Threats & Protection

Palo Alto Networks Certified Detection and Remediation Analyst

KNOWLEDGE CHEATSHEET

LAYERED ENDPOINT DEFENSE

- **File** — Verdict & analysis
- **Exploit** — Technique prevention
- **Behavior** — Activity patterns
- **Response** — Contain & repair

01 Threats and endpoint protection

Attack lifecycle and attacker goals

- **Attack lifecycle:** reconnaissance, weaponization and delivery, exploitation, installation, command and control, then actions on objectives. Interrupting a required stage can disrupt the attack; verify that other footholds are contained.
- **MITRE ATT&CK tactics** describe attacker objectives; techniques describe how they are achieved. Phishing commonly provides **Initial Access**; phishing for information supports **Reconnaissance**. Command and Control, Lateral Movement and Exfiltration are distinct objectives.
- **Supply-chain compromise** abuses trusted software, updates or vendors to reach downstream victims. A trusted signature or delivery channel does not prove that observed behavior is safe.
- **Ransomware** can combine file encryption, data theft, service disruption and extortion. Malicious email attachments are one entry vector; encrypting hypervisors or VM storage can affect many workloads. Payment does not guarantee recovery.

Malware verdicts and analysis layers

- **WildFire** analyzes submitted file samples and returns verdicts and reports. **Local Analysis** evaluates files on the endpoint, including when cloud connectivity or a known verdict is unavailable.
- **Hash reputation** identifies a particular file; **behavioral detection** evaluates activity. A benign file verdict does not establish that every command line, child process or use of that file is benign.
- **Malware profiles** configure endpoint malware controls. Restrictions, file examination, exploit prevention and behavioral protection address different conditions; identify the module responsible for a block before tuning it.

Behavioral and ransomware protection

- **Behavioral Threat Protection (BTP)** evaluates endpoint activity against behavioral rules. It can recognize a malicious sequence even when a file hash is unfamiliar; keep protection content and effective policy current.
- **Respond to Malicious Causality Chains** supports terminating processes involved in malicious activity. Review the causality context and configured action mode rather than treating an alert as proof that every related action was prevented.
- **Ransomware protection** uses decoy files to expose suspicious encryption behavior. Behavioral prevention complements file analysis; maintain recoverable backups and investigate activity around a prevention event.

Threats & Protection / Platform & Agents

Palo Alto Networks Certified Detection and Remediation Analyst

KNOWLEDGE CHEATSHEET

FROM SENSOR TO INVESTIGATION

Sensors Agents & logs → **Transport** Proxy & collectors → **Data** Queryable telemetry → **Operations** Health & coverage

Exploits, memory and library loading

- **Exploitation** uses a vulnerability to gain an unintended capability. Application exploits target application flaws; kernel exploits target privileged operating-system code. Discovering a vulnerable service alone is not successful exploitation.
- **Exploit Protection Modules (EPMs)** interrupt exploitation techniques. **UASLR** increases memory-location randomization; heap-spray and JIT protections target different memory-abuse patterns.
- **DLL Security** protects against unsafe Windows library loading; **Dylib Hijacking protection** addresses unsafe dynamic-library loading on macOS. Match the protection to the platform and attack mechanism.

02 Platform, ingestion and administration

Licensing and telemetry

- **Cortex XDR agents** are endpoint sensors and enforcement components. **Prevent** focuses on endpoint prevention; **Pro per Endpoint** adds endpoint investigation and response capabilities.
- **Pro per TB** is the ingestion-based licensing term associated with external data in this product family. Separate endpoint entitlement, external-log ingestion and feature add-ons when planning a deployment.
- **Enhanced endpoint data** supplies process, file, network and registry context for investigation. Confirm collection settings, endpoint health and actual event availability before interpreting an empty search.

Broker VM roles

- **Broker VM** hosts applets that connect local sources and agents to Cortex services. A **Syslog Collector** receives supported third-party device logs; a **NetFlow Collector** receives network flow records.
- **Agent Proxy** routes agent communication through a controlled access point when endpoints lack direct internet access. The proxy still needs upstream connectivity; it does not create a fully disconnected cloud deployment.

