3.3 Incident response techniques	27
4.0 Reporting and Communication	29
4.1 Vulnerability management reporting	29
4.2 Incident response reporting and communication	31
A.0 Ports and Protocols	34
A.1 File transfer and remote access	34
A.2 Web and email	35
A.3 Name resolution, directory and authentication	35
A.4 Management, monitoring and time	36
A.5 Databases	36
A.6 Industrial, virtualisation and other	37

A.7	Ports that usually mean trouble	38
B.0	Command Reference	39
B.1	What is on this host?	39
B.2	What is on the network?	39
B.3	What is in this traffic?	40
B.4	What is in these logs?	41
B.5	What is this file?	43
B.6	Encoding, hashing and encryption	44
B.7	Evidence acquisition	44
B.8	Quick conversions	45
C.0	Queries, Rules and Patterns	46
C.1	Reading any query language	46
C.2	Detections worth recognising	46
C.3	Regular expressions worth carrying	49
D.0	Frameworks at a Glance	50
D.1	Attack and intrusion models	50
D.2	MITRE ATT&CK enterprise tactics, in order	51
D.3	Process and lifecycle models	51
D.4	Standards, benchmarks and regulations	52
D.5	Scoring and classification systems	53
D.6	Intelligence sharing	53
E.0	Acronyms	55

How to use this review

This is the condensed companion to the Study Guide. It contains the same core material with the explanation removed: the published objective terms, grouped the way the exam groups them and defined in a sentence you can scan. Supporting industry context is included where it prevents a misleading simplification. This is an independent study aid, not an endorsement by or publication of CompTIA.

Who it is for

Somebody in the last two or three weeks before the exam who already understands the concepts and now needs *recall*. If a definition here does not make sense, that is a signal to go back to the corresponding numbered section of the Study Guide — the numbering is identical in both documents.

How it is organised

Four chapters, one per domain, each divided by objective. Inside each objective the material appears as grouped reference blocks: a dark header naming the group, then one row per term. Distinctions that the exam deliberately blurs are called out in place rather than buried in prose.

Block	What it holds
GROUPED TERMS	A theme, then term and one-line meaning. The bulk of the document.
EXAM TRAP	Two or more ideas that look alike. These are the highest-value lines in the review.
KEY POINT	The thing the exam actually tests about a topic.
CODE	Syntax and flags, labelled with their language.

A suggested schedule

When	What
Two weeks out	Read one domain per day, marking anything you cannot restate without looking.
One week out	Re-read only what you marked. Work the appendices — ports, commands, queries — because those are pure recall and pure marks.
Three days out	Exam traps only. Every one of them exists because candidates get it wrong.
The day before	The checklists at the end of each Study Guide objective, and the ports table. Then stop.

THE FIVE SENTENCES THAT ANSWER THE MOST QUESTIONS

1. Compare against a baseline before calling anything anomalous.
2. Isolate, do not power off; capture volatile evidence first.

3. Prioritise on exploitability in context, not on the highest score.
4. A legal hold overrides a retention schedule, always.
5. Match the message to the audience: impact for executives, the specific fix for owners.

Security Operations

Architecture, indicators, tooling, threat intelligence, process efficiency and artificial intelligence. The largest domain, and the one with the most performance-based material.

1.1 System and network architecture

COMPTIA OBJECTIVE 1.1

Explain concepts related to system and network architecture in security operations.

LOGGING CONCEPTS

Ingestion	Collecting events from sources into a central platform where they can be parsed, indexed and searched.
Agent-based collection	Software on the host reads and forwards logs. Buffers through outages; must be deployed and maintained.
Agentless collection	Syslog, an API, or a Windows Event Collector subscription. Nothing to install; limited to what the protocol exposes.
Configuration	What gets recorded. Windows audit policy; <code>rsyslog</code> and <code>auditd</code> on Linux.
Integrity	Assurance that stored records have not been altered: hashing, signing, write-once storage, and forwarding off-host quickly.
Log security	Access control, encryption in transit and at rest, and protecting the logging infrastructure itself.
Time synchronisation	NTP, one authoritative source, everything in UTC. Kerberos fails beyond five minutes of skew.
Retention	How long logs are kept, normally tiered: hot, warm, cold.
Preservation	Actively protecting specific data from the retention schedule.
Legal hold	A formal instruction that makes preservation mandatory. Overrides retention.
Normalisation	Mapping vendor field names onto one common schema.
Enrichment	Adding context the raw event lacked: owner, criticality, geo-IP, threat intelligence.

RETENTION VS. PRESERVATION VS. LEGAL HOLD

Retention deletes on a timer. Preservation stops the timer for specific items. A legal hold makes preservation compulsory and always beats the policy.

OPERATING SYSTEM CONCEPTS

System hardening	Removing or disabling everything not needed, then configuring what remains to a known baseline.
Baseline	The documented, approved configuration.
Configuration drift	Silently moving away from the baseline.
File structure	Where the operating system keeps what matters — and therefore where an attacker leaves traces.
Critical files (Linux)	<code>/etc/passwd</code> , <code>/etc/shadow</code> , <code>/etc/sudoers</code> , <code>crontab</code> , <code>authorized_keys</code> , <code>sshd_config</code> , <code>/var/log/auth.log</code> .
Critical files (Windows)	<code>System32</code> , registry hives (SAM, SYSTEM), Run keys, Services key, Scheduled Tasks, <code>Prefetch</code> , <code>winevt\Logs</code> .
System processes	Running programs, each with a PID, a parent and a security context. Parentage and path are what make a detection.
Windows process chain	<code>System</code> → <code>smss</code> → <code>wininit</code> → <code>services</code> → <code>svchost</code> .

INFRASTRUCTURE AND SYSTEM ARCHITECTURE

Virtualisation	Multiple full operating systems on one machine, separated by a hypervisor.
Type 1 hypervisor	Bare metal — ESXi, Hyper-V, KVM.
Type 2 hypervisor	Hosted on an operating system — VirtualBox, Workstation.
VM escape	Breaking out of a guest onto the hypervisor or another guest.
VM sprawl	Unmanaged virtual machines nobody patches or decommissions.
Containerisation	An application and its libraries as an isolated process on a <i>shared</i> kernel.
Container risks	Shared kernel, image provenance, privileged containers, secrets in layers, ephemerality, registry security.
Cloud native	Microservices, containers, declarative infrastructure, managed services, automated pipelines.
IaaS / PaaS / SaaS	The provider secures more of the stack at each step; the customer still owns its identities, permissions, data classification and configuration. Check the service contract for the exact boundary.
API	A defined contract allowing one program to call another. Both an automation enabler and an attack surface.
Webhook	The reverse direction: the remote service calls you on an event. Must be authenticated.

DEVICE MANAGEMENT

Endpoint management	Centralised inventory, configuration, patching and agent deployment for workstations and servers.
Mobile device management	Enrolment, policy enforcement, application distribution, remote lock and wipe for mobile devices.
Work profile / containerisation	A cryptographically separated corporate workspace on a personal device; enables selective wipe.

continued on the next page

DEVICE MANAGEMENT

Jailbreak / root detection	Rooted devices bypass the controls MDM relies on; normally blocked.
BYOD / COPE / CYOD / COBO	Personal / corporate-owned personally enabled / choose from a list / corporate business-only. Control rises across that sequence.

ZERO TRUST (NIST SP 800-207)

Zero Trust	No implicit trust from network location; every request authenticated, authorised and encrypted, per session, using all context.
Policy Engine (PE)	Decides grant or deny. Control plane.
Policy Administrator (PA)	Executes the decision; establishes or tears down the session. Control plane.
Policy Decision Point (PDP)	PE plus PA together.
Policy Enforcement Point (PEP)	Sits in the traffic path and allows or blocks. The only component in the data plane.
Adaptive identity	Authentication strength that varies with assessed risk.
Implicit trust zone	The region behind a PEP where traffic is no longer individually inspected.
Microsegmentation	Policy enforced between individual workloads, not just between subnets.

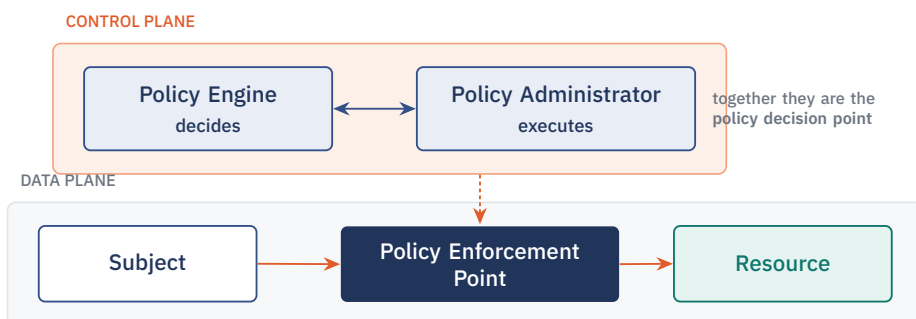


Figure 1. Zero Trust components. Everything that decides is control plane; the only component a packet touches is the policy enforcement point.

WHICH PLANE?

PE and PA are *control plane*. PEP is *data plane*. The PEP is the only component a packet ever touches.

SASE AND HYBRID CLOUD

SASE	Cloud-delivered networking plus security, applied at a point of presence near the user rather than after a backhaul to headquarters.
SWG	Secure web gateway: URL filtering, malware inspection, TLS decryption.

continued on the next page

SASE AND HYBRID CLOUD

CASB	Cloud access security broker: visibility and policy over SaaS use.
CASB API mode	Out of band; sees data at rest; cannot block in real time.
CASB proxy mode	In line; can block; must sit in the traffic path.
ZTNA	Per-application access brokered after identity and posture checks; replaces “VPN gives you the network”.
FWaaS	Firewall and IPS delivered from the provider’s edge.
Hybrid cloud	On-premises plus one or more public clouds, connected so workloads and identity span both.
Hybrid risks	Identity sprawl, inconsistent logging, inconsistent controls, an unmonitored interconnect, unclear ownership.

IDENTITY AND ACCESS MANAGEMENT

Identification	The claim of who you are.
Authentication	Proving the claim.
Authorisation	What you are permitted to do.
Accounting	The record of what you did.
Factors	Something you know, have, are; plus location and behaviour as attributes.
MFA	Two or more factors from <i>different</i> categories.
SSO	One authentication event grants access to many services.
Federation	Trusting another organisation’s identity provider. SAML 2.0, OpenID Connect. IdP asserts, SP consumes.
Passwordless / FIDO2	Origin-bound public-key authentication; phishing resistant.
Kerberos	Windows domain authentication; ticket-granting ticket exchanged for service tickets; five-minute skew limit.
DAC / MAC / RBAC / ABAC	Owner’s discretion / system labels / role / attributes evaluated by policy.
PAM	Vaulting, rotation, just-in-time access, session recording, discovery of privileged accounts.
Privilege creep	Rights accumulating across role changes. Found by access recertification.
Secrets management	Storage, distribution, rotation and revocation of non-human credentials — API keys, service passwords, certificates.

MFA VS. TWO STEPS

Password plus SMS code is MFA (know + have), though weak. Password plus security question is single-factor with extra clicks.

ENCRYPTION AND DATA PROTECTION

Symmetric	One key encrypts and decrypts. AES. Fast; key distribution is the problem.
Asymmetric	Linked key pair. RSA, ECC. Solves distribution; slow.
Confidentiality	Encrypt with the recipient's <i>public</i> key.
Authenticity / non-repudiation	Sign with the sender's <i>private</i> key.
Hashing	One way, fixed length. SHA-256, SHA-3. MD5 and SHA-1 are broken for collision resistance.
Salting	Unique random value added before hashing a password; defeats rainbow tables.
Key exchange	Diffie–Hellman, ECDHE.
Perfect forward secrecy	Ephemeral keys, so a stolen long-term key does not decrypt past traffic.
PKI	CAs, RAs, CRLs, OCSP and the policies binding them.
Encoding	Reversible representation change with no key. Base64, hex, URL encoding. Not encryption.
Data classification	Labelling by sensitivity so controls follow the label.
DLP	Inspects data at rest, in motion and in use against policy.
Tokenisation	Replace a value with an unrelated token; mapping held in a vault. Removes data from scope.
Masking	Hides part of a value for display only.
Anonymisation	Irreversible removal of identifiers.
Pseudonymisation	Reversible with separately held information.
Data sovereignty	Data is subject to the law of the country it sits in.

CRITICAL INFRASTRUCTURE

OT	Operational technology: anything monitoring or controlling a physical process.
ICS	Industrial control system: PLCs, RTUs, DCSs and the interfaces above them.
SCADA	Supervisory control and data acquisition, often across large distances.
PLC	The ruggedised controller that actually operates the equipment.
HMI	The operator's screen.
Historian	The database of process values over time.
Purdue model	Levels 0–5, with level 3.5 as the industrial DMZ between OT and IT.
OT priorities	Safety and availability first, confidentiality last.
OT scanning	Passive only. Active scanning has crashed controllers.
OT protocols	Modbus, DNP3, Profinet, EtherNet/IP — no authentication, no encryption.

1.2 Indicators of potential malicious activity

COMPTIA OBJECTIVE 1.2

Given a scenario, analyze indicators of potential malicious activity.

IOC VS. IOA

An **indicator of compromise** is evidence a breach already happened — a known-bad hash, a C2 domain, a cleared log. An **indicator of attack** is behaviour suggesting an attack in progress — enumeration, a burst of failed logons, mass file renaming.

