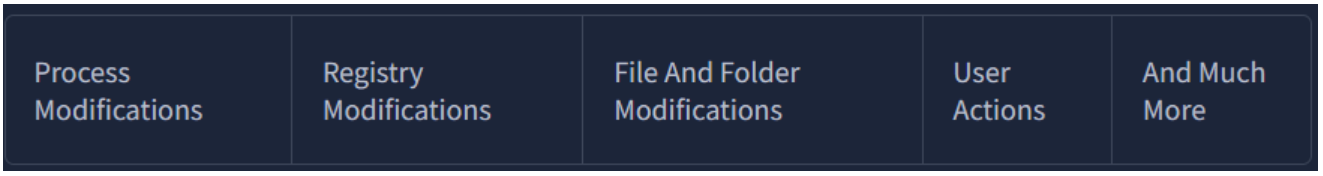
EDR - Endpoint Detection and Response

Endpoint Detection and Response (EDR) is a security solution designed to monitor, detect, and respond to advanced threats at the endpoint level.

Visibility

- The level of visibility EDR provides is impressive. It collects detailed data from the endpoints, which includes process modifications, registry modifications, file and folder modifications, user actions, and much more.
- It then presents this information in a very structured format to the analyst. The analyst can see the whole process tree with a complete activity timeline of the sequence of actions.



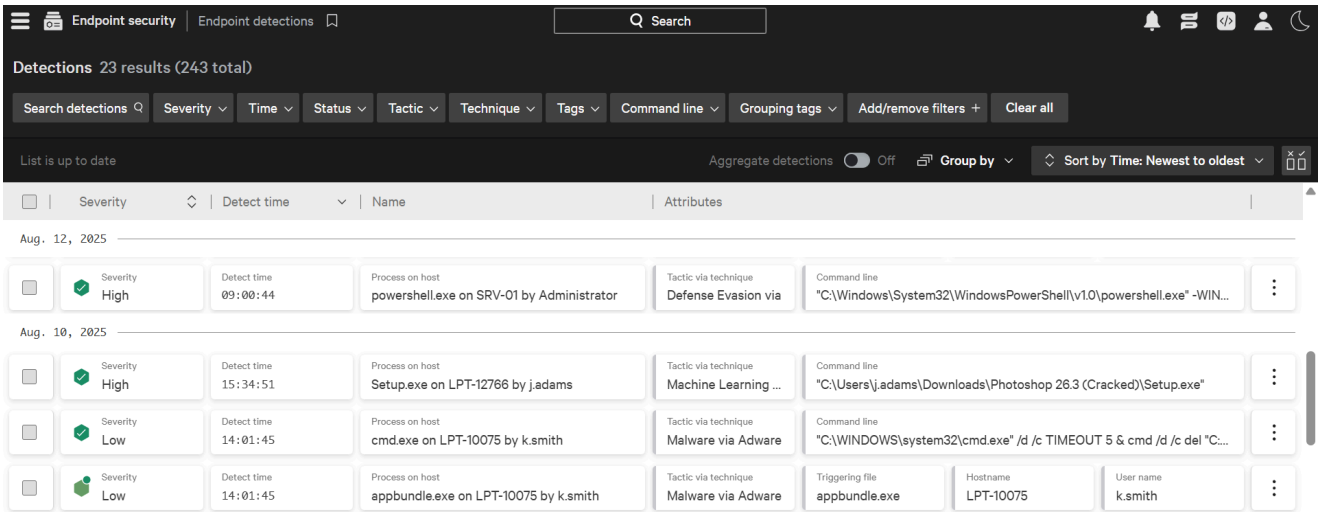
Detection

The detection feature of EDR wins over traditional detection capabilities. It incorporates signature-based detections as well as behavior-based detections, such as unexpected user activities.

- With modern machine learning capabilities, it identifies any deviation from the baseline behavior and instantly flags it. It can also detect fileless malware that resides in memory. It also allows us to feed custom IOCs for threat detections.

The following screenshot shows a dashboard of all the detections happening on the different endpoints. Each detection is represented by a row with different fields including the severity of the detection, time, triggering file, hostname, username, and more.

