Monitoring Threats Menggunakan Huntbox dengan Metode MDR (*Managed Detection and Response*) pada *Security Operation Center* (SOC)

Wisnu Murti Adi Santoso[1)], Noora Qotrun Nada[2)].

[1,2] Jurusan Informatika, Fakultas Teknik dan Informatika, Universitas PGRI Semarang Gedung B Lantai 3, Kampus 1 Jl. Sidodadi Timur 24, Semarang
[1]Email : Mwishnu030@gmail.com
[2]Email : noora@upgris.ac.id

Abstrak *– Pusat operasi keamanan atau Security Operation Center (SOC) yang bertanggung jawab untuk melakukan praktik Cyber Threat Hunting yang merupakan praktik mendeteksi ancaman tingkat lanjut dengan mengidentifikasi, dan memahami tingkah laku threat actor dan cyber threat seperti: phising, ransomware, dan malware. Maka dari itu, untuk mempermudah praktik Threat Hunting dibutuhkannya Huntbox, sebuah platform layanan keamanan didunia cyber yang menyediakan seperangkat alat untuk memantau, menanggapi kejadian, dan deteksi ancaman. Metode yang digunakan pada Huntbox ini adalah metode MDR (Managed, Detection, and Response) solusi mengidentifikasi ancaman secara real-time untuk mengaktifkan tindakan menanggapi ancaman dengan segera untuk memusatkan, menghubungkan, dan menganalisis kumpulan data yang dihasilkan dari berbagai alat yang digunakan di lingkungan keamanan digital.*

Kata Kunci : *Pusat Operasi Keamanan, Security Operation Center (SOC), Huntbox, Cyber Threat Hunting, MDR (Managed, Detection, and Response).*

PENDAHULUAN

Seiring tingginya arus digitalisasi dengan mengadopsi teknologi informasi dan penyedia media informasi dibidang industri dan bisnis, melalui internet juga menjadi kegiatan komunikasi komersial dengan bagian terbesar dan pesatnya pertumbuhan sehingga aspek kemanan *cyber* perlu lebih diwaspadai mengingat dampak positif maupun negatif sangat besar dalam dunia hubungan internasional saat ini.

Keberadaan *cyber threats* yang merupakan tindak kejahatan dari perilaku orang yang tidak bertanggung jawab untuk kepentingan pribadi dengan cara merugikan orang lain terus membayangi aktifitas digital dan ditambah terjadinya lonjakan traffic data sehingga meningkatnya pengguna layanan digital membuat potensi cyber crime semakin meningkat dan membuat kebutuhan akan teknologi jaringan komputer semakin meningkat dan perlu kita pahami bahwasannya kita tidak dapat mencegah para *Hacker* untuk melakukan tindak kejahatan *cyber,* namun yang dapat kita upayakan secara maksimal adalah meminimalisir resiko dan dampak cyber attack, dengan *proactive* melakukan upaya pencegahan, serta bersiap diri melakukan *response* jika sesuatu terjadi *compromise* atau *breach* pada infrastruktur kita.

Dengan adanya Pusat Operasi Keamanan atau *Security Operation Center* (SOC), *Cyber Security* berupaya atau bertindak untuk menganalisis dan mendeteksi ancaman sehingga dapat melindungi akses jaringan, sistem, program, dan data dari maraknya tindak kejahatan di dunia digital yang berupa *hacking, espionage industry, sabotage*, penyebaran informasi palsu (*hoax*), pembobolan bank dan lain-lain dapat dicegah peretasannya dengan pendeteksian aktivitas ilegal dalam sistem berbasis informasi.