NETWORK-RELATED INDICATORS

Rogue device	Any unauthorised device on the network.
Rogue access point	Unauthorised wireless AP plugged into the wired network.
Evil twin	An AP impersonating a legitimate SSID to harvest credentials.
Rogue switch	Multiple MAC addresses learned on one access port.
Enumeration	Systematic listing of hosts, ports, services, shares and users. Noisy and therefore detectable.
Port scanning	Many SYNs to many ports, few completed handshakes.
DNS enumeration	Attempted AXFR; brute-forced subdomains; NXDOMAIN floods.
SMB/LDAP enumeration	Events 4661, 4662, 5145; large LDAP result sets from one account.
Activity on unexpected ports	A service on a non-standard port, <i>or</i> the wrong protocol on a standard port.
Beaconing	Periodic implant check-in. Detected by the regularity of the interval, not the destination.
Jitter	Randomisation added to a beacon interval. Widens the variance; does not remove the pattern.
DNS tunnelling	Data in long, high-entropy subdomain labels; TXT and NULL floods; resolution with no follow-up connection.
ICMP tunnelling	Echo requests with large or variable payloads at a steady rate.
Irregular peer-to-peer	Workstations talking to workstations on 445, 3389 or 5985. Lateral movement.

HOST-RELATED INDICATORS

Resource consumption	CPU (mining, cracking, compression), memory (in-memory malware, credential dumping), disk (staging, encryption), network (exfiltration).
Inverted traffic ratio	Far more bytes out than in, sustained. One of the strongest exfiltration signals.
Unauthorised software	Anything outside the allow-list; portable executables; dual-use tools; remote access software outside IT.
Unauthorised configuration	Disabled AV or firewall, new local administrator, weakened password policy, audit logging off, modified <code>hosts</code> .

continued on the next page

HOST-RELATED INDICATORS

AV exclusions	Quieter and more durable than disabling AV outright.
Suspicious process	Wrong parent, wrong path, near-miss name, no matching disk image, unsigned in a system directory, unexpected network activity.
LOLBins	Signed, expected system binaries used for attacker goals: powershell, certutil, bitsadmin, mshta, rundll32, regsvr32, wmic, msbuild, vssadmin.
File system changes	Mass modification, writes to system directories, timestomping, alternate data streams, deleted logs, large archives in temp.
Timestomping	Timestamps altered to blend in; the MFT's two timestamp sets disagree afterwards.
Data exfiltration	Cloud upload, DNS or ICMP tunnel, HTTPS to attacker infrastructure, e-mail, removable media, steganography.

KEY POINT

The flag combination `-enc` with `-w hidden` and `-ep bypass` on `powershell.exe` is malicious until proven otherwise. `-enc` decodes base64 of UTF-16LE text.

APPLICATION, CLOUD AND IDENTITY INDICATORS

Service disruption	Slow, unresponsive or crashing application: DoS, resource exhaustion, or a failing exploit.
Web shell	New or modified file in the web root taking a command parameter.
Application anomalies	Error bursts, unusual parameter values, SQL errors in responses, new administrative accounts.
Cloud: new regions	Resources created where nobody looks. Classic cryptomining.
Cloud: cost spike	Frequently the first detection of cloud compromise.
Cloud: disabled logging	CloudTrail stopped, GuardDuty suspended, flow logs deleted. Identify the actor and verify an approved change.
Cloud: public storage	Bucket or container ACL opened to anonymous read.
Cloud: new IAM principal	User, role or policy created outside the pipeline, especially with a wildcard action.
Cloud: new access key	CreateAccessKey for another principal is persistence that survives a password reset.
Impossible travel	Two successful sign-ins too far apart for the elapsed time. Corporate VPN is the top false positive.
Password spraying	Many accounts, few passwords. Stays under lockout.
Credential stuffing	Many accounts, each with a known breached password.
Brute force	One account, many passwords.
MFA fatigue	Repeated push prompts until one is approved.
Dormant reactivation	An unused account suddenly authenticating.

SOCIAL ENGINEERING AND EMAIL

Typosquatting	A domain relying on a mistyped character.
Homoglyph / IDN	Visually identical characters from another script; Punycode (xn -) reveals it.
Combosquatting	Brand plus a plausible word.
Subdomain deception	Find the public suffix first; the registrable domain is the label immediately to its left plus that suffix (for example, example.co.uk).
URL shortener	Hides the destination. Expand from an isolated analysis host or a reputation service; even a HEAD request contacts every redirect.
Newly registered domain	One of the strongest single phishing features.
BEC	Email impersonation to redirect payment or extract data. Usually no malware at all.
SPF	May this IP send for the envelope domain?
DKIM	Is the signature valid and the body unmodified?
DMARC	Does the visible From domain align with SPF or DKIM, and what should I do if not?
Header red flags	From vs. Return-Path vs. Reply-To mismatch; unexpected relay low in the Received chain; new inbox rule after takeover.

1.3 Tools to determine malicious activity

COMPTIA OBJECTIVE 1.3

Given a scenario, use tools to determine malicious activity.

DECODING, PARSING AND PACKET ANALYSIS

CyberChef	Browser-based chained data transformations ("recipes"): base64, hex, XOR, URL decode, regex extract, Magic, entropy, file-type detection.
tcpdump	Command-line capture with BPF filters; prints summaries or writes PCAP.
Wireshark	Graphical protocol analyser; dissects, reassembles, filters what is <i>displayed</i> .
Snort	Signature-based IDS/IPS; rule = action, protocol, source, direction, destination, options.
Suricata	Multi-threaded equivalent; adds protocol logging, file extraction and eve.json output.
Zeek	Network security monitor. Primarily writes transaction logs (conn, dns, http, ssl, files); scripts and the Notice framework can also raise notice.log.

CAPTURE FILTER VS. DISPLAY FILTER

Capture filters use BPF and decide what is written (tcp port 80). Packets excluded here are gone forever. **Display filters** use Wireshark syntax and decide only what you see (tcp.port == 80). The dotted field name and == give it away.

TCPDUMP ESSENTIALS

<code>-i iface</code>	Interface; any for all.
<code>-nn</code>	No host or port name resolution.
<code>-s 0</code>	Full packet, not truncated.
<code>-w / -r</code>	Write / read a PCAP.
<code>-A / -X</code>	Payload as ASCII / hex and ASCII.
<code>-e</code>	Include link-layer headers (MACs).
<code>-c n</code>	Stop after <i>n</i> packets.

WIRESHARK DISPLAY FILTERS WORTH KNOWING

<code>ip.addr == x</code>	Either direction.
<code>tcp.flags.syn == 1 && tcp.flags.ack == 0</code>	Connection attempts — scanning.
<code>http.request.method == "POST"</code>	Uploads; exfiltration and web shells.
<code>dns.flags.rcode == 3</code>	NXDOMAIN — DGA hunting.
<code>tls.handshake.type == 1</code>	Client Hello, where the SNI is visible.
<code>tcp.stream eq n</code>	One conversation, for Follow Stream.
<code>frame contains "s"</code>	Raw byte search.

SNORT / SURICATA RULE OPTIONS

<code>msg</code>	Alert text.
<code>flow</code>	Session state and direction, e.g. <code>established, to_server</code> .
<code>content</code>	Byte string; hex inside pipes.
<code>nocase</code>	Case-insensitive for the preceding content.
<code>depth / offset</code>	Where in the payload to look.
<code>distance / within</code>	Position relative to the previous match.
<code>pcre</code>	Full regular expression; expensive, so gate it with content.
<code>dsize</code>	Payload size condition.
<code>flowbits</code>	State carried across packets in a session.
<code>threshold</code>	Rate limiting.
<code>classtype</code>	Category, which drives priority.
<code>sid / rev</code>	Unique signature ID and revision. Local rules from 1000000.

LOG ANALYSIS, INTELLIGENCE AND ENDPOINT

SIEM	Collect, normalise, enrich, correlate, alert, retain.
------	---

continued on the next page

LOG ANALYSIS, INTELLIGENCE AND ENDPOINT

Correlation rule	Fires on a combination of events across sources and time.
Alert tuning	Refining conditions, thresholds and scoped exclusions — not disabling.
OTX	Community pulses of indicators. <i>Subscribes</i> .
MISP	Controlled sharing between organisations. <i>Shares</i> .
OpenCTI	STIX 2.1 knowledge graph of actors, malware, techniques. <i>Relates</i> .
STIX	The format.
TAXII	The transport.
TLP	RED recipients only, AMBER organisation, GREEN community, CLEAR unrestricted.
EDR	Continuous endpoint telemetry, behavioural detection, retrospective search, and remote response including host isolation.
XDR	EDR correlated with e-mail, identity, cloud and network.
MDM	Mobile device inventory, posture and policy.
UEBA	Statistical baselines per user and entity; scores deviation. OpenUBA is the named open-source framework.

REPUTATION AND FILE ANALYSIS

WHOIS	Registration data. The <i>creation date</i> is the field that matters.
AbuseIPDB	Community abuse reports with a confidence score.
GEO-IP	Country and ASN from an address. Approximate; VPNs and carriers mislead it.
strings	Prints printable sequences from a binary. <code>-e 1</code> for Windows UTF-16LE strings.
VirusTotal	Aggregated engine verdicts, relations and behaviour. Submit <i>hashes</i> , not files.
YARA	Pattern-matching rules: meta, strings, condition. Matches content, so it survives recompilation.
Cuckoo Sandbox	Open-source, self-hosted dynamic analysis.
Joe Sandbox	Commercial deep analysis with strong evasion detection.
Sandbox evasion	Sleeps, VM artefact checks, no mouse movement, geofencing. A clean report is not proof of safety.

PATTERN RECOGNITION AND FORMATS

Regex metacharacters	<code>. * + ? {n,m} [] ^ \$ () \</code>
Character classes	<code>\d \w \s</code> and their negations <code>\D \W \S</code> ; <code>\b</code> is a word boundary.
Greedy vs. lazy	<code>.*</code> takes as much as possible; <code>.+?</code> stops at the first match.
Lookbehind	<code>(?<=...)</code> — requires <code>grep -P</code> .
JSON	Braces and brackets; real types. Cloud audit logs, APIs, STIX.
XML	Nested tags with attributes. SAML, Nessus, nmap <code>-oX</code> , Windows event XML.
YAML	Indentation-significant. Playbooks, pipelines, Kubernetes, Sigma.

continued on the next page

PATTERN RECOGNITION AND FORMATS

EVTX	Binary Windows Event Log. Parse with <code>Get-WinEvent</code> or <code>wevtutil</code> ; do not grep it.
Sigma	Vendor-neutral detection rules in YAML, compiled to each SIEM.
MXToolbox	Mail diagnostics: MX, SPF, DKIM, DMARC, blacklists, header analysis.

SCRIPTING LANGUAGES

Shell (bash)	Pipes <i>text</i> between tools. Unbeatable for filtering.
PowerShell	Pipes <i>objects</i> , so properties survive the pipeline. <code>Get-CimInstance Win32_Process</code> exposes parent PID and command line; <code>Get-Process</code> does not.
Python	Structured logic, APIs, parsing, automation beyond a one-liner.

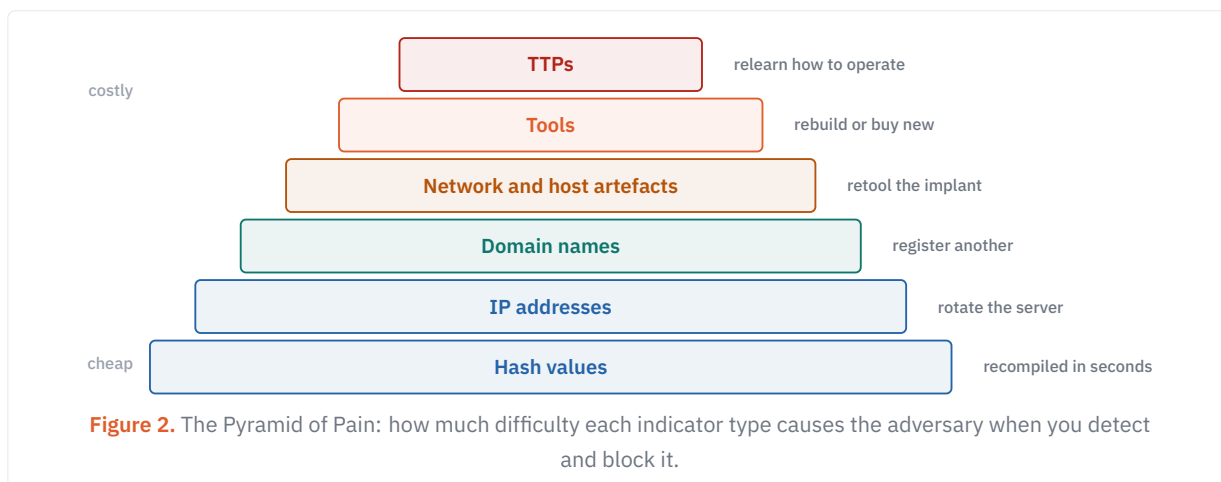
1.4 Threat intelligence and threat hunting

COMPTIA OBJECTIVE 1.4

Explain threat intelligence and threat-hunting concepts.

ACTORS AND TTPS

Threat intelligence	Evidence-based knowledge with context that supports a decision. Data alone is not intelligence.
Strategic / operational / tactical / technical	Board / campaign / TTP / atomic indicator.
APT	Well-resourced, usually state-sponsored, defined by <i>persistence</i> .
Insider threat	Malicious, negligent or compromised. Addressed by separation of duties, least privilege, recertification, DLP and UEBA.
Tactic / technique / procedure	Objective / method / specific implementation.
Pyramid of Pain	Hash, IP, domain, artefact, tool, TTP — cheapest to costliest for the adversary to change.
MITRE ATT&CK	Matrix of tactics (columns) and techniques (cells) with identifiers such as T1059.001. Not sequential.
Heat map	The matrix coloured by actor behaviour, detection coverage, or validation results — state which.
Attribution	Assigning an intrusion to an actor. Slow, uncertain, and subject to deliberate false flags.