The Tactic via Technique field maps the detection with MITRE. Any detection when clicked will show us rich details which helps a SOC analyst during the analysis.



Response

EDR also empowers analysts to take action on detected threats. These actions can be taken at any endpoint within the central EDR console.

Imagine getting a detection on the EDR with full-fledged details on when, where, and what happened, and you have to opt for the best possible action for that detection.

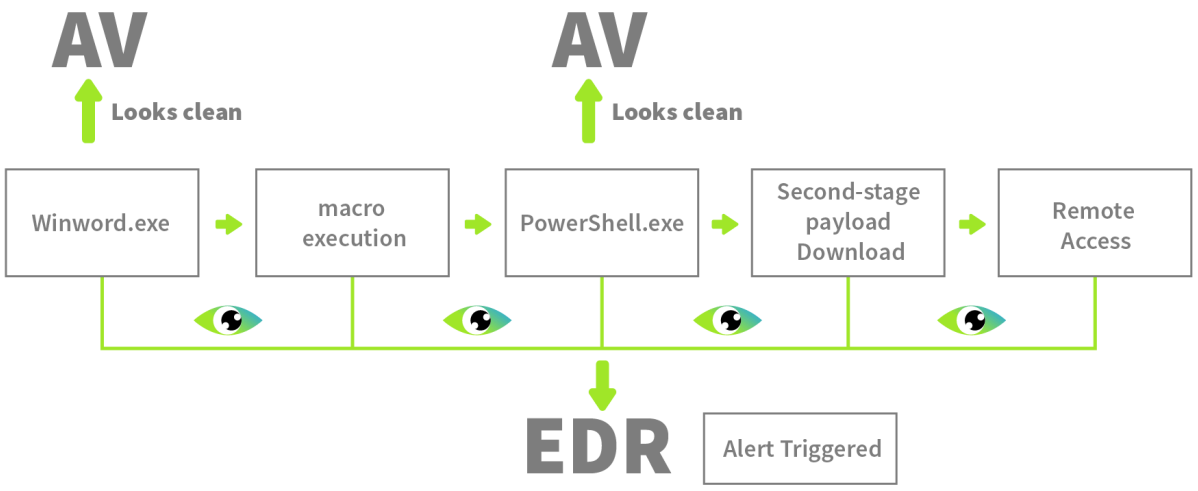
As an analyst, you may decide to isolate a complete endpoint, terminate a process, or quarantine some files. You can also connect to the host remotely and execute actions independently. You can do this all from within the EDR console.

The following screenshot shows the actions available that can be taken on the host after connecting to it.

Examining an advanced malicious activity step by step on an endpoint and compare the response of an AV and EDR at each stage.

Scenario Breakdown

- **Step #1:** A user receives a phishing email with a Word document embedded with a malicious macro (VBA script)
- **Step #2:** The user downloads the document and opens it
- **Step #3:** The malicious macro is silently executed, and it spawns PowerShell
- **Step #4:** The malicious macro runs an obfuscated PowerShell command to download a sophisticated second-stage payload
- **Step #5:** The payload is injected into a legitimate svchost.exe
- **Step #6:** The attacker gains remote access to the system



