Architecture & Deployment

Fortinet NSE 5 - FortiEDR 5.0

KNOWLEDGE CHEATSHEET

COMPONENT RESPONSIBILITIES

- **Collector** — Observe & enforce
- **Core** — Analyze activity
- **Aggregator** — Relay telemetry
- **Manager** — Configure & investigate

01 Architecture and deployment

Know the component roles

- **Collector** is the endpoint agent: it observes activity, enforces protection and reports telemetry. FortiEDR combines central management with endpoint protection across supported operating systems.
- **Core** analyzes endpoint activity and supplies real-time protection decisions. **Aggregator** carries Collector registration, status and event communications toward the management environment.
- **Central Manager** provides the web console for inventory, policies, events and administration. **FCS** enriches events and confirms or revises classifications after deeper analysis.
- **Threat Hunting Repository** stores collected activity for searches. Keep the repository, the management console and the endpoint enforcement role distinct.

Collector registration and connectivity

- **Registration password** authorizes component enrollment; it is separate from a console user password. Check the organization name and registration credentials when onboarding a Collector.
- Know the default destinations: **Core TCP 555**, **Aggregator TCP 8081**, and **Central Manager HTTPS 443**. A custom listener requires the matching configured port.
- For a missing Collector, first check the local **FortiEDR services**, then routing, DNS, firewall and proxy access to its Core and Aggregator. Check registration errors and the console organization and inventory filters.
- Use local status output, connection tests and logs together. A listening port, an established connection and a failed authentication describe different faults; changing ports does not fix an incorrect password.

Accounts and organization scope

- **Admin** manages all organizations. **Local Admin** administers its own organization. **User** can investigate events and change operational settings but cannot access the **ADMINISTRATION** tab.
- **LDAP** and **SAML** support remote console authentication. Authentication proves identity; the assigned role and organization determine authorization.
- For **REST API** access, check the account permission, API availability and credentials. Complete any required initial password change before using a new account for API authentication.
- In **multi-tenancy**, inspect the selected organization before changing policy. Apply Communication Control policies to the intended Collector Groups in each organization; a similarly named policy elsewhere does not protect this group.
- **Global exceptions** require the appropriate all-organization administrative scope. Local administration remains organization-bound; verify the organizations actually included in an exception.

Protection & Control

Fortinet NSE 5 - FortiEDR 5.0

KNOWLEDGE CHEATSHEET

PROTECTION LAYERS

- **NGAV** — Before execution
- **Exfiltration** — Outbound activity
- **Ransomware** — Data modification
- **Communication** — Application access

02 Protection and communication control

Pre-infection and post-infection protection

- **Execution Prevention / NGAV** uses file analysis and machine learning to stop malicious files before execution. Reading or executing a malicious file can trigger NGAV inspection; a scan event does not prove the program ran.
- **Post-infection protection** limits damage after compromise. **Exfiltration Prevention** blocks malicious outbound activity; **Ransomware Prevention** blocks malicious attempts to encrypt or alter data.
- **Device Control** governs supported peripheral-device use. Inspect whether its rules are enabled and which action is configured before assuming a device is restricted.
- FortiEDR combines **real-time prevention**, investigation and automated response. Blocking harmful activity can preserve business operation while responders investigate the compromised endpoint.

Rules, modes and effective actions

- **Protection mode** enforces configured blocking rules. **Simulation mode** records what would have been blocked while allowing the operation; a simulated block is not an enforced block.
- Check the **effective policy**, rule action and Collector Group assignment together. A policy name alone does not reveal whether enforcement is active.
- An **Execution Prevention** block stops execution at that point. A later network or file-operation block can occur after the process has already launched; identify the blocked operation before describing the outcome.

Application communications and risk

- **Communication Control** allows or denies application network communication. A communication denial does not by itself prohibit application execution.
- Collectors report applications observed making communication attempts. An installed application absent from this inventory may simply have made no observed connection attempt; absence does not establish safety.

Protection & Control / Events & Forensics

Fortinet NSE 5 - FortiEDR 5.0

KNOWLEDGE CHEATSHEET

INVESTIGATION SEQUENCE

Event Read context → **Forensics** Follow activity → **Assessment** Verify safety → **Exception** Scope & retest

- **Proactive risk mitigation** can restrict communication using application reputation and vulnerability information. **CVE** identifies a vulnerability; reputation and vulnerability severity answer different risk questions.
- To deny an application for a team, change its decision in the **Communication Control policy assigned to that team's Collector Group**. Confirm policy mode and effective assignment on the affected endpoint.

03 Events, forensics and exceptions

Read each event on separate axes

- **Classification** describes threat assessment: Malicious, Suspicious, Inconclusive, Likely Safe, Safe or **PUP** (potentially unwanted program). It is separate from the action actually enforced.
- **Action** shows block, log or simulated block. **Handled** records analyst workflow status; marking an event handled does not delete the file or prove remediation.
- Correlate the **device**, process, file path and hash, destination, timestamp, triggered policy and rule. Do not infer execution, isolation or cleanup from the event title alone.
- When a third-party application is affected, **investigate its safety first**. Check the precise operation and behavior, reproduce carefully, and gather evidence before creating an exception.