CONFIDENCE, SOURCES AND INDICATORS

Timeliness	Is it current enough to act on?
Relevance	Does it apply to our technology, sector and geography?
Accuracy	Is it correct and correctly scoped? Failures here make analysts ignore the source.
OSINT	Free, broad, unverified, and equally available to the adversary.
Closed source	Curated and contextual; costly and sometimes unverifiable.
Sharing communities	ISACs, MISP communities, national CERTs. Reciprocity expected.
Internal intelligence	Your own incidents. The most relevant source you have.
Atomic indicator	A single indivisible fact — an IP, a domain.
Computed indicator	Derived: a hash, a regex match.
Behavioural indicator	A described pattern of activity. Survives retooling.
IoC lifecycle	Collect, analyse, apply (block, detect, hunt, enrich), expire.

THREAT MODELLING AND HUNTING

STRIDE	Spoofing/authentication, Tampering/integrity, Repudiation/non-repudiation, Information disclosure/confidentiality, Denial of service/availability, Elevation/authorisation.
Threat mapping	Relating generic threats to this environment's assets and data flows.
Threat hunting	Proactive, hypothesis-driven search for what detections missed. Assumes compromise.
Hypothesis	Specific and falsifiable, e.g. "an adversary is using WMI for lateral movement".
Stack counting	Frequency analysis; sort ascending. What is rare is interesting.
Hunt output	Ideally a new detection rule, not just an incident.

CYBER DECEPTION

Honeypot	A decoy system. Any interaction is suspicious by construction.
----------	--

continued on the next page

CYBER DECEPTION

Honeynet	A network of honeypots, to observe lateral movement.
Honeyfile	A decoy document whose access raises an alert.
Honeytoken	A decoy credential or record. Its use proves where it leaked.
Breadcrumbs	Deliberate traces leading an attacker toward the deception.
Deceptive endpoint	A decoy host inside the production network.
DNS sinkhole	Resolving known-bad domains to a controlled address; blocks C2 and identifies infected hosts.
Tarpit	Deliberately slow responses to waste attacker time.

1.5 Efficiency and process improvement

COMPTIA OBJECTIVE 1.5

Explain the importance of efficiency and process improvement in security operations.

PLAYBOOK VS. RUNBOOK

A **playbook** is strategic and conditional: the overall response to a class of incident, with decision points, roles and escalation. A **runbook** is tactical and procedural: the exact steps for one task. Playbooks reference runbooks.

AUTOMATION VS. ORCHESTRATION

Automation makes one task happen without a human. **Orchestration** coordinates many tasks across many systems into a workflow with branching and state.

STANDARDISATION AND STREAMLINING

Standardisation	One agreed, documented way to perform a recurring task. Must precede automation.
Team coordination	Defined roles, structured handover, ticket hygiene, tiering, written escalation criteria.
SOAR	Ingests alerts, runs playbooks through integrations, manages cases, measures each step.
Automate first	Enrichment, deduplication, evidence creation, notification, and containment only on high-confidence signals.
Human in the loop	Required for destructive actions on low-confidence signals.
IaC	Infrastructure defined in version-controlled files. Gives repeatability, review and drift detection — and deploys mistakes everywhere at once.
Data enrichment	Adding owner, criticality, geo-IP, identity and intelligence context before a human sees the alert.

continued on the next page

STANDARDISATION AND STREAMLINING

Rule / alert tuning	Threshold change, scoped exclusion, added context conditions, suppression, severity re-rating, retirement.
Precision and recall	Tuning raises precision; disabling destroys recall.
Dashboards	One audience, one question per panel, trend over snapshot, actionable thresholds, drill-through, honest denominators.

TOOL INTEGRATION

API	You call them, on demand. Pull.
Webhook	They call you, on an event. Push. Must be authenticated.
Plug-in	Code loaded inside another product to extend it.
Connector	Vendor-maintained integration package.
Message queue	Asynchronous, buffered, many-to-many; survives a consumer outage.
Rate limiting	HTTP 429. An unhandled limit silently stops enrichment mid-morning.

1.6 Artificial intelligence in security operations

COMPTIA OBJECTIVE 1.6

Summarize concepts related to the use of AI in security operations.

AI RISKS

Hallucination	Confident, fluent output that is wrong or invented.
Data exposure	Confidential input transmitted to, retained by, or trained on by a third party.
Model poisoning	Training or fine-tuning data manipulated so the model learns the attacker's preferred behaviour.
Malicious prompts	Prompt injection, jailbreaking, system-prompt extraction.
Indirect prompt injection	The instruction arrives inside the <i>data</i> the model is asked to read — a web page, a document, an e-mail body.
Over-reliance	Analysts stop verifying; skills erode.
Bias	Training data patterns reproduced, including unfair ones.
Explainability	A model that cannot say why is hard to defend to an auditor.
Shadow AI	Unsanctioned tools adopted without approval.
Adversarial input	Crafted perturbations causing misclassification.

GOVERNANCE AND USE CASES	
AI usage policy	Approved tools, permitted data by classification, permitted reliance on output, named accountability, disclosure, logging, review cadence.
Accountability	Always the human who acts on the output.
NIST AI RMF	Govern, Map, Measure, Manage.
ISO/IEC 42001	Certifiable AI management system.
EU AI Act	Risk-tiered obligations.
GDPR Article 22	Restricts decisions made solely by automated processing.
OWASP Top 10 for LLMs	Application-level risks, led by prompt injection.
Use cases	Comparing artifacts, analysing logs, document creation, incident investigation, event correlation, automation and orchestration.
Limits	Generated code, regex and rules must be tested; facts and timelines must be verified; regulated data never goes into a public model.

Vulnerability Management

Scanning method, tool output, prioritisation, and the control and risk vocabulary that frames all of it.

2.1 Vulnerability scanning methods

COMPTIA OBJECTIVE 2.1

Given a scenario, implement the appropriate vulnerability scanning method.

ASSET INVENTORY AND PLANNING

Asset inventory	Authoritative record of what is owned, with identity, owner, criticality, classification, software, network position and lifecycle state. The precondition for everything else.
Scheduling	When a scan may run without disrupting the business.
Operations	What the target does and who depends on it.
Performance	The load the target and the network will tolerate.
Sensitivity levels	How fragile the device class is — PLCs, medical devices, legacy printers.
Segmentation	Where the scanner sits relative to the target. A path with a firewall in it produces a falsely clean report.
Regulatory requirements	What must be scanned, how often, and by whom. PCI DSS: quarterly internal and external, external by an ASV, rescan after significant change.

SCAN TYPES — FIVE PAIRS

Internal vs. external	Inside the perimeter vs. from the public internet.
Agent vs. agentless	Host software reports itself vs. the scanner reaches across the network. Agents cover roaming laptops; agentless finds unknown hosts.
Credentialed vs. non-credentialed	Authenticates and reads real package versions vs. infers from banners. Credentialed removes back-port false positives.
Passive vs. active	Observes traffic vs. sends probes. Passive is the answer for OT and fragile devices.
Discovery vs. full scan	Mapping and fingerprinting vs. complete vulnerability assessment.
Mapping scan	Which hosts exist and which ports are open.
Device fingerprinting	What each host is: OS, version, device type, service versions.

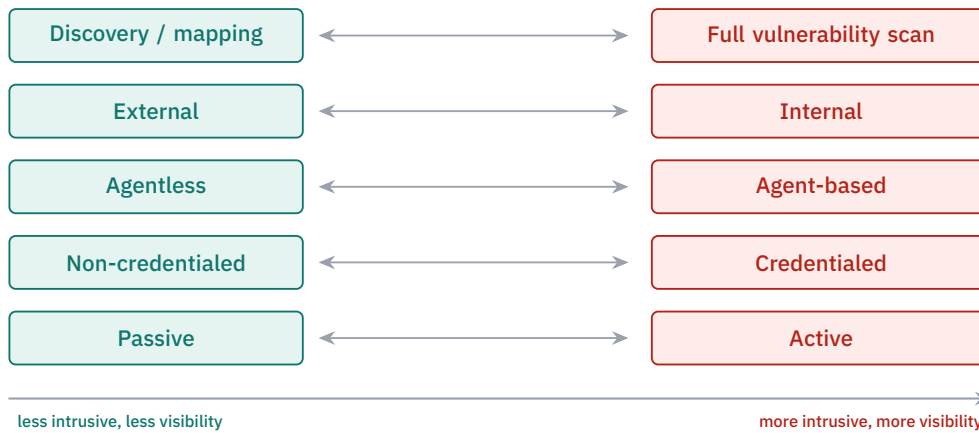


Figure 3. Every scan-type choice is the same trade-off. Everything to the right sees more and disturbs more.

THE BACK-PORT FALSE POSITIVE

“The scanner reports a flaw the patch team says is fixed” is a banner-based false positive. Red Hat and Debian back-port fixes without changing the version string. The proof is the package changelog or vendor advisory, and the cure is a credentialed scan.

NMAP PORT STATES

open	A service accepted the connection.
closed	The host sent a reset. Reachable, nothing listening — which also proves the host is alive.
filtered	No reply, or ICMP unreachable. Something in the path dropped the probe.
unfiltered	Reachable but state undetermined (ACK scans).
open filtered	No response and both states look identical — typical of UDP and FIN/NULL/Xmas scans.

SECURITY BASELINE SCANNING

Baseline scan	Compares configuration against a defined standard, rather than looking for known software flaws.
PCI DSS	Cardholder data. Prescriptive scanning requirements; external scans by an Approved Scanning Vendor.
CIS Benchmarks	Platform hardening guidance; Level 1 safe, Level 2 defence in depth.
ISO/IEC 27000 series	27001 is the certifiable requirements standard; 27002 is control guidance.
DISA STIG	US Department of Defense hardening; stricter than CIS.
NIST SP 800-53	Control catalogue for US federal and regulated contexts.

2.2 Vulnerability assessment tool output

COMPTIA OBJECTIVE 2.2

Given a scenario, analyze output from vulnerability assessment tools.

NETWORK SCANNING AND MAPPING

Angry IP Scanner	Small graphical host and port scanner. Quick sweeps; not a vulnerability scanner.
Masscan	Asynchronous mass port scanner; internet-scale speed. Finds open ports; does not fingerprint well. <code>--rate</code> must be agreed in advance.

MULTIPURPOSE TOOLS

Nmap	Discovery, port scanning, service and OS fingerprinting, NSE scripts.
Metasploit (MSF)	Exploitation framework. Module types: exploit, payload, auxiliary, post, encoder. Meterpreter runs in memory. Analyst use is <i>validation</i> , with authorisation.
Maltego	Graphical link analysis; entities and transforms build a relationship graph.
Recon-ng	Command-line OSINT framework with workspaces, modules and a results database. Scriptable and repeatable.
theHarvester	Collects e-mail addresses, subdomains and hostnames from public sources.

NMAP SWITCHES

<code>-sS / -sT</code>	SYN (half-open, needs root) / full connect.
<code>-sU</code>	UDP. Slow and ambiguous.
<code>-sn</code>	Host discovery only. <code>-PR</code> uses ARP locally.
<code>-Pn</code>	Skip discovery; assume hosts are up. Needed when ICMP is filtered.
<code>-p- / --top-ports n</code>	All ports / the <i>n</i> most common.
<code>-sV / -O</code>	Service versions / OS fingerprint.
<code>-A</code>	Aggressive: <code>-sV</code> , <code>-O</code> , scripts, traceroute. Loud.
<code>-T0 ...-T5</code>	Timing. T0 evasive, T3 default, T4 normal LAN.
<code>--script name</code>	Run NSE scripts or a category such as <code>vu1n</code> .
<code>-iL file</code>	Targets from a file.
<code>-oN / -oX / -oG / -oA</code>	Normal / XML / greppable / all three.

WEB APPLICATION SCANNERS

Burp Suite	Intercepting proxy with scanner, repeater and intruder. Interactive manual testing; Community edition omits the active scanner.
------------	---

continued on the next page

WEB APPLICATION SCANNERS

OWASP ZAP	Open-source intercepting proxy and scanner; runs headless in CI.
Nikto	Web <i>server</i> scanner: dangerous files, outdated software, default configuration, missing headers. Noisy; not application-aware.

VULNERABILITY SCANNERS

Nessus	Commercial standard; large plugin library, credentialed scanning, compliance auditing.
OpenVAS	Open-source equivalent; network vulnerability tests; more setup effort.
Nuclei	Fast, YAML-template-driven; ideal for sweeping an estate for one new CVE quickly.
Plugin Output	The evidence field in a Nessus finding. A finding without it is an inference.
Port 0	Marks a finding from a local credentialed check, not a network service.

FALSE POSITIVE VS. FALSE NEGATIVE

A **false positive** is a reported flaw that is not there — visible and wasteful. A **false negative** is a real flaw not reported — invisible and dangerous. Causes of false negatives: host off, port filtered, no credentials, no plugin, asset not in scope.

CLOUD ASSESSMENT AND BAS

ScoutSuite	Multi-cloud configuration review via provider APIs; offline HTML report. Post-deployment.
Prowler	AWS-focused checks mapped to CIS, PCI, HIPAA, GDPR, NIST. Compliance-framed. Post-deployment.
Trivy	Container images, filesystems, repositories, IaC. Vulnerable packages, secrets, misconfiguration. Build time.
Checkov	Static analysis of Terraform, CloudFormation, Kubernetes, Helm, ARM. Pre-deployment.
Atomic Red Team	Library of small tests, one per ATT&CK technique, with cleanup.
Caldera	MITRE's automated adversary emulation platform; chained abilities and planning.
BAS	Measures whether controls prevent, detect and log — a finding about the <i>programme</i> , not the estate.

2.3 Prioritising and mitigating vulnerabilities

COMPTIA OBJECTIVE 2.3

Given a scenario, analyze data to prioritize and mitigate vulnerabilities.

