CMC CYBER SECURITY LTD.

15th Floor, CMC Tower, Duy Tan Street, Dich Vong Hau Ward, Cau Giay District, Hanoi | Tel: 84.4.3795 8282 | Fax: 84.4.3984 5053 | www.cmcinfosec.com

DATASHEET FOR ENDPOINT DETECTION & RESPONSE SOLUTION

Official Member of AVAR and ICSA

Hanoi, 15/09/2020

CMC CYBER SECURITY
Aspire to Inspire the Digital World

CMC CYBER SECURITY Ltd.

Version	1.0
Date	15/09/2020
Document Type	Datasheet
Prepared By	Luu Duc Hien

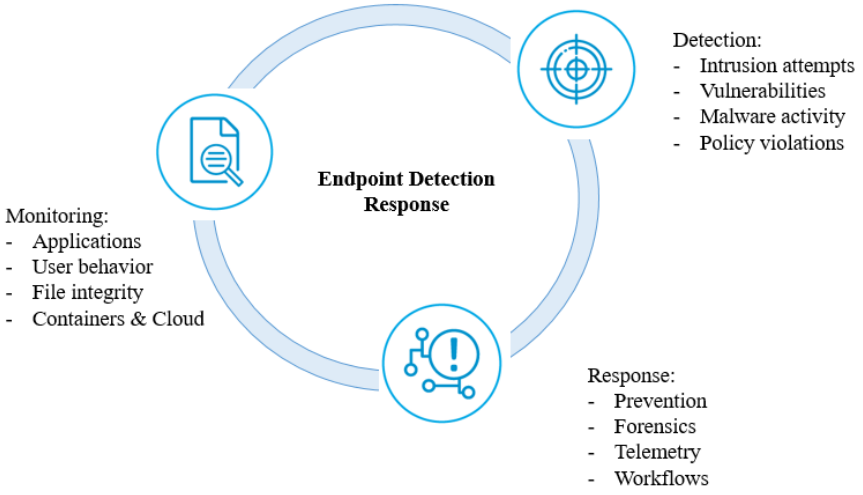
CMC CYBER SECURITY
Aspire to Inspire the Digital World

Contents

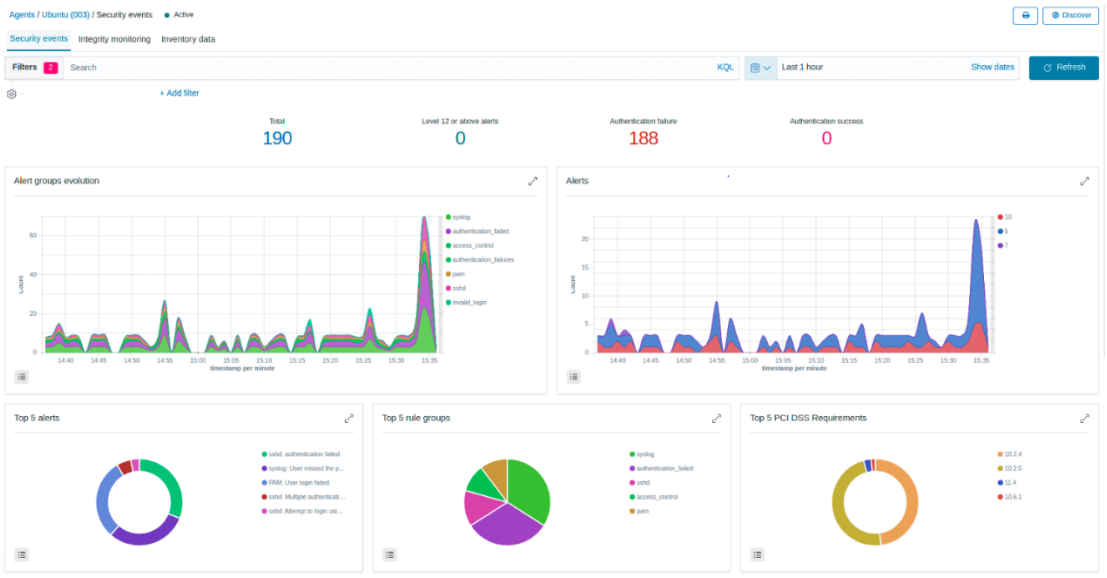
1. Introduction to CMC EDR

a. Description

CMC EDR is an AI-integrated Threat-prevention solution responsible for stopping the infection of malware, with additional security controls to manage protective measures against script-based, file-less, memory, and external device-based attacks.



