Cybersecurity Fundamentals

Palo Alto Networks Certified Cybersecurity Entry-level Technician

KNOWLEDGE CHEATSHEET

INTERRUPT THE ATTACK CHAIN

Discover Reconnaissance → **Prepare** Weaponize & deliver → **Compromise** Exploit & install → **Act** C2 & objectives

01 Cybersecurity fundamentals

Security goals and access control

- **Confidentiality** prevents unauthorized disclosure; **integrity** protects against improper change; **availability** keeps services accessible. Resilience needs backups, redundancy and tested recovery.
- **Authentication** verifies identity; **authorization** determines permitted actions; **accounting** records activity. **MFA** combines distinct factor types, such as a password and a security key.
- **IAM** manages identities, roles and permissions. Apply **least privilege**, role-based access, periodic reviews and prompt removal of obsolete accounts.
- **Directory services** store objects such as users, groups, computers and services. **LDAP** accesses directory information; a directory is not itself a complete access-control policy.

Adversaries, vulnerabilities and exposure

- **Cybercriminals** pursue unlawful gain; **hacktivists** promote causes; **state-affiliated groups** support national objectives; **cyberterrorists** seek intimidation. A **script kiddie** reuses tools with limited expertise.
- An **advanced persistent threat (APT)** is sustained, targeted adversary activity with resources to adapt and maintain access. It is not a particular malware family.
- A **vulnerability** is a weakness; an **exploit** uses it; a **patch** fixes a software defect. A **zero-day** vulnerability lacks an available fix when first exploited or disclosed; an exposure window lasts until effective protection is applied.
- **CVE** identifiers label publicly disclosed vulnerabilities. The CVE Program, operated by **MITRE**, supports common identification; an identifier alone does not indicate severity or whether a system is affected.

Cyberattack lifecycle

- **Reconnaissance** discovers targets; **weaponization** prepares a payload; **delivery** brings it to the victim. Scanning can reveal exposed services, while packet analysis reveals traffic behavior.
- **Exploitation** triggers a weakness; **installation** establishes malicious code or persistence; **command and control (C2)** enables remote direction; **actions on objectives** include theft, disruption or destruction.
- Interrupt the chain at several stages: reduce exposed services, filter malicious delivery, patch weaknesses, prevent execution, detect persistence and block C2. No single control covers every stage.
- **MITRE ATT&CK** organizes observed adversary behavior: **tactics** describe goals, **techniques** describe how goals are achieved, and **procedures** are specific implementations.

Cybersecurity Fundamentals

Palo Alto Networks Certified Cybersecurity Entry-level Technician

KNOWLEDGE CHEATSHEET

INTERRUPT THE ATTACK CHAIN

Discover Reconnaissance → **Prepare** Weaponize & deliver → **Compromise** Exploit & install → **Act** C2 & objectives

Malware and denial of service

- A **virus** attaches to a host file and spreads when it runs; a **worm** propagates between systems without needing a host file. Both can replicate, but their propagation differs.
- A **Trojan** disguises malicious functionality as legitimate software. **Spyware** gathers information; **ransomware** denies access, often through encryption, and may also steal data.
- A **rootkit** conceals privileged access or malicious activity, often by modifying low-level system behavior. Concealment makes detection difficult, not impossible.
- A **botnet** comprises remotely controlled compromised devices. Disrupt C2, isolate infected hosts and remove persistence; blocking one address may be insufficient when infrastructure changes.
- **DoS** exhausts resources or disrupts service; **DDoS** distributes the attack across sources. Motives include extortion and political disruption; rate controls, upstream filtering and resilient capacity reduce impact.

Social engineering and wireless attacks

- **Phishing** uses deceptive messages or sites to solicit actions or secrets. **Spear phishing** targets selected victims; **whaling** targets senior figures. Unwanted bulk mail is **spam**, which may carry phishing content.
- A **watering hole** compromises a site likely to attract the target. **Pharming** redirects users toward a fraudulent site through name-resolution or related manipulation.
- An **evil twin** imitates a legitimate Wi-Fi access point. **Jasager/KARMA-style** attacks answer clients' network probes to lure automatic association; success depends on client behavior and wireless protections.
- A **meddler-in-the-middle** intercepts or alters communications. Validate certificates, use trusted wireless networks and avoid bypassing TLS warnings; a VPN protects traffic only after its tunnel is established.