CRITERIA

Exploitability	How difficult to exploit in practice.
Active exploitation	CISA KEV membership. An observation, not a prediction — it should override scores.
Asset value	What the system does and what data it holds.
Impact	What actually happens if exploited here.
Patch availability	No fix means the conversation moves to compensating controls.
True / false positives	Confirm the finding before spending effort.
True / false negatives	Coverage gaps are findings in their own right.

CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:L/SI:L/SA:N/AU:Y/R:U/RE:M/U:Green

Base — exploitability

Base — impact on the vulnerable system

Base — impact on subsequent systems

Supplemental — context only, never changes the score

No E: (Threat) and no CR: /MAV: (Environmental) metrics are present in this vector

Figure 4. A CVSS v4.0 vector, colour-coded by metric group.

CVSS V4.0 — BASE EXPLOITABILITY

AV	Attack Vector: Network, Adjacent, Local, Physical. Severity falls across that list.
AC	Attack Complexity: Low (no evasion needed) or High.
AT	Attack Requirements: None or Present. New in v4.0.
PR	Privileges Required: None, Low, High.
UI	User Interaction: None, Passive, Active. New granularity in v4.0.

CVSS V4.0 — IMPACT AND OTHER GROUPS

VC / VI / VA	Confidentiality, Integrity, Availability impact on the <i>vulnerable</i> system.
SC / SI / SA	The same for <i>subsequent</i> systems. Together these replaced v3.1's Scope metric.
E (Threat)	Exploit Maturity: Attacked, Proof-of-concept, Unreported, X not defined. X is scored as <i>Attacked</i> .
CR / IR / AR (Environmental)	Confidentiality, Integrity and Availability <i>requirements</i> for this asset. How asset value enters the score.
M-prefixed metrics	Modified base metrics reflecting your environment, e.g. MAV:L.

continued on the next page

CVSS V4.0 — IMPACT AND OTHER GROUPS

Supplemental: S, AU, R, V, RE, U	Safety, Automatable, Recovery, Value density, Response Effort, provider Urgency. <i>Context only — never changes the score.</i>
CVSS-B / BT / BE / BTE	Which groups were used. BTE is the operational score.
Ratings	0.1–3.9 Low, 4.0–6.9 Medium, 7.0–8.9 High, 9.0–10.0 Critical.

WHICH VERSION AM I LOOKING AT?

S:C or S:U means CVSS v3.1. VC: and SC: mean v4.0. AT: and a three-value UI: are also v4.0 only.

EPSS AND CONTEXT

EPSS	Probability of exploitation in the next 30 days, 0–1, plus a percentile. Recalculated daily.
CVSS vs. EPSS	Severity if exploited vs. likelihood of being exploited. Use both; let KEV override both.
Internal	Reachable only from inside. Reduces exposure, not insider risk.
External	Internet reachable. Raises priority sharply.
Isolated	Segmented or air-gapped. Reduces priority — verify the claim before relying on it.

MITIGATION STRATEGIES

Attack surface management	Continuous discovery and reduction of what is exposed.
Secure coding	Input validation, output encoding, parameterised queries, safe libraries, least privilege.
Patching and configuration management	The primary remediation, with testing, staging and rollback.
Exceptions	Documented, time-limited, risk-accepted, approved by the owner.
Compensating controls	Alternative controls when the fix cannot be applied. Must meet the intent and rigour of the original requirement.
Virtual patching	WAF or IPS rule blocking exploitation while the flaw remains.
Validation of remediation	Credentialed rescan, configuration review, version verification, or an authorised exploit attempt. A closed ticket is not validation.

KEY POINT

Two validation failures the exam likes: the patch was installed but the service was never restarted, and the change was applied to one host in a load-balanced pool.

2.4 Control types, risk and vulnerability management

COMPTIA OBJECTIVE 2.4

Explain concepts related to control types, risks, and vulnerability management.

CONTROL TYPES (WHAT IT IS)

Administrative	Also managerial. Policies, procedures, standards, training, background checks, separation of duties.
Technical	Also logical. Firewalls, encryption, authentication, ACLs, IDS, EDR.
Physical	Locks, fences, guards, cameras, vestibules, fire suppression.

CONTROL FUNCTIONS (WHAT IT DOES)

Preventative	Stops the event. Acts before.
Detective	Identifies that it happened or is happening.
Responsive	Reacts during the event to limit it.
Corrective	Restores and fixes the underlying cause, after.
Also seen	Deterrent (discourages the attempt), directive (instructs behaviour), compensating (alternative to the primary control).

RISK CONCEPTS

Inherent risk	Before any controls.
Residual risk	What remains after controls.
Risk appetite	How much risk the organisation is willing to pursue.
Risk tolerance	Acceptable variation around appetite for a specific activity.
Accepted risk	Residual risk a named owner formally decided to live with.
Risk register	Risk, owner, likelihood, impact, controls, residual score, treatment, review date.
Qualitative	Ratings and heat maps. Fast, subjective.
Quantitative	$SLE = \text{asset value} \times \text{exposure factor}$; $ALE = SLE \times ARO$.

RISK MANAGEMENT STRATEGIES

Mitigate	Reduce likelihood or impact with controls. The default.
Transfer	Move the financial consequence — insurance, contractual indemnity, outsourcing. Accountability never transfers.
Avoid	Stop doing the activity.
Accept	Documented, approved decision to live with the residual risk.

GOVERNANCE VOCABULARY

Policy is mandatory intent (what and why). **Standard** is a mandatory specific requirement. **Procedure** is how. **Guideline** is advisory. **Baseline** is the minimum configuration.

SLA is the external contract. **SLO** is the internal target, normally stricter. **SLI** is the measurement.

APPLICATION SECURITY

SAST	Static. Reads source or byte code without running it. Early, needs source, many false positives, blind to runtime and configuration.
DAST	Dynamic. Tests the running application from outside. Later, no source needed, few false positives, blind to unreachable code paths.
IAST	Instrumented inside the running application; sees code path and runtime behaviour.
RASP	Runtime self-protection that blocks attacks. A control, not a test.
Fuzzing	Malformed or random input to find crashes and unhandled conditions.
SAMM	OWASP Software Assurance Maturity Model. Measures the maturity of the programme, not the security of an application.

THIRD-PARTY RISK

Supply chain risk	Risk inherited from software, hardware and services you consume.
SCA	Software composition analysis: identifies third-party and open-source components, their versions, vulnerabilities and licences.
SBOM	A formal machine-readable inventory of every component and dependency. Formats: SPDX and CycloneDX.
Why SBOM	Log4Shell. The question was not “is Log4j vulnerable” but “where do we have it”.
Vendor due diligence	Questionnaires, certification evidence (ISO 27001, SOC 2 Type II), test summaries — before signature.
Contractual controls	Right to audit, breach notification timelines, security standards, subcontractor limits, data location.
Continuous monitoring	Reassessment through the relationship, not once at onboarding.

Incident Response and Management

Models, lifecycle, and the techniques that contain an incident without destroying the evidence.

3.1 Attack methodology frameworks

COMPTIA OBJECTIVE 3.1

Summarize concepts related to attack methodology frameworks.

CYBER KILL CHAIN — SEVEN PHASES

Reconnaissance	Research the target; harvest addresses. Defence: attack surface management.
Weaponisation	Couple an exploit with a payload. <i>No defensive opportunity — it happens on their infrastructure.</i>
Delivery	E-mail, web, removable media, supply chain. The highest-value control point.
Exploitation	The vulnerability or the user is triggered.
Installation	Persistence is established.
Command and control	The implant calls home.
Actions on objectives	Exfiltrate, encrypt, destroy, pivot.
Limitation	Linear and perimeter-shaped; weak on insiders, credential-only attacks, and repeated lateral movement.

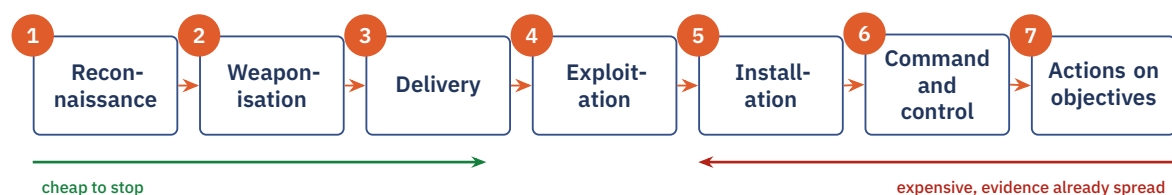


Figure 5. The Cyber Kill Chain. Stopping an intrusion gets rapidly more expensive from left to right.

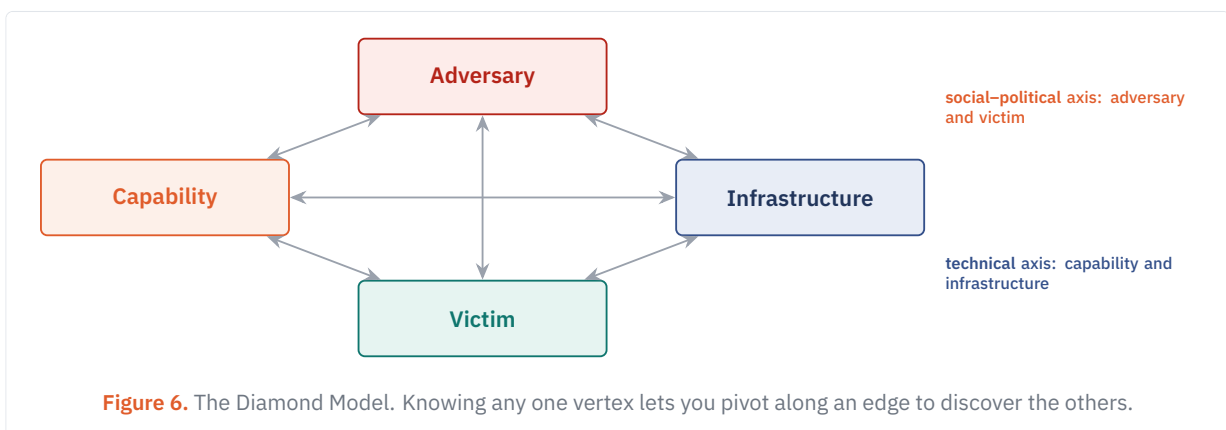
DIAMOND MODEL

Adversary	Who is doing it.
Capability	Malware, exploit, technique.
Infrastructure	Domains, addresses, mail, C2.
Victim	Organisation, host, person, data.
Social–political axis	Adversary to victim.

continued on the next page

DIAMOND MODEL

Technical axis	Capability to infrastructure.
Event	One diamond, with meta-features: timestamp, phase, result, direction, methodology, resources.
Activity thread	Related events ordered by phase.
Activity group	Threads sharing features — how an “actor” is defined in practice.
Analytic pivot	Moving along an edge from a known vertex to an unknown one. The model’s operational purpose.



MITRE ATT&CK IN RESPONSE

Structure	Tactics are columns (objectives); techniques and sub-techniques are cells, identified as T1059.001.
Tagging	Record each observation against a technique ID.
Prediction	Credential Access is usually followed by Discovery and Lateral Movement.
Scoping	A technique implies artefacts, which turns a vague scope into a query.
Gap analysis	Which observed techniques were detected, found late, or missed entirely.
Reporting	Technique IDs make the after-action report shareable.

KEY POINT

Kill chain gives the *narrative*; the Diamond Model gives the *pivots*; ATT&CK gives the *detections*. They are complementary.

3.2 The incident response process

COMPTIA OBJECTIVE 3.2

Summarize the incident response process.

THE SEVEN PHASES

Preparation	Plan, people, authority, tooling, telemetry, training, tested offline backups. Determines how every other phase goes.
Detection	Automated detection, hunting, human report, external notification, third-party monitoring.
Analysis	Is it real, what is the scope, when did it start, how did they get in, what is the impact, is it ongoing.
Containment	Stop the spread while preserving evidence. Short-term and long-term.
Eradication	Remove every persistence mechanism <i>and</i> close the entry point.
Recovery	Restore from a clean point, validate, return in priority order, monitor closely.
Post-incident	Lessons learned, after-action report, root cause analysis, metrics, owned improvements.
NIST grouping	Preparation; Detection and Analysis; Containment, Eradication and Recovery; Post-Incident Activity.

EVENT, ALERT, INCIDENT

An **event** is any observable occurrence. An **alert** is an event a detection flagged. An **incident** is an event that harms or imminently threatens confidentiality, integrity or availability. *Declaration* starts the clocks and the obligations.

CONTAINMENT: THE ONE TO REMEMBER

Do not power the machine off. Isolate it from the network, capture volatile evidence, image the disk, and only then consider shutdown. Power-off destroys RAM, and with it processes, injected code, network state and sometimes the encryption key.

EXERCISES AND RECOVERY OBJECTIVES

Tabletop	Discussion-based walk-through. Cheap; finds plan and communication gaps; does not test tooling.
Walk-through / drill	Stepping through procedures on real systems.
Simulation	Executing the response against a controlled injected scenario.
Red / purple team	Adversarial, with purple adding attacker–defender collaboration.
RTO	Recovery time objective — how quickly service must return. Time forward.
RPO	Recovery point objective — how much data loss is acceptable. Time backward; sets backup frequency.

3.3 Incident response techniques

COMPTIA OBJECTIVE 3.3

Given a scenario, implement incident response techniques.

PLANS AND PLAYBOOKS

Incident response plan	Scope, definitions, severity criteria, roles, <i>authority to act</i> , escalation, evidence handling, legal obligations, external support, review cycle.
Communication plan	Stakeholders, single spokesperson, approved statements, channels including out-of-band, regulatory timelines, approval.
Playbook	Strategic, conditional response to a class of incident.
Runbook	Tactical, ordered steps for one task.
Roles	Incident commander, lead analyst, scribe, communications lead — named in advance.
Training	Tabletop and simulation, repeated.

