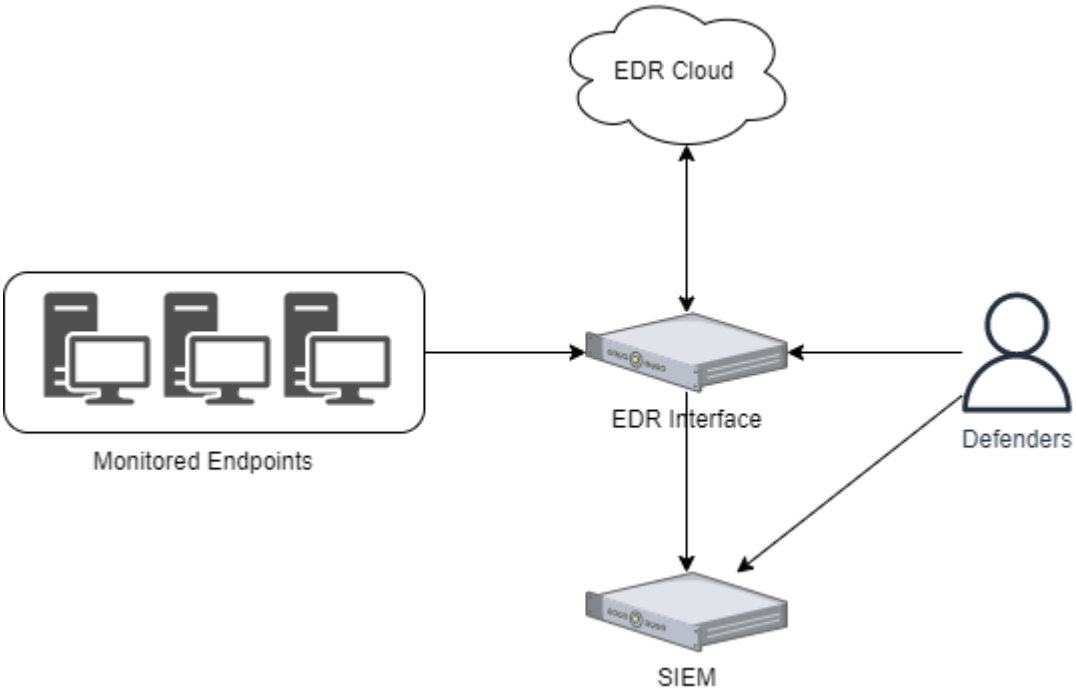
Chapter 7 - Endpoint Detection and Response Evasion

Endpoint Detection and Response

Endpoint Detection and Response (EDR) is the name given to an integrated security solution which combines real-time monitoring of endpoints (and possibly other log telemetry) with analysis and response capabilities. Think of an EDR like AV on steroids. An EDR will primarily:

- Collect event data from managed endpoints.
- Analyse the data to identify known threat patterns.
- Where applicable, automatically respond to threats (such as blocking/containing) and raise alerts.
- Aid manual investigations by providing forensic and analysis capabilities.

Each vendor may architect their solution differently, but the following is a generic high-level view of what an EDR might look like.



The protected endpoints will typically have the EDR's "agent" installed on them. This is responsible for collecting and shipping log data to a central repository, responding to detected threats, and provides those forensic capabilities. For instance, a defender may request a file sample from an endpoint, which is collected and returned by the agent.

EDR solutions may also talk back to the vendor's cloud infrastructure, which is useful for deploying software and signature updates. Some vendors also offer "threat hunting" as a service, where they will hunt for "unknown" malicious activity (activity that is malicious but not detected by the automated analysis) on the customers behalf.

Defenders may interact directly with the EDR's main interface, which is where the policies and alerts are controlled - essentially a single pain of glass to view and manage the overall solution. Alerts generated by the EDR may also be forwarded to a SIEM.