Platform & Agents / Investigation

Palo Alto Networks Certified Detection and Remediation Analyst

KNOWLEDGE CHEATSHEET

FROM SENSOR TO INVESTIGATION

Sensors Agents & logs → **Transport** Proxy & collectors → **Data** Queryable telemetry → **Operations** Health & coverage

- **Agent Installer and Content Caching** distributes cached installation packages and content locally. Configure a trusted TLS certificate, name resolution and endpoint trust for the secure service.
- **Collector selection** follows the source format: CSV for tabular files, database collection for supported database inputs, and Syslog for device messages. Validate parsing, timestamps and resulting datasets as well as transport connectivity.

Agent deployment and health

- **Agent upgrades** change installed software; **content updates** deliver detection and protection intelligence. Monitor both, stage rollout and investigate pending or failed updates instead of assuming all agents share the same protection.
- **Kubernetes DaemonSet** deployment places an agent workload on eligible nodes. Validate the supported agent, node OS and kernel, privileges and entitlement before deployment; cluster support differs from ordinary desktop installation.
- **Host Insights** provides host inventory and vulnerability visibility when licensed and enabled. Inventory, vulnerability findings, disk-encryption state and device-control violations answer different operational questions.

Research, hunting and support

- **Unit 42** provides threat research, malware analysis and incident-response expertise. **Managed Threat Hunting** proactively investigates tenant telemetry and reports findings; it is distinct from software deployment or content publishing.
- **TAC escalation** needs the affected agent identity, relevant alerts and an agent technical-support file. Include reproduction context and a prevention archive when available; support logs and forensic evidence serve different purposes.

03 Incident triage and investigation

Alerts, incidents and ownership

- **Alert** means a detected condition. **Incident** groups related alerts into an investigation. **Causality analysis** correlates relevant activity and artifacts; a shared host or timestamp alone does not establish a single attack.
- **Triage** reviews severity, affected assets, detection source, action taken and business impact. Check ownership and assign an analyst; bulk actions can update assignments and statuses for selected incidents.
- **Incident starring** highlights investigations for priority review. Manual starring and configured starring rules support consistent prioritization; use starred filters in incident widgets to focus the view.

Investigation

Palo Alto Networks Certified Detection and Remediation Analyst

KNOWLEDGE CHEATSHEET

BUILD INCIDENT CONTEXT

Triage Impact & action → **Causality** Relationships → **Timeline** Event sequence → **Decision** Classify & respond

Causality, Timeline and artifacts

- **Causality view** explains relationships among processes and associated events. Follow parent and child processes, command lines, files, registry changes and network connections to establish how activity began and spread.
- **Timeline** orders events chronologically. Pivot from a result or alert into its card, causality view or timeline to combine relationship context with event sequence.
- **Key Artifacts** surface investigation-relevant files, hosts, users and addresses. Open an artifact for context and review the **WildFire report** for a submitted file when available.
- For a **prevented malicious document**, examine the document, originating process, attempted child execution, dropped files and connections. Confirm the prevention action and search for earlier or parallel activity before declaring the host clean.

Classification and safe tuning

- **True positive:** malicious activity correctly detected. **False positive:** benign activity flagged. **False negative:** malicious activity missed. **True negative:** benign activity correctly accepted. Resolve verdict disagreements with context and evidence.
- **Alert exclusions** suppress matching alerts in the console and their contribution to incidents. They do not change endpoint prevention behavior. Excluding an alert is different from permitting the blocked activity.
- **Endpoint policy exceptions** change selected protection behavior. Use a narrow endpoint scope where possible; a **global exception** extends the change broadly. Match the exception to the actual protection module.
- **Hash exceptions** identify a specific file; **signer exceptions** trust a broader identity. A path or filename may match changing content. Document the business reason and review the scope before allowing software.

Dashboards and operational metrics

- **MTTR** measures mean time to resolution. Define the start, end and incident population consistently; use security-administration and incident-management dashboards to assess workload and response performance.
- **Widget Library** stores reusable widgets, including custom **XQL widgets**. Save a descriptive name and query, then apply dashboard filters and verify the data period before interpreting the result.
- **Scheduled reports** distribute recurring views; configured outbound integrations such as Slack support operational sharing. Distinguish a report schedule from an alert notification and verify the destination and filters.