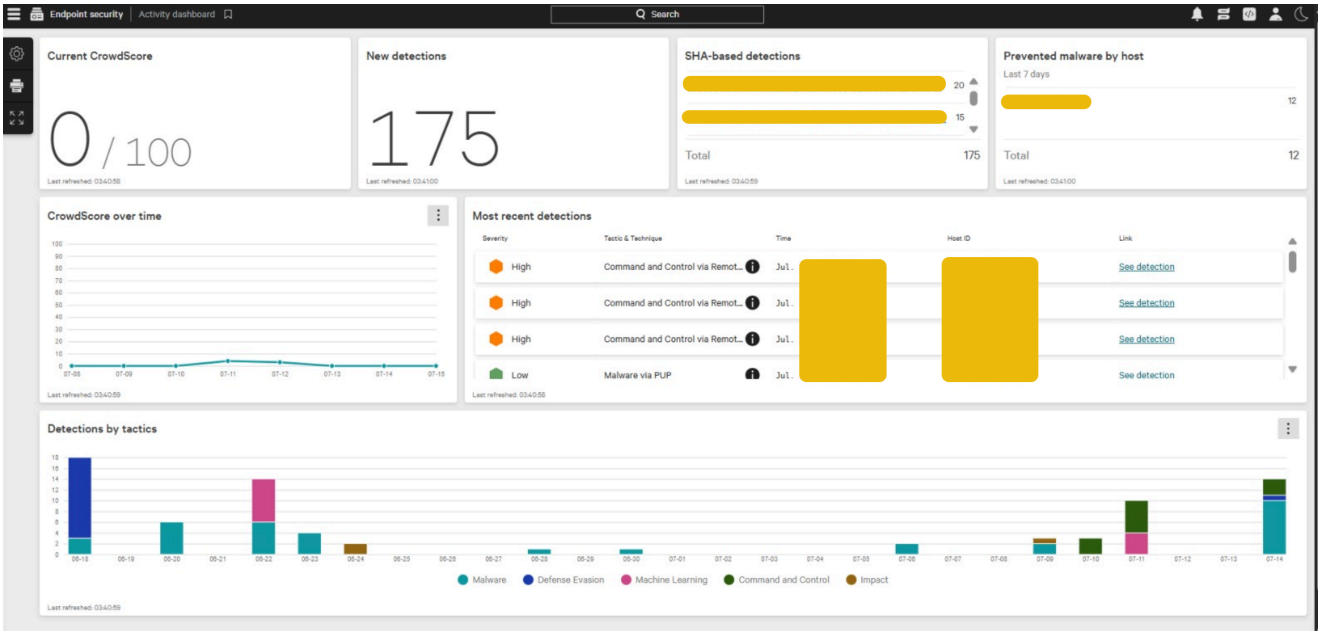
Attack Steps	AV's Response	EDR's Response
Step #1	Does nothing if the downloaded file has no previous signature in the database	Logs the file download activity and monitors it
Step #2	Does nothing upon the opening of the document since winword.exe is a legitimate utility	Records the execution of winword.exe and keeps monitoring
Step #3	Does nothing if the executed macro has no previous signature	Detects and flags the macro execution due to the unusual parent-child relationship of winword.exe and PowerShell.exe processes
Step #4	Typically, AVs will not detect obfuscated PowerShell scripts	Flags the obfuscated script execution
Step #5	Will not flag malicious injection into svchost.exe since it does not monitor the memory injections	Detects Process Injection in svchost.exe
Step #6	Lacks Network Level Visibility	Flags the unexpected behaviour of svchost.exe, making an outbound connection
Final Action	May be marked as clean	Generates an alert with the full attack chain and enables the analyst to take actions from within the EDR

Agents

We can integrate multiple endpoints with our EDR and manage them through a centralized console. There are EDR agents that we have to deploy inside those endpoints.

These agents are also sometimes referred to as **sensors**. They are the eyes and ears of the EDR. Their job is to sit at the endpoint and monitor all the activities.

The information about these activities is sent in detail to the EDR central console in real time. The EDR agents can do some basic signature-based and behavior-based detections by themselves and send them to the EDR console, which triggers alerts.



What happens after Detection?

When a detection comes, it's a SOC analyst's responsibility to acknowledge the alert and prioritize it. The prioritization is made easy by the EDR itself.

It gives severities to all the alerts (Critical, High, Medium, Low, Informational). The alert with the highest severity is investigated as a priority. For the investigation, once the alert is clicked, the analyst can see all the details of the detection.

This includes any files executed, processes executed, network connection attempts, registry modifications, and much more. Based on the available data, the analyst's job is first to use their expertise to determine if the alert is a false positive or a true positive. In case of a true positive, the analyst can take actions from within the EDR console.