Endpoint and mobile protection

- **Patching** reduces known software weaknesses. **Exploit prevention** and behavioral controls help interrupt exploitation; endpoint firewalls restrict connections but do not replace application fixes.
- **Signature-based antivirus** recognizes known patterns and can alert, quarantine or remove malicious files. **Behavior-based protection** evaluates actions and context; **anti-spyware** targets covert information collection.

Cybersecurity Fundamentals / Cloud Security

Palo Alto Networks Certified Cybersecurity Entry-level Technician

KNOWLEDGE CHEATSHEET

INTERRUPT THE ATTACK CHAIN

Discover Reconnaissance → **Prepare** Weaponize & deliver → **Compromise** Exploit & install → **Act** C2 & objectives

- **Full-disk encryption** protects data at rest on a lost device when keys remain protected. Backups support recovery; strong authentication and screen locking protect access while the device is in use.
- **Mobile device management (MDM)** enforces settings, distributes updates, inventories devices and can remotely lock or wipe them. Separate work data with managed containers; remote wipe depends on reachability and management state.
- **EDR** collects endpoint telemetry for detection, investigation and response. Isolating a host limits spread while preserving evidence. **APK** denotes an Android application package.

Sensitive information and obligations

- **PII** identifies or can be linked to an individual, such as a name combined with other identifying attributes. Classify personal, payment and proprietary information before defining access and retention rules.
- **DLP** detects and controls sensitive data movement using policy and content inspection. Apply controls to uploads, sharing and downloads, including restrictions for unmanaged devices.
- **PCI DSS** is a payment-card security standard. **GDPR** governs personal-data protection within its scope and restricts certain international transfers. Match handling and reporting requirements to the applicable data and organization.

02 Cloud security

Cloud models and shared responsibility

- The **NIST cloud model** combines **on-demand self-service**, broad network access, resource pooling, rapid elasticity and measured service. **Public cloud** shares provider infrastructure; **private cloud** serves one organization; **hybrid cloud** integrates distinct environments.
- **IaaS** supplies infrastructure while customers manage guest operating systems and applications. **PaaS** also manages the platform; **SaaS** delivers a provider-operated application.
- Customers retain responsibility for their **identities, data, access decisions and permitted use** across cloud models. Provider management of a SaaS platform does not remove customer configuration or governance duties.
- In **IaaS**, customers generally patch guest operating systems. In **PaaS/SaaS**, providers patch the managed operating-system layer. Exact responsibility follows the service boundary and agreement.
- **Multitenancy** shares underlying resources among customers for efficiency. Logical isolation, access controls and configuration guard against cross-tenant exposure; shared infrastructure is not automatically insecure.

Cloud Security

Palo Alto Networks Certified Cybersecurity Entry-level Technician

KNOWLEDGE CHEATSHEET

SECURE EVERY CLOUD LAYER

- **Code** — Secure development
- **Container** — Images & runtime
- **Cluster** — Access & workloads
- **Cloud** — Identity & posture

Virtual machines and hypervisors

- A **Type 1**, or bare-metal, hypervisor runs directly on hardware. A **Type 2** hypervisor runs within a host operating system. Each VM has a guest OS; neither hypervisor type is inherently free of vulnerabilities.
- **Virtualization** consolidates workloads and supports recovery or migration. Protect the management plane, patch hypervisors and guests, and avoid making one host a failure point for all replicas.
- **North-south traffic** crosses a cloud or data-center boundary. **East-west traffic** moves between internal workloads, including communication within or between hosts; both paths require protection.
- Group workloads by **trust level**, enforce inspection between groups and extend virtual enforcement as workloads move. Intra-host traffic can bypass physical perimeter appliances unless the design explicitly steers or inspects it.

Containers, Kubernetes and serverless

- **Containers** package applications and dependencies while sharing the host kernel. VMs virtualize hardware and run separate guest operating systems. Container portability still depends on compatible runtimes and architectures.
- **Docker** builds and runs containers; **Kubernetes** orchestrates containerized workloads across nodes. A **Pod** is Kubernetes' smallest deployable workload unit and can contain closely coupled containers.
- **CaaS** provides managed container capabilities, between infrastructure and a higher-level application platform. **Amazon ECS** and **Azure Kubernetes Service (AKS)** support managed container deployment with different orchestration models.
- **Serverless/FaaS** runs code without customer provisioning of individual servers. **AWS Lambda** is an example. Providers operate infrastructure; developers still secure code, permissions, dependencies and data.
- Containers and serverless can support **automated scaling** and rapid deployment. They do not guarantee infinite capacity, zero cost or automatic security.

