Threat Hunting Platform

DATA SHEET

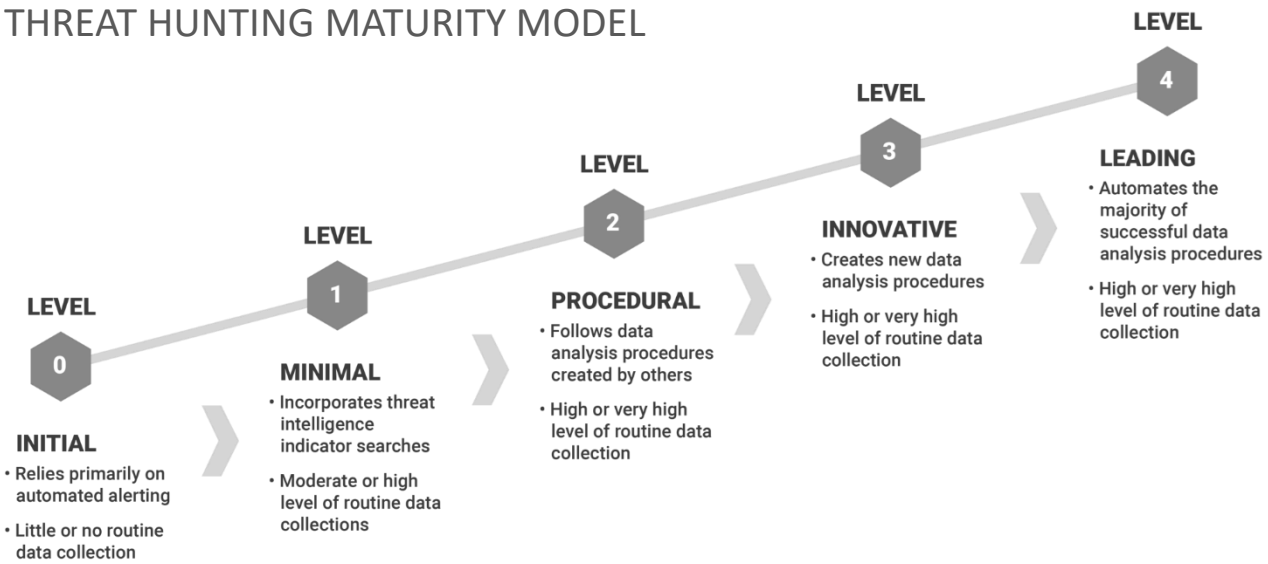
A fully integrated security analytics and automated threat Hunting solution that is based on MITRE ATTACK matrix frameworks in security operations by combining the capabilities of some of the best solutions in their corresponding domain and leveraging the power of automation.

activebytes
innovations

1. About The Threat Hunting

*Cyber Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in an IT Infrastructure. Unlike traditional alert driven method currently being followed by security operations , **Threat hunting is an assumed breach approach**. The new generation security threats and persistent attack tactics can only be detected with such futuristic approach over high fidelity data from the infrastructure which may size way bigger than what current SIEMs are processing now a days.*

THREAT HUNTING MATURITY MODEL



Current Blue Team Challenges

for effective threat hunting

The Quality of data being collected to SIEM for an effective threat hunting. Analyst eventually get stuck while investigating an attack tactic due to lack of enough data from host or network

The Quantity of data when organization decides to collect quality logs from host and network for a better visibility and hunting capability. The scalability openness of SIEM triggers cost for each expansion based on licensing model.

Organization can receive a threat information and Indicators of Compromise from communities, vendors, peers or even from regulatory authorities. **The Knowledge from community** is not getting utilized in the right way.

Skilled Human resource availability is a struggle for all organizations to achieve required level of security. This results under utilized security solutions and undetected threats impacting Business on an unexpected way.

activebytes innovations

2. Our Approach

As the problem needs a brand new approach of a platform combining best in class solutions from security industry with minimal cost to organization. We combine a special formula of multiple solutions which brings up **an ecosystem** of unbeatable capabilities.

1

A **Host sensor** which collects Rich data from hosts or endpoints which can answer what happened inside a host

2

A **Network sensor** which collects Rich data from network which can answer what happened inside a network

3

A **BigData Analytic** Engine with best in class analytics and processing capability satisfies the organization's data analysis needs for future as well.

4

A **Threat Intelligence Platform** Which keeps knowledge of cyber security threats going on in the industry at the moment accessible to both technical and non technical team of Organization

5

All the four components of our platform together brings and ecosystem for Threat hunting. Rich data being collected by network and host sensors are getting stored into our Data lake in a unified format which can process such huge volume of data, enlightens with IOC information from Threat Intelligence platform . This Opens up the capability of