EDR with Other Tools

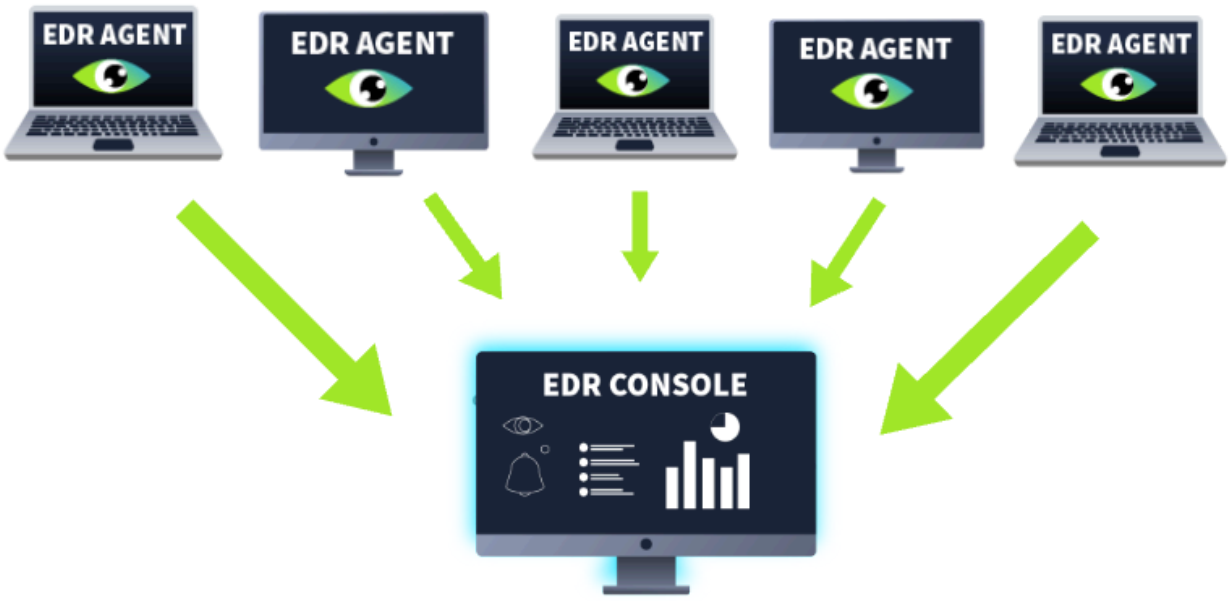
As a SOC Analyst, it is essential to understand that although a standalone EDR provides enough information to detect and respond to threats in an endpoint, it works alongside other security solutions to form a larger security ecosystem.

Within a network, you will see Firewalls, DLPs, Email Security Gateways, IAMs, EDRs, and other security solutions protecting the different components of the network.

To minimize the effort and maximize the efficiency, all these security solutions are integrated with a SIEM solution that becomes the central point of investigation for the analysts. We will also discuss the SIEM solution in detail in the upcoming rooms of this module.

What is Telemetry?

The collected different data from their endpoints and push it to the EDR console. This data is known as Telemetry. Telemetry is the black box of an endpoint with everything necessary for detection and investigation.



Collected Telemetry

Usually, many activities are going on in the endpoints, most of which are legitimate. It is often difficult to differentiate between regular and malicious activity. The more data is collected, the better judgments can be made. EDR collects detailed telemetry from the endpoints. Let's take a brief look at some of the telemetry that it collects:

- **Process Executions and Terminations**
  It keeps track of all the running and idle processes, which helps to identify suspicious child-parent process relationships, suspicious executables initiating a process, malware payload, etc.
- **Network Connections**
  All the endpoints' network connections are monitored, which helps identify any connection to a C2 server, unusual port usage, data exfiltration, or lateral movement within the network.
- **Command Line Activity**
  It captures all the commands executed on the endpoints in CMD, PowerShell, etc., which helps to identify malicious command execution, obfuscated PowerShell script executions, which are often missed by a traditional antivirus.
- **Files and Folders Modifications**
  Threat actors modify different files and folders during data staging, ransomware executions, and malicious file dropping. The EDR tracks this.

- **Registry Modifications**
  The registry is a goldmine of information about the configurations in a Windows system. There are many registry modifications that occur during a malicious activity, and most of these are monitored by the EDR.