Sebagai solusi memadukan dan pengembangan produk layanan kemanan dunia digital, Maka penulis membutuhkan *Huntbox* yang merupakan sebuah platform yang membantu untuk memonitoring *cyber threats* dengan metode *Managed, detected,* & *response* (MDR) yang menyediakan seperangkat alat untuk memantau, incident response, dan mendeteksi ancaman untuk membantu menangkal serangan dan dirancang untuk melindungi data dan aset. Dengan kontrol keamanan tingkat lanjut yang mencakup berbagai aktifitas keamanan mendasar termasuk keamanan *cloud* yang terkelola dengan menggabungkan konsep layanan *advanced analytics, threat intelligence*, dan keahlian dalamm *incident investigation response* di tingkat *host* dan jaringan.

METODE

Tinjauan Pustaka

1. Pengertian Cyber Security

   Upaya atau tindakan beberapa pihak untuk melindungi akses jaringan, sistem, program, dan data dari berbagai ancaman *cyber* atau akses illegal dengan praktik yang memastikan kerahasiaan, integritas, dan ketersediaan informasi agar terjaga dengan aman.

2. Pengertian Security Operation Center

   Pihak yang bertanggung jawab untuk melakukan mendeteksi serta menganalisis serangan dan ancaman dengan menilai dampak yang diakibatkan oleh serangan cyber sehingga dapat menanggapi insiden keamanan yang terjadi[2].

3. Pengertian Cyber Threats

   Ancaman keamanan digital yang mengacu pada serangan berbahaya yang berupaya mengakses data secara tidak sah, mengganggu operasi digital, atau merusak informasi.

4. Threat Hunting

   Praktek pencarian iterative melalui data untuk mendeteksi ancaman tingkat lanjut yang memfokuskan aktivitas dan bersifat berulang kali dengan melakukan pendekatan untuk mengidentifikasi, dan memahami threat actor yang mungkin sudah masuk kedalam dan berada didalam infrastruktur Teknolologi Informasi.

5. Managed, Detection, and Response

   Metode dengan cara merekam kronologi perilaku pengguna dan mengeksekusi program dalam sistem dan mengumpulkan informasi kontekstual tambahan untuk mendeteksi perilaku berbahaya dalam infrastruktur.

Tools Pengembang

1. Perangkat Lunak
   a. HuntBox atau Threat Hunting Framework

      Framework yang dirancang untuk mendeteksi serangan bertarget yang kompleks dan ancaman yang tidak diketahui sehingga dapat mencari ancaman baik dari dalam maupun luar infrastruktur yang dilindungi, menanggapi kejadian, dan meneliti ancaman yang terjadi [1].
2. Perangkat Keras
   a. Sensor

      Dirancang untuk mendeteksi ancaman jaringan secara analisis mendalam pada lalu lintas jaringan [4].

   b. Polygon

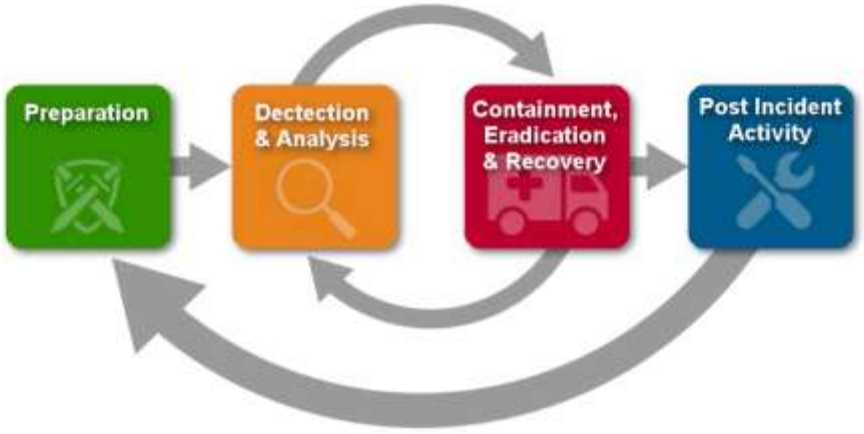
      Sebuah hardware peledak malware yang dirancang untuk mendeteksi ancaman melalui analisis perilaku email, file, dan URL dalam lingkungan yang terisolasi [6].

   c. HuntPoint

      Dirancang untuk melindungi workstation pengguna dari ancaman dengan menghadirkan garis keras waktu lengkap peristiwa di workstation, mendeteksi anomaly, memblokir file berbahaya, mengisolasi host, dan mengumpulkan data forensic.