DevOps and layered cloud protection

- **DevOps** is a collaborative culture supported by automation, shared ownership and feedback. **Git** provides version control; **Jenkins** automates pipelines. Tools support the culture rather than define it.
- **Continuous integration** frequently merges changes and runs automated builds/tests. **Continuous delivery** keeps releases deployable with a release decision; **continuous deployment** automatically releases passing changes to production.
- **DevSecOps** embeds security throughout design, build, test, deployment and operation. Scan code, secrets, dependencies, images and infrastructure definitions, then monitor runtime behavior.

Cloud Security

Palo Alto Networks Certified Cybersecurity Entry-level Technician

KNOWLEDGE CHEATSHEET

SECURE EVERY CLOUD LAYER

- **Code** — Secure development
- **Container** — Images & runtime
- **Cluster** — Access & workloads
- **Cloud** — Identity & posture

- The cloud-native **four C's** run from **code** to **container**, **cluster** and **cloud**. Weaknesses in an outer infrastructure layer can undermine protection applied to an inner workload.
- A **cloud-native security platform** combines asset inventory, configuration assessment, compliance, vulnerability management and workload protection. **CNAPP** means cloud-native application protection platform. **Prisma Cloud** maps to cloud posture and workload security; one feature does not provide complete cloud coverage.

SaaS governance and exposure

- **Sanctioned** SaaS is approved by IT; **tolerated** SaaS is permitted under restrictions; **unsanctioned** SaaS lacks approval; **prohibited** SaaS is explicitly disallowed. Business value and policy determine the treatment.
- A **CASB** provides SaaS visibility and policy enforcement. **Prisma SaaS** uses API-based integration to examine supported sanctioned-service content and sharing; inline controls inspect supported traffic as users access services.
- SaaS exposure includes public links, excessive permissions and onward sharing. **Promiscuous sharing** spreads access beyond intended recipients; **ghost/stale sharing** preserves access for someone who has left or no longer needs it. **Accidental sharing** grants access to the wrong recipient.
- Apply **least-privilege sharing**, expiration, access reviews, encryption and DLP. Fast SaaS deployment and provider operation do not eliminate user training, finite service limits or customer accountability.
- **Web 2.0** emphasizes interactive, collaborative services and user-generated content. Decentralized **Web3** systems use technologies such as blockchains; a cryptocurrency is not a security control or a cloud service model.

Secure access and cloud enforcement

- **SASE** combines wide-area connectivity with cloud-delivered security for users, branches and applications. **SD-WAN** handles connectivity; security services include **FWaaS**, secure web access, CASB and ZTNA.
- **SD-WAN** uses centrally defined policy and available links to select paths. Direct cloud access can reduce backhaul; centralized management and zero-touch provisioning simplify branch deployment.
- **ZTNA** grants access to specific applications based on identity, device and policy. A traditional **VPN** creates a protected network connection; both still require authentication and authorization.
- **Prisma Access** supplies cloud-delivered access security. **VM-Series** deploys virtual firewalls; **CN-Series** provides containerized enforcement for Kubernetes environments; **PA-Series** provides hardware appliances.
- Use **microsegmentation** to restrict workload-to-workload access. Integrate virtual enforcement with provisioning APIs and automation, then plan availability, scaling, traffic steering and consistent policy across environments.

Network Security

Palo Alto Networks Certified Cybersecurity Entry-level Technician

KNOWLEDGE CHEATSHEET

BUILD POLICY FROM CONTEXT

- **Segment** — Limit paths
- **Identify** — App, user & device
- **Inspect** — Content & threats
- **Enforce** — Least privilege

03 Network security

Network scope, devices and topology

- A **PAN** connects personal devices; a **LAN** connects devices in a local area; a **campus network** joins nearby LANs; a **WAN** connects geographically separated locations.
- A **hub** repeats signals; a **Layer 2 switch** forwards frames using MAC addresses; a **router** forwards IP packets between networks. A router separates broadcast domains; a switch does so through distinct VLANs.
- A **wireless access point** connects wireless clients to a LAN. A **firewall** enforces traffic policy; device function matters more than an unfamiliar diagram symbol.
- **Star** topology uses a central connection point; **bus** uses a shared backbone; **mesh** supplies multiple interconnections. **Leaf-spine** connects each leaf to every spine for predictable data-center paths.