TRIAGE AND TIMELINE

Triage	Rapid assessment of whether it is real, how severe, and what response it gets.
Severity factors	Data sensitivity, system criticality, scope, attack stage, reversibility, exposure, regulatory trigger.
Log collection	Gather relevant logs including those not normally forwarded; record who collected what, when, with hashes.
Log correlation	Join across sources on a common key.
Log augmentation	Add owner, criticality, identity, geo-IP, intelligence.
Timeline	One ordered sequence in UTC, every line sourced, inference marked as inference.

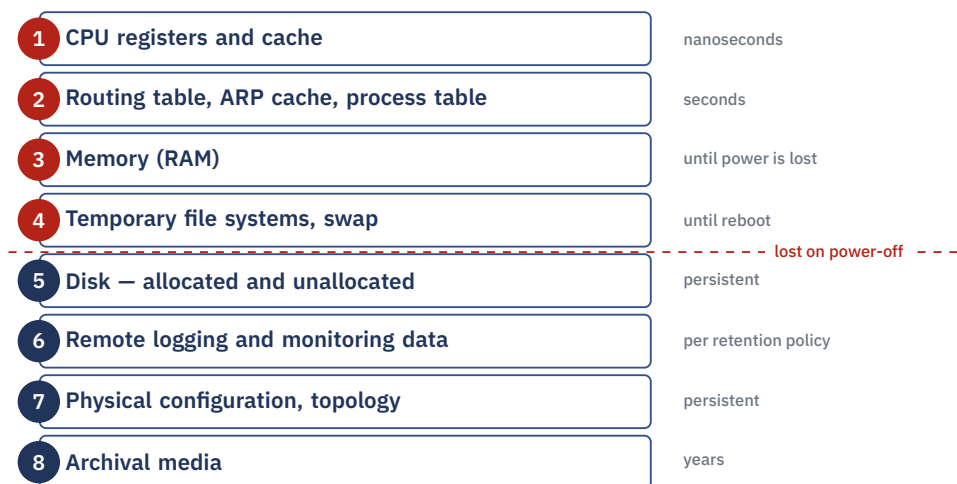


Figure 7. Order of volatility. Everything above the line is gone the moment the machine loses power.

EVIDENCE HANDLING

Work on a copy	Acquire an image; never analyse the original.
Write blocker	Prevents any write to the source medium.
Bit-for-bit image	Captures unallocated space as well as files.
Hashing	Hash source and image; re-verify at each transfer. SHA-256.
Chain of custody	Item, date and time in UTC, person, purpose, hashes, storage location — signed, with no gaps.
Data integrity validation	Re-hashing to prove nothing changed.
Preservation	Protecting specific evidence from deletion or rotation.
Legal hold	Formal instruction making preservation compulsory; overrides retention.
Spoliation	Destroying or altering evidence relevant to a legal matter.
e-Discovery	Identifying, preserving, collecting and producing electronic information for legal process.

ISOLATION, ESCALATION, REMEDIATION

EDR host isolation	Blocks all traffic except the management channel. Fast, reversible, preserves memory. The default answer.
NAC quarantine	Move the host to a restricted VLAN.
Account disablement	Disable, do not delete — deletion destroys the audit trail and the SID.
Firewall / DNS block	Contains C2 across the estate rather than one host.
Cloud isolation	Detach, deny-all security group, revoke instance role sessions.
Escalation	By written criteria — severity, data type, criticality, duration, inability to contain — not by instinct.
Remediation	Patch, reconfigure, reset credentials, rebuild.
Verification	Rescan, re-hunt, confirm persistence gone and entry closed.
Release from isolation	Only after verification, with heightened monitoring.

ROOT CAUSE ANALYSIS

Five whys	Ask why until the answer is systemic, not an event.
Fishbone (Ishikawa)	Categorise causes: people, process, technology, environment.
Fault tree	Work backwards from the failure through contributing conditions.
Timeline analysis	The timeline itself often exposes the systemic gap.
Corrective action	Addresses the root cause; has a named owner, a due date and tracking. “Improve awareness” is not one.

Reporting and Communication

Telling the right people the right thing, at the right time, in language they can act on.

4.1 Vulnerability management reporting

COMPTIA OBJECTIVE 4.1

Explain the importance of vulnerability management reporting and communication.

VULNERABILITY SCAN REPORTS

Scope and method	What was scanned, when, from where, credentialed or not — and explicitly what was <i>not</i> scanned.
Executive summary	Posture, trend, and the two or three decisions needed. No CVE numbers.
Findings	Identifier, affected assets, severity with the scoring method named, evidence, remediation, effort.
Prioritised action plan	Ordered list with owners and dates.
Exceptions	What will not be fixed, why, who approved, when it is reviewed.
Trend data	Comparison with previous cycles.
Appendices	Raw output, methodology, tool versions, disproved false positives.

COMPLIANCE FINDINGS AND SCORECARDS

Framed by requirement	“Requirement 6.3.3 not met”, not “CVE-2024-1234”.
Binary outcome	Pass or fail per requirement.
External deadlines	Audit dates do not move for engineering capacity.
Evidence	Being compliant and demonstrating compliance are different problems.
Scope reduction	Tokenise, segment, or stop holding the data. Often cheaper than remediation.
Risk scorecard	A small number of consistent measures per unit, system or supplier, tracked over time. Not a findings list.
Stable denominators	A scorecard whose denominator changes each quarter measures nothing.

ACTION PLANS

Owner	A named individual, not a team mailbox.
Deadline	Derived from the SLA for that severity.

continued on the next page

continued from the previous page

ACTION PLANS

Escalation	What happens when the date passes, and to whom.
Dependencies	Vendor patch, change window, test cycle, downstream systems. The most common cause of a missed date.
Validation	How the fix will be proved, and by whom.
Interim risk	The compensating control applying meanwhile.

INHIBITORS TO REMEDIATION

Contractual agreements	Supplier contract forbids change, or an MSP controls the system.
Organisational governance	Change approval or competing priorities delay work.
Business process interruption	The required downtime is refused.
Degrading functionality	The patch breaks something the business relies on.
Legacy systems	Out of support, unsupported by the fix, or too fragile.
Proprietary systems	Vendor appliance you may not patch without voiding support.
Patch availability	No fix exists yet.
The shape of every answer	Reduce exposure with a compensating control, state the residual risk, get it accepted by a named owner, set a review date.

STAKEHOLDERS

Executive leadership	Business risk, cost, regulatory exposure. Give them a page, a trend, and the decision needed.
System owner	The specific finding, the specific fix, the window, the risk of deferring.
IT operations	A prioritised, scheduled work list with tested procedures.
Development	Findings in the issue tracker, mapped to the component, with the fixed version.
Legal and compliance	Facts, dates, obligations, what is documented.
Risk management	Risk statements with likelihood, impact and treatment.
Auditors and regulators	Evidence of a functioning process.

METRICS AND KPIS

Mean time to remediate	Detection to verified fix, split by severity. The headline metric.
SLA compliance rate	Percentage remediated within the agreed window.
Open findings by severity	Backlog. Needs a trend and a denominator.
Vulnerability age	Distribution, which exposes the long tail an average hides.
Scan coverage	Percentage of known assets actually scanned. Validates every other number.

continued on the next page

METRICS AND KPIS

Recurrence rate	How often the same finding returns. Measures whether remediation is real.
Exception count and age	How much risk is formally accepted, and whether it is reviewed.
Top risks	The few findings carrying most of the exposure.
Misleading metrics	Total vulnerabilities (rewards not scanning), average CVSS (arithmetic on an ordinal scale), patches applied (activity, not risk).

4.2 Incident response reporting and communication

COMPTIA OBJECTIVE 4.2

Explain the importance of security operations and incident response reporting and communication.

DECLARATION AND ESCALATION

Incident declaration	Formally stating an event is an incident. Activates the plan, assigns the commander, starts every clock.
What it triggers	Plan activation, pre-agreed authority, regulatory and contractual clocks, preservation obligations, notification assessment, cost recording.
Declare early	Regulatory clocks run from when you <i>knew</i> . De-escalating a benign declaration costs almost nothing.
Escalation	By written criteria; technical, managerial and external paths each with their own trigger.

EXECUTIVE SUMMARY

What happened	Plain language, no jargon.
Impact	Customers affected, data types, downtime, financial and regulatory exposure.
Status	Contained, eradicated, recovered, or still active.
Actions taken	The three or four that matter.
Next steps	And when.
Decisions required	Explicitly — including “none”.
Confidence	What is known, what is assessed, what is unknown.

COMMUNICATION PLAN

Stakeholder identification	Executives, legal, PR, regulators, law enforcement, customers, employees, suppliers, insurers.
----------------------------	--

continued on the next page

COMMUNICATION PLAN

Legal team	Engage early — privilege and deadlines both depend on it.
Public relations	One authorised spokesperson; approved holding statements.
Regulatory agencies	Factual notification within the statutory deadline, with supplementary reports as facts develop.
Law enforcement	Evidence, timeline, indicators.
Customers	What happened, what data, what it means, what to do, where to get help.
Operational security	Out-of-band channels; need to know; one source of truth; no speculation in writing; record decisions and reasoning.

NOTIFICATION DEADLINES TO RECOGNISE

GDPR	72 hours to the supervisory authority; without undue delay to data subjects where the risk is high.
HIPAA	60 days to individuals; 500 or more also to HHS and the media.
PCI DSS	Immediately to the acquirer and card brands on suspicion.
SEC (US public)	Four business days from determining materiality.
NIS2	Early warning typically within 24 hours, fuller report to follow.
Contractual	Often stricter than regulation. Read the contract.

POST-INCIDENT REPORTING

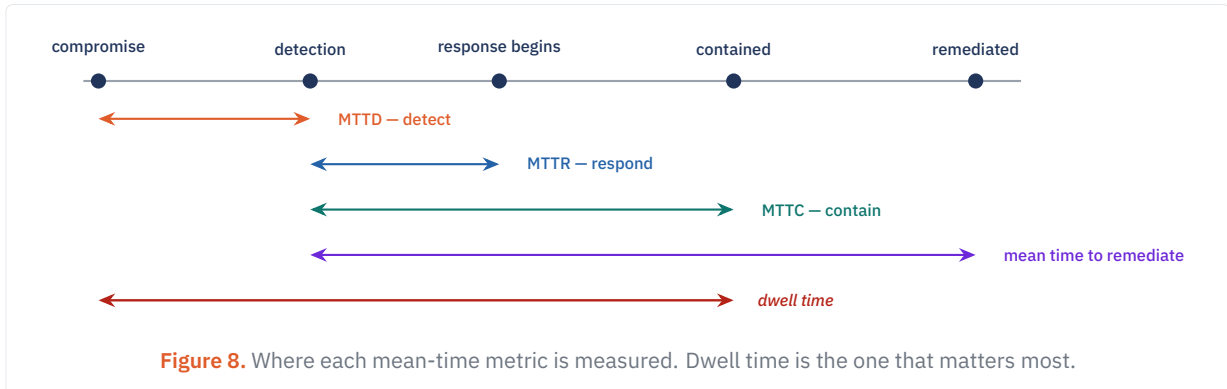
After-action report	Executive summary, timeline, scope and impact, attack narrative, detection and response performance, root cause, indicators, lessons learned, recommendations, appendices.
Lessons learned	The meeting and its findings. Blameless, prompt, attended by everyone involved.
Root cause analysis	Why it was possible, not what happened.
Shift / incident handover	Status, actions with times, pending items, decisions <i>and their reasoning</i> , outstanding decisions, evidence location, contacts, watch items.
Internal threat intelligence report	What this incident revealed, tailored to your environment. The most relevant intelligence you will ever have.

METRICS AND KPIS

Alert volume	Workload and noise.
False-positive rate	Wasted effort; the leading cause of genuine alerts being dismissed.
True-positive rate	Detection quality. Only meaningful beside the false-positive rate.
Mean time to detect	How long an adversary operates unseen.
Mean time to respond	Detection to the start of human action.
Mean time to contain	How quickly the bleeding stops.

continued on the next page

METRICS AND KPIS	
Mean time to remediate	How quickly the cause is removed.
Mean time to close	Administrative closure including documentation.
Dwell time	Compromise to containment. The most honest single measure.
Phishing click rate	Pair it with the <i>report</i> rate.
Escalation rate	Rising escalation usually means tier 1 lacks tooling or authority.



METRICS CHANGE BEHAVIOUR

Measure time-to-close alone and tickets get closed faster, including the ones that needed investigating. Measure alert volume alone and rules get disabled. Measure click rate alone and people stop reporting. Always pair a speed metric with a quality metric.

Ports and Protocols

Ports, protocols and the security question each one raises. The selection is weighted towards what a CySA+ analyst actually meets in logs, scans and packet captures.

HOW TO USE THIS TABLE

Memorising numbers is necessary but not sufficient. For each port, know three things: the number, what runs there, and *what it means when you see it somewhere unexpected*. The rightmost column is the one the exam tests.