Metode Pengembang

Dalam pengembangan model Threat Hunting digunakan metode Incident Response yang bertujuan untuk memuat dan meminimalkan dampak dari kejadian cyber incident, baik dari akibat serangan, penyalahgunaan, atau bahkan bencana besar dari ancaman digital sehingga dapat menangani situasi dengan cara yang membatasi kerusakan dan mengurangi waktu pemulihan dan biaya yang diakibatkan ancaman digital.

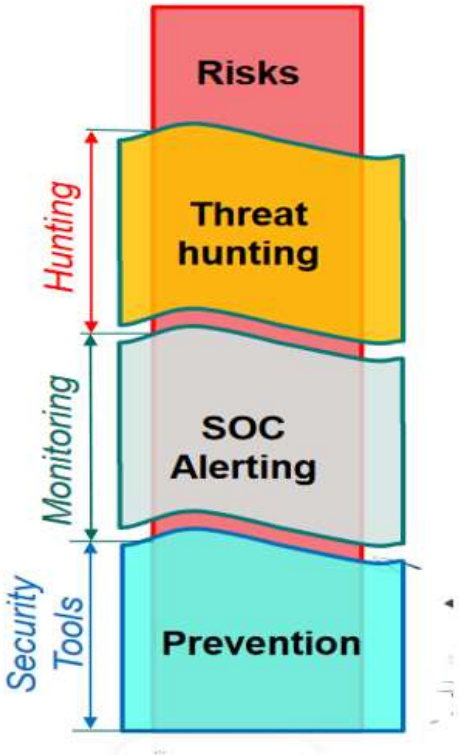


Gambar 1. Siklus Metode Incident Response

Tahapan Penelitian

Supaya penelitian berjalan sesuai dengan yang direncanakan, dibutuhkannya kerangka penelitian. Penulis menggunakan tahapan pada metode *Managed, Detection, and Response* (MDR) pada penelitian ini, sehingga urutan

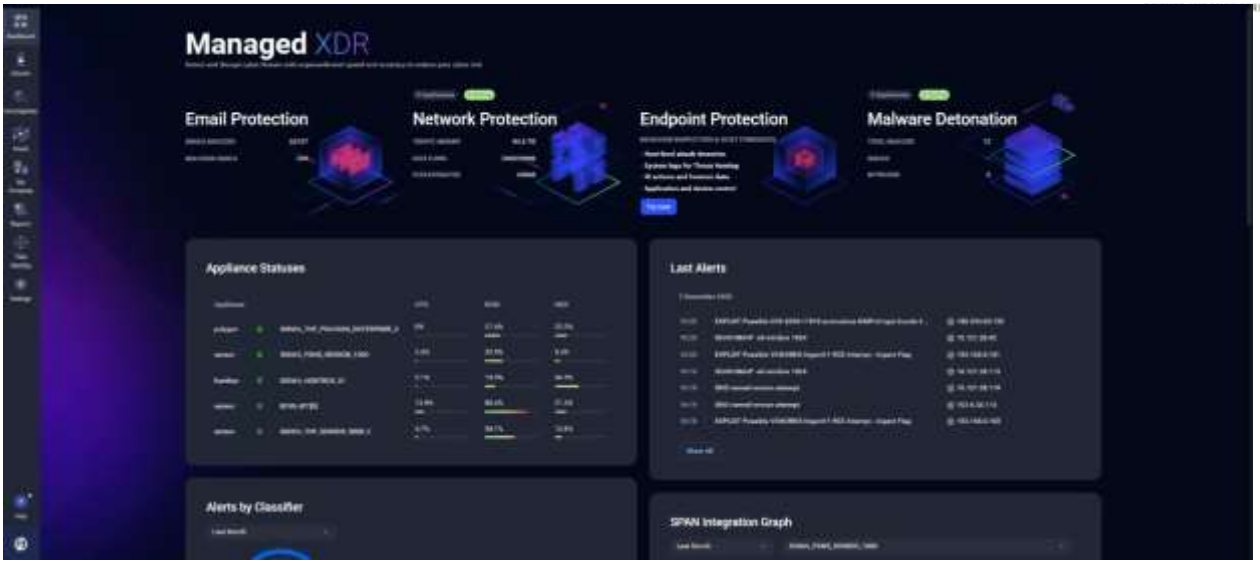
kerangka penelitian berdasarkan pada konsep metode *Managed, Detection, and Response* (MDR). Berikut pada Gambar 2 merupakan struktur kerangka penelitian pada *Security Operation Center* (SOC) yang didasari pada 3 fungsi utama yaitu panulis (*People*) sebagai faktor kunci yang bertugas *Monitoring* dalam *Alerting Security Operations Center* atas insiden atau analisis keamanan sehingga dapat mendefinisikan dan mendokumentasikan Proses (*Processes*) *Threat Hunting* sehingga eksekusi dapat dilakukan dengan Teknologi (*Technology*) *Security Tools* yang memastikan bahwa pusat keamanan operasi akan memiliki kontrol untuk melakukan pemantauan dilingkungan infrastruktur yang kritis dan bermasalah.