Unlike traditional enpoint security products which base on signatures and behaviour analysis to detect threats within the network infrastructure, CMC EDR with these significant features along with minimal system impact and protection against Zero-day is capable of securing endpoints and organisation against compromises from attackers:



- Using Artificial Intelligence (AI) instead of Signatures to identify and protect against both known and unknown malware operating on endpoints.
- Prevent both widely known and Zero-day attacks without Internet connection
- Constant protection of endpoints without interruptions to end-users' activities
- Early identification and prevention of APT attacks.
- Assessing and identifying violations to policies or regulations.

b. Functions:

CMC EDR provides:

- *Security Events Analysis:*
  - EDR is used to collect, synthesize, index and analyse security data, assisting organisations in detecting infiltration, threats or Endpoint anomalous behaviours.
  - As cyber threats are becoming more and more sophisticated, real-time event monitoring and analysis are more and more necessary for fast detecting and resolving these threats.
- *Intrusion Detection:*
  - Our EDR Agent will be scanning the monitored endpoints, looking for malware, rootkits and abnormal events. CMC EDR is capable of detecting hidden files, processes or unknown registry,…

  - Apart from Agent's and Signature-based server's detection capability, our EDR also uses AI to analyze collected data and look for IoCs.
- *Data Log Analysis:*
  - Data logs and events that are collected from Endpoints and sent to CMC SOC via VPN encrypted transmission will then be analysed by the SOC Team.
  - The data that is collected includes: application and system errors, incorrect configurations, malicious activities that are attempting to execute or have successfully executed, policies violations and other security issues, …
- *Monitoring Packet Integrity:*
  - EDR monitors packets, identifying alterations in contents, rights, ownership rights and attributes of these packets. Moreover, the Agent also identifies the users and applications used for creating and modifying packets.
  - The EDR 's monitoring packet integrity capability is AI-assisted, helping with identifying threats or servers under intrusion. Furthermore, EDR monitors compliance to the PCI DSS
  - Activating alerts when alterations occur. The Cryptographic Checksum and good attributes of packets along with known Windows Registry keys are stored and frequently matched with currently used packets in the system to monitor and detect alterations.
- *Vulnerability Detection:*
  - EDR Agent collects data and checks on relevant information of applications and software, then sent it to our Threat Intelligence-integrated EDR Server, assisting in analysing events and constant updating of CVEs and threats that may impact the system negatively.
  - Automatic assessment of vulnerabilities will assist system administrators in identifying fragilities in important assets to devise solutions before attackers can exploit them, damaging the system integrity or stealing sensitive data.
- *Audit Assessment:*