OSI, TCP/IP and encapsulation

- The **OSI model** is: 7 Application, 6 Presentation, 5 Session, 4 Transport, 3 Network, 2 Data Link, 1 Physical. Each layer provides services to the layer above it.
- The four-layer **TCP/IP model** maps Application to OSI 5-7, Transport to 4, Internet to 3, and Network Access to 1-2. Layer numbers depend on which model is being used.
- Encapsulation adds headers as data moves down the stack: **TCP segment** or **UDP datagram**, **IP packet**, **Ethernet frame**, then bits. IP addresses identify network endpoints; MAC addresses serve local-link delivery.
- **TCP** provides connection-oriented, reliable, ordered delivery. **UDP** sends datagrams without built-in retransmission or ordering. **HTTP, DNS, SNMP and NFS** are application-layer protocols.

Addressing, subnetting and translation

- An **IPv4 address** has 32 bits; **CIDR /n** states how many are network bits. For ordinary IPv4 LAN subnets, usable hosts equal **2^(32-n) - 2**, excluding network and broadcast addresses.
- Common sizes: **/25 = 255.255.255.128, 126 hosts**; **/26 = .192, 62**; **/27 = .224, 30**; **/28 = .240, 14**; **/29 = .248, 6**; **/30 = .252, 2**. The shortened masks retain 255.255.255 in the first three octets.
- Subnet boundaries advance by the **block size** in the relevant octet. A /27 advances by 32: an address ending in .36 lies in .32-.63. Use **VLSM** to allocate the largest required subnet first without overlap.
- Private IPv4 ranges are **10.0.0.0/8**, **172.16.0.0/12** and **192.168.0.0/16**. **NAT** translates addresses; **PAT** also translates ports so many internal hosts can share a public address.
- **IPv6** uses 128-bit addresses and has no broadcast. **NAT** conserves public IPv4 space and hides internal addressing, but address translation alone is not a security policy.

Network Security

Palo Alto Networks Certified Cybersecurity Entry-level Technician

KNOWLEDGE CHEATSHEET

BUILD POLICY FROM CONTEXT

- **Segment** — Limit paths
- **Identify** — App, user & device
- **Inspect** — Content & threats
- **Enforce** — Least privilege

Local delivery and route selection

- **ARP** resolves an IPv4 next-hop address to a MAC address on the local link. **DNS** resolves names; **DHCP** supplies addressing configuration. These functions are distinct from NAT.
- A host uses its **subnet mask** to determine local delivery. Traffic for another network normally goes to the **default gateway**; an unusable or missing route prevents delivery.
- A route identifies a **destination prefix**, next hop or exit interface, and selection information. **Longest-prefix match** chooses the most specific matching route; a default route is the least-specific fallback.
- **Static routes** are manually configured and predictable but need maintenance when paths change. **Dynamic routing** learns routes and adapts to topology changes, adding protocol overhead and configuration requirements.
- **RIP** uses hop count; **OSPF** is link-state and builds a topology database within an area; **BGP** exchanges reachability between autonomous systems using path attributes and policy. **IP** carries routed packets; routing protocols exchange route information.

DNS records and common ports

- **A** maps a name to IPv4; **AAAA** maps it to IPv6; **CNAME** aliases one name to another. **PTR** supports reverse lookup; an AAAA record is not a reverse or alias record.
- **MX** identifies mail exchangers; **NS** identifies authoritative name servers; **SOA** holds zone authority metadata; **TXT** carries text used by functions such as domain verification. A **registrar** manages domain registrations through a registry.
- Recognize common defaults: **FTP 20/21**, **SSH 22**, **SMTP 25**, **DNS 53**, **HTTP 80**, **HTTPS 443**, **SNMP 161/162** and **LDAP 389**. DNS uses both UDP and TCP; application identification cannot rely on ports alone.
- **HTTPS** protects HTTP using TLS. Encryption protects communications in transit but can also conceal malicious content from controls that cannot inspect the encrypted session.

Segmentation and Zero Trust

- A **VLAN** creates a logical Layer 2 broadcast domain. A **security zone** groups interfaces or resources for policy; a trust label alone does not enforce safe behavior.
- A **DMZ** hosts externally reachable services behind controlled access. Restrict internet-to-DMZ, DMZ-to-internal and outbound flows separately; a public server should not have unrestricted internal access.