Automation

3. About the components

1 **Host sensor**

- Rich Host data collection for threat hunting and forensic.
- Centralized Host Sensor management through for streamlined agent installation and data collection management.
- Not just OS data from Host, Same agent can collect other log sources like Web server, Firewall, TI Platforms, Cloud solutions and even custom logs which is **Key for easy expansion**
- Minimal Resource utilization and kernel level existence for collecting the best possible host data

activebytes innovations

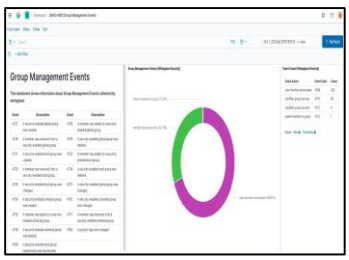
2 Network sensor

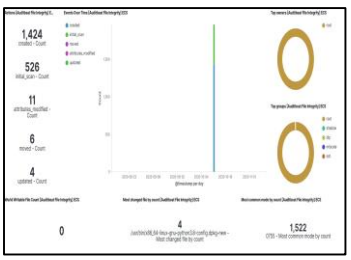
- Rich network data collection and processing of mirrored network traffic for threat hunting and forensic.
- Unlike NDRs which focuses very heavily on traffic going to or coming from the Internet (North-South traffic)as it's looking for signs of communication with command-and-control servers. We gives priority to Specific East-West traffic , like traffic to and from Active Directory –which has significance on detecting new generation cyber attacks.
- These logs include not only a comprehensive record of every connection seen on the wire, but also application-layer transcripts
- Analysis of file content exchanged over application-layer protocols, including MD5/SHA1 computation for fingerprinting.
- 50+ Application Layer Protocol support

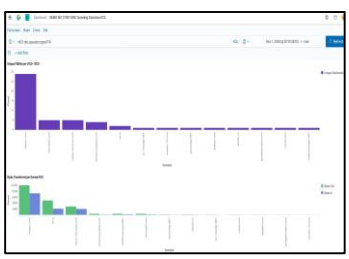
3 S Analytics Engine

- Store large volume of data without any licensing concerns. Even for years
- Look for an IOC occurrence days, weeks ,month or even years back.
- Unmatched data analytics and visualization capabilities.
- Rich infrastructure logs in a single place – Analysts comes with best answer.
- Scalability for future expansions without restrictions.
- An exclusive list of pre-built dashboards for easy understanding.

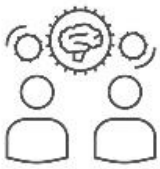
Our dashboards power up your data for both Technical and Non Technical people.







activebytes innovations



4 Threat Intelligence Platform

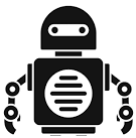
- A Threat intelligence Platform with connected TI Information ingestion from Commercial , Community and Internal trusted sources.
- Contribution for intelligence inputs inside organization by multiple analysts
- An effective way to view all threat intelligence information at a single place
- Capability to Record all type of Indicators
- Co-relation of Same “IOC” from other threat intelligence events.
- APIs and Integration capabilities for Automation.
- Curated intelligence information provided by dedicated analysts
- Add on services like domain take down, dark web and social media monitoring

5 The Idea of Automation

We combined a set of solutions to make an ecosystem for effective automation of threat hunting process. Once the rich data collected by host and network sensors are made available into the data lake along with threat intelligence information in a unified format. It is possible to automate the whole threat hunting process into a workflow.

Eco-System

of structured and organized detailed hunt data



Our Threat Hunting Bot and Playbooks

Automated hunting capability utilizing the whole Security ecosystem

activebytes innovations

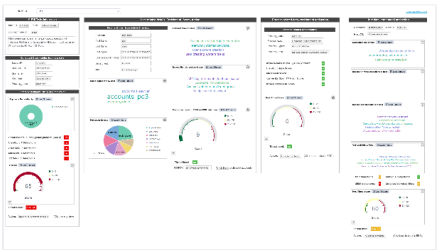
Threat hunting approaches used by Our Bot

1 **Hypothesis-driven investigation:**
Hypothesis-driven investigations are often triggered by a new threat that's been identified through a large pool of attack data, giving insights into attackers' latest tactics, techniques, and procedures (TTP). Once a new TTP has been identified, threat hunters will then look to discover if the attacker's specific behaviors are found in their own environment.

2 **Investigation based on known Indicators of Compromise or Indicators of Attack:**
This approach to threat hunting involves leveraging tactical threat intelligence to catalog known IOCs associated with new threats. These then become triggers that threat hunters use to uncover potential hidden attacks or ongoing malicious activity.

3 **Advanced analytics and machine learning investigations:**
The third approach combines powerful data analysis and machine learning to sift through a massive amount of information in order to detect irregularities that may suggest potential malicious activity. These anomalies become hunting leads that are investigated to identify stealthy threats.

Its not just automation of detection, its everything what a human analyst does, and showing all those information in a single screen



Our Playbooks are not just detecting a threat. They are built to execute end to end investigation, enrichment and incident response actions like a human. Additionally complex use cases which even human cant do .

- What about looking into entire activity of an account in a big infrastructure if that account has been identified as a victim of an attack ?
- What about investigating threat score of every unusual process executed inside a host for a whole day of a threat detection ?
- Do you want to block a bad IP directly on a firewall or just to send a notification to Network Admin when a threat has been confirmed

YES, We've got you covered- Our Bot and playbooks literally does everything and present a full investigation report like a human.

Now, What remains for the team is – Just **DECIDE!!**

activebytes innovations