A.1 File transfer and remote access

Port	Transport	Service	Analyst note
20, 21	TCP	FTP	Credentials and data are clear text unless protected separately. Port 21 is control; port 20 carries data in active mode, while passive mode uses a negotiated high port. Unexpected or anonymous FTP merits investigation.
22	TCP	SSH / SCP / SFTP	Encrypted admin access. Outbound SSH to the internet from a server is a common tunnelling and exfiltration channel.
23	TCP	Telnet	Clear text. Should not exist. Its presence on a network device is a hardening failure.
69	UDP	TFTP	No authentication at all. Used for device configuration backups, and abused to pull or push firmware.
115	TCP	Simple File Transfer Protocol	A historical protocol unrelated to SSH File Transfer Protocol (also called SFTP), which normally uses port 22.
989, 990	TCP	FTPS	Implicit FTP over TLS: 990 is control and 989 is active-mode data. Explicit FTPS starts on 21; passive data uses negotiated high ports.
3389	TCP/UDP	RDP	Legitimate when restricted to approved administrators and jump hosts. Direct internet exposure is high risk; an ordinary endpoint initiating RDP to an unusual peer may indicate lateral movement.
5900–5905	TCP	VNC	Often unauthenticated or weakly authenticated.
5985, 5986	TCP	WinRM (HTTP / HTTPS)	PowerShell Remoting. Workstation to workstation on these ports is lateral movement.

A.2 Web and email

Port	Transport	Service	Analyst note
80	TCP	HTTP	Clear text. Where web shells, C2 and downloads hide in plain sight.
443	TCP	HTTPS / TLS	Encrypted. Almost always permitted outbound, which is exactly why C2 uses it. Inspect SNI, JA3 and certificate details.
8080, 8443	TCP	Alternate HTTP / HTTPS	Proxies, management interfaces, application servers. Frequently forgotten and unpatched.
25	TCP	SMTP	Mail transfer. Outbound 25 from a workstation means either a misconfigured client or a spam bot.
587	TCP	SMTP submission	Authenticated client submission, with STARTTLS.
465	TCP	SMTPS	Implicit TLS submission.
110	TCP	POP3	Clear text mail retrieval.
995	TCP	POP3S	POP3 over TLS.
143	TCP	IMAP	Clear text mail access.
993	TCP	IMAPS	IMAP over TLS.

A.3 Name resolution, directory and authentication

Port	Transport	Service	Analyst note
53	TCP/UDP	DNS	UDP for queries, TCP for zone transfers and large responses. Long random labels and TXT floods mean tunnelling.
853	TCP	DNS over TLS (DoT)	Encrypted DNS. Defeats plaintext DNS monitoring; often blocked for that reason.
443	TCP	DNS over HTTPS (DoH)	Indistinguishable from web traffic without endpoint controls. A real detection problem.
67, 68	UDP	DHCP (server, client)	Rogue DHCP servers enable man-in-the-middle.
88	TCP/UDP	Kerberos	Windows domain authentication. Watch for ticket requests with weak encryption — Kerberoasting.
389	TCP/UDP	LDAP	Clear text directory queries. Large result sets from one account is enumeration.
636	TCP	LDAPS	LDAP over TLS.
3268, 3269	TCP	Global Catalog (LDAP, LDAPS)	Forest-wide directory queries.

continued on the next page

continued from the previous page

Port	Transport	Service	Analyst note
464	TCP/UDP	Kerberos password change	
137–139	TCP/UDP	NetBIOS (name, datagram, session)	Legacy Windows networking. Should not cross network boundaries.
445	TCP	SMB / CIFS	File sharing and remote administration. <i>Outbound 445 to the internet is almost always malicious.</i>
1812, 1813	UDP	RADIUS (auth, accounting)	Network access authentication.
49	TCP	TACACS+	Device administration authentication; encrypts the whole payload, unlike RADIUS.

A.4 Management, monitoring and time

Port	Transport	Service	Analyst note
123	UDP	NTP	Time synchronisation. Also a reflection and amplification vector; <code>monlist</code> should be disabled.
161, 162	UDP	SNMP (agent, trap)	v1 and v2c use clear-text community strings; <code>public</code> and <code>private</code> are still found in the wild. Use v3.
514	UDP	Syslog	Unauthenticated and unencrypted; trivially spoofed.
6514	TCP	Syslog over TLS	The correct choice for log transport.
9997	TCP	Splunk forwarder	Agent to indexer. Worth knowing when troubleshooting ingestion.
5044	TCP	Beats / Logstash	Elastic ingestion.
514	TCP	Shell (rsh)	Legacy remote shell. Clear text.

A.5 Databases

Port	Transport	Service	Analyst note
1433, 1434	TCP, UDP	Microsoft SQL Server (service, browser)	Exposure beyond the application tier is a segmentation finding.
1521	TCP	Oracle TNS listener	
3306	TCP	MySQL / MariaDB	

continued on the next page

continued from the previous page

Port	Transport	Service	Analyst note
5432	TCP	PostgreSQL	
27017	TCP	MongoDB	Historically shipped without authentication; a long-running source of public data exposure.
6379	TCP	Redis	Historically deployed without authentication. Modern versions add protected mode and ACLs, but internet exposure or a permissive bind remains a serious remote-code-execution risk.
9200, 9300	TCP	Elasticsearch (REST, transport)	Another frequent public exposure.
11211	TCP/UDP	Memcached	Massive UDP amplification factor; should never be internet facing.

A.6 Industrial, virtualisation and other

Port	Transport	Service	Analyst note
502	TCP	Modbus TCP	No authentication, no encryption. Seeing it outside the OT segment is a serious finding.
20000	TCP/UDP	DNP3	Utility SCADA protocol. Same concerns.
44818	TCP/UDP	EtherNet/IP	Industrial automation.
102	TCP	S7comm (Siemens)	Programmable controller protocol.
2375, 2376	TCP	Docker API (plain, TLS)	An exposed unauthenticated Docker socket is equivalent to root on the host.
6443	TCP	Kubernetes API server	
2049	TCP/UDP	NFS	Network file system; check export permissions.
873	TCP	rsync	Often unauthenticated; a quiet exfiltration channel.
1194	UDP	OpenVPN	
500, 4500	UDP	IPsec IKE, NAT-T	
1723	TCP	PPTP	Obsolete and broken; flag it.
3128	TCP	Squid proxy	
9001, 9030	TCP	Tor (OR, directory)	Tor use from a corporate host is worth investigating.

A.7 Ports that usually mean trouble

Port	Associated with	Why it matters
4444	Metasploit default handler	The most recognisable malicious port on the exam. Almost never legitimate.
1337, 31337	Traditional backdoors	“Elite” numbering; still used by commodity tooling.
5555	Android Debug Bridge	Exposed ADB gives full device control.
6660–6669	IRC	Classic botnet command channels; also legitimate chat, so correlate.
8333	Bitcoin	Cryptomining or wallet activity on a corporate host.
3333, 4444, 5555, 7777	Mining pool ports	Common Stratum ports; pair with sustained high CPU.
0	Nmap “port 0” in a report	Not a real port — it marks a finding that came from a local credentialed check.

THE TEN TO KNOW WITHOUT HESITATION

22 SSH • 53 DNS • 80 HTTP • 88 Kerberos • 389 LDAP • 443 HTTPS • 445 SMB • 3389 RDP • 514 syslog • 4444 Metasploit. Between them these account for the large majority of port-related exam questions.

Command Reference

Every command in this guide, collected in one place, with the flags that matter and nothing that does not. Organised by the question you are trying to answer.

NOTE

Commands shown with `sudo` require privileges. Placeholders are *italic*. Where a command differs between Linux and Windows, both are given.

B.1 What is on this host?

BASH Linux triage, first five minutes

```
uname -a; hostnamectl                # kernel, distribution, hostname
uptime; who -a; last -n 20           # load, sessions, login history
id; sudo -l                          # my identity and my privileges
ps -eo pid,ppid,user,lstart,pcpu,args --sort=-pcpu | head -n 20
sudo ss -tulpn                       # listening sockets with owning process
sudo lsof -n -P -i                   # every process holding a network socket
sudo crontab -l; ls -la /etc/cron.*   # scheduled execution
systemctl list-units --type=service --state=running --no-pager
sudo find / -xdev -perm -4000 -type f 2>/dev/null # setuid binaries
sudo find /tmp /dev/shm /var/tmp -type f -executable 2>/dev/null
```

POWERSHELL Windows triage, first five minutes

```
systeminfo | Select-String 'OS Name','OS Version','Hotfix'
Get-LocalUser | Where-Object Enabled
Get-LocalGroupMember -Group 'Administrators'
Get-CimInstance Win32_Process | Select ProcessId,ParentProcessId,Name,CommandLine
Get-NetTCPConnection -State Listen,Established | Sort-Object State
Get-ScheduledTask | Where-Object { $_.Author -notmatch 'Microsoft' }
Get-Service | Where-Object Status -eq 'Running' | Select Name,DisplayName,PathName
Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run'
Get-MpComputerStatus | Select RealTimeProtectionEnabled,AntivirusSignatureAge
Get-MpPreference | Select -ExpandProperty ExclusionPath
```

B.2 What is on the network?

DISCOVERY AND SCANNING

<code>nmap -sn <i>cidr</i></code>	Host discovery only. Add <code>-PR</code> for ARP on a local segment.
<code>nmap -sS -p- <i>host</i></code>	SYN scan, all 65,535 TCP ports.

continued on the next page

DISCOVERY AND SCANNING

<code>nmap -sU -top-ports 100 host</code>	The hundred most common UDP ports. UDP scanning is slow and ambiguous by nature.
<code>nmap -sV -O host</code>	Service versions and operating-system fingerprint.
<code>nmap -Pn host</code>	Skip discovery; treat the host as up. Essential when ICMP is filtered.
<code>nmap --script vuln host</code>	Run the vulnerability NSE category.
<code>nmap -oA base</code>	Write all three output formats.
<code>masscan cidr -pports -rate n</code>	Very fast port discovery at scale. Agree the rate first.
<code>ss -tulpn</code>	Listening sockets, numeric, with process.
<code>ip -br addr; ip -br link</code>	Interfaces and addresses, brief.
<code>ip neigh</code>	The ARP/neighbour table.
<code>arp -a</code>	Same, portable form.
<code>traceroute / tracet host</code>	Path to a destination.

NAME RESOLUTION AND REPUTATION

<code>dig name A</code>	Query an A record.
<code>dig +short name</code>	Answer only.
<code>dig -x ip</code>	Reverse lookup.
<code>dig name TXT</code>	TXT records — SPF, DKIM, DMARC, and DNS tunnels.
<code>dig @server domain AXFR</code>	Attempt a zone transfer. Should fail; if it succeeds, that is the finding.
<code>nslookup name</code>	Portable equivalent, available on Windows.
<code>Resolve-DnsName name</code>	The PowerShell version.
<code>whois domain</code>	Registration data. The creation date is the field that matters.
<code>whois ip</code>	Netblock owner, country, abuse contact.
<code>curl -sIL url</code>	Follow redirects with headers only — expand a shortened link without loading the page.

B.3 What is in this traffic?

TCPDUMP

<code>-i iface</code>	Interface. any for all.
<code>-nn</code>	No name or port resolution. Always use it.

continued on the next page

TCPDUMP	
<code>-s 0</code>	Capture the full packet.
<code>-w file</code>	Write a PCAP.
<code>-r file</code>	Read a PCAP.
<code>-c n</code>	Stop after <i>n</i> packets.
<code>-A / -X</code>	Payload as ASCII / as hex and ASCII.
<code>-e</code>	Include link-layer (MAC) headers.
<code>-G secs -W n</code>	Rotate output files.
<code>host ip</code>	Filter: to or from that address.
<code>net cidr</code>	Filter: that network.
<code>port n</code>	Filter: that port, either direction.
<code>tcp[tcpflags] & (tcp-syn) != 0</code>	Filter: SYN set — connection attempts.
<code>greater n</code>	Filter: packets larger than <i>n</i> bytes.

TSHARK AND WIRESHARK DISPLAY FILTERS	
<code>tshark -r file -Y 'filter'</code>	Read a capture, apply a display filter.
<code>tshark -T fields -e field</code>	Print bare field values, one record per line.
<code>tshark -q -z conv,tcp</code>	Conversation statistics — find exfiltration by bytes.
<code>ip.addr == x</code>	Either direction.
<code>tcp.flags.syn == 1 && tcp.flags.ack == 0</code>	Connection attempts.
<code>http.request.method == "POST"</code>	Uploads.
<code>dns.qry.name contains "s"</code>	Suspicious query names.
<code>dns.flags.rcode == 3</code>	NXDOMAIN responses.
<code>tls.handshake.type == 1</code>	Client Hello — where the SNI lives.
<code>tcp.stream eq n</code>	One conversation, for Follow Stream.
<code>frame contains "text"</code>	Raw byte search.

B.4 What is in these logs?

BASH The text-processing idioms worth memorising

```
# Count occurrences of a field and show the most frequent.
awk '{print $9}' access.log | sort | uniq -c | sort -rn | head -n 20

# The inverse: show the RAREST values. This is stack counting, and it is how
```

BASH continued

```
# threat hunting finds the one odd parent process among ten thousand.
awk '{print $9}' access.log | sort | uniq -c | sort -n | head -n 20

# Extract all IPv4 addresses from anything.
grep -aoE '\b(?:[0-9]{1,3}\.){3}[0-9]{1,3}\b' *.log | sort -u

# Extract a value that follows a label, without the label.
grep -oP '(?<=user=)\S+' auth.log | sort | uniq -c | sort -rn

# Everything in a time window (works because ISO-8601 sorts correctly).
awk -F'"' '$0 >= "2026-09-21T03:00" && $0 <= "2026-09-21T04:00"' events.log

# Join two files on a common key.
sort -k1,1 hosts.txt > /tmp/a; sort -k1,1 owners.txt > /tmp/b
join -1 1 -2 1 /tmp/a /tmp/b

# Lines in A that are not in B (requires both sorted).
comm -23 <(sort a.txt) <(sort b.txt)

# Watch a log live, filtered.
tail -F /var/log/auth.log | grep --line-buffered -E 'Failed|Accepted'
```

GREP FLAGS THAT EARN THEIR PLACE

-r	Recurse into directories.
-i	Ignore case.
-n	Show line numbers.
-v	Invert — lines that do <i>not</i> match.
-c	Count matching lines.
-l	List only the filenames that matched.
-o	Print only the matching portion.
-a	Treat binary files as text.
-I	Skip binary files entirely.
-E	Extended regular expressions.
-P	Perl-compatible regular expressions (lookarounds, \K).
-F	Fixed strings — no regex, much faster.
-w	Match whole words only.
-A n / -B n / -C n	Lines of context after, before, or both.
-exclude-dir=d	Skip a directory such as <code>.git</code> .