Network Security

Palo Alto Networks Certified Cybersecurity Entry-level Technician

KNOWLEDGE CHEATSHEET

BUILD POLICY FROM CONTEXT

- **Segment** — Limit paths
- **Identify** — App, user & device
- **Inspect** — Content & threats
- **Enforce** — Least privilege

- A **perimeter-based model** often assumes internal systems are trusted. Compromised endpoints, cloud services and remote users undermine that assumption; protect internal east-west paths as well as boundary crossings.
- **Zero Trust** removes implicit trust based on location. Verify identity and device context, grant least privilege, inspect permitted traffic and continually reassess access.
- **Segmentation** limits lateral movement. Combine application, user and content awareness with threat intelligence and enforcement at appropriate boundaries; encryption and authentication alone do not establish least privilege.

Firewalls, applications and threat inspection

- **Stateless packet filters** evaluate packet headers such as addresses, protocols and ports. **Stateful firewalls** also track connection state, typically using network and transport information.
- A **proxy firewall** mediates application connections. A **next-generation firewall (NGFW)** adds application-layer identification and threat inspection to traffic control, with identity and content context.
- **App-ID** identifies applications beyond port numbers; **User-ID** maps traffic to users; **Content-ID** inspects content and threats. **Device-ID** adds device context for policy.
- Applications can use **nonstandard ports**, **port hopping**, TLS or **tunneling** inside allowed services. Allowing a port does not prove the application, user or payload is safe.
- **URL Filtering** controls web destinations and categories; **DNS Security** addresses malicious DNS activity; **Threat Prevention** inspects for supported exploits and malware; **WildFire** analyzes suspicious files and shares verdicts for prevention.
- Serial security appliances can add latency and fragmented policy. Integrated inspection reduces handoffs, but deployment still needs capacity planning, high availability, decryption policy and visibility into every required traffic path.

IDS, IPS and detection outcomes

- An **IDS** detects and alerts; an inline **IPS** can block matching activity. **Signature/knowledge-based** detection matches known patterns; **behavior/anomaly-based** detection compares activity with expected behavior.
- **True positive** means malicious activity correctly detected; **false positive** means benign activity incorrectly flagged. **True negative** means benign activity correctly accepted; **false negative** means an attack was missed.
- Tune baselines and rules to reduce noise without masking attacks. Continuous monitoring and flow inspection help detect reconnaissance; filtering and limiting exposed services reduce what a scan can reach.

Network Security / Security Operations

Palo Alto Networks Certified Cybersecurity Entry-level Technician

KNOWLEDGE CHEATSHEET

TURN TELEMETRY INTO RESPONSE

- **Collect** — Logs & telemetry
- → **Correlate** — SIEM & XDR
- → **Investigate** — Evidence & context
- → **Respond** — SOAR & people

VPNs, tunneling and connected devices

- **IPsec** commonly protects site-to-site IP traffic. **IKE** negotiates keys and security associations; **ESP** can provide confidentiality and integrity; **AH** provides authentication/integrity without encryption.
- **TLS VPNs** protect supported remote-access connections; **GlobalProtect** supports protected remote access to Palo Alto Networks enforcement points. **Split tunneling** sends selected traffic through the VPN and other traffic directly to its destination, changing inspection coverage.
- **GRE** encapsulates traffic without native encryption; **L2TP** tunnels Layer 2 traffic and commonly pairs with IPsec. **PPTP** uses obsolete security mechanisms and is unsuitable for modern protection.
- IoT connectivity includes **Wi-Fi**, **Bluetooth/BLE**, **ANT+** for low-power sensors and wearables, cellular networks and **satellite L-band** links. Choose controls for the device's range, bandwidth and power constraints.
- **IoT/IoMT** risks include weak credentials, poor inventory, legacy protocols and outdated software. **IoT Security** supports device discovery and risk visibility. Restrict device communication, monitor behavior and isolate sensitive equipment; not every device has the same weaknesses.

04 Security operations

SOC mission and operating process

- A **SOC** monitors, investigates and coordinates response to security events. **SecOps** joins security and operations through people, processes and technology aligned with business priorities.
- Define **objectives**, responsibilities, escalation paths, coverage and success measures. Visibility provides telemetry; interfaces connect external teams and tools; business context determines what matters most.
- **Identify** assets, threats and suspicious activity; **investigate** scope and cause; **mitigate** impact; document decisions and report outcomes. Content engineering builds and tunes detections, while initial research informs triage.
- Use response stages such as preparation, detection/analysis, containment, eradication, recovery and lessons learned. Record the incident, monitor progress and follow applicable notification procedures.