XQL & Detection

Palo Alto Networks Certified Detection and Remediation Analyst

KNOWLEDGE CHEATSHEET

TURN A LEAD INTO DETECTION

Hypothesis Behavior or IOC → **Query** Scope & schema → **Test** Review matches → **Rule** Monitor & refine

04 XQL, hunting and detection rules

Datasets, presets and query stages

- **Dataset** is a queryable collection with a logical schema of fields and types. **xdr_data** holds core XDR event data. Built-in and ingested third-party datasets can expose different schemas.
- **Preset** provides a predefined view of selected fields and events for a common use case. Use the schema browser to find the actual field names; presets and datasets are query sources, not interchangeable field values.
- **XQL pipelines** pass results through stages separated by a pipe. **filter** selects rows, **fields** selects columns, **alter** derives values, and **comp** aggregates. Time range and source selection determine which data can match.
- **Event type** selects an activity class, such as PROCESS; **event subtype** narrows it, such as PROCESS_START. Distinguish the initiating process from the target or action process when reading field names.

IOC versus BIOC

- **IOC rules** match known observables such as hashes, IP addresses, domains or file paths where supported. An indicator match needs investigation; adding an IOC for detection is not the same as blocking execution.
- **BIOC rules** describe behavioral patterns, including process, file, registry and network activity. Turn a useful hunting lead into a repeatable behavior rule after reviewing its normal and malicious matches.
- **XQL-based BIOCs** must filter on **event_type**. A process-start rule should also specify **event_sub_type = PROCESS_START** and then its behavioral conditions. A valid ad hoc query is not automatically a valid BIOC query.
- **Test BIOC** against historical telemetry before enabling it. Refine overly broad conditions and use supported rule stages; aggregation and presentation stages useful in dashboards may be unsuitable for a BIOC.

From hunting lead to detection

- **Threat hunting** starts with a hypothesis, queries relevant data and pivots across related entities. Broaden from a known file or host to behavior, affected users and other endpoints.
- **Analytics** detects suspicious patterns across available telemetry, including command-and-control, lateral-movement and exfiltration behavior. Detection supplies evidence for response; verify the actual enforcement action separately.
- **Query results** show only collected data within the selected scope. For network evidence, retain source and destination IPs, ports, protocol, time and initiating process; an address without direction or context is ambiguous.

Response

Palo Alto Networks Certified Detection and Remediation Analyst

KNOWLEDGE CHEATSHEET

RESPONSE LIFECYCLE

Contain Isolate & stop → **Investigate** Terminal & scripts → **Remediate** Remove & repair → **Validate** Monitor & close

05 Response and remediation

Containment and file handling

- **Endpoint isolation** restricts network communication while preserving required management connectivity and configured exceptions. It contains spread; it does not remove malware or repair persistence.
- **Quarantine** moves a file into protected storage and prevents its execution. **Process termination** stops running activity. **Deletion** removes an artifact; select the action that addresses the threat state.
- **File Search and Destroy** locates matching files across selected endpoints and supports subsequent removal. Use a validated file identifier and inspect matches before destruction; finding a file and eradicating its persistence are separate tasks.
- **Action Center** tracks response requests and results. Check completed, failed and pending actions on each endpoint, then confirm containment and remediation through fresh telemetry.

Live Terminal and response scripts

- **Live Terminal** provides interactive remote investigation and response on supported endpoints. **Secure WebSocket (wss)** supports its bidirectional communication; a connected console still needs a reachable, eligible agent.
- **Live Terminal tasks** include managing files and processes and running supported OS commands or Python commands and scripts. The supported Python environment and XDR libraries differ from an unrestricted local development environment.
- **Agent scripts** automate repeatable collection or response. Review script purpose, platform, inputs, permissions and output; use the supplied script library for the supported names and operations.
- **Access controls** govern remote response. Restrict Live Terminal permission and configure the agent setting where required; desktop capabilities should not be assumed available on Android or every OS.

Response

Palo Alto Networks Certified Detection and Remediation Analyst

KNOWLEDGE CHEATSHEET

RESPONSE LIFECYCLE

Contain Isolate & stop → **Investigate** Terminal & scripts → **Remediate** Remove & repair → **Validate** Monitor & close

Repair, verify and close

- **Remediation Suggestions** derive candidate cleanup actions from a malicious causality chain. Review affected files and configuration changes before execution; supported actions depend on endpoint capabilities.
- **Windows Registry** is a hierarchical settings database for the OS and applications. Malicious changes can establish persistence; removing the executable alone may leave registry or scheduled-task persistence behind.
- **Recovery validation** checks for remaining processes, persistence, files and network activity. Restore required services, monitor for recurrence, record response results and close the incident with a supported resolution reason.