POWERSHELL The Windows Event Log, properly

```
# Filter at the source. FilterHashtable is dramatically faster than Where-Object.
Get-WinEvent -FilterHashtable @{
    LogName      = 'Security'
    Id           = 4625, 4624, 4672
    StartTime    = (Get-Date).AddHours(-24)
} -MaxEvents 5000
```

POWERSHELL continued

```
# Read a saved .evtx file.
Get-WinEvent -Path C:\evidence\Security.evtx -FilterXPath "*[System[EventID=4688]]"

# Export for analysis elsewhere.
Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4688} |
  Select-Object TimeCreated, Id, @{n='Cmd';e={$_.Properties[8].Value}} |
  Export-Csv -NoTypeInfo C:\evidence\proc.csv

# The command-line utility equivalents.
wevtutil qe Security /q:"*[System[(EventID=4625)]]" /f:text /c:20
wevtutil epl Security C:\evidence\Security.evtx
```

Event ID	Meaning
4624	Successful logon. Check the <i>logon type</i> : 2 interactive, 3 network, 10 remote interactive (RDP).
4625	Failed logon. The volume and pattern distinguish brute force from spraying.
4634 / 4647	Logoff / user-initiated logoff.
4648	Logon with explicit credentials — often <code>runas</code> , often lateral movement.
4672	Special privileges assigned. Effectively “an administrator logged on”.
4688	New process created. With command-line auditing enabled, the single most valuable event on Windows.
4697	A service was installed. Classic persistence.
4698 / 4702	Scheduled task created / updated.
4719	System audit policy changed. Somebody is turning off the lights.
4720 / 4726	User account created / deleted.
4728 / 4732	Member added to a security-enabled group.
4740	Account locked out.
1102	The audit log was cleared. Always investigate.
7045	A service was installed (System log).
4104	PowerShell script block logging — the actual script text.

B.5 What is this file?**BASH** Static file triage

```
file suspicious.bin
xxd suspicious.bin | head -n 4
sha256sum suspicious.bin
strings -n 8 suspicious.bin | head -n 60
strings -e l -n 6 suspicious.bin | head
yara -r -s rules.yar suspicious.bin
exiftool document.docx
binwalk -e firmware.bin

# identify by magic bytes
# 'MZ' = PE, 'PK' = zip/OOXML, '7F ELF'
# the identifier to look up, never upload
# ASCII strings
# UTF-16LE strings (Windows)
# match against rules, show why
# metadata: author, tool, timestamps
# find and extract embedded files
```

POWERSHELL The Windows equivalents

```
Get-FileHash -Algorithm SHA256 .\suspicious.bin
Get-AuthenticodeSignature .\suspicious.bin | Select Status, SignerCertificate
Get-Content .\suspicious.bin -Encoding Byte -TotalCount 4 | ForEach-Object { '{0:X2}' -f $_ }
Get-Item .\suspicious.bin -Stream * # alternate data streams
certutil -hashfile .\suspicious.bin SHA256
```

B.6 Encoding, hashing and encryption

BASH Three operations that are frequently confused

```
echo -n 'text' | base64 # encode (reversible, no key)
echo -n 'dGV4dA==' | base64 -d # decode
echo -n 'dGV4dA==' | base64 -d | iconv -f UTF-16LE -t UTF-8 # PowerShell -enc payloads

echo -n 'text' | sha256sum # hash (one way, no key)
sha256sum -c manifest.sha256 # verify a set of files

openssl enc -aes-256-cbc -pbkdf2 -in a -out a.enc # encrypt (reversible, needs a key)
openssl enc -d -aes-256-cbc -pbkdf2 -in a.enc -out a

openssl s_client -connect host:443 -servername host < /dev/null 2>/dev/null |
openssl x509 -noout -subject -issuer -dates # inspect a certificate
```

B.7 Evidence acquisition

BASH In order of volatility

```
# 1. Volatile state, to external media
ss -tunap > /mnt/ev/sockets.txt
ps -eo pid,ppid,user,lstart,args > /mnt/ev/processes.txt
ip neigh > /mnt/ev/arp.txt; ip route > /mnt/ev/routes.txt
lsof -n -P > /mnt/ev/openfiles.txt

# 2. Memory
sudo ./avml /mnt/ev/memory.lime
sha256sum /mnt/ev/memory.lime > /mnt/ev/memory.lime.sha256

# 3. Disk, through a write blocker
sudo dcflddd if=/dev/sda of=/mnt/ev/sda.dd hash=sha256 \
hashlog=/mnt/ev/sda.hashes bs=4M conv=sync,noerror

# 4. Verify
sha256sum /dev/sda > /mnt/ev/source.sha256
```

KEY POINT

Two flags in that block are the ones a performance-based question is likely to probe. `conv=sync,noerror` keeps every byte at its correct offset when a sector cannot be read — without it, one bad sector corrupts the remainder of the image. And hashing *both* the source and the image, recorded separately, is what makes the copy defensible.

B.8 Quick conversions

BASH Things you will want at 03:00

```
date -u -d @1758421047 +%FT%TZ      # epoch seconds -> ISO-8601 UTC
date -u -d '2026-09-21T03:14:07Z' +%s  # and back again
TZ=UTC date -d '2026-09-21 03:14:07 EDT' # convert a local timestamp to UTC

python3 -c "import ipaddress;print(list(ipaddress.ip_network('10.20.30.0/28')))"
python3 -c "import ipaddress;print(ipaddress.ip_address('10.20.30.55') in
↪ ipaddress.ip_network('10.20.0.0/16'))"

printf '%d\n' 0x1f90                # hex -> decimal (8080)
printf '0x%x\n' 4444                # decimal -> hex
```

Queries, Rules and Patterns

Detection logic in the four languages the exam is most likely to show you, plus the regular expressions worth carrying in your head.

C.1 Reading any query language

KEY POINT

Every query language on this exam expresses the same five ideas. Find them in whatever syntax is on the screen and the query reads itself: *filter* (narrow the events), *extract* (pull a field out), *group* (by some key), *aggregate* (count, sum, distinct count), and *threshold* (keep only the interesting groups).

Idea	Splunk SPL	Sentinel KQL	Elastic
filter	search / where	where	field:value
group + aggregate	stats count by f	summarize count() by f	terms aggregation
distinct count	dc(f)	dcount(f)	cardinality
collect values	values(f)	make_set(f)	top hits
rename	rename a AS b	project b = a	–
sort	sort - f	order by f desc	sort
limit	head n	take n	size
time window	earliest=-24h	ago(24h)	range filter
regex extract	rex field=x "..."	extract() / parse	grok / dissect

C.2 Detections worth recognising

SIEM QUERY Password spraying — many accounts, few passwords

```
index=wineventlog EventCode=4625 earliest=-1h
| stats count AS failures, dc(TargetUserName) AS accounts,
  values(WorkstationName) AS sources by IpAddress
| where accounts > 10 AND failures/accounts < 5
| sort - accounts
```

NOTE

The second condition is what separates spraying from brute force: many distinct accounts, but few attempts *per* account. Reverse the ratio and you have a brute-force detection instead.

SIEM QUERY Impossible travel — two sign-ins, two countries

```
index=azuread ResultType=0 earliest=-24h
| sort 0 user, _time
| streamstats current=f last(_time) AS prev_t last(Country) AS prev_c by user
| where Country != prev_c
| eval minutes = round((_time - prev_t)/60, 1)
| where minutes < 240
| table _time, user, prev_c, Country, minutes
```

SIEM QUERY Beaconing — regularity, not destination

```
index=proxy earliest=-24h
| sort 0 src_ip, dest, _time
| streamstats current=f last(_time) AS prev_t by src_ip, dest
| eval gap = _time - prev_t
| stats count AS hits, avg(gap) AS avg_gap, stdev(gap) AS sd_gap by src_ip, dest
| where hits > 20 AND avg_gap > 20 AND sd_gap < (avg_gap * 0.15)
| sort sd_gap
```

SIEM QUERY Data exfiltration — an inverted byte ratio

```
index=firewall direction=outbound earliest=-24h
| stats sum(bytes_out) AS out, sum(bytes_in) AS in by src_ip, dest_ip
| eval ratio = round(out/(in+1), 1)
| where out > 500000000 AND ratio > 10
| sort - out
```

SIEM QUERY Rare parent-child pairs — stack counting in query form

```
index=edr event_type=process_create earliest=-7d
| stats count AS n, values(host) AS hosts by parent_name, process_name
| where n < 5
| sort n
```

SNORT / SURICATA RULE Four rules, four techniques

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 4444 ( msg:"Possible Meterpreter C2";
  flow:established,to_server; dsize:>100; threshold:type limit, track by_src,
  count 1, seconds 300; classtype:trojan-activity; sid:1000401; rev:2; )

alert udp $HOME_NET any -> any 53 ( msg:"Possible DNS tunnelling - long query";
  dns.query; bsize:>100; threshold:type threshold, track by_src, count 50,
  seconds 60; classtype:policy-violation; sid:1000402; rev:1; )

alert http $EXTERNAL_NET any -> $HOME_NET any ( msg:"Directory traversal attempt";
  flow:established,to_server; http.uri; content:"../"; nocase;
  pcre:"/(\.\\.|\\|/|%2f){2,}/i"; classtype:web-application-attack;
  sid:1000403; rev:3; )

alert tcp $HOME_NET any -> $EXTERNAL_NET 445 ( msg:"SMB leaving the network";
  flow:established,to_server; classtype:policy-violation; sid:1000404; rev:1; )
```

YARA RULE A rule that survives recompilation

```
rule Generic_Encoded_PowerShell_Cradle
{
  meta:
    author      = "soc-team"
    description = "Encoded PowerShell download cradle, any family"
```

YARA RULE continued

```
reference = "attack.mitre.org/techniques/T1059/001"

strings:
    $p = "powershell"          nocase ascii wide
    $e1 = "-EncodedCommand"    nocase ascii wide
    $e2 = "-enc "              nocase ascii wide
    $e3 = "FromBase64String"    nocase ascii wide
    $d1 = "DownloadString"      nocase ascii wide
    $d2 = "DownloadFile"        nocase ascii wide
    $d3 = "Invoke-WebRequest"  nocase ascii wide
    $h1 = "IEX"                 nocase ascii wide
    $h2 = "Invoke-Expression"  nocase ascii wide

condition:
    filesize < 5MB and $p and any of ($e*) and any of ($d*) and any of ($h*)
}
```

YAML The same idea as Sigma, which compiles to any SIEM

```
title: Encoded PowerShell download cradle
id: 3f1b9d64-2a77-4e0a-9d0b-0d4f1c6a9d21
status: stable
description: Detects base64-encoded PowerShell that downloads and executes code
references:
  - https://attack.mitre.org/techniques/T1059/001/
logsource:
  category: process_creation
  product: windows
detection:
  selection_img:
    Image|endswith: '\powershell.exe'
  selection_enc:
    CommandLine|contains:
      - '-enc '
      - '-EncodedCommand'
      - 'FromBase64String'
  selection_dl:
    CommandLine|contains:
      - 'DownloadString'
      - 'DownloadFile'
      - 'Invoke-WebRequest'
  condition: selection_img and selection_enc and selection_dl
falsepositives:
  - Legitimate administrative automation that encodes its own payloads
level: high
tags:
  - attack.execution
  - attack.t1059.001
```

C.3 Regular expressions worth carrying

REGEX Identifiers

<code>\b(?:\d{1,3}\.){3}\d{1,3}\b</code>	IPv4 address (loose)
<code>\b((25[0-5] 2[0-4]\d 1\d\d [1-9]?\d)\.){3}(25[0-5] 2[0-4]\d 1\d\d [1-9]?\d)\b</code>	IPv4 (strict)
<code>\b(?:[A-Fa-f0-9]{2}[:-]){5}[A-Fa-f0-9]{2}\b</code>	MAC address
<code>\b[A-Fa-f0-9]{32}\b</code>	MD5
<code>\b[A-Fa-f0-9]{40}\b</code>	SHA-1
<code>\b[A-Fa-f0-9]{64}\b</code>	SHA-256
<code>\b[\w.+-]+@[\w-]+\.[\w.]{2,}\b</code>	email address
<code>\bhttps?://[^\s"<>]+</code>	URL
<code>\b(?:[a-z0-9-]+\.)+(?:com net org io ru cn xyz top)\b</code>	domain (crude)
<code>\bCVE-\d{4}-\d{4,7}\b</code>	CVE identifier
<code>\bT\d{4}(?:\.\d{3})?\b</code>	ATT&CK technique id
<code>\b4[0-9]{12}(?:[0-9]{3})?\b</code>	Visa card number
<code>\b\d{3}-\d{2}-\d{4}\b</code>	US social security number

REGEX Attack patterns

<code>(?i)(\bunion\b.{0,40}\bselect\b \bor\b\s+1\s*=\s*1)</code>	SQL injection probe
<code>(?i)(%2e%2e(%2f %5c) \.\.(\./ \\))\{2,\}</code>	directory traversal
<code>(?i)<script\b[^\>]*> javascript: onerror\s*=</code>	cross-site scripting
<code>(?i)(; \ && \` \\$)\s*(cat curl wget nc bash sh powershell)\b</code>	command injection
<code>(?i)-e(nc ncodedcommand)\s+[A-Za-z0-9+/=]{40,\}</code>	encoded PowerShell
<code>(?i)\b(vssadmin wbadmin)\b.{0,40}\b(delete shadows)\b</code>	ransomware precursor
<code>[A-Za-z0-9+/]{60,\}={0,2}</code>	long base64 blob
<code>(?i)\b(AKIA ASIA)[A-Z0-9]{16}\b</code>	AWS access key id
<code>-----BEGIN (RSA OPENSSH EC)?PRIVATE KEY-----</code>	private key material

REGEX Log field extraction with named groups