Gambar 2. Kerangka Penelitian

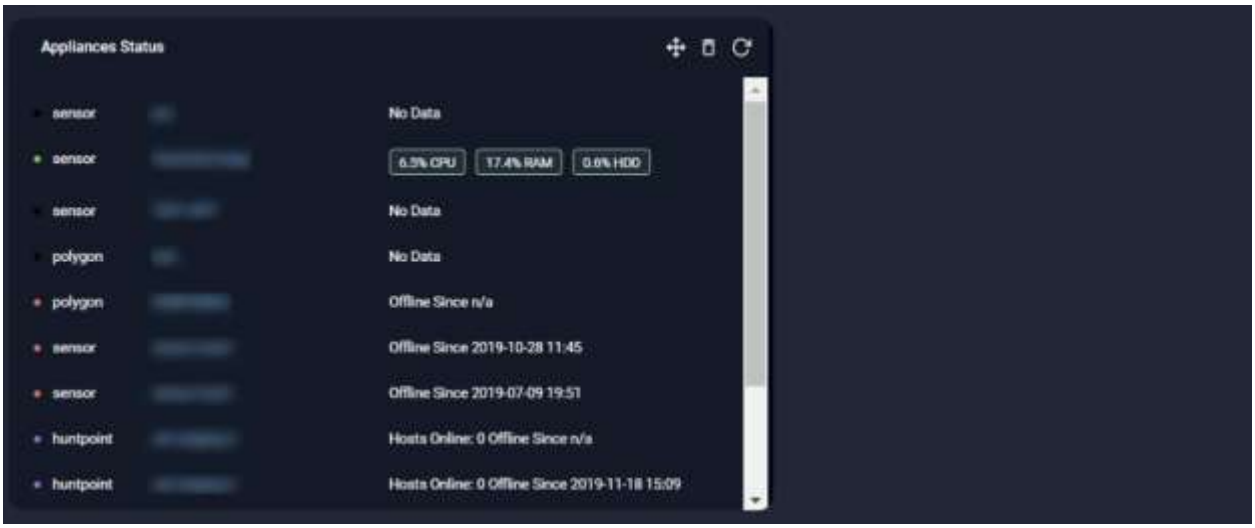
Metode Pengumpulan Data

Sebagai bahan pendukung dalam mencari dan mengumpulkan data yang diperlukan pada penelitian untuk penulis, data yang dicari harus sesuai dengan tujuan penelitian. Metode yang digunakan adalah Studi Pustaka. Untuk mendapatkan data yang bersifat konstektual maka penulis melakukan pengumpulan data pada *huntbox threat hunting framework* yang menyediakan *dashboard* yang memuat informasi terkait dari *appliance status* hingga *execution*. Gambar 3 yang merupakan tangkapan layar dari *dashboard* yang tersedia pada *Threat hunting framework* yang mencakup informasi dan *fitur* didalamnya [4].