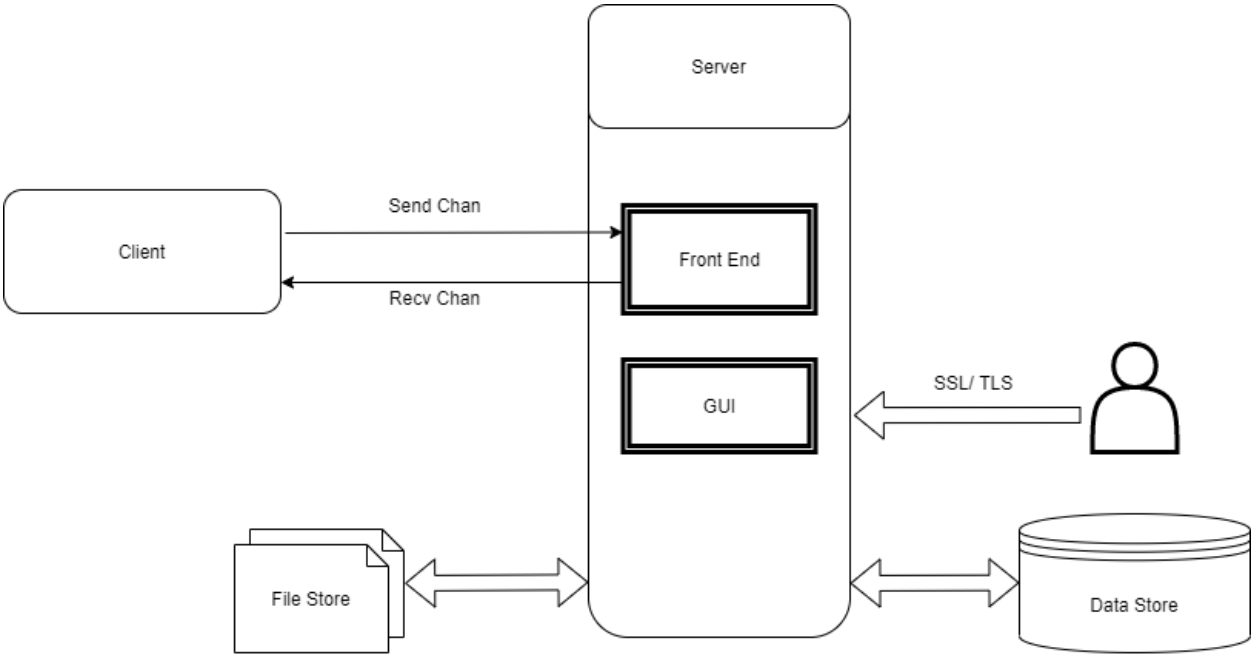
  - EDR monitors system and application configuration to ensure compliance with security policies and standards as well as organization's own policies. Agent will scan periodically to detect any exploitability, unpatched vulnerability or non-secured configuration on known applications.
  - Furthermore, configuration assessment can be modified or customized, tailoring different organisations' different system structures. The alerts will include recommendations for configuration in reference to and mapped with organisations' own policies.
- *Incidents Investigating and Responding:*
  - EDR provided response scenarios along with actions and steps to handle threats
  - Assist in responding to incidents happening on workstations (such as: workstations isolation, removing files, removing/isolating processes, removing values in registry, blocking network connections, etc.)
  - Furthermore, EDR can be used to run commands or remote queries to identify IoC (Indicators of Compromise) and assisting in digital forensics or direct incident response.
- *Monitoring and Assessing Compliance:*
  - CMC EDR provides a few security controls necessary for organisations' policies and standards compliance. These functions, combining with expandability across multiple platforms help organisation comply with technical standards and requirements.
- *Threat intelligence:*
  - Threat Intelligence acts like a virtual appliance monitored and integrated into EDR Server, responsible for storing and updating all information on known Advanced Malware/APT Attacks from CMC's APT analysis system
  - CMC Threat Intelligence updates information on threats, malware behaviours, attack methods, Zero-day exploitation method, etc. in real-time from CMC and sharing in real-time this info with Agent-installed. CMC Threat Intelligence constantly collects and updates

data from multiple sources, ensuring the fastest response to threat when one of the sources is tipped.

- *Concentrated Monitoring Dashboard:* The Web-based Dashboard helps with information lookup and display on workstations (file's hash, registry, network connection)

2. Operating

a. Mechanism



Installed EDR Agent on guest machines are connected to the server. The administrator can access to the Web Portal Dashboard via a browser, with connections encrypted with SSL/TLS Protocol. Admins can query the Endpoints from Dashboard to collect information for forensics and analysis or monitoring security events.

Log collection:

- For supported OS, CMC SOC will provide compatible agent to install on compatible devices.
- For OS and applications that are not in the support list, CMC SOC will provide compatible log decoder. This ensures easier system expansion in the future.

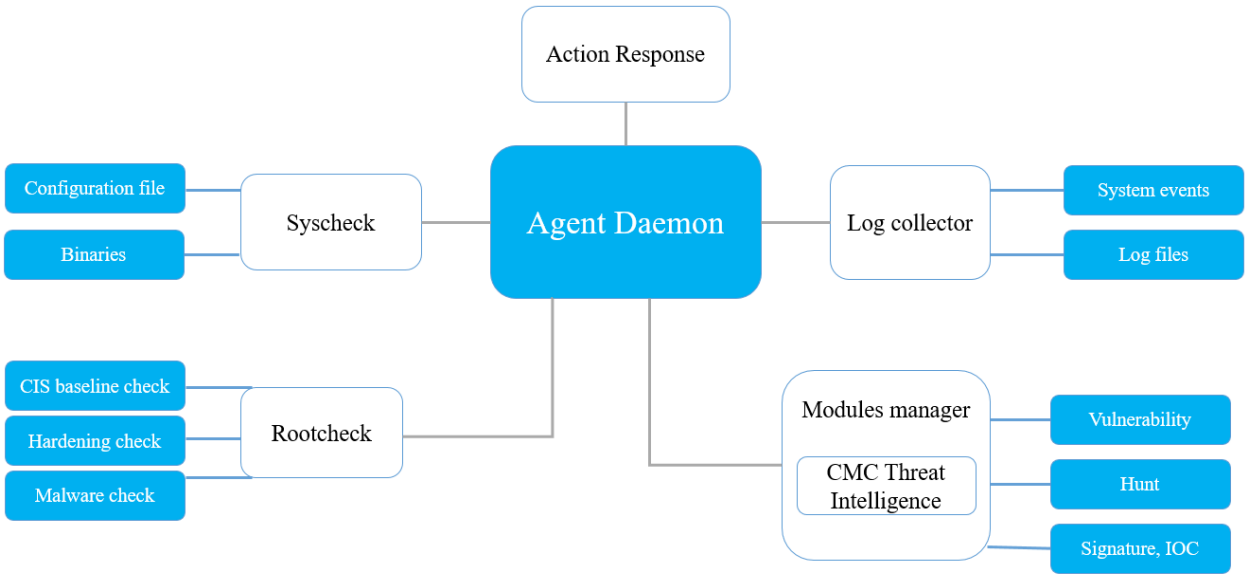
Installment and Integration:

- Upon implementing, CMC will be installing our EDR on clients' important workstations within the system
- Apart from passing logs from Agent to the EDR Server, CMC SOC personnel can configure to pass log from our EDR Server to clients' SIEM for integration

b. EDR Agent

EDR Agent is compatible with OS such as Windows, Unix, Linux, etc. It is used for collecting information on application data and system data, based on customisations from EDR Server. The data will then be transferred to the server via an encrypted and verified channel. In order to set up these security channel, each and every Agent will be assigned their own key

The Agents are able to monitor physical host servers, virtual machines, cloud, network devices, etc. Install packs for Agent is readily available for Windows, Unix, Linux, etc. Different actions and processes are also used for system monitoring such as: Monitoring Packet Integrity, Examining system data logs, and so on



Description:

- Rootcheck:
  - This process contains actions related to rootkit, malware and system anomalies detection.
  - Agent will also be performing basic security tests on system's configuration files.
- Log collector:
  - This component reads data log information collected from applications and operation systems, including: log access, log activity, log security, …
  - Log collecting can be tailored to specific monitoring demand on specific system.
- Syscheck:
  - This process monitors file integrity (FIM) and Registry keys created in the system.
  - Ability to detect alterations in a file, content, ownership, etc. as well as adding and removing files.
  - Scanning FIM frequently can also be configured to generate real-time alerts.
- CMC Threat Intelligence:
  - This module uses the CMC Threat Intelligence threat database including: vulnerability, signature, IOC, …
  - By scanning the system frequently, EDR is able to detect vulnerable applications or configurations that are not complying to standards
- Action Response:
  - EDR Server will command Agents to perform executive actions on Endpoints
  - Scanning and collecting information from Endpoints such as processes, connections, system info
  - Performing Block or Allow actions following results from EDR server when security issues surface. . Performing Remediate actions for workstations in case the workstations have already been attacked

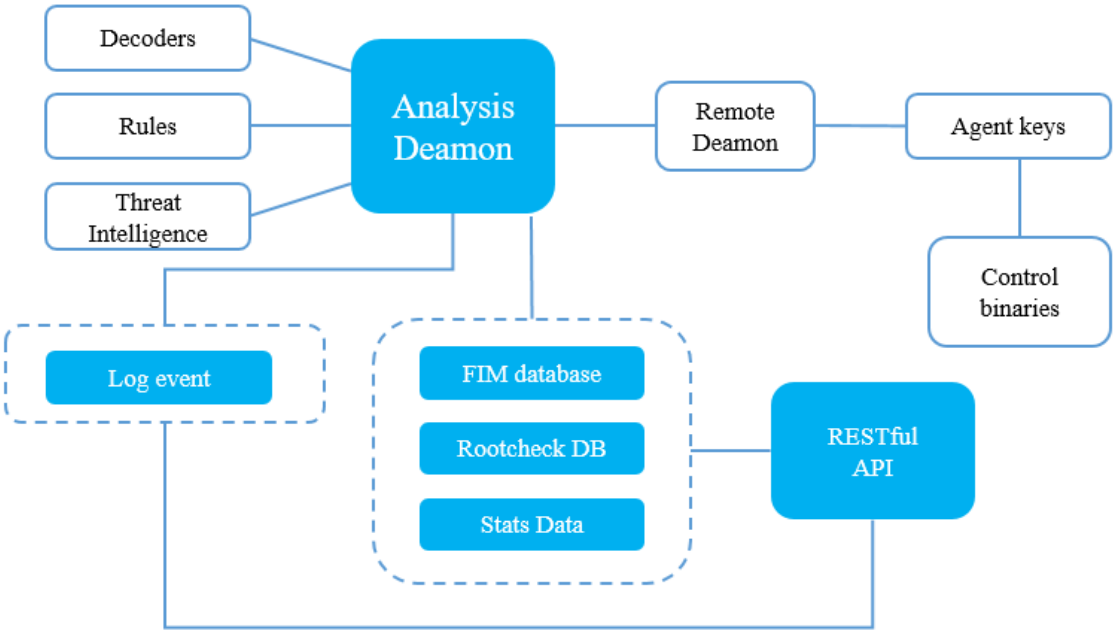
- Agent Deamon:
    - This is the process of receiving data collected or generated from Agent installed on Endpoints. The data is compressed, encrypted and sent to the server via a verified channel.

c. EDR Server

EDR Server is responsible for analysing data collected from Agent and generating alerts on collected events. For example: intrusion detection, file alteration, potential rootkit, configurations not complying to policies…

EDR Server provides a Portal interface for:

- Collecting data from Agents
- Looking up, and extracting data for forensics and analysis
- Adding/editing/removing monitoring and collecting rules on Agents
- Remote accessing into Agent-installed to download files and examine Registry, …



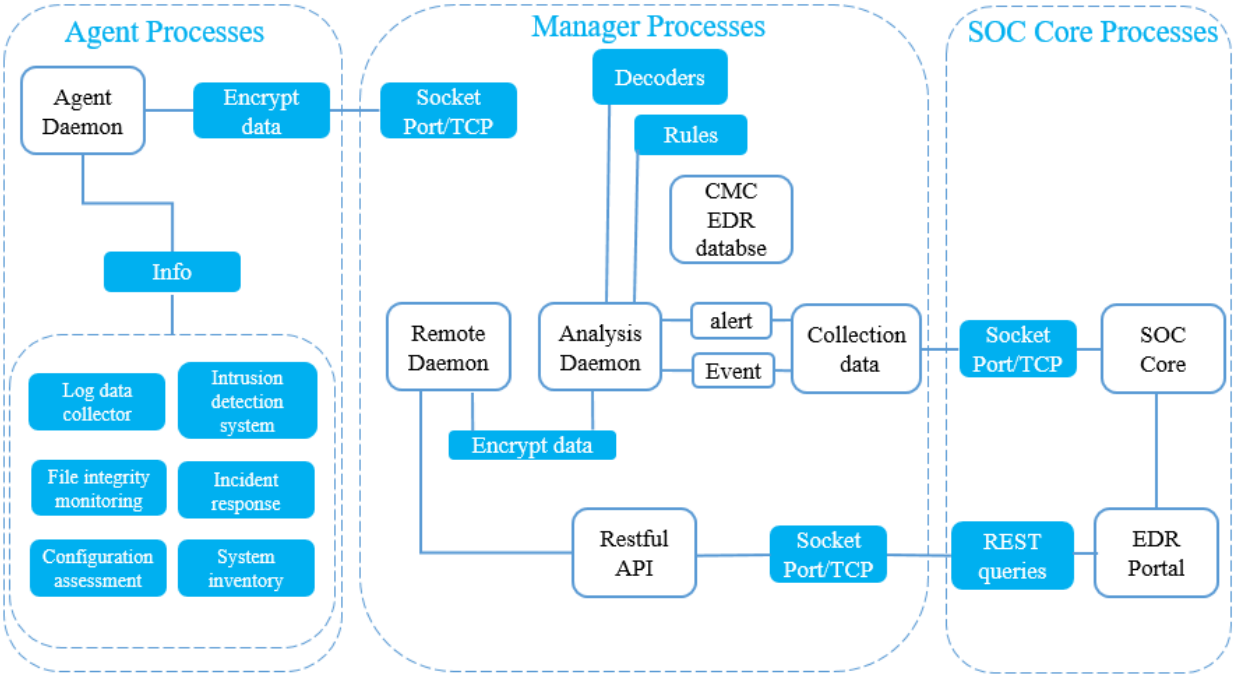
The EDR server is often deployed on an independent physical host server or a virtual machine, with the following modules:

- Registration service:
  - Used for registering new Agents with verification key (each Agent will be assigned one key only)
- Remote Deamon service:
  - Sending and receiving data from Agents. Data are sent and received using pre-verified keys.

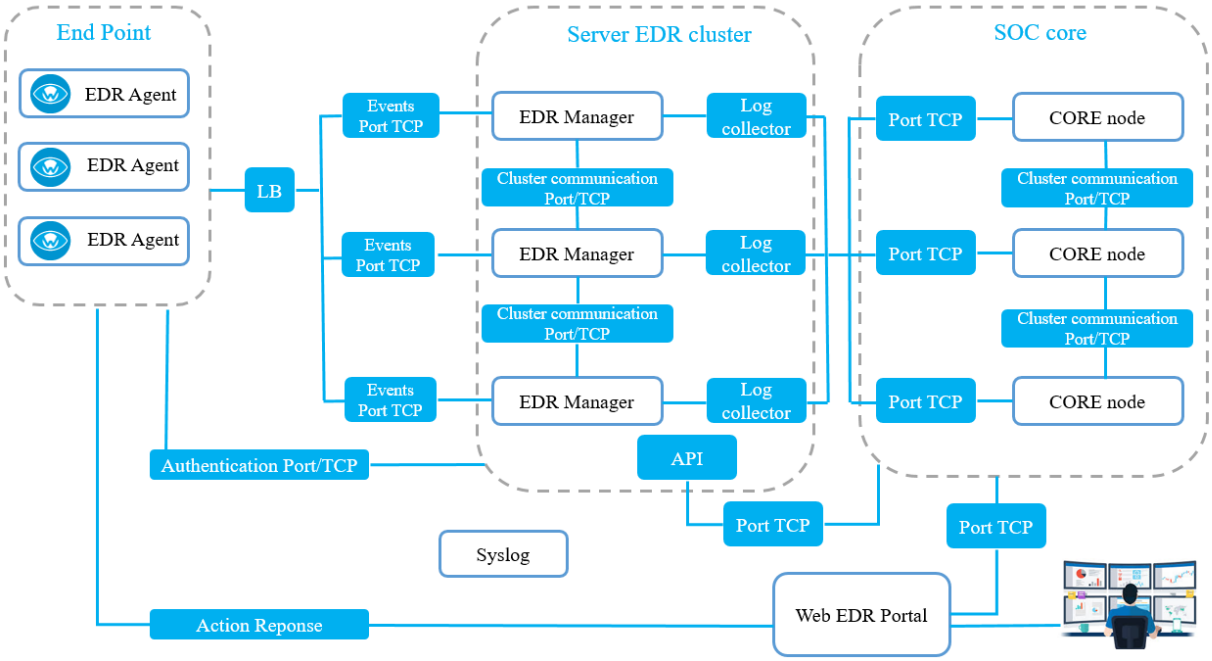
  - EDR Server can also sends commands to the Agents to perform incident response tasks when there is a threat surfaces on Endpoints.
- Analysis Deamon:
  - This is the process of data analysing using Decoders to identify the type of info currently under analysis: event logs, servers' data logs, etc.), then extracting event-related data such as: Source IP, Event ID, Users, etc.
  - Rulesets, threat data packets are used in combination with analysis based on AI algorithm to generate alerts as well as recommendation for each detected risk.
- RESTful API:
  - Provide interface for managing and monitoring Agent's configuration and status.