```
^(?<ts>\S+\S+\S+\S+\S+)\s+(?<host>\S+)\s+sshd\[ (?<pid>\d+)\]:\s+Failed password for (?:  
  ↳ invalid user )?(?<user>\S+) from (?<ip>\S+) port (?<port>\d+)  
  
^(?<ip>\S+)\s+\S+\s+\[(?<ts>[^\]]+)\]\s+"(?<method>[A-Z]+) (?<uri>\S+) (?<proto>[^\"]+)" (?<  
  ↳ status>\d{3}) (?<size>\d+|-)  
  
^(?<ts>\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:\d{2}(?:\.\d+)?Z)\s+(?<level>\w+)\s+(?<msg>.*)$
```

THE THREE REGEX MISTAKES THAT COST MARKS

1. An unescaped `.` matches any character, so `10.0.0.1` also matches `10x0y0z1`. Escape it: `10\.0\.0\.1`. 2. `.*` is greedy and will swallow everything to the last possible match; `.*?` stops at the first. 3. Anchors matter: without `^` and `$`, a pattern matches anywhere in the line, which is usually what you want for hunting and exactly what you do not want for validation.

Frameworks at a Glance

Every framework, model and standard named in the objectives, reduced to what it is, what it is for, and how to tell it from the one it is usually confused with.

D.1 Attack and intrusion models

Model	Answers	Shape
Cyber Kill Chain	What sequence did the intrusion follow?	Seven linear phases: reconnaissance, weaponisation, delivery, exploitation, installation, command and control, actions on objectives.
Diamond Model	How do the pieces of this event relate?	Four vertices: adversary, capability, infrastructure, victim. Two axes: social–political and technical.
MITRE ATT&CK	What exactly did they do, and what is it called?	A matrix of tactics (columns) and techniques (cells), with identifiers such as T1059.001. Not sequential.
Unified Kill Chain	Both of the above, in more detail	Eighteen phases across <i>in</i> , <i>through</i> and <i>out</i> . Addresses the original kill chain's weakness on lateral movement.
STRIDE	What could go wrong with this design?	Six threat categories, each the violation of one security property.
Pyramid of Pain	Which indicator hurts the adversary most?	Six tiers: hash, IP, domain, artefact, tool, TTP — cheapest to costliest to change.

	STRIDE threat	Property violated
S	Spoofing identity	Authentication
T	Tampering with data	Integrity
R	Repudiation	Non-repudiation
I	Information disclosure	Confidentiality
D	Denial of service	Availability
E	Elevation of privilege	Authorisation

D.2 MITRE ATT&CK enterprise tactics, in order

	Tactic	The adversary is trying to
TA0043	Reconnaissance	gather information for planning.
TA0042	Resource Development	establish infrastructure and capability.
TA0001	Initial Access	get into the network.
TA0002	Execution	run malicious code.
TA0003	Persistence	maintain their foothold.
TA0004	Privilege Escalation	gain higher permissions.
TA0005	Defense Evasion	avoid detection.
TA0006	Credential Access	steal credentials.
TA0007	Discovery	learn the environment.
TA0008	Lateral Movement	move through the environment.
TA0009	Collection	gather the data of interest.
TA0011	Command and Control	communicate with compromised systems.
TA0010	Exfiltration	steal the data out.
TA0040	Impact	manipulate, interrupt or destroy.

NOTE

Technique identifiers worth recognising on sight: T1566 phishing, T1059 command and scripting interpreter (.001 PowerShell, .003 Windows command shell, .004 Unix shell), T1003 OS credential dumping (.001 LSASS memory), T1053 scheduled task/job, T1071 application layer protocol (C2), T1486 data encrypted for impact (ransomware), T1078 valid accounts, T1190 exploit public-facing application.

D.3 Process and lifecycle models

Model	Phases
CompTIA incident response	Preparation → Detection → Analysis → Containment → Eradication → Recovery → Post-incident.
NIST SP 800-61	Preparation → Detection and Analysis → Containment, Eradication and Recovery → Post-Incident Activity. The same work, grouped into four.
Intelligence lifecycle	Direction → Collection → Processing → Analysis → Dissemination → Feedback.
Vulnerability management	Identify → Assess and prioritise → Remediate or mitigate → Validate → Report → repeat.
NIST Cybersecurity Framework 2.0	Govern, Identify, Protect, Detect, Respond, Recover. <i>Govern</i> is the function added in version 2.0.

continued on the next page

Model	Phases
NIST AI Risk Management Framework	Govern, Map, Measure, Manage.

D.4 Standards, benchmarks and regulations

Name	Type	What it is for
ISO/IEC 27001	Certifiable standard	Requirements for an information security management system. What you certify against.
ISO/IEC 27002	Guidance	The control catalogue that supports 27001.
ISO/IEC 42001	Certifiable standard	Management system for artificial intelligence.
NIST SP 800-53	Control catalogue	Controls for US federal systems; widely used elsewhere.
NIST SP 800-61	Guidance	Computer security incident handling.
NIST SP 800-207	Guidance	Zero Trust architecture; the source of PE, PA, PDP and PEP.
CIS Benchmarks	Configuration standard	Platform-specific hardening, Level 1 (safe) and Level 2 (defence in depth).
CIS Critical Security Controls	Prioritised control set	Eighteen controls in implementation groups IG1–IG3.
DISA STIGs	Configuration standard	US Department of Defense hardening; stricter than CIS.
PCI DSS	Regulation (contractual)	Cardholder data. Quarterly internal and external scans, external by an ASV, rescan after significant change.
HIPAA	Regulation (US)	Protected health information; 60-day breach notification to individuals.
GDPR	Regulation (EU/UK)	Personal data; 72-hour notification to the supervisory authority.
SOX	Regulation (US)	Financial reporting integrity; drives change control and audit logging.
NIS2	Regulation (EU)	Critical-sector cybersecurity and incident reporting.
EU AI Act	Regulation (EU)	Risk-tiered obligations for AI systems.
OWASP Top 10	Awareness document	The ten most critical web application risks. There is also a Top 10 for LLM applications and one for APIs.
OWASP SAMM	Maturity model	Assessing and improving a software security programme.
OSSTMM	Methodology	Open Source Security Testing Methodology Manual.

D.5 Scoring and classification systems

System	Measures	Notes
CVSS v4.0	Severity, 0.0–10.0	Groups: Base, Threat, Environmental, Supplemental. Supplemental never changes the score.
EPSS	Probability of exploitation in 30 days, 0–1	Updated daily; pairs with CVSS rather than replacing it.
CISA KEV	Observed exploitation	A catalogue, not a score. Membership should override other prioritisation.
CVE	Identifier	A unique name for a vulnerability. Not a score.
CWE	Classification	The <i>type</i> of weakness, e.g. CWE-89 SQL injection. A CVE is an instance of a CWE.
CPE	Identifier	A structured name for a platform or product.
CAPEC	Classification	Common attack patterns.
TLP	Handling label	RED (recipients only), AMBER (organisation), GREEN (community), CLEAR (unrestricted).
Admiralty scale	Source and information grading	Letter A–F for reliability, digit 1–6 for credibility.

EXAM TRAP: CVE VS. CWE

CVE names one specific vulnerability in one specific product — CVE-2021-44228 is Log4Shell. **CWE** names the *class* of weakness — CWE-917 is expression-language injection, which is what Log4Shell is. Vulnerability reports cite CVEs; secure-coding guidance and SAST findings cite CWEs.

D.6 Intelligence sharing

Term	Meaning
STIX	The format. A JSON language for describing indicators, actors, campaigns and relationships.
TAXII	The transport. An HTTPS protocol with collections and channels. The taxi carries the STIX.
MISP	An open-source platform for <i>sharing</i> intelligence between organisations, with sharing groups and automatic correlation.
OpenCTI	An open-source platform for <i>structuring</i> intelligence as a knowledge graph, modelled on STIX 2.1.
OTX	AlienVault/LevelBlue Open Threat Exchange — community pulses of indicators, free to subscribe.
ISAC	Information Sharing and Analysis Center — a sector-specific trust community.

continued on the next page

continued from the previous page

Term	Meaning
CERT / CSIRT	Computer Emergency Response Team / Computer Security Incident Response Team — national or organisational response bodies.
Sigma	Vendor-neutral detection rules in YAML, compiled into each SIEM's query language. Detection as code.
YARA	Pattern-matching rules for identifying files and memory by content.

Acronyms

Every acronym on CompTIA's published list for CS0-004, plus the ones this guide uses. If you can expand all of them, a surprising number of questions answer themselves.

Acronym	Expansion
A	
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AI	Artificial Intelligence
ALE	Annualized Loss Expectancy
API	Application Programming Interface
APT	Advanced Persistent Threat
ARO	Annual Rate of Occurrence
ASN	Autonomous System Number
ASV	Approved Scanning Vendor
AV	Attack Vector (CVSS) / Antivirus
AWS	Amazon Web Services
B	
BAS	Breach Attack Simulation
BC	Business Continuity
BEC	Business Email Compromise
BIA	Business Impact Analysis
BPF	Berkeley Packet Filter
BYOD	Bring Your Own Device
C	
CASB	Cloud Access Security Broker
CERT	Computer Emergency Response Team
CHD	Cardholder Data
CI/CD	Continuous Integration / Continuous Delivery
CIS	Center for Internet Security
CPE	Common Platform Enumeration
CSIRT	Cybersecurity Incident Response Team
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System

continued on the next page

continued from the previous page

Acronym	Expansion
CWE	Common Weakness Enumeration
D	
DAST	Dynamic Application Security Testing
DKIM	Domain Keys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name Service
DoH	DNS over HTTPS
DoT	DNS over TLS
DR	Disaster Recovery
E	
EDR	Endpoint Detection and Response
EPSS	Exploit Prediction Scoring System
EVTX	Windows Event Log (binary format)
F	
FIM	File Integrity Monitoring
G	
GCP	Google Cloud Platform
GDB	GNU Debugger
GDPR	General Data Protection Regulation
GeoIP	Geolocation by IP
H	
HIPAA	Health Insurance Portability and Accountability Act
HMI	Human–Machine Interface
I	
IaC	Infrastructure as Code
IAM	Identity and Access Management
IAST	Interactive Application Security Testing
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IoA	Indicator of Attack
IoC	Indicator of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization

continued on the next page

continued from the previous page

Acronym	Expansion
J	
JSON	JavaScript Object Notation
K	
KEV	Known Exploited Vulnerabilities (CISA catalogue)
KPI	Key Performance Indicator
L	
LFI	Local File Inclusion
LOLBin	Living Off the Land Binary
M	
MDM	Mobile Device Management
MFA	Multifactor Authentication
MISP	Malware Information Sharing Platform
MOU	Memorandum of Understanding
MSF	Metasploit Framework
MTTD	Mean Time to Detect
MTTR	Mean Time to Respond (or Remediate)
N	
NSE	Nmap Scripting Engine
NTP	Network Time Protocol
O	
OpenCTI	Open Cyber Threat Intelligence
OpenUBA	Open User Behavior Analytics
OpenVAS	Open Vulnerability Assessment Scanner
OSINT	Open-Source Intelligence
OSSTMM	Open Source Security Testing Methodology Manual
OT	Operational Technology
OTX	Open Threat Exchange
OWASP	Open Web Application Security Project
P	
PA	Policy Administrator
PAM	Privileged Access Management
PCAP	Packet Capture
PCI DSS	Payment Card Industry Data Security Standard
PDP	Policy Decision Point
PE	Policy Engine / Portable Executable
PEP	Policy Enforcement Point

continued on the next page

continued from the previous page

Acronym	Expansion
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
R	
RASP	Runtime Application Self-Protection
RCA	Root Cause Analysis
RFI	Remote File Inclusion
RPO	Recovery Point Objective
RTO	Recovery Time Objective
S	
SAMM	Software Assurance Maturity Model
SASE	Secure Access Service Edge
SAST	Static Application Security Testing
SBOM	Software Bill of Materials
SCA	Software Composition Analysis
SCADA	Supervisory Control and Data Acquisition
SDLC	Software Development Life Cycle
SDN	Software-Defined Networking
SIEM	Security Information and Event Management
SLA	Service-level Agreement
SLE	Single Loss Expectancy
SLI	Service-level Indicator
SLO	Service-level Objective
SNI	Server Name Indication
SOAR	Security Orchestration, Automation and Response
SPF	Sender Policy Framework
SPL	Search Processing Language (Splunk)
SSL	Secure Sockets Layer
SSO	Single Sign-on
STIX	Structured Threat Information eXpression
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
SWG	Secure Web Gateway
T	
TAXII	Trusted Automated eXchange of Intelligence Information
TCP	Transmission Control Protocol
TLP	Traffic Light Protocol

continued on the next page

continued from the previous page

Acronym	Expansion
TLS	Transport Layer Security
TTPs	Tactics, Techniques and Procedures
U	
UEBA	User and Entity Behavior Analysis
UTM	Unified Threat Management
V	
VM	Virtual Machine
W	
WORM	Write Once, Read Many
X	
XDR	Extended Detection and Response
XML	Extensible Markup Language
XSS	Cross-Site Scripting
Y	
YAML	Yet Another Markup Language
YARA	Yet Another Recursive Acronym
Z	
ZAP	Zed Attack Proxy
ZTNA	Zero Trust Network Access