



Qualys Endpoint Detection and Response v1.x

Release Notes

Version EDR 1.2.0

January 14, 2020

Here is what you get with Qualys EDR 1.2.0!

[Leverage MITRE ATT&CK Framework](#)
[MITRE ATT&CK Tokens](#)

Note: You must upgrade to Cloud Agent version 4.1 or above to utilize all the EDR functionalities.

Leverage MITRE ATT&CK Framework

With this release, we are excited to leverage the MITRE ATT&CK framework. MITRE ATT&CK defines the tactics, techniques, and procedures that are leveraged by adversaries and malware.

Unlike the traditional endpoint tools that decide if a file is malicious or not, MITRE ATT&CK is more behavioral focused that analyzes when humans or malware leverage the built-in operating system binaries, utilities, or capabilities which otherwise might not be malicious on their own.

EDR helps detect malicious behavior on the endpoint by evaluating the events in context with MITRE ATT&CK. Having ATT&CK context also aids analysts when hunting for and responding to incidents within their environment.

EDR will now analyze the events registered on the agents and apply ATT&CK tactics and techniques where appropriate on the Event Details page.

The screenshot displays the 'Event Details' page for a process named 'chrome.exe'. The page is divided into several sections:

- Summary:** Shows the process name 'chrome.exe'.
- Event:** Displays event details including ID, Event Collected Date, and Object Type.
- MITRE ATT&CK Technique/s:** A red-bordered box highlights this section, which lists the technique ID (T1148) and name (Abuse Elevation Control Mechanism).
- MITRE ATT&CK Tactic/s:** Lists the tactic ID (TA0043) and name (Reconnaissance).
- Process:** Provides details about the process, including its state (RUNNING), name (chrome.exe), full path, and arguments.
- Asset Details:** A sidebar on the right containing information about the asset, including its hostname, FQDN, IP addresses, and activity logs.

MITRE ATT&CK Tokens

We have added the following four MITRE ATT&CK tokens on the Hunting tab:

- **mitre.attack.tactic.id:** This token will help you find events with the tactic ID from the MITRE ATT&CK framework.
- **mitre.attack.tactic.name:** This token will help you find events with the tactic name from the MITRE ATT&CK framework.
- **mitre.attack.technique.id:** This token will help you find events with the technique ID from the MITRE ATT&CK framework.
- **mitre.attack.technique.name:** This token will help you find events with the technique name from the MITRE ATT&CK framework.

For detailed information on each token, see Hunting tab on EDR UI.