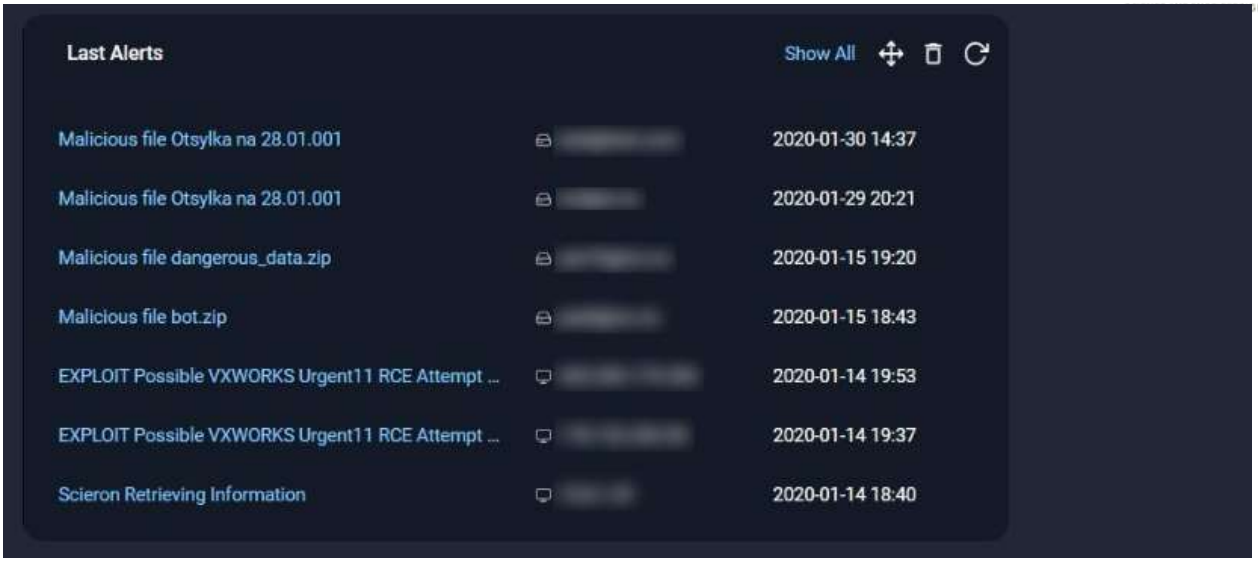
Gambar 3. Tangkapan layar Dashboard

Terdapat appliance *statuses* pada Gambar 4 yang berisikan informasi mengenai *sensor, polygon*, dan *huntbox* dari *client* yang aktif beroperasi sebagai pondasi berjalanya praktik *threat hunting* pada platform ini.



Gambar 4. Informasi pada appliance statuses

Selain itu, *fiture* yang sangat penting dan berisikan informasi mengenai *threat hunting framework* adalah *alerts* pada Gambar 5 yang melaporkan *threats* yang masuk pada infrastruktur dengan menampilkan klasifikasi hingga informasi mendetail mengenai malware yang menyerang pada infrastruktur.