Follow the activity and its context

- **Flow Analyzer** presents the event as a graphical activity flow. Follow related processes and their operations to understand how the suspicious action arose.
- **Process relationships**, command lines, users, file operations and network destinations add context. A legitimate signed process can still be abused; an unsigned file alone is not proof of malicious behavior.
- **Stacks view** provides call-stack context around the triggering operation. A stack is a sequence of execution frames, not a process tree or a complete endpoint memory image.
- For a **system crash or hang**, a full memory dump can preserve kernel and process state for support analysis. Routine connectivity faults usually start with service status, network checks and logs.

Events & Forensics / Threat Hunting

Fortinet NSE 5 - FortiEDR 5.0

KNOWLEDGE CHEATSHEET

HUNT AND VALIDATE

Collect Profile & retention → **Search** Scope & indicators → **Investigate** Correlate activity → **Remediate** Confirm outcome

Keep exceptions narrow and deliberate

- An **exception** changes handling for matching rule conditions. Inspect the process or file identity, triggered rules, devices, groups and organization scope before approving it.
- A **partial exception** covers selected rule violations; other matching rules can still trigger. Allowing one stage can expose a later action to a different protection policy.
- Limit an exception to the verified business need and retest the application. **Exception**, **handled event**, **isolated device** and **remediated file** are separate states.

04 Threat hunting and remediation

Collection depth and search coverage

- **Threat Hunting** searches endpoint evidence for indicators and behavior across an organization. The **Repository** supports telemetry searches; collection settings determine which activity is available.
- **Inventory**, **Standard Collection** and **Comprehensive** profiles represent different collection depths. Comprehensive collects the broadest activity and has the greatest resource and storage impact.
- Choose collection scope against **endpoint overhead**, event volume and retention. No result can mean no match, excluded activity, missing telemetry or data outside the retained interval.
- Use a **file hash** to identify identical content even if it has been renamed. A changed binary normally has a different hash; a file name alone is neither unique identity nor proof of maliciousness.

Interpret queries and activity details

- Check **time range**, organization, Collector or group, event category and query conditions. Understand **AND / OR** grouping before interpreting a match.
- **Process**, **file** and **network** activity describe different observations. Read the action, initiating process, user, command line and destination rather than inferring behavior from a file name.
- **MITRE ATT&CK** mappings organize observed behavior by tactics and techniques. A mapping adds investigation context; it is not itself an enforcement result.
- A **hunt query** retrieves evidence. Alert generation or blocking requires the corresponding detection or response configuration; a search containing RDP does not inherently block RDP.

Threat Hunting / Response & Integrations

Fortinet NSE 5 - FortiEDR 5.0

KNOWLEDGE CHEATSHEET

RESPONSE SEQUENCE

Core Initial assessment → **FCS** Final classification → **Playbook** Selected actions → **Endpoint** Verify result

Find, contain and remove

- Use a known-malicious **hash or file indicator** to locate matching instances on managed endpoints. Confirm the intended matches and endpoint scope before initiating remediation.
- **Remediation** can remove the identified file from affected Collectors. Distinguish file removal or quarantine from stopping a running process and from isolating the entire device.
- Check the **action result** on each affected endpoint and revisit unreachable endpoints. A submitted remediation request is not proof that every copy has been removed.

05 Playbooks, isolation and integrations

Classification drives response

- **Core classification** is the initial assessment. **FCS** can confirm or revise it after enrichment; use classification history to follow the chronology.
- **Playbook policies** associate event classifications with response actions. If FCS revises Inconclusive to Malicious, evaluate the configured actions for the final **Malicious** classification.
- Keep **detection**, classification and response separate: the triggering rule identifies the behavior, the classification assesses it, and the playbook determines which configured actions follow.
- **FortiXDR** extends detection, investigation and response across the Security Fabric. FCS analytics correlate evidence, and **playbooks** coordinate automated response through configured integrations.

Response & Integrations

Fortinet NSE 5 - FortiEDR 5.0

KNOWLEDGE CHEATSHEET

RESPONSE SEQUENCE

Core — Initial assessment → **FCS** — Final classification → **Playbook** — Selected actions → **Endpoint** — Verify result

Automate with the right connector

- Playbooks can **notify**, isolate an endpoint, move it to a **High Security Collector Group**, terminate a process, delete a file or clean supported persistence. Check enabled actions and their classification columns.
- **FortiGate** firewall integration can block malicious destinations; **FortiNAC** integration can isolate through network access control. **FortiSandbox** supplies analysis, while SIEM integrations support central event handling.
- **Action Manager** manages **Python** scripts that call external APIs. Uploading an action makes it available; select it in the applicable playbook to make it run.
- **Security Fabric integrations** require FCS connectivity, a suitable authorized API account and working connectors. A **Core with JumpBox functionality** provides access to integrations such as FortiAnalyzer; Core-only functionality does not supply that bridge.

Understand the boundary of isolation

- **Collector isolation** restricts endpoint network communication for containment. It is separate from deleting malware and from a Communication Control denial for one application.
- For this FortiEDR behavior, **incoming RDP** and **ICMP** are exempt from isolation and Communication Control denial. Restrictions apply to new session attempts; previously established sessions can remain active.
- **NAC isolation** is enforced by the external NAC system. Track containment and release in the system that performed it, then verify endpoint state before restoring normal access.