SIEM and security telemetry

- **SIEM** means Security Information and Event Management. It centralizes and correlates logs for monitoring, investigation, reporting and compliance; collection does not itself contain an incident.
- **Connectors, APIs, agents and syslog** bring source events into the platform. Parsing and normalization translate formats into usable fields; check timestamps, time zones, ingestion health and retention.

Security Operations

Palo Alto Networks Certified Cybersecurity Entry-level Technician

KNOWLEDGE CHEATSHEET

TURN TELEMETRY INTO RESPONSE

Collect Logs & telemetry → **Correlate** SIEM & XDR → **Investigate** Evidence & context → **Respond** SOAR & people

- Forward relevant **endpoint, authentication, network and cloud logs** centrally. Select sources and access controls around detection needs and governance, risk and compliance requirements.
- A **security data lake** stores telemetry for analysis. **Cortex Data Lake** denotes Palo Alto Networks' cloud log-repository capability; **UEBA** analyzes user/entity behavior to identify unusual activity.

SOAR, playbooks and case management

- **SOAR** means Security Orchestration, Automation and Response. **Orchestration** coordinates tools; **automation** executes repeatable tasks; **response** applies actions according to policy.
- **Playbooks** encode investigation and response workflows, including enrichment, decision points, approvals and escalation. Vet actions, handle failures and audit execution to make machine-driven responses consistent.
- **Integrations** connect products and external services. **Case management** consolidates incident evidence, ownership, tasks, communications and status, enabling teams to coordinate from a shared record.
- **Cortex XSOAR** provides orchestration, playbooks and case workflows. **Threat Intelligence Management (TIM)** ingests, normalizes, enriches and manages indicators so analysts can prioritize relevant information.

XDR and integrated security platforms

- **XDR** correlates endpoint, network and cloud telemetry for prevention, detection, investigation and response. **Cortex XDR** adds endpoint protection and cross-source investigation; it does not replace every other security control.
- **Cortex XSIAM** applies integrated analytics, AI and automation to security operations. Automated correlation and response can reduce analyst workload, while human review remains important for consequential decisions.
- An integrated **Security Operating Platform** combines visibility, known/unknown threat prevention and automated sharing of intelligence. Enable required applications by identity and device context, then block unnecessary access.
- **AutoFocus** associates threat intelligence with investigation context; **PAN-DB** supplies URL categorization; **MineMeld** aggregates and processes threat indicators. Understand these functions separately from endpoint prevention or orchestration.

Security Operations

Palo Alto Networks Certified Cybersecurity Entry-level Technician

KNOWLEDGE CHEATSHEET

TURN TELEMETRY INTO RESPONSE

Collect Logs & telemetry → **Correlate** SIEM & XDR → **Investigate** Evidence & context → **Respond** SOAR & people

Malware analysis and threat intelligence

- **Static analysis** examines files without executing them. **Dynamic analysis** executes a sample in a controlled sandbox to observe behavior. **Bare-metal analysis** can help reveal behavior that evades virtual environments.
- **WildFire** uses multiple analysis methods to assess suspicious submissions. Recognize verdicts such as **benign**, **malware**, **grayware** and **phishing**; suspicious or unwanted behavior is not always equivalent to a confirmed malicious executable.
- Endpoint execution controls can evaluate **policy**, local analysis and available reputation before permitting a file. Unknown submissions may undergo deeper cloud analysis; do not assume every file follows an identical analysis sequence.
- **IoCs** include suspicious hashes, domains, IPs and other observables. **STIX** structures threat intelligence; **TAXII** exchanges it. Enrichment adds context, while deduplication and expiration keep indicator collections useful.

Investigation tools and evidence

- For a suspicious successful **login**, correlate activity before and after it: source, device, time, authentication changes and subsequent access. One event rarely establishes the complete incident scope.
- **Wireshark** analyzes packet captures and can record traffic; **Nessus** scans for vulnerabilities. **Windows Event Viewer** inspects event logs. Use each tool for the evidence type it understands.
- Decode an **encoded string** safely to inspect its content; encoding such as Base64 is not encryption. Preserve the original and do not execute decoded commands or suspicious samples on a production system.
- **Digital forensics** collects, preserves and analyzes evidence. Maintain timestamps, provenance, integrity and chain of custody; preserve originals and use controlled copies for examination.
- Record hypotheses, supporting evidence, containment actions and outcomes in the **incident case**. Treat AI-generated analysis and automated verdicts as inputs that require context and validation.