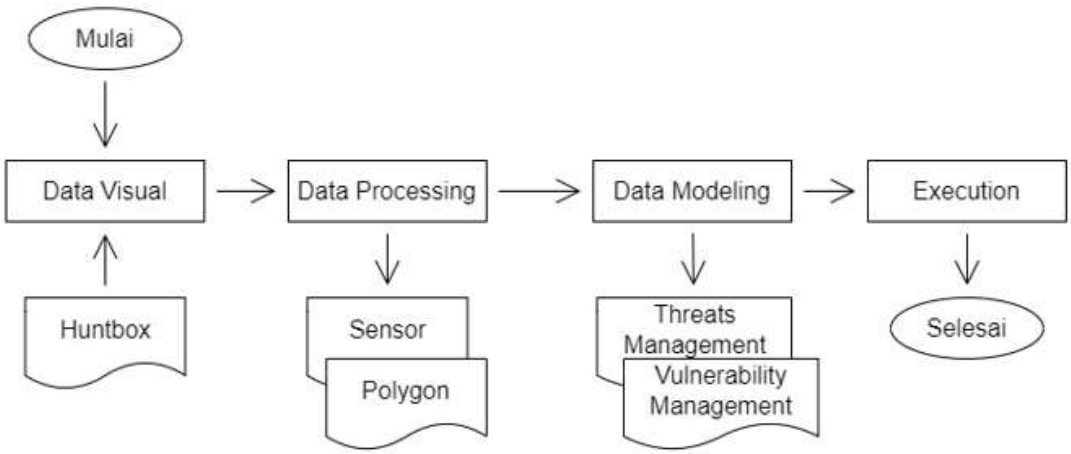


Gambar 5. Malware yang dilaportkan alerts pada infrastruktur yang dilindungi.

Data diatas memuat informasi mengenai infrastruktur yang dilindungi pada *huntbox* yang nantinya data tersebut akan dianalisis dan dilaporkan agar dapat ditindak lanjuti dengan mengklasifikasikan anomali *malware* yang masuk.

Pembangunan Metode Managed, Detection & Response (MDR)

Huntbox dirancang menggunakan metode *Managed, Detection, and Desponse* untuk menghasilkan sebuah metode yang efektif untuk praktik *threat hunting* hingga mempermudah proses *monitoring* pada pusat operasi keamanan, dengan *sensor* dan *polygon* yang juga dirasa dapat mempermudah kinerja. Pada Gambar 6 berikut adalah diagram alir (*flowchart*) dari perancangan pembangunan *Huntbox*.



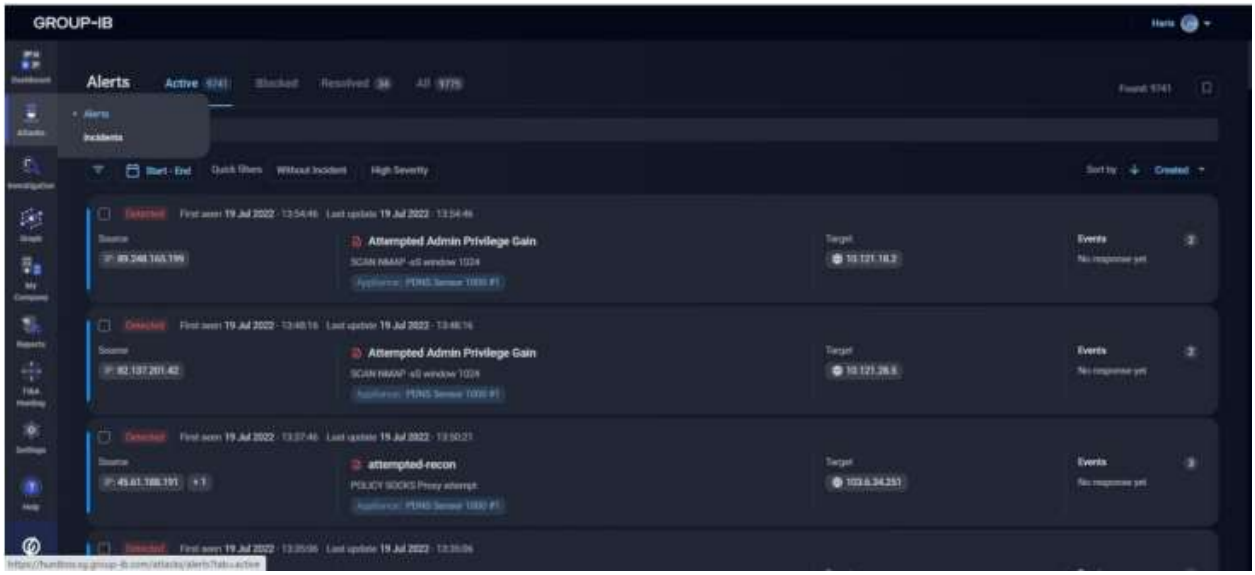
Gambar 6. Flowchart perancangan pembangunan Huntbox