Detection And Response Capabilities

Detection

Based on the telemetry received from the endpoints, some advanced detection techniques are applied to this data. Some of these techniques include:

- **Behavioral Detection**
  Instead of just matching the signatures with known threats, it observes the complete behavior of a file. Advanced threats craft their malware to look clean and use legitimate processes to carry out their attack. EDR catches this behavior.
  Example: A process winword.exe spawning PowerShell.exe will be flagged by the EDR due to the behavior. A Word document spawning a PowerShell is an unusual parent-child relationship.
- **Anomaly Detection**
  With time, EDR understands the baseline behavior of the endpoints. Any activity that deviates from this behavior will be flagged. During any malicious activity, the endpoint's behavior deviates from normal. EDR picks it up. Sometimes, this can generate false positives as well. However, with the full context it gives, the analyst can identify its legitimacy.

  Example: On one of the endpoints, a process modifies an auto-start registry key, which is not a common behavior on the endpoint.
- **IOC matching**
  EDRs have some strong threat intelligence field integrations. Except for zero-day attacks, most of the attacks have indicators published in the threat intelligence feeds. EDR flags any activity that matches any known IOC.

  Example: A user downloads a file that drops an executable. The executable is often used in a specific attack. The hash of this executable will get matched with the threat intelligence feed and instantly flagged by the EDR.
- **MITRE ATT&CK Mapping**
  Any activity flagged by the EDR is not only marked as malicious or suspicious but also mapped with the MITRE Tactic and Technique (attack stage) that the particular activity was on. This proves to be very helpful for the analysts.

  Example: If the EDR flags the creation of a scheduled task for any reason, it will likely map this activity to the following:
  - Tactic: Persistence
  - Technique: Scheduled Task/Job
- **Machine Learning Algorithms**
  Advanced threat actors try to evade defenses as much as possible, and their activities may sometimes bypass advanced detection techniques. Modern EDRs have machine learning models trained by a large dataset of normal and malicious behaviors. This can detect complex patterns of an attack.

  Example: Attacks in which the individual actions are not inherently malicious, but the ML algorithm identifies the whole chain of activities as malicious. Fileless attacks and multi-staged intrusions are often detected through this.

Response

The next step after any detection is the response. EDR offers both automated and manual responses. You can make policies to block known malicious behaviors automatically. However, manual response gives you a wide range of response capabilities. Let's discuss some of them.

- **Isolate Host**
  During any malicious activity on an endpoint, you can isolate that endpoint from the network through EDR. This is a very effective function for containing malicious activity. Most attacks start from a single endpoint and move laterally to other endpoints to compromise the whole network. Isolating the infected endpoint on time can stop this from happening.
- **Terminate Process**
  Not every malicious activity requires host isolation. Some hosts run the core business operations, and isolating them can cause more loss than the malicious activity. In such cases, terminating a process is enough to neutralize the malicious activity. The analysts get this option in the EDR. They can terminate any process at any time. This action should be taken consciously since terminating a legitimate process can disrupt the endpoint.
- **Quarantine**
  If a malicious file comes into the endpoint, it can be quarantined. Quarantine ensures that the file is moved to an isolated location where it can not be executed. The analysts can then review the file to restore or permanently remove it.
- **Remote Access**
  Analysts can also remotely access the shell of any endpoint. This is often done when the EDR's built-in response is not enough to take action on a specific activity. Through remote access, analysts can gain deeper visibility into the system or take custom actions within the endpoints. The analysts can also run scripts or collect their desired data from the host through remote access.

  Below is an example of CrowdStrike Falcon EDR's RTR (Real Time Response) console, which allows analysts to remotely access the shell of any endpoint and run commands and scripts.


Falcon Real Time Response
hq-prd-website | Console
Search
Hostname
hq-prd-website
Platform
Linux
Connection status
Connected (Session start: Aug. 12, 2025 20:05:12)
End session
/> help
Jump to bottom
cat Read a file from disk and display as ASCII.
cd Change the current working directory.
clear Clear screen.
cp Copy a file or directory.
encrypt Encrypt a file with AES-256.
env Print out the environment.
Run commands
Edit & run scripts
1 grep -REi 'base64_decode|eval\(|assert\(|shell_exec|system\(|passthru|exec\(|popen\(|proc_open\(' /var/www/html
Arguments
Enter arguments
Save as
Run script