d. EDR Structure

The EDR Structure is designed based on monitored Agents running on Endpoints for transferring data logs to EDR Server. Moreover, for devices that Agents cannot be installed on such as Firewall, Switches, Routers, access Points, etc., CMC will configure to send data log via syslog. The EDR Server will then decrypt and analyse this data and perform actions if necessary.



3. Deployment blueprints



EDR Agent:

- The EDR Agent software is installed on Endpoints in the system that uses EDR solution. The Agents are responsible for collecting information such as logs, processes, file info, hash function, etc. for forensics and Block/Remediate actions when attacks are detected on Endpoints
- Agent's componenets:
  - EDR Agent software
  - Solutions suchs as: Threat Intelligence Exchange and Data Exchange Layer for receiving and updating patches as well as Threat Intelligence data packets from EDR Server; and transferring data (including processes, connections, scan results, etc.) from Agent to EDR Server
- Agent's responsibilities:
  - Scanning and collecting information from Endpoints including processes, connections, system info, etc. and transferring to EDR Server (The server includes Threat Intelligence Exchange and Active Response).
  - Performing Block or Allow actions following results from EDR server when security issues surface. . Performing Remediate actions for workstations in case the workstations have already been attacked

EDR Server:

- EDR Server is responsible for managing and storing information on malware activities, attacking behaviours, known APT behaviours, etc
- Information on newly discovered threats are collected and analysed on CMC Threat Intelligence will also be updated frequently for the EDR Server, ensuring its capability for identifying, detecting and blocking attacks.
- CMC EDR provides a Web-based interface, assisting admins in operation such as Threat Intelligence Exchange and Active Response actions, detecting system issues, etc.

4. Integration capability

CMC EDR is compatible for integration with system including:

Microsoft Windows (32-bit or 64-bit)	Linux	Mac OS
• Windows XP SP3 • Windows Vista • Windows 7 • Windows 8 and 8.1 • Windows 10 • Windows Server 2003 SP2 • Windows Server 2008 / 2008 R2 • Windows Server 2012 / 2012 R2 • Windows Server 2016	• Red Hat Enterprise Linux / CentOS 6.6 — 32-bit and 64-bit • Red Hat Enterprise Linux / CentOS 6.7 — 32-bit and 64-bit • Red Hat Enterprise Linux / CentOS 6.8 — 32-bit and 64-bit • Red Hat Enterprise Linux / CentOS 7.0 — 64-bit • Red Hat Enterprise Linux / CentOS 7.1 — 64-bit • Red Hat Enterprise Linux / CentOS 7.2 — 64-bit • Red Hat Enterprise Linux / CentOS 7.3 — 64-bit	• Mac OS X 10.9 (Mavericks)* • Mac OS X 10.10 (Yosemite)* • Mac OS X 10.11 (El Capitan)* • Mac OS X 10.12 (Sierra)* *Complements Apple's built-in XProtect

• 2GB Memory • 500MB Available Disk Space • Microsoft .NET Framework 3.5 SP1 • Internet browser • Internet connection to register product • Local admin rights to install software	• 2GB Memory • 500MB Available Disk Space • Internet browser • Internet connection to register product • Local admin rights to install software	• 2GB Memory • 500MB Available Disk Space • Internet browser • Internet connection to register product • Local admin rights to install software

Log Collection:

- For supported OS, CMC SOC will provide compatible agent to install on compatible devices.
- For OS and applications that are not in the support list, CMC SOC will provide compatible log decoder. This ensures easier system expansion in the future.

Installment and Integration:

- Upon implementing, CMC will be installing our EDR on clients' important workstations within the system
- Apart from passing logs from Agent to the EDR Server, CMC SOC personnel can configure to pass log from our EDR Server to clients' SIEM for integration