Data Visual menampilkan *Huntbox* dalam bentuk informasi mendetail dari *malware* sehingga data dapat lebih mudah untuk dianalisis yang dihasilkan oleh Data Processing. Sensor bertugas sebagai alat pendeteksi dan mengklasifikasikan *malware*, sedangkan Polygon yang dirancang untuk melakukan pembedahan lebih lanjut dalam ruang terisolasi agar dapat mendeteksi threats melalui anomali yang disebabkan dan terhindar dari infrastruktur yang dilindungi. Data Modeling adalah tahapan paling berpengaruh dalam keberhasilan pembangunan model sistem *Managed, Detection, and Response* yang terdiri

dari *Threats Management* dan *Vulnerability Management.* Setelah menganalisis *malware*, bentuk ancaman yang berupa IP atau *E-mail* yang terjangkit dapat segera diblokir pada web *open source* yang tersedia.

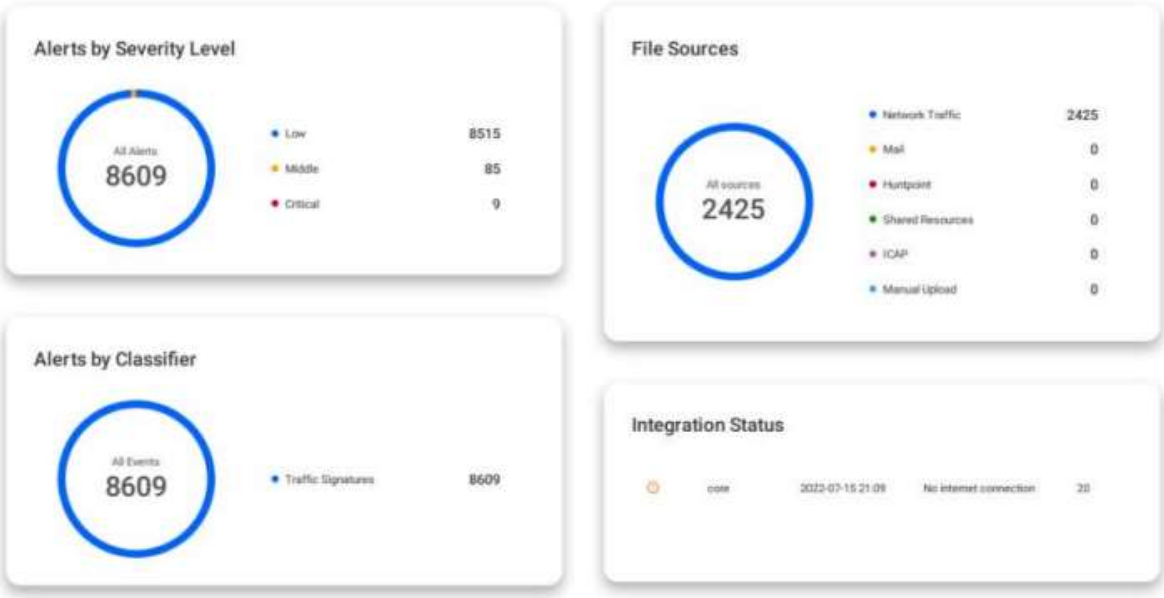
HASIL DAN PEMBAHASAN

Pada proses Data Visual menghasilkan *alerts* yang merupakan tampilan *malware* yang terdeteksi dalam bentuk daftar atau *list* yang mempermudah proses analisis. Gambar 7 menunjukan daftar *malware* yang masuk pada infrastruktur yang dilindungi.



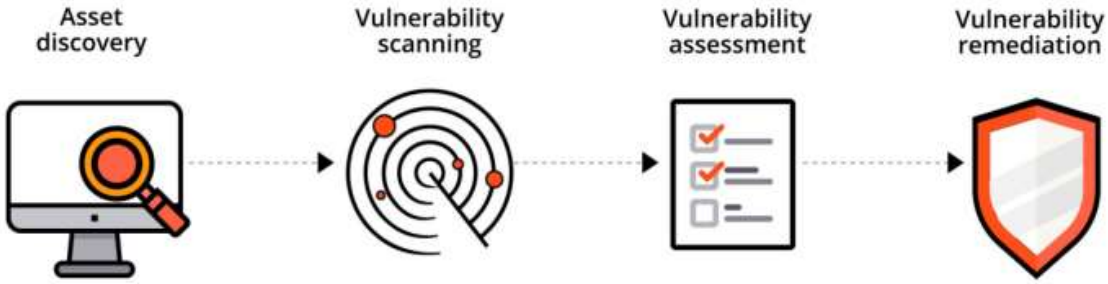
Gambar 7. Daftar malware pada infrastruktur

Gambar 8 menampilkan klasifikasi *malware* pada *alerts* yang dibedakan menjadi 3 berdasarkan anomali yang terdapat pada sumber file dan tingkatan bahaya pada ancaman tersebut, yaitu *Low, Meddle,* dan *Critical.*



Gambar 8. Laporan hasil Klasifikasi malware

Pada proses *Threats and Vulnerability Management* memprioritaskan penguatan keamanan dengan penilaian dan pengujian untuk mencari ancaman yang berdampak pada infrastruktur yang dilindungi. Melakukan pengujian secara stabil pada mekanisme pertahanan dilingkungan pusat operasi keamanan. Gambar 9 adalah tahapan *Vulnerability Management* untuk memanajemen kerentanan infrastruktur yang layak dibutuhkan bagi para tim operasi keamanan yang bertanggung jawab dan menangani ancaman tersebut.



Gambar 9. Tahapan Threats and Vulnerability Management pada Pusat Operasi Keamanan

KESIMPULAN

Dengan adanya metode *Managed, Detection, and Response* menghasilkan *alerts* yang merupakan tampilan *malware* yang terdeteksi dalam bentuk daftar atau *list* yang mempermudah proses analisis, sehingga operasi keamanan pada unit *cyber security* menjadi lebih cepat dan efisien dengan terciptanya sistem yang terintegrasi dengan baik.

SARAN

Berdasarkan hasil pembangunan model *Managed, Detection, and Response,* saran diajukan adalah perlu adanya optimasi yang lebih lanjut terkait belum adanya automatisasi pemblokiran pada sumber yang terdeteksi adanya ancaman pada lingkungan infrastruktur yang dilindungi serta perlu adanya survey lanjutan untuk menentukan fungsi apa saja yang perlu ditambahkan pada saat penerapan dalam *framework* nantinya.

DAFTAR PUSTAKA

AOAC. (2002). Guidelines for single laboratory validation of chemical methods for dietary supplements and botanicals. *AOAC International*, 1–38.

A. Vpn and C. Fireeye, "AKSES VPN, HUNTBOX, Qradar, CarbonBlack dan FireEye".

Cisco and Author, "Network Infrastructure Security Guidance Network Infrastructure Security Guidance Notices and history Disclaimer of warranties and endorsement Trademark recognition Publication information Network Infrastructure Security Guidance," no. March, 2022.

E. I. C. T. Company, "Integrated & End to End ICT Company".

G. T. Hunting and F. Huntbox, "Group-IB Threat Hunting Framework / Huntbox".

J. Antonio, "Introduction".

I. Levy, "Connected Places: Cyber Security